UNIVERSITE SCIENTIFIQUE ET MEDICALE DE GRENOBLE

Jéomatri

◆◆◆

les groupes dans le premier cycle

I.R.E.M. de GRENOBLE – B.P. 41 – 38402 SAINT MARTIN D'HERES CEDEX

SOMMAIRE

Introduction 5

A — Activités dans une classe : premières propriétés 7

I En regardant une montre 8
II En jouant avec les gobelets 11
III Jouons encore avec les gobelets 16
IV D'autres observations sur les groupes 18
V Quelques réflexions 19
VI Propriétés d'un groupe 19
VII Quelques problèmes 21

B — Activités dans une classe : pour écarter quelques idées fausses 25

I De nouveau l'horloge 25
II Le groupe de Klein 29
III Un groupe non commutatif 34

C — Pour les enseignants 37

1 Les groupes 37

1.1 Lois et opérations 37
1.2 Associativité et compagnie 38
1.3 Monoïdes et groupes 40
1.4 Exemples de groupes non commutatifs 41

2 Que faire avec les groupes ? 43

2.1 Deux propriétés bien utiles 43
2.2 Deux lois sur un même ensemble 44
2.3 Equations 46

Réponses aux questions posées 49

Index terminologique 57

INTRODUCTION

Les groupes sont des objets mathématiques relativement récents : Galois a introduit le mot en 1831, avec un sens voisin de celui que nous lui donnons, et Cayley en a donné la définition moderne en 1854. Par ailleurs, on ne peut guère déceler son existence avant les travaux que Lagrange et Vandermonde ont consacrés à la résolution des équations algébriques dans le dernier quart du 18ème siècle.

Mais en une période aussi courte, ils ont envahi la plupart des domaines mathématiques, ouvrant la voie aux autres structures algébriques qui font partie du matériel de base des mathématiciens (anneaux et corps, espaces vectoriels et algèbres, monoïdes).

Les programmes des collèges de 1971 avaient fait une large place à ces structures, probablement excessives. L'une des critiques faites à cette introduction visait le verbalisme, et il est sûr qu'il n'a pas toujours été épargné aux élèves. Mais une autre critique paraît moins justifiée : il est vrai que, dans le premier cycle, l'usage que l'on peut faire des groupes est modeste ; les outils puissants de la théorie des groupes ne peuvent pas être raisonnablement utilisés. Il nous semble pourtant que ce premier contact avec les groupes apporte beaucoup aux élèves.

Dans la mesure où cette introduction se fait sans formalisme excessif, il est bon de donner une idée de l'un des outils couramment utilisés dans les mathématiques actuelles ; on pourra probablement commencer à faire sentir qu'une structure mathématique est un moyen de mieux comprendre, et plus économiquement parce que de façon organisée et condensée ; il faut naturellement pour cela que cette structure soit illustrée dans des domaines variés.

Mais il se trouve que des groupes divers sont étudiés dans les classes de 4ème et de 3ème. En algèbre, on rencontre les groupes additif ($\mathbb{R}$, +) et multiplicatif ($\mathbb{R}^*$, $\times$), et leurs sous-groupes naturels, avec lesquels les élèves vont beaucoup travailler ; on lira dans les articles des parties A et B des réflexions à ce sujet. Pour prendre une autre illustration algébrique plus marginale, on peut penser qu'un élève

familiarisé, même superficiellement, avec les groupes, n'aura pas trop de mal à assimiler que si p et q sont des entiers (relatifs) et si $a \in \mathbb{R}^*$, alors $a^p a^q = a^{p+q}$.

L'autre domaine où il sera agréable que les élèves aient quelques idées sur les groupes est évidemment la géométrie. Pour des raisons que nous avons développées ailleurs, il nous paraît clair que les transformations (translations, symétries,...) permettent de présenter la géométrie de la façon la plus attrayante et la plus efficace. On comprendra évidemment d'autant mieux ce que sont les transformations que l'on aura pris en compte leur organisation en groupe.

On trouvera dans ce fascicule deux articles qui présentent des activités destinées aux élèves. La plupart de ces activités ont été effectivement utilisées dans les classes et l'on trouvera, surtout dans le premier article, de nombreuses réflexions pédagogiques.

La troisième partie, destinée aux enseignants, présente de façon organisée les propriétés des groupes qui sont effectivement utilisées dans le premier cycle ; de nombreuses questions posées aux lecteurs devraient en rendre la lecture plus active. On trouvera à la fin de cette partie des réponses très détaillées à la quasi totalité des questions posées et, comme il se doit, un index terminologique.

La parution d'un deuxième fascicule est envisagée ; destiné aux enseignants, il serait plus théorique et passerait en revue les propriétés de la plupart des groupes que l'on rencontre dans le premier cycle.

A – Activités dans une classe

PREMIERES PROPRIETES

L'acquisition d'une structure donnée représente une sérieuse économie de pensée : elle introduit une analogie entre des situations qui de premier abord paraissent complétement différentes. Dans ce domaine, le programme de 1971 de la classe de 4ème contenait cet alinéa : «Notion de groupe : définition (on la dégagera des exemples du programme)». Cet alinéa n'a pas été repris dans le libellé du programme de 1978, mais les «exemples du programme» n'ont pas disparu pour autant.

En fait, la structure de groupe apparaît dès la classe de 5ème, même si on ne la dégage pas : $(\mathbb{Z}, +)$, $(\{-1, 1\}, \times)$, peut-être $(\mathcal{P}(E), \Delta)$ avec un ensemble E comportant un petit nombre d'éléments. En classe de 4ème, vont apparaître $(D, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^*, \times)$, le groupe des puissances de 10, le groupe des translations et celui des vecteurs.

Il y a donc largement matière à constater cette analogie entre situations différentes dont nous parlions ci-dessus.

Voici des manipulations qui ont été utilisées pour introduire la notion de groupe en début d'année de 4ème, dans le cadre du programme de 1971. Elles ont été faites en partie, ou en totalité, dans un certain nombre de classes, par exemple en travaux dirigés. Il nous semble qu'elles peuvent être utiles également dans le cadre du programme de 1978.

Ces exercices sont aussi l'occasion d'une première réflexion sur les équations.

Le sujet de ces manipulations – construction de certains groupes finis – ne faisait évidemment pas partie du programme. Elles nous paraissent cependant intéressantes, d'abord parce qu'elles permettent une bonne activité de la classe en début d'année, ensuite parce qu'elles pourront faciliter l'étude des groupes du programme. Enfin les manipulations concernant les gobelets permettent de voir des applications, des bijections, d'introduire la composition des applications et les notations relatives à ces notions. Nous sommes bien là dans le cadre du programme, aussi bien celui de 1978 que celui de 1971.

Ce premier article contient trois parties qui peuvent être lues séparément.

La partie la plus importante (paragraphes I à V) comprend la description de ces manipulations et quelques commentaires sur le contenu et sur les réactions des élèves. Pour en faciliter la lecture, nous avons utilisé deux caractères d'imprimerie différents, l'un pour le texte de l'article et l'autre pour les extraits du texte proposé aux élèves.

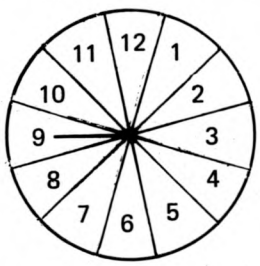
La deuxième partie (paragraphe VI) est un rappel des propriétés des groupes qui reviennent trés souvent dans le premier cycle.

Enfin, nous avons donné trois énoncés de problèmes sur les groupes (paragraphe VII). Nous les avons choisis parce qu'ils étudient des groupes assez différents et aussi parce que le troisième nous a permis quelques commentaires sur les groupes finis. Cela ne signifie évidemment pas que ces problèmes (et à plus forte raison les commentaires) doivent être proposés aux élèves. En particulier le problème 3 est incontestablement difficile.

I – EN REGARDANT UNE MONTRE

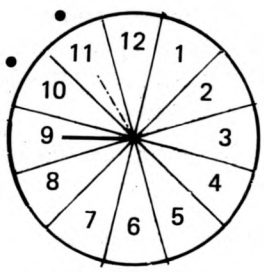
Cette manipulation est une illustration du groupe cyclique à 12 éléments. Voici le début du texte proposé aux élèves.

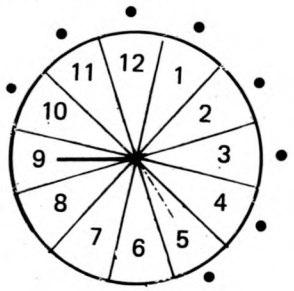
1.1 Imaginons une montre simplifiée dont le cadran ne comporte qu'une seule aiguille, elle indique les heures. Le cadran est gradué comme l'indique le dessin. Nous dirons qu'il est 9 heures si l'aiguille est sur la région numérotée 9.



La montre indique 9 heures.

Quelle heure sera-t-il dans 2 heures ? Dans 8 heures ?





Désignons par H. l'ensemble des nombres écrits sur le cadran :

$$H = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.$$

Ce que nous avons fait est un exemple d'une opération dans l'ensemble H. Nous noterons cette opération par le symbole $\oplus$.

$$9 \oplus 2 = 11,$$
$$9 \oplus 8 = 5.$$

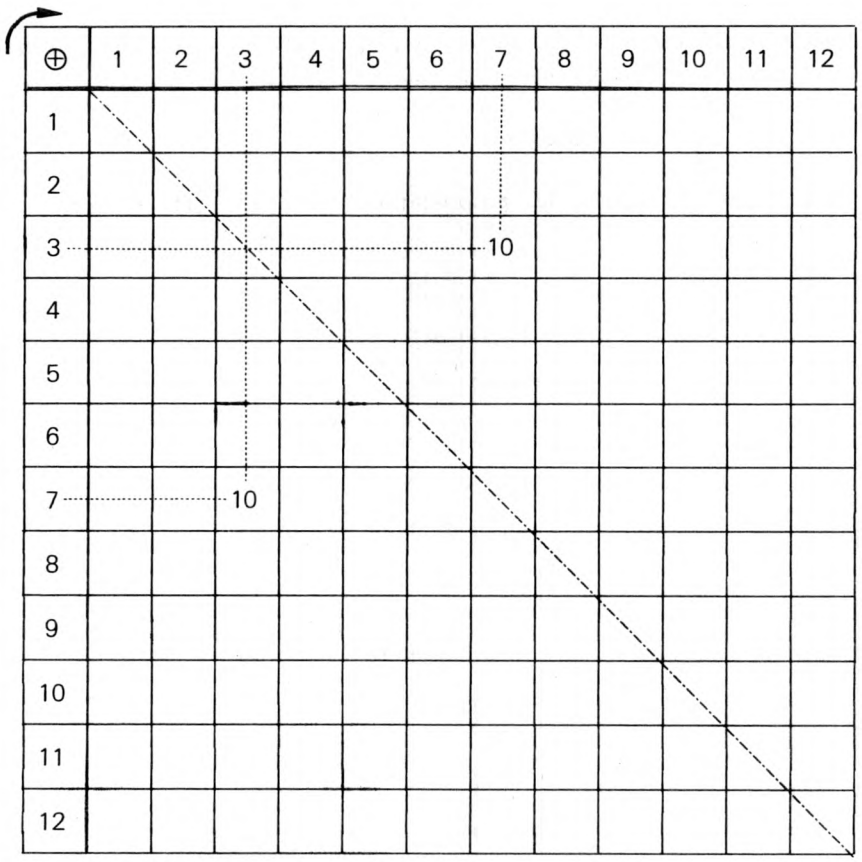
Les élèves peuvent ensuite dresser la table de l'opération $\oplus$, ce qui est l'occasion de préciser les conventions habituelles pour l'élaboration de telles tables. En particulier, les éléments sont rangés dans le même ordre dans la première colonne et dans la première ligne.

1.2 La vérification que 12 est élément neutre et que tout élément a un symétrique est immédiate.

1.3 En ce qui concerne la commutativité, voici comment on peut s'y prendre.

Tu remarques que $7 \oplus 3 = 10$ et $3 \oplus 7 = 10$.

Regarde comment ces deux résultats sont inscrits sur la table.



Tu vois que si tu pliais la feuille de papier autour du trait ponctué, les deux cases correspondant à $7 \oplus 3$ et $3 \oplus 7$ viendraient l'une sur l'autre.

Tu vois, de plus, que dans ces deux cases on a écrit le même résultat : 10.

Les deux cases correspondant à $2 \oplus 9$ ***et*** $9 \oplus 2$ ***viennent-elles aussi l'une sur l'autre ? Contiennent-elles le même résultat ?***

La droite ponctuée est appelée DIAGONALE PRINCIPALE de la table.

On dit que la table est SYMETRIQUE PAR RAPPORT A SA DIAGONALE PRINCIPALE si, dans le pliage autour de cette droite, deux cases qui viennent l'une sur l'autre contiennent le même résultat.

Vérifie que ta table est symétrique par rapport à sa diagonale principale.

On peut ainsi discuter de la question de la commutativité avec les élèves.

1.4 En ce qui concerne l'associativité, les élèves de la classe où j'ai proposé cette manipulation étaient tous plus ou moins capables d'en écrire une définition formelle. Nous avons donc écrit au tableau :

si a, b et c sont des éléments quelconques de H,

$$(a \oplus b) \oplus c = a \oplus (b \oplus c).$$

Puisque nous disposions d'un cas fini, c'était l'occasion de réfléchir sur un énoncé contenant des lettres muettes et nous avons cherché «par quoi on pouvait remplacer a ?» «par quoi on pouvait remplacer b ?» «par quoi on pouvait remplacer c ?».

Il a fallu ensuite un moment pour établir et comprendre que si on voulait démontrer l'associativité de l'opération $\oplus$, il fallait examiner $12 \times 12 \times 12$, soit 1 728 situations. Remarquons qu'il n'a pas été facile de faire accepter à tous que a et b par exemple puissent être remplacés en même temps par le même élément de H.

Nous avons ensuite cherché comment on pouvait réduire le nombre de situations à examiner : cas où figure 12, cas qui se ramènent à un calcul dans $\mathbb{Z}$, utilisation de la commutativité ; mais nous n'avons pas cherché le nombre minimum d'examens nécessaires.

Nous avons ensuite admis la propriété.

1.5 On peut alors récapituler les propriétés du couple $(H,\oplus)$ (et non de H) et proposer des exercices. Par exemple :

Considérons l'égalité suivante,

$$7 \oplus x = 7 \oplus y,$$

où x et y désignent des éléments de H.

Le symétrique de 7 est 5. On peut écrire que

$$5 \oplus (7 \oplus x) = 5 \oplus (7 \oplus y) \ ;$$

comme la loi $\oplus$ est associative, on peut donc écrire que

$$(5 \oplus 7) \oplus x = (5 \oplus 7) \oplus y,$$

et puisque $5 \oplus 7 = 12$,

$$12 \oplus x = 12 \oplus y \ ;$$

comme 12 est élément neutre de la loi $\oplus$,

$$x = y.$$

De l'égalité $7 \oplus x = 7 \oplus y$, nous pouvons donc déduire l'égalité $x = y$.

Forme d'autres exemples analogues.

Il faut donc noter ici que pour les élèves, a priori $x = y$ et que par conséquent il ne voient pas la nécessité d'une telle démonstration. Il serait donc intéressant de fournir l'exemple d'une opération ne possédant pas cette propriété. (Le cas du 0 pour la multiplication risque bien de ne pas les convaincre non plus).

Examinons maintenant l'égalité

$$9 \oplus x = 4,$$

où x désigne un élément de H. On peut écrire que

$$3 \oplus (9 \oplus x) = 3 \oplus 4.$$

Remarque que 3 *est le symétrique de* 9 *; justifie les égalités suivantes :*

$$(3 \oplus 9) \oplus x = 7 \ ;$$
$$12 \oplus x = 7 \ ;$$
$$x = 7.$$

Est-ce que $9 \oplus 7 = 4$ *?*

Tu aurais aussi pu trouver x *à l'aide de ta table ; comment ?*

Remarques.

* Ici, l'utilisation de la table semble plus naturelle. La démonstration ci-dessus est cependant importante puisque nous n'aurons pas d'autres moyens pour résoudre le même problème dans un groupe infini.

* Dans la résolution de l'équation en x dans H

$$9 \oplus x = 4,$$

après avoir montré que si x est solution, nécessairement $x = 7$, il faut établir la réciproque, c'est-à-dire montrer que 7 est une solution du problème posé en vérifiant que $9 \oplus 7 = 4$. Il nous semble prématuré d'expliquer ici aux élèves ce que sont des équations équivalentes. Voyez à ce sujet la deuxième partie, page 28, et la troisième partie, page 40.

1.6 Notion de groupe cyclique.

On peut remarquer que

$5 \oplus 5 = 10$; $5 \oplus 5 \oplus 5 = 3$ et $5 \oplus 5 \oplus 5 \oplus 5 = 8$.

En continuant, on constaterait que tout élément de H peut être obtenu ainsi. On dit que $(H, \oplus)$ est un groupe cyclique, et que 5 engendre H.

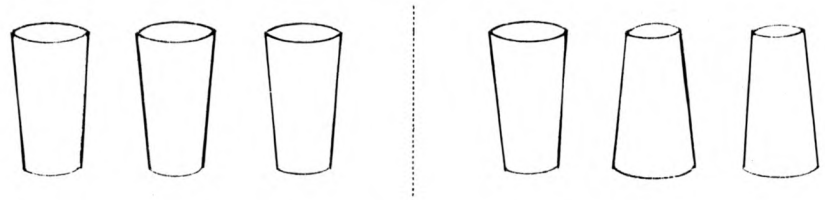
II – JOUONS AVEC DES GOBELETS

Le groupe $(H, \oplus)$ est un groupe commutatif. Voici une manipulation conduisant à un nouveau groupe, non commutatif. (On appelle souvent ce groupe «groupe du triangle équilatéral»).

2.1 *Tu disposes de trois gobelets. Tu peux utiliser trois pots de yaourts vides et identiques, ou bien trois gobelets de distributeur automatique de boissons.*

Tu poses ces trois gobelets sur ta table, en ligne, chacun étant droit ou renversé.

Voici, par exemple, deux dispositions.



Donne toutes les dispositions possibles.

Nous avons donc un ensemble de huit dispositions, que nous noterons E. Nous allons coder ces huit dispositions en utilisant les signes V et Λ. Ainsi les deux dispositions dessinées ci-dessus seront codées VVV et VΛΛ.

Notons que la recherche des 8 dispositions n'a pas été si simple pour tous les élèves, qui ne procèdent évidemment pas de façon systématique.

Pour la suite, nous avons ordonné l'ensemble E pour que tous les élèves donnent les résultats demandés sous la même forme.

2.2 Sur le tableau ci-dessous, nous avons recopié la liste des huit dispositions. Ecris en face de chacune d'elles la disposition obtenue en appliquant la consigne suivante :

«On échange le premier et le troisième gobelets sans toucher au second».

Ainsi, par exemple :

$$\underset{\text{disposition initiale}}{\Lambda VV} \xrightarrow{\text{mise en œuvre de la consigne}} \underset{\text{disposition finale}}{VV\Lambda}$$

Nous avons inscrit ce résultat sur le tableau.

table de	
VVV	
VVΛ	
VΛV	
VΛΛ	
ΛVV	VVΛ
ΛVΛ	
ΛΛV	
ΛΛΛ	

Vérifie qu'à cette consigne nous avons ainsi associé une bijection de E ***dans*** E.

Appelons S cette bijection.

Complète le titre de la table : c'est la table de S.

