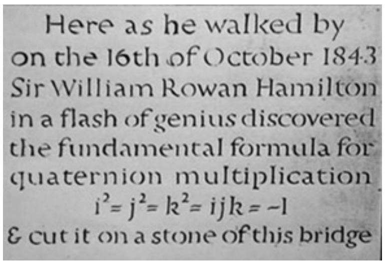
Lecture Notes On Abstract Algebra (Week 2)

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

Contents

1 Lecture 3 (Sep 12, 2023): Hamilton Quaternion and Ideals

1.1 Hamilton Quaternion —A Division Ring Which Is Not A Field



Here as he walked by
on the 16th of October 1843
Sir William Rowan Hamilton
in a flash of genius discovered
the fundamental formula for
quaternion multiplication
$i^2 = j^2 = k^2 = ijk = -1$
& cut it on a stone of this bridge

Quaternion Plaque on Broom Bridge, under which Hamilton was walking when he discovered quaternions

Hamilton, William Rowan (1805-1865) was an Irish mathematician who was born at midnight on August 3/4, 1805, so there is some confusion over his birthdate. As a child, his linguist uncle James taught him 14 languages. Hamilton taught himself mathematics at age 17, and discovered an error in Laplace's Celestial Mechanics. He predicted conical refraction in biaxial crystals, which was soon experimentally observed by Lloyd. Hamilton also extended the least action principle described earlier by Maupertuis.

Hamilton developed the mathematical theory of quaternions, which is an anticommutative algebra. Anticommutative algebra was later found to have important applications to quantum mechanics. The idea for quaternions occurred to Hamilton while he was walking with his wife from Dunsink Observatory to Dublin along the Royal Canal on 16th October, 1843 to a meeting of the Irish Academy, and was so pleased with his discovery that he scratched the fundamental formula of quaternion algebra,

$$\boxed{\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1}$$

into the stone of the Brougham bridge. The quaternions are a single example of a more general class of hypercomplex numbers discovered by Hamilton. While the quaternions are not commutative, they are associative, and they form a group known as the quaternion group.

Definition 1.1. *The* **Hamilton quaternion** (Hamilton四元数环) *is the set*

$$\mathbb{H} = \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbb{C} \right\}. \tag{1}$$

Here $\overline{z}$ denotes the complex conjugate of $z \in \mathbb{C}$.

Let $A = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in \mathbb{H}$. If $A \neq 0$, then $\alpha\beta \neq 0$ and $\det A = |\alpha|^2 + |\beta|^2 \neq 0$. Hence

$$A^{-1} = \frac{1}{\det A} \begin{pmatrix} \overline{\alpha} & -\beta \\ \overline{\beta} & \alpha \end{pmatrix} \in \mathbb{H}.$$

It's clearly that $\mathbb{H}$ is closed under addition and multiplication. So $\mathbb{H}$ is a division ring.

We may understand $\mathbb{H}$ in another way. Write $\alpha = a_0 + a_1\sqrt{-1}, \beta = a_2 + a_3\sqrt{-1}$, $a_0, a_1, a_2, a_3 \in \mathbb{R}$. Here $\sqrt{-1}$ is a fixed root to the equation $x^2 + 1 = 0$. Then an element of $\mathbb{H}$ must be of the form

$$\begin{pmatrix} a_0 + a_1\sqrt{-1} & a_2 + a_3\sqrt{-1} \\ -a_2 + a_3\sqrt{-1} & a_0 - a_1\sqrt{-1} \end{pmatrix}.$$

Set

$$\mathbf{i} = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}, \ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{k} = \begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix}, \ \mathbf{e} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{2}$$

By the definition of $\mathbb{H}$, one can see that $\mathbf{e}, \mathbf{i}, \mathbf{j}, \mathbf{k} \in \mathbb{H}$ and

$$\begin{pmatrix} a_0 + a_1\sqrt{-1} & a_2 + a_3\sqrt{-1} \\ -a_2 + a_3\sqrt{-1} & a_0 - a_1\sqrt{-1} \end{pmatrix} = a_0\mathbf{e} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}. \tag{3}$$

Notice $\mathbf{e}$ is the identity of the ring $\mathrm{M}_n(\mathbb{C})$ and one can check that

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -\mathbf{e}, \ \mathbf{ij} = -\mathbf{ji} = \mathbf{k}. \tag{4}$$

Moreover, $a_0\mathbf{e} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} = 0$ in $\mathbb{H}$ if and only if $a_0 = a_1 = a_2 = a_3 = 0$. Hence

$$\mathbb{H} = \left\{ a_0\mathbf{e} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \;\middle|\; a_0, a_1, a_2, a_3 \in \mathbb{R} \right\} \tag{5}$$

is a vector space of dimension 4 over $\mathbb{R}$.

Now we come to prove that $\mathbb{H}$ is a subring of $\mathrm{M}_2(\mathbb{C})$.

Obviously $\mathbb{H}$ is an abelian group under the usual addition of matrices.

