Problems and Solutions for Groups, Lie Groups, Lie Algebras with Applications

Willi-Hans Steeb
Igor Tanski
Yorick Hardy

World Scientific

Problems and Solutions for Groups, Lie Groups, Lie Algebras with Applications

Willi-Hans Steeb
Igor Tanski
Yorick Hardy
University of Johannesburg, South Africa

World Scientific

NEW JERSEY · LONDON · SINGAPORE · BEIJING · SHANGHAI · HONG KONG · TAIPEI · CHENNAI

Published by

World Scientific Publishing Co. Pte. Ltd.
5 Toh Tuck Link, Singapore 596224
USA office: 27 Warren Street, Suite 401-402, Hackensack, NJ 07601
UK office: 57 Shelton Street, Covent Garden, London WC2H 9HE

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

PROBLEMS AND SOLUTIONS FOR GROUPS, LIE GROUPS, LIE ALGEBRAS WITH APPLICATIONS

ISBN-13 978-981-4383-90-5
ISBN-10 981-4383-90-2

Printed in Singapore by World Scientific Printers.

Preface

The purpose of this book is to supply a collection of problems in group theory, Lie group theory and Lie algebras. Furthermore, chapter 4 contains applications of these topics. Each chapter contains 100 completely solved problems. Chapters 1, 2 and 3 give a short but comprehensive introduction to the topics providing all the relevant definitions and concepts. Chapters 1, 2 and 3 also contain two solved programming problems and eight supplementary problems. Chapter 4 contains 10 solved programming problems and 10 supplementary problems. Chapter 4 covers mainly applications in mathematical and theoretical physics as well as quantum mechanics, differential geometry and relativity. Problems cover beginner, advanced and research topics. The problems are self-contained.

Accompanying problem books for this book are:

Problems and Solutions in Introductory and Advanced Matrix Calculus

by Willi-Hans Steeb
World Scientific Publishing, Singapore 2006
ISBN 981 256 916 2
`http://www.worldscibooks.com/mathematics/6202.html`

Problems and Solutions in Quantum Computing and Quantum Information, third edition

by Willi-Hans Steeb and Yorick Hardy
World Scientific, Singapore, 2006
ISBN 981-256-916-2
`http://www.worldscibooks.com/physics/6077.html`

The International School for Scientific Computing (ISSC) provides certificate courses for this subject. Please contact the author if you want to do this course or other courses of the ISSC.

e-mail addresses of the authors:

`steebwilli@gmail.com`
`yorickhardy@gmail.com`

Home page of the authors:

`http://issc.uj.ac.za`

Notation

$:=$	is defined as
$\in$	belongs to (a set)
$\notin$	does not belong to (a set)
$T \subset S$	subset T of set S
$S \cap T$	the intersection of the sets S and T
$S \cup T$	the union of the sets S and T
$\emptyset$	empty set
$\mathbb{N}$	set of natural numbers
$\mathbb{Z}$	set of integers
$\mathbb{Q}$	set of rational numbers
$\mathbb{R}$	set of real numbers
$\mathbb{R}^+$	set of nonnegative real numbers
$\mathbb{C}$	set of complex numbers
$\mathbb{R}^n$	n-dimensional Euclidean space
	space of column vectors with n real components
$\mathbb{C}^n$	n-dimensional complex linear space
	space of column vectors with n complex components
$\mathcal{H}$	Hilbert space
i	$\sqrt{-1}$
$\Re z$	real part of the complex number z
$\Im z$	imaginary part of the complex number z
$\|z\|$	modulus of the complex number z
	$\|x+iy\| = (x^2+y^2)^{1/2}, \ x, y \in \mathbb{R}$
$f(S)$	image of the set S under the mapping f
$f \circ g$	composition of two mappings $(f \circ g)(x) = f(g(x))$
G	group
$Z(G)$	center of the group G
$\mathbb{Z}_n$	cyclic group $\{0, 1, \ldots, n-1\}$
	under addition modulo n
G/N	factor group
D_n	nth dihedral group
S_n	symmetric group on n letters, permutation group
A_n	alternating group on n letters, alternating group
L	Lie algebra
$\mathbf{x}$	column vector in the vector space $\mathbb{C}^n$
$\mathbf{x}^T$	transpose of $\mathbf{x}$ (row vector)
$\mathbf{0}$	zero (column) vector
$\\|\cdot\\|$	norm

