1. Ideals and Quotient Rings

1.1. Ideals

Let $(A, +, \cdot)$ be a ring (not necessarily with unity). Recall that S a subring of A if $(S, +)$ is a subgroup of $(A, +)$ and $S \cdot S \subseteq S$, i.e., S is closed under multiplication. In other words, S is a subring of A if S is a subset of A that together with the operations of A is itself a ring. Notice that, if A is a ring with unity, we do not require subrings of A to contain the unity 1_A.

The beginning student may think that a subring plays the same importance of the analogue concept of subgroup in group theory. This is not the case. To define the important notion of quotient ring, for example, subrings are not suitable. Instead, we need a more appropriate notion: that of *ideal*. We will focus on studying ideals and their properties.

Definition 1.1. An **ideal** of a ring A is a subset $I \subseteq A$ such that

(i) $(I, +) \leq (A, +)$,

(ii) $aI \subseteq I$ and $Ia \subseteq I$ for every $a \in A$.

The condition $aI \subseteq I$ means that if $a \in A$ and $b \in I$, then $ab \in I$. Recall that $aI = \{ab \mid b \in I\}$ and $Ia = \{ba \mid b \in I\}$. This automatically implies that I is closed under multiplication, as the reader should check. Thus, any ideal is a subring. Sometimes, the notation $I \trianglelefteq A$ is used to indicate that I is an ideal of A. An ideal I is called **proper** if $I \neq A$.

If $J \subseteq A$ verifies

$$aJ \subseteq J \quad \text{for every } a \in A$$

we say J absorbs products from the left. We say J absorbs products from the right with the obvious modification. Therefore, an ideal is an additive subgroup that absorbs products from left and from the right.

Remark 1.1.1. A **left ideal** of a ring A is an additive subgroup of $(A, +)$ that absorbs products from the left. Similarly, a **right ideal** is an additive subgroup of $(A, +)$ that absorbs products from the right. Thus, a **two sided ideal**, or ideal for short, is an additive subgroup that is both a left and right ideal. If A is commutative, all these notions are the same.

Example 1. (i) For any ring A, both $\{0\}$ and A are ideals of A. We call $\{0\}$ the trivial ideal of A, and it is usually denoted 0.

(ii) $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$ for every $n \in \mathbb{Z}$.

(iii) Given integers $0 \leq n < m$, the set $n\mathbb{Z}_m$ is an ideal of $\mathbb{Z}_m$.

(iv) The set

$$I = \left\{ \begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix} : a, c \in A \right\}$$

is a left-ideal but not a right-ideal of the ring of 2×2 matrices with entries in a ring A.

(v) Let R be a commutative ring with unity and let $a \in R$. The set

$$\langle a \rangle = \{ra \mid r \in R\}$$

is an ideal of R called the principal ideal generated by a.

(vi) Let $\mathbb{R}[x]$ denote the set of all polynomials with real coefficients and let A denote the subset of all polynomials with constant term 0 . Then A is an ideal of $\mathbb{R}[x]$. In fact, $A = \langle x \rangle$.

(vii) Let T be the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$. Let I be the subset consisting of those functions g such that $g(2) = 0$. Then I is a subring of T. Furthermore, if $f \in T$ and $g \in I$, then

$$(fg)(2) = f(2)g(2) = f(2) \cdot 0 = 0$$

Therefore, $fg \in I$. Similarly, $gf \in I$, so that I is an ideal in T.

(viii) Let R be the ring of all real-valued functions of a real variable. The subset of all differentiable functions is a subring of R but not an ideal of R.

Exercise 1. Show the following are equivalent for a subset $J \subseteq \mathbb{Z}$:

(i) J is a subgroup of $\mathbb{Z}$

(ii) J is an ideal of $\mathbb{Z}$

(iii) $J = n\mathbb{Z}$ for some $n \in \mathbb{Z}$

Exercise 2. Let A be a commutative ring with unity and $a \in A$. Prove $\langle a \rangle = A$ if and only if a has an inverse.

1.1.1. Operations with ideals

Definition 1.2. Let I and J be two ideals of a ring A.

(i) The sum of I and J is

$$I + J := \{a + b \mid a \in I, b \in J\}$$

(ii) The product of I and J is

$$IJ := \left\{a_1 b_1 + \cdots + a_n b_n \mid n \in \mathbb{Z}^+, a_i \in I, b_i \in J\right\}$$

Proposition 1.3. *Let $I, J, K \trianglelefteq A$ and $(I_\lambda)_{\lambda \in \Lambda}$ a family of ideals of A.*

(i) Both $I + J$ and IJ are ideals of A.