Secondly, the unit $\mathbf{e} \in \mathbb{H}$. For $a_0\mathbf{e} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}, b_0\mathbf{e} + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k} \in \mathbb{H}$, we have

$$\begin{aligned}
&(a_0\mathbf{e} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k})(b_0\mathbf{e} + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}) \\
=&(a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3)\mathbf{e} + (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)\mathbf{i} \\
&+ (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1)\mathbf{j} + (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0)\mathbf{k}.
\end{aligned} \tag{6}$$

This shows that the multiplication is closed in $\mathbb{H}$. Hence $\mathbb{H}$ is a subring of $\mathrm{M}_2(\mathbb{C})$.

On the other hand, let $A = a_0\mathbf{e} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \mathbb{H}$. Then

$$\det A = a_0^2 + a_1^2 + a_2^2 + a_3^2. \tag{7}$$

If $A \neq 0$, then $\det A > 0$ and A is a unit in $\mathrm{M}_n(\mathbb{C})$ with

$$\begin{aligned}
A^{-1} =& \frac{1}{\det A} A^* = \frac{1}{\det A}\begin{pmatrix} a_0 - a_1\sqrt{-1} & -a_2 - a_3\sqrt{-1} \\ a_2 - a_3\sqrt{-1} & a_0 + a_1\sqrt{-1} \end{pmatrix} \\
=& \frac{a_0}{\det A}\mathbf{e} - \frac{a_1}{\det A}\mathbf{i} - \frac{a_2}{\det A}\mathbf{j} - \frac{a_3}{\det A}\mathbf{k}.
\end{aligned}$$

Consequently $A^{-1} \in \mathbb{H}$ and

$$(a_0\mathbf{e} + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k})^{-1} = \frac{a_0}{\det A}\mathbf{e} - \frac{a_1}{\det A}\mathbf{i} - \frac{a_2}{\det A}\mathbf{j} - \frac{a_3}{\det A}\mathbf{k}.$$

That is, every non-zero element in $\mathbb{H}$ is a unit. This shows that $\mathbb{H}$ is a division ring.

It's clear from (4) that $\mathbb{H}$ is not commutative. Hence $\mathbb{H}$ is not a field. In summary, we have shown that

The Hamilton quaternion $\mathbb{H}$ is a 4-dimensional vector space over $\mathbb{R}$. It is a noncommutative division ring.

Exercises

1. We know that $\mathrm{M}_2(\mathbb{C})$ is a vector space over $\mathbb{C}$ of dimension 4. Is the Hamilton quaternion $\mathbb{H}$ a subspace of $\mathrm{M}_2(\mathbb{C})$?

2. Show that the Hamilton quaternion $\mathbb{H}$ is a subspace of $\mathrm{M}_2(\mathbb{C})$ over $\mathbb{R}$.

3. Verify that the set I of $\mathbb{H}$ in which all the coordinates a_0, a_1, a_2, a_3 are either integers or all are halves of odd integers is a subring of $\mathbb{H}$. Is this a division ring? Determine $I^\times$.

4. Let m, n be non-zero integers and let R be the subset of $\mathrm{M}_n(\mathbb{C})$ consisting of the matrices of then form
$$\begin{pmatrix} a + b\sqrt{m} & c + d\sqrt{m} \\ c(c - d\sqrt{m}) & a - b\sqrt{m} \end{pmatrix}$$
where $a, b, c, d \in \mathbb{Q}$. Show that R is a subring of $\mathrm{M}_n(\mathbb{C})$ and that R is a division ring if and only if the only rational number of x, y, z, t satisfying the equation $x^2 - my^2 - nx^2 + mnt^2 = 0$ are $x = y = z = t = 0$. Give a choice of m, n that R is a division ring and a choice of m, n that R is not a division ring.

5. Determine the center of $\mathbb{H}$, the set of elements which commutate with every element of $\mathbb{H}$.

6. Let S be a division subring of $\mathbb{H}$ which is stabilized by every map $x \mapsto dxd^{-1}$, $d \neq 0$ in $\mathbb{H}$. Show that either $S = \mathbb{H}$ or S is contained in the center.

7. (*Cartan-Brauer-Hua*) Let D be a division ring, C its center and let S be a division subring of D which is stabilized by every map $x \mapsto dxd^{-1}$, $d \neq 0$ in D. Show that either $S = D$ or $S \subseteq C$.

1.2 Ideals

Since we are interested in rings with identity, $2\mathbb{Z}$ is not a subring of $\mathbb{Z}$. Actually, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for every $n \in \mathbb{Z}$.

Definition 1.2 (ideal)**.** *An* **ideal** *I (理想) of R is a subgroup of the additive group $(R, +, 0)$ such that*

$$ra, ar \in I,$$

for all $r \in R$ and $a \in I$.

If only $ra \in I$ is satisfied, then I is called a **left ideal** *(左理想). If only $ar \in I$ is satisfied, then I is called a* **right ideal** *(右理想).*

For a commutative ring, the concept of left ideal and that of right ideal coincide. In a noncommutative ring, a left or right ideal is called a *one-sided ideal* (单边理想) and an ideal is called a **two-sided ideal** (双边理想).

