# Lecture Notes On Abstract Algebra (Week 1)

Guohua PENG (彭国华)
email: peng@scu.edu.cn

## Contents



# 1 Lecture 1 (Sep 5, 2023): Opening

## 1.1 Syllabus

- **Course Title**

  *Abstract Algebra*

- **Credits**

  4

- **Course Information**

  The main contents of the course include an overview on group theory which you had learnt in *Number Theory and Basics of Algebra* (数论与代数基础) more than a year ago; basic ring theory; basic module theory; the structure of finitely generated abelian groups; field extension; finite fields; Galois theory.

- **Learning Outcomes**

  You are hoped to know the basic concepts and properties of groups, rings, fields and their applications. It is required to grasp the typical examples and the basis technique of abstract reasoning.

  We try to solve the following problems:

  ♣ Why a disk is symmetric than a square?

  ♣ Prove the first case of Fermat's Last Theorem (费马大定理) under some assumptions.

- ♣ What kind of numbers are acceptable in ancient Greeks' eyes?
- ♣ Why is it impossible to trisect (divide into three equal parts) a general angle by using compasses and straightedge (without marks on it, for drawing straight line segments through two points)?
- ♣ Why is it impossible to construct a cube having twice the volume of some given cube by using compasses and straightedge?
- ♣ Why is it impossible to construct a square having the same area as a given circle by using compasses and straightedge?
- ♣ Why a quintic polynomial is not solvable by radicals? (Why it is impossible to give out a formula to the zeros of a general quintic polynomial?)

- **Lectures**

  We will *NOT* strictly follow the textbook. But the final exam will only dependent on the textbook.

  There will be two lectures each week, on Tuesday (Room 313, No.3 Teaching Building) and Thursday (Room 246, No.3 Teaching Building) 8:00-9:40 am. Total learning-hour is about 64.

- **Exercises**

  Some exercises will not be included in the textbook. You are encouraged to hand in your homework on each *Tuesday*. Please notice that your homework and your presentation in class will contribute to your final marks.

- **Tutorial and Teaching Assistant**

  Xiantao Deng (邓先涛), email: 2567972968@qq.com (xiantao.deng@qq.com), mobile phone: 15111541247.

  QQ learning group: 611286706 (川大2023《抽象代数》学习)


- **Teaching and Learning Methods**

  The learning methods dependent on you. Any method which has been proven to be successful to you is still applicable.

- **Learning Materials**

  There are many books on Abstract Algebra most of which have almost the same title and contain much the same material.

✠ **Books**

1. Linzhao Nie and Shisun Ding, Introduction to Algebra (3rd edition, in Chinese), Higher Education Press, 2021
2. N. Jacobson, Basic Algebra I (2nd edition), W. H. Freeman and Company, New York, 1985
3. M. Artin, Algebra, Addison Wesley, 2010

✠ **Internet Resources for Abstract Algebra** You may search Bing, Google (currently not available in mainland) or Baidu to find a lot of online learning materials. Wiki (not available in mainland) is also a good helper for your learning.

- **Assessment** Your final marks for the course will be calculated as follows:

  ♠ 10%: Response in class.

  ♠ 10%: Homework marks.

  ♠ 20%: Quiz marks.

  ♠ 60%: Final exam.

- **Quizzes**

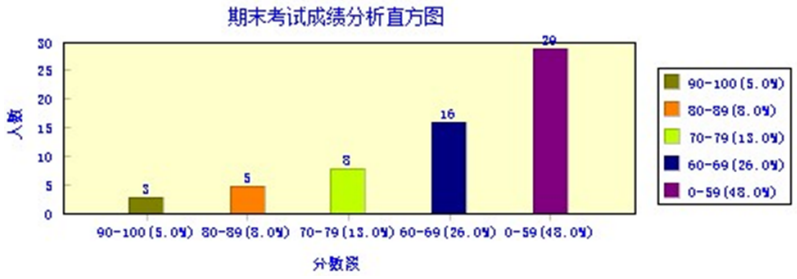
  There will be 5 quizzes. They are scheduled on Sep 14, Sep 28, Oct 26, Nov 23 and Dec 21. These quizzes will play an important role in your final marks.

