Algebra

(代数学)

Wu Zhixiang

SCIENCE PRESS
Beijing

A [redacted]

(代数学)

Wu Zhixiang

SCIENCE PRESS
Beijing

Responsible Editor: Li Xin

Published by Science Press
16 Donghuangchenggen North Street
Beijing 100717, P. R. China

Printed in Beijing

ISBN 978-7-03-040877-8

Preface

I have taught algebra for undergraduates or graduates at Zhejiang University for several years. During this period, I have used several different textbooks for my teaching. However, I found that there was no suitable textbook for my teaching. This is exactly the motivation to write this book. This book is intended to provide a reasonably self-contained theory of basic algebra suitable for an introductory course. The text consists of five chapters which are designed for a one-semester course taken by the students who have learned linear algebra. All contents in this book are standard and essential as an introductory course in algebra. There is a fairly large number of examples to help the readers understand the contents of this book. Hopefully, these examples will make the theory more alive, more meaningful, more visual, and easier to be grasped. Moreover, there is a series of exercises at the end of each section. Some of the exercises test the understanding of the text in the usual way, while some are arranged as a supplement and extension of the contents in this book. The reader is involved in providing proofs and working on problems that have not been completely solved in the text; and furthermore, they are asked to extend some of the theories which are essential for further study.

I have striven to craft the text that presents some concepts at the center of algebras in a coherent, tightly knitted way. I believe that there are enough challenging problems. Needless to say, several aspects of this book are experimental, I would be very grateful for critical comments and suggestions from the people who used it.

Acknowledgments This book is partly supported by the national natural science foundation of China(No.11171296), ZJNSF (No. LZ 14A010001), Department of Mathematics, and Graduated school of Zhejiang University. The author would like to thank Department of Mathematics, and Graduated School of Zhejiang University for their constant support and help. He is deeply indebted to many of his students and colleagues for their ideas and encouragements during the preparation of this book. Finally, the author apologize to many authors whose works we have used but not specifically cited. Virtually all of the results can be found either in books or articles which are listed in our bibliography.

Notations We fix some notations which are used throughout the book. $\mathbb{Q}, \mathbb{R}$, $\mathbb{C}, \mathbb{P}$ are the rational number field, the real number field, the complex number field, and a number field respectively. $\mathbb{H}$ is the quaternion division. $\mathbb{Z}_+$, $\mathbb{N}$, $\mathbb{Z}$ are the set of all positive integers, nonnegative integers, and integers respectively. $M_n(A)$

is the set of all $n \times n$ matrices with entries in A. Suppose A contains the elements 1 and 0. Then E or E_n is the diagonal matrix $\mathrm{diag}(1, \cdots, 1) \in M_n(A)$, which is an identity matrix of $M_n(A)$. δ_{ij} is the Kronecker symbol, that is, $\delta_{ii} = 1$, and $\delta_{ij} = 0$ for any $i \neq j$. For any set X, $|X|$ is the cardinal of X and $\mathrm{id}_X : X \to X$, $x \mapsto x$ is the identity mapping. Suppose $f : A \to B$ is a mapping, and $C \subset A$. Then $f|_C : C \to B$, $x \mapsto f(x)$ is denoted as a restricted mapping of f, and we also say f is an extension mapping of $f|_C$. A commutative diagram is a diagram of sets (also known as vertices) and mappings (also known as arrows or edges) such that all directed paths in the diagram with the same start and endpoints lead to the same result by the composition of mappings. For example, the diagram

$$\begin{array}{ccccc} A_1 & \xrightarrow{f_1} & B_1 & \xrightarrow{g_1} & C_1 \\ {\scriptstyle\varphi_1}\downarrow & & {\scriptstyle\varphi_2}\downarrow & & {\scriptstyle\varphi_3}\downarrow \\ A_2 & \xrightarrow{f_2} & B_2 & \xrightarrow{g_2} & C_2 \end{array}$$

is commutative if $\varphi_2 f_1 = \varphi_1 f_2$, $\varphi_3 g_1 = g_2 \varphi_2$. It is not commutative if one of these two equations fails.

Wu Zhixiang
Feb., 2014

Contents

Chapter 1
Groups

The concept of a group is of fundamental importance in algebra and other subjects. We say two groups are the same if they are isomorphic. Just as classifications of finite-dimensional vector spaces over a number field, one of the fundamental question in group theory is to classify all groups up to isomorphism of groups, which means to find a necessary and sufficient condition for two groups to be isomorphic. This is a very complicated question. However, a larger amount of miscellaneous information on structure of a group has been explored in this chapter.

1.1 Semigroups, monoids and groups

Let's first recall some known binary operations. For example, for any two $n \times n$ matrices A, B over the complex number field $\mathbb{C}$, we can define binary operations of A and B, such as $A + B, A - B$ and AB. For any two mappings $f : X \to Y$ and $g : Y \to Z$, where X, Y and Z are nonempty sets, we can define the composition of f and g by $g \circ f : X \to Z$, $x \mapsto g(f(x))$. A binary operation on a nonempty set S is a mapping from $S \times S$ to S, where $S \times S := \{(a, b)|a, b \in S\}$ is the Cartersian product of S. Under this map, there is only one element in S corresponding to each $(a, b) \in S \times S$. The unique element is usually denoted by $a \cdot b$, simply denoted by ab sometimes.

