GROUPS AND APPLICATIONS

Tadao ODA
Tohoku University, Japan

Keywords: group, homomorphism, quotient group, group action, transformation, symmetry, representation

Contents

1. Groups
2. Commutative Groups
3. Examples
4. Subgroups
5. Homomorphisms
6. Quotient Groups
7. Homomorphism and Isomorphism Theorems
8. Cyclic Groups
9. Direct Products
10. Finitely Generated Abelian Groups
11. Group Actions and Symmetry
12. Solvable Groups
13. Representations of Finite Groups
Glossary
Bibliography
Biographical Sketch

Summary

Groups are sets with one algebraic operation. Their basic properties are explained with many typical examples.

The notion of groups with simple but very abstract form historically grew out of more concrete "transformations" and turns out to be extremely powerful thanks to the very abstractness.

Results on matrices and linear algebra in *Matrices, Vectors, Determinants and Linear Algebra* will be freely used.

1. Groups

A *group* is a set G endowed with a map $G \times G \ni (x, y) \mapsto xy \in G$ called the group operation (alternatively, group law, or multiplication) satisfying the following conditions:

(Associativity) $(xy)z = x(yz)$ holds for all $x, y, z \in G$.

(Existence of the unity) There exists $e \in G$, called the unity, such that $xe = ex = x$ holds

for any $x \in G$.

(Existence of the inverse) For any $x \in G$ there exists $x^{-1} \in G$, called the inverse of x, such that $xx^{-1} = x^{-1}x = e$.

When G is a finite set with g elements, G is called a *finite group* of *order* g. The notation $g =: |G|$ is often used. Otherwise, G is called an infinite group.

2. Commutative Groups

A group G is said to be *commutative* (alternatively, *Abelian*) if the following condition is satisfied:

(Commutativity) $xy = yx$ holds for all $x, y \in G$.

The group operation for a commutative group G is often denoted as an *addition* $G \times G \ni (x, y) \mapsto x + y \in G$ so that the conditions are of the following form:

(Associativity) $(x + y) + z = x + (y + z)$ holds for all $x, y, z \in G$.

(Existence of the zero) There exists $0 \in G$, called the zero, such that $x + 0 = 0 + x = x$ holds for any $x \in G$.

(Existence of the minus) For any $x \in G$ there exists $-x \in G$, called the minus of x, such that $x + (-x) = (-x) + x = 0$.

(Commutativity) $x + y = y + x$ holds for all $x, y \in G$.

3. Examples

- The set $\mathbb{Z} = \{.., -2, -1, 0, 1, 2, ..\}$ of integers under the usual addition is an infinite commutative group.
- The subset $\{1, -1\}$ of $\mathbb{Z}$ under the usual multiplication is a commutative group of order 2.
- The subset $\{1, -1, i, -i\} \subset \mathbb{C}$ of complex numbers under the usual multiplication is a commutative group of order 4.
- The subset $\{1, -1, i, -i, j, -j, k, -k\} \subset \mathbb{H}$ of Hamilton's quaternions under the usual multiplication is a non-commutative group of order 8, and is called the *quaternion group*.
- The sets $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ of rational numbers, real numbers, complex numbers and Hamilton's quaternions, respectively, are commutative groups under the usual addition.
- The set $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$ of nonzero rational numbers is a group under the usual multiplication. Similarly, $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$, $\mathbb{H}^* := \mathbb{H} \setminus \{0\}$ are groups under the usual multiplication.

- Let X be a set. Then the set $\mathrm{Aut}(X)$ of one-to-one and onto maps $f : X \xrightarrow{\sim} X$ of X to itself is a group under the composition $f' \circ f$ of $f, f' \in \mathrm{Aut}(X)$. The identity map $\mathrm{id} : X \xrightarrow{\sim} X$ is the unity, while the inverse map f^{-1} is the inverse of $f \in \mathrm{Aut}(X)$.
- In the previous example, let $X := \{1, 2, 3, \ldots, n\}$. Then $S_n := \mathrm{Aut}(\{1, 2, \ldots, n\})$ is usually called the *symmetric group* of degree n. It has order $|S_n| = n!$, and consists of the *permutations* of $\{1, 2, \ldots, n\}$.
- The set $GL_n(\mathbb{R})$ of real square invertible matrices of size n is a group under the matrix multiplication, and is called the *general linear group*. The identity matrix $\mathbf{I}_n$ is the unity, while the inverse matrix A^{-1} is the inverse of $A \in GL_n(\mathbb{R})$. Similarly, $GL_n(\mathbb{Q})$ (resp. $GL_n(\mathbf{C})$) is the group of rational (resp. complex) square invertible matrices of size n.
  Note that *no* quaternionic analog of these groups exists.
  Note further that if $X := \mathbb{R}^n$, for instance, in the example above, then $GL_n(\mathbb{R})$ is a subset of $\mathrm{Aut}(\mathbb{R}^n)$ consisting of those one-to-one and onto maps $\mathbb{R}^n \xrightarrow{\sim} \mathbb{R}^n$ which are *linear*, that is, which "preserve" the vector space structure of $\mathbb{R}^n$ consisting of the real column vectors of size n.