(ii) $(IJ)K = I(JK)$.

(iii) $I(J+K) = IJ + IK$.

(iv) $(I+J)K = IK + JK$.

(v) $\bigcap_{\lambda\in\Lambda} I_\lambda$ *is an ideal of* A

Proof. Exercise. □

Given a subset X of a ring A, we can build the smallest ideal of A that contains X, denoted $\langle X\rangle$, by intersecting all ideals I of A such that $X \subseteq I$. In other words,

$$\langle X\rangle = \bigcap_{\substack{I\lhd A\\ X\subseteq I}} I$$

This ideal is called the **ideal generated** by X. The elements of X are called generators of the ideal (X). We simply write $\langle b_1 \ldots, b_n\rangle$ instead of $\langle\{b_1, \ldots, b_n\}\rangle$.

Exercise 3. Let I and J be ideals of a ring A. Show that

(i) $I + J = \langle I \cup J\rangle$

(ii) $IJ = \langle ab \mid a \in I, b \in J\rangle$.

(iii) $I = \langle I\rangle$

Remark 1.3.1. We can extend Definition 1.2 by defining the sum and product of more than two ideals. For instance, $I_1 I_2 \cdots I_n = \langle a_1 a_2 \cdots a_n \mid a_i \in I_i \text{ for all } i \in [n]\rangle$. In particular, the power of an ideal I^n is the product of I with itself n times, and by definition is the ideal generated by products $a_1 \cdots a_n$ with $a_i \in I$ for all $i \in [n]$. Be careful: I^n is not the same as $\langle a^n \mid a \in I\rangle$.

An ideal generated by a finite set is called a **finitely generated ideal**. An ideal generated by a single element is called a **principal ideal**. In particular, if A is commutative and $X = \{x\}$, then $\langle X\rangle$ equals

$$\langle x\rangle = \{ax \mid a \in A\}.$$

We also employ the notation xA for $\langle x\rangle$. If A is not commutative, $\{ras \mid r, s \in R\}$ is not necessarily the two-sided ideal generated by a since it need not be closed under addition. Sometimes, parenthesis $(\cdot)$ are used instead of the angular brackets $\langle\cdot\rangle$. So, for example, you may see (x) instead of $\langle x\rangle$. We prefer the latter notation.

Proposition 1.4. *Let X be a subset of a ring A. Define*

$$RXR = \left\{r_1 x_1 r_1' + \cdots + r_n x_n r_n' \mid r_i, r_i' \in R, x_i \in X, n \in \mathbb{Z}^+\right\}$$

Then RXR is an ideal of A and $\langle X\rangle = RXR$.

Proof. We can assume that $X \neq \emptyset$. If $X = \emptyset$, then $\langle X\rangle = 0 = RXR$. Let us first show that AXA is an ideal of A. It is clear that $AXA \neq \emptyset$. Let

$$\sum_{i=1}^{m} a_i x_i b_i, \quad \sum_{j=1}^{n} c_j y_j d_j \in AXA$$

Then

$$\sum_{i=1}^{m} a_i x_i b_i - \sum_{j=1}^{n} c_j y_j d_j = \sum_{i=1}^{m} a_i x_i b_i + \sum_{j=1}^{n} c_j(-y_j) d_j \in AXA$$

which shows that AXA is a subgroup of A. On the other hand, let

$$\sum_{i=1}^{m} a_i x_i b_i \in AXA$$

and $c \in A$. We find

$$c\left(\sum_{i=1}^{m} a_i x_i b_i\right) = \sum_{i=1}^{m} (ca_i) x_i b_i \in AXA$$

and

$$\left(\sum_{i=1}^{m} a_i x_i b_i\right) c = \sum_{i=1}^{m} a_i x_i (b_i c) \in AXA$$

Thus, AXA is an ideal of A. We now show $\langle X \rangle = RXR$. As it is clear that every $x \in X$ can be written as $x = 1 \cdot x \cdot 1$, we have $X \subseteq AXA$. Thus $\langle X \rangle \subseteq RXR$ because $\langle X \rangle$ is the smallest ideal that contains X. On the other hand, let J be an ideal of A containing X. Since J is closed under multiplication, $axb \in J$ for all $x \in X$ and $a, b \in A$. Thus

$$\text{if } \sum_{i=1}^{m} a_i x_i b_i \in AXA, \text{ then } \sum_{i=1}^{m} a_i x_i b_i \in J.$$

Consequently, $AXA \subseteq J$. This shows that $\langle X \rangle = AXA$. □

Remark 1.4.1. If A is noncommutative, the ideal generated by $a \in A$ is the ideal AaA, which consists of all finite sums of elements of the form ras where $r, s \in R$.