Definition 1.1.1 *A binary operation on a set G is to be* **associative** *if $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for any $a, b, c \in G$. A* **semigroup** *is a nonempty set G together with an associative binary operation $\cdot$ on G. The binary operation of a semigroup G is usually called the product, or multiplication of G.*

Example 1.1.1 Let $\mathbb{N}$ be the set of all natural numbers. Then $(\mathbb{N}, +)$ with addition of numbers and $(\mathbb{N}, \times)$ with multiplication of numbers are semigroups.

It is well known that $h \cdot (g \cdot f) = (h \cdot g) \cdot f$ for any mappings $X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} W$. For any nonempty set X, $X^X := \{f|f$ is a mapping from X to $X\}$ is a semigroup with composition of mappings.

Let $M_n(\mathbb{P})$ be the set of all $n \times n$ matrices over a number field $\mathbb{P}$. Then $(M_n(\mathbb{P}), +)$ with usual matrix addition and $(M_n(\mathbb{P}), \cdot)$ with usual matrix multiplication are semigroups. $(M_n(\mathbb{P}), -)$ with usual matrix subtraction is not a semigroup.

Let $\mathbb{H} := \left\{ \begin{pmatrix} a+b\sqrt{-1} & c+d\sqrt{-1} \\ -c+d\sqrt{-1} & a-b\sqrt{-1} \end{pmatrix} | a,d,c,d \in \mathbb{R} \right\}$. Then $\mathbb{H}$ is a semigroup with matrix addition. It is also a semigroup with matrix multiplication. $\mathbb{H}$ is called a **quaternion division**.

Suppose Ω is an open subset of $\mathbb{R}^2$ and $x_0 \in \Omega$ is a fixed point. A **loop** with a fixed point x_0 in Ω is a continuous mapping $\varphi : [0,1] \to \Omega$ such that $\varphi(0) = \varphi(1) = x_0$. Let L be the set of all loops with a fixed point x_0 in Ω. Define $\phi_1 \cdot \phi_2(t) = \phi_1(2t)$ if $0 \leqslant t \leqslant \frac{1}{2}$, $\phi_1 \cdot \phi_2(t) = \phi_2(2t-1)$ if $\frac{1}{2} \leqslant t \leqslant 1$. It is easy to check that L is not a semigroup with this binary operation $\cdot$.

Example 1.1.2 Given any nonempty set A. Let $S(A)$ be the set of all finite sequences (or strings) of elements from A. Then elements in $S(A)$ are also called **words** over A, or words with alphabets in A. Then $S(A)$ becomes a semigroup with the string concatenation.

Definition 1.1.2 *An element e of a semigroup S is called an* **identity** *of S provided that $ea = ae = a$ for all $a \in S$. A* **monoid** *is a semigroup with an identity.*

Suppose e_1, e_2 are identities of a monoid M. Since e_2 is an identity, $e_1 = e_1 e_2$. Similarly, $e_2 = e_1 e_2$. Hence $e_1 = e_2$. Thus a monoid has a unique identity. We denote the unique identity of a monoid by e in this chapter unless otherwise specified. If there are several monoids, we usually use e_M to emphasis that it is the identity of M.

Example 1.1.3 $(\mathbb{N}, +)$ is a monoid with identity 0 and $(\mathbb{N}, \cdot)$ is a monoid with identity 1. The set $2\mathbb{Z}$ of all even numbers is not a monoid with the multiplication of numbers. It is only a semigroup.

Example 1.1.4 Let S be a semigroup and choose an element $e \notin S$. Define a binary operation on $S^+ := S \cup \{e\}$ as follows. If $a, b \in S$, then ab is the product of a and b in S. Otherwise $ae = ea = a$ for any $a \in S^+$. It is easy to check that S^+ is a monoid with the identity e. In particular, for any given nonempty set A, $M(A) := S(A)^+$ is a monoid, where $S(A)$ is the semigroup defined in Example 1.1.2. The identity of $M(A)$ is also called an **empty word**.

Definition 1.1.3 *Let M be a monoid with identity e. An element $a \in M$ is* **invertible** *in M if there is an element $b \in M$ such that $ab = ba = e$. A* **group** *is a monoid such that every element is invertible.*

We know that an invertible matrix has only one inverse matrix. Similarly, every invertible element in a monoid has only one element b satisfying $ab = ba = e$. In fact, if there are two elements b, c such that $ab = ba = ac = ca = e$, then $b = eb = (ca)b = c(ab) = ce = c$. This unique element b is called the **inverse** of a, denoted

by a^{-1}. For any invertible element a, its inverse a^{-1} is invertible and $(a^{-1})^{-1} = a$ by Definition 1.1.3.

Let a be an element in a semigroup G. Define $a^1 := a$, $a^2 := aa$, and $a^n := a^{n-1}a$ for $n > 1$. Further, define $a_1a_2\cdots a_n := (a_1\cdots a_{n-1})a_n$ inductively for $a_1, \cdots, a_n \in G$. Let $a^0 := e$ if a is in a monoid G. For any invertible a, define $a^{-n} := (a^{-1})^n$ for any $n \geqslant 1$.

Example 1.1.5 $(M_n(\mathbb{P}), \cdot)$ with matrix product is a monoid and it is not a group. Its identity is the identity matrix E_n. $(M_n(\mathbb{P}), +)$ with the matrix addition is a group, whose identity is the zero matrix 0.