4. Subgroups

A *nonempty* subset $H \subset G$ of a group G is called a *subgroup* of G if $xy^{-1} \in H$ holds for all $x, y \in H$. It is easily seen that H itself is a group under the operation induced by that of G, since it contains the unity $e \in G$, is closed under the group operation of G and $y^{-1} \in H$ holds for all $y \in H$. (Here is how to show these facts: There exists at least one $x_0 \in H$ since H is assumed to be nonempty. Hence $e = x_0 x_0^{-1}$ is in H. Moreover, $y^{-1} = ey^{-1} \in H$ for any $y \in H$ by definition. Consequently, $xy = x(y^{-1})^{-1} \in H$ holds for all $x, y \in H$.)

Sometimes, the notation $H < G$ is used to mean that H is a subgroup of G.

The intersection $H \cap H'$ of subgroups $H < G$ and $H' < G$ is a subgroup of G. One obviously has $H \cap H' < H$ as well as $H \cap H' < H'$.

A subgroup N of G is said to be *normal* if $xyx^{-1} \in N$ holds for all $y \in N$ and all $x \in G$. It is convenient to describe this fact as $xNx^{-1} = N$ for any $x \in G$, where $xNx^{-1} := \{xyx^{-1} \,|\, y \in N\}$.

It is convenient to denote $N \lhd G$ to say that N is a normal subgroup of G.

One obviously has $N \cap N' \lhd G$ for $N \lhd G$ and $N' \lhd G$. Obviously, $N \cap N' \lhd N$ and $N \cap N' \lhd N'$ hold. Moreover, $N \cap H \lhd H$ for any subgroup $H < G$. However, a

normal subgroup M of a normal subgroup $N \lhd G$ need not be a normal subgroup of G. Namely, $M \lhd N \lhd G$ does *not* imply $M \lhd G$.

Note that subgroups of a commutative group are automatically normal. Note also that $\{e\}$ and G itself are normal subgroups of any group G.

Here are examples of subgroups and normal subgroups:

- Any of the additive groups in the sequence $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$ is a subgroup of those to the right.
- Any of the multiplicative groups in the sequence $\mathbb{Q}^* \subset \mathbb{R}^* \subset \mathbb{C}^* \subset \mathbb{H}^*$ is a subgroup of those to the right.
- The multiplicative group $\{1,-1\}$ is a subgroup of the multiplicative group $\mathbb{Q}^*$.
- The multiplicative group $\{1,-1,i,-i\}$ is a subgroup of the multiplicative group $\mathbb{C}^*$, and contains the multiplicative group $\{1,-1\}$ above as a subgroup.
- The quaternion group $\{1,-1,i,-i,j,-j,k,-k\}$ is a subgroup of the multiplicative group $\mathbb{H}^*$, and contains the multiplicative group $\{1,-1,i,-i\}$ above as a subgroup.
- Subgroups of S_n's are called permutation groups.
- The set $SL_n(\mathbb{R})$ of real square matrices $\mathbf{A}$ of size n with $\det(\mathbf{A}) = 1$ is a normal subgroup of $GL_n(\mathbb{R})$, called the real *special linear group*. The normality is an easy consequence of $\det(\mathbf{PAP}^{-1}) = \det(\mathbf{P})\det(\mathbf{A})\det(\mathbf{P})^{-1} = \det(\mathbf{A})$. The normal subgroups $SL_n(\mathbb{Q}) \lhd GL_n(\mathbb{Q})$ and $SL_n(\mathbb{C}) \lhd GL_n(\mathbb{C})$ are defined similarly.
- The set $\mathbb{R}_{>0}$ of positive real numbers is a subgroup of the multiplicative group $\mathbb{R}^*$ of nonzero real numbers.
- The *orthogonal group* $O(n)$ is the subgroup of $GL_n(\mathbb{R})$ consisting of orthogonal matrices.
- The *unitary group* $U(n)$ is the subgroup of $GL_n(\mathbb{C})$ consisting of unitary matrices. One has $O(n) = U(n) \cap GL_n(\mathbb{R})$.
- A subgroup of the additive group $\mathbb{Z}$ can be shown to be either $\{0\}$ or, for each positive integer n, the subset
  $n\mathbb{Z} := \{an \,|\, a \in \mathbb{Z}\} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$ of the multiples of n.