L'exemple donné ci-dessus peut se noter

$$S : \Lambda VV \longmapsto VV\Lambda,$$

encore

$$S(\Lambda VV) = VV\Lambda.$$

Ecris S(VΛV), ***puis*** S(ΛΛV).

2.3 ***Recommence le même travail sur le tableau ci-dessous avec la consigne suivante :*** «On prend le gobelet de gauche et on le place à droite sans le retourner».

Ainsi, par exemple,

$$\underset{\text{disposition initiale}}{\Lambda\Lambda V} \xrightarrow{\text{application de la consigne}} \underset{\text{disposition finale}}{\Lambda V\Lambda}$$

Nous avons inscrit ce résultat sur le tableau.

table de	
VVV	
VVΛ	
VΛV	
VΛΛ	
ΛVV	
ΛVΛ	
ΛΛV	ΛVΛ
ΛΛΛ	

Vérifie qu'à cette consigne est encore associée une bijection de E ***dans*** E.

Nous l'appellerons D.

Complète le titre de la table. Tu vois que

$$D(\Lambda\Lambda V) = \Lambda V\Lambda.$$

Ecris D(VVV), ***puis*** D(VΛV).

2.4 Nous allons maintenant appliquer successivement la bijection D et la bijection S. Pour cela utilisons le tableau suivant.

D	S	
VVV	VVV	
VVΛ	VΛV	
VΛV	ΛVV	VVΛ
VΛΛ	ΛΛV	
ΛVV	VVΛ	ΛVV
ΛVΛ	VΛΛ	
ΛΛV	ΛVΛ	
ΛΛΛ	ΛΛΛ	

Dans les deux premières colonnes, nous avons recopié la table de la bijection D.
Tu vois que $D(V\Lambda V) = \Lambda VV$.

Sur la table de la bijection S, la disposition ΛVV figure à la 5ème ligne et tu vois que $S(\Lambda VV) = VV\Lambda$. C'est donc ce résultat que nous avons inscrit à la 3ème ligne du tableau.

De même, tu vois que $D(\Lambda VV) = VV\Lambda$.

Sur la table de la bijection S, la disposition VVΛ figure à la 2ème ligne et tu vois que $S(VV\Lambda) = \Lambda VV$. C'est donc ce résultat que nous avons inscrit à la 5ème ligne du tableau.

Fais de même pour les 6 autres éléments de E.

A tout élément de E, tu as associé un élément de E.

Vérifie qu'on a défini ainsi une bijection de E ***dans*** E.

Appelons M cette nouvelle bijection.

Recopie le résultat obtenu sur le tableau suivant.

Table de la bijection M	
VVV	
VVΛ	
VΛV	
VΛΛ	
ΛVV	
ΛVΛ	
ΛΛV	
ΛΛΛ	

Remarque sur la notation.

Nous avons écrit ci-dessus :

$$D(V\Lambda V) = \Lambda VV, \quad S(\Lambda VV) = VV\Lambda.$$

Nous pouvons donc écrire :

$$S[\,D(V\Lambda V)\,] = VV\Lambda.$$

Vérifie que les égalités suivantes sont vraies :

$$D(\Lambda VV) = VV\Lambda,$$
$$S(VV\Lambda) = \Lambda VV,$$
$$S[\,D(\Lambda VV)\,] = \Lambda VV.$$

A tout élément x de E, on a donc associé par une bijection un élément de E, qui est S [D(x)].

Nous noterons cette bijection S ∘ D. Ainsi,

$$S \circ D(V\Lambda V) = VV\Lambda :$$

$$VV\Lambda \xleftarrow{S} \Lambda VV \xleftarrow{D} V\Lambda V$$

$$VV\Lambda \xleftarrow{S \circ D} V\Lambda V.$$

Nous avons noté M la bijection S ∘ D.

La lecture de ces notations a évidemment demandé un certain temps. Par contre la notation S ∘ D pour la composée des applications D et S a été bien acceptée et en général utilisée convenablement pendant le reste de l'année.

2.5 On procédera de même pour établir la table des bijections

$$D \circ S \quad ; \quad S \circ S \quad \text{et} \quad D \circ D$$

qu'on notera respectivement N, I et L, après avoir fait constater que $D \circ S \neq S \circ D$.

On demandera aux élèves à quelle consigne simplifiée est associée la bijection I. Cette consigne, qu'on peut écrire

«on ne touche pas les gobelets»

est évidemment sans intérêt pratique ; mais la bijection associée, qu'on pourra appeler application identique sur E, est indispensable comme élément neutre de la loi ∘.

A cette étape, les élèves peuvent dire ce que sont les bijections :

I ∘ I, S ∘ I, I ∘ S, D ∘ I, I ∘ D, M ∘ I, I ∘ M, N ∘ I, I ∘ N, L ∘ I, I ∘ L.

Remarques.

1. Trop souvent, dans des présentations de groupes finis à l'aide de manipulations, on trouve des confusions fâcheuses entre situations (ici les 8 dispositions des gobelets), consignes de passage d'une situation à une autre et bijections associées. Nous les avons soigneusement distinguées.

2. Pour définir une bijection, il faut connaître les images par celle-ci des 8 dispositions. C'est une tâche très longue et difficile à organiser. C'est pourquoi, pour ne pas perdre trop de temps, nous avons été très directifs sur la méthode.

En procédant de cette façon, et en partageant le travail dans la classe pour les 3 bijections D ∘ S, S ∘ S et D ∘ D, il a été possible d'obtenir les six tables sans trop de difficultés et en un temps raisonnable (une séance).

2.6 Les élèves possèdent maintenant les tables des 6 bijections S, D, M, N, I et L et un certain nombre de résultats. Il s'agit maintenant de construire la table de l'opération ∘ sur l'ensemble G de ces bijections. On peut continuer comme suit.

Dans les paragraphes précédents, nous avons étudié l'ensemble E des 8 dispositions de 3 gobelets, et nous avons défini 6 bijections de E dans E : I, D, L, S, N et M. Notons G l'ensemble {I, D, L, S, N, M}.

Tu as dressé la table de ces 6 bijections.

Regarde le tableau suivant.

∘	I	D	L	S	N	M
I						
D				N		
L						
S						
N						
M						

Nous avons noté la bijection D ∘ S. On lit D dans la colonne de gauche et S dans la ligne du haut. Le résultat N est lu en face des deux lettres précédentes.

Nous connaissons d'autres résultats. Reportons-les sur le tableau.

∘	I	D	L	S	N	M
I	I	D	L	S	N	M
D	D	L		N		
L	L					
S	S	M		I		
N	N					
M	M					

Pour remplir les 21 cases qui restent, vous allez vous partager le travail dans la classe, de façon bien sûr à avoir tous les résultats nécessaires mais aussi à pouvoir contrôler ces résultats.

Par exemple, chacun d'entre vous peut calculer deux résultats. Pour cela, tu peux utiliser les 2 tableaux ci-dessous.

VVV		
VVΛ		
VΛV		
VΛΛ		
ΛVV		
ΛVΛ		
ΛΛV		
ΛΛΛ		

VVV		
VVΛ		
VΛV		
VΛΛ		
ΛVV		
ΛVΛ		
ΛΛV		
ΛΛΛ		

Là encore, nous avons proposé une organisation de la classe pour éviter que la construction de la table ne prenne trop de temps. Chaque élève a été ainsi amené à remplir deux tableaux de composition de 2 bijections. Le nombre des élèves de la classe a permis que chaque tableau soit calculé trois fois. Cela a permis un contrôle bien nécessaire : plusieurs élèves (un tiers de la classe environ) n'avait pas très bien compris le mécanisme de ces compositions.

Cette construction de la table de l'opération a occupé une séance complète. Voici cette table.

$\circ$	I	D	L	S	N	M
I	I	D	L	S	N	M
D	D	L	I	N	M	S
L	L	I	D	M	S	N
S	S	M	N	I	L	D
N	N	S	M	D	I	L
M	M	N	S	L	D	I

2.7 On a maintenant tout ce qui est nécessaire pour établir que $(G, \circ)$ est un groupe, non commutatif, avec la même réserve que pour $(H, \oplus)$ en ce qui concerne l'associativité, à moins que les élèves ne sachent déjà que la composition des applications est associative !

2.8 On peut, à la suite, proposer des exercices d'application. Par exemple :

Simplifie les écritures suivantes :

$$D \circ D \circ D \circ S \circ D \ ;$$
$$(D \circ S) \circ (S \circ D) \circ D \ ;$$
$$D \circ (D \circ D) \circ (D \circ S) \circ (S \circ D \circ S) \circ D.$$

Pour chacune des égalités suivantes, détermine l'ensemble des bijections X *pour lesquelles l'égalité est vérifiée.*

$$D \circ X = S \ ;$$
$$L \circ X \circ M = D \ ;$$
$$X \circ X = I \ ;$$
$$X \circ X = D.$$

On remarquera utilement que si la dernière équation n'admet qu'une solution, la troisième en a quatre. Bonne occasion de rappeler que ce n'est pas pour cela que la question est «indéterminée».

Pour résoudre ces équations, les élèves utilisent la table plutôt que de faire le raisonnement du paragraphe 1.5. C'est peut-être pour cela qu'ils n'hésitent pas à proposer un ensemble à 4 éléments comme réponse à la troisième équation.

III – JOUONS ENCORE AVEC DES GOBELETS

En utilisant toujours les 3 gobelets, l'ensemble des 8 positions et des consignes de passage d'une position à une autre, on peut construire un autre groupe de 6 bijections de la manière suivante.

On prend les bijections I, D et L de l'exercice précédent.

On associe une bihection R à la consigne

«on retourne tous les gobelets sans les changer de place».

On convient que $R \circ D = A$ et $A \circ D = C$.

Notons G_1 l'ensemble $\{I, D, L, R, A, C\}$; il est formé de 6 éléments distincts et l'on peut vérifier que $(G_1, \circ)$ est un groupe.

Voici la table de ce nouveau groupe.

$\circ$	I	C	D	R	L	A
I	I	C	D	R	L	A
C	C	D	R	L	A	I
D	D	R	L	A	I	C
R	R	L	A	I	C	D
L	L	A	I	C	D	R
A	A	I	C	D	R	L

C'est une illustration du groupe cyclique à 6 éléments. Il est commutatif.

Bien entendu si on a fait l'exercice précédent, on pourra en utiliser les résultats et aussi ne pas faire toutes les vérifications nécessaires pour ne pas perdre trop de temps et ne pas lasser les élèves.

Voici des exercices sur $(G_1, \circ)$.

Simplifie les écritures suivantes :

$D \circ R \circ A \circ L \circ D$; $D \circ D \circ D$;
$D \circ D \circ D \circ D \circ D \circ D \circ D$; $A \circ A \circ A \circ A \circ A \circ A \circ A$;
$(A \circ L) \circ C \circ (D \circ L)$; $(A \circ L) \circ (A \circ L) \circ (A \circ L)$.

Résous les équations en X *suivantes dans* G_1 :

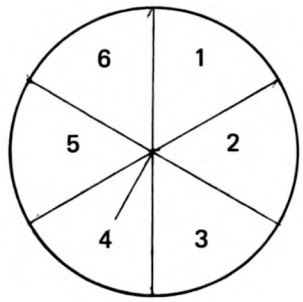
$A \circ X = R$; $C \circ X = D$;
$A \circ X \circ L = R$; $X \circ X = I$;
$C \circ X = D \circ X \circ R$.

On remarquera que l'ensemble des solutions de la dernière équation est l'ensemble vide. Bonne occasion de rappeler que ce n'est pas parce qu'une question est posée qu'elle admet toujours le même type de réponse. Ce n'est pas pour cela non plus que la question est «impossible».

Cette dernière équation a beaucoup inquiété les élèves. Ils n'ont pas proposé de solution mais avec semble-t-il l'idée que s'ils ne trouvaient pas de solution, c'est qu'ils ne savaient pas faire. Aucun n'a cherché de lui-même à démontrer qu'effectivement l'ensemble des solutions de cette équation est vide.

IV – D'AUTRES OBSERVATIONS SUR LES GROUPES

4.1 A l'aide d'une montre simplifiée,



on peut construire un nouveau groupe $(P, \oplus)$ comme il a été fait au paragraphe I.

On fera constater aux élèves que le groupe $(G_1, \circ)$ et le groupe $(P, \oplus)$ sont isomorphes. On n'est pas du tout obligé d'utiliser ce vocabulaire et on peut simplement s'y prendre comme ci-dessous.

L'ensemble P comporte six éléments, tout comme l'ensemble G_1 du paragraphe précédent. Définissons une bijection de G_1 dans P de la façon suivante :

$$I \longmapsto 6 \qquad R \longmapsto 3$$
$$C \longmapsto 5 \qquad L \longmapsto 2$$
$$D \longmapsto 4 \qquad A \longmapsto 1.$$

Prends un calque de la table du groupe $(P, +)$ *et pose-le sur la table du groupe* $(G_1, \circ)$.

Que constates-tu pour deux éléments superposés ?

4.2 Des tables des groupes $(P, \oplus)$, $(G_1, \circ)$ et $(G, \circ)$ on peut tirer les extraits suivants.

$\oplus$	6	4	2
6	6	4	2
4	4	2	6
2	2	6	4

$(P, \oplus)$

$\circ$	I	D	L
I	I	D	L
D	D	L	I
L	L	I	D

$(G_1, \circ)$

$\circ$	I	D	L
I	I	D	L
D	D	L	I
L	L	I	D

$(G, \circ)$

On remarque que les 2 derniers extraits sont identiques.

En convenant que $P' = \{6, 4, 2\}$ et $G' = \{I, D, L\}$, on vérifie aisèment que :

– $(P', +)$ et $(G', \circ)$ sont des groupes commutatifs isomorphes,

– $(G', \circ)$ est un sous-groupe commutatif d'un groupe non commutatif.

V – QUELQUES REFLEXIONS

J'ai personnellement fait faire tous ces exercices et manipulations dans une classe de 4ème en début d'année, et j'y ai consacré 8 heures de travaux dirigés. Cela a donné des séances très animées où, je crois, les élèves ne se sont pas ennuyés et où, dans une certaine mesure, ils ont commencé à apprendre à collaborer.

Quant à savoir ce qu'ils en ont tiré, c'est évidemment très difficile à évaluer. Ce que je peux dire cependant, c'est que pendant le reste de l'année :

– il leur semblait normal qu'on essaie de rapprocher une situation nouvelle d'une situation déjà étudiée ;

– ils savaient que dès qu'on a établi qu'un ensemble muni d'une opération interne vérifie les axiomes de groupe, il en découle automatiquement un certain nombre de propriétés et par exemple l'étude parallèle des groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$, ou du groupe des translations et de celui des vecteurs du plan, a semblé très facile ;

– plusieurs élèves ont pris l'habitude de rechercher la propriété des opérations à utiliser lorsqu'ils hésitent dans un calcul. Cette habitude d'autocontrôle n'empêche malheureusement pas les erreurs de calcul numérique, ou les erreurs dues à une mauvaise maîtrise des règles de priorité dans l'écriture des opérations ;

– en ce qui concerne les applications, ce qui continuait à poser problème, même en fin d'année, ce n'est pas la notation $f \circ g$, mais bien la notion même d'application sur des ensembles non finis, et surtout l'utilisation de lettres muettes lorsqu'on définit de telles applications, notamment en géométrie.

Bien entendu, ces résultats peuvent être obtenus par d'autres moyens que les manipulations proposées ici. Je laisse donc au lecteur le soin de décider si 8 heures de travaux dirigés, c'est payer trop cher l'introduction de la notion de groupe.

De toute façon, il doit être possible, en utilisant quelques une de ces idées (ou d'autres), de faire un travail utile dans un temps estimé raisonnable.

VI – PROPRIETES D'UN GROUPE

Nous avons dit au début de cet article que la notion de structure permettait de rapprocher des situations apparemment très différentes. Or il se trouve qu'en 5ème, et surtout en 4ème, trois propriétés, conséquences de la structure de groupe, reviennent très souvent. C'est l'occasion de faire ce rapprochement.

Rappelons et démontrons ces trois propriétés.

Dans tout ce qui suit, $(G, *)$ est un groupe, e l'élément neutre de ce groupe, a, b, c et x sont des éléments de G et a', b' et c' sont les symétriques de a, b et c pour l'opération $*$.

Dans les démonstrations ci-dessous, nous laissons au lecteur le soin de justifier toutes les égalités écrites.

6.1 Si $a * c = b * c$ alors $(a * c) * c' = (b * c) * c'$;

$$(a * c) * c' = a * (c * c') \quad \text{et} \quad (b * c) * c' = b * (c * c') \ ;$$
$$a * (c * c') = a * e \quad \text{et} \quad b * (c * c') = b * e \ ;$$
$$a * e = a \quad \text{et} \quad b * e = b .$$

Donc, quels que soient les éléments a, b et c de G,

$$\text{si } a * c = b * c, \quad \text{alors} \quad a = b.$$

On dit que c est régulier pour l'opération $*$.

Cette propriété est utilisée très souvent, notamment dans les groupes $(\mathbb{R}, +)$ et $(\mathbb{R}^*, \times)$.

On peut remarquer que des lois qui ne sont pas des lois de groupe peuvent être régulières. Il en est ainsi par exemple de l'addition dans $\mathbb{N}$.

Remarquons également que la propriété réciproque

« si $a = b$ alors $a * c = b * c$ »

n'est pas une propriété de la structure de groupe : en effet, si $a = b$, $a * c$ et $b * c$ sont deux écritures du même objet. Nous reviendrons sur cette question plus loin (page 43.

6.2
$$(a * b) * (b' * a') = ((a * b) * b') * a' ;$$
$$((a * b) * b') * a' = (a * (b * b')) * a' ;$$
$$(a * (b * b')) * a' = (a * e) * a' ;$$
$$(a * e) * a' = a * a' ;$$
$$a * a' = e ;$$

donc
$$(a * b) * (b' * a') = e.$$

Nous avons montré que quels que soient les éléments a et b de G,

$$(a * b)' = b' * a'.$$

Si le groupe $(G, *)$ est commutatif, on peut évidemment écrire que

$$\text{aussi } (a * b)' = a' * b'.$$

On rencontre également plusieurs fois cette propriété dans la classe de 4ème.

- Dans $(\mathbb{R}, +)$: $-(a + b) = (-a) + (-b)$.
- Dans $(\mathbb{R}^*, \times)$: $\frac{1}{ab} = \frac{1}{a} \times \frac{1}{b}$.
- Dans l'ensemble des puissance de 10 : $(10^n \times 10^p)^{-1} = 10^{-n} \times 10^{-p}$.
- Mais aussi dans l'ensemble des bijections d'un ensemble sur lui-même : $(f \circ g)^{-1} = g^{-1} \circ f^{-1}$.

6.3 Si $b * x = a$ alors $b' * (b * x) = b' * a$,
$$b' * (b * x) = (b' * b) * x ,$$
$$(b' * b) * x = e * x ,$$
$$e * x = x.$$

Donc, quels que soient les éléments a, b et x de G,

si $b * x = a$, alors $x = b' * a$.

Nous avons montré que s'il existe un nombre x tel que $b * x = a$ ce nombre est nécessairement $b' * a$.

Mais
$$b * (b' * a) = (b * b') * a,$$
$$(b * b') * a = e * a,$$
$$e * a = a,$$

donc
$$b * (b' * a) = a.$$

Nous avons montré qu'il existe un nombre x tel que $b * x = a$; ce nombre est $b' * a$.

En conclusion, l'équation sur G

$$b * x = a$$

admet une solution unique, et cette solution est $b' * a$.

Si le groupe est commutatif, on peut noter cette solution $a * b'$.

