Math 210B Notes

Spring, 2026

Contents

1 Introduction to Rings **3**

1.1 Ring and Field Definitions . . . 3

1.2 Zero Divisors and Integral Domains . . . 7

1.3 Polynomials and Ring Homomorphisms . . . 9

1.4 Quotient Rings and the Isomorphism Theorems . . . 12

1.5 Generated Ideals . . . 15

1.6 Maximal Ideals . . . 17

1.7 Rings of Fractions . . . 19

Chapter 1

Introduction to Rings

1.1 Ring and Field Definitions

We move on from studying groups to studying rings and fields. First, lets compare some analogues between groups and rings.

Groups:

(i) 1 operation
(ii) Subgroups
(iii) Normal groups N
(iv) Quotient groups G/N
(v) Morphisms of groups

Rings:

(i) 2 operations
(ii) Subrings
(iii) Ideals I
(iv) Quotient rings R/I
(v) Morphisms of rings

We build the theory of rings and fields in a similar way to the theory of groups. An important type of ring we wish to study is the ring of polynomials with coefficients in a field. Our goal is to be able to study Galois Theory and make a connection between automorphisms of fields and their subfields.

Before we get started, consider the following example.

Example 1.1.1. Let R be a set with operations $+$ and $\times$ such that distribution holds for all elements in the set:

$$\begin{aligned} \forall a, b, c \in R \quad a \times (b + c) &= (a \times b) + (a \times c) \\ (a + b) \times c &= (a \times c) + (b \times c) \end{aligned}$$

Further assume $+$ and $\times$ are associative and that there exists $1 \in R$ such that $1 \times a = a \times 1 = a$ for all $a \in R$. Let $-a$ and $-b$ be the additive inverses of $a, b \in R$. Show that

$$a + b = b + a$$

Proof.

$$\begin{aligned} (a + b) \times (1 + 1) &= (a + b) \times 1 + (a + b) \times 1 \\ &= a \times 1 + b \times 1 + a \times 1 + b \times 1 \\ &= a + b + a + b \qquad \text{(I)} \end{aligned}$$

$$\begin{aligned} (a + b) \times (1 + 1) &= a \times (1 + 1) + b \times (1 + 1) \\ &= a \times 1 + a \times 1 + b \times 1 + b \times 1 \\ &= a + a + b + b \qquad \text{(II)} \end{aligned}$$

From (I) and (II), we have

$$\begin{aligned} a+b+a+b &= a+a+b+b \\ \implies a+b+a+b-b &= a+a+b+b-b \\ \implies -a+a+b+a+0 &= -a+a+a+b+0 \\ \implies 0+b+a &= 0+a+b \\ \implies b+a &= a+b \end{aligned}$$

□

This example motivates the following definition.

Definition 1.1.1. (Ring)
A ring is a set R together with two binary operations $+$ (called addition) and $\times$ (called multiplication) satisfying the following:

(i) $(R,+)$ is an abelian group

(ii) Multiplication is associative $\forall a,b,c \in R$

$$(a \times b) \times c = a \times (b \times c)$$

(iii) Distributive laws hold $\forall a,b,c \in R$

$$\begin{aligned} \text{Left distribution: } a \times (b \times c) &= (a \times b) + (a \times c) \\ \text{Right distribution: } (a+b) \times c &= (a \times c) + (b \times c) \end{aligned}$$

If multiplication is commutative, we call R a commutative ring. The ring R is said to have an identity denoted 1 (or contains a unity element) if

$$1 \times a = a \times 1 = a \quad \forall a \in R$$

In this case, R is called a ring with unity.

Notation . $a \times b$ will be written as ab. The additive identity of $(R,+)$ will be denoted 0. The additive inverse of an element $a \in R$ will be denoted $-a$.

Notice that our definition for a ring does not require the existence of a multiplicative inverse for each element in the ring. The addition of multiplicative inverses leads to more specific types of rings, and with the addition of multiplicative commutativity, we get fields.

Definition 1.1.2. (Division Ring, Field)
A ring R with unity 1 (where $1 \neq 0$) is called a division ring if every $a \in R$ where $a \neq 0$ has an element $b \in R$ such that $ab = ba = 1$. That is, if all nonzero elements have a multiplicative inverse. If R is also commutative, then R is called a field.

Example 1.1.2. (i) Trivial rings: Given any group $(G,*)$ if we take $*$ as addition and define multiplication as $ab = 0 \quad \forall a,b \in G$, then this forms a ring.

(ii) If $R = \{0\}$, this is called the zero ring with multiplication and addition defined as $0 \cdot 0 = 0$ and $0+0=0$. Note that this is the only ring where $1=0$. Show that if $1=0$, then $R=\{0\}$.

Proof. Let $a \in R$.

$$\begin{aligned} a \cdot 0 = a(0+0) &= a \cdot 0 + a \cdot 0 \\ \implies a \cdot 0 &= a \cdot 0 + a \cdot 0 \\ \implies 0 &= a \cdot 0 = a \cdot 1 = a \end{aligned}$$

□

Many theorems will state $1 \neq 0$ instead of $R \neq 0$.