5. Homomorphisms

A *homomorphism* from a group G to another group G' is a map $f : G \to G'$ such that $f(xy) = f(x)f(y)$ for all $x, y \in G$. It is easily seen that $f(e)$ coincides with the unity $e' \in G'$, and $f(x^{-1}) = f(x)^{-1}$ for any $x \in G$.

A one-to-one homomorphism is also called an *injective* homomorphism or an injection, while an onto homomorphism is called a *surjective* homomorphism or a surjection. An *isomorphism* is a homomorphism that is both one-to-one and onto.

A homomorphism of a group G to itself is called an *endomorphism* of G. An isomorphism of a group G to itself is called an *automorphism* of G.

The *image* $f(G) := \{f(x) \mid x \in G\}$ of a homomorphism $f : G \to G'$ is easily seen to be a subgroup of G'. More importantly, the *kernel* $\ker(f) := \{x \in G \mid f(x) = e'\}$ is a normal subgroup of G, since $f(yxy^{-1}) = f(y)f(x)f(y)^{-1} = f(y)ef(y)^{-1} = e$ holds for any $x \in \ker(f)$ and any $y \in G$.

Here are examples:

- $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ sending $\mathbf{A}$ to its determinant $\det(\mathbf{A})$ is a (surjective) homomorphism. By definition, $\ker(\det) = SL_n(\mathbb{R})$. Likewise, surjective homomorphisms $\det : GL_n(\mathbb{Q}) \to \mathbb{Q}^*$ and $\det : GL_n(\mathbb{C}) \to \mathbb{C}^*$ have respective kernel $SL_n(\mathbb{Q})$ and $SL_n(\mathbb{C})$.
- The *signature* homomorphism $\operatorname{sgn} : S_n \to \{1, -1\}$ from the symmetric group S_n to the multiplicative group $\{1, -1\}$ is defined as follows: Consider the polynomial called the *difference product* in n variables $x_1, x_2, \ldots, x_n$ defined by

$$\Delta(x_1, x_2, \ldots, x_n) := \prod_{1 \le i < j \le n} (x_i - x_j).$$

For each permutation $\sigma \in S_n$, the variables are permuted by σ and

$$\Delta(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(i)}, \ldots, x_{\sigma(n)}) = \operatorname{sgn}(\sigma)\Delta(x_1, x_2, \ldots, x_i, \ldots, x_n)$$

with $\operatorname{sgn}(\sigma) = \pm 1$. The kernel $A_n := \ker(\operatorname{sgn})$ is called the *alternating group* of degree n.

- The map $|\ |: \mathbb{C}^* \to \mathbb{R}_{>0}$ sending $z \in \mathbb{C}^*$ to its absolute value $|z|$ is a homomorphism. Its kernel is the set

$$U(1) := \{\exp(i\theta) = \cos\theta + i\sin\theta \mid \theta \in \mathbb{R}\}$$

of complex numbers with absolute value 1.

- The kernel $SO(n)$ of $\det : O(n) \to \{\pm 1\}$ is called the *group of rotations*. Obviously, $SO(n) = O(n) \cap SL_n(\mathbb{R})$.
- The kernel $SU(n)$ of $\det : U(n) \to U(1)$ is called the *special unitary group*. Obviously, $SU(n) = U(n) \cap SL_n(\mathbb{C})$ as well as $SO(n) = SU(n) \cap GL_n(\mathbb{R})$.
- For any element a of a group G, a map $I_a : G \to G$ is defined to be the one sending $x \in G$ to $I_a(x) := axa^{-1}$. It is an automorphism of G since $I_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = I_a(x)I_a(y)$ with $I_{a^{-1}}$ as the inverse map. I_a is called an *inner*

automorphism of G. Note that $I_{ab} = I_a \circ I_b$, since $I_{ab}(x) = (ab)x(ab)^{-1} = a(bxb^{-1})a^{-1} = I_a(I_b(x)) = (I_a \circ I_b)(x)$.