Si le groupe n'est pas commutatif, on peut étudier l'équation $x * b = a$ dont la solution unique est $a * b'$.

Cette propriété permet évidemment de résoudre les équations sur $(\mathbb{R}, +)$ du type $b + x = a$ ou sur $(\mathbb{R}^*, \times)$ du type $bx = a$ mais tout aussi bien les équations du type $r \circ x = t$ sur l'ensemble des translations, l'équation $7 + x = 2$ dans $\mathbb{Z}/8\mathbb{Z}$, etc...

Insistons une nouvelle fois sur l'intérêt de ces rapprochements : c'est bien là l'économie de pensée dont nous parlions tout au début.

VII – QUELQUES PROBLEMES

7.1 Tu sais que $(\mathbb{Z}, +)$ est un groupe commutatif. Nous pouvons nous demander s'il existe des parties de $\mathbb{Z}$ qui possèdent aussi cette qualité vis-à-vis de l'addition.

1. Désignons par P l'ensemble des entiers relatifs pairs : dire que $x \in P$, c'est dire qu'il existe un entier relatif k tel que $x = 2k$.
Ainsi par exemple 14 et -6 sont pairs, car $14 = 2 \times 7$ et $-6 = 2 \times (-3)$.

La somme de deux nombres de P *est-elle un nombre de* P *?*
Le nombre 0 *est-il élément de* P *?*
L'opposé d'un nombre de P *est-il un nombre de* P *?*

2. *Justifie l'affirmation suivante :*

$(P, +)$ est un groupe commutatif.

3. Désignons par I l'ensemble des entiers relatifs impairs : dire que y est un élément de I, c'est dire qu'il existe un entier relatif n tel que $y = 2n + 1$.
Ainsi par exemple 15, 1 et -11 sont impairs car
$15 = 2 \times 7 + 1$, $1 = 2 \times 0 + 1$ et $-11 = 2 \times (-6) + 1$.

Explique pourquoi on ne peut pas dire que $(I, +)$ *est un groupe.*

4. Désignons par T l'ensemble des entiers relatifs multiples de 3 : dire que $z \in T$, c'est dire qu'il existe un entier relatif m tel que $z = 3m$.
Ainsi par exemple 12, -6 et 0 sont des éléments de T car
$12 = 3 \times 4$, $-6 = 3 \times (-2)$ et $0 = 3 \times 0$.

Justifie l'affirmation suivante :

$(T, +)$ est un groupe commutatif.

5. *Essaie d'imaginer une partie* A *de* $\mathbb{Z}$ *telle que* $(A, +)$ *soit un groupe commutatif.*

Remarque.

Les groupes $(P, +)$ et $(T, +)$ sont isomorphes à $(\mathbb{Z}, +)$.
De façon générale, si m est un entier non nul et si l'on désigne par M l'ensemble des multiples de m, alors M est un sous-groupe de $(\mathbb{Z}, +)$, et $(M, +)$ est isomorphe à $(\mathbb{Z}, +)$. A l'exception de $\{0\}$ (qui est d'ailleurs l'ensemble des multiples de 0), tous les sous-groupes de $(\mathbb{Z}, +)$ sont de cette forme.

7.2 Dans l'ensemble $\mathbb{Z}$ des entiers relatifs, on définit l'opération $*$ par

$$a * b = a + b - 2.$$

Par exemple, $(-3) * 1 = (-3) + 1 - 2 = -4$.

1. ***Calcule*** $5 * 0$, $0 * 5$, $6 * 2$ ***et*** $(-8) * 2$.

2. Soit a et b deux entiers.

Calcule $a * b$, ***puis*** $b * a$; ***conclus.***

3. ***Calcule*** $(2 * 5) * 3$, ***puis*** $2 * (5 * 3)$.

Soit a, b et c trois entiers relatifs.

Calcule $a * b$, ***puis*** $(a * b) * c$;
Calcule $b * c$, ***puis*** $a * (b * c)$. ***Conclus.***

4. ***Montre que le nombre*** 2 ***est élément neutre pour l'opération*** $*$.

5. Soit a un entier relatif.

Montre que le nombre $4 - a$ ***est symétrique de*** a ***pour l'opération*** $*$.

6. ***Que peux-tu conclure pour*** $(\mathbb{Z}, *)$ ***?***

Remarque.

Le groupe $(\mathbb{Z}, +)$ est isomorphe à $(\mathbb{Z}, *)$; voici l'un des deux isomorphismes de $(\mathbb{Z}, +)$ vers $(\mathbb{Z}, *)$:

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z} \\ n & \longmapsto & n+2 \end{array} .$$

7.3 Voici la table du groupe $(P', \oplus)$ que tu as déjà étudié.

$\oplus$	6	4	2
6	6	4	2
4	4	2	6
2	2	6	4

Ce groupe a 3 éléments. Tu as étudié deux autres groupes à 3 éléments, et les tables de tous ces groupes étaient «superposables».

Tu vas montrer qu'il en est de même pour tous les groupes à trois éléments.

Soit a, b et c trois éléments distincts ; notons A l'ensemble $\{a, b, c\}$. Supposons que $\bullet$ soit une opération sur A telle que

– $(A, \bullet)$ soit un groupe,
– a soit l'élément neutre de cette loi.

1. ***Justifie les résultats portés dans la table suivante.***

$\bullet$	a	b	c
a	a	b	c
b	b		
c	c		

2. *Est-il possible que* $b \bullet b = b$ *?*

3. Supposons que $b \bullet b = a$.

Serait-il alors possible que $b \bullet c = a$ *?* $b \bullet c = b$ *?* $b \bullet c = c$ *?*

4. *Justifie l'égalité suivante :*

$$b \bullet b = c.$$

Recopie et complète la table de la question 1 *(tu pourras étudier successivement* $b \bullet c$, $c \bullet b$ *puis* $c \bullet c$*).*

Peux-tu affirmer que la table ainsi complétée est une table de groupe ?

5. *Vérifie que la bijection définie par* $6 \longmapsto a$, $4 \longmapsto b$ *et* $2 \longmapsto c$ *permet de «superposer» cette table et celle du groupe* $(P', +)$. *Conclus.*

Remarque.

Cet exercice est très difficile : il repose sur un raisonnement par l'absurde.

A la question 4, or peut affirmer que si $(A, \bullet)$ est un groupe dont a est l'élément neutre, la loi $\bullet$ est nécessairement donnée par le tableau. Mais on n'a pas encore montré que cette condition est suffisante ; on peut le faire soit directement, soit en utilisant la question 5.

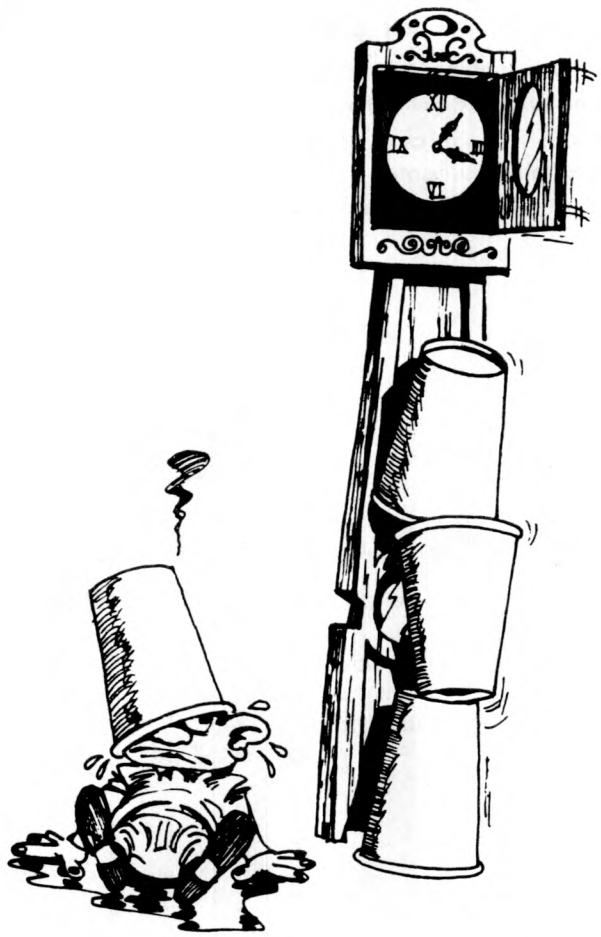
Les questions 2, 3 et 4 reposent sur le fait qu'une loi de groupe est régulière : un élément figure une et une seule fois dans chaque ligne et chaque colonne.

Autrement dit, un groupe est un carré latin. (Voyez page 48). Mais la réciproque est fausse, comme le montrent les deux tables suivantes, qui sont des tables de carrés latin, mais non de groupe (les éléments a, b, c, d et e sont supposés distincts) :

$\perp$	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

$\top$	a	b	c	d	e
a	a	b	c	d	e
b	b	a	d	e	c
c	c	e	a	b	d
d	d	c	e	a	b
e	e	d	b	c	a

en effet, pour la première loi, on constate par exemple que $(b \perp a) \perp c = c \perp c = a$, $b \perp (a \perp c) = b \perp c = b$ et $a \neq b$ (le fait que $(a \perp b) \perp c = a \perp (b \perp c)$ ou $(a \perp a) \perp b = a \perp (a \perp b)$ ne change évidemment rien à la conclusion) ; pour la seconde loi, on constate par exemple que $(d \top c) \top b = e \top b = d$, $d \top (c \top b) = d \top e = b$ et $d \neq b$. On peut remarquer que la loi $\perp$ n'a pas d'élément neutre et que la loi $\top$ en a un (l'élément a).


XII
IX
III
VI

B – Activités dans une classe

POUR ECARTER QUELQUES IDEES FAUSSES

Dans l'article précédent, le lecteur a trouvé un exposé des raisons qui justifient à nos yeux des séances de travail sur les groupes en classe de 4ème ou de 3ème, aussi bien dans le cadre des programmes de 1978 que dans celui du programme de 1971.

L'élaboration progressive d'une structure, même si elle n'est qu'imparfaitement maîtrisée, nous semble être un objectif important, sinon essentiel, pour le premier cycle.

Tout professeur qui aura proposé des exercices simples et concrets sur les groupes à ses élèves sera récompensé par le simple fait d'entendre dire «c'est pareil». Cette expression, dans le langage des élèves, signifie bien une reconnaissance diffuse, mais réelle, de la structure sous-jacente et éventuellement d'un isomorphisme.

Nous sommes convaincus qu'en exploitant ce thème, nous donnons vraiment à l'élève l'occasion et les moyens de « construire son savoir ».

Voici donc d'autres manipulations et exercices sur les groupes, utilisables dans une classe de 4ème. Le lecteur pourra nous reprocher de ne pas proposer d'exemples « géométriques » (toutefois, au chapitre III on rencontrera un déguisement bien transparent du groupe du rectangle). Les manipulations, absolument indispensables, deviennent alors longues et par suite incompatibles avec les programmes et horaires de 4ème et 3ème. Nous suggérons d'effectuer à la fin de la classe de 5ème des séances de travail dirigé sur les groupes de frises et sur les groupes de pavages du plan.

I – DE NOUVEAU L'HORLOGE

Dans l'article précédent, le problème de la régularité a été évoqué (page 19)

Voici maintenant un exemple d'opération qui n'est pas régulière ; on garde pour cet exemple le même ensemble $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, noté ici encore H. L'opération $\oplus$ sur H a été définie page 8 (c'est l'«addition» des horloges).

1. On trouvera d'abord de nouvelles équations dans H, sous une forme un peu différente.

1.1 Egalités et équations.

Examinons les phrases suivantes.

1. $5 \oplus 8 = 1$: elle est vraie.
2. $3 \oplus 6 = 10$: elle est fausse.

3. $\square \oplus 3 = 2$: elle est vraie si à la place de $\square$ on met 11.

Vérifie sur la table que 11 ***est le seul élément de*** H ***qui convient.***

L'énoncé 3 pose une question : «quel nombre ou quels nombres peut-on écrire à la place du symbole $\square$ pour que la phrase obtenue soit vraie».

On appelle cette question une EQUATION. On dit que 11 est une SOLUTION de cette équation. Tu as constaté que c'est la seule.

Les équations suivantes ont-elles une solution ? En ont-elles plusieurs ?

4. $8 \oplus \square = 5$; 5. $\square \oplus \square = 10$;

6. $\square \oplus \square = 3$; 7. $12 \oplus \Delta = \Delta$.

En général, au lieu de symboles comme $\square$, Δ, ... on emploie des lettres. Lorsqu'on dit : « résous l'équation en x dans H suivante : $8 \oplus x = 5$ », cela signifie : « trouve l'ensemble des solutions de cette équation ». Tu as vu que cette équation a une est une seule solution qui est 9. L'ensemble des solutions de cette équation est donc $\{9\}$.

Il se peut que l'ensemble des solutions d'une équation soit vide ; c'est le cas de l'équation 6 ci-dessus.

Il est assez naturel, chez de jeunes élèves à qui l'on vient de faire découvrir une nouveauté, de voir ensuite cette nouveauté partout. Il est donc très utile, sur le plan pédagogique, de donner très vite un exemple de « non groupe » ; c'est ce qui a été fait ci-dessous avec la loi $\otimes$ dans H.

Il faut frapper l'imagination de l'élève :

- **tout ensemble, muni d'une loi interne, n'est pas nécessairement un groupe ;**
- **à partir du moment où le couple (E, $*$) n'est pas un groupe tout peut arriver en ce qui concerne les équations.**

2. Une autre opération dans H.

2.1 Tu sais que $2 \times 10 = 20$, le nombre du cadran qui correspond à 20 heures est 8, car 20 heures cela fait un tour de cadran, et il reste 8 heures.

A 2 et 10 on peut ainsi faire correspondre un nombre du cadran, le nombre 8. Nous écrirons que $2 \otimes 10 = 8$.

De même, $9 \times 7 = 63$; cela fait 5 tours de cadran et il reste 3. Nous écrirons que $9 \otimes 7 = 3$.

Tu sais que $6 \times 8 = 48$; cela fait 4 tours de cadran et il reste 0. Le nombre qui correspond à 0 sur le cadran est 12 : nous écrirons que $6 \otimes 8 = 12$.

Trouve les nombres $8 \otimes 2$ ***et*** $7 \otimes 5$.

Sur la table ci-dessous nous avons placé ces 5 résultats.

Regarde comment nous avons fait. Recopie cette table et complète-la.

Tu constates que tu as pu inscrire un élément de H dans chaque case de la table. Nous avons ainsi défini une nouvelle loi sur H ; nous l'avons notée $\otimes$.

Comme nous l'avons fait pour la loi $\oplus$, nous admettrons que la loi $\otimes$ est associative ; naturellement, ici aussi, il conviendra de faire au préalable quelques essais, et de remarquer que ces essais, n'étant pas exhaustifs, ne sauraient constituer une preuve.

⊗	1	2	3	4	5	6	7	8	9	10	11	12
1												
2										8		
3												
4												
5												
6										12		
7					11							
8		4										
9							3					
10												
11												
12												

2.2 Tu as vu que 12 est élément neutre pour l'opération $\oplus$ dans H.

Y a-t-il dans H ***un élément neutre pour l'opération*** $\otimes$ ***?***

2.3 Nous avons dit que 4 est le symétrique de 8 pour l'opération $\oplus$ dans H, car $4 \oplus 8 = 12$ et $8 \oplus 4 = 12$, et que 12 est élément neutre de l'opération $\oplus$ dans H.

Tu vas maintenant chercher si 8 a un symétrique pour l'opération $\otimes$ dans H. Autrement dit tu vas chercher s'il existe un élément x de H tel que

$$8 \otimes x = 1 \quad \text{et} \quad x \otimes 8 = 1,$$

puisque 1 est élément neutre de l'opération $\otimes$ dans H.

Quelle est ta réponse ?
Quels sont les éléments de H ***qui ont un symétrique pour l'opération*** $\otimes$ ***dans*** H ***?***
Penses-tu que $(H, \otimes)$ ***soit un groupe ?***

2.4 Des résultats curieux !

Résous l'équation en x ***dans*** H : $8 \otimes x = 4$.
Trouves-tu une solution est une seule ?
Fais le même travail pour les équations en y ***dans*** H ***suivantes :***

$$9 \otimes y = 3 \ ;$$
$$10 \otimes y = 5 \ ;$$
$$11 \otimes y = 2.$$

Les équations ci-dessus sont toutes faites sur le même modèle et tu constates pourtant qu'elles ont

soit plusieurs solutions,
soit pas de solution,
soit une seule solution.

Ecris une équation en x *dans* H, *du même modèle et qui ait six solutions.*

2.5 Soit x et y des éléments de H. Tu as démontré que si $7 \oplus x = 7 \oplus y$, alors $x = y$.

Démontre que si $7 \otimes x = 7 \otimes y$, *alors* $x = y$.
Vérifie maintenant que $8 \otimes 2 = 8 \otimes 5$.

Et pourtant 2 n'est pas égal à 5 !

La phrase suivante est-elle vraie ?

Soit x **et** y **des éléments de** H **; si** $8 \otimes x = 8 \otimes y$, **alors** $x = y$.

Au paragraphe 1.5.2 de la première partie (page 10), nous avons proposé aux élèves de résoudre l'équation en x dans H

$$9 \oplus x = 4 \ ;$$

après les avoir conduit à montrer que si cette équation a une solution c'est nécessairement 7, nous leur demandions de vérifier que 7 est bien solution.
Cette deuxième démarche leur paraît en général bien inutile.
Voici un paragraphe qui les aidera peut-être à comprendre sa nécessité.

2.6 Surprenant.

Cherche dans ta table l'ensemble des solutions de l'équation en x *dans* H

$$6 \otimes x = 6.$$

Nous allons étudier l'équation en x dans H suivante :

$$3 \otimes x = 9.$$

Tu pourrais chercher directement dans la table l'ensemble des solutions ; mais pour mieux comprendre ce que nous avons fait au paragraphe 1.5.2 (première partie, page 10), nous allons suivre une démarche un peu analogue.

Supposons que a soit une solution de cette équation.

Donc $3 \otimes a = 9$,
et $6 \otimes (3 \otimes a) = 6 \otimes 9$.

Justifie l'égalité suivante :

$$6 \otimes (3 \otimes a) = (6 \otimes 3) \otimes a$$

On peut donc écrire que

$$\mathbf{(6 \otimes 3) \otimes a = 6 \otimes 9}$$

et puisque $6 \otimes 3 = 6$ et $6 \otimes 9 = 6$, on peut écrire que

$$6 \otimes a = 6.$$

Le nombre a est donc une solution de l'équation en x dans H

$$6 \otimes x = 6.$$

Tu as vu que l'ensemble des solutions de l'équation $6 \otimes x = 6$ est $\{1, 3, 5, 7, 9, 11\}$.

Quel est l'ensemble des solutions de l'équation $3 \otimes x = 9$ *?*

On constate aisément sur la table que l'ensemble des solutions de cette équation est $\{3, 7, 11\}$, et non $\{1, 3, 5, 7, 9, 11\}$.

II – LE GROUPE DE KLEIN

Voici une autre manipulation, qui conduit à la construction d'un groupe de bijections à quatre éléments.

Mais tout d'abord, nous introduisons le groupe de Klein par sa table.

1. Etude d'une table d'opération.

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

On considère quatre objets distincts, que l'on note e, a, b et c.

Désignons par K l'ensemble de ces éléments. La table ci-dessus est la table d'une opération dans K.

Pourquoi ?

Nous avons noté $*$ cette opération ; ainsi

$$b * c = a.$$

Tu peux remarquer que dans chaque ligne et chaque colonne de cette table, on retrouve tous les éléments de K.