Let $\alpha = \begin{pmatrix} a+b\sqrt{-1} & c+d\sqrt{-1} \\ -c+d\sqrt{-1} & a-b\sqrt{-1} \end{pmatrix} \in \mathbb{H}$. Define $\bar{\alpha} := \begin{pmatrix} a-b\sqrt{-1} & -c-d\sqrt{-1} \\ c-d\sqrt{-1} & a+b\sqrt{-1} \end{pmatrix}$, and $||\alpha|| := \sqrt{a^2+b^2+c^2+d^2}$. Then $||\alpha||$ is called the **norm** of α. Assume that $\alpha \neq 0$. Let $\beta = \dfrac{1}{||\alpha||^2}\bar{\alpha}$. Then $\alpha\beta = \beta\alpha = E_2$ (2×2 identity matrix). Thus every nonzero element in $\mathbb{H}$ is an invertible matrix.

Suppose G is a group with product $\cdot$. Then the set G is also a group with a new product $\circ$, where $a \circ b = b \cdot a$ for any $a, b \in G$. The group G with the product $\circ$ is denoted by G^{op}, which is called the **opposite group** of the group G with product "$\cdot$".

Proposition 1.1.1 *Let M be a monoid, and $a, b \in M$. (i) Suppose a and b are invertible. Then $(ab)^{-1} = b^{-1}a^{-1}$ and $a^{-n} = (a^n)^{-1}$ for any integer $n \geqslant 1$. (ii) Let $G = \{a \in M | a$ is invertible$\}$. Then G is a group.*

Proof (i) $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = e$. Similarly, $(b^{-1}a^{-1})(ab) = e$. Hence $(ab)^{-1} = b^{-1}a^{-1}$. Let n be a nonnegative integer, and $aa^n = a^na$ for $a \in M$. Then $aa^{n+1} = a(a^na) = (aa^n)a = (a^na)a = a^{n+1}a$. Thus $aa^n = a^na$ for any nonnegative integer n by induction on n. Suppose $a^{-n} = (a^n)^{-1}$. Then $a^{-(n+1)} = (a^{-1})^{n+1} = (a^{-1})^na^{-1} = (a^n)^{-1}a^{-1} = (aa^n)^{-1} = (a^na)^{-1} = (a^{n+1})^{-1}$. So $a^{-n} = (a^n)^{-1}$ for any positive integer n by induction.

(ii) Since $e \in G$, $G \neq \varnothing$. $\forall a, b \in G$, we have $ab \in G$ by (i), which means that the product of M is a binary operation of G. It is obvious that this binary operation is associative. Since every element of G is invertible, G is a group by Definition 1.1.3. □

Example 1.1.6 For any nonempty set X, $\mathrm{Sym}(X) := \{f \in X^X | f$ is invertible, equivalently, f is bijective$\}$ is a group by Proposition 1.1.1. This group is called the **symmetric group** of X. In particular, if $X = \{1, 2, \cdots, n\}$, then $\mathrm{Sym}(X)$ is denoted by S_n. For any $\sigma \in S_n$, σ can be denoted by $\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$, where the second line is the image of $1, 2, \cdots, n$, under σ, i.e., $i_j = \sigma(j)$ for $j = 1, 2, \cdots, n$.

Since σ is a bijective mapping, $i_1, i_2, \cdots, i_n$ is a permutation of $1, 2, \cdots, n$. Note that different permutations of $1, 2, \cdots, n$ in the second line of σ determine different mappings in S_n, and any permutation of $1, 2, \cdots, n$ in the second line of σ determines an element in S_n. The cardinal $|S_n|$ of S_n is $n!$.

Let $GL(n, \mathbb{P}) := \{A \in M_n(\mathbb{P}) | A \text{ is invertible}\}$ is a group with multiplication of matrices. $GL(n, \mathbb{P})$ is called a **general linear group** over $\mathbb{P}$. In particular, $GL(1, \mathbb{P}) = \mathbb{P}^* := \mathbb{P} \setminus \{0\}$ with multiplication of numbers is a group. Let $\mathbb{H}^* := \mathbb{H} \setminus \{0\}$. Then $\mathbb{H}^*$ with multiplication of matrices is a group.

Definition 1.1.4 *A semigroup S is said to be* **commutative** *if its binary operation is commutative, i.e., $ab = ba$ for all $a, b \in S$. A commutative monoid is a commutative semigroup with identity. An* **abelian** *group is a group with a commutative binary operation. A group G is* **finite (infinite)** *if the cardinal $|G|$ of G, is finite (infinite). $|G|$ is also called the* **order** *of G.*

The symmetric group S_n is a noncommutative finite group if $n \geqslant 3$. The general linear group $GL(n, \mathbb{P})$ over a number field $\mathbb{P}$ is a noncommutative infinite group if $n \geqslant 2$. $(M_n(\mathbb{P}, n), +)$ is a commutative infinite group.

Example 1.1.7 For any fixed integer $n \geqslant 1$, $G_n := \left\{ \exp\left(\frac{2k\pi\sqrt{-1}}{n}\right) | k \in \mathbb{Z} \right\}$ is a finite abelain group with product of numbers. The order $|G_n|$ of G_n is equal to n.

If G is an abelian group, then the product of G is usually denoted by "$+$", i.e., $ab := a + b$. If the binary operation of an abelian group G is denoted by "$+$", then the identity of G is denoted by 0, a^{-1} by $-a$, and a^n by na for any integer n. In particular, $0a = 0$. Further define the subtraction in G via $a - b := a + (-b)$ for $a, b \in G$. Similar cases can be applied in commutative semigroups and monoids.