(iii) $\mathbb{Z}$ with the usual multiplication and addition. Note that in $\mathbb{Z}/\{0\}$ we do not have a group with respect to multiplication.

(iv) $\mathbb{Q}$ is a ring with the usual operations and $\mathbb{Q}/\{0\}$ is a group with respect to multiplication, that is $\mathbb{Q}$ is a field (multiplication in $\mathbb{Q}$ is commutative). $\mathbb{C}$ and $\mathbb{R}$ are fields as well.

(v) $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with unity $\bar{1}$ ($\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, ..., n \bar{-} 1\}$) where the multiplication is defined $\bar{a} \cdot \bar{b} = \bar{ab}$.

(vi) The quaternians: recall the imaginary units $i^2 = j^2 = k^2 = ijk = -1$. Looking at the set $\mathbb{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ where addition is defined by

$$(a + bi + cj + dk) + (a' + b'i + c'j + d'k) = (a + a') + (b + b')i + (c + c')j + (d + d')k$$

and multiplication is defined by distribution

$$\begin{aligned}&(a + bi + cj + dk)(a' + b'i + c'j + d'k)\\ =&aa' - bb' - cc' - dd' + (ab' + ba' + cd' - dc')i + (a'c - bd' + ca' + db')j + (ad' + bc' - cb' + da')k\end{aligned}$$

Then $\mathbb{H}$ forms a ring. We see that, for $x \in \mathbb{H}$,

$$\begin{aligned}x\bar{x} &= (a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2\\ x^{-1} &= \frac{\bar{x}}{x\bar{x}} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}\end{aligned}$$

each analogous to the complex numbers. Every $x \neq 0$ in $\mathbb{H}$ has a multiplicative inverse. However, multiplication does not commute in all of $\mathbb{H}$ ($ik = -j \neq j = ki$), so $\mathbb{H}$ is a division ring but not a field.

(vii) Let X be a nonempty set and A be any ring. The set of all mappings $f : X \to A$ where $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ forms a ring.

Since rings add an additional operation to a group structure, we have new properties that arise from the interaction of the two operations.

Proposition 1.1.1. Let R be a ring.

(i) $0 \cdot a = a \cdot 0 = 0 \quad \forall a, b \in R$

(ii) $(-a)b = a(-b) = -(ab) \quad \forall a, b \in R$

(iii) $(-a)(-b) = ab \quad \forall a, b \in R$

(iv) If R has identity 1, then that identity is unique and

$$-a = (-1)a \quad \forall a \in R$$

Proof. (i) Given $a \in R$, we have

$$\begin{aligned}a \cdot 0 = a(0 + 0) &= a \cdot 0 + a \cdot 0\\ \implies 0 &= a \cdot 0\end{aligned}$$

Similarly,

$$\begin{aligned}0 \cdot a = (0 + 0)a &= 0 \cdot a + 0 \cdot a\\ \implies 0 &= 0 \cdot a\end{aligned}$$

(ii) Given $a, b \in R$, we have

$$\begin{aligned}ab + (-a)b &= (a + -a)b\\ &= 0 \cdot b\\ &= 0 \implies -(ab) && = (-a)b\end{aligned}$$

$-(ab) = a(-b)$ is analogous.

(iii) Given $a, b \in R$, we have

$$\begin{aligned} -(ab) + (-a)(-b) &= (-a)b + (-a)(-b) \\ &= (-a)(b + -b) \\ &= (-a) \cdot 0 \\ &= 0 \\ \implies -(-(ab)) &= (-a)(-b) \\ \implies ab &= (-a)(-b) \end{aligned}$$

(iv) Let 1 and e both be identity elements in R. Then

$$\left.\begin{aligned} 1 \cdot e = e \\ 1 \cdot e = 1 \end{aligned}\right\} \implies 1 = e$$

Thus the identity element of R is unique. Let $a \in R$ be given. We have

$$\begin{aligned} 0 &= (1 + (-1))a \\ &= 1 \cdot a + (-1) \cdot a \\ &= a + (-1)a \\ \implies -a &= (-1)a \end{aligned}$$

□

1.2 Zero Divisors and Integral Domains

This semester we are adding multiplicative structure and we hope it is a good structure, but sometimes it is not. Consider the statement $3 \cdot 4 = 0$. Is this a true statement? In $\mathbb{R}$, no, it is not. However, if we consider the ring $\mathbb{Z}/6\mathbb{Z}$, then the statement is true. We call this blend of bad multiplicative behavior zero divisors.

Definition 1.2.1. (Zero Divisor)
Let R be a ring. A nonzero element $a \in R$ is called a zero divisor if there exists a nonzero $b \in R$ such that $ab = 0$ or $ba = 0$.