Nous allons maintenant étudier des propriétés de l'opération $*$.

L'ensemble K possède un élément neutre pour la loi $*$.

Lequel ?

L'élément b a un symétrique pour la loi $*$.

Lequel ?

L'élément c a un symétrique pour la loi $*$.

Lequel ?

Pose-toi la même question pour les éléments e *et* a.

Pourquoi l'opération $*$ *est-elle commutative dans* K *?*

Notre objectif est maintenant de démontrer que l'opération $*$ est associative.

Plus précisément, nous poursuivons un double objectif : démontrer l'associativité de l'opération $*$, et analyser cette démonstration pour essayer de faire comprendre ce que veut dire démontrer.

Nous avons employé des « boîtes » pour la démonstration : l'emploi de lettres muettes aurait sans doute perturbé les élèves.

2. Etude de l'associativité.

Nous voulons prouver que l'opération $*$ est associative dans K. Nous devons donc vérifier que quels que soient les éléments de K que l'on mette dans les boîtes,

$$(\square * O) * \Delta = \square * (O * \Delta).$$

Combien y a-t-il de choix possibles lorsque l'on veut mettre un élément de K ***dans la boîte*** $\square$ ***? Dans la boîte*** O ***? Dans la boîte*** Δ ***?***

Quel est le nombre de vérifications à effectuer ?

Ce nombre étant important, nous allons procéder autrement.

2.1 Quel que soit l'élément de K que l'on mette dans O,

$$e * O = O.$$

Dis pourquoi.

Donc, dans K, $(e * O) * \Delta = O * \Delta.$

De même, dans K, $e * (O * \Delta) = O * \Delta$;
donc, dans K, $(e * O) * \Delta = e * (O * \Delta).$

Fais une démonstration analogue pour les deux égalités suivantes.

$$(\square * e) * \Delta = \square * (e * \Delta) ;$$
$$(\square * O) * e = \square * (O * e).$$

Nous savons donc que si l'on met l'élément neutre e dans l'une quelconque des boîtes, alors

$$(\square * O) * \Delta = \square * (O * \Delta).$$

Il ne nous reste donc qu'à examiner les cas où l'on met des éléments de $\{a, b, c\}$ dans les boîtes : il n'y a donc plus que 27 vérifications.

2.2 La table de l'opération $*$ montre que le composé de deux éléments différents choisis parmi a, b et c est égal au troisième élément :

$$a * b = b * a = c, \qquad b * c = c * b = a, \qquad a * c = c * a = b.$$

Si l'on met dans les boîtes $\square$, O et Δ trois éléments différents de $\{a, b, c\}$, alors

$$\square * O = \Delta,$$

car $\square$ est différent de O ;
donc $(\square * O) * \Delta = \Delta * \Delta,$
$= e.$

De même $O * \Delta = \square,$

car O est différent de Δ ;
donc $\square * (O * \Delta) = \square * \square,$
$= e.$

Conclus.

2.3 Nous allons maintenant supposer que l'on met le même élément de $\{a, b, c\}$ dans les trois boîtes.

On est ramené à étudier l'égalité dans K

$$(\diamondsuit * \diamondsuit) * \diamondsuit = \diamondsuit * (\diamondsuit * \diamondsuit).$$

Or $(\diamondsuit * \diamondsuit) * \diamondsuit = e * \diamondsuit,$
$= \diamondsuit.$

et $\diamondsuit * (\diamondsuit * \diamondsuit) = \diamondsuit * e,$
$= \diamondsuit.$

Conclus.

2.4 Il ne nous reste donc plus qu'a examiner les cas où l'on met le même élément dans deux des boîtes et un autre élément dans la troisième boîte.

Etudions d'abord l'égalité dans K

$$(\square * \square) * \Delta = \square * (\square * \Delta).$$

D'une part $(\square * \square) * \Delta = e * \Delta,$
$= \Delta.$

D'autre part $\square * (\square * \Delta) = \square * O,$
$= \Delta.$

(on mets des objets différents dans $\square$, Δ et O),

Conclus.

Etudie aussi les deux égalités suivantes dans K.

$$(\square * O) * \square = \square * (O * \square),$$
$$(\square * O) * O = \square * (O * O).$$

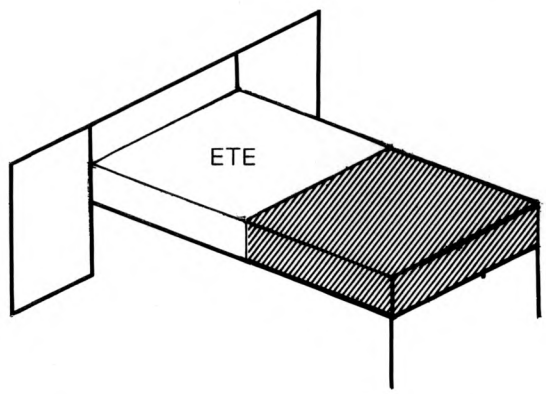
Nous avons montré que l'opération $*$ est associative dans K.

Nous proposons maintenant une version « concrète » du groupe de Klein. Il va s'agir d'abord d'étudier certaines bijections ; puis nous demandons aux élèves de reconnaître le groupe de Klein pas «isomorphisme» des deux tables.

L'exercice introduit sur le mode humoristique procède des mêmes intentions que l'exercice sur les gobelets. Il s'agit de distinguer les états matériels, les consignes et les bijections qui correspondent aux changements d'états, puis de composer ces bijections.

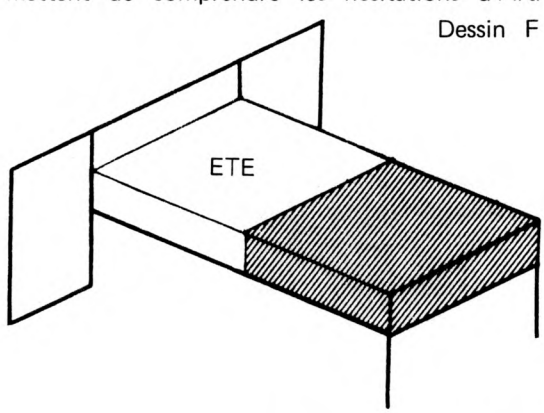
3. La première rencontre d'Arthur avec les groupes.

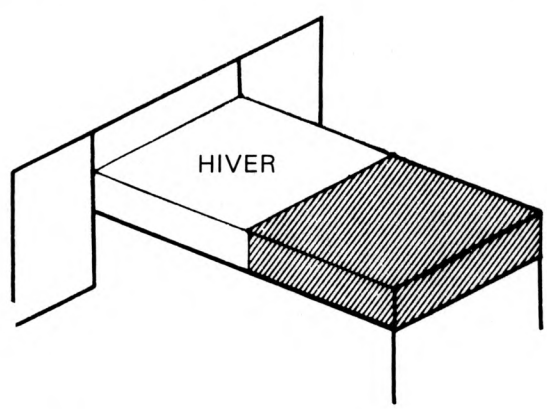
Lorsque Arthur est allé en classe (était-ce en quatrième ou en maternelle ?), sa maman lui a dit : «tu es grand maintenant, tu feras toi-même ton lit tous les jours ; et de temps en temps, tu tourneras le matelas. Au mois d'octobre, un mercredi matin (enfin, ce n'était peut être plus vraiment le matin) Arthur, ayant enlevé ses couvertures et ses draps, s'est retrouvé avec son lit et son matelas dans la position suivante.



« Comment puis-je retourner ce matelas ? » se demande-t-il. Les dessins suivants te permettent de comprendre les hésitations d'Arthur.

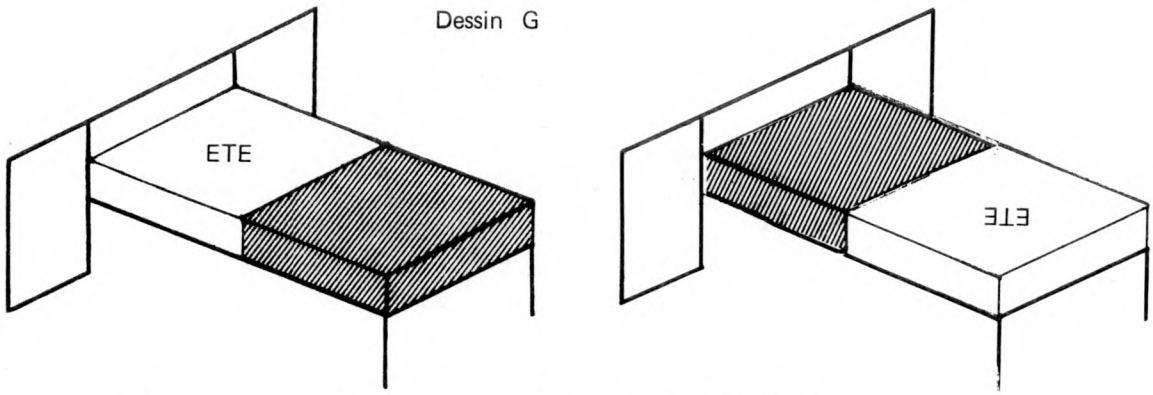
Dessin F





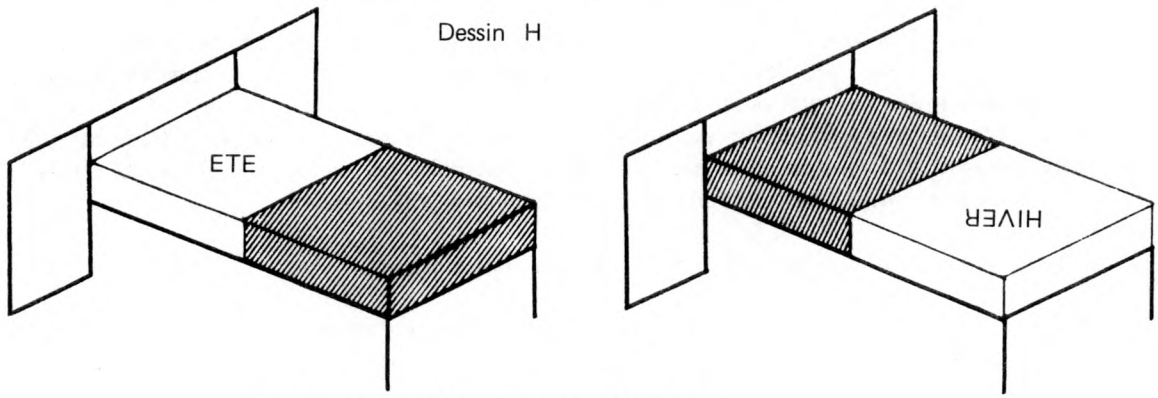
Il fait froid je le retourne Eté-Hiver

Dessin G



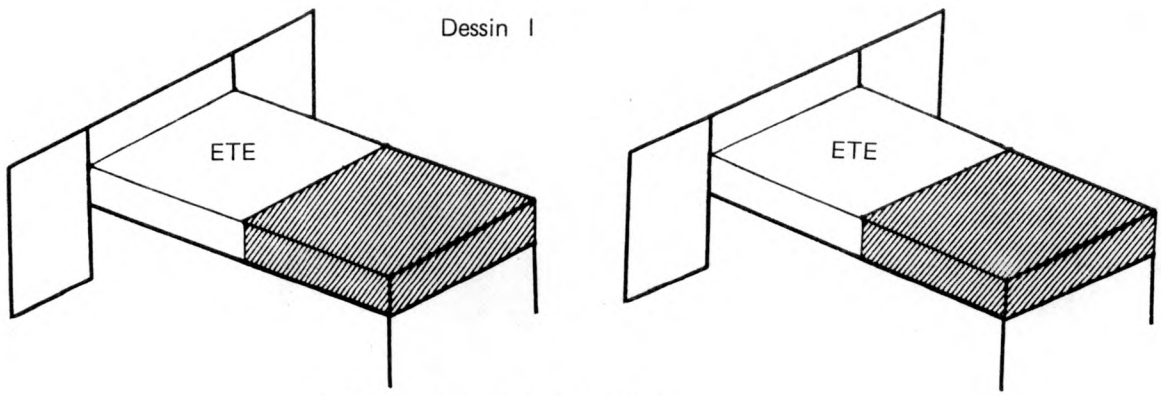
Il y a un trou à la place de ma tête je le pivote Pieds-Tête.

Dessin H



Je le retourne Pieds-Tête **et** Eté-Hiver.

Dessin I



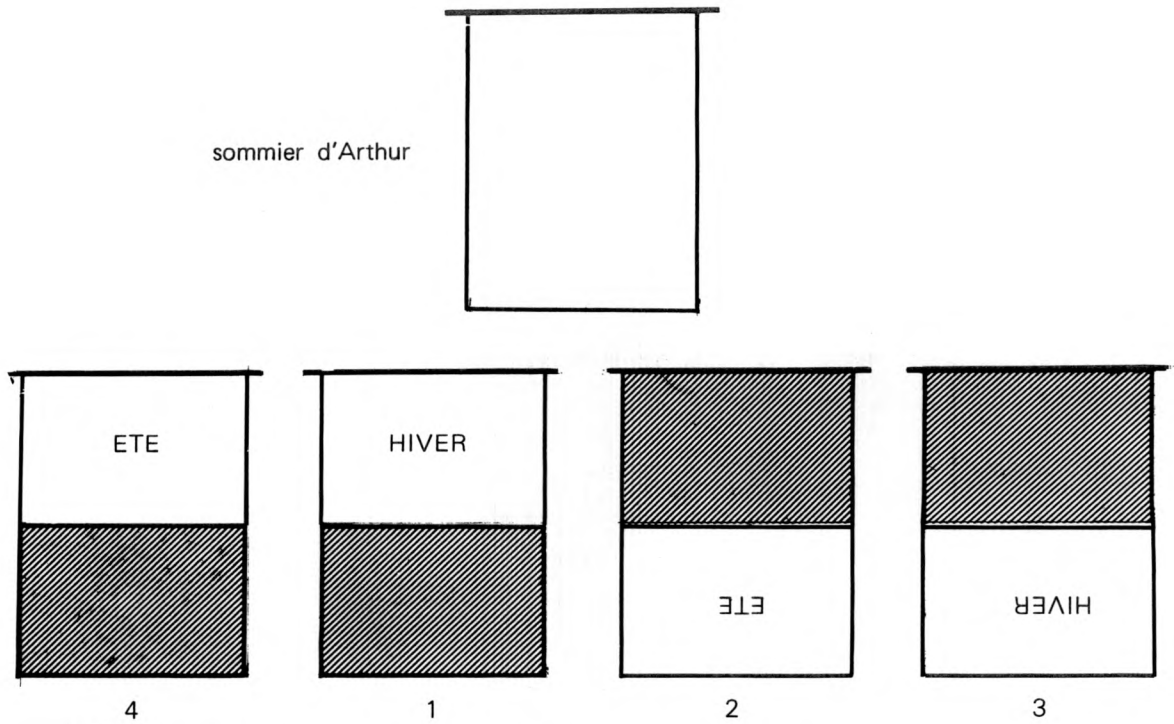
Je suis fatigué, je ne fais rien.

Après avoir hésité entre quatre possibilités, Arthur se dit : mais ce n'est pas terminé, si je tourne mon matelas deux fois de suite, que va-t-il se passer ? Je pourrais bien essayer, mais ce matelas est lourd. Si je faisais des dessins... ça marche bien quelques fois dans le cours de mathématiques... pourquoi ça ne marcherait pas ici ?

Nous allons venir au secours d'Arthur.
Nous avons dessiné le sommier du lit d'Arthur.

Découpe un rectangle qui a les mêmes dimensions, colorie-le à moitié, comme le matelas des dessins a été hachuré. Dans les parties blanches, tu écriras sur une face ETE, et sur l'autre HIVER.

Constate que tu peux poser le matelas que tu viens de fabriquer de quatre façons différentes sur le sommier. Nous allons coder ces quatre positions.



Désignons par M l'ensemble $\{1, 2, 3, 4\}$.

Mets le matelas sur le sommier dans la position 3, ***retourne-le comme sur le dessin*** F : ***tu constates que le matelas est maintenant en position*** 2.

Nous avons marqué ce résultat sur le tableau ci-dessous.

f	
1	
2	
3	2
4	

Recopie ce tableau.
Mets maintenant le matelas dans la position 4, ***retourne-le comme sur le dessin*** F.
Dans quelle position est le matelas ?
Inscris le résultat sur ton tableau.
Recommence le même travail pour les positions 1 ***et*** 2.

Nous avons ainsi défini une application de M vers M. Appelons-la f.

Vérifie que l'application f ***est une bijection de l'ensemble*** M ***vers*** M.

Le dessin G montre une autre façon de tourner le matelas.

Fais la table associée. Tu définis ainsi une nouvelle bijection de M ***vers*** M. ***Appelle-la*** g.

Refais le même travail pour les façons de tourner le matelas indiquées par les dessins par les dessins H ***et*** I.

Nous avons ainsi défini quatre bijections de M vers M, notées f, g, h et i.

Nous allons enfin pouvoir répondre à Arthur.
Regardons ce qui se passerait si Arthur retournait son matelas comme l'indique le dessin H, puis comme l'indique le dessin G.

	h	g
1	2	4
2	1	3
3	4	2
4	3	1

Lisons ensemble la première ligne du tableau. Elle signifie que $2 = h(1)$ et $4 = g(2)$.

Lis de même les trois autres lignes.

En recopiant la première et la troisième colonne du tableau, nous obtenons la table de la composée des bijections h et g ; tu sais qu'on la note $g \circ h$.

$g \circ h$	
1	4
2	3
3	2
4	1

Tu constates que c'est la table de la bijection f, donc $g \circ h = f$.

Recopie et complète le tableau suivant.

$\circ$	i	f	g	h
i				
f				
g				f
h				

Désignons par W l'ensemble $\{i, f, g, h\}$.

Compare cette table avec celle que nous t'avons donnée au paragraphe II.1 ***(page*** 29 ***Que constates-tu ?***

Tu peux en déduire facilement que $(W, \circ)$ est un groupe commutatif.

Résous les équations en x ***dans*** W ***suivantes.***

$x \circ g = g$; $f \circ x = h$; $f \circ x \circ g = g$; $x \circ x = i$; $x \circ x = f$.

4. Il est possible de proposer l'exemple suivant comme autre illustration du groupe de Klein. Désignons par A l'ensemble

{noir, noire, noirs, noires, blanc, blanche, blancs, blanches}.

Appliquons aux différents mots de l'ensemble A la consigne « changer le genre ». Il faut faire vérifier aux élèves qu'à cette consigne correspond une bijection de l'ensemble A dans lui-même. On notera g cette bijection (ainsi g(*noires*) = *noirs*).

De même, à la consigne « changer le nombre », correspond une bijection de l'ensemble A dans lui-même ; on notera n cette bijection (ainsi n(*blancs*) = *blanc*).

On notera enfin d la bijection associée à la consigne « changer le genre et le nombre » et i la bijection associée à la consigne « ne rien changer ». En désignant par G l'ensemble {g, n, d, i}, on pourra faire apparaître le groupe (G, ∘).

A mon avis il faudrait proposer une illustration du groupe cyclique à 4 éléments, pour ne pas laisser croire que tout groupe fini à quatre éléments est un groupe de Klein (voyez par exemple le paragraphe 7.3 de l'article précédent, page 23). Il ne s'agit absolument pas de prétendre faire avec des élèves une étude exhaustive de la notion de groupe mais un contre-exemple peut, de façon salutaire, provoquer le doute devant des généralisations abusives.

III — UN GROUPE NON COMMUTATIF

En accord avec ces principes, nous proposons un exemple de groupe non commutatif. Le groupe du triangle équilatéral, introduit pour les gobelets, jouait ce rôle dans l'article précédent (page 11).