$\mathbf{x} \cdot \mathbf{y} \equiv \mathbf{x}^* \mathbf{y}$	scalar product (inner product) in $\mathbb{C}^n$
$\mathbf{x} \times \mathbf{y}$	vector product in $\mathbb{R}^3$
S^2	two sphere
A, B, C	$m \times n$ matrices
$\det(A)$	determinant of a square matrix A
$\mathrm{tr}(\mathrm{A})$	trace of a square matrix A
$\mathrm{rank}(A)$	rank of a matrix A
A^T	transpose of the matrix A
$\overline{A}$	conjugate of the matrix A
A^*	conjugate transpose of matrix A
$A^\dagger$	conjugate transpose of matrix A (notation used in physics)
A^{-1}	inverse of the square matrix A (if it exists)
I_n	$n \times n$ unit matrix
I	unit operator
0_n	$n \times n$ zero matrix
AB	matrix product of an $m \times n$ matrix A and an $n \times p$ matrix B
$[A, B] := AB - BA$	commutator of square matrices A and B
$[A, B]_+ := AB + BA$	anticommutator of square matrices A and B
$A \otimes B$	Kronecker product of matrices A and B
$A \oplus B$	Direct sum of matrices A and B
δ_{jk}	Kronecker delta with $\delta_{jk} = 1$ for $j = k$ and $\delta_{jk} = 0$ for $j \neq k$
λ	eigenvalue
ϵ	real parameter
t	time variable
$\hat{H}$	Hamilton operator
$\hat{N}$	Number operator
g	metric tensor field
ϵ	real parameter
$\wedge$	exterior product
d	exterior derivative

The *Pauli spin matrices* are used extensively in the book. They are given by

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

In some cases we will also use σ_1, σ_2 and σ_3 to denote σ_x, σ_y and σ_z .

Contents

Chapter 1

Groups

A *group* G is a set of objects $\{a, b, c, \ldots\}$ (not necessarily countable) together with a binary operation which associates with any ordered pair of elements a, b in G a third element ab in G (closure). The binary operation (called group multiplication) is subject to the following requirements:

1) There exists an element e in G called the *identity element* (also called *neutral element*) such that $eg = ge = g$ for all $g \in G$.
2) For every $g \in G$ there exists an *inverse element* g^{-1} in G such that $gg^{-1} = g^{-1}g = e$.
3) *Associative law.* The identity $(ab)c = a(bc)$ is satisfied for all $a, b, c \in G$.

If $ab = ba$ for all $a, b \in G$ we call the group *commutative.*

If G has a finite number of elements it has *finite order* $n(G)$, where $n(G)$ is the number of elements. Otherwise, G has infinite order. *Lagrange theorem* tells us that the order of a subgroup of a finite group is a divisor of the order of the group.

If H is a subset of the group G closed under the group operation of G, and if H is itself a group under the induced operation, then H is a *subgroup* of G.

Let G be a group and S a subgroup. If for all $g \in G$, the *right coset*

$$Sg := \{ sg \, : \, s \in S \}$$

is equal to the *left coset*

$$gS := \{ gs : s \in S \}$$

then we say that the subgroup S is a normal or invariant subgroup of G. A subgroup H of a group G is called a *normal subgroup* if $gH = Hg$ for all $g \in G$. This is denoted by $H \lhd G$. We also define

$$gHg^{-1} := \{ ghg^{-1} : h \in H \}.$$

The *center* $Z(G)$ of a group G is defined as the set of elements $z \in G$ which commute with all elements of the group, i.e.

$$Z(G) := \{ z \in G : zg = gz \text{ for all } g \in G \}.$$

Let G be a group. For any subset X of G, we define its *centralizer* $C(X)$ to be

$$C(X) := \{ y \in G : xy = yx \text{ for all } x \in X \}.$$

If $X \subset Y$, then $C(Y) \subset C(X)$.

A *cyclic group* G is a group containing an element g with the property that every other element of G can be written as a power of g, i.e. such that for all $h \in G$, for some $n \in \mathbb{Z}$, $h = g^n$. We then say that G is the cyclic group generated by g.

