

Groupes

Table des matières

1 Généralités	1
2 Sous-groupes	1
3 Morphismes de groupes	2
4 Groupes finis	3

Sont censées connues : la définition d'une loi de composition sur un ensemble E , et les propriétés intéressantes (associativité, commutativité, élément neutre, élément régulier, élément inversible, inverse, partie stable).

1 Généralités

Définition : un *groupe* est un couple (G, \star) où G est un ensemble *non vide* muni d'une loi \star vérifiant :

- (G1) \star est associative ;
- (G2) \star possède un élément neutre ;
- (G3) tout élément de G possède un symétrique pour la loi \star .

Définition : un groupe (G, \star) est dit *commutatif* (ou *abélien*) lorsque la loi \star est commutative.

Exemples — $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, (\mathbb{Q}^*, \times) , (\mathbb{R}_+^*, \times) , (\mathbb{U}, \times) où \mathbb{U} désigne l'ensemble des complexes de module 1 sont des groupes commutatifs. Pour $n \geq 3$, le groupe des permutations de $\llbracket 1, n \rrbracket$ (ou *groupe symétrique*), noté (\mathfrak{S}_n, \circ) , n'est pas commutatif : les transpositions $\tau_{1,2}$ et $\tau_{1,3}$ ne commutent pas. Pour la composition, le groupe des «manipulations» du cube de Rubik n'est pas commutatif.

Notation : un groupe commutatif est souvent noté additivement : la loi est notée $+$, le symétrique de a est noté $-a$ et appelé *opposé* de a . Avec la notation multiplicative, la loi est notée \cdot ou \times , voire est omise ; le symétrique de x est noté x^{-1} , on parle alors de l'*inverse* de x . Si le groupe est abélien, on peut noter $\frac{1}{x}$ pour x^{-1} ; sinon, cette notation est ambiguë : $\frac{a}{b}$ désigne-t-il $a \star b^{-1}$ ou $b^{-1} \star a$?). Lorsqu'aucune confusion n'est possible, on parlera du groupe G sans préciser la loi.

Proposition : tout élément d'un groupe (G, \star) est régulier pour la loi \star .

Preuve : soient a, x et y trois éléments de G . Notons e le neutre de G . Alors :

$$a \star x = a \star y \Rightarrow a^{-1} \star (a \star x) = a^{-1} \star (a \star y) \Rightarrow (a^{-1} \star a) \star x = (a^{-1} \star a) \star y \Rightarrow e \star x = e \star y \Rightarrow x = y$$

Définition : l'*ordre* d'un groupe G fini est le nombre d'éléments de G .

Exemples — l'ordre de \mathfrak{S}_n est $n!$; l'ordre du groupe des manipulations du cube de Rubik est $2^{10} \cdot 3^7 \cdot 8! \cdot 12!$.

2 Sous-groupes

Définition : une partie H *non vide* d'un groupe (G, \star) est un *sous-groupe* de G si elle est stable pour la loi \star , et si celle-ci induit sur H une structure de groupe.

Exemples — $(\mathbb{Z}, +)$ est un sous-groupe de $(\mathbb{R}, +)$; (\mathbb{R}_+^*, \times) est un sous-groupe de (\mathbb{R}^*, \times) ; (\mathbb{U}, \times) est un sous-groupe de (\mathbb{C}^*, \times) ; tout groupe G contient les sous-groupes G et $\{e\}$ (confondus lorsque $|G| = 1$).

Proposition : le neutre de G est aussi celui de H .

Preuve : notons e_G le neutre de G , et e_H celui de H . Alors $e_G \star e_H = e_H = e_H \star e_G$ donc $e_G = e_H$ puisque e_H est régulier.

Proposition : le symétrique dans H d'un élément a de H est égal à son symétrique dans G .

Preuve: notons a^{-1} (resp. a') le symétrique de a dans G (resp. H). Alors $a \star a' = e_H = e_G$, et de même $a' \star a = e_G$ donc $a' = a^{-1}$.

Remarque: voici une façon peut-être plus claire de définir un sous-groupe d'un groupe (G, \star) : c'est une partie H non vide de G , stable pour la loi \star , contenant le neutre de G et stable pour le passage à l'inverse. La proposition suivante donne une caractérisation «rapide».

Proposition: H est un sous-groupe de (G, \star) ssi:

- H est non vide;
- si x et y sont dans H , alors $x \star y^{-1}$ est dans H .