Example 1.1. For any integer n, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Example 1.2. In the ring $\mathrm{M}_2(\mathbb{R})$, the subset

$$I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$$

is a left ideal. But I is not a (two-sided) ideal, even $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in I$, but

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

Similarly, the subset

$$J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \;\middle|\; a, b \in \mathbb{R} \right\}$$

is a right ideal, but not a left ideal.

Example 1.3. Let I_0 be the set of those polynomials whose constant coefficient is even. Then I_0 is an ideal of $\mathbb{Z}[x]$.

Example 1.4. Let R be a commutative ring and $a, b \in R$. Then

$$I = \{au + bv \mid u, v \in R\}$$

is an ideal of R. In particular, the set $I_1 = \{au + bv \mid u, v \in \mathbb{Z}\}$ is an ideal of $\mathbb{Z}$ and $I_2 = \{2u + xv \mid u, v \in \mathbb{Z}[x]\}$ is an ideal of $\mathbb{Z}[x]$, where $\mathbb{Z}[x]$ is the ring of polynomials over $\mathbb{Z}$.

Ideals were first proposed by Richard Dedekind in 1876 in the third edition of his book *Vorlesungen über Zahlentheorie* (Lectures on Number Theory). Dedekind defined an ideal as a subset of a set of numbers, composed of algebraic integers that satisfy polynomial equations with integer coefficients. Ideals generalize Ernst Eduard Kummer's ideal numbers, devised as part of Kummer's 1843 attempt to prove Fermat's last theorem by introducing ideal numbers. The concept underwent further development in the hands of David Hilbert and, especially, of Emmy Noether.

Remark 1.1. (1) Obviously $\{0\}$ and R are ideals of R. They are called **trivial ideals** (平凡理想). And R is called the **unit ideal** (单位理想). The ring $\mathrm{M}_n(\mathbb{R})$ has no ideals other than the trivial ones.

(2) An ideal I of R in not a subgroup of the multiplicative group $(R, \cdot, 1)$. Actually I is only a multiplicative semigroup and an ideal may not contain the unit "1".

Proposition 1.1. *An ideal I is the unit ideal if and only if $1 \in I$.*

The proof is clear.

1.3 Operations on Ideals

In this part, we always assume R is a ring. The fact that I is an ideal of R is simply denoted by the notation "$\underline{I \lhd R}$".

Proposition 1.2. *Let $I, J \lhd R$. Then*

$$I \cap J \text{ and } I + J = \{i + j \mid i \in I, j \in J\}$$

are ideals of R. The ideal $I + J$ is called the **sum** *(和) of I and J. And $I \cap J$ is called the* **intersection** *(交) of I and J.*

If $I_1, I_2, \ldots, I_n$ are ideals of R, then $I_1 + I_2 + \cdots + I_n$ and $I_1 \cap I_2 \cap \cdots \cap I_n$ may be defined in an obvious way. They are simultaneously ideals of R.

Lemma 1.1. *Let S be a subset of R, then*

$$\bigcap_{\substack{I \lhd R \\ I \supseteq S}} I \lhd R.$$

It is the smallest ideal containing S and is called the **ideal generated by** *S (由S生成的理想).*

We denote the ideal generated by S by (S).

Theorem 1.1. *Let S be a subset of R (with identity). Then*

$$(S) = \{r_1 a_1 s_1 + r_2 a_2 s_2 + \cdots + r_n a_n s_n \mid a_i \in S,\ r_i, s_i \in R,\ 1 \leq i \leq n\}. \tag{8}$$

If $S = \{a_1, a_2, \ldots, a_n\}$ is a finite set, then we write $(a_1, a_2, \ldots, a_n)$ for (S).

The proof is straightforward.

Remark 1.2. 1. We can define the left (right) ideal generated by a nonempty subset in a similar way. For example, the left ideal generated by $a_1, a_2, \ldots, a_n$ can be described by

$$(a_1, a_2, \ldots, a_n)_L = \{r_1 a_1 + r_2 a_2 + \cdots + r_n a_n \mid r_1, r_2, \ldots, r_n \in R\}.$$

The right ideal generated by $a_1, a_2, \ldots, a_n$ can be described by

$$(a_1, a_2, \ldots, a_n)_R = \{a_1r_1 + a_2r_2 + \cdots + a_nr_n \mid r_1, r_2, \ldots, r_n \in R\}.$$

In particular, $(a)_L = Ra, (a)_R = aR$.

2. The ideal $(a_1, a_2, \ldots, a_n)$ generated by $a_1, a_2, \ldots, a_n$ is

$$\left\{\sum_{i_1} r_{1i_1}a_1s_{1i_1} + \sum_{i_2} r_{2i_2}a_2s_{2i_2} + \cdots + \sum_{i_n} r_{ni_n}a_ns_{ni_n} \,\middle|\, a_i \in S,\ r_{i_j}, s_{i_j} \in R\right\}. \tag{9}$$

If R is commutative, then the ideal generated by $a_1, a_2, \ldots, a_n$ may be described by

$$(a_1, a_2, \ldots, a_n) = \{r_1a_1 + r_2a_2 + \cdots + r_na_n \mid r_1, r_2, \ldots, r_n \in R\}.$$

For example, $R = (1)$ is true for any ring. And $(2, 4, 6, 8, 10, \ldots) = (2)$, $(2, 3) = (1)$ in $\mathbb{Z}$. In Example (1.4), $I_1 = (a, b)$ is the ideal of $\mathbb{Z}$ generated by a and b. And $I_2 = (2, x)$ is the ideal of $\mathbb{Z}[x]$ generated by 2 and x.