- **Score Distribution of Final Exam 2022**

四川大学课程考核结果分析

2022-2023学年秋（两学期）

| | | | | | |
|---|---|---|---|---|---|
| 课程名称 | 抽象代数 | 学时 | 64 | 学分 | 4 |
| 成绩构成 | 总成绩 = 期末考试*60%+平时成绩*40% | | | | |
| 上课人数 | 63 | 考核人数 | 61 | | |
| 平均分 | 71.1 | 最高分 | 98. | 最低分 | 28. |
| 未参与考核原因及人数 | 缺考<br>2 | | | | |




- **Office Hour**

  ♡ Office: E-217, Management Building, Wangjiang Campus

  ♡ Time: Thursday 15:00-16:30 or by appointment

  ♡ Email: peng@scu.edu.cn

## 1.2 Review: Group Theory

1. Definition of group, subgroup, normal group, simple group, quotient group

2. Direct sum of groups
3. Lagrange Theorem: $H < G$ with $|G| < \infty$, then $|H| \mid |G|$.
4. Cayley Theory: $G \hookrightarrow \mathrm{Aut}(G)$.
5. Homomorphism Theorem
6. Sylow Theorem

In the field of finite group theory, the Sylow theorems are a collection of theorems named after the Norwegian mathematician Ludwig Sylow (1872) that give detailed information about the number of subgroups of fixed order that a given finite group contains. The Sylow theorems form a fundamental part of finite group theory and have very important applications in the classification of finite simple groups.

The Sylow theorems assert a partial converse to Lagrange's theorem that for any finite group $G$ the order of every subgroup of $G$ divides the order of $G$. *The converse of Lagrange's theorem is false.* The simplest example of this is the group $A_4$, of order 12, which has no subgroup of order 6.

**Notation**

- Let $p$ be a prime number and $m, n \in \mathbb{Z}$ with $n > 0$. The notation $p^n \| m$ means $p^n$ is a divisor of $m$ and $p^{n+1}$ is not, i.e, $p^n | m$ but $p^{n+1} \nmid m$. Thus $p^n \| m$ if and only if $m = p^n s$ with $(p, s) = 1$.
- Let $g$ be an element in a group $G$. The symbol $o(g)$ denotes the order of $g$ in $G$.

Let $G$ be a finite group and $p^n \| |G|$ with $n > 0$, where $p$ is prime. Then any subgroup of $G$ with order $p^n$ is called a **Sylow $p$-subgroup** (西洛$p$-子群) of $G$. For example, a subgroup of order 8 is a 2-sylow subgroup of a group with order 24.

**Example 1.1.** For the alternative group (交错群) $A_4$ whose order is 12, there is a unique 2-Sylow subgroup:

$$\{(1), (12)(34), (13)(24), (14)(23)\}$$

and there are four 3-Sylow subgroups:

$$\{(1), (123), (132)\}, \quad \{(1), (124), (142)\}, \quad \{(1), (134), (143)\}, \quad \{(1), (234), (243)\}.$$

**Example 1.2.** For the dihedral group (二面体群)

$$\begin{aligned} D_6 &= \langle S, T \mid o(S) = 2, o(T) = n, STS = T^{-1} \rangle \\ &= \{1, T, \ldots, T^5, S, TS, \ldots, T^5 S\}, \end{aligned}$$

the symmetry group of a regular hexagon (正六边形的对称群) with order 12, there are three 2-Sylow subgroups:

$$\{1, T^3, S, T^3 S\} = \langle T^3, S \rangle, \quad \{1, T^3, TS, T^4 S\} = \langle T^3, TS \rangle, \quad \{1, T^3, T^2 S, T^5 S\} = \langle T^3, T^2 S \rangle.$$

The only 3-Sylow subgroup of $D_6$ is $\{1, T^2, T^4\}$.