Example 1.2.1. Consider the matrices in $M_2(\mathbb{R})$. Let $A = \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix}$. Then

$$AB = \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$
$$BA = \begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 1 & -1 \end{bmatrix}$$

We now introduce the notion of multiplicative inverses. For a ring to be field, every element needs to have a multiplicative inverse. However, in some rings we might have some elements that have inverses but not all. We call these elements units.

Definition 1.2.2. (Unit)
Assume a ring R has identity $1 \neq 0$. An element $a \in R$ is called a unit in R if there exists an element $u \in R$ such that $uv = 1 = vu$. The set of all units in R is denoted by $R^\times$.

Example 1.2.2. $\mathbb{Z}/6\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$, $\mathbb{Z}/9\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}\}$.
Here, $(\mathbb{Z}/6\mathbb{Z})^\times = \{\bar{1}, \bar{5}\}$ and $(\mathbb{Z}/9\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$.

Concerning rings of the form $\mathbb{Z}/n\mathbb{Z}$ for $n \geq 0$, we have the following result regarding units.

Proposition 1.2.1. $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ is a unit if and only if $\gcd(a, n) = 1$.

Proof. ($\implies$) Suppose $\bar{a}$ is a unit. Then there exists $\bar{b} \in R$ such that $\bar{a}\bar{b} = \bar{1}$. This means that $ab \equiv 1($ mod $n)$, so $n \mid ab - 1$. Thus there exists some $y \in \mathbb{Z}$ such that $ab - 1 = ny$. More specifically, $ab - ny = 1$. Thus any common divisor d of a and n must also divide 1, so $d = 1$. Hence $\gcd(a, n) = 1$.
($\impliedby$) Suppose $\gcd(a, n) = 1$. By Bézout's identity, there exist $x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Thus $ax \equiv 1($ mod $n)$, so $\bar{a}\bar{x} = \bar{1}$. Hence, $\bar{a}$ is a unit. □

Remark 1.2.1. A consequence of the above proposition: $\mathbb{Z}/p\mathbb{Z}$ where p is prime is a field as $(\mathbb{Z}/p\mathbb{Z})^t imes = \{\bar{1}, \bar{2}, ..., p \bar{-} 1\}$.

Remark 1.2.2. Any nonzero element $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $\gcd(a, n) > 1$ is a zero divisor.

Example 1.2.3. In $Z/12\mathbb{Z}$, $\bar{8}$ is not relatively prime to 12 and $\bar{8}\bar{3} = \overline{24} = \bar{0}$.

In general, given $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ with $\bar{a} \neq 0$, we have that

$$\bar{a}\overline{\left(\frac{n}{\gcd(a,n)}\right)} = \frac{\bar{a}}{\gcd(a,n)} \cdot \bar{n} = \bar{0}$$

as $\frac{a}{\gcd(a,n)} \in \mathbb{Z}$. Further, since $\gcd(a, n) > 1$, we have that

$$0 < \frac{n}{\gcd(a,n)} < n$$

Proposition 1.2.2. Zero divisors can never be units.

Proof. Let R be a ring. Suppose that $a \in R$ is a unit and a zero divisor. Since a is a unit,

$$\exists b \in R \text{ such that } ab = 1 = ba$$

Since a is a zero divisor, ”

$$\exists c \in R \text{ such that } c \neq 0 \text{ and } ac = 0 \text{ or } ca = 0$$

If $ac = 0$, then

$$\begin{aligned} b(ac) &= b \cdot 0 \\ \implies (ba)c &= 0 \\ \implies 1 \cdot c &= 0 \\ \implies c &= 0 \end{aligned}$$

a contradiction. The case for $ca = 0$ is analogous. □

It follows that fields contain no zero divisors. We now introduce the notion of an integral domain which is a ring with no zero divisors.

Definition 1.2.3. (Integral Domain)
A commutative ring with identity $1 \neq 0$ si called an integral domain if it has no zero divisors.

Proposition 1.2.3. Let R be a ring and assume $a, b, c \in R$ with a not a zero divisor. If $ab = ac$, then $b = c$ or $a = 0$.

Proof.

$$\begin{aligned} ab &= ac \\ \implies ab - ac &= 0 \\ \implies a(b - c) &= 0 \end{aligned}$$

a is not a zero divisor, so either $a = 0$ or $a \neq 0$. If $a = 0$, then we are done. If $a \neq 0$, then $b - c = 0$ which implies $b = c$. □

The proposition above applies for any integral domain. From this proposition, we can derive the following corollary.

Corollary 1.2.1. Any finite integral domain is a field.

Proof. Let R be a finite integral domain and let $a \in R$ such that $a \neq 0$. Define the mapping

$$\begin{aligned} f_a &: R \to R \\ f_a(x) = ax \quad &\forall x \in R \end{aligned}$$

By the previous proposition, f_a is injective and since R is finite f_a is a bijection. In particular,

$$\exists b \in R \text{ such that } f_a(b) = ab = 1$$

Therefore a is a unit and since a was an arbitrary nonzero element of R, R is a field. □

In group theory, an important structure of study was the subgroup. For rings, we have an analogous structure called a subring.