L'exemple proposé ici est «numérique». Il présente à nos yeux un certain nombre d'avantages pédagogiques.

▪ Le support de la structure est ℤ. Il nous semble intéressant de montrer aux élèves que le même ensemble amorphe, muni de deux lois différentes, conduit à deux structures distinctes.

▪ On obtient un groupe non commutatif et il est essentiel d'en montrer au moins un aux élèves.

▪ Pour arriver à la conclusion, il y a un certain nombre de calculs à effectuer, et nous pensons qu'il faut saisir toutes les occasions de faire du calcul algébrique.

▪ L'expérience montre que les élèves sont d'abord surpris et même parfois déroutés par la « double définition » de l'opération dans ℤ que nous avons notée ⊥. Il y a là matière à une discussion sur ce qu'est une opération dans un ensemble.

Nous allons maintenant définir dans ℤ une opération (que nous noterons ⊥) de la façon suivante.

Soit a et b des entiers relatifs :
si a est pair, alors $a \perp b = a + b$;
si a est impair, alors $a \perp b = a - b$.

Quels sont les nombres : $2 \perp 3$; $100 \perp 6$; $3 \perp 3$; $-8 \perp (-8)$; $-7 \perp (-6)$ ***?***

Calcule $2 \perp 5$ ***et*** $5 \perp 2$.

L'opération ⊥ ***est-elle commutative ?***

Calcule $0 \perp 2$ ***et*** $0 \perp (-3)$.

Soit a un entier relatif.

Calcule $0 \perp a$.

Calcule $2 \perp 0$ ***et*** $-5 \perp 0$.

Soit a un entier relatif pair ; ***calcule*** $a \perp 0$.
Soit a un entier relatif impair ; ***calcule*** $a \perp 0$.

Tu as donc démontré que si a est un entier relatif, alors

$$0 \perp a = a \quad \text{et} \quad a \perp 0 = a.$$

Nous conclurons : 0 est élément neutre pour l'opération ⊥ dans ℤ.

Nous allons chercher si les éléments de ℤ ont des symétriques pour l'opération ⊥. Autrement dit, étant donné un élément a de ℤ, nous allons chercher s'il existe un élément x de ℤ tel que

$$a \perp x = 0 \quad \text{et} \quad x \perp a = 0.$$

Tu sais que si l'entier a est pair

$$a \perp x = a + x,$$

et si l'entier a est impair

$$a \perp x = a - x.$$

Intéressons-nous maintenant aux entiers pairs.

Exemple	Soit a un entier relatif pair.
	Résous l'équation en x ***dans*** ℤ
$4 \perp x = 0$.	$a \perp x = 0$.

Conclus (n'oublie pas que a^* ***est le symétrique de*** a ***si*** $a \perp a^* = 0$ **et** $a^* \perp a = 0$**).**

Intéressons nous maintenant aux entiers impairs.

Exemple	Soit a un entier relatif impair.
	Résous l'équation en y ***dans*** ℤ
$-3 \perp y = 0$.	$a \perp y = 0$.

Tu constates qu'un entier relatif impair est son propre symétrique. Nous conclurons :

tout élément de $\mathbb{Z}$ a un symétrique pour l'opération $\perp$.

Recopie et complète le tableau suivant.

a	b	c	$a \perp b$	$(a \perp b) \perp c$	$b \perp c$	$a \perp (b \perp c)$
2	4	5				
2	4	6				
2	3	2				
2	3	7				
1	-2	-8				
1	-2	5				
-3	5	2				
-3	5	-1				

Pour remplir ce tableau, tu as été amené à te poser la question « le nombre a est-il pair ? ».

As-tu été amené à te poser la même question pour le nombre b ***? Et pour le nombre*** c ***?***

Il nous suffit donc, pour avoir tous les cas possibles, d'en considérer quatre.

Recopie et complète le tableau suivant.

a	b	c	$a \perp b$	$(a \perp b) \perp c$	$b \perp c$	$a \perp (b \perp c)$
a pair	b pair	c				
a pair	b impair	c				
a impair	b pair	c				
a impair	b impair	c				

Utilise ce tableau pour vérifier que $(a \perp b) \perp c = a \perp (b \perp c)$.

L'opération $\perp$ est donc associative dans $\mathbb{Z}$. Il y a un élément neutre et tout élément de $\mathbb{Z}$ admet un symétrique.

Nous conclurons : $(\mathbb{Z}, \perp)$ est un groupe.

Puisque l'opération $\perp$ n'est pas commutative, le groupe $(\mathbb{Z}, \perp)$ n'est pas commutatif.

Résous les équations en x ***dans*** $\mathbb{Z}$ ***suivantes.***

$3 \perp x = 7$; $x \perp 3 = 7$; $x \perp 2 = 3$; $2 \perp x = -8$; $x \perp 2 = 6$; $x \perp x = 0$;

$x \perp x = 1$.

C – Pour les enseignants

1
LES GROUPES

1.1 Lois et opérations.

1.1.1 Loi sur un ensemble.

Rappelons d'abord ce qu'on appelle une loi.

Soit E un ensemble ; une **loi** (ou encore une **loi interne**, ou encore une **loi de composition**) sur E est une application du produit cartésien $E \times E$ vers E ; c'est donc une correspondance qui, à chaque couple d'éléments de E, fait correspondre un unique élément de E.

Voici quelques exemples :

- sur $\mathbb{Z}$, la soustraction (si p et q sont des entiers, p – q en est un) ;
- sur l'ensemble $\mathbb{D}$ des décimaux, la multiplication ;
- sur $\mathbb{N}^*$, ensemble des naturels autres que 0, l'exponentiation : si a et b sont des éléments de $\mathbb{N}^*$, alors $a^b \in \mathbb{N}^*$.

1.1.2 Opération sur un ensemble.

On appelle souvent **opération** sur un ensemble E une correspondance de $E \times E$ vers E qui, à un couple d'éléments de E, fait correspondre zéro ou un élément de E ; autrement dit, une opération sur E est une fonction de $E \times E$ vers E.

Avec cette définition, toute loi est évidement une opération. Mais il existe des opérations qui ne sont pas des lois ; par exemple, la soustraction sur $\mathbb{N}$ est une opération qui n'est pas une loi : au couple (3 ; 7) d'éléments de $\mathbb{N}$, la soustraction sur $\mathbb{N}$ ne fait rien correspondre ; si – désigne uniquement la soustraction sur $\mathbb{N}$, l'écriture 3 – 7 n'a pas de sens.

Q1 *Donnez d'autres exemples d'opérations qui ne sont pas des lois.*

Dans la suite, nous ne nous occuperons plus des opérations qui ne sont pas des lois.

1.1.3 Notations.

Si A et B sont des ensembles et si f est une application de A vers B, on note le plus souvent f(x) l'image par f d'un élément x de A. Nous avons remarqué qu'une loi interne sur un ensemble E est une application de $E \times E$ vers E ; on pourrait donc s'attendre que l'image par une loi interne f sur E d'un couple (x, y) soit notée f(x, y). On rencontre pourtant très rarement ce genre de notation.

Le plus souvent, on note une loi interne (c'est-à-dire une application) par un signe tel que +, –, $\times$ ou $\cdot$, : ou $\div$ ou /, ..., $*$; l'image du couple (u, v) par une loi notée $*$, par exemple, sera notée $u * v$; on dira que $u * v$ est le **composé** de u et v par la loi $*$. Pour certaines lois, un nom particulier est utilisé pour désigner les composés : on dira plus volontiers *la somme de* 5 *et de* 2 que *le composé de* 5 *et* 2 *pour l'addition.*

Donnez d'autres exemples de noms particuliers de composés.

Ce type de notation souffre des exceptions ; voici les plus courantes :

▪ pour certaines lois, en particulier celles qui sont notées $\times$ ou $\cdot$, au lieu d'écrire $p \times q$ (ou $p \cdot q$), on se permettra d'écrire pq ; cette convention est sans inconvénient s'il s'agit de noter le composé de deux éléments désignés chacun par une lettre ; mais on ne substituera pas sans inconvénient 2 3 à 2×3, ni même y2 à $y \times 2$ (en particulier à cause de la confusion possible avec y^2, surtout lorsqu'on lit à voix haute cette écriture) ;

▪ la division est une loi sur l'ensemble $\mathbb{R}^*$ des réels non nuls, qui est notée couramment : ; mais l'écriture $\frac{1,5}{3}$ est aussi usuelle que l'écriture 1,5 : 3. Remarquons que la division est également notée /, et $\div$; ce dernier signe, employé par les Anglo-saxons, est universellement utilisé sur les machines à calculer ; compte tenu de la diffusion de celles-ci, il n'est pas possible d'ignorer le signe $\div$, et guère raisonnable de l'employer à un autre usage.

Vous avez remarqué que dans les deux exemples précédents, une même loi est désignée de plusieurs façons ; ceci est dû à des raisons historiques, et aussi de commodité.

▪ Signalons pour terminer la notation de l'exponentiation sur $\mathbb{N}^*$: l'image du couple (5 ; 17) par cette loi est notée 5^{17}. Cette notation cache souvent aux débutants qu'il s'agit d'une loi ; ainsi devinent-ils difficilement que l'égalité

$$(ab)^c = a^c b^c,$$

vraie quels que soient les naturels non nuls a, b et c, indique que l'exponentiation est distributive à droite sur la multiplication.

1.2 Associativité et compagnie.

Les définitions suivantes sont bien connues du lecteur ; c'est pourquoi nous nous permettons de les rappeler ainsi, à la file. Mais il est bien clair qu'il est totalement dépourvu d'intérêt de définir à des débutants l'associativité, par exemple, s'ils n'ont pas déjà rencontré *des* lois associatives et *des* lois qui ne le sont pas, et si on ne leur a pas fait sentir ce qu'apporte la présence — ou l'absence — de l'associativité.

Dans tout ce paragraphe 1.2, on désigne par E un ensemble et par $*$ une loi sur E.

1.2.1 Associativité.

On dit que la **loi** $*$ est **associative** si, quels que soient les éléments u, v et w de E,

$$(u * v) * w = u * (v * w).$$

Cette propriété est fondamentale ; quelques exemples nous le montreront un peu plus loin.

02 *Donnez des exemples de lois associatives, de lois qui ne le sont pas.*

Soient a, b et c des éléments de E ; on convient généralement que $a * b * c$ désigne l'élément $(a * b) * c$; avec cette convention, $7 - 3 - 1 = (7 - 3) - 1$ $(= 3)$. Cette convention peut être une source de confusion pour des débutants, et il vaut probablement mieux y renoncer avec eux, sauf si la loi $*$ est associative ; dans ce dernier cas $a * b * c$ remplace sans inconvénient $(a * b) * c$ et $a * (b * c)$, qui désignent le même élément.

1.2.2 Commutativité.

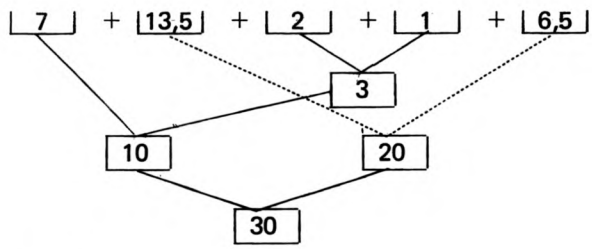
On dit que la **loi** $*$ est **commutative** si, quels que soient les éléments u et v de E,

$$u * v = v * u.$$

03 *Donnez des exemples de lois commutatives, de lois qui ne le sont pas.*

1.2.3 Associativité et commutativité.

Pour calculer numériquement une somme telle que $7 + 13{,}5 + 2 + 1 + 6{,}5$, il est commode de tirer parti de la commutativité *et* de l'associativité de l'addition sur $\mathbb{D}$. Voici un schéma possible de calcul.



Notons S cette somme :

$$
\begin{aligned}
S &= (((7 + 13{,}5) + 2) + 1) + 6{,}5 \quad , \quad \text{(a)} \\
&= ((7 + 13{,}5) + (2 + 1)) + 6{,}5 \quad , \quad \text{(b)} \\
&= ((7 + 13{,}5) + 3) + 6{,}5 \quad , \quad \text{(c)} \\
&= (7 + (13{,}5 + 3)) + 6{,}5 \quad , \quad \text{(d)} \\
&= (7 + (3 + 13{,}5)) + 6{,}5 \quad , \quad \text{(e)} \\
&= ((7 + 3) + 13{,}5) + 6{,}5 \quad , \quad \text{(f)} \\
&= (7 + 3) + (13{,}5 + 6{,}5) \quad , \quad \text{(g)} \\
&= 10 + 20 \quad , \quad \text{(h)} \\
&= 30 \quad . \quad \text{(i)}
\end{aligned}
$$

04 *Dans cette suite d'égalités, indiquez où l'associativité de l'addition doit être invoquée, et où l'on a fait appel à la commutativité.*

1.2.4 Elément neutre.

On dit que e, élément de E, est **neutre** (ou **élément neutre**) pour la loi $*$ si, quel que soit a dans E,

$$a * e = e * a = a.$$

05 *Pourquoi ne suffit-il pas d'indiquer que, quel que soit a dans E,*

$$a * e = a$$

(ou que $e * a = a$*) ?*

06 *Donnez des exemples de lois ayant un élément neutre, de lois n'en ayant pas.*

Supposons que p et q soient des éléments de E, neutres pour la loi $*$. Puisque p est neutre, quel que soit x dans E, il est vrai que $p * x = x$; en particulier $p * q = q$. De même, quel que soit y dans E, il est vrai que $y * q = y$, et en particulier $p * q = p$. Donc $p = q$, et la loi $*$ a au plus un élément neutre.

1.2.5 Symétrique.

Nous supposons ici que la loi $*$ a un élément neutre, noté e.
Soit a un élément de E. On dit que a' est **symétrique** de a pour la loi $*$ si

$$a * a' = e \quad \text{et} \quad a' * a = e.$$

Remarquez que e a un symétrique, qui est lui-même : en effet, $e * e = e$.

Si la loi $*$ est associative, un élément de E a au plus un symétrique pour la loi $*$. En effet, soit a un élément de E ; supposons que a' et a'' soient des symétriques de a pour la loi $*$:

$$a' * a = e \quad \text{et} \quad a * a'' = e \ ;$$

donc

$$
\begin{aligned}
a' &= a' * e \ , \\
&= a' * (a * a'') \ , \\
&= (a' * a) * a'' \qquad \text{(ici l'associativité est essentielle)}, \\
&= e * a'' \ , \\
&= a'' .
\end{aligned}
$$

Cette démonstration est un deuxième exemple de l'importance de l'associativité.

Si une loi a un élément neutre et n'est pas associative, il peut se faire qu'un élément ait deux symétriques. Voici un exemple : l'ensemble des trois éléments u, a et b est muni de la loi $\perp$ donnée par la table ci-contre ; cette loi n'est pas associative.

$\perp$	u	a	b
u	u	a	b
a	a	u	u
b	b	u	a

07 *Vérifiez-le.*

Pour cette loi, u est neutre.

Vous pouvez constater que l'élément a a deux symétriques : lui-même et b.

Vous pouvez remarquer que la loi $\perp$ est commutative.

Soit a un élément de E admettant un symétrique ; notons a' ce symétrique.

08 *Est-ce que* a' *a un symétrique ? Si oui, lequel ?*

Remarquez que pour l'addition, les symétriques se nomment aussi les **opposés**, et que pour la multiplication, ils se nomment aussi les **inverses.**

1.2.6 Remarque.

L'associativité et, à un degré moindre, la commutativité sont des propriétés fort agréables. Il ne faudrait pas en déduire que les lois qui n'ont aucune de ces deux propriétés soient toutes dénuées d'intérêt.

Par exemple, on définit sur les vecteurs de l'espace de dimension 3 une loi, appelée *produit vectoriel* et notée Λ, qui n'est ni associative, ni commutative ; elle n'en est pas moins fort utile.

On peut se rappeler aussi que la soustraction, la division et l'exponentiation ne sont ni associatives, ni commutatives.

1.3 Monoïdes et groupes.

1.3.1 Monoïdes.

Soit M un ensemble. On dit que $(M, *)$ est un **monoïde**$^{\Delta}$ si $*$ est une loi sur M qui est associative et a un élément neutre (le mot *monoïde* n'est probablement pas utile pour de jeunes élèves ; dans la suite, nous marquerons du signe $^{\Delta}$ les mots que nous introduirons et qui nous paraîtrons inutiles, voire nuisibles, pour des élèves du premier cycle ; cela ne signifie aucunement que les mots qui ne sont pas marqués de ce signe doivent obligatoirement être connus des élèves ; c'est naturellement à chaque professeur de juger de l'opportunité d'introduire tel ou tel mot dans sa classe).

09 *Donnez des exemples de monoïdes ; donnez des exemples de lois qui ne soient pas des lois de monoïdes.*

1.3.2 Définition des groupes.

Soit G un ensemble. On dit que $(G, *)$ est un **groupe** si $*$ est une loi sur G
qui est associative,
qui a un élément neutre,
et telle que tout élément de G ait un symétrique.

Autrement dit, un groupe est un monoïde dont tous les éléments ont un symétrique.

Remarquez bien qu'un groupe est donné par deux objets : un ensemble et une loi sur cet ensemble. La coutume est de donner ces deux objets sous la forme d'un couple. Il n'est probablement pas essentiel d'imposer cette forme aux débutants, mais il faut absolument faire comprendre qu'un ensemble seul n'est pas un groupe. C'est ainsi que lorsqu'on parle du groupe $\mathbb{Z}$, on

commet un abus de langage : on sous-entend la loi de groupe la plus habituelle sur $\mathbb{Z}$, à savoir l'addition. Un tel abus n'est probablement pas souhaitable avec de jeunes élèves.

10 *Donnez des exemples de groupes ; donnez des exemples de monoïdes qui ne soient pas des groupes.*

11 *La loi* $(a, b) \longmapsto a + b - 1$ *sur* $\mathbb{R}$ ***est-elle une loi de groupe ?*** *Même question pour* $(a, b) \longmapsto a + b - ab$.

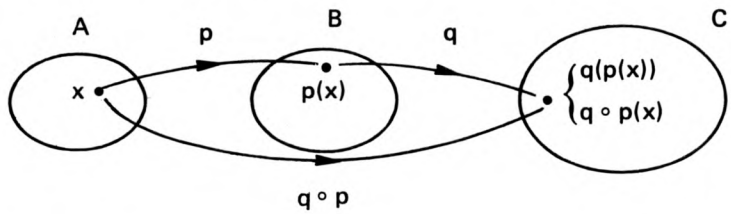
Soit $(G, *)$ un groupe ; si la loi $*$ est commutative, on dit que $(G, *)$ est un **groupe commutatif** (ou encore **groupe abélien**, en l'honneur du mathématicien norvégien Niels Abel né en 1802 et mort en 1829).

Les groupes que vous avez cités en exemple sont peut-être tous commutatifs ; en tout cas, ceux qui proviennent des lois usuelles sur les ensembles de nombres le sont tous. Pourtant les groupes non commutatifs sont très importants. En voici quelques exemples.

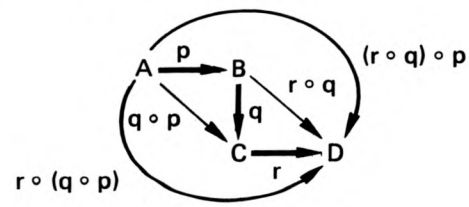
1.4 Exemples de groupes non commutatifs.