The symmetry group of a snowflake is $D_6$

**Example 1.3.** We know the symmetric group (对称群) $S_4$ is of order $24 = 2^3 \times 3$. How many 3-Sylow and 2-Sylow subgroups are there in $S_4$? Firstly every 3-Sylow subgroup of $S_4$ is a 3-Sylow subgroup of $A_4$ (an element of 3-power order in $S_4$ must be a 3-cycle, which all lie in $A_4$). We determined the 3-Sylow subgroups of $A_4$ in Example 1.1; there are four of them. Secondly there are three 2-Sylow subgroups of $S_4$, and they are interesting to work out since they can be understood as copies of $D_4$ inside $S_4$.

**Theorem 1.1 (Sylow Theorem).** *Let $|G| = p^n m$, where $p$ is a prime and $p \nmid m$.*

1. (First Sylow Theorem) *For $0 \leq k \leq n$, there is a subgroup of order $p^k$.*
2. (Second Sylow Theorem) *Let $P$ be a Sylow $p$-subgroup. Then every subgroup of order $p^k$ with $0 \leq k \leq n$ is contained in a conjugate of $P$. In particular, all Sylow $p$-subgroups are conjugate.*
3. (Third Sylow Theorem) *Let $n_p$ be the number of Sylow $p$-subgroups. Then $n_p \mid m$ and $n_p \equiv 1 (\mathrm{mod}\, p)$.*

**Corollary 1.1.** *If $n_p = 1$, then the Sylow $p$-subgroup is normal. The converse is true.*

**Remark 1.1.** Sylow's theorem in the theory of finite groups consists of the following three parts: If the order of a group $G$ is divisible by $p^n$, $p$ being a prime number, but not by a higher power of $p$, then $G$ contains at least one subgroup of order $p^n$, and if it contains more than one such subgroup all of these subgroups are conjugate under $G$ and their number $n_p$ is of the form $1 + tp$. The first of these three parts can be proved independently of the other two parts. In fact, these two parts follow almost directly from the first of these three parts.

## 1.3 A Mathematical Love Song: Finite Simple Group (of Order Two)

Sometimes Mathematical terminology appears beautiful, instead of boring as usual. The following song *Finite simple group* (*of order two*) created by *The Klein Four* sounds interesting. The Klein Four is a very talented cappella group "of the world of higher mathematics" of the Northwestern University mathematics department, composed of Clark Alexander, Scott Bailey, Mike Johnson, Kal Nanes, and Matt Salomone. Their viral single, a mathematical love song called *Finite simple group* (*of order two*), is funny and clever in an endearingly nerdy way. The Klein Four Group have recorded two albums, *Musical Fruitcake* and *Elements*. Video on Finite Simple Group (of Order Two) is available at https://www.bilibili.com/video/av292318/

or

https://www.bilibili.com/video/av12003536

**The lyrics for Finite Simple Group (of Order Two)**

*The path of love is never smooth*
*But mine's continuous for you*

*You're the upper bound in the chains of my heart*
*You're my Axiom of Choice, you know it's true.*

*But lately our relation's not so well-defined*
*And I just can't function without you*
*I'll prove my proposition and I'm sure you'll find*
*We're a finite simple group of order two.*

*I'm losing my identity*
*I'm getting tensor every day*
*And without loss of generality*
*I will assume that you feel the same way.*

*Since every time I see you you just quotient out*
*The faithful image that I map into*
*But when we're one-to-one you'll see what I'm about*
*'Cause we're a finite simple group of order two.*

*Our equivalence was stable*
*A principal love bundle sitting deep inside*
*But then you drove a wedge between our two-forms*
*Now everything is so complexified.*

*When we first met we simply connected*
*My heart was open but too dense*
*Our system was already directed*
*To have a finite limit in some sense.*

*I'm living in the kernel of a rank-one map*
*From my domain its image looks so blue*
*'Cause all I see are zeroes it's a cruel trap*
*But we're a finite simple group of order two.*

*I'm not the smoothest operator in my class*
*But we're a mirror pair me and you*
*So let's apply forgetful functors to the past*
*And be a finite simple group, a finite simple group*
*Let's be a finite simple group of order two.*
*(Oughter: "Why not three?")*

*I've proved my proposition now as you can see*
*So let's both be associative and free*
*And by corollary this shows you and I to be*
*Purely inseparable. Q. E. D.*

# 2 Lecture 2 (Sep 7, 2023): Rings

## 2.1 History of Rings

The study of rings originated from the theory of polynomial rings and the theory of algebraic integers. Furthermore, the appearance of hypercomplex numbers in the mid-19th century undercut the preeminence of fields in mathematical analysis.