Definition 1.2.4. (Subring)
A subring of a ring R is a subgroup of R with respect to addition which is closed under multiplication.

Proposition 1.2.4. (Subring Check)
Let $H \subseteq R$ where R is a ring.

(i) Subgroup check:

  (a) Show H is nonempty (e.g., show $0 \in H$)

  (b) Show $\forall x, y \in H \quad x - y \in H$

(ii) Closure under multiplication: $\forall x, y \in H \quad xy \in H$

1.3 Polynomials and Ring Homomorphisms

One of the big motivations for studying rings is to understand polynomials. Polynomials are a fundamental object in algebra and in this section we will define ring homomorphisms to help us understand the structure of polynomials.

Definition 1.3.1. (Polynomial)
Let R be a ring with unity 1. Let x be an indeterminate.

(i) The sum

$$\sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + ... + a_n x^n = f(x)$$

with $n \geq 0$ and each $a_i \in R$ is called a polynomial in x with coefficients in R.

(ii) If $a_n \neq 0$, then $\deg(f(x)) = n$. The zero polynomial has all $a_i = 0$, and the degree of the zero polynomial is undefined. The zero polynomial is denoted by 0.

(iii) The collection of all polynomials with coefficients in R is denoted $R[x]$, and is a ring with respect to the opperations

$$\left(\sum_{i=0}^{n} a_i x^i\right) + \left(\sum_{i=0}^{n} b_i x^i\right) = \sum_{i=0}^{n} (a_i + b_i) x^i$$

and

$$\left(\sum_{i=0}^{n} a_i x^i\right) \cdot \left(\sum_{i=0}^{n} b_i x^i\right) = a_0 b_0 + (a_0 b_1 + b_0 a_1) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + ... + (a_0 b_n + a_1 b_{n-1} + ... + a_n b_0) x^n$$

Example 1.3.1. When $R = \mathbb{Z}/3\mathbb{Z}$ (the polynomial ring $\mathbb{Z}/3\mathbb{Z}[x]$) Let $p(x) = x^2 + 2x + 1$ and $q(x) = x^3 + x + 2$. Then

$$p(x) + q(x) = x^3 + x^2 + 3x + 3 = x^3 + x^2$$

and

$$p(x)q(x) = x^5 + 2x^4 + 2x^3 + 4x^2 + 5x + 2$$

Example 1.3.2. In $\mathbb{Z}/2\mathbb{Z}[x]$

$$x^2 + 1 = (x+1)(x+1)$$

Ring homomorphisms are defined in a similar way to group homomorphisms.

Definition 1.3.2. (Ring Homomorphism)
Let R and S be rings.

(i) A ring homormorphism is a mapping $\phi : R \to S$ such that for all $a, b \in R$

(a) $\phi(a + b) = \phi(a) + \phi(b)$

(b) $\phi(ab) = \phi(a)\phi(b)$

(ii) The kernel of ϕ is defined as

$$\ker \phi = \{x \in R : \phi(x) = 0_S\}$$

(iii) A bijective ring homomorphism is an isomorphism.

Example 1.3.3. Let $\phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ be defined by

$$\phi(x) = \begin{cases} 0 & \text{if } x \text{ is even} \\ 1 & \text{if } x \text{ is odd} \end{cases}$$

Case 1: x and y are both even.

$$\phi(x+y) = 0 = \phi(x) + \phi(y), \phi(xy) = 0 = 0 \cdot 0 = \phi(x)\phi(y)$$

Case 2: x and y are both odd.

$$\phi(x+y) = 0 = 1 + 1 = \phi(x) + \phi(y), \phi(xy) = 1 = 1 \cdot 1 = \phi(x)\phi(y)$$

Case 3: One of x and y is even and the other is odd.
Without loss of generality, let x be even and y be odd.

$$\phi(x+y) = 1 = 0 + 1 = \phi(x) + \phi(y), \phi(xy) = 0 = 0 \cdot 1 = \phi(x)\phi(y)$$

We have two notable properties involving ring homomorphisms.

Proposition 1.3.1. Let R and S be rings and let $\phi : R \to S$ be a ring homomorphism.

(i) $\phi(R)$ is a subring of S.

(ii) $\ker\phi$ is a subring of R. Furthermore, if $\alpha \in \ker\phi$ and $r \in R$, the $r\alpha \in \ker\phi$ and $\alpha r \in \ker\phi$. That is, $\ker\phi$ is closed under the entire ring multiplication.

Proof. (i) We know that $\phi(R)$ is an additive subgroup of S from last semester. It remains to show that if $s_1, s_2 \in \phi(R)$, then $s_1s_2 \in \phi(R)$. Let $s_1, s_2 \in \phi(R)$ be given. Then

$$\exists r_1, r_2 \in R \text{ such that } s_1 = \phi(r_1) \text{ and } s_2 = \phi(r_2)$$

Then

$$s_1s_2 = \phi(r_1)\phi(r_2) = \phi(r_1r_2) \in \phi(R)$$

as desired.

(ii) We know that $\ker\phi$ is an additive subgroup of R from last semester. It suffices to show that if $r \in R$ and $\alpha \in \ker\phi$, then $r\alpha, \alpha r \in \ker\phi$. Let $r \in R$ and $\alpha \in \ker\phi$ be given. We have

$$\begin{aligned} \phi(r\alpha) &= \phi(r)\phi(\alpha) \\ &= \phi(r) \cdot 0_S \\ &= 0_S \\ \implies r\alpha &\in \ker\phi \end{aligned}$$

Similarly,

$$\begin{aligned} \phi(\alpha r) &= \phi(\alpha)\phi(r) \\ &= 0_S \cdot \phi(r) \\ &= 0_S \\ \implies \alpha r &\in \ker\phi \end{aligned}$$

□

The kernel of a ring homomorphism is a special type of subring. In particular, the kernel of a ring homomorphism is closed under multiplication by any element in the ring. We call this the absorbative property it allows us to define coset multiplication for rings.

Let I be the kernel of a ring homomorphism $\phi : R \to S$. We know that the additive left cosets of I form a group. Because every subgroup of an abelian group is normal, the definition of coset addition is well-defined:

$$(\alpha + I) + (\beta + I) = (\alpha + \beta) + I \quad \forall \alpha, \beta \in R$$

We aim to show that the absorbative property of $\ker\phi = I$ makes coset multiplication well-defined. We define coset multiplication as

$$(\alpha + I)(\beta + I) = (\alpha\beta) + I$$

Suppose that $\alpha + I = \alpha' + I$ and $\beta + I = \beta' + I$. We want to show that

$$(\alpha\beta) + I = (\alpha'\beta') + I$$

Note that

$$\begin{aligned} \alpha + I = \alpha' + I &\implies \alpha = \alpha' + x \text{ where } x \in I \\ \beta + I = \beta' + I &\implies \beta = \beta' + y \text{ where } y \in I \end{aligned}$$

Then

$$\alpha\beta = (\alpha' + x)(\beta' + y) = \alpha'\beta' + \alpha' y + x\beta' + xy$$

$\alpha' y, x\beta', xy \in I$, so $\alpha\beta = \alpha'\beta' + z$ where $z = \alpha' y + x\beta' + xy \in I$. Thus $\alpha\beta - \alpha'\beta' \in I$. Therefore, $(\alpha\beta) + I = (\alpha'\beta') + I$ and so coset multiplication is well-defined. We have now motivated the following definition.

Definition 1.3.3. (Ideals)
Let R be a ring and let $I \subseteq R$. Let $r \in R$.

(i) $rI = \{rx : x \in I\}$ and $Ir = \{xr : x \in I\}$

(ii) I is a left ideal of R if

  (a) I is a subring of R

  (b) $\forall r \in R \;\; rI \subseteq I$

(iii) I is a right ideal of R if

  (a) I is a subring of R

  (b) $\forall r \in R \;\; Ir \subseteq I$

(iv) If I is both a left and right ideal of R, then I is called an ideal of R.

1.4 Quotient Rings and the Isomorphism Theorems

Now that we have defined ideals, we can use them to construct new rings called quotient rings, similar to how we used normal subgroups to construct quotient groups. We will then use ideals and quotient rings to discuss isomorphisms between ring structures. First, given a ring R and an ideal I of R, we will show that the set R/I has any meaning.

Proposition 1.4.1. Let R be a ring and I be an ideal of R. Then R/I is a ring under the binary operations

$$\forall r, s \in I \quad (r+I)+(s+I) = (r+s)+I$$
$$\forall r, s \in I \quad (r+I)(s+I) = (rs)+I$$

Proof. Note that we proved multiplication is well-defined and we also know the group structure exists from last semester. Distribution and associativity in R/I follow from distribution and associativity in R. □

Definition 1.4.1. (Quotient Ring)
When I is an ideal of a ring R, the ring R/I is called the quotient ring of R by I.

We can now establish the isormophism theorems for rings.

Theorem 1.4.1. (The First Isomorphism Theorem for Rings)

(i) If $\phi : R \to S$ is a ring homomorphism, then $\ker\phi$ is an ideal of R, $\phi(R)$ is a subring of S, and

$$\frac{R}{\ker\phi} \cong \phi(R)$$

(ii) If I is any ideal of R, then the map

$$\pi : R \to R/I$$
$$\pi(r) = r + I$$

is a surjective ring homomorphism with kernel I. This is called the natural projection of R onto R/I.

Proof. Last semester we established the mapping

$$\mu : R/\ker\phi \to \phi(R)$$
$$\mu(r+K) = \phi(r)$$

as a well-defined bijection which preserved the group operation (in this case, +). It remains to show that μ preserves coset multiplication.

$$\begin{aligned}\mu\left((r+K)(s+K)\right) &= \mu(rs+K)\\ &= \phi(rs)\\ &= \phi(r)\phi(s)\\ &= \mu(r+K)\mu(s+K)\end{aligned}$$

□

Example 1.4.1. Let R be a ring.

(i) The trivial ideal is 0.

(ii) R is an ideal of R.

(iii) If I is an ideal of R where $I \neq R$, then I is a proper ideal of R.

Example 1.4.2. Last semester (when studying cyclic groups) we proved the only subgroups of $\mathbb{Z}$ were of the form $n\mathbb{Z}$ for some $n \geq 0$. This tells us that all the ideals of $\mathbb{Z}$ must be of the same form. It is a straightforward exercise to show that $n\mathbb{Z}$ ($n \geq 0$) is an ideal of $\mathbb{Z}$:

$$\begin{aligned} x \in \mathbb{Z}, y \in n\mathbb{Z} \implies y = nz \ \text{ for } z \in \mathbb{Z} \text{ and } xy &= x(nz) = n(xz) \in n\mathbb{Z} \\ yx &= (nz)x = n(zx) \in n\mathbb{Z} \end{aligned}$$

In this setting,

$$\begin{aligned} &\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ &\pi(x) = \bar{x} \text{ (reduction modulo } n) \\ &\mathbb{Z}/5\mathbb{Z} \quad 7 = 2 \end{aligned}$$

Example 1.4.3. Consider $I = \{p(x) \in \mathbb{Z}[x] : p(x) = 0$ or whose terms are of at least degree $2\}$. Does I have the absorbative property of an ideal? Let $f(x) \in \mathbb{Z}[x]$ and $q(x) \in I$. Then

$$f(x) = \sum_{i=0}^{n} a_i x^i \quad q(x) = \sum_{i=0}^{n} b_i x^i \quad \text{where } b_0 = 0, b_1 = 0$$

Then the constant coefficient of $f(x)q(x)$ is $a_0 b_0 = a_0 \cdot 0 = 0$ and the linear coefficient of $f(x)q(x)$ is $a_1 b_0 + a_0 b_1 = a_1 \cdot 0 + a_0 \cdot 0 = 0$.

Example 1.4.4. Let A be a ring and X be a nonempty set. Let R be the ring of all functions from X to A. For each $c \in X$ we can define the mapping

$$\begin{aligned} E_c &: R \to A \\ E_c(f) = f(c) &\text{ (the evaluation homomorphism)} \end{aligned}$$

Let $f, g \in R$. Then

$$\begin{aligned} E_c\left((f \cdot g)(x)\right) &= (f \cdot g)(c) \\ &= f(c) \cdot g(c) \\ &= E_c\left(f(x)\right) \cdot E_c\left(g(x)\right) \end{aligned}$$

Addition follows similarly. Notice

$$\ker E_c = \{f \in R : E_c(f) = 0\} = \{f \in R : f(c) = 0\}$$

By the first isomorphism theorem, we have

$$\frac{R}{\ker E_c} \cong E_c(R)$$

What is $E_c(R)$? Let $a \in A$. Notice the constant function $h(x) = a \ \forall x \in X$ gives

$$E_c\left(h(x)\right) = h(c) = a$$

Thus $E_c(R)$ is surjective and so

$$\frac{R}{\ker E_c} \cong A$$

Theorem 1.4.2. (The Second, Third, and Fourth Isomorphism Theorems for Rings) Let R be a ring.

(i) Let A be a subring of R and let B be an ideal of R. Then

$$A + B = \{a + b : a \in A, b \in B\}$$

is a subring of R, $A \cap B$ is an ideal of A, and

$$\frac{A + B}{B} \cong \frac{A}{A \cap B}$$

(ii) Let I and J be ideals of R with $I \subseteq J$. Then J/I is an ideal of R/I and

$$\frac{R/I}{J/I} \cong \frac{R}{J}$$

(iii) Let I be an ideal of R. The correpsondence $A \leftrightarrow A/I$ is an inclusion preserving bijection between the set of subrings of R containing I and the subrings of R/I. Furthermore, A (a subring containing I) is an ideal of R if and only if A/I is an ideal of R/I.

Similar to groups, ring homomorphisms will map subrings to subrings. Can the same be said for ideals? The answer is no, this is only true for surjective homomorphisms.

1.5 Generated Ideals

Proposition 1.5.1. Let I and J be ideals of a ring R. Define

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

Then $I + J$ is the smalles ideal of R that contains both I and J.

Proof. We know that I and J are normal additive subgroups of R, so $I + J$ is a subgroup of R.

$$\begin{aligned} a_1 + b_1, a_2 + b_2 \in I + J \implies & (a_1 + b_1)(a_2 + b_2) \\ & = a_1a_2 + a_1b_2b_1a_2 + b_1b_2 \end{aligned}$$

Notice

$$a_1 \in I \implies \begin{matrix} a_1a_2 \in I \\ a_1b_2 \in I \end{matrix} \qquad\qquad b_1 \in J \implies \begin{matrix} b_1b_2 \in J \\ b_1a_2 \in J \end{matrix}$$

since I and J are ideals. Hence, $(a_1 + b_1)(a_2 + b_2) \in I + J$ and so $I + J$ is an ideal of R.
Futhermore, $I + J$ is the smalles ideal of R which contains I and J. We can verify that I and J are contained in $I + J$. Letting $b = 0$, we see any $a \in I$ is in $I + J$. Similarly, letting $a = 0$ we see any $b \in J$ is in $I + J$. Hence both I and J are contained in $I + J$. Let K be an ideal of R which contains both I and J. Let $a + b \in I + J$. Then

$$\begin{aligned} a \in I \text{ and } b \in J & \implies a \in K \text{ and } b \in K \\ & \implies a + b \in K \\ & \implies I + J \subseteq K \end{aligned}$$

□

Definition 1.5.1. (Finitely Generated Ideal)
Let R be a ring with identity 1. Let A be a subset of R. Let (A) denote the smallest ideal of R containing A. We can define (A) more concretely by

$$(A) = \bigcap_{I \subseteq A} I, \ I \text{ is an ideal of } R$$

An ideal genearted by a finite set is called a finitely generated ideal. If $A = \{a_1, a_2, ..., a_n\}$, then (A) will be written as $(a_1, a_2, ..., a_n)$.
$(I, J) = I \cup J$ (where I and J are subsets of R)

What is the simplest group generated by a set? Cyclic groups that are generated with a single element. Given a ring R with unity $1 \neq 0$ and some $a \in R$, consider (a), the ideal generated by a. (a) needs to contain ra and ar for all $r \in R$. What's more is (a) must be closed with respect to addition so we need all finite sums of ra's and ar's

$$(r_1a + r_2a + ar_3 + ar_4 + ...)$$

If we suppose that R is commutative, then (a) is very simple.

Definition 1.5.2. (Principal Ideal)
Let R be a ring and $a \in R$. When R is commutative with $1 \neq 0$,

$$(a) = \{ar : r \in R\}$$

and (a) is called the principal ideal of R generated by a.

Example 1.5.1. (i) In any ring, $0 = (0)$ and when R has unity 1, $(1) = R$.

(ii) Let R be a commutatie ring with unity $1 \neq 0$.

$$(a) + (b) = (a + b) \text{ (from what we proved about } I + J)$$

(iii) All ideals are principal.

(iv) All additive subgroups of $\mathbb{Z}$ are of the form $n\mathbb{Z}, n \geq 0$ and $n\mathbb{Z}$ is an ideal for all $n \geq 0$. Furthermore, $n\mathbb{Z} = \{nx : x \in \mathbb{Z}\} = (n)$.

Proposition 1.5.2. Let I be an ideal of R.

(i) $I = R$ if and only if I contains a unit.

(ii) Assume R is commutative. R is a field if and only if its only ideals are 0 and R.

Proof. (i) If $I = R$, then $1 \in I$. Conversely, if u is a unit in I with inverse $v \in R$, then for any $r \in R$

$$r = r \cdot 1 = r(vu) = (rv)u \in I$$

Thus $R = I$.

(ii) The ring R is a field if and only if every nonzero element is a unit. Hence, any nonzero ideal contains a unit. Thus the only nonzero ideal of R is R. Conversely, if 0 and R are the only ideals of R, we let u be any nonzero element of R. By hypothesis, $(u) = R$ so $1 \in (u)$. That is, $1 = uv$ for some $v \in R$. That is, u is a unit. Thus every nonzero element of R is a unit so R is a field.

□

Let's say I is a nonzero ideal in $\mathbb{Q}$. Then there exists $a \in I$ such that $a \neq 0$. Since ideals have the absorbative property, we know that $\frac{1}{a} \in \mathbb{Q}$ and $\frac{1}{a} \cdot a \in I$ which implies $1 \in I$. Then for any $b \in \mathbb{Q}$ we have $b = b \cdot 1 \in I$ which implies $\mathbb{Q} \subseteq I$. Thus $I = \mathbb{Q}$.

1.6 Maximal Ideals

Note that for any $n \in \mathbb{N}$ and $a \in R$ a ring, we define

$$na = a + a + ... + a \quad n \text{ times}$$

Proposition 1.6.1. Let $m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$. Then $m \mid \binom{m}{n}$.

Proof.

$$\begin{aligned}\binom{m}{n} &= \frac{m!}{n!(m-n)!} \\ &= \frac{m}{n}\frac{(m-1)!}{(n-1)!(m-n)!} \\ &= \frac{m}{n}\binom{m-1}{n-1}\end{aligned}$$

So,

$$n\binom{m}{n} = m\binom{m-1}{n-1}$$

so $m \mid n\binom{m}{n}$. But $\gcd(m, n) = 1$, so $m \mid \binom{m}{n}$. □

Corollary 1.6.1. If R is a field, then any nonzero ring homomorphism from R into another ring is an injection.

Proof. Let R be a field and let $\phi : R \to S$ be a nonzero ring homomorphism. Since $\ker \phi$ is an ideal fo the field R, $\ker \phi$ is either 0 or R itself. If $\ker \phi = R$, then $\phi(r) = 0$ for all $r \in R$. Hence, contrary to our assumption, ϕ is the zero homomorphism. This leaves us with $\ker \phi = 0$. As we know from our work with groups,

$$\ker \phi = 0 \iff \phi \text{ is injective}$$

□

Definition 1.6.1. (Maximal Ideal)
An ideal M in a ring S is called a maximal ideal if $M \neq S$ ans the only ideals that contain M are S and M itself.

A maximal ideal gives the notion of a ”largest proper ideal” of a ring. That is, if M is the maximal ideal to a ring R and H is a proper ideal of R such that $M \subseteq H \subseteq R$, then either $H = R$ or $H = M$.

Proposition 1.6.2. In a ring with unity, every proper ideal is contained in a maximal ideal.

The next result characterizes maximal ideals with their quotient structures of a commutative ring.

Proposition 1.6.3. Assume R is commutative. The ideal M is a maximal ideal if and only if R/M is a field.

Proof. M is a maximal ideal if and only if there are no ideals I with

$$M \subset I \subset R$$

By the fourth isomorphism theorem, ideals of R containing M are in 1-1 correspondence with the ideals of R/M. So M is maximal if and only if there are no ideals I with $M \subset I \subset R$ if and only if there are no maximal ideals of R/M if and only if the only ideals of R/M are R/M and 0 if and only if R/M is a field. Some things to verify: R/M is commutative (since R is commutative, we have R/M is commutative), R/M has unity $(1 + M \in R/M)$, and R/M is not the zero ring $(M \neq R, R/M \neq 0)$. □

Example 1.6.1. What are the maximal ideals in $\mathbb{Z}$? We know all subrings of Z are of the form $n\mathbb{Z}, n \geq 0$. It takes very little work to show that $n\mathbb{Z}, n \geq 0$ is an ideal. The maximal ideals are those such that $\mathbb{Z}/n\mathbb{Z}$ is field. We know that $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime. Thus $n\mathbb{Z}, n \geq 0$ is a maximal ideal if and only if n is prime.

We now look to generalize the notion of a prime number through ideals. Looking at $\mathbb{Z}$, suppose $n\mathbb{Z}, n \geq 0$ is an ideal of $\mathbb{Z}$. Suppose $a, b \in \mathbb{Z}$ such that $a \in n\mathbb{Z}$ or $b \in n\mathbb{Z}$. Note

$$a \in (n) \iff a = nx \quad \text{for some integer } x$$

So $n \mid a$. Equivalently, we can say if $n \mid ab$ then $n \mid a$ or $n \mid b$. This is exactly the behavior of a prime number. This motivates the following definition.

Definition 1.6.2. (Prime Ideal)
Assume R is commutative. An ideal P is called a prime ideal if $P \neq R$ and if $ab \in P$, then $a \in P$ or $b \in P$.

The defining trait of a prime ideal is that whenever a product lands in the ideal, one of the factors must already be there. In a quotient ring, this looks like the following: if $(a+P)(b+P) = 0+P$ then either $(a+P) = 0+P$ or $(b+P) = 0+P$. This leads us to the following characterization.

Proposition 1.6.4. Assume R is commutative. The ideal P is a prime ideal in R if and only if R/P is an integral domain.

Proof. The ideal P is prime if and only if $P \neq R$ and if $ab \in P$, then $a \in P$ or $b \in P$. Recall that

(i) $ab \in P \iff (a+P)(b+P) = ab + P = 0 + P$

(ii) $a \in P \iff a + P = 0 + P$

(iii) $b \in P \iff b + P = 0 + P$

So, P is a prime ideal if and only if $R/P \neq 0$ and if $(a+P)(b+P) = 0+P$, then $a+P = 0$ or $b+P = 0$ if and only if R/P is an integral domain (since we know R/P is a commutative ring with unity). □

1.7 Rings of Fractions

We take a brief look at fractions. Fractions are equivalence cleases, as given any two fractions a/b and c/d we have

$$\frac{a}{b} = \frac{c}{d} \iff da = cb$$

If we look at $R \times R$ where R is a ring we can define fractions as ordered pairs under the relation

$$(a, b) = (c, d) \iff da = cb$$

What this allows us to do when R is an integral domain is to create a field which contains an isomorphic copy of R. We will not spend much time here, so we end this chapter with the following remark.

Remark 1.7.1. Every integral domain is contained in a field and the smalles field which contains an integral domain is called the field of fractions of the integral domain.

In the next chapter, we will discuss different types of integral domains. More specifically, we will discuss the following:

(i) Euclidean domain (ED)

(ii) Principal ideal domain (PID)

(iii) Unique factorization domains (UFD)