3. For ideal I and J, $I + J = (I \bigcup J)$. In other words, $I + J$ is the smallest ideal containing I and J.

If $I = (S)$ is an ideal of R, then I is said to be generated by S. If an ideal can be generated by finite elements, then it is called a **finitely generated ideal** (有限生成理想). If $I = (a)$ for some $a \in R$, then I is called a **principal ideal** (主理想). For example, the trivial ideals are always principal ideals. In $\mathbb{Z}$, $n\mathbb{Z} = (n)$ is a principal ideal of $\mathbb{Z}$. In Example (1.4), the ideal $I_2 = (2, x)$ is not principal.

Generally the complexity of a ring is measured by its units and ideals, while the complexity of an ideal is determined by its minimal number or generators to some extent. We can prove that every ideal of $F[x]$ is finitely generated, where F is a field.

A ring that every ideal is finitely generated is called a **Noetherian ring** (诺特环). A ring whose ideals are principal is called a **principal ideal ring** (主理想环). The ring $\mathbb{Z}$ and $\mathbb{R}[x]$ are principal ideal domain, hence Noetherian.

Example 1.5. Let a, b be two non-zero integers in $\mathbb{Z}$. Then $(a, b) = (d)$, where d is the greatest common divisor of a and b.

Actually this is an immediate consequence of the Euclidean algorithm in $\mathbb{Z}$.

Example 1.6. In $\mathbb{Q}[x]$, the set

$$I = \left\{f(x) \in \mathbb{Q}[x] \,\middle|\, x + 1 \mid f(x)\right\}$$

is an principal ideal. Actually $I = (x + 1)$.

Corollary 1.1. $(a_1, a_2, \ldots, a_n) = (a_1) + (a_2) + \cdots + (a_n)$.

Definition 1.3. *The* **product** (积) *of ideal I and J, denoted by IJ, is the ideal generated by all elements xy, where $x \in I, y \in J$. That is,*

$$IJ = \{a_1b_1 + a_2b_2 + \cdots + a_nb_n \mid a_1, a_2, \ldots, a_n \in I, b_1, b_2, \ldots, b_n \in J\}.$$

Example 1.7. Let $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$. We have

$$\begin{aligned}(7, 3 + \sqrt{-5})(7, 3 - \sqrt{-5}) &= \big(7 \times 7, 7(3 + \sqrt{-5}), 7(3 - \sqrt{-5}), (3 + \sqrt{-5})(3 - \sqrt{-5})\big)\\ &= \big(49, 7(3 + \sqrt{-5}), 7(3 - \sqrt{-5}), 14\big)\\ &= \big(7, 7(3 + \sqrt{-5}), 7(3 - \sqrt{-5})\big)\\ &=(7).\end{aligned}$$

Remark 1.3. Note that $\boxed{IJ \neq \{ab \mid a \in I, b \in J\}}$. Because $\{ab \mid a \in I, b \in J\}$ is not even a subgroup of $(R, +, 0)$.

Remark 1.4. One can also define the sum, product and intersection of finitely many left or right ideals.

Remark 1.5. The polynomial ring $F[x]$ is a PID (principal ideal domain) for any field F.

Properties of the ring $\mathbb{Z}$ Let $m, n \in \mathbb{Z}$ be nonzero.

1. $(m) \subseteq (n) \Longleftrightarrow n \mid m$;
2. $(m) = (n) \Longleftrightarrow m = \pm n$;
3. $(m) \cap (n) = (\mathrm{lcm}(m, n))$;
4. $(m)(n) = (mn)$;
5. $(m) + (n) = (m, n) = (\gcd(m, n))$;
6. $\mathbb{Z}$ is a principal ideal domain (PID).

Exercises

1. Show that the set $I = \{f(x) \in \mathbb{R}[x] \mid f(2023) = f(2024) = 0\}$ is an ideal of $\mathbb{R}[x]$. Describe this ideal explicitly.

2. Let F be a number field and $0 \neq f(x), g(x) \in F[X]$. Show that $(g(x)) \subseteq (f(x))$ if and only if $f(x) \mid g(x)$. When $(f(x)) = (g(x))$?

3. Let $f(x), g(x) \in F[X]$. Show that
$$(f(x)) + (g(x)) = (\gcd(f(x), g(x))),\ (f(x)) \cap (g(x)) = ([f(x), g(x)]),\ (f(x))(g(x)) = (f(x)g(x))$$
hold in the polynomial ring $F[X]$.