Preuve: le sens direct est banal. Pour la réciproque: H n'est pas vide: soit $a \in H$; alors le neutre $e = a \star a^{-1}$ est dans H ; soit maintenant $b \in H$ quelconque: $b^{-1} = e \star b^{-1}$ est dans H ; soient enfin $b, c \in H$ quelconques: $b \star c = b \star (c^{-1})^{-1}$ est dans H .

Proposition: l'intersection de deux sous-groupes d'un même groupe G est encore un sous-groupe de G .

Preuve: le neutre de G est dans H_1 et H_2 , donc dans $H_1 \cap H_2$, qui du coup n'est pas vide. Soient a et b deux éléments de $H_1 \cap H_2$: alors a et b sont dans H_1 , donc $a \star b^{-1}$ est aussi dans H_1 ; même raisonnement pour H_2 . Donc $a \star b^{-1}$ est dans $H_1 \cap H_2$.

Remarque: plus généralement, on peut montrer que l'intersection d'une famille *quelconque* de sous-groupes d'un même groupe G est encore un sous-groupe de G .

3 Morphismes de groupes

Définition: soient (G, \star) et (H, \wedge) deux groupes; une fonction $p : G \mapsto H$ est un (*homo*)*morphisme* de groupes si elle vérifie $p(x \star y) = p(x) \wedge p(y)$ quels que soient $x, y \in G$.

Définition: un *isomorphisme* de groupes est un morphisme bijectif; un automorphisme d'un groupe (G, \star) est un isomorphisme de G sur lui-même.

Exemples — la fonction $x \mapsto x^2$ est un morphisme du groupe (\mathbb{R}^*, \times) sur (\mathbb{R}_+^*, \times) , surjectif mais non injectif; la fonction \exp est un isomorphisme du groupe $(\mathbb{R}, +)$ sur le groupe (\mathbb{R}^*, \times) ; la fonction $t \mapsto e^{it}$ est un morphisme de $(\mathbb{R}, +)$ sur (\mathbb{U}, \times) , surjectif mais non injectif; la fonction $z \mapsto \bar{z}$ est un automorphisme de $(\mathbb{C}, +)$ et de (\mathbb{C}^*, \times) . Pour tout groupe G de neutre e , id_G et $x \mapsto e$ sont des morphismes de G sur lui-même.

Proposition: la composée de deux morphismes de groupes est un morphisme de groupes.

Preuve: soient G, H, K trois groupes, $p : G \mapsto H$ et $q : H \mapsto K$ deux morphismes de groupes. Alors, en notant \star les lois des trois groupes:

$$(q \circ p)(a \star b) = q(p(a \star b)) = q(p(a) \star p(b)) = q(p(a)) \star q(p(b)) = (q \circ p)(a) \star (q \circ p)(b)$$

Proposition: soient G et H deux groupes et p un isomorphisme de G sur H . Alors p^{-1} est un isomorphisme de H sur G .

Preuve: soient $x, y \in H$. Comme p est bijectif, il existe $a, b \in G$ tels que $p(a) = x$ et $p(b) = y$; alors $a = p^{-1}(x)$ et $b = p^{-1}(y)$. Par suite, $p(ab) = xy$, donc $ab = p^{-1}(xy)$. Donc $p^{-1}(x) \star p^{-1}(y) = ab = p^{-1}(xy)$.

Proposition: l'ensemble des automorphismes d'un groupe G est noté $\text{Aut}(G)$; c'est un groupe pour la loi \circ .

Preuve: id_G est le neutre de $\text{Aut}(G)$; il est clair que la composée de deux automorphismes est elle-même un automorphisme; enfin, si p est un automorphisme de G , alors c'est un morphisme bijectif, donc sa bijection réciproque est un morphisme, et elle est bijective (établi plus haut).

Proposition: soient G et H deux groupes et $p : G \mapsto H$ un morphisme de groupes; soient J un sous-groupe de G , et K un sous-groupe de H . Alors $p(J)$ est un sous-groupe de H et $p^{-1}(K)$ est un sous-groupe de G .

Preuve: soient $x, y \in p(J)$: il existe $a, b \in G$ tels que $p(a) = x$ et $p(b) = y$; alors $x \star y = p(a) \star p(b) = p(a \star b)$, et donc $x \star y \in p(J)$. Soient maintenant $c, d \in p^{-1}(K)$: alors $p(c)$ et $p(d)$ sont dans K ; du coup, $p(c \star d) = p(c) \star p(d)$ est dans K , et donc $c \star d$ est dans $p^{-1}(K)$.