Proposition 1.5. *Let A be a commutative ring with unity $1 \neq 0$. Then A is a field if and only if the only ideals of A are A and 0.*

Proof. ($\Rightarrow$) Let $I \neq 0$ be an ideal of A, and let $a \in I$ such that $a \neq 0$. Since A is a field, a is invertible. Then $I = A$.

($\Leftarrow$) Suppose A has no non-trivial proper ideals, and let $a \neq 0$ be an element of A. We seek $x \in A$ such that $ax = 1$. Clearly $\langle a \rangle \neq 0$. Then, necessarily we get $\langle a \rangle = A$. It follows that $1 \in \langle a \rangle$, meaning there exists $x \in A$ such that $1 = ax = xa$.

□

Exercise 4. Use Bézout's identity to show $a\mathbb{Z} + b\mathbb{Z} = \mathbb{Z}$ for $a, b \in \mathbb{Z}$ coprime.

1.2. Quotient Rings

Let A be a ring. Since every ideal $I \trianglelefteq A$ is an abelian subgroup of A (and thus a normal subgroup), the quotient A/I is also an abelian group. Recall this set consist of the cosets

$a + I = \{a + b \mid b \in I\}$ with $a \in A$. Our next objective is to endow A/I with a multiplication so that it becomes a ring. We define

$$(a + I)(b + I) = ab + I$$

for $a, b \in A$. The fact that I is an ideal and not only a subring help us to show this operation is well defined, i.e., that if $a + I = a' + I$ and $b + I = b' + I$, then $ab + I = a'b' + I$. This verification is left to the reader.

Proposition 1.6. *Let I be an ideal of a ring A. The set A/I is a ring with the operations given by*

$$(a + I) + (b + I) = (a + b) + I \quad \text{and} \quad (a + I)(b + I) = ab + I$$

where $a, b \in A$. Moreover, if A is commutative, then so is A/I.

Proof. Exercise. □

The set A/I, endowed with the two operations of addition $+$ and multiplication $\cdot$, is called the **quotient ring** of A by the ideal I. The map $\pi\colon A \to A/I$ defined by $a \mapsto a + I$ is called the canonical projection of A onto A/I. Note π is surjective.

Example 2. (i) Let $A = \mathbb{Z}$ and $I = 4\mathbb{Z}$. The elements of the quotient ring $A/I = \mathbb{Z}/4\mathbb{Z}$ are the classes modulo the ideal $I = 4\mathbb{Z}$, that is

$$\begin{aligned}
\overline{0} &= 0 + 4\mathbb{Z} = \{4k \mid k \in \mathbb{Z}\},\\
\overline{1} &= 1 + 4\mathbb{Z} = \{4k + 1 \mid k \in \mathbb{Z}\},\\
\overline{2} &= 2 + 4\mathbb{Z} = \{4k + 2 \mid k \in \mathbb{Z}\}, \quad \text{and}\\
\overline{3} &= 3 + 4\mathbb{Z} = \{4k + 3 \mid k \in \mathbb{Z}\}.
\end{aligned}$$

(ii) Let A and B be two rings. We have

$$I = \{(a, 0) \mid a \in A\}$$

is an ideal of the product ring $A \times B$. The elements of the quotient ring $(A \times B)/I$ are the classes

$$(a, b) + I = (0, b) + I$$

where $a \in A, b \in B$. Indeed, $(a, b) - (0, b) = (a, 0) \in I$. The addition and multiplication rules are given by

$$\begin{aligned}
[(0, b) + I] + [(0, b') + I] &= (0, b + b') + I \quad \text{and}\\
[(0, b) + I] \cdot [(0, b') + I] &= (0, bb') + I.
\end{aligned}$$