4. Let I be a nonzero ideal of the polynomial ring $\mathbb{Q}[x]$. Show that $I = d(x)\mathbb{Q}[x] = (d(x))$, where $d(x)$ is a polynomial in I with smallest degree. Deduce that $\mathbb{Q}[x]$ is a principal ideal domain.

5. Let I be a nonzero ideal of $\mathbb{Z}$. Show that $I = d\mathbb{Z} = (d)$, where
$$d = \min\{n \in I \mid n > 0\}.$$
Deduce that $\mathbb{Z}$ is a principal ideal domain.

6. Show that $I = \{f(x) \in \mathbb{Z}[x] \,\big|\, f(0) \equiv 0 (\mathrm{mod}\ 2)\}$ is an ideal of $\mathbb{Z}[x]$ and $I = (2, x)$.

7. Show that $(a, b)(x, y) = (ax, ay, bx, by)$ holds in a commutative ring.

8. Let $\mathbb{Z}[\sqrt{10}] = \{a + b\sqrt{10} \mid a, b \in \mathbb{Z}\}$. Show that
$$(6) = (2)(3) = \left(6, 2 + \sqrt{10}\right)\left(6, 2 - \sqrt{10}\right).$$

9. Let I, J, K be ideals of R. Show that $(IJ)K = I(JK)$.

10. Does the distributive law of ideals, $I(J+K) = IJ + IK$ hold?

11. Let R be a ring, S a subring, I an ideal in R. Show that $S + I = \{s + i \mid s \in S, i \in I\}$ is a subring of R containing I and $S \cap I$ is an ideal in S.

12. Let R be a commutative domain and $a, b \in \mathbb{R}$. Show that $(a) = (b)$ if and only if there exist $u \in R^{\times}$ such that $a = bu$.

13. Let R be a commutative ring (with identity). Show that R is a field if and only if the only ideals in R are trivial ones.

14. Let I be an ideal of R and let $\mathrm{M}_n(I)$ denote the set of $n \times n$ matrices with entries in I.

    (a) Show that $\mathrm{M}_n(I)$ is an ideal of $\mathrm{M}_n(R)$.

    (b) Show that every ideal in $\mathrm{M}_n(R)$ has the form $\mathrm{M}_n(I)$ for some ideal I of R.

    (c) Show that $I \mapsto \mathrm{M}_n(I)$ is a bijection from the set of ideals of R to the set of ideals of $\mathrm{M}_n(R)$.

    (d) Determine all ideals of $\mathrm{M}_n(\mathbb{R})$.

15. Let $\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.

    (a) Show that $\mathbb{Z}[\sqrt{-5}]$ is a commutative domain.

    (b) Show that $(3) = (3, \sqrt{-5}+1)(3, \sqrt{-5}-1)$ holds in $\mathbb{Z}[\sqrt{-5}]$. Hence the principal ideal (3) is not a prime ideal in $\mathbb{Z}[\sqrt{-5}]$.

    (c) Show that $I = (3, \sqrt{-5}+1)$ is not principal in $\mathbb{Z}[\sqrt{-5}]$.

2 Lecture 4 (Sep 14, 2023): Quotient Rings and Prime Ideals

2.1 Quotient Rings

Let I be an ideal of R. Then I is a normal subgroup of $(R, +, 0)$. Naturally we have an additive factor group

$$R/I = \{\overline{a} \mid a \in R\} = \{a + I \mid a \in R\}. \tag{10}$$

Here $\overline{a} = a + I$ is the coset of $a \in R$. Now define the addition and multiplication in R/I by

$$\begin{aligned} \overline{a} + \overline{b} =& \overline{a+b}, \text{ or equivalently } (a+I) + (b+I) = (a+b) + I, \\ \overline{a}\overline{b} =& \overline{ab}, \text{ or equivalently } (a+I)(b+I) = ab + I. \end{aligned} \tag{11}$$

Clearly the operations are well-defined. If $\overline{a} = \overline{b}$ (i.e., $a + I = b + I$), we write $a \equiv b (\mathrm{mod}\ I)$. Actually $a \equiv b (\mathrm{mod}\ I)$ if and only if $a - b \in I$. The notation " $\equiv$ " coincides with what we have seen in fundamental number theory.

$$\boxed{\begin{aligned} \overline{a} = \overline{b} &\Longleftrightarrow a - b \in I \\ &\Longleftrightarrow a \equiv b (\mathrm{mod}\ I) \end{aligned}}$$

Example 2.1. For $n \in \mathbb{Z}$, (n) is a principal ideal of $\mathbb{Z}$. If $\overline{a} = \overline{b}$, then $n \mid a - b$, which means $a \equiv b (\mathrm{mod}\ n)$. That is, a and b are in the same residue class modulo n. Conversely, if $a \equiv b (\mathrm{mod}\ n)$, then $a = b + nx$ for some $x \in \mathbb{Z}$. Hence $a + (n) = b + (n)$, i.e., a and b are in the same coset. This shows that $a \equiv b (\mathrm{mod}\ n)$ if and only if $a \equiv b (\mathrm{mod}\ I)$, where $I = (n)$.