Let $(G_1, *)$ and $(G_2, \circ)$ be groups. A function $f : G_1 \to G_2$ with

$$f(a * b) = f(a) \circ f(b), \qquad \text{for all } a, b \in G_1$$

is called a *homomorphism*. If f is invertible, then f is an *isomorphism*.

Groups have matrix representations with invertible $n \times n$ matrices and matrix multiplication as group multiplication. The identity element is the identity matrix. The inverse element is the inverse matrix. An important subgroup is the set of unitary matrices U, where $U^* = U^{-1}$.

Let $GL(n, \mathbb{F})$ be the group of invertible $n \times n$ matrices with entries in the field $\mathbb{F}$, where $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$. Let G be a group. A *matrix representation* of G over the field $\mathbb{F}$ is a homomorphism ρ from G to $GL(n, \mathbb{F})$. The degree of ρ is the integer n. Let $\rho : G \to GL(n, \mathbb{F})$. Then ρ is a representation if and only if

$$\rho(g \circ h) = \rho(g)\rho(h)$$

for all $g, h \in G$.

Problem 1. Let $x, y \in \mathbb{R}$. Does the composition

$$x \bullet y := \sqrt[3]{x^3 + y^3}$$

define a group?

Solution 1. Yes. We have $\sqrt[3]{x^3 + y^3} \in \mathbb{R}$. The neutral element is 0. The inverse element of x is $-x$. The associative law

$$\begin{aligned}(x \bullet y) \bullet z &= (\sqrt[3]{x^3 + y^3}) \bullet z = \sqrt[3]{(\sqrt[3]{x^3 + y^3})^3 + z^3} \\ &= \sqrt[3]{x^3 + y^3 + z^3} = \sqrt[3]{x^3 + (\sqrt[3]{y^3 + z^3})^3} \\ &= x \bullet (y \bullet z)\end{aligned}$$

also holds. The group is commutative since $x \bullet y = y \bullet x$ for all $x, y \in \mathbb{R}$.

Problem 2. Let $x, y \in \mathbb{R} \setminus \{0\}$ and $\cdot$ denotes multiplication in $\mathbb{R}$. Does the composition

$$x \bullet y := \frac{x \cdot y}{2}$$

define a group?

Solution 2. Yes. We have $(x \cdot y)/2 \in \mathbb{R} \setminus \{0\}$. The neutral element is 2 and $4/x$ is inverse to x. The associative law also holds. The group is commutative.

Problem 3. Let $x, y \in \mathbb{R}$. Is the composition $x \bullet y := |x + y|$ associative? Here $|\,.\,|$ denotes the absolute value.

Solution 3. The answer is no. We have

$$0 = |(|1 + (-1)|) + 0| \neq |1 + (|(-1) + 0|)| = 2\,.$$

Problem 4. Consider the set

$$G = \{\, (a, b) \in \mathbb{R}^2 \;:\; a \neq 0 \,\}\,.$$

We define the composition

$$(a, b) \bullet (c, d) := (ac, ad + b)\,.$$

Show that this composition defines a group. Is the group commutative?

Solution 4. The composition is associative. The neutral element is $(1,0)$. The inverse element of (a,b) is $(1/a, -b/a)$. The group is not commutative since

$$(a,b) \bullet (c,d) = (ac, ad+b) \quad \text{and} \quad (c,d) \bullet (a,b) = (ca, cb+d).$$

Problem 5. Show that the set $\{+1, -1, +i, -i\}$ forms a group under multiplication. Find all subgroups.

Solution 5. The multiplication table is

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

From the table we find that the group is commutative. We can also deduce this property from the commutativity of complex multiplication. From the table we find that the inverse elements are

$$1^{-1} = 1, \quad (-1)^{-1} = -1, \quad (i)^{-1} = -i, \quad (-i)^{-1} = i.$$

The associative law follows from the associative law for multiplication of complex numbers. Thus the set $\{+1, -1, +i, -i\}$ forms a group under multiplication. We classify subgroups by their orders. There is only one subgroup of order 1, the trivial group - $\{1\}$. Subgroups of order 2 contain two elements - the identity element $e = 1$ and one additional element a. There are two possibilities: $a^2 = e$ or $a^2 = a$. The first possibility provides one subgroup: $\{1, -1\}$ which is commutative. The element (-1) is inverse to itself, it is in involution. The second possibility reduce to the trivial group $\{1\}$. There are no subgroups of order 3, because the order of a subgroup must divide the order of the group (*Lagrange's theorem*). There is only one subgroup of order 4 - this is the group itself. Therefore the group has in total $1+1+1=3$ subgroups with one proper subgroup.