1.4.1 Permutations.

Soient A, B et C des ensembles ; soient q une application de B vers C et p une application de A vers B (ou, avec une définition un peu différente, vers une partie de B). On désigne par $q \circ p$ l'**application composée** de p et q (aussi appelée q **suivie de** p) qui à un élément x de A fait correspondre $q(p(x))$ dans C.



Soient A, B, C et D des ensembles ; soient p une application de A vers B, q une application de B vers C et r une application de C vers D. On sait que $r \circ (q \circ p) = (r \circ q) \circ p$.



Soit X un ensemble. Rappelons qu'une **permutation**[△] de X est une bijection de X vers X. Notons S_X l'ensemble des permutations de X. Si p et q sont des permutations de X (c'est-à-dire des bijections de X vers X), il en est de même pour $q \circ p$; donc la loi de composition $\circ$ est une loi sur S_X ; d'après ce qui précède, cette loi est associative ; l'application identique sur X, que nous noterons id_X, est une permutation de X et est neutre pour cette loi : si $p \in S_X$, quel que soit x dans X,

$$id_X \circ p(x) = id_X(p(x)) = p(x) \quad \text{et} \quad p \circ id_X(x) = p(id_X(x)) = p(x) \ ;$$

donc $id_X \circ p = p \circ id_X = p$. Enfin, si p est une bijection de X vers X, son application réciproque notée p^{-1}, est définie, est une permutation de X, et $p \circ p^{-1} = p^{-1} \circ p = id_X$.

Il en résulte que $(S_X, \circ)$ est un groupe.

12 *Montrez que si* X *a moins de trois éléments, le groupe* $(S_X, \circ)$ *est commutatif ; montrez que si* X *a au moins trois éléments, le groupe* $(S_X, \circ)$ *n'est pas commutatif.*

Cet exemple de groupe est extrêmement important. A titre d'exercice, voici d'autres exemples.

1.4.2 Premier exercice.

On munit le produit cartésien $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ de la loi $\square$, ainsi définie : si a, b, c, u, v et w sont des entiers,

$$(a, b, c) \square (u, v, w) = (a + u, b + v, c + w + av).$$

13 *Montrez que* $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, \square)$ *est un groupe non commutatif.*

1.4.3 Deuxième exercice.

Notons T l'ensemble des rationnels autres que 0 et 1. Définissons ainsi les six applications a, b, c, f, g et h de T vers T :

$$a : x \longmapsto x, \qquad b : x \longmapsto \frac{x-1}{x}, \qquad c : x \longmapsto \frac{1}{1-x},$$

$$f : x \longmapsto \frac{1}{x}, \qquad g : x \longmapsto 1 - x, \qquad h : x \longmapsto \frac{x}{x-1}.$$

(On vérifie aisément que l'image d'un élément de T par l'une quelconque de ces six applications est bien un élément de T).

Notons G l'ensemble de ces six applications.

14 *Montrez que ces six applications sont des permutations de* T. *Montrez que si* u *et* v *sont des éléments de* G, *alors* $u \circ v \in G$. *Montrez que* $(G, \circ)$ *est un groupe, non commutatif.*

1.4.4 Troisième exercice.

Notons A l'ensemble des applications de $\mathbb{Z}$ vers $\mathbb{Z}$ de la forme

$$t \longmapsto \epsilon t + b, \quad \text{où} \quad \epsilon \in \{-1, 1\} \quad \text{et} \quad b \in \mathbb{Z}.$$

Par exemple $\mathbb{Z} \longrightarrow \mathbb{Z}$, $t \longmapsto -t$ et $\mathbb{Z} \longrightarrow \mathbb{Z}$, $t \longmapsto t - 46$ sont des éléments de A.

15 *Montrez que les éléments de* A *sont des permutations de* $\mathbb{Z}$; *montrez que si* f *et* g *sont des éléments de* A, *alors* $f \circ g \in A$.

Montrez que $(A, \circ)$ *est un groupe non commutatif.*

C – Pour les enseignants

2

QUE FAIRE AVEC LES GROUPES ?

Nous ne parlerons dans ce chapitre que des propriétés des groupes que l'on utilise habituellement en algèbre dans le premier cycle. Pour d'autres réponses à la question posée en titre, voyez les derniers chapitres du deuxième fascicule.

2.1 Deux propriétés bien utiles.

Dans ce paragraphe, $(G, *)$ désigne un groupe dont l'élément neutre est noté e ; si $g \in G$, on notera g' le symétrique de g pour la loi $*$.

2.1.1 La régularité.

Revenons ici sur le problème de la régularité, déjà évoqué dans la première partie, page 19. Soit a un élément de G ; nous avons vu que, quels que soient les éléments x et y de G,

$$\text{si} \quad a * x = a * y, \quad \text{alors} \quad x = y.$$

De même, quels que soient les éléments x et y de G, si $x * a = y * a$, alors $x = y$. On dira que a est **régulier** (ou **simplifiable**) pour la loi $*$. Comme tous les éléments de G sont réguliers pour la loi $*$, on dit que la loi $*$ est **régulière** (ou **simplifiable**).

16 *Donnez des exemples de lois régulières qui ne soient pas des lois de groupe ; donnez des exemples de lois qui ne soient pas régulières.*

Donc, si a, b et c sont des éléments de G, et comme $(G, *)$ est un groupe, de l'égalité

$$a * b = a * c \quad \text{on peut déduire l'égalité} \quad b = c.$$

D'autre part écrire $b = c$, c'est écrire que b et c sont deux écritures d'un même objet ; donc si $b = c$, alors $(a, b) = (a, c)$ (ou encore : (a, b) et (a, c) sont deux écritures d'un même objet) ; la loi $*$, qui est une application, fait correspondre à ce couple, dont nous donnons ici deux écritures, une image bien définie qui s'écrit indifféremment $a * b$ ou $a * c$:

$$\text{si} \quad b = c, \quad \text{alors} \quad a * b = a * c.$$

MAIS CETTE DERNIERE RELATION NE DOIT RIEN AUX PROPRIETES DES GROUPES ET TOUT A CELLES DE L'EGALITE.

Il est donc vrai que les égalités $b = c$ et $a * b = a * c$ sont équivalentes si a, b et c sont des éléments de G. Mais, malgré ce qu'on trouve écrit trop souvent, il n'y a qu'une « moitié » de cette équivalence qui est un bénéfice des propriétés des groupes ! Il est d'ailleurs bien délicat de demander à des élèves de justifier l'autre moitié.

2.1.2 Symétrique du composé de deux éléments.

Rappelons simplement ici un résultat fréquemment utilisé, déjà démontré page 20.
Si a et b sont des éléments de G, le symétrique de $a * b$ est $b' * a'$.

Remarquez qu'il n'est important d'écrire $b' * a'$ et non $a' * b'$ que si le groupe n'est pas commutatif.

2.2 Deux lois sur un même ensemble.

2.2.1 Distributivité.

Soit E un ensemble ; soient $\top$ et $\bullet$ des lois sur E ; on dit que la loi $\bullet$ est **distributive sur** la loi $\top$ si, quels que soient les éléments x, y et z de E,

$$x \bullet (y \top z) = (x \bullet y) \top (x \bullet z) \quad \text{et} \quad (y \top z) \bullet x = (y \bullet x) \top (z \bullet x).$$

Si la loi $\bullet$ est distributive sur la loi $\top$, on écrit souvent

$$a \bullet b \top c \quad \text{au lieu de} \quad (a \bullet b) \top c \ :$$

on dit que la loi $\bullet$ a **priorité** sur la loi $\top$.

17 *Donnez des exemples d'ensembles munis de deux lois, dont l'une est distributive sur l'autre. Est-il possible qu'une loi soit distributive sur elle-même ?*

Supposons que la loi $\bullet$ soit distributive sur la loi $\top$, et qu'en outre E ait un élément neutre pour la loi $\top$; notons e cet élément.

18 *Montrez que si la loi* $\top$ *est régulière, quel que soit* x *dans* E,

$$e \bullet x = x \bullet e = e.$$

On dit que e est **absorbant**$^{\Delta}$ pour la loi $\bullet$.

Soit F un ensemble ; soit $\blacklozenge$ une loi sur F.

19 *Est-il possible que deux éléments de* F *soient absorbants pour la loi* $\blacklozenge$ *?*
La loi $\blacklozenge$ *peut-elle être régulière si elle a un élément absorbant ?*

Supposons à nouveau que la loi $\bullet$ est distributive sur la loi $\top$.

20 *Est-il possible que* $(E, \top)$ *et* $(E, \bullet)$ *soient des groupes tous les deux ?*

2.2.2 Loi induite.

Parmi les monoïdes bien connus des élèves du premier cycle, citons $(\mathbb{N}, \times)$ et $(\mathbb{D}_+, \times)$; nous remarquons que $\mathbb{N} \subset \mathbb{D}_+$, et que la loi sur $\mathbb{N}$ est *la même* que la loi sur $\mathbb{D}_+$. Précisons ce point.

Soit E un ensemble ; soit $*$ une loi sur E ; soit F une partie de E. Si, quels que soient u et v dans F, il est vrai que $u * v \in F$, nous dirons que F est **stable**$^{\Delta}$, ou encore **fermée**$^{\Delta}$, pour la loi $*$. Dans ce cas, à chaque couple (x, y) d'éléments de F, la loi $*$ fait correspondre l'élément $x * y$ de F ; nous définissons ainsi une loi sur F. Cette nouvelle loi est appelée la **restriction**$^{\Delta}$ de la loi $*$ à F (ou encore : la **loi induite**$^{\Delta}$ par $*$ sur F) ; ainsi, la multiplication sur $\mathbb{N}$ est la restriction de la multiplication sur $\mathbb{D}_+$ à $\mathbb{N}$.

Cette nouvelle loi n'est pas la loi $*$ si $F \neq E$: la loi $*$ est une application de $E \times E$ vers E, et la restriction de la loi $*$ à F est une application de $F \times F$ vers F. Mais d'habitude, on désigne de la même manière cette nouvelle loi ; cet abus de langage ne présente en général pas d'inconvénient, et est le plus souvent bien commode.

Donnez des exemples de restrictions de loi.

2.2.3 Anneaux unitaires et corps.

Soient K un ensemble ayant au moins deux éléments, $\perp$ et $\triangledown$ des lois sur K telles que
$(K, \perp)$ soit un groupe,
$(K, \triangledown)$ soit un monoïde,
la loi $\triangledown$ soit distributive sur la loi $\perp$:
on dit alors que $(K, \perp, \triangledown)$ est un **anneau unitaire**$^{\Delta}$.

Par exemple, $(\mathbb{Z}, +, \times)$ et $(\mathbb{D}, +, \times)$ sont des anneaux unitaires.
Soit $(K, \perp, \nabla)$ un anneau unitaire.

21 *Montrez que les éléments neutres des lois* $\perp$ *et* ∇ *sont distincts.*

22 *Montrez que la loi* $\perp$ *est commutative.*

Ce dernier résultat montre qu'il était inutile de préciser dans la définition que la loi $\perp$ est commutative. Par contre, la loi ∇ n'est pas forcément commutative ; si elle est commutative, on dit que $(K, \perp, \nabla)$ est un **anneau unitaire commutatif**$^{\Delta}$.

Notons e l'élément neutre de la loi $\perp$.
Notons $K^{\square}$ l'ensemble des éléments de K qui ont un symétrique pour la loi ∇.

23 *Montrez que* $e \notin K^{\square}$ *; montrez que* $K^{\square}$ *est stable pour la loi* ∇ *et que* $(K^{\square}, \nabla)$ *est un groupe.*

Le groupe $(K^{\square}, \nabla)$ est appelé le **groupe multiplicatif**$^{\Delta}$ de l'anneau unitaire $(K, \perp, \nabla)$.

24 *Quel est le groupe multiplicatif de* $(\mathbb{Z}, +, \times)$ *? De* $(\mathbb{D}, +, \times)$ *?*

Notons K^* l'ensemble $K \setminus \{e\}$. Si $K^{\square} = K^*$ on dit que $(K, \perp, \nabla)$ est un **corps**$^{\Delta}$. Dire que $K^{\square} = K^*$, c'est dire que tous les éléments de K sauf e ont un symétrique pour la loi ∇.

Par exemple, $(\mathbb{Q}, +, \times)$ et $(\mathbb{R}, +, \times)$ sont des corps ; par contre, $(\mathbb{Z}, +, \times)$ et $(\mathbb{D}, +, \times)$ n'en sont pas : dans ces derniers cas, il y a d'autres éléments que 0 qui n'ont pas d'inverse.

2.2.4 Anneaux.

Soient A un ensemble, $\perp$ et ∇ des lois sur A telles que
$(A, \perp)$ soit un groupe *commutatif,*
la loi ∇ soit associative,
la loi ∇ soit distributive sur la loi $\perp$:
on dit alors que $(A, \perp, \nabla)$ est un **anneau**$^{\Delta}$.

Compte tenu de la définition des anneaux unitaires et des corps, et de la question 22, il est clair que les anneaux unitaires et les corps sont des anneaux. Mais il existe des anneaux qui ne sont pas unitaires : soit k un élément de $\mathbb{N}^*$; notons $k\mathbb{Z}$ l'ensemble des entiers multiples de k ; cet ensemble est fermé pour l'addition et la multiplication des entiers, et $(k\mathbb{Z}, +, \times)$ est un anneau, qui n'est unitaire que si $k = 1$. Soit $(G, *)$ un groupe ; notons e l'élément neutre de ce groupe ; notons $\diamond$ la loi $(x, y) \longmapsto e$ sur G ; on constate facilement que cette loi est distributive sur la loi $*$, et qu'elle est associative ; donc si la loi $*$ est une loi commutative, $(G, *, \diamond)$ est un anneau (qui n'est pas unitaire) ; si la loi $*$ n'est pas commutative, $(G, *, \diamond)$ n'est pas un anneau. On voit pourquoi on a imposé ici dans la définition que la loi $\perp$ soit *commutative.*

Les anneaux qui ne sont pas unitaires ne jouent pas un grand rôle en algèbre. Mais on rencontre des anneaux unitaires, y compris non commutatifs, et des corps dans beaucoup de questions. Nous ne nous y attarderons pas ici ; cependant, un chapitre du deuxième fascicule donnera des indications sur une utilisation importante des corps.

On appelle généralement addition et on note souvent $+$ la première loi d'un anneau, son élément neutre est alors noté 0 ; la deuxième loi est appelée multiplication, notée $\times$ (ou $\cdot$), et si elle a un élément neutre il est noté 1.

Les termes *anneau* et *corps* ne sont guère utiles dans le premier cycle ; mais le mot *corps* semble encore plus inutile que l'autre : on n'y rencontrera pas d'autre corps que $(\mathbb{Q}, +, \times)$ et $(\mathbb{R}, +, \times)$ et, dans la pratique, les élèves ne sauront pas distinguer ce qui sépare ces deux corps, bien que les différences, même purement algèbriques, soient très importantes (pour quelques unes de ces différences, voyez le deuxième fascicule). Par contre, outre les corps cités, ils utiliseront $(\mathbb{Z}, +, \times)$, $(\mathbb{D}, +, \times)$ et, au moins de façon implicite, l'anneau des applications polynômes à coefficients réels (si f et g sont deux applications polynômes, par définition $f + g$ est l'application $\mathbb{R} \longrightarrow \mathbb{R}$, et $f \times g$ est définie de façon analogue).
$t \longmapsto f(t) + g(t)$

2.3 Equations.

Dans ce paragraphe $(G, *)$ désigne un groupe ; son élément neutre est noté e ; si $g \in G$, son symétrique sera noté g'.

Nous revenons ici au problème important des équations, déjà examiné dans la première partie, page 10.

2.3.1 Résolution détaillée d'une équation.

Soient a et b des éléments de G. **Résoudre l'équation en** x **dans** G

$$a * x = b,$$

c'est trouver l'ensemble des éléments g de G tels que $a * g = b$; remarquez que c'est donc trouver l'ensemble des antécédents de b pour l'application $G \longrightarrow G$, $t \longmapsto a * t$. Une **solution** de cette équation est un élément de cet ensemble.

Supposons que s soit une solution de cette équation :

$$a * s = b$$

(en faisant cette suppositior nous n'avons pas résolu le problème de savoir s'il existe au moins une telle solution).

On en déduit (voyez page 10) que $a' * (a * s) = a' * b$ et que $s = a' * b$.

Autrement dit, nous avons montré que si s est une solution de l'équation, alors

$$s = a' * b.$$

NOUS N'AVONS RIEN MONTRE D'AUTRE, et si c'était nécessaire, l'exemple donné dans la deuxième partie, page 28, nous convaincrait du danger qu'il y aurait à croire avoir démontré plus.

Il reste à vérifier si $a' * b$ est bien, ou n'est pas solution ; on constate facilement que $a' * b$ est solution car $a * (a' * b) = (a * a') * b = b$. Donc l'équation a une solution, unique, qui est $a' * b$.

25 *Donnez un exemple de résolution d'équation où l'omission de cette dernière étape conduirait à des déboires.*

2.3.2 Equivalences.

Naturellement, pour résoudre cette équation, il est possible d'utiliser des relations équivalentes. Faisons-le.

Soit g un élément de G.

D'après ce que nous avons vu au paragraphe 2.1 (page 37), les égalités

$$a * g = b \quad \text{et} \quad a' * (a * g) = a' * b$$

sont équivalentes.

Puisque $a' * (a * g) = (a' * a) * g$, les égalités

$$a' * (a * g) = a' * b \quad \text{et} \quad (a' * a) * g = a' * b$$

sont équivalentes.

De même, puisque $(a' * a) * g = g$, les égalités

$$(a' * a) * g = a' * b \quad \text{et} \quad g = a' * b$$

sont équivalentes.

De ces trois équivalences, on déduit par transitivité que les égalités

$$a * g = b \quad \text{et} \quad g = a' * b$$

sont équivalentes. Ceci se traduit évidemment par : g *est solution de l'équation si et seulement si* $g = a' * b$, ou encore par : *l'équation admet* $a' * b$ *pour unique solution.*

2.3.3 Quelques considérations pédagogiques.

Le paragraphe 2.3.2 explique pourquoi la résolution de cette équation se réduit souvent à la

succession (S) des quatre égalités suivantes :

$$(S)\quad \begin{cases} a * x = b\,, \\ a' * (a * x) = a' * b\,, \\ (a' * a) * x = a' * b\,, \\ x = a' * b. \end{cases}$$

Ceci nous paraît très facheux avec des débutants.

Tout d'abord, de nombreux indices conduisent à penser qu'un élève de 4ème comprend très mal ce qu'est une équivalence, et confond fréquemment équivalence et implication.

Il est vrai que la recherche du rendement nous incite à faire acquérir des tours de main plutôt qu'à faire réfléchir sur les calculs ; et cela se comprend, car une pratique passable du calcul est nécessaire pour faire des mathématiques. Mais les recettes n'ont pas que des avantages : une pratique *constante* des recettes, sans essayer de comprendre les mécanismes et les difficultés, rend stupide devant des situations nouvelles (question 25), et obscurcit la notion de raisonnement — ou plutôt, l'empêche de naître.

C'est pourquoi nous pensons qu'il faut une longue période, peut-être au moins un an, avant d'aborder la résolution des équations par équivalence. Dans un premier temps, il nous paraît plus raisonnable qu'après avoir examiné quelques exemples qui « marchent », l'on démontre (éventuellement) et l'on énonce un théorème tel que

«si a et b sont des réels, l'équation en x dans IR

$$a + x = b$$

a une solution unique»,

et la même chose dans $(\mathbb{Z}, +)$, $(\mathbb{R}^*, \times)$, etc... Ce, jusqu'à ce que les élèves eux-mêmes, lassés, disent :

«et la même chose dans n'importe quel groupe».