In the 1880s Richard Dedekind introduced the concept of a ring, and the term *Zahlring* (Number ring) was coined by David Hilbert in 1892 and published in the article *Die Theorie der algebraischen Zahlkörper, Jahresbericht der Deutschen Mathematiker Vereinigung*, Vol. 4, 1897. In 19th-century German, the word "Ring" could mean "association", which is still used today in English in a limited sense (e.g., spy ring (间谍组织)), so if that were the etymology then it would be similar to the way "group" entered mathematics by being a non-technical word for "collection of related things".

According to Harvey Cohn, Hilbert used the term for a specific ring that had the property of "circling directly back" to an element of itself. Specifically, in a ring of algebraic integers, all high powers of an algebraic integer can be written as an integral combination of a fixed set of lower powers, and thus the powers "cycle back". For instance, if $a^3 - 4a + 1 = 0$ then $a^3 = 4a - 1, a^4 = 4a^2 - a, a^5 = 4a^3 - a^2 = -a^2 + 16a - 4, a^6 = 16a^2 - 8a + 1, a^7 = -8a^2 + 65a - 16$, and so on; in general, $a^n$ is going to be an integral linear combination of $1, a$ and $a^2$.

The first axiomatic definition of a ring was given by Adolf Fraenkel in an essay in *Journal für die reine und angewandte Mathematik* (A. L. Crelle), vol. 145, 1914. In 1921, Emmy Noether gave the first axiomatic foundation of the theory of commutative rings in her monumental paper *Ideal Theory in Rings*.

Basically, a fair bit of ring theory was developed for algebraic number theory. This in turn was because people were trying to prove Fermat's Last Theorem (FLT).

Let $p$ be a prime. Then the equation $x^p + y^p = z^p$ can be written as $\prod_{i=0}^{p-1}(x + \zeta_p^i y) = z^p$ for a primitive $p$-th root of unity $\zeta_p$. All these quantities are elements of the ring $\mathbb{Z}[\zeta_p]$. So if $p > 3$ and there is unique factorization in the ring $\mathbb{Z}[\zeta_p]$, it isn't terribly hard to show that this is impossible at least in the basic case where $p$ does not divide $xyz$ (We will prove this at the end of our *Ring Theory*).

Lame actually thought he had a proof of FLT via this argument. But he was wrong: these rings generally don't admit unique factorization. So, it became a problem to study these "generalized integers" $\mathbb{Z}[\zeta_p]$, which of course are basic examples of rings. It wasn't until Dedekind that the right notion of unique factorization—namely, factorization of ideals—was found. In fact, the case of FLT just mentioned generalizes to the case where $p$ does not divide the class number of $\mathbb{Z}[\zeta_p]$ (the class number is the invariant that measures how far it is from being a UFD). And, according to this article, Dedekind was the first to define a ring.

## 2.2 Definition of Rings

**Definition 2.1** (ring)**.** *A* **ring** (环) *is a structure consisting of a non-empty set $R$ together with two binary operation, say $+$ and $\cdot$, in $R$ and one distinguished element $0 \in R$ such that*

1. *$(R, +, 0)$ is an abelian group;*
2. *multiplication "$\cdot$" is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;*
3. *the distributive laws*

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(b + c) \cdot a = b \cdot a + c \cdot a$$

*holds for all* $a, b, c \in R$.