Example 1.1.8 Let A be a nonempty set, $A^- := \{a^{-1} | a \in A\}$. Suppose B is a disjoint union of A and A^-, and $M(B)$ is the monoid defined in Example 1.1.4. If $a \in A$, then a is also denoted by $(a^{-1})^{-1}$ in $M(B)$ in the sequel. Suppose $a \in B$ lies immediately to a^{-1}. Then the word may be simplified by omitting the pair $a^{-1}a$, equivalently, cancelling $a^{-1}a$. A word that cannot be further simplified is said to be reduced. We claim that every word in $M(B)$ has a unique reduced word by cancelling all pairs $a^{-1}a$ for $a \in B$. We prove this claim by induction on the length of a word, the number of letters in the word. If $w \in M(B)$ is reduced, there is nothing to prove. If not, there must be some $a \in B$ lies immediately to a^{-1}. If we prove that we can obtain every reduced form of w by omitting $a^{-1}a$ first, then the claim will follow by induction because the word is shorter after this omitting. Let w_0 be the reduced word of w. It is obtained from w by some sequence of cancellations. The first case is that our pair $a^{-1}a$ is cancelled at some step in this sequence. If so,

we may as well omit $a^{-1}a$ first. So this case is settled. On the other hand, since w_0 is reduced, the pair $a^{-1}a$ cannot remain in w_0. At least one of a^{-1} and a must be cancelled at some time. If the pair $a^{-1}a$ itself is not omitted, the first omitting involving the pair must look like $\cdots \underline{a(a^{-1}a)} \cdots$, or $\cdots \underline{(a^{-1}a)a^{-1}} \cdots$. Notice that the word obtained by this omitting (omit the underline pairs) is the same as the one obtained by cancelling the pair $a^{-1}a$. So at this stage we may omit the original pair instead. Then we are back in the first case. Thus the claim is proved.

Let $F(A)$ be the set of all reduced words in $M(B)$. Define a binary operation on $F(A)$ as in $M(B)$ followed by reduction if necessary. Then this binary operation is well-defined. Suppose $w_i \in F(A)$ for $i = 1, 2, 3$. Then $(w_1w_2)w_3 = w_1(w_2w_3)$ in $M(B)$. They have the same reduced word w_0 in $F(A)$. So $w_1(w_2w_3) = (w_1w_2)w_3$ in $F(A)$. Hence $F(A)$ is a monoid with identity the empty word. Since the inverse of $a_1^{\varepsilon_1} \cdots a_n^{\varepsilon_n}$, where $\varepsilon_i = \pm 1$ and $a_i^1 = a_i$, is $a_n^{-\varepsilon_n} \cdots a_2^{-\varepsilon_2} a_1^{-\varepsilon_1}$, $F(A)$ is a group.

Exercises

1. Let A_n be the set of all ways of placing brackets (grammatically correctly) in the product $a_1 \cdot a_2 \cdots a_n$, i.e., the set of all expressions of the form $(a_1 \cdot a_2)((a_3 \cdot a_4) \cdots a_n)$. Prove that $|A_n| = \frac{1}{n} C_{2n-2}^{n-1}$. (Hint: $|A_n| = \sum_{k=1}^{n-1} |A_k||A_{n-k}|$.)
2. Given any sequence of elements $\{a_1, a_2, \cdots, a_n\}$ in a semigroup S. Prove that repeated application of the product of S produces the same result regardless how valid pairs of parenthesis are inserted among $a_1a_2 \cdots a_n$.
3. Suppose $a_1, \cdots, a_n$ are elements in a commutative semigroup. Show that $a_1 \cdots a_n = a_{\sigma(1)}a_{\sigma(2)} \cdots a_{\sigma(n)}$ for any $\sigma \in S_n$.
4. Define $a \circ b = a + b - ab$ in $\mathbb{Z}$. Show that $(\mathbb{Z}, \circ)$ is a commutative monoid.
5. Let $M := \mathbb{Z} \times \mathbb{Z}$ the set of all pairs of integers (x, y). Define $(x_1, x_2)(y_1, y_2) = (x_1y_1 + 2x_2y_2, x_1y_2 + x_2y_1)$. Show that this defines a commutative monoid. Show that the cancellation law holds for $(x_1, x_2) \neq (0, 0)$, that is, $(x_1, x_2)(y_1, y_2) = (x_1, x_2)(z_1, z_2)$ implies $(y_1, y_2) = (z_1, z_2)$
6. Let G be a semigroup. Show that G is a group if and only if there is an element $e \in G$ such that $ea = a$ for any $a \in G$, and there is an element $b \in G$ such that $ba = e$ for each $a \in G$. Show that G may be not a group if $ba = e$ is replaced by $ab = e$.
7. Suppose a, b are two elements in a group G with identity e. Prove that $b = a^{-1}$ if $ab = e$.
8. Let A, B be $m \times n$ and $n \times m$ matrices. Prove that $E_m - AB$ is invertible if and only if $E_n - BA$ is invertible.
9. Suppose $\mathbb{R}/\mathbb{Q} := \{a + \mathbb{Q} | a \in \mathbb{R}\}$, where $a + \mathbb{Q} := \{a + x | x \in \mathbb{Q}\} \subseteq \mathbb{R}$. Show that (1) $a + \mathbb{Q} = b + \mathbb{Q}$ if and only if $a - b \in \mathbb{Q}$; (2) the addition $(a + \mathbb{Q}) + (b + \mathbb{Q}) = (a + b) + \mathbb{Q}$ is well-defined in $\mathbb{R}/\mathbb{Q}$, that is, if $a + \mathbb{Q} = a' + \mathbb{Q}$, and $b + \mathbb{Q} = b' + \mathbb{Q}$, then $(a + b) + \mathbb{Q} = (a' + b') + \mathbb{Q}$; (3) $\mathbb{R}/\mathbb{Q}$ is an abelian group with the addition defined in (2).