Problem 6. Let $i = \sqrt{-1}$. Let S be the set of complex numbers of the form $q + pi\sqrt{5}$, where $p, q \in \mathbb{Q}$ and are not both simultaneously 0. Show that this set forms a group under multiplication of complex numbers.

Solution 6. Consider the product of two numbers $q_1 + ip_1\sqrt{5}$ and $q_2 + ip_2\sqrt{5}$.

$$q_3 + ip_3\sqrt{5} = (q_1 + ip_1\sqrt{5})(q_2 + ip_2\sqrt{5}) = q_1q_2 - 5p_1p_2 + i\sqrt{5}(q_1p_2 + p_1q_2).$$

Thus

$$q_3 = q_1q_2 - 5p_1p_2 \in \mathbb{Q}, \qquad p_3 = q_1p_2 + p_1q_2 \in \mathbb{Q}$$

and

$$q_3^2 + 5p_3^2 = (q_1^2 + 5p_1^2)(q_2^2 + 5p_2^2) > 0\,.$$

Therefore the product of two numbers of the form $q + ip\sqrt{5}$ belongs to the same set. The identity element is 1, i.e. $q = 1$ and $p = 0$. The inverse element is

$$\frac{q - ip\sqrt{5}}{q^2 + 5p^2} = \frac{q}{q^2 + 5p^2} + \left(\frac{-p}{q^2 + 5p^2}\right) i\sqrt{5}\,.$$

The existence of the inverse element follows from the fact that $p, q \in \mathbb{Q}$ and are not both simultaneously 0. Thus the inverse element belongs to the same set. The associative law follows from the same law of multiplication of complex numbers. Thus the set of numbers of the form $q + ip\sqrt{5}$, where $p, q \in \mathbb{Q}$ forms an abelian group under multiplication.

Problem 7. Let p be a prime number with $p \geq 3$. Let r and s be rational numbers ($r, s \in \mathbb{Q}$) with $r^2 + s^2 > 0$. Show that the set given by the numbers $r + s\sqrt{p}$ form a commutative group.

Solution 7. Associativity and commutativity follow from the multiplication of real numbers. We have

$$(r_1 + s_1\sqrt{p})(r_2 + s_2\sqrt{p}) = (r_1r_2 + ps_1s_2) + (r_1s_2 + r_2s_1)\sqrt{p}\,.$$

Since $r_1r_2 + ps_1s_2 \in \mathbb{Q}$ and $r_1s_2 + r_2s_1 \in \mathbb{Q}$ the operation is closed. The neutral element is 1, i.e. $r = 1$ and $s = 0$. The inverse element is

$$\frac{r - s\sqrt{p}}{(r + s\sqrt{p})(r - s\sqrt{p})} = \frac{r}{r^2 - s^2p} + \left(\frac{-p}{r^2 - s^2p}\right)\sqrt{p}\,.$$

Problem 8. Show that the set

$$\{\, e^{i\alpha} \,:\, \alpha \in \mathbb{R} \,\}$$

forms a group under multiplication. Note that $|e^{i\alpha}| = 1$.

Solution 8. We have

$$e^{i\alpha}e^{i\beta} = e^{i(\alpha+\beta)}\,.$$

The neutral element is given by $\alpha = 0$, i.e $e^0 = 1$. The inverse element of $e^{i\alpha}$ is $e^{-i\alpha}$. The associative and commutative laws follow from the same laws of multiplication for complex numbers. Thus the set $\{e^{i\alpha} : \alpha \in \mathbb{R}\}$ forms a 1-dimensional group under multiplication of complex numbers.

Problem 9. Consider the additive group $(\mathbb{Z}, +)$. Give a proper subgroup.

Solution 9. An example of a proper subgroup would be all even numbers, since the sum of two even numbers is again an even number.