*A subset* $S$ *of* $R$ *is called a* **subring** (子环) *if* $S$ *together with the operations in* $R$ *form a ring.*

More precisely, a non-empty set $R$ is called a ring, if there are two operations " $+$ " and " $\cdot$ " such that for all $a, b, c \in R$,

(1) $(a + b) + c = a + (b + c)$;

(2) $a + b = b + a$;

(3) there exists a zero element "0" such that $a + 0 = 0 + a = a$;

(4) there exists an inverse $-a$ such that $a + (-a) = -a + a = 0$;

(5) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(6) $a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$.

Further more, if there is an element "1" such that that

(7) $a \cdot 1 = 1 \cdot a = a$, then $R$ is called a **ring with identity** (幺环).

**Remark 2.1.**

1. The structure $(R, +, 0)$ is called the *additive group* of $R$ and $(R, \cdot, 1)$ is called the *multiplicative monoid* of $R$ if $R$ is a ring with identity.
2. For simplicity, we write "$ab$" for $a \cdot b$.
3. We have $0a = a0 = 0$ and $(ma)b = a(mb) = m(ab)$ for $m \in \mathbb{Z}$ and $a, b \in R$.
4. A subset $S$ of a ring $R$ (with identity) is a subring, if $1 \in S$ and $a - b \in S$, $ab \in S$ for all $a, b \in S$.
5. We do not exclude the possibility in (7) that 1 might be equal to 0. If so, then
$$x = x \cdot 1 = x \cdot 0 = 0$$
for any $x \in R$, and $R$ has only one element 0. In such case, $R$ is called the *zero ring*.
6. Throughout our lectures, the word "ring" always means a ring with identity, unless otherwise specified. Hence a ring (with identity) has at least two elements: 0 and 1.

**Example 2.1.** The integers $\mathbb{Z}$ with the usual addition and multiplication is a ring with identity. We call $\mathbb{Z}$ the *ring of (rational) integers* (整数环). Similarly, one can see $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are ring.

**Example 2.2.** The set $\mathbb{Z}[\sqrt{-1}] = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Z}\}$ is a subring of $\mathbb{C}$. We call $\mathbb{Z}[\sqrt{-1}]$ the *ring of Gaussian integers* (高斯整数环).

**Example 2.3.** Let $F$ be a number field. Then $F[x]$, the set of all polynomials in one variable over $F$, becomes a ring with respect to the usual operations. The ring $F[x]$ is called the *ring of polynomials over* $F$, or simply say the polynomial ring (多项式环).

**Example 2.4.** The set $C[a,b]$ of all real continuous function on the closed interval $[a,b]$. Here we define

$$(f+g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x).$$

One can see that $\mathbb{R}[x]$ is a proper subring of $C[a,b]$.

**Example 2.5.** Let $F$ be a number field and $V$ an $n$-dimensional vector space over $F$. Then $\mathrm{End}(V)$, the set of all linear transformations of $V$, is a ring under the following operations:

$$(\mathbf{A}+\mathbf{B})(\alpha) = \mathbf{A}\alpha + \mathbf{B}\alpha, \quad (\mathbf{AB})(\alpha) = \mathbf{A}(\mathbf{B}\alpha).$$

Notice that here the multiplication is the composition of maps.

**Example 2.6.** The set

$$\frac{1}{p^\infty}\mathbb{Z} = \left\{ \frac{a}{p^n} \,\middle|\, a, n \in \mathbb{Z}, n \geq 0 \right\}$$

is a ring endowed with the usual addition and multiplication.

**Example 2.7.** The set $\mathrm{M}_n(F)$ of all $n \times n$ matrices over a number field $F$ becomes a ring in an obvious way. But $\mathrm{GL}_n(F)$ is not a subring of $\mathrm{M}_n(F)$.