6. Quotient Groups

For a subgroup H of a group G and $x \in G$, the subset $xH := \{xy \,|\, y \in H\}$ of G is called the *left coset* of $x \in G$ with respect to H. One calls x a *representative* of the coset xH. Note that elements of the form xy_0 for $y_0 \in H$ are representatives of the coset xH as well. Likewise, $Hx := \{yx \,|\, y \in H\}$ is called the *right coset* of $x \in G$ with respect to H, while x is called a representative of the coset. Elements of the form $y_0 x$ are representatives of Hx as well. (In the case of additive groups, the notation $x + H := \{x + y \,|\, y \in H\}$ is used.)

The set G/H of all the left cosets xH in G with respect to H is called the *left coset space* of G with respect to a subgroup H. Likewise, the set $H \backslash G$ is the set of all the right cosets Hx in G with respect to H and is called the *right coset space* of G with respect to a subgroup H. The left coset space and the right coset space are also called *homogeneous spaces* of G with respect to a subgroup H.

$[G : H]$ is defined to be the number of cosets in G with respect to H, and is called the *index* of H in G. It does not matter whether the left cosets or the right cosets are counted. Indeed, the one-to-one and onto set map $G \xrightarrow{\sim} G$ sending $x \in G$ to $x^{-1} \in G$ maps each left coset xH to the right coset Hx^{-1} inducing a one-to-one and onto set map $G/H \xrightarrow{\sim} H \backslash G$.

When G is a finite group, the formula

$$|G| = [G : H]\,|H|$$

due to *Lagrange* turns out to be very useful, where $|G|$ and $|H|$ are the orders of the groups G and H, respectively.

Of special interest are the coset spaces with respect to normal subgroups. For a normal subgroup $N \lhd G$ of a group G, the left coset and the right coset of any $x \in G$ coincide so that $xN = Nx$ by the definition of normality. Moreover, the coset space G/N turns out to be a group, called the *quotient group* with respect to N under the following group law: The product of cosets xN and $x'N$ is defined to be

$$(xN)(x'N) := xx'N,$$

which is well-defined independently of the choice of representatives. Indeed, let xy and $x'y'$ with $y, y' \in N$ be other representatives. Then

$(xy)(x'y')N = xx'((x')^{-1}yx')y'N = xx'N$, since $(x')^{-1}yx' \in N$ by normality. The coset $eN = N$ is the unity of G/N, while $x^{-1}N$ is easily seen to be the inverse of xN.

The map $\pi : G \to G/N$ sending $x \in G$ to $\pi(x) := xN$ is called the *projection*, and is easily seen to be an onto homomorphism with kernel $\ker(\pi) = N$.

The quotient groups produce interesting new groups.

7. Homomorphism and Isomorphism Theorems

A homomorphism of groups $f : G \to G'$ induces an isomorphism

$$\overline{f} : G/\ker(f) \xrightarrow{\sim} f(G),$$

which is known as the *homomorphism theorem*.

For normal subgroups N and N' of a group G with $N \subset N'$, one has a natural surjective homomorphism $f : G/N \to G/N'$ sending xN to xN'. Its kernel is $\ker(f) = N'/N$, so that by the above theorem the so-called *first isomorphism theorem*

$$(G/N)/(N'/N) \xrightarrow{\sim} G/N'$$

holds. Any subgroup of G/N is of the form H/N for a subgroup H of G containing N. Moreover, H/N is normal in G/N if and only if H is normal in G.

In general, let H be a subgroup of a group G and N a normal subgroup of G. Then the set $HN := \{hn \,|\, h \in H, n \in N\}$ is easily seen to be a subgroup of G containing N as a normal subgroup. (In the case of additive groups, the notation $H + N := \{h + n \,|\, h \in H, n \in N\}$ is used.)

The projection $\pi : G \to G/N$ induces a homomorphism $\pi_{|H} : H \to G/N$ by restriction. Its kernel is $\ker(\pi_{|H}) = H \cap N$, while its image is the quotient group HN/N. Thus the so-called *second isomorphism theorem*

$$H/(H \cap N) \xrightarrow{\sim} HN/N$$

holds. These simple innocuous looking theorems turn out to be extremely useful as shown later.