10. Let a be an invertible element in a monoid G. Show that $a^m a^n = a^{m+n}$ (additive notation: $(m+n)a = ma+na$) and $(a^n)^m = a^{mn}$ (additive notation: $(mn)a = m(na)$) for any $m, n \in \mathbb{Z}$.

11. Suppose a, b are two elements in a group such that $ab = ba$, and $n \in \mathbb{Z}$. Show that $(ab)^n = a^n b^n$. Does $(ab)^n = a^n b^n$ hold if $ab \neq ba$?

12. Prove that the following conditions on a group G are equivalent: (1) G is abelian; (2) $(ab)^2 = a^2 b^2$ for all $a, b \in G$; (3) $(ab)^{-1} = a^{-1} b^{-1}$ for all $a, b \in G$; (4) $(ab)^n = a^n b^n$ for three consecutive integer n and any $a, b \in G$. Show that (4) $\Rightarrow$ (1) is false if "three" is replaced by "two".

13. If G is a finite group with identity e of even order, then G contains an element $a \neq e$ such that $a^2 = e$.

14. Let H be a subset of a finite group G and $|H| > |G|/2$. Prove that each element of G is a product of two elements in H.

15. Compute $\sigma\tau$, σ^2 and $\tau^{-1}\sigma\tau$, where $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ and $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}$.

16. Let $2^X := \{A | A \subseteq X\}$ for a set X. Show that 2^X is a group with multiplication defined by $A \Delta B := (A \setminus B) \cup (B \setminus A)$ for $A, B \in 2^X$. Suppose $|X| = n$. Prove that $|2^X| = 2^n$.

17. Let $A = \{t\}$ be a set of one element. Describe $S(A), M(A)$, and $F(A)$ defined in Examples 1.1.2, 1.1.4 and 1.1.8 respectively.

18. Suppose $y^2 = x^3 + ax + b$ is an elliptic curve, where a and b are real numbers, and the discriminant $\Delta = -16(4a^3 + 27b^2) \neq 0$. Let $G := \{(x, y) \in \mathbb{R}^2 | y^2 = x^3 + ax + b\} \cup \{E\}$. For any two points $P = (x_1, y_1), Q = (x_2, y_2)$ in G, define $R = P + Q$, where

$$R = \left(\left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 - x_1 - x_2, \frac{y_2 - y_1}{x_2 - x_1} \left(2x_1 + x_2 - \left(\frac{y_2 - y_1}{x_2 - x_1} \right)^2 \right) - y_1 \right) \text{ if } x_1 \neq x_2;$$

$$R = \left(\left(\frac{3x_1^2 + a}{2y_1} \right)^2 - 2x_1, \frac{3x_1^2 + a}{2y_1} \left(3x_1 - \frac{3x_1^2 + a}{2y_1} \right)^2 - y_1 \right) \text{ if } x_1 = x_2, y_1 = y_2 \neq 0;$$

and $R = E$ if $x_1 = x_2, y_1 = -y_2$, Show that G is an abelian group with the identity E. (Hint: if $x_1 \neq x_2$, then R is the third point which is the intersection of the curve with the line through P and Q.)

1.2 Subgroups

Recall that a nonempty subset U of a vector space V is a subspace if it is a vector space with the operations obtained from V by restriction. Similarly we call a nonempty subset H of a group G is a subgroup if it is a group with the binary operation followed from G by restriction. Explicitly, we have

Definition 1.2.1 *Let H and Z be two subsets of a group G.*

(a) *If $H \neq \varnothing$ and $a^{-1} b \in H$ for any $a, b \in H$, then H is called a* **subgroup** *of G, denoted by $H \leqslant G$.*

(b) *The intersection of all subgroups of G containing Z is denoted by $\langle Z\rangle$, which is called a* **subgroup generated by** *Z. If $Z = \{a_1, a_2, \cdots, a_n\}$, then $\langle Z\rangle$ is simply denoted by $\langle a_1, a_2, \cdots, a_n\rangle$.*

(c) *If Z is a subset of a group of G such that $G = \langle Z\rangle$, then Z is called a* **generator set** *of G. A group G is said to be* **cyclic** *if $G = \langle a\rangle$ for some $a \in G$.*

(d) *The order of $\langle a\rangle$ is also called the* **order** *of a, denoted by $|a|$.*

(e) *A group G is called a* **periodical group** *if $|a|$ is finite for any $a \in G$.*

Let H be a subset of a group of G. Then H said to be closed under the inverse (resp. the product) in G if $a^{-1} \in H$ (resp. $ab \in H$) for any $a, b \in H$. A nonempty subset H of a group G is a subgroup if and only if H is closed under the inverse and the product of G. In fact, if $H \leqslant G$ and $a, b \in H$, then $a^{-1} = a^{-1}(a^{-1}a) \in H$ and $ab = (a^{-1})^{-1}b \in H$ for any $a, b \in H$. Conversely, suppose H is closed under the inverse and the product of G. Then $a^{-1}b \in H$ for any $a, b \in H$ and $H \leqslant G$. Similarly, we can prove that a subset H of a group G is closed under the inverse and the product of G if and only if $ab^{-1} \in H$ for any $a, b \in H$. Thus a nonempty subset H of a group G is a subgroup if and only if $ab^{-1} \in H$ for any $a, b \in H$.