**Example 2.8.** Let $n$ be a nonzero integer. We know that

$$\mathbb{Z}/n\mathbb{Z} = \{\overline{a} \mid a \in \mathbb{Z}\}, \tag{1}$$

where $\overline{a} = a + n\mathbb{Z}$ denotes the residue class of $a$ modulo $n$. Define

$$\overline{a} + \overline{b} = \overline{a+b},$$
$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

It's easy to verify that these two operations are well-defined:

$$\overline{a} = \overline{a_1},\ \overline{b} = \overline{b_1} \Longrightarrow \overline{a} + \overline{b} = \overline{a_1} + \overline{b_1},$$
$$\overline{a} \cdot \overline{b} = \overline{a_1} \cdot \overline{b_1}.$$

And $\mathbb{Z}/n\mathbb{Z}$ becomes a ring with $|n|$ elements with the above operations. Its zero element is $\overline{0}$ and $\overline{1}$ is the unit. We call $\mathbb{Z}/n\mathbb{Z}$ the **residue ring modulo** $n$ (模$n$的剩余类环).

**Example 2.9.** The set $R = \{0,1,2,3\}$. The operations are given by

| $+$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

and

| $\times$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | 2 | 3 |
| 2 | 0 | 2 | 0 | 2 |
| 3 | 0 | 3 | 2 | 1 |

.

Actually, this ring is isomorphic to the residue ring $\mathbb{Z}/4\mathbb{Z}$.

## 2.3 Types of Rings

Let $R$ be a ring (with identity). Denote $R^* = \{x \in R \mid x \neq 0\}$ to be the set of non-zero elements.

**Definition 2.2** (commutative ring)**.** *If $ab = ba$ for $a, b \in R$, then $R$ is called a* **commutative ring** (交换环).

A commutative ring is a ring whose multiplicative monoid is commutative. For example, $\mathbb{Z}$, $\mathbb{C}$, $F[x]$ and $C[a,b]$ are commutative rings. But $\mathrm{M}_n(F)$ is not a commutative ring if $n \geq 2$.

**Remark 2.2.** In a commutative ring $R$, we have the *binomial theorem*:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i} \tag{2}$$

for all $a, b \in R$ and $n \geq 0$.

**Example 2.10.** Let $R$ be a commutative ring and let $M_n(R)$ be the set of all $n \times n$ matrices whose entries are in $R$. If $R$ is a number field, we know that $M_n(R)$ becomes a ring with the addition and multiplication of matrices. For general commutative ring $R$, $M_n(R)$ becomes a ring in a similar way. We call $M_n(R)$ the **ring of $n \times n$ matrices over $R$**. For example, $M_n(\mathbb{Z})$ is the ring of $n \times n$ matrices with integral entries. And $M_n(\mathbb{Z}/m\mathbb{Z})$ is a finite ring of $m^n$ elements. If $n \geq 2$, $M_n(R)$ is not a commutative ring.

**Definition 2.3** (zero divisor)**.** *Let $a \in R^*$. If there exists an element $b \in R^*$ such that $ab = 0$ (or $ba = 0$), then $a$ is called a* **left zero divisor** *(or* **right zero divisor***). Left zero divisors and right zero divisors are called* zero divisors (零因子).

For example, $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is a left zero divisor and a right zero divisor in $\mathrm{M}_2(F)$, since

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

In example (2.9), 2 is a left zero divisor as well as a right zero divisor, since $2 \cdot 2 = 0$.

**Definition 2.4** (domain)**.** *If $R$ is commutative and has no zero divisors, then $R$ is called a* **domain** *(or* **integral domain**, 整环).

For example, $\mathbb{Z}$ and $F[x]$ are (integral) domains, but $\mathrm{M}_n(F)$ and $C[a,b]$ are not domains when $n \geq 2$, $a < b$.

**Remark 2.3.** 1. By the definition, we have

$$\begin{aligned} &R \text{ is a domain} \iff R^*, \text{ non-zero elements of } R, \text{ is a submonoid of } (R, \cdot, 1) \\ &\iff ab = 0 \text{ implies either } a = 0 \text{ or } b = 0. \end{aligned} \tag{3}$$

2. The cancellation law (消去律) holds in a domain: if $ab = ac$ and $a \neq 0$, then $b = c$; if $ba = ca$ and $a \neq 0$, then $b = c$.