Problem 10. Let $S := \mathbb{R} \setminus \{-1\}$. We define the binary operation on S

$$a \bullet b := a + b + ab\,.$$

Show that $\langle S, \bullet \rangle$ forms a group. Is the group commutative?

Solution 10. When a, b are elements of S, then $a \bullet b$ is an element of S. Suppose instead that $a + b + ab = -1$. Then $a(1+b) = -(1+b)$. Thus $b = -1$ or $a = -1$. Since $a \neq -1$ and $b \neq -1$ we have $a + b + ab \neq -1$. The neutral element is $e = 0$ since

$$a \bullet e = a + 0 + a0 = a, \qquad e \bullet b = 0 + b + 0b = b\,.$$

To find the inverse of an arbitrary element g we consider right multiplication by its inverse g^{-1}. We obtain

$$g \bullet g^{-1} = g + g^{-1} + gg^{-1} = 0 \Rightarrow g^{-1} = -g/(1+g).$$

All elements are invertible, because $g \neq -1$. The associative law holds

$$\begin{aligned}(a \bullet b) \bullet c &= (a + b + ab) \bullet c = (a + b + ab) + c + (a + b + ab)c \\ &= a + b + c + (ab + bc + ca) + abc = a \bullet (b \bullet c)\,.\end{aligned}$$

The group is commutative since $a \bullet b = b \bullet a$.

Problem 11. Let G be a group and $x, y \in G$. Show that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution 11. Let e be the neutral element of G. We have

$$xyy^{-1}x^{-1} = xex^{-1} = xx^{-1} = e$$

and

$$y^{-1}x^{-1}xy = y^{-1}ey = y^{-1}y = e\,.$$

Problem 12. Let S be the set of all rational numbers $\mathbb{Q}$ in the interval $0 \le q < 1$. Define the operation $(q, p \in S)$

$$q \bullet p := \begin{cases} q+p & \text{if } 0 \le q+p < 1 \\ q+p-1 & \text{if } \quad q+p \ge 1 \end{cases} .$$

Show that S with this operation is an abelian group.

Solution 12. The group neutral element is 0, i.e. $p+0 = 0+p = p$. The inverse element is $p^{-1} = 1-p$ since

$$p + p^{-1} = 1 \ge 1 \Rightarrow p \bullet p^{-1} = 1 - 1 = 0.$$

The inverse element exists for all p, because $p < 1$. Associativity follows from the associative law for addition of rational numbers. Commutativity follows from the commutativity of addition of rational numbers. We can write each nonzero element of the group as the proper fraction

$$p = \frac{a}{b}, \quad a, b \in \mathbb{N}, \quad a < b$$

where the fraction is irreducible (a and b have no common divisors).

Problem 13. Show that the finite set

$$\mathbb{Z}_n := \{ 0, 1, \ldots, n-1 \}$$

for $n \ge 1$ forms an abelian group under addition modulo n. The group is referred to as the group of integers modulo n.

Solution 13. The neutral element is 0. The inverse of 0 is 0. For any $j > 0$ in $\mathbb{Z}_n$ the inverse of j is $n - j$. Obviously the associative law holds. The group law is

$$a + b < n \Rightarrow a \bullet b = a + b$$

$$a + b \ge n \Rightarrow a \bullet b = a + b - n, \quad a, b \in \mathbb{Z}_n.$$

The expressions are symmetric in the two arguments a, b. Thus the group is abelian.

Problem 14. Let $n \in \mathbb{N}$. Let $U(n)$ be the set of all positive integers less than n and relatively prime to n. Then $U(n)$ is a commutative group under multiplication modulo n. Find the group table for $U(8)$.

Solution 14. Obviously 1 and $n-1$ are elements of $U(n)$, where 1 is the neutral element. For $n = 8$ we have $U(8) = \{ 1, 3, 5, 7 \}$. The group table is

mod 8	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Problem 15. Consider the subset of odd integers

$$\{1, 3, 7, 9, 11, 13, 17, 19\}.$$

Show that this set forms an abelian group under multiplication modulo 20.