Il n'y a évidemment aucun intérêt à faire retenir la forme générale de la solution : les élèves seront amenés à montrer, par implications, que s'il y a une solution, alors c'est nécessairement..., et comme d'après le théorème il y en a effectivement une, etc...

Il faut remarquer que la succession (S) d'égalités présente encore d'autres difficultés.

L'utilisation d'une même lettre, ici x, pour poser le problème (par quoi faut-il remplacer x pour que l'égalité $a * x = b$ soit vraie ?) et comme variable (si $x \in G$, alors les égalités $a * x = b$ et $x = a' * b$ sont toutes les deux vraies et toutes les deux fausses) rend la compréhension des choses difficile.

En outre, la dernière ligne $(x = a' * b)$, donnée si souvent sans aucun commentaire, fait dire à d'innombrables élèves que

« la solution est $x = a' * b$ »,

et non que

« la solution est $a' * b$ » ;

ceci ne les aide évidemment pas à comprendre ce que signifient les mots *solution d'une équation.*

2.3.4 Equations et commutativité.

Si le groupe $(G, *)$ est commutatif, les deux équations en x dans G

$$a * x = b \quad \text{et} \quad x * a = b$$

ont la même solution : dans ce cas, quel que soit x dans G, il est vrai que $a * x = x * a$, et donc que $a * x = b$ si et seulement si $x * a = b$. L'étude de la seconde équation n'a alors aucun intérêt si l'on a déjà étudié la première.

Par contre, si le groupe n'est pas commutatif, il peut se faire que les deux équations n'aient pas la même solution. On montre, de façon tout à fait analogue, que l'équation $x * a = b$ a également une solution unique, qui est $b * a'$.

26 *Reprenez la question* 15 *(chapitre* 1, *paragraphe* 1.4.4, *page* 42*) et résolvez les quatre équations en* f *dans* A *suivantes.*

(1) $f \circ (t \longmapsto t + 2) = (t \longmapsto -t + 4)$; (3) $f \circ (t \longmapsto t + 2) = (t \longmapsto t - 4)$;

(2) $(t \longmapsto t + 2) \circ f = (t \longmapsto -t + 4)$; (4) $(t \longmapsto t + 2) \circ f = (t \longmapsto t - 4)$.

2.3.5 Les groupes sont-ils indispensable ?

Voici les tables de trois lois, définies respectivement sur les ensembles à trois, cinq et six éléments $\{a, b, c\}$, $\{a, b, c, d, e\}$ et $\{a, b, c, d, e, f\}$; les deux premières ont déjà été présentées dans la première partie (page 23).

$\perp$	a	b	c
a	a	b	c
b	c	a	b
c	b	c	a

T	a	b	c	d	e
a	a	b	c	d	e
b	b	a	d	e	c
c	c	e	a	b	d
d	d	c	e	a	b
e	e	d	b	c	a

☆	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	a	d	e	f	c
c	c	d	f	a	b	c
d	d	e	a	f	c	b
e	e	f	b	c	d	a
f	f	c	c	b	a	d

Ces tables ont la propriété que dans chaque ligne et chaque colonne chaque élément de l'ensemble concerné figure une et une seule fois ; autrement dit, si $*$ est l'une de ces trois lois et si p et q sont des éléments de l'ensemble concerné, il existe un unique élément x et un unique élément y de l'ensemble concerné tels que

$$p * x = q \quad \text{et} \quad y * p = q.$$

Si $\blacksquare$ est une loi sur l'ensemble E qui a la propriété que, quels que soient les éléments p et q de E, chacune des équations en x dans E

$$p \blacksquare x = q \quad \text{et} \quad x \blacksquare p = q$$

a une solution unique, on dit que $(E, \blacksquare)$ est un **carré latin**$^{\Delta}$ (certains réservent ce nom au cas où E est fini).

D'après ce qui a été indiqué aux paragraphes 2.3.1 et 2.3.4, tout groupe est un carré latin. Mais les trois lois proposées ici, qui sont des lois de carrés latins comme on peut le constater sur leurs tables, montrent chacune que la réciproque est fausse. On a vu (page 23) que $(\{a, b, c\}, \perp)$ n'a pas d'élément neutre et n'est pas associative, et que $(\{a, b, c, d, e\}, T)$ n'est pas associative ; et la loi ☆ n'est pas associative non plus : par exemple,

$$(b ☆ c) ☆ d = d ☆ d = f, \quad b ☆ (c ☆ d) = b ☆ a = b \quad \text{et} \quad f \neq b.$$

(On peut montrer que tout carré latin qui a moins de 3 éléments est un groupe ; tout carré latin qui a un élément neutre et qui a moins de 5 éléments est un groupe ; tout carré latin qui a un élément neutre, qui est commutatif et qui a moins de 6 éléments est un groupe).

Bien que, d'une certaine manière, les carrés latins apportent une réponse satisfaisante au problème des équations — une solution et une seule — ils sont peu maniables quand l'associativité manque ; ils ne permettent pas, dans ce cas, d'élaborer des méthodes simples et générales de résolution.

C _ Pour les enseignants

REPONSES AUX QUESTIONS POSEES

01 La division dans $\mathbb{N}$, dans $\mathbb{Z}$, dans $\mathbb{D}$, dans $\mathbb{Q}$ (la division dans $\mathbb{Q}$ n'est pas une loi car, par exemple, elle ne fait rien correspondre au couple $(6\,;0)$).

02 * Exemples de lois associatives.

L'addition sur $\mathbb{N}$ (et sur $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$) ; la multiplication sur $\mathbb{N}$ (et sur $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$).

Soit A un ensemble ; on note $\mathcal{P}(A)$ l'ensemble des sous-ensembles de A ; l'intersection, qui aux sous-ensembles X et Y de A fait correspondre $X \cap Y$, est une loi associative ; il en est de même pour l'union sur $\mathcal{P}(A)$.

La loi qui, à deux éléments a et b de $\mathbb{N}$ (ou de $\mathbb{Z}$, ou de $\mathbb{D}$,...) fait correspondre le minimum de a et b est associative ; il en est de même pour le maximum.

Sur un ensemble B, la loi qui à un couple (u, v) d'éléments de B fait correspondre v est associative.

* Exemples de lois qui ne sont pas associatives.

La soustraction sur $\mathbb{Z}$ (et sur $\mathbb{D}$, sur $\mathbb{Q}$, sur $\mathbb{R}$).

La division sur $\mathbb{Q}^*$ (et sur $\mathbb{Q}_+^*$, sur $\mathbb{R}^*$,...) ; ainsi $(8 : 4) : 2 = 1$ et $8 : (4 : 2) = 4$.

L'exponentiation sur $\mathbb{N}^*$: ainsi $(2^3)^2 = 8^2 = 64$ et $2^{(3^2)} = 2^9 = 512$.

03 Soit B un ensemble ayant plus d'un élément ; la loi $(u, v) \longmapsto v$ sur B n'est pas commutative. A cette exception près, toutes les lois associatives citées à la question 02 sont commutatives ; les lois non associatives qui y sont citées ne sont pas non plus commutatives.

Pour d'autres exemples de lois associatives qui ne sont pas commutatives, voyez le paragraphe 1.4, page 41.

Au paragraphe 1.2.5, page 40 est donnée la table d'une loi qui est commutative, sans être associative. La loi $(u, v) \longmapsto \frac{u+v}{2}$ définie sur $\mathbb{D}$ (ou $\mathbb{Q}$, ou $\mathbb{R}$) est également commutative sans être associative ; elle n'a pas d'élément neutre.

04 Associativité : a ► b c ► d e ► f ► g
Commutativité : d ► e
Calcul numérique : b ► c g ► h ► i (2 fois)

05 Si la loi $*$ n'est pas commutative, il peut se faire qu'un élément f de E soit tel que, quel que soit a dans E, il soit vrai que $a * f = a$ et que, pourtant, il existe au moins un élément b de E tel que $f * b \neq b$; ainsi, quel que soit le réel x il est vrai que $x - 0 = x$ mais, par exemple, $0 - 4 \neq 4$ (dans un tel cas, on dit que f est neutre à droite). Naturellement, il peut

également se faire qu'un élément g de E soit tel que, quel que soit a dans E, il soit vrai que $g * a = a$ et que g ne soit pas neutre pour la loi $*$.

06 * Exemples de lois ayant un élément neutre.

L'addition sur $\mathbb{N}$ (et sur $\mathbb{Z}$,...) — élément neutre : 0.
La multiplication sur $\mathbb{N}$ — élément neutre : 1.
Si A est un ensemble, l'union sur $\mathcal{P}(A)$ — élément neutre : ϕ ; l'intersection sur $\mathcal{P}(A)$ — élément neutre : A.
Sur $\mathbb{N}$, la loi $(a, b) \longmapsto \max(a, b)$ — élément neutre : 0.

* Exemples de lois sans élément neutre.

La soustraction sur $\mathbb{Z}$ (et sur $\mathbb{D}$,...).
La division sur $\mathbb{Q}^*$.
L'exponentiation sur $\mathbb{N}^*$.
Sur $\mathbb{N}$, la loi $(a, b) \longmapsto \min(a, b)$: si e était neutre pour cette loi, il faudrait que $\min(e, x) = x$ quel que soit le naturel x, c'est-à-dire que $x \leqslant e$ quel que soit le naturel x ; autrement dit, e serait le maximum de $\mathbb{N}$!

07 $(a \perp b) \perp b = u \perp b = b$, $a \perp (b \perp b) = a \perp a = u$ et $b \neq u$.

08 L'élément a est symétrique de a', car $a * a' = a' * a = e$.

09 Exemples de monoïdes : $(\mathbb{N}, +)$, $(\mathbb{N}, \times)$, et de façon générale les couples de la forme $(A, +)$ et $(A, \times)$ où A est l'un des ensembles $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$ et $\mathbb{R}$. Si B est un ensemble, $(\mathcal{P}(B), \cup)$ et $(\mathcal{P}(B), \cap)$ sont des monoïdes ; si l'on note max la loi $(a, b) \longmapsto \max(a, b)$ sur $\mathbb{N}$, le couple $(\mathbb{N}, \max)$ est un monoïde (voyez en particulier la question 06). Notons $\vee$ la loi $(a, b) \longmapsto \sqrt{a^2 + b^2}$ sur $\mathbb{R}$ (ou sur $\mathbb{R}_+$) ; on constate que, quels que soient les éléments a, b et c de $\mathbb{R}$ (ou de $\mathbb{R}_+$),

$(a \vee b) \vee c = a \vee (b \vee c)$ $(= \sqrt{a^2 + b^2 + c^2})$ et $a \vee 0 = 0 \vee a = a$;

donc $(\mathbb{R}, \vee)$ est un monoïde, dont l'élément neutre est 0 (de même pour $\mathbb{R}_+$).

Par contre $(\{u, a, b\}, \perp)$ (page 40) n'est pas un monoïde, car la loi $\perp$ n'est pas associative ; $(\mathbb{N}, \min)$ non plus, car la loi $(a, b) \longmapsto \min(a, b)$ sur $\mathbb{N}$ n'a pas d'élément neutre. Pour les exemples suivants, associativité et élément neutre font défaut : $(\mathbb{Z}, -)$, $(\mathbb{Q}^*, :)$, $(\mathbb{N}^*, \exp)$ si l'on note exp l'exponentiation sur $\mathbb{N}^*$.

10 Parmi les exemples de monoïdes donnés à la question 09, les couples de la forme $(A, +)$ ou A est l'un des ensembles $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des groupes. De même $(\mathcal{P}(\phi), \cup)$ et $(\mathcal{P}(\phi), \cap)$ sont des groupes ; ces deux derniers exemples sont d'ailleurs dénués d'intérêt.

Aucun des autres monoïdes donnés en exemple à la question 09 n'est un groupe.

Remarquez que $(\mathbb{Q}^*, \times)$, $(\mathbb{Q}_+^*, \times)$, $(\mathbb{R}^*, \times)$ et $(\mathbb{R}_+^*, \times)$ sont des groupes et que $(\mathbb{D}^*, \times)$ n'en est pas un.

Vous pourrez également reprendre les exemples de groupes donnés dans la première partie : $(H, \oplus)$ («groupe de l'horloge» pages, 8 et s.), $(G, \circ)$ (premier «groupe de gobelets», pages 11 et s.), $(G_1, \circ)$ (deuxième «groupe de gobelets», pages 16 et s.) et $(P, *)$ (montre simplifiée, pages 18 et s.); et dans la deuxième partie : le groupe de Klein, en deux versions (pages 29 et s.) ; $(\mathbb{Z}, \perp)$ (pages 34 et s.). Par contre, $(H, \otimes)$ (pages 26 et s.) est un monoïde qui n'est pas un groupe.

11 Notons $\perp$ la première loi et $\bullet$ la seconde.
Elles sont associatives toutes les deux : quels que soient les réels a, b et c,

$(a \perp b) \perp c = a \perp (b \perp c) = a + b + c - 2$,
$(a \bullet b) \bullet c = a \bullet (b \bullet c) = a + b + c - bc - ca - ab + abc$.

Les deux lois ont un élément neutre : 1 pour $\perp$ et 0 pour $\bullet$.
Pour la loi $\perp$, tout réel a un symétrique : si $x \in \mathbb{R}$,

$$x \perp (2 - x) = x + (2 - x) - 1 = 1,$$

et comme la loi $\perp$ est commutative, $(2-x)\perp x = 1$. Donc $(\mathbb{R}, \perp)$ est un groupe.

Si $x \in \mathbb{R} \setminus \{1\}$,

$$x \bullet \frac{x}{x-1} = x + \frac{x}{x-1} - \frac{x^2}{x-1} = 0,$$

et puisque la loi $\bullet$ est commutative, $\frac{x}{x-1} \bullet x = 0$; donc si $x \in \mathbb{R} \setminus \{1\}$, le réel x admet un symétrique pour la loi $\bullet$, qui est $\frac{x}{x-1}$; remarquez qu'alors $\frac{x}{x-1} \in \mathbb{R} \setminus \{1\}$. Par contre 1 n'a pas de symétrique pour la loi $\bullet$: quel que soit le réel x, il est vrai que $x \bullet 1 = 1$ et donc que $x \bullet 1 \neq 0$. Donc $(\mathbb{R}, \bullet)$ n'est pas un groupe.

12 Soit X un ensemble à deux éléments ; notons a et b ces deux éléments. Sous cette hypothèse, S_X est formé de id_X et de la permutation t telle que $t(a) = b$ et $t(b) = a$. Voici la table de $(S_X, \circ)$ dans ce cas ; elle montre que le groupe est commutatif.

$\circ$	id_X	t
id_X	id_X	t
t	t	id_X

Soit X un singleton ; alors $S_X = \{id_X\}$, et le groupe $(S_X, \circ)$ est commutatif (toutes les lois sur un ensemble à un élément sont commutatives).

$\circ$	id_X
id_X	id_X

Nous n'examinerons pas ici le cas, peu intéressant, où $X = \phi$; indiquons seulement qu'avec les définitions usuelles, $(S_\phi, \circ)$ est un groupe à un élément.

Soit maintenant X un ensemble ayant au moins trois éléments ; soient a, b et c trois éléments distincts de X. Définissons les permutations p et q de X :

$p(a) = b$, $p(b) = a$ et, si $x \in X \setminus \{a, b\}$, alors $p(x) = x$;
$q(b) = c$, $q(c) = b$ et, si $x \in X \setminus \{b, c\}$, alors $q(x) = x$.

(Autrement dit, p échange a et b et laisse inchangés les autres élémebts de X, et q échange b et c et laisse inchangés les autre éléments de X).

Alors

$(q \circ p)(a) = q(p(a)) = q(b) = c$ et $(p \circ q)(a) = p(q(a)) = p(a) = b$;

donc

$q \circ p \neq p \circ q$, et $(S_X, \circ)$ n'est pas commutatif.

13 On constate que, quels que soient les éléments u, v et w de $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$, si $u = (u_1, u_2, u_3)$, etc...

$(u \square v) \square w = u \square (v \square w)$ $[= (u_1 + v_1 + w_1, u_2 + v_2 + w_3, u_3 + v_3 + w_3 + u_1v_2 + u_1w_2 + v_1w_2)]$

(et la loi est associative),

$u \square (0,0,0) = (0,0,0) \square u = u$ (et donc $(0,0,0)$ est neutre pour $\square$),

$(u_1, u_2, u_3) \square (-u_1, -u_2, -u_3 + u_1u_2) = (-u_1, -u_2, -u_3 + u_1u_2) \square (u_1, u_2, u_3) = (0,0,0)$ (et u admet un symétrique).

Donc $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}, \square)$ est un groupe. Il n'est pas commutatif : en effet, par exemple,

$(1,0,0) \square (0,1,0) = (1,1,1)$, $(0,1,0) \square (1,0,0) = (1,1,0)$ et $(1,1,1) \neq (1,1,0)$.

On peut remplacer $\mathbb{Z}$ en particulier par $\mathbb{D}$, $\mathbb{Q}$ ou $\mathbb{R}$.

14 Remarquons que $a = id_T$, et donc que a est une permutation de T. Montrons par exemple que b est une permutation de T : soient x et y des éléments de $\mathbb{Q} \setminus \{0, 1\}$; les égalités sui-

vantes sont équivalentes :

$$b(x) = y \quad ; \quad \frac{x-1}{x} = y \quad ; \quad x = \frac{1}{1-y} \quad ; \quad x = c(y).$$

Donc si $y \in T$, l'élément y est l'image par b d'un unique élément de T, qui est $c(y)$; donc b est bien une bijection de T vers T ; on remarque en outre que $b^{-1} = c$, et donc que c est aussi une permutation de T ; on procède de même pour f, g et h.

Le tableau suivant montre que la composée de deux de ces six applications est un élément de G ; autrement dit, que $\circ$ est une loi sur G. Suivant le **paragraphe 1.4.1**, elle est associative ; elle a un élément neutre, qui est a ; enfin chaque élément a un symétrique (a, f, g et h sont leurs propres symétriques, b et c sont symétriques l'un de l'autre).

$\circ$	a	b	c	f	g	h
a	a	b	c	f	g	h
b	b	c	a	g	h	f
c	c	a	b	h	f	g
f	f	h	g	a	c	b
g	g	f	h	b	a	c
h	h	g	f	c	b	a

Par exemple, $b \circ f = g$: en effet, quel que soit soit x dans T,

$$b \circ f(x) = b(f(x)) = b(\tfrac{1}{x}) = \frac{(\frac{1}{x}) - 1}{(\frac{1}{x})} = 1 - x = g(x).$$

Nous avons bien affaire à un groupe.

Mais ce groupe n'est pas commutatif : en effet, par exemple,

$$b \circ f = g, \quad f \circ b = h \quad \text{et} \quad g \neq h.$$

Remarquez qu'on aurait pu remplacer T par $\mathbb{R} \setminus \{0, 1\}$, ou encore par $\{-1, \frac{1}{2}, 2\}$; dans ce dernier cas, le groupe est le groupe des permutations de $\{-1, \frac{1}{2}, 2\}$.

15 Soient ϵ un élément de $\{-1, 1\}$ et b un entier. Soient t et u des entiers ; les égalités suivantes sont équivalentes (car $\frac{1}{\epsilon} = \epsilon$) :

$$u = \epsilon t + b, \quad t = \epsilon u - \epsilon b.$$

Donc si u est un entier, il est l'image par $(t \mapsto \epsilon t + b)$ d'un unique entier, $\epsilon u - \epsilon b$; donc $(t \mapsto \epsilon t + b)$ est une permutation de $\mathbb{Z}$.