Remarque: en particulier, $p^{-1}(\{e_H\})$ est un sous-groupe de G appelé *noyau* de p et noté $\ker(p)$; et $p(G)$ est un sous-groupe de H , appelé *image* de p et noté $\text{im}(p)$.

Proposition: un morphisme de groupes $p : G \mapsto H$ est injectif ssi $\ker(p) = \{e_G\}$.

Preuve: soit $a \in \ker(p)$; alors $p(a) = e_H$; mais $p(e_G) = e_H$; comme p est injectif, $a = e_G$.

Remarque: sur tout ensemble de groupes, la relation *est isomorphe à* est une équivalence, en ce sens que:

- tout groupe G est isomorphe à lui-même (via l'automorphisme id_G);

- si G est isomorphe à H , alors H est isomorphe à G (via l'isomorphisme inverse);
- si G est isomorphe à H (via p) et H isomorphe à K (via q), alors G est isomorphe à K (via $q \circ p$).

Remarque : en pratique, on confond souvent deux groupes isomorphes. Classifier les groupes, c'est déterminer les différentes classes modulo cette relation, et, pour chacune d'entre elles, préciser un représentant. Ce travail de classification a été achevé vers 1985 pour les groupes finis dits *simples*, qui sont (un peu) aux groupes ce que les nombres premiers sont aux entiers naturels : un groupe fini quelconque est toujours le produit (en un certain sens) de groupes finis simples.

4 Groupes finis

Remarque : un groupe fini peut être décrit par une *table*, comme la suivante, qui est la table de la multiplication dans \mathbb{U}_3 ; j désigne le complexe $\exp\left(\frac{2i\pi}{3}\right)$.

\times	1	j	j^2
1	1	j	j^2
j	j	j^2	1
j^2	j^2	1	j

On trouve des tables de ce genre pour l'addition et la multiplication des nombres de 1 à 10 au dos de certains cahiers d'écolier.

Définition : un *carré latin* d'ordre n est un tableau à n lignes et n colonnes, vérifiant la propriété suivante : dans chaque ligne et dans chaque colonne, chacun des nombres 1 à n apparaît une fois (et une seule, en application du principe des tiroirs).

Exemple — une grille de Sudoku (remplie sans erreur) est un carré latin d'ordre 9.

Remarque : nous généralisons cette notion comme suit : soit $E = \{x_1, x_2, \dots, x_n\}$ un ensemble. Un carré latin d'ordre n basé sur E est un tableau à n lignes et n colonnes, vérifiant la propriété suivante : dans chaque ligne et dans chaque colonne, chacun des éléments de E apparaît une fois (et une seule, donc).

Proposition : la table d'un groupe G fini est un carré latin.

Preuve : Observons par exemple une ligne : soit a l'élément placé devant la ligne. Comme a est régulier, la fonction $x \in G \mapsto a \star x$ est injective ; donc tous les éléments de la ligne sont distincts ; de par le principe des tiroirs, chacun apparaît exactement une fois.

Nous allons maintenant décrire les groupes d'ordre 1 à 3 ; pour chaque ordre, nous donnerons un groupe *abstrait* et plusieurs groupes *concrets*. Pour les groupes abstraits, le neutre sera toujours noté e .

Voici d'abord quelques groupes d'ordre 1 :

\star	e
e	e

+	0
0	0

\times	1
1	1

Et voici quelques groupes d'ordre 2 ; le deuxième est la table d'addition modulo 2.

\star	e	a
e	e	a
a	a	e

+	0	1
0	0	1
1	1	0

\times	1	-1
1	1	-1
-1	-1	1

Voici le groupe abstrait d'ordre 3 :

\star	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Notez que le remplissage de la table de ce groupe ne pose aucun problème : dans la première ligne et la première colonne, les valeurs sont évidentes ; puis, comme a et b sont distincts de e , le produit $a \star b$ ne peut être égal ni à a , ni à b , donc il est égal à e . Le reste se remplit automatiquement.

Exercice — Montrez qu'il existe deux groupes abstraits d'ordre 4 ; pour chacune des deux structures mises en évidence, donnez un exemple de groupe concret qui lui est isomorphe. Indications : la première ligne et la première colonne ne posent aucun problème. Observez ensuite que : soit chacun des éléments a , b et c est son propre inverse ; soit l'un de ces éléments (disons a) est son propre inverse, tandis que b et c sont inverses l'un de l'autre. Complétez alors chacune des deux tables.

FIN