Proposition 2.1. *Let I be an ideal of R. Then R/I is a ring under the operations in (11). We call R/I the* **quotient ring of R with respect to I** *(商环).*

Let $n \in \mathbb{Z}$. Then (n) is a principal ideal of $\mathbb{Z}$. Then $\mathbb{Z}/(n)$ is a ring, which is called the **ring of residues modulo n**. We also write $\mathbb{Z}/(n)$ for $\mathbb{Z}/n\mathbb{Z}$, since the ideal $(n) = n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$. In some literatures, $\mathbb{Z}/(n)$ is also denoted by $\mathbb{Z}_n$.

The following theorem shows the corelation between ideals of a ring and ideals of its quotient ideals.

Theorem 2.1. *Let I be an ideal of a ring R. For a subset J of R, we denote*

$$\overline{J} = \{\overline{a} \mid a \in J\}.$$

1. *If J is an ideal of R with $J \supseteq I$, then $\overline{J}$ is an ideal of R/I. Conversely every ideal of R/I must be of this form. That is, If $\mathfrak{a}$ is an ideal of R/I, then there is an ideal J of R such that $J \supseteq I$ and $\mathfrak{a} = \overline{J}$.*

2. *There is a inclusion-preserving one-to-one correspondence between the set of ideals of R containing I and the set of ideals of R/I:*

$$\{J \mid J \text{ is an ideal of } R \text{ such that } I \subseteq J\} \leftrightarrow \{\text{ideal of } R/I\}$$
$$J \mapsto \overline{J}.$$

For example, $\mathbb{Z}/(12)$ has 6 ideals:

$$\begin{aligned}
\mathfrak{a}_0 =& \{\overline{0}\} = (\overline{0}) = \overline{0\mathbb{Z}},\\
\mathfrak{a}_1 =& \{\overline{0}, \overline{2}, \overline{4}, \overline{8}, \overline{10}\} = (\overline{2}) = \overline{2\mathbb{Z}},\\
\mathfrak{a}_2 =& \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} = (\overline{3}) = \overline{3\mathbb{Z}},\\
\mathfrak{a}_3 =& \{\overline{0}, \overline{4}, \overline{8}\} = (\overline{4}) = \overline{4\mathbb{Z}},\\
\mathfrak{a}_4 =& \{\overline{0}, \overline{6}\} = (\overline{6}) = \overline{6\mathbb{Z}},\\
\mathfrak{a}_5 =& \mathbb{Z}/(12) = (\overline{1}) = \overline{\mathbb{Z}}.
\end{aligned}$$

Remark 2.1. Every ideal contained in I will be killed in R/I. In other words, if $J \subseteq I$, then $\overline{J} = \{\overline{0}\}$. For a general ideal J of R, $\overline{J} = \overline{I + J}$, where $I + J$ is an ideal containing I.

Exercises

1. Write out all ideals in $\mathbb{Z}/24\mathbb{Z}$.

2. Describe all ideals of $\mathbb{Z}[x]/(2)$.

3. Let $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$ be the decomposition of prime factors. Show that the residue ring $\mathbb{Z}/n\mathbb{Z}$ has $(e_1 + 1)(e_2 + 1) \cdots (e_t + 1)$ ideals.

4. Describe all ideals of $\mathbb{Q}[x]/(x^4 - 1)$.

5. Describe all ideals of $\mathbb{R}[x]/(x^4 + 1)$.

2.2 Prime Ideals and Maximal Ideals

Definition 2.1. *Let $\wp$ be an ideal of R and $\wp \neq R$. If $a, b \in R$ and $ab \in \wp$ always implies $a \in \wp$ or $b \in \wp$, then $\wp$ is called a* **prime ideal** (素理想).

Equivalently an ideal $\wp$ is a prime ideal if and only if $\wp \neq R$ and $x, y \notin \wp$ implies $xy \notin \wp$, i.e., $R \setminus \wp$ is closed under multiplication.

$$\boxed{\begin{aligned} (1) \neq \wp \text{ is prime} &\iff \text{“}xy \in \wp \Rightarrow x \in \wp \text{ or } y \in \wp\text{”} \\ &\iff \text{“}x, y \notin \wp \Rightarrow xy \notin \wp\text{”} \end{aligned}}$$

Definition 2.2. *An ideal I is called a* **maximal ideal** (极大理想) *if $I \neq R$ and there are no other in-between ideals. That is,*

if J is an ideal such that $I \subseteq J \subseteq R$, then either $J = I$ or $J = R$.

Example 2.2. Let p be a prime integer. Then $(p) = p\mathbb{Z}$ is a prime ideal as well as a maximal ideal of $\mathbb{Z}$.

Example 2.3. Let R be the set of all Cauchy sequences in the rational number field $\mathbb{Q}$. Then R becomes a commutative ring with the obvious operations. The null sequences (a null sequence is a Cauchy sequence that has zero as its limit) form a maximal ideal $\mathfrak{m}$. The quotient ring $R/\mathfrak{m}$ is a field. One can check that $\mathbb{Q}$ can be canonically embedded in $R/\mathfrak{m}$ and the real number field $\mathbb{R}$ is isomorphic to $R/\mathfrak{m}$.