(iii) Let $R = \mathbb{Z}[x]$ be the ring of polynomials in x with integer coefficients. Let I be the collection of polynomials whose terms are of degree at least 2 (i.e., having no terms of degree 0 or degree 1) together with the zero polynomial. Then I is an ideal: the sum of two such polynomials again has terms of degree at least 2 and the product of a polynomial

whose terms are of degree at least 2 with any polynomial again only has terms of degree at least 2. Two polynomials $p(x), q(x)$ are in the same coset of I if and only if they differ by a polynomial whose terms are of degree at least 2, i.e., if and only if $p(x)$ and $q(x)$ have the same constant and first degree terms. For example, the polynomials $3+5x+x^3+x^5$ and $3+5x-x^4$ are in the same coset of I. It follows easily that a complete set of representatives for the quotient R/I is given by the polynomials $a+bx$ of degree at most 1.

Addition and multiplication in the quotient are again performed by representatives. For example,

$$(\overline{1+3x})+(\overline{-4+5x})=\overline{-3+8x}$$

and

$$(\overline{1+3x})(\overline{-4+5x})=\overline{(-4-7x+15x^2)}=\overline{-4-7x}.$$

Note that in this quotient ring R/I we have $\bar{x}\bar{x}=\overline{x^2}=\bar{0}$, for example, so that R/I has zero divisors, even though $R=\mathbb{Z}[x]$ does not.

(iv) Let $A=\mathbb{Z}[x]$ and $I=\langle x\rangle$, the ideal generated by x. Note a polynomial belongs to I if and only if its constant term is zero. The elements of $A/I=\mathbb{Z}[x]/\langle x\rangle$ are the classes

$$f(x)+\langle x\rangle=\{f(x)+xp(x)\mid p(x)\in\mathbb{Z}[x]\}$$

where $f\in\mathbb{Z}[x]$. Suppose

$$f(x)=a_0+a_1x+\cdots+a_dx^d$$

Then $f(x)+\langle x\rangle=a_0+\langle x\rangle$ since

$$f(x)-a_0=a_1x+\cdots+a_dx^d=x\left(a_1+\cdots+a_dx^{d-1}\right)\in\langle x\rangle$$

It follows that every polynomial belongs to the class of its constant term. Consequently, the elements of $\mathbb{Z}[x]/\langle x\rangle$ are the classes:

$$a+\langle x\rangle=\{a+xp(x)\mid p(x)\in\mathbb{Z}[x]\}$$

where $a\in\mathbb{Z}$. For $a,b\in\mathbb{Z}$, the rules of addition and multiplication are

$$\begin{aligned}(a+\langle x\rangle)+(b+\langle x\rangle)&=(a+b)+\langle x\rangle\quad\text{and}\\(a+\langle x\rangle)\cdot(b+\langle x\rangle)&=ab+\langle x\rangle.\end{aligned}$$

(v) Consider the ring A and its ideal I defined by

$$A=\left\{\begin{bmatrix}a&0\\b&c\end{bmatrix}\;\middle|\;a,b,c\in\mathbb{Z}\right\},\quad I=\left\{\begin{bmatrix}0&0\\x&0\end{bmatrix}\;\middle|\;x\in\mathbb{Z}\right\}.$$

The elements of the quotient A/I are the classes of the form

$$\begin{bmatrix}a&0\\b&c\end{bmatrix}+I=\begin{bmatrix}a&0\\0&c\end{bmatrix}+I$$

where $a, b, c \in \mathbb{Z}$. Indeed,

$$\begin{bmatrix} a & 0 \\ b & c \end{bmatrix} - \begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ b & 0 \end{bmatrix} \in I.$$

The rules of addition and multiplication are given by

$$\left(\begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix} + I\right) + \left(\begin{bmatrix} a' & 0 \\ 0 & c' \end{bmatrix} + I\right) = \begin{bmatrix} a+a' & 0 \\ 0 & c+c' \end{bmatrix} + I, \quad \text{and}$$
$$\left(\begin{bmatrix} a & 0 \\ 0 & c \end{bmatrix} + I\right) \cdot \left(\begin{bmatrix} a' & 0 \\ 0 & c' \end{bmatrix} + I\right) = \begin{bmatrix} aa' & 0 \\ 0 & cc' \end{bmatrix} + I.$$

Exercise 5. (i) Let A be a ring, and I and J two ideals of A such that $J \supseteq I$. Show that J/I is an ideal of A/I, where $J/I = \{x + I \mid x \in J\}$.