**Definition 2.5** (unit)**.** *If $a \in R$ is invertible, i.e., there exists $b \in R$ such that $ab = ba = 1$, then $a$ is called a* **unit** (单位)*. Denote the set of all units of $R$ by $R^\times$ (or $U(R)$).*

**Remark 2.4.** 1. A unit in a ring is an element which has an inverse under multiplication. So a unit is also called an *invertible element* (逆元). The inverse of a unit $a$ is unique and denoted by $a^{-1}$.

2. If $ab = 1$, then $a$ is called a *left inverse* (左逆元) of $b$, and $b$ is called a *right inverse* (右逆元) of $a$.

For example, $(\mathrm{M}_n(F))^\times = \mathrm{GL}_n(F)$, $\mathbb{Z}^\times = \{1, -1\}$, $\mathbb{C}^\times = \mathbb{C}^*$ and

$$C[a,b]^\times = \{f \in C[a,b] \mid f(x) \neq 0 \text{ for all } a \leq x \leq b\}.$$

**Proposition 2.1.** *We have $(R^\times, \cdot, 1)$ is a group, called the* **group of units** (单位群) *of $R$.*

**Definition 2.6** (division ring)**.** *The ring $R$ is called a* **division ring** (除环) *(or skew field) if every non-zero element of $R$ is a unit. A commutative division ring is called a* **field** (域) *.*

In other words, $R$ is a division ring if and only if $(R^*, \cdot, 1)$ is a group. For example, $\mathbb{Q}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Q}\}$ is a division ring, hence a field. The number fields we discussed in linear algebra are just fields contain in $\mathbb{C}$. We know that $\mathbb{Q}[\sqrt{-5}]$ is a number field.

Let $D$ be a (open) region in the plane. Then

$$\mathbb{C}(D) = \{f : D \to \mathbb{C} \mid f \text{ is meromorphic}\}$$

is a field under the usual addition and multiplication of complex functions. This field is not a number field in general.

Consider the subset $\mathbb{H}$ of the ring $\mathrm{M}_2(\mathbb{C})$ of matrices having the form

$$A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} = \begin{pmatrix} a_0 + a_1\sqrt{-1} & a_2 + a_1 3\sqrt{-1} \\ -a_2 - a_3\sqrt{-1} & a_0 - a_1\sqrt{-1} \end{pmatrix},$$

where $\alpha, \beta \in \mathbb{C}$ and $a_0, a_1, a_2, a_3 \in \mathbb{R}$. We will show that $\mathbb{H}$ is a division ring (hence a subring of $\mathrm{M}_2(\mathbb{C})$), but not a field. The ring $\mathbb{H}$ is called the *Hamilton quaternion* (Hamilton四元数环).

**Theorem 2.1.** *A finite domain is a field.*

**Remark 2.5.** Let $p$ be a prime number. The residue ring $\mathbb{Z}/p\mathbb{Z}$ is a domain with $p$ elements. Hence $\mathbb{Z}/p\mathbb{Z}$ is a field with $p$ elements. Such fields are called *finite fields*. We write $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. In particular,

$$\mathbb{F}_2 = \{0, 1\}$$

is a finite field with 2 elements, and the addition group $(\mathbb{F}_2, +, 0)$ is a finite simple group of order 2.

**Exercises**

1. Show that if all the axioms for a ring (with identity) except commutativity of addition are satisfied, then commutativity follows, and hence we have a ring structure.

2. Let $G$ be an additive group. For $a, b \in G$, define the multiplicative operation " $\cdot$ " by $a \cdot b = 0$.

   (1) Show that $G$ becomes a ring.

   (2) If $G$ has at least two elements, then $G$ is a ring with no identity.

3. Let $M$ be an abelian group and let $\mathrm{End}(M)$ denote the set of all endomorphisms of $M$. The addition and multiplication in $\mathrm{End}(M)$ are given as follows. For $f, g \in \mathrm{End}(M), a \in M$, define

   $$(f+g)(a) = f(a) + g(a), \quad (f \cdot g)(a) = f(g(a)).$$

   Show that $\mathrm{End}(M)$ becomes a ring with identity, called the *endomorphism ring* of $M$.