Example 2.4. In the ring $\mathbb{Z}[x]$, the principal ideal (x) is a prime ideal, since $fg \in (x)$ implies $x \mid fg$, yielding $x \mid f(x)$ or $x \in g(x)$. But (x) is not maximal, since $(x) \subsetneq (2, x) \subsetneq \mathbb{Z}[x]$.

Theorem 2.2 (Krull, 1929)**.** *Every proper ideal of a ring with identity is contained in some maximal ideal. Consequently, every ring (with identity) has at least one maximal ideal.*

Proof. Let I be a proper ideal of R. The argument is a typical application of Zorn's Lemma. Consider the collection S of all proper ideals containing I, partially ordered by inclusion:

$$S = \{J \lhd R \mid I \subseteq J, J \neq R\}.$$

Note that S is nonempty since $I \in S$. Every chain $\{J_i \in S \mid i \in T\}$ of proper ideals containing I has an upper bound, namely the union of the chain. More precisely, let $\{J_i \mid i \in T\}$ be a chain of ideals in S (a totally ordered subset), define

$$J = \bigcup_{i \in T} J_i.$$

Clearly, $J \lhd R$ and $1 \notin J$. Hence $J \in S$ and J is maximal to every J_i. Applying Zorn's Lemma to S, there is a maximal element M of S. We contend M is a maximal ideal in R containing I. Actually, let P be an ideal of R such that $M \subseteq P \subsetneq R$. Then $I \subseteq P$ and hence $P \in S$. By the maximality of M, we have $P = M$. Thus M is a maximal ideal.

Now take $I = \{0\}$ to conclude that every ring has at least one maximal ideal. □

Remark 2.2.

1. Zorn's Lemma (Zorn 引理), also known as *Kuratowski-Zorn lemma* originally called *maximum principle* (极大原理), statement in the language of set theory, equivalent to the *axiom of choice* (选择公理), that is often used to prove the existence of a mathematical object when it cannot be explicitly produced. Zorn's Lemma says: if S is any nonempty partially ordered set in which every chain has an upper bound, then S has a maximal element.

2. Renteln and Dundes (2005) give the following (bad) mathematical jokes about Zorn's lemma:

   Q: What's sour, yellow, and equivalent to the axiom of choice? A: Zorn's lemon.

   Q: What is brown, furry, runs to the sea, and is equivalent to the axiom of choice? A: Zorn's lemming (旅鼠).

   (Renteln, P. and Dundes, A. *Foolproof: A Sampling of Mathematical Folk Humor.* Notices Amer. Math. Soc. 52, 24-34, 2005)

3. Krull's theorem can fail if we do not emphasis a ring endowed with identity.

   For example, let $R = \mathbb{Q}$. The addition in $\mathbb{Q}$ is as usual, but the multiplication is trivial: $x \cdot y = 0$ for all $x, y \in \mathbb{Q}$. It's clear that $\mathbb{Q}$ becomes a ring with no identity and an ideal of $\mathbb{Q}$ is essentially an additive subgroup. Since $\mathbb{Q}$ is a divisible additive group (an additive group G is said to be divisible if for any $a \in G$ and any positive integer n, there is an element $x \in G$ such that $nx = a$.), it has no maximal subgroups (actually, any divisible abelian group has no maximal subgroups). Consequently, R has no maximal ideals. For more examples, search

   http://sierra.nmsu.edu/morandi/notes/NoMaxIdeals.pdf

4. In a commutative ring with identity, every maximal ideal is a prime ideal. The converse is not always true: for example, in any integral domain which is not a field the zero ideal is a prime ideal which is not maximal.

Proposition 2.2. *Let R be a commutative ring and I an ideal with $I \neq (1)$. Then the quotient ring R/I is also commutative. And*

1. *I is a prime ideal if and only if R/I is a domain;*

2. *I is a maximal ideal if and only if R/I is a field.*

Proof. It's clear that R/I is a commutative ring. Assume I is prime and $\overline{a}\overline{b} = \overline{0}$ holds in R/I. We have $\overline{ab} = \overline{0}$, i.e., $ab \in I$. Then either $a \in I$ or $b \in I$ by the primality of I. So $\overline{a} = \overline{0}$ or $\overline{b} = \overline{0}$ in R/I. This shows that R/I is a domain. Conversely, Assume R/I is a domain and $xy \in I$. Then $\overline{xy} = \overline{x}\,\overline{y} = \overline{0}$. So $\overline{x} = \overline{0}$ or $\overline{y} = \overline{0}$. That is, $x \in I$ or $y \in I$. It follows that I is a prime.