Solution 15. The multiplication table modulo 20 reads

·	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

The table shows that products of each two elements of the set is again an element of the set. The identity element is 1 - implied by the same property of modulo 20 multiplication for all integer numbers (or from the multiplication table). The inverse elements are

$$1^{-1} = 1, \quad 3^{-1} = 7, \quad 7^{-1} = 3, \quad 9^{-1} = 9,$$

$$11^{-1} = 11, \quad 13^{-1} = 17, \quad 17^{-1} = 13, \quad 19^{-1} = 19.$$

The associative law for modulo 20 multiplication for all integer numbers implies the same law for the set in question.

Problem 16. Give the group table for the cyclic group $\mathbb{Z}_6$ of 6 elements.

Solution 16. The neutral element is 0. The group is commutative. The group table is

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Problem 17. Consider the finite group $\mathbb{Z}_2 \times \mathbb{Z}_3$ which has $2 \cdot 3 = 6$ elements given by $(0,0)$, $(0,1)$, $(0,2)$, $(1,0)$, $(1,1)$, $(1,2)$. The neutral element is $(0,0)$. Show that $\mathbb{Z}_2 \times \mathbb{Z}_3$ is cyclic.

Solution 17. It is only necessary to find a generator. We start with $(1,1)$. Then

$$\begin{aligned}
(1,1) &= (1,1)\\
2(1,1) &= (1,1) + (1,1) = (0,2)\\
3(1,1) &= 2(1,1) + (1,1) = (1,0)\\
4(1,1) &= 3(1,1) + (1,1) = (1,0) + (1,1) = (0,1)\\
5(1,1) &= 4(1,1) + (1,1) = (0,1) + (1,1) = (1,2)\\
6(1,1) &= 5(1,1) + (1,1) = (1,2) + (1,1) = (0,0)\,.
\end{aligned}$$

Therefore the element $(1,1)$ generates all elements of the commutative group $\mathbb{Z}_2 \times \mathbb{Z}_3$.

Problem 18. Consider the functions defined on $\mathbb{R} \setminus \{0,1\}$

$$f_1(x) = x, \quad f_2(x) = \frac{1}{x}, \quad f_3(x) = 1 - x,$$

$$f_4(x) = \frac{x}{x-1}, \quad f_5(x) = \frac{1}{1-x}, \quad f_6(x) = 1 - \frac{1}{x}\,.$$

Show that these functions form a group with the *function composition* $f_j \circ f_k$, where

$$(f_j \circ f_k)(x) := f_j(f_k(x))\,.$$

Solution 18. The neutral element is f_1. The group table is

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_5	f_6	f_3	f_4
f_3	f_3	f_6	f_1	f_5	f_4	f_2
f_4	f_4	f_5	f_6	f_1	f_2	f_3
f_5	f_5	f_4	f_2	f_3	f_6	f_1
f_6	f_6	f_3	f_4	f_2	f_1	f_5

For example

$$(f_3 \circ f_4)(x) = f_3(f_4(x)) = 1 - \frac{x}{x-1} = \frac{1}{1-x} = f_5(x)$$

$$(f_4 \circ f_3)(x) = f_4(f_3(x)) = \frac{1-x}{1-x-1} = 1 - \frac{1}{x} = f_6(x)\,.$$

Each element has an inverse. The associativity law holds for function composition. The group is not commutative.

Problem 19. An *isomorphism* of a group G with itself is an *automorphism*. Show that for each $g \in G$ the mapping $i_g : G \to G$ defined by

$$xi_g := g^{-1}xg$$

is an automorphism of G, the inner automorphism of G under conjugation by the group element g. We have to show that i_g is an isomorphism of G with itself. Thus we have to show it is one to one, onto, and that

$$(xy)i_g = (xi_g)(yi_g)$$

for all $g \in G$.

Solution 19. If $xi_g = yi_g$, then $g^{-1}xg = g^{-1}yg$. Thus $x = y$. For onto, if $x \in G$, then applying the associative law yields

$$(gxg^{-1})i_g = g^{-1}(gxg^{-1})g = x\,.$$

Now $(xy)i_g = g^{-1}xyg$ and

$$(xi_g)(yi_g) = (g^{-1}xg)(g^{-1}yg) = g^{-1}xyg$$

since $gg^{-1} = e$. Thus $(xy)i_g = (xi_g)(yi_g)$.

Problem 20. Let C_n be the *cyclic group*. Show that $C_6 \simeq C_3 \times C_2$.