By Definition 1.2.1, $\langle\varnothing\rangle = \{e\}$. It is easy to prove that an intersection of subgroups is a subgroup. Thus $\langle Z\rangle$ is a subgroup of G for any subset Z of G.

Every group G has subgroups G and $\{e\}$. They are called **trivial subgroups**. A nontrivial subgroup is said to be **proper**.

Example 1.2.1 Let $\mathbb{Q}/\mathbb{Z} := \{a+\mathbb{Z} | a \in \mathbb{Q}\}$, and $\mathbb{Z}(p^\infty) := \left\{ \frac{a}{p^n} + \mathbb{Z} \middle| a \in \mathbb{Z}, n \in \mathbb{N} \right\}$, where p is a fixed prime number. Then $\mathbb{Z}(p^\infty)$ and $\mathbb{Q}/\mathbb{Z}$ are proper subgroups of $\mathbb{R}/\mathbb{Z}$. Moreover $\mathbb{Z}(p^\infty)$ and $\mathbb{Q}/\mathbb{Z}$ are periodical, but $\mathbb{R}/\mathbb{Z}$ is not periodical by Corollary 1.2.1 below.

Example 1.2.2 Let $SL(n, \mathbb{P}) := \{A \in GL(n, \mathbb{P}) | \det(A) = 1\}$, where $\det(A)$ is the determinant of the matrix A. Then $SL(n, \mathbb{P})$ is a subgroup of $GL(n, \mathbb{P})$. $SL(n, \mathbb{P})$ is called a **special linear group** over $\mathbb{P}$. Let $B(n, \mathbb{P})$ be the set of all upper triangular matrices in $GL(n, \mathbb{P})$. Then $B(n, \mathbb{P})$ is a subgroup of $GL(n, \mathbb{P})$, which is called a **Borel subgroup** of $GL(n, \mathbb{P})$. $W := \{A \in GL(n, \mathbb{P}) |$ every column and every row of A have only one nonzero number $1\}$ is a subgroup of $GL(n, \mathbb{P})$ (see Example 1.5.1), which is called a **Weyl subgroup** of $GL(n, \mathbb{P})$.

Let $J_{p,q} := \begin{pmatrix} E_p & 0 \\ 0 & -E_q \end{pmatrix}$. Then $O(p+q, \mathbb{P}) := \{A \in GL(p+q, \mathbb{P}) | A^{\mathrm{T}} J_{p,q} A = J_{p,q}\}$ is a subgroup of $GL(n, \mathbb{P})$, where A^{T} is the transpose of A. The group $O(p+q, \mathbb{P})$ is called the **orthogonal group** over $\mathbb{P}$. The group $SO(p+q, \mathbb{P}) := O(p+$

$q,\mathbb{P}) \cap SL(p+q,\mathbb{P})$ is called the **special orthogonal group** over $\mathbb{P}$. $SO(p+0,\mathbb{P})$ and $O(p+0,\mathbb{P})$ are simply denoted by $SO(p,\mathbb{P})$ and $O(p,\mathbb{P})$ respectively.

Let $A = (a_{ij})$ be a matrix with entries in the complex number field $\mathbb{C}$. Then $\bar{A} := (\overline{a_{ij}})$, where $\bar{a}$ is the conjugate complex number of a. Let $U(n) := \{A \in GL(n,\mathbb{C}) | \bar{A}^{\mathrm{T}}A = E\}$. Then $U(n) \leqslant GL(n,\mathbb{C})$. $U(n)$ is called a **unitary group**. $SU(n) := SL(n,\mathbb{C}) \cap U(n)$ is called a **special unitary group**.

Let $J := \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix}$. Then $Sp(2n,\mathbb{P}) := \{A \in GL(2n,\mathbb{P}) | A^{\mathrm{T}}JA = J\}$ is a subgroup of $GL(2n,\mathbb{P})$, which is called a **symplectic group**.

Remark 1.2.1 *If $\mathbb{P}$ is either $\mathbb{R}$ or $\mathbb{C}$, then all groups G defined in Example* 1.2.2 *are subspaces of Euclidean spaces. In addition, the product map $G \times G \to G$, $(A,B) \mapsto AB$ and inverse map $G \to G$, $A \mapsto A^{-1}$ are analytical. A group with an analytical product map and an analytical inverse map is called a* **Lie group**. *All groups defined in Example* 1.2.2 *are Lie groups when $\mathbb{P}$ is either $\mathbb{R}$ or $\mathbb{C}$.*

Theorem 1.2.1 *Let Z be a nonempty subset of a group G. Then*

$$\langle Z\rangle = \{x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n} \mid x_i \in Z, \varepsilon_i = \pm 1, n \in \mathbb{N}\}.$$

Note that it is possible that $x_i = x_j$ for some $i \neq j$. In particular, if G is an abelian group and its binary operation is denoted by "$+$", then

$$\langle Z\rangle = \left\{ \sum_{i=1}^{m} n_i x_i \middle| n_i \in \mathbb{Z}, x_i \in Z, m \in \mathbb{N} \right\}.$$

Proof Let $X := \{x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n} \mid x_i \in Z, \varepsilon_i = \pm 1, n \in \mathbb{N}\}$. It is obvious that $Z \subseteq X$. $\forall x = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n} \in X$ and $\forall y = y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_n^{\alpha_n} \in X$, we have $x^{-1}y = x_n^{-\varepsilon_n}x_{n-1}^{-\varepsilon_{n-1}}\cdots x_1^{-\varepsilon_1}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_n^{\alpha_n} \in X$. So $X \leqslant G$. Conversely, suppose H is a subgroup of G containing Z. For any $x = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_n^{\varepsilon_n} \in X$, since $H \leqslant G$ and $x_i \in Z \subseteq H$, $x_i^{\varepsilon_i} \in H$. So $x \in H$ and $X \subseteq H$. Thus $\langle Z\rangle = X$. □