Now assume I is a maximal ideal of R and $0 \neq \overline{x} \in R/I$. Then $x \notin I$ and $(x, I) = R$. In particular, $1 \in (x, I)$ and there exist $a \in R, b \in I$ such that $ax + b = 1$. Thus $\overline{ax + b} = \overline{1}$, yielding $\overline{a}\,\overline{x} = \overline{1}$. Therefore $\overline{x}$ is invertible in R/I and so R/I is a field. Conversely we assume R/I is a field and J is a ideal such that $I \subsetneq J \subseteq R$. Then there exists $y \in J \backslash I$. Thus $\overline{y} \neq 0$ in R/I and $\overline{y}$ is invertible. This implies that there exist $z \in R$ such that $\overline{y}\,\overline{z} = \overline{1}$ in R/I. So $yz - 1 = a \in I$. Note that $y \in J$. So $1 = yz - a \in J$. Therefore $J = R$. This proves that I is maximal. □

Corollary 2.1. 1. *A commutative ring is a domain if and only the zero ideal is a prime.*

2. *A maximal ideal in a commutative ring is always a prime ideal.*

Remark 2.3. A maximal ideal of a commutative ring without identity may not be prime. See the following Exercise 5.

Let R be commutative and $(1) \neq I \lhd R$.

- I is a prime ideal $\Longleftrightarrow$ R/I is a domain.
- I is a maximal ideal $\Longleftrightarrow$ R/I is a field.

Recall a principal ideal domain (PID) is an integral domain in which every ideal is principal. The integer ring $\mathbb{Z}$ is a PID. Let $n > 0$, it's easy to see (n) is a prime ideal of $\mathbb{Z}$ if and only if n is a prime number. If p is prime, then the ideal (p) is maximal and consequently $\mathbb{Z}/(p) = \mathbb{Z}/p\mathbb{Z}$ is a field, which is called a **finite field** (有限域) with p elements. Such a finite field is also denoted by $\mathbb{F}_p$ or $\mathbb{Z}/p\mathbb{Z}$. A finite field is also called a *Galois field*.

Exercises

1. Let I be an ideal of R and $U = R^\times$ the group of units of R. Let

$$U_1 = \{a \in U \mid a \equiv 1 (\text{mod } I)\}.$$

Show that U_1 is a normal subgroup of U.

2. Let I be an ideal of R. If there exist two ideals J and K such that $I \subsetneq J, I \subsetneq K$ and $I = JK$, then I is not a prime.

3. Let c be a number in the closed interval $[a, b]$ and let $\mathfrak{m}$ be the set of real functions $f(x) \in C[a, b]$ such that $f(c) = 0$. Show that $\mathfrak{m}$ is a maximal ideal of $C[a, b]$.

4. Let I be an ideal of R. If J is a prime ideal containing I, then $\overline{J} = \{\overline{a} = a + I \mid a \in J\}$ is a prime ideal of R/I. Is the converse true?

5. Show that $M = 4\mathbb{Z}$ is a maximal ideal in $2\mathbb{Z}$ (without identity), but M is not a prime.

6. Let $R = 2\mathbb{Z}/4\mathbb{Z} = \{0, \alpha\}$ be a ring with two elements, where α is the image of 2 under the natural map $2\mathbb{Z} \to 2\mathbb{Z}/4\mathbb{Z}$. Clearly $\alpha + \alpha = \alpha \cdot \alpha = 0$. Show that the zero ideal (0) is maximal, but not prime.

7. Show that $\mathbb{Z}/(n)$ contains nonzero nilpotents (i.e. $x^k = 0$ for some $k \geq 0$) if and only if n is not square-free (i.e., n is divisible by the square of a prime).

8. Show that every nonzero prime ideal of a principal ideal domain is maximal.

9. Note that $\mathbb{F}_p$ denotes the finite field with p elements, where p is a prime integer.

   (a) Prove that $a^p = a$ for every $a \in \mathbb{F}_p$. In other words, the polynomial $x^p - x$ has p roots in $\mathbb{F}_p$.

   (b) Compute $|\mathrm{GL}_2(\mathbb{F}_p)|$. Can you generalize this result to $|\mathrm{GL}_n(\mathbb{F}_p)|$ for $n > 0$.

10. Do you think there is a finite field with 6 elements? More generally, if $\mathbb{F}_n$ is a finite field with n elements, what's the possible value for n?

11. An additive group G is said to be divisible if for any $a \in G$ and any positive integer n, there is an element $x \in G$ such that $nx = a$.

    (a) Let H be a maximal subgroup of a divisible additive group G. Then the quotient group G/H is of prime order.

    (b) Show that a divisible abelian group has no maximal subgroups.

12. Let F be a field of characteristic 0 (i.e., for $x \in F^*$ and $n \in \mathbb{Z}$, $nx = 0$ if and only if $n = 0$). Then $(F, +, 0)$ has no maximal subgroups.

2.3 Quiz 1

1. (10分) 刻画剩余类环 $\mathbb{Z}/n\mathbb{Z}$ 的零因子和单位群 $(\mathbb{Z}/n\mathbb{Z})^{\times}$.

2. (10分) 用群论观点证明 Wilson 定理:

$$\text{若 } p \text{ 为素数, 则 } (p-1)! \equiv -1 (\bmod p).$$

Homework Exercise 34, 36, 39 on page 57. Exercise 21, 23, 30, 40, 53 on page 133-135.