4. Show that the set
$$\mathbb{Z}[\sqrt{-5}] = \{x + y\sqrt{-5} \mid x, y \in \mathbb{Z}\}$$
is a ring, under the usual addition and multiplication. And compute the unit group $\mathbb{Z}[\sqrt{-5}]^\times$.

5. Let $\mathbb{Z}[x]$ be the set of polynomials with integer coefficients. That is,
$$\mathbb{Z}[x] = \{a_n x^n + \cdots + a_1 x + a_0 \mid a_0, a_1, \ldots, a_n \in \mathbb{Z}\}.$$
Show that $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$.

6. Show that
$$\mathbb{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbb{C} \right\}$$
is a subring of $M_2(\mathbb{C})$.

7. If $e^2 = e$ in a ring $R$, then $e$ is called *idempotent* (幂等元). An element $x$ is called *nilpotent* (幂零元) if $x^n = 0$ for some positive integer $n$. Show that a domain contains no idempotents except 0 and 1 and that 0 is the only nilpotent in a domain.

8. Let $a$ be a nilpotent. Show that $1 - a$ is a unit.

9. Let $R$ be a ring and $a \in R$. Suppose that there exists a $b \neq 0$ such that $aba = 0$. Show that $a$ is either a left or a right zero divisor.

10. Let $R$ be a domain. Assume $ab = ac$ or $ca = cb$ for some $a \neq 0$. Show that $b = c$.

11. Let $a$ be a unit in $R$. Show that there exists a unique $x$ such that $ax = xa = 1$.

12. Show that if $1 - ab$ is a unit in a ring so is $1 - ba$.

13. Let $R$ be a commutative ring and $e_{ij} \in \mathrm{M}_n(R)$ the matrix with the $(i, j)$-th entry being 1 and the other entries being 0. Verify that for any $p \in R$ and $i \neq j$, $1 + pe_{ij}$ is invertible in $\mathrm{M}_n(R)$ with inverse $1 - pe_{ij}$.

14. Show that the set $\mathbb{Q}[\sqrt{2}] = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$ is a field.

15. Let $F$ be a number field. Describe $F[x]^\times$.

16. Describe all zero divisors and units in the residue ring $\mathbb{Z}/n\mathbb{Z}$.

17. Describe $(\mathrm{M}_n(\mathbb{Z}))^\times$.

18. Let $R$ be a commutative ring and $n \geq 2$. Show that $M_n(R)$ is a noncommutative ring with zero divisors.

19. Is it true that a subring of a division ring is a division ring?

20. Show that any finite domain is a division ring.

21. (*Hua's identity*) Let $R$ be a ring and $a, b \in R$. Suppose that $a, b$ and $ab - 1$ are units. Show that $a - b^{-1}$ and $(a - b^{-1})^{-1} - a^{-1}$ are units and
$$\left((a - b^{-1})^{-1} - a^{-1}\right)^{-1} = aba - a.$$

22. Let $\zeta$ be a complex number such that $\zeta^5 = 1$ and $\zeta \neq 1$. Set

$$\mathbb{Q}[\zeta] = \{f(\zeta) \mid f(x) \in \mathbb{Q}[x]\}.$$

Show that

(1) $\mathbb{Q}[\zeta] = \{a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3 + a_4\zeta^4 \mid a_0, a_1, \ldots, a_4 \in \mathbb{Q}\}$;

(2) $\mathbb{Q}[\zeta]$ is a subring of $\mathbb{C}$. Is $\mathbb{Q}[\zeta]$ a subfield of $\mathbb{C}$?

23. Let $n$ be a positive integer.

(1) Let $\alpha$ be a non-zero element in $\mathbb{Z}/n\mathbb{Z}$, the residue ring modulo $n$. Show that $\alpha$ is either an invertible element or zero divisor.

(2) Prove that there are $n - \varphi(n) - 1$ zero divisors in $\mathbb{Z}/n\mathbb{Z}$, where $\varphi(n)$ is the Euler's totient function.

(3) Deduce that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if $n$ is prime.

**Homework** Exercise 37, 38, 40, 41 on page 57. Exercise 1, 2, 3 on page 131.