Remark 1.2.2 *Let $A_i \leqslant G (i \in I)$, where G is an abelian group with a binary operation "$+$". Then* $\left\langle \bigcup_{i\in I} A_i \right\rangle = \left\{ \sum_{k=1}^{n} a_{i_k} \middle| a_{i_k} \in A_{i_k}, n \in \mathbb{N} \right\}$ *by Theorem* 1.2.1. *In this case* $\left\langle \bigcup_{i\in I} A_i \right\rangle$ *is denoted by* $\sum_{i\in I} A_i$.

For example, $GL(n,\mathbb{P}) = \langle Z\rangle$, where Z is the set of all $n \times n$ elementary matrices over the number field $\mathbb{P}$. Thus Z is a generator set of $GL(n,\mathbb{P})$. A mirror reflection γ_η determined by the unit vector $\eta \in \mathbb{R}^n$ is the mapping: $\gamma_\eta(\alpha) = \alpha - 2(\alpha,\eta)\eta$ for all $\alpha \in \mathbb{R}^n$. Let X be the set of matrices of all mirror reflections under a fixed normal

orthogonal basis. Since $O(n,\mathbb{R}) = \langle X\rangle$, X is a generator set of $O(n,\mathbb{R})$. For any nonempty set A, $F(A)$ defined in Example 1.1.8 is a group with a generator set A.

In the remainder of this chapter, we always use $m|n$ to indicate that m divides n for $m, n \in \mathbb{Z}$.

Corollary 1.2.1 *Let a be an element of a group G. Then $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$. Moreover, $|a| = t$ if and only if $a^t = e$ and $t|N$ for any integer N satisfying $a^N = e$.*

Proof $\langle a\rangle = \{a^n \mid n \in \mathbb{Z}\}$ follows from Theorem 1.2.1 directly. Let t be the minimal positive integer such that $a^t = e$. $\forall n \in \mathbb{Z}$, there are elements $m, r \in \mathbb{Z}$, such that $n = mt + r$, where $0 \leqslant r < t$. Then $a^n = a^{mt+r} = (a^t)^m a^r = a^r$. So $\langle a\rangle = \{e, a, \cdots, a^{t-1}\}$. If there are integers s, l satisfying $0 \leqslant s < l \leqslant t-1$ such that $a^s = a^l$, then $a^{l-s} = a^l(a^s)^{-1} = e$. Since $0 < l - s \leqslant t-1$, this contradicts the assumption about t. So $|\langle a\rangle| = t$.

Conversely, assume that $|\langle a\rangle| = t$. Since $\langle a\rangle$ is finite, there are positive integers $k < s$ such that $a^k = a^s$. Then $a^{s-k} = a^s(a^k)^{-1} = e$. Thus, there is a least positive integer l such that $a^l = e$. Then $l = |\{e, a, a^2, \cdots, a^{l-1}\}| = |\langle a\rangle| = t$. Now suppose there is an integer N such that $a^N = e$ and $N = qt + r$ for $0 \leqslant r < t$. Then $e = a^N = (a^t)^q a^r = a^r$. So $r = 0$ by the choice of t, that is, $t|N$. □

Theorem 1.2.2 *Suppose $|\langle a\rangle| = n$ and $d|n$. Then $\langle a\rangle$ has a unique subgroup with order d, which is generated by $a^{\frac{n}{d}}$.*

Proof Suppose $d|n$ and $m = \dfrac{n}{d}$. If $|\langle a^m\rangle| = t$, then t is the minimal positive integer such that $(a^m)^t = a^{mt} = e$. Hence $t|d$ as $(a^m)^d = e$. Since $|\langle a\rangle| = md$, $md|mt$, i.e., $d|t$. Thus $d = t$. Next, let H be an arbitrary subgroup of order d and let s be the least positive integer such that $a^s \in H$. Suppose $a^k \in H$, where $k = qs + r$ for some $0 \leqslant r < s$. Then $a^r = a^k((a^s)^q)^{-1} \in H$. So $r = 0$. Thus $H = \langle a^s\rangle$. Since $|H| = d$, $(a^s)^d = a^{sd} = a^{dm} = e$. Then $dm|sd$, i.e., $m|s$. From this, we have $a^s \in \langle a^m\rangle$ and $H = \langle a^s\rangle \subseteq \langle a^m\rangle$. Thus $H = \langle a^s\rangle = \langle a^m\rangle$ since $|H| = |\langle a^m\rangle| = d$. □

Example 1.2.3 Let $\sigma \in S_n$ satisfying $\sigma(i_j) = i_{j+1}$ for $j = 1, 2, \cdots, k-1$, $\sigma(i_k) = i_1$, and $\sigma(m) = m$ for any other integers m. Then this σ, denoted by $(i_1, i_2, \cdots, i_k)$, is called a **k-cycle** of S_n. It is obvious that k is the least positive integer such that $\sigma^k(l) = l$ for any $1 \leqslant l \leqslant n$. Hence $|\sigma| = k$ and $\langle\sigma\rangle$ is a cyclic group with order k. The 2-cycle is called a **transposition**. For the sake of convenience, the identity mapping id is denoted by 1-cycle (i) for any $1 \leqslant i \leqslant n$. The 1-cycle is called a **trivial cycle**. A **nontrivial cycle** is a k-cycle for $k \geqslant 2$.