Si ϵ et ϵ' sont dans $\{-1, 1\}$ et si b et b' sont des entiers,

$(t \mapsto \epsilon' t + b') \circ (t \mapsto \epsilon t + b) = (t \mapsto \epsilon' \epsilon t + \epsilon' b + b')$, et $\epsilon \epsilon' \in \{-1, 1\}$ et $\epsilon' b + b' \in \mathbb{Z}$; donc $\circ$ est une loi sur A.

Cette loi est associative d'après le paragraphe 1.4.1 et admet $id_{\mathbb{Z}}$ (c'est-à-dire $t \mapsto t$) comme élément neutre ; enfin, si $\epsilon \in \{-1, 1\}$ et $b \in \mathbb{Z}$,

$(t \mapsto \epsilon t + b) \circ (t \mapsto \epsilon t - \epsilon b) = (t \mapsto \epsilon t - \epsilon b) \circ (t \mapsto \epsilon t + b) = id_{\mathbb{Z}}$, donc tout élément de A a un symétrique pour la loi $\circ$. Finalement $(A, \circ)$ est un groupe. Il n'est pas commutatif car, par exemple,

$$(t \mapsto -t) \circ (t \mapsto t + 1) = (t \mapsto -t - 1), \quad (t \mapsto t + 1) \circ (t \mapsto -t) = (t \mapsto -t + 1) \text{ et}$$
$$(t \mapsto -t - 1) \neq (t \mapsto -t + 1).$$

Remarquez qu'on peut remplacer $\mathbb{Z}$ par $\mathbb{D}$, $\mathbb{Q}$ ou $\mathbb{R}$.

16 Exemples de lois régulières qui ne sont pas des lois de groupe : l'addition sur $\mathbb{N}$, la multiplication sur $\mathbb{N}^*$, sur $\mathbb{Z}^*$, sur $\mathbb{D}^*$, la soustraction sur $\mathbb{Z}$, la division sur $\mathbb{Q}^*$, l'exponentiation sur $\mathbb{N} \setminus \{0, 1\}$.

Exemples de lois qui ne sont pas régulières : la multiplication sur $\mathbb{N}$, sur $\mathbb{Z}$,... (par exemple : $0 \times 0 = 0 \times 7$ et $0 \neq 7$), l'exponentiation sur $\mathbb{N}^*$ (par exemple : $1^2 = 1^3$ et $2 \neq 3$) ; si A est un ensemble autre que ϕ, l'union et l'intersection sur $\mathcal{P}(A)$ (par exemple : $A \cup \phi = A \cup A$ et $\phi \neq A$, $\phi \cap \phi = \phi \cap A$ et $\phi \neq A$).

Remarque.

Pour qu'une loi $*$ sur un ensemble E soit régulière, il faut que pour **tout** élément a, **tout** élément x et **tout** élément y de E,

si $a * x = a * y$, alors $x = y$ (et si $x * a = y * a$, alors $x = y$).

Il suffit donc qu'il existe **un seul** élément a, **un seul** élément x et **un seul** élément y de E (même si $a = x$ ou $a = y$) tels que $a * x = a * y$ et $x \neq y$ pour que la loi ne soit pas régulière.

17 Dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{D}$, $\mathbb{Q}$, $\mathbb{R}$ la multiplication est distributive sur l'addition ; elle est distributive sur la soustraction dans $\mathbb{Z}$, $\mathbb{D}$,...

Quels que soient les éléments a, b et c de $\mathbb{N}^*$, il est vrai que $(b \times c)^a = (b^a) \times (c^a)$, mais $2^{(2 \times 1)} = 2^2 = 4$, $(2^2) \times (2^1) = 4 \times 2 = 8$ et $4 \neq 8$: l'exponentiation n'est pas distributive sur la multiplication dans $\mathbb{N}^*$ (on peut dire qu'elle est distributive à droite).

Soit A un ensemble ; l'union est distributive sur l'intersection, et l'intersection est distributive sur l'union dans $\mathcal{P}(A)$.

Sur $\mathbb{N}$, $\mathbb{Z}$,... l'addition est distributive sur la loi $(a, b) \longmapsto \max(a, b)$ et sur la loi $(a, b) \longmapsto \min(a, b)$: par exemple, si u, v et w sont des naturels, $u + \max(v, w) = \max(u + v, u + w)$ et, bien sûr, $\max(v, w) + u = \max(v + u, w + u)$.

Les lois $(u, v) \longmapsto \max(u, v)$ et $(u, v) \longmapsto \min(u, v)$ sont chacune distributives sur elles-mêmes ; par exemple, si u, v et w sont des naturels, $\max(u, \max(v, w)) = \max(\max(u, v), \max(u, w))$ $(= \max(u, v, w))$.

Soit E un ensemble ; la loi $(x, y) \longmapsto y$ sur E est distributive sur elle-même.

18 Soit x un élément de E ; avec les hypothèses faites,
$(e \bullet x) \top (e \bullet x) = (e \top e) \bullet x = e \bullet x = (e \bullet x) \top e$; donc

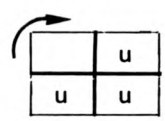
$$(e \bullet x) \top (e \bullet x) = (e \bullet x) \top e \ ;$$

puisque la loi $\top$ est régulière, $e \bullet x = e$; on montre de même que $x \bullet e = e$.

19 Supposons que u et v soient des éléments absorbants de F pour $\blacklozenge$; il en résulte que $u \blacklozenge v = u$, car u est absorbant, et que $u \blacklozenge v = v$, car v est absorbant ; donc $u = v$: il y a au plus un élément absorbant pour une loi donnée.

Supposons que F ait un élément absorbant u pour $\blacklozenge$.
Supposons d'abord que F ait au moins deux éléments ; soit a un élément de F autre que u ; alors $u \blacklozenge a = u \blacklozenge u$ $(= u)$, et $a \neq u$, donc la loi $\blacklozenge$ n'est pas régulière.

Supposons maintenant que F ait un seul élément ; notons u cet élément. Il existe une et une seule loi sur F, donnée par la table ci-contre ; cette loi est régulière et u est absorbant. Ce dernier cas a peu d'intérêt.



20 Supposons que $(E, \top)$ soit un groupe ; notons e son élément neutre.
Puisque $(E, \top)$ est un groupe, la loi $\top$ est régulière ; d'après la question 18, l'élément e, neutre pour la loi $\top$, est absorbant pour la loi $\bullet$.
D'après la question 19, si E a au moins deux éléments, la loi $\bullet$ n'est pas régulière car elle a un élément absorbant. Donc la loi $\bullet$ n'est pas une loi de groupe.

Concluons : si E a au moins deux éléments, $(E, \top)$ et $(E, \bullet)$ ne peuvent être des groupes tous les deux.

Si E a un seul élément, noté par exemple a, il y a une unique loi sur E donnée par la table ci-contre ; les lois $\top$ et $\bullet$ sont donc égales. On constate sans peine que cette unique loi est une loi de groupe, distributive sur elle-même.

	a
a	a

Si $E = \phi$, il ne peut exister d'élément neutre dans E et ni $(E, \top)$ ni $(E, \bullet)$ n'est un groupe. Ces deux derniers cas sont sans intérêt.

On sait que dans $\mathbb{Q}$ (et dans $\mathbb{R}$) l'élément neutre de l'addition est absorbant pour la multiplication, et que $(\mathbb{Q}, \times)$ n'est pas un groupe ; ce qui précède, montre que cela n'a rien de surprenant, et est même inévitable dès lors qu'on souhaite que $(\mathbb{Q}, +)$ soit un groupe et que la multiplication soit distributive sur l'addition ; aucun «bricolage» ne permettra de modifier cet état de fait.

On sait également que les éléments neutres de l'addition et de la multiplication de $\mathbb{Q}$ sont distincts, et que 0 n'a pas d'inverse : ceci est également inévitable. En effet supposons à nouveau que E ait plus d'un élément, que $(E, \top)$ soit un groupe dont l'élément neutre est noté e, et que la loi $\bullet$ sur E soit distributive sur la loi $\top$; supposons en outre que la loi $\bullet$ ait un élément neutre, noté f.

Soit alors a un élément de E autre que e ; alors $a \bullet e = e$, puisque e est absorbant ; donc $a \bullet e \neq a$ et e n'est pas neutre pour $\bullet$ il en résulte que $f \neq e$. D'autre part, quel que soit x dans E, il est vrai que $e \bullet x = e$, et donc que $e \bullet x \neq f$: le neutre e de la loi $\top$ n'a donc pas de symétrique pour la loi $\bullet$ (ce serait un élément e' tel que $e \bullet e' = f$).

21 Notons e l'élément neutre de la loi $\perp$.

Puisque $(K, \perp)$ est un groupe, la loi $\perp$ est régulière ; donc, d'après la question 18, l'élément e est absorbant pour la loi ∇.

Soit k un élément de K distinct de e (il en existe : K a au moins deux éléments) : $e \nabla k = e$ et $e \neq k$, donc e n'est pas neutre pour la loi ∇.

On voit pourquoi on a exclu le cas où K est un singleton : soit k un objet ; sur $\{k\}$ il existe une unique loi interne, qui à (k, k) fait correspondre k ; si on la note à la fois $\perp$ et ∇, alors $(\{k\}, \perp)$ est un groupe, $(\{k\}, \nabla)$ est un monoïde et la loi ∇ est distributive sur la loi $\perp$. C'est totalement dépourvu d'intérêt.

22 Notons u l'élément neutre de la loi ∇.

Soient x et y des éléments de E ; on constate

d'une part que
$$\begin{aligned}(u \perp u) \nabla (x \perp y) &= (u \nabla (x \perp y)) \perp (u \nabla (x \perp y)),\\ &= (x \perp y) \perp (x \perp y),\\ &= x \perp y \perp x \perp y\ ;\end{aligned}$$

et de l'autre que
$$\begin{aligned}(u \perp u) \nabla (x \perp y) &= ((u \perp u) \nabla x) \perp ((u \perp u) \nabla y),\\ &= ((u \nabla x) \perp (u \nabla x)) \perp ((u \nabla y) \perp (u \nabla y)),\\ &= x \perp x \perp y \perp y.\end{aligned}$$

Donc
$$\begin{aligned}x \perp y \perp x \perp y &= x \perp x \perp y \perp y\ ; \quad \text{puisque la loi } \perp \text{ est régulière,}\\ y \perp x \perp y &= x \perp y \perp y, \quad \text{et}\\ y \perp x &= x \perp y.\end{aligned}$$

23 Notons u l'élément neutre de la loi ∇.

On sait que $u \neq e$ (question 21), et que e est absorbant pour la loi ∇ (voyez la réponse à la question 21). Donc, quel que soit x dans K,

$$e \nabla x = e \quad \text{et, donc} \quad e \nabla x \neq u\ :$$

il n'existe aucun élément e' dans K tel que $e \nabla e' = u$, l'élément e n'a pas de symétrique pour la loi ∇.

Soit a et b des éléments de $K^{\square}$; ils ont des symétriques pour la loi ∇, notons-les a' et b' :

$$(a \nabla b) \nabla (b' \nabla a') = a \nabla (b \nabla b') \nabla a' = a \nabla u \nabla a' = a \nabla a' = u,$$

et de même $(b' \nabla a') \nabla (a \nabla b) = u$; donc $a \nabla b$ a un symétrique pour la loi ∇ (qui est $b' \nabla a'$), et $a \nabla b \in K^{\square}$: l'ensemble $K^{\square}$ est stable pour la loi ∇.

Soit a, b et c des éléments de $K^{\square}$; ce sont des éléments de K et la loi ∇ est associative sur K, donc,

$$(a \nabla b) \nabla c = a \nabla (b \nabla c) \ :$$

la restriction de la loi ∇ à $K^{\square}$ est associative.

Puisque $u \nabla u = u$, l'élément u a un symétrique pour la loi ∇ (lui-même) ; donc $u \in K^{\square}$, et u est évidemment élément neutre de la restriction de la loi ∇ à $K^{\square}$.

Soit a un élément de $K^{\square}$; notons a' son symétrique pour la loi ∇ :

$$a \nabla a' = a' \nabla a = u.$$

Donc a est le symétrique de a', et $a' \in K^{\square}$: l'élément a a un symétrique dans $K^{\square}$.

Nous pouvons conclure : $(K^{\square}, \nabla)$ est un groupe.

24 $Z^{\square} = \{-1, 1\}$.

$D^{\square}$ est l'ensemble les élément de la forme $\epsilon 2^p 5^q$ où $\epsilon \in \{-1, 1\}$, $p \in \mathbb{Z}$ et $q \in \mathbb{Z}$; par exemple $-\frac{5}{4} \in \mathbb{D}^{\square}$ car $-\frac{5}{4} = (-1) \times 2^{-2} \times 5^1$.

25 Etudions l'équation en x dans $\mathbb{R}$

$$|x - 2| = 2x - 1.$$

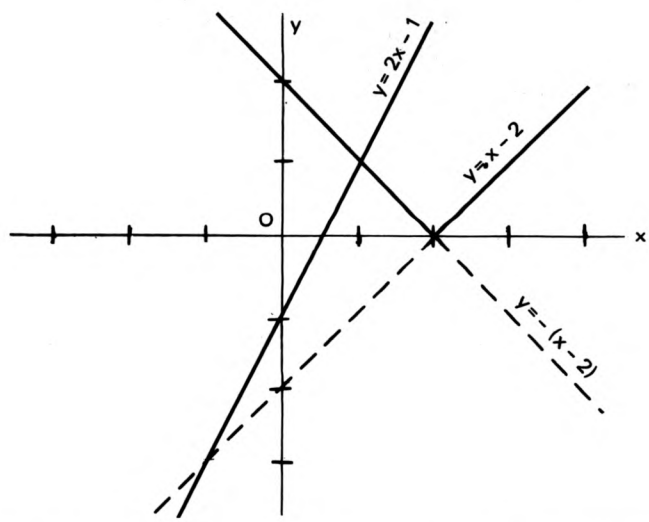
Si s est une solution de cette équation,

$$s - 2 = 2s - 1 \quad \text{ou} \quad s - 2 = -(2s - 1) = -2s + 1 \ ;$$

on en déduit que

$$s = -1 \quad \text{ou} \quad s = 1.$$

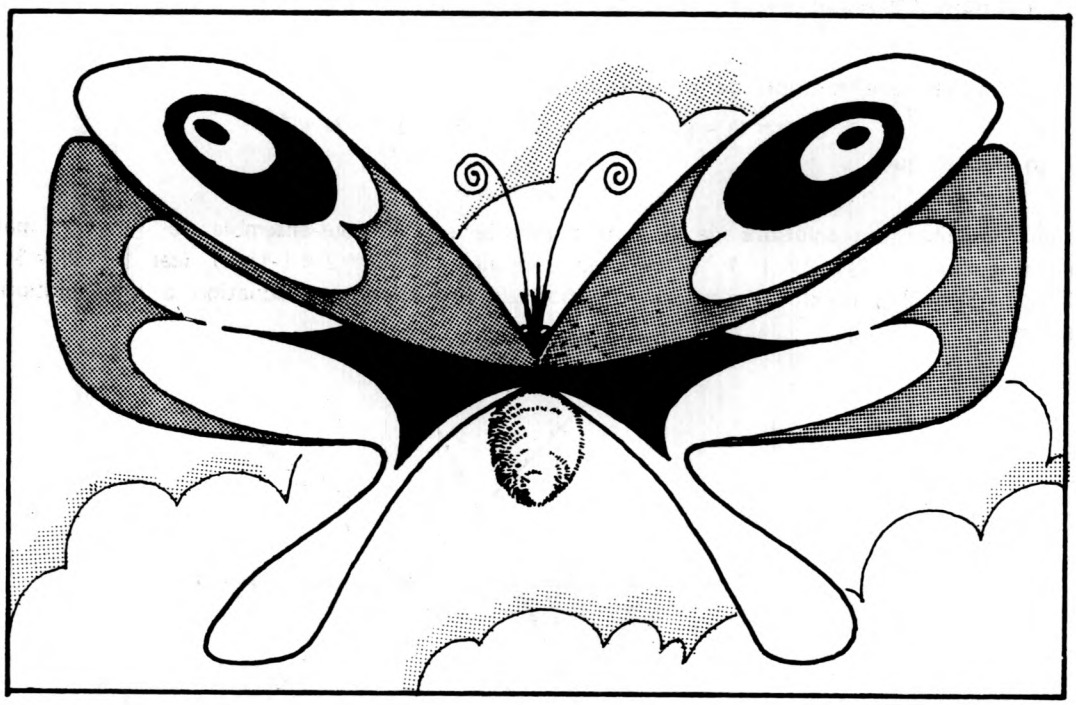
Donc l'ensemble des solutions de l'équation étudiée est un sous-ensemble de $\{-1, 1\}$; mais s'il est bien vrai que $|1 - 2| = 2 \times 1 - 1 \ (= 1)$, au contraire $|-1 - 2| \neq 2 \times (-1) - 1$ (car $|-1 - 2| = 3$ et $2 \times (-1) - 1 = -3$) ; donc -1 n'est pas solution de l'équation, et l'équation a une solution unique qui est 1.



26 Résolvons par exemple l'équation (1) : puisque $(A, \circ)$ est un groupe, les théorèmes généraux nous assurent que cette équation a une solution unique. Notons ϵ l'élément de $\{-1, 1\}$ et p l'entier tels que $t \longmapsto \epsilon t + p$ soit solution :

$$(t \longmapsto \epsilon t + p) \circ (t \longmapsto t + 2) = (t \longmapsto -t + 4), \quad \text{donc}$$
$$(t \longmapsto \epsilon t + 2\epsilon + p) = (t \longmapsto -t + 4), \quad \text{et}$$
$$\epsilon = -1 \quad \text{et} \quad p = 6.$$

La solution de (1) est $t \longmapsto -t + 6$. Elle est différente de la solution de l'équation (2), qui est $t \longmapsto -t + 2$. Par contre les équations (3) et (4) ont la même solution : $t \longmapsto t - 6$.



INDEX TERMINOLOGIQUE

Abélien (groupe –) 41
Δ Absorbant 44
Δ Anneau 45
Δ Anneau unitaire 44
Δ Anneau unitaire commutatif 45
Application composée 41
Associative (loi –) 38

Δ Carré latin 48
Commutatif (groupe –) 41
Commutative (loi –) 38
Composé (de deux éléments) 37
Composée (application –) 41
Composition (loi de –) 37
Δ Corps 45

Distributive (loi –) 44

Δ Elément absorbant 44
Elément neutre 39
Elément régulier 43
Elément simplifiable 43
Equation 46

Δ Fermé (sous-ensemble –) 44

Groupe 40
Groupe abélien 41
Groupe commutatif 41
Δ Groupe multiplicatif d'un anneau unitaire 45

Δ Induite (loi –) 44
Interne (loi –) 37
Inverse 40

Δ Latin (carré –) 48
Loi associative 38
Loi commutative 38
Loi de composition 37
Loi distributive 44
Δ Loi induite 44
Loi interne 37
Loi régulière 43
Loi simplifiable 43

Δ Monoïde 40

Neutre 39
Neutre (élément –) 39

Opération 37
Opposé 40

Δ Permutation 41
Priorité 44

Régulier (élément –) 43
Régulière (loi –) 43
Résoudre une équation 46
Restriction 44

Simplifiable (élément –) 43
Simplifiable (loi –) 43
Solution 46
Δ Stable (sous-ensemble –) 44
Symétrique 39

Nous avons marqué du signe Δ les termes qu'il nous semble inutile, voire nuisible de proposer à de jeunes élèves.