(ii) Let A be a ring, I the ideal generated by elements of the form $ab - ba$, where $a, b \in A$, and J an arbitrary ideal of A. Show that A/J is commutative if and only if $I \subseteq J$.

(iii) Let A be a commutative ring. Knowing that the set N of all nilpotent elements of A is an ideal of A, show that the quotient A/N has no non-zero nilpotent elements.

(iv) Let A be a commutative ring, and I an ideal of A. Show that every element of A/I is invertible or a zero divisor if and only if, for every $a \notin I$, there exists $x \notin I$ such that $1 - ax \in I$ or $ax \in I$, respectively.

(v) A ring is said to be *anticommutative* if $xy = -yx$ for all x, y in the ring. Show that if A is a ring and I is an ideal of A, then A/I is anticommutative if and only if $ab + ba \in I$ for all $a, b \in A$.

1.3. Types of Ideals

Apart from being the right notion to define quotients, ideals are important because they appear as kernels of ring homomorphisms, which we will address in the next lecture. The first two types of ideals in the following definition are the most important.

Definition 1.7. An ideal I of a commutative ring A is

(i) **maximal** if I is proper and there is no other ideal $J \trianglelefteq A$ such that $I \subsetneq J \subsetneq A$. In other words, I is a proper ideal not contained in any other proper ideal. Equivalently, if $I \subseteq J \subseteq A$, then either $I = J$ or $J = A$.

(ii) **prime** if I is proper and

$$ab \in I \implies a \in I \text{ or } b \in I$$

for every $a, b \in A$.

(iii) **radical** if for any $a \in A$, $a^n \in I$ for some $n \geq 1$ implies $a \in I$. Equivalently, the nilradical of the quotient ring A/I is zero.

(iv) **primary** if for all $a, b \in A$, $ab \in I$ implies $a \in I$ or $b^n \in I$ for some $n \geq 1$. Every prime ideal is primary, but not all primary ideals are prime.

(v) **irreducible** if I cannot be expressed as an intersection of two proper ideals of A that properly contain I.

(vi) **nilpotent** if there exists some $n \geq 1$ such that $I^n = \{0\}$, meaning every element of I raised to the n-th power equals zero.

(vii) **principal** if it is generated by a single element.

We will see that every maximal ideal is prime. A ring is local if it contains exactly one maximal ideal.

Example 3. (i) Let n be a nonnegative integer. The ideal $n\mathbb{Z}$ of $\mathbb{Z}$ is a maximal ideal if and only if $\mathbb{Z}/n\mathbb{Z}$ is a field.

(ii) In fact, the principal ideals generated by primes in $\mathbb{Z}$ are both prime and maximal ideals. The zero ideal in $\mathbb{Z}$ is prime but not maximal.

(iii) If p is a prime number, $\langle p \rangle \subseteq \mathbb{Z}[x]$ is a prime ideal that is not maximal.

(iv) $\langle x^2 \rangle \subseteq k[x]$ is not radical. Here k is a field.

(v) The ideal $\langle x \rangle$ in $\mathbb{Z}[x]$ is not a maximal ideal because $\langle x \rangle \subseteq \langle 2, x \rangle \subseteq \mathbb{Z}[x]$ is a chain of proper containments.

Proposition 1.8. *In a ring with identity, every proper ideal is contained in a maximal ideal.*

Proof. Let R be a ring with identity and let I be a proper ideal (so R cannot be the zero ring, i.e., $1 \neq 0$). Let S be the set of all proper ideals of R which contain I. Then S is nonempty ($I \in S$) and is partially ordered by inclusion. If C is a chain in S, define

$$J = \bigcup_{A \in C} A.$$

We first show that J is an ideal. Certainly J is nonempty because C is nonempty — specifically, $0 \in J$ since 0 is in every ideal A. If $a, b \in J$, then there are ideals $A, B \in C$ such that $a \in A$ and $b \in B$. By definition of a chain, either $A \subseteq B$ or $B \subseteq A$. In either case $a - b \in J$, so J is closed under subtraction. Since each $A \in C$ is closed under left and right multiplication by elements of R, so is J. This proves J is an ideal.

If J is not a proper ideal, then $1 \in J$. In this case, by definition of J we must have $1 \in A$ for some $A \in C$. This is a contradiction because each A is a proper ideal ($A \in C \subseteq S$). This proves that each chain has an upper bound in S. By Zorn's Lemma, S has a maximal element which is therefore a maximal (proper) ideal containing I. □