Definition 1.2.2 *Two nontrivial cycles $(i_1, \cdots, i_k)$ and $(j_1, \cdots, j_s)$ are* **disjoint** *if $\{i_1, \cdots, i_k\} \cap \{j_1, \cdots, j_s\} = \varnothing$.*

Theorem 1.2.3 *Suppose $\sigma = (i_1, i_2, \cdots, i_k)$ is a k-cycle of S_n, and $\tau \in S_n$. Then (1) $\tau\sigma\tau^{-1} = (\tau(i_1), \tau(i_2), \cdots, \tau(i_k))$. In particular, $\tau\sigma\tau^{-1}$ is also a k-cycle of S_n.*

(2) *Let* $\rho = (j_1, j_2, \cdots, j_s)$. *If* ρ *is disjoint to* σ, *then* $\rho\sigma = \sigma\rho$.

(3) $S_n = \langle \sigma_1, \sigma_2, \cdots, \sigma_{n-1} \rangle$, *where* $\sigma_i = (i, i+1)$. *Moreover,* $\sigma_i^2 = \mathrm{id}$, $\sigma_i\sigma_j = \sigma_j\sigma_i$ *if* $|i-j| \geqslant 2$, *and* $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} = (i, i+2)$.

Proof (1) Observe that $\tau\sigma\tau^{-1} = (\tau(i_1), \tau(i_2), \cdots, \tau(i_k))$ if and only if $\tau\sigma = (\tau(i_1), \tau(i_2), \cdots, \tau(i_k))\tau$. If $m = i_j$, then $\tau\sigma(m) = \tau\sigma(i_j) = \tau(i_{j+1}) = (\tau(i_1), \tau(i_2), \cdots, \tau(i_k))\tau(m)$ for $j = 1, 2, \cdots, k-1$, and $\tau\sigma(i_k) = \tau(i_1) = (\tau(i_1), \tau(i_2), \cdots, \tau(i_k))\tau(i_k)$. If $m \neq i_j$ for any $j = 1, 2, \cdots, k$, then $\tau(m) \neq \tau(i_j)$, and $\tau\sigma(m) = \tau(m) = (\tau(i_1), \tau(i_2), \cdots, \tau(i_k))\tau(m)$. Thus, (1) follows.

(2) If $m = i_s$, then $\sigma\rho(m) = \sigma(i_s) = \rho\sigma(m)$. Similarly we have $\sigma\rho(m) = \rho(j_s) = \rho\sigma(m)$ if $m = j_s$. For any other m, we have $\sigma\rho(m) = m = \rho\sigma(m)$. So (2) holds.

(3) It suffices to prove $S_n = \langle \sigma_i | i = 1, 2, \cdots, n-1 \rangle$ since the rest follows from (1). For $n = 2$, (1) $= \sigma_1^2$. For any $\sigma \in S_n$, if $\sigma(n) = n$, then $\sigma \in S_{n-1}$ is a product of some elements $\sigma_i (i = 1, \cdots, n-2)$ by the inductive assumption. If $\sigma(n) \neq n$, then there is an integer k such that $\sigma(k) = n$. Thus $\tau = \sigma \circ (k, n)$ satisfying $\tau(n) = n$. So $\sigma \circ (k, n) = \tau = \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_t}$ and $\sigma = \sigma_{i_1}\sigma_{i_2}\cdots\sigma_{i_t}(k, n)$. Since $\sigma_{n-2}\cdots\sigma_{k+1}\sigma_k(k, n)\sigma_k\sigma_{k+1}\cdots\sigma_{n-2} = \sigma_{n-1}$, we have $(k, n) = \sigma_k\sigma_{k+1}\cdots\sigma_{n-2}\sigma_{n-1}\sigma_{n-2}\cdots\sigma_{k+1}\sigma_k$. This completes the proof. □

Exercises

1. Show that an infinite group is cyclic if and only if each of its proper subgroups is an infinite cyclic group. Try to determine all subgroups of $(\mathbb{Z}, +)$.
2. Let G be an abelian group generated by $a_1, \cdots a_n$. Suppose $|a_i| < \infty$ for all i. Prove that G is finite.
3. Suppose $a_1, \cdots, a_n \in \mathbb{Q}$. Show that $\langle a_1, \cdots, a_n \rangle$ is a cyclic subgroup of the additive group $(\mathbb{Q}, +)$.
4. Let G be a group. For any elements $a, b \in G$, prove that the order of ab and that of ba are equal.
5. Let G be a cyclic group of order 12. How many elements a in G such that $G = \langle a \rangle$?
6. Suppose H, K are two subgroups of G and $HK = \{ab | a \in H, b \in K\}$. Show that HK is a subgroup of G if and only if $HK = KH$.
7. Show that S_n is generated by $(12), (13), \cdots, (1n)$.
8. Let G be a group generated by $a_1, \cdots, a_n$. Show that G is abelian if and only if $a_ia_j = a_ja_i$ for all $1 \leqslant i < j \leqslant n$.
9. Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}$. Suppose Q_8 is the group (under matrix multiplication) generated by A and B. Usually, the indentity matrix E, A, B and AB in Q_8 are denoted by 1, i, j, and k respectively. Show that $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$. Q_8 is called the **quaternion group**.
10. Let $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, and D_4^* be the group (under matrix multiplication) generated by A and B. Show that D_4^* is a noncommutative group of order 8. D_4^* is called the **group of symmetries of a square**.