- The map $f : \mathbb{R} \to U(1)$ sending $\theta \in \mathbb{R}$ to $f(\theta) := \exp(2\pi i\theta) \in U(1)$ is a surjective homomorphism with kernel $\ker(f) = \mathbb{Z}$. Thus an isomorphism

$$\mathbb{R}/\mathbb{Z} \xrightarrow{\sim} U(1).$$

- It was seen earlier that the subgroups of the additive group $\mathbb{Z}$ are $\{0\}$ and $n\mathbb{Z}$ for positive integers n. For positive integers n and m, one has $n\mathbb{Z} \subset m\mathbb{Z}$ if and only if m divides n. Denote by $\gcd(m,n)$ and $\operatorname{lcm}(m,n)$ the greatest common divisor and the least common multiple of m and n, respectively. Then

$$m\mathbb{Z} \cap n\mathbb{Z} = \operatorname{lcm}(m,n)\mathbb{Z} \qquad \text{and} \qquad m\mathbb{Z} + n\mathbb{Z} = \gcd(m,n)\mathbb{Z}.$$

The well-known formula

$$\operatorname{lcm}(m,n)\gcd(m,n) = mn$$

is the second isomorphism theorem in disguise.

- The subgroups of $\mathbb{Z}/n\mathbb{Z}$ for a positive integer n are $m\mathbb{Z}/n\mathbb{Z}$ for the divisors m of n.

8. Cyclic Groups

Let x be an element of a group G. Then a homomorphism $f_x : \mathbb{Z} \to G$ is defined to be the map sending $m \in \mathbb{Z}$ to

$$f_x(m) := x^m := \begin{cases} xx\cdots x \quad (m \text{ times}) & \text{if } m > 0 \\ e & \text{if } m = 0. \\ x^{-1}x^{-1}\cdots x^{-1} \quad (-m \text{ times}) & \text{if } m < 0 \end{cases}$$

Its kernel could be either $\{0\}$ or $n\mathbb{Z}$ for a positive integer n as was seen before. Its image is denoted by $f_x(\mathbb{Z}) =: \langle x \rangle$ and is called the subgroup of G *generated by* x.

$x \in G$ is said to be of *infinite order* if $\ker(f_x) = \{0\}$. In this case, the image $\langle x \rangle$ of f_x consists of *mutually distinct* x^m 's for all $m \in \mathbb{Z}$ and one has an isomorphism

$$\mathbb{Z} \xrightarrow{\sim} \langle x \rangle = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}.$$

Any of these isomorphic groups is called an *infinite cyclic group*.

- $x \in G$ is said to be of *order* n if $\ker(f_x) = n\mathbb{Z}$ for a positive integer n. In this case, the image consists of n *distinct* elements and one has an isomorphism

$$\mathbb{Z}/n\mathbb{Z} \xrightarrow{\sim} \langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}.$$

-

-

-

Bibliography

Artin, M. (1991). Algebra, xviii+618 pp. Prentice Hall, Inc., Englewood Cliffs, NJ, ISBN 0-13-004763-5 [This is one of the advanced comprehensive textbooks on algebra suitable for further study.]

Birkhoff, G. and Mac Lane, S. (1965). A Survey of Modern Algebra, Third Edition, x+437 pp. The Macmillan Co., New York; Collier-Macmillan Ltd., London [A standard textbook on algebra.]

Birkhoff, G. and Mac Lane, S. (1988). Algebra, Third Edition, xx+626 pp., Chelsea Publishing Company, New York, ISBN 0-8284-0330-9[A classic comprehensive textbook on algebra. Originally published from Macmillan, Inc.]

Lang, S. (2002). Algebra, Revised Third Edition, xvi+914 pp.,Graduate Texts in Mathematics 211, Springer-Verlag, New York, ISBN 0-387-95385-X[An advanced comprehensive textbook on algebra

suitable for graduate students. Originally published from Addison-Wesley Publishing Company.]

Ronan, M. (2006). Symmetry and the Monster. One of the Greatest Quests of Mathematics, vi+251 pp. Oxford University Press, Oxford, ISBN 978-0-19-280722-9; 0-19-280722-6 [A book intended primarily for a non-mathematical audience, explains the history of groups since the ancient Greek period till the recent classification of finite simple groups.]

Biographical Sketch

Tadao ODA, born 1940 in Kyoto, Japan

Education: BS in Mathematics, Kyoto University, Japan (March, 1962). MS in Mathematics, Kyoto University, Japan (March, 1964). Ph.D. in Mathematics, Harvard University, U.S.A. (June, 1967).

Positions held: Assistant, Department of Mathematics, Nagoya University, Japan (April, 1964-July, 1968) Instructor, Department of Mathematics, Princeton University, U.S.A. (September, 1967-June, 1968) Assistant Professor, Department of Mathematics, Nagoya University, Japan (July, 1968-September, 1975) Professor, Mathematical Institute, Tohoku University, Japan (October, 1975-March, 2003) Professor Emeritus, Tohoku University (April, 2003 to date)