

Math 110.1

ABSTRACT ALGEBRA I: Unit III

Course Notes by: Jeremiah Daniel Regalario

II-BS Mathematics

University of the Philippines - Diliman

Dr. Lilibeth Valdez

Rings

Definition:

A ring $\langle R, +, \cdot \rangle$ is a set together with two binary operations $+$ (called *addition*) and \cdot (called *multiplication*) such that the following axioms are satisfied:

1. $\langle R, + \rangle$ is an abelian group.
2. Multiplication is associative, that is, for all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
3. For all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ (left and right distributive laws holds.)

Examples:

1. \mathbb{Z} is closed under the usual addition $+$ and multiplication \cdot .
 1. $\langle \mathbb{Z}, + \rangle$ is an abelian group.
 2. \cdot is associative.
 3. Left and right distributive laws holds

Thus, $\langle \mathbb{Z}, +, \cdot \rangle$ is a ring.

2. $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ and $\langle \mathbb{C}, +, \cdot \rangle$ are rings.

Remarks:

1. If the operations $+$ and \cdot are clear from context we denote the ring $\langle R, +, \cdot \rangle$ simply by R .
2. The identity of the group $\langle R, + \rangle$ is denoted 0 and is called the zero element of R .
3. The inverse of a in the group $\langle R, + \rangle$ is denoted $-a$.
4. We write $a - b$ for $a + (-b)$.
5. To simplify notations, we write ab for $a \cdot b$.
6. In the absence of parentheses, multiplication is assumed to be performed before addition, that is, $ab + c = (ab) + c$

Commutative Rings, Rings with Unity, and Units

Definition:

Let R be a ring.

1. If multiplication in R is commutative, then R is called a commutative ring.
2. An element 1_R such that $\forall r \in R, 1_R r = r = r 1_R$ is called a multiplicative identity or a unity.
3. If R has a multiplicative identity, then R is called a ring with unity.
4. Suppose R is a ring with unity $1_R \neq 0$. An element $u \in R$ is a unit if u has a multiplicative inverse, that is $\exists u^{-1} \in R$ such that $uu^{-1} = 1_R = u^{-1}u$.

Remarks:

1. Some rings are not commutative and some have no unity.
2. If R has unity, then this unity is unique.
3. If R has unity 1_R , then 1_R is a unit in R .
4. If R has unity, not all elements in the ring are units.

Examples:

1. $\langle \mathbb{Z}, +, \cdot \rangle$ is a commutative ring with unity 1. The units of \mathbb{Z} : 1, -1.
2. $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ and $\langle \mathbb{C}, +, \cdot \rangle$ are commutative rings with unity 1.

Every nonzero element in these rings is a unit.

3. $\langle \mathbb{Z}_n, +_n, \cdot_n \rangle$ is a commutative ring with unity 1. The set of units of \mathbb{Z}_n is denoted $U(n)$.

Exercise: Determine the elements of $U(4)$ and $U(5)$.

- $U(4) = \{a \in \mathbb{Z}_4 \mid \exists k \in \mathbb{Z} \text{ s.t. } a \cdot_4 k = 1\} = \{1, 3\}$
- $U(5) = \{a \in \mathbb{Z}_5 \mid \exists k \in \mathbb{Z} \text{ s.t. } a \cdot_5 k = 1\} = \{1, 2, 3, 4\}$

4. $\langle 2\mathbb{Z}, +, \cdot \rangle$ is a commutative ring with no unity.
5. Let $M_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \mid a, b, c, d, \in \mathbb{R} \right\}$. Define $+$ and \cdot on $M_2(\mathbb{R})$ as:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} + \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} a+e & b+f \\ c+g & d+h \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{bmatrix}$$

Then $M_2(\mathbb{R})$ is a noncommutative ring with unity:

- $+$ is associative and commutative (Exercise)
- \cdot is associative but not commutative (Exercise)
- left and right distributive laws hold (Exercise)
- zero element: $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$; additive inverse: $\begin{bmatrix} -a & -b \\ -c & -d \end{bmatrix}$; unity: $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

Theorem 2.13**Definition:**

Let R be a ring with additive identity 0. Let $a, b, c \in R$.

1. $a \cdot 0 = 0 \cdot a = 0$
2. $a(-b) = (-a)b = -(ab)$.
3. $(-a)(-b) = ab$
4. $a(b-c) = ab - ac$ and $(a-b)c = ac - bc$.

Proof:

- (1.) $a \cdot 0 + a \cdot 0 = a(0 + 0) = a \cdot 0$. By left cancellation, $a \cdot 0 = 0$. The proof for $0 \cdot a = 0$ follows analogously.
- (2.) $ab + a(-b) = a(b - b) = a \cdot 0 = 0$. Since the additive inverse of ab is unique, $-(ab) = a(-b)$. The proof that $(-a)b = -(ab)$ proceeds analogously.

$$(3.) (-a)(-b) = -[a(-b)] = -[-(ab)] = ab$$

Remarks:

1. If R is a nonzero ring with unity then $1 \neq 0$. (Why?)
2. If R is a ring with unity and $a \in R$ then $(-1)a = -a$. In particular $(-1)(-1) = 1$.
3. Let R be a ring and $a, b, c \in R$. If $a \neq 0$ and $ab = ac$, then b and c are not necessarily equal. ($a \neq 0 \wedge ab = ac \not\Rightarrow b = c$)
 - e.g. in \mathbb{Z}_4 , $2 \cdot_4 1 = 2 = 2 \cdot_4 3$ but $1 \neq 3$.
4. In a ring R , $ab = 0$ does not necessarily mean that either $a = 0$ or $b = 0$.
 - e.g. in \mathbb{Z}_6 , $2 \cdot_6 3 = 0$

Group of Units of R (Theorem 2.14)

Definition:

Let R be a ring with unity. The units of R form a group under multiplication.

Remark:

The group of units of a ring with unity R is denoted $U(R)$.

Proof:

- Closure under multiplication: Let $a, b \in U(R)$. (WTS: $ab \in U(R)$). Since $a, b \in U(R)$, $\exists a^{-1}, b^{-1} \in R$ such that $aa^{-1} = bb^{-1} = 1$. Note that $b^{-1}a^{-1} \in R$ and

$$\begin{aligned} (b^{-1}a^{-1})(ab) &= b^{-1}[(a^{-1})(ab)] \\ &= b^{-1}[(a^{-1}a)b] \\ &= b^{-1}[1 \cdot b] \\ &= b^{-1}b = 1 \end{aligned}$$

Thus $(ab)^{-1} = b^{-1}a^{-1}$ and so $ab \in U(R)$.

- Associativity of multiplication: Follows from \mathcal{R}_2 .
- Identity element under multiplication: unity $1 \in U(R)$ has the property that

$$\forall a \in U(R) \subseteq R, a \cdot 1 = 1 \cdot a = a.$$

- Inverse under multiplication: Let $a \in U(R)$. Then $\exists a^{-1} \in R$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$. From this, we see that $a^{-1} \in U(R)$.

$\therefore \langle U(R), \cdot \rangle$ is a group.

Examples:

1. $U(\mathbb{Z}) = \{1, -1\} \cong \mathbb{Z}_2$
2. $U(\mathbb{Q}) = \mathbb{Q}^*$, $U(\mathbb{R}) = \mathbb{R}^*$, $U(\mathbb{C}) = \mathbb{C}^*$
3. $U(\mathbb{Z}_n) = U(n)$ = set of all elements of \mathbb{Z}_n that are relatively prime to n
4. $U(M_2(\mathbb{R})) = \text{GL}(2, \mathbb{R})$

Fields and Division Rings

Definition:

Let R be a ring with unity $1 \neq 0$. If every nonzero element of R is a unit then R is called a division ring.

If R is a commutative division ring, then R is called a field.

Remarks:

Let R be a ring with unity $1 \neq 0$.

1. If R is a field, we write $\frac{a}{b}$ for $ab^{-1} = b^{-1}a$. In particular, we write $b^{-1} = \frac{1}{b}$.
2. A division ring can be thought of as an algebraic structure that is closed under addition, subtraction, multiplication and division by nonzero elements.
3. R is a division ring if and only if $R^* := R \setminus \{0\}$ is a group.
4. R is a field if and only if $R^* := R \setminus \{0\}$ is an abelian group.

Examples:

1. \mathbb{Z} is not a division ring, and hence not a field.
2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ are fields.
3. \mathbb{Z}_4 is not a division ring. $\because 0 \neq 2 \in \mathbb{Z}_4$ is not a unit.
4. \mathbb{Z}_5 is a field.

In \mathbb{Z}_5 :

- $\frac{3}{4} = 3 \cdot_5 4^{-1} = 3 \cdot_5 4 = 2$
- $2 \frac{1}{3} = 2 +_5 \frac{1}{3} = 2 +_5 3^{-1} = 2 +_5 2 = 4$

Subrings and Subfields

Subring

Definition:

A subset S of a ring R which is also a ring itself under the same operations as in R is called a subring of R .

Theorem 2.15

Let R be a ring and S a nonempty subset of R . Then S is a subring of R if and only if for all $a, b \in S$, $a - b \in S$ and $ab \in S$.

Proof:

(\Rightarrow) Since S is a ring, then $\langle S, + \rangle$ is an abelian group hence $a - b \in S$.

Also, $ab \in S$ since \cdot is a binary operation on S .

(\Leftarrow) Suppose $a - b \in S$ and $ab \in S$ for all $a, b \in S$. $\mathcal{R}_1 : a - b \in S$ for all $a, b \in S \Rightarrow \langle S, + \rangle$ is a subgroup of $\langle R, + \rangle$. Thus, $\langle S, + \rangle$ is an abelian group.

\mathcal{R}_2 : and \mathcal{R}_3 : follows since operations in S and R are the same.

Remarks:

Let R be a ring and S a subring of R .

1. If R is commutative, then S is also commutative.
2. S may be without unity even if R has unity.

Subfields

Definition:

A subset S of a field F which is also a field itself under the same operations as in F is called a subfield of F .

Theorem 2.16

Let F be a field and S a nonempty subset of F . Then S is a subfield of F if and only if the following hold:

1. $S \neq \{0\}$
2. for all $a, b \in S$, $a - b \in S$ and $ab \in S$
3. for all $0 \neq a \in S$, $a^{-1} \in S$ (i.e. every nonzero element is a unit.)

Proof:

Exercise!

Examples:

1. If R is a ring then $\{0\}$ (trivial subring) and R (improper subring) are subrings of R .

2. \mathbb{Q} is a subfield of \mathbb{R} .
3. For any $n \in \mathbb{Z}$, $n\mathbb{Z}$ is a subring of \mathbb{Z} . (Why?) Note that if $n \neq 1, -1$, then $n\mathbb{Z}$ has no unity.
4. Let $D_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbb{R} \right\}$. Let $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}, \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} \in D_2(\mathbb{R})$,

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} - \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} a-c & 0 \\ 0 & b-d \end{bmatrix} \in D_2(\mathbb{R})$$

$$\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \begin{bmatrix} c & 0 \\ 0 & d \end{bmatrix} = \begin{bmatrix} ac & 0 \\ 0 & bd \end{bmatrix} \in D_2(\mathbb{R})$$

$\therefore D_2(\mathbb{R})$ is a subring of $M_2(\mathbb{R})$. ■

Zero Divisors

Definition:

Let R be a commutative ring. A nonzero element $a \in R$ is called a zero divisor (or a divisor of zero) if there is a non-zero element $b \in R$ such that $ab = 0$.

Example:

1. zero divisors of \mathbb{Z}_{12} : 2, 3, 4, 6, 7, 8, 9, 10
2. \mathbb{Z} has no zero divisors.

Theorem 2.17:

The zero divisors of \mathbb{Z}_n are its non-zero elements that are not relatively prime to n .

Proof. Let $0 \neq a \in \mathbb{Z}_n$.

(\implies) Suppose a is a zero divisor of \mathbb{Z}_n . Then, $\exists (0 \neq b \in \mathbb{Z}_n)$ s.t. $ab = 0 \implies n \mid ab$.

Suppose (on the contrary) that a is relatively prime to n , then $n \mid b \implies b = 0$. \nmid

$\therefore a$ is NOT relatively prime to n .

(\impliedby) Suppose $d = \gcd(a, n) > 1$. Let $a = dk_1$ and $n = dk_2$ for some $k_1, k_2 \in \mathbb{Z}$.

Note that $0 \neq k_2 \in \mathbb{Z}_n$. Then

$$ak_2 = dk_1k_2 = dk_2k_1 = nk_1 = 0.$$

$\therefore a$ is a zero divisor. ■

Integral Domain

Definition:

A commutative ring with unity $1 \neq 0$ is said to be an *integral domain* if it has no zero divisors.

Remark:

In an integral domain D , if $ab = 0$, then either $a = 0$ or $b = 0$.

Example:

Division rings that are integral domains.

1. \mathbb{Z} ✓
2. $\mathbb{Q}, \mathbb{C}, \mathbb{R}$ ✓
3. \mathbb{Z}_p ✓, where p is prime.
4. $\mathbb{Z} \times \mathbb{Z}$ - has zero divisors $(0, a)$ and $(b, 0)$ for some $0 \neq a, b \in \mathbb{Z}$.
5. $M_2(\mathbb{R})$ - not a commutative ring
6. $2\mathbb{Z}$ - has no unity

Theorem 2.18:

Let R be a commutative ring with unity $1 \neq 0$. Then, the cancellation law for multiplication holds in R if and only if R is an integral domain.

Proof.

(\implies) Suppose that $\forall a, b, c \in R$ with $a \neq 0$, $ab = ac \implies b = c$.

Let $a \in R$ with $a \neq 0$. Suppose that $ab = 0 = a \cdot 0$ for some $b \in R$. Then, $b = 0$.
Hence, a is a non-zero divisor of R .

$\therefore R$ is an integral domain.

(\impliedby) Suppose that R is an integral domain. Let $a, b, c \in R$ with $a \neq 0$ and $ab = ac$.

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

$\therefore \forall a, b, c \in R$ with $a \neq 0$, $ab = ac \implies b = c$.

\therefore Cancellation law for multiplication holds if and only if R is an integral domain. ■

Remarks:

Let R be an integral domain. Let $a, b \in R$ with $a \neq 0$.

1. Then $ax + b$ has at most one solution.
2. If a is a unit in R , then $ax = b$ has exactly one solution, given by $x = \frac{b}{a} = a^{-1}b$.

Theorem 2.19:

Every field is an integral domain.

Proof.

Let F be a field. Then, F is commutative with unity $1 \neq 0$.

Let $a \in F$ s.t. $a \neq 0$.

Suppose $ab = 0$ for some $b \in F$.

$$\Rightarrow \frac{1}{a}(ab) = \frac{1}{a} \cdot 0$$

$$\Rightarrow \left(\frac{1}{a} \cdot a\right)b = 0$$

$$\Rightarrow 1 \cdot b = 0$$

$$\Rightarrow b = 0$$

$\therefore a$ is not a zero divisor.

$\therefore F$ is an integral domain. ■

Theorem 2.20:

Every finite integral domain is a field.

Proof.

Let D be a finite integral domain. Then, D is commutative with unity $1 \neq 0$.

Let $0 \neq a \in D$. (WTS: a is a unit.)

Consider the function f defined as:

$$\begin{aligned} f : D &\rightarrow D \\ x &\mapsto ax \end{aligned}$$

Suppose $f(x) = f(y)$ for some $x, y \in D$. Then, $ax = ay \Rightarrow x = y$. (via C. L.)

So, f is one-to-one $\Rightarrow f$ is onto.

Since $1 \in D \Rightarrow \exists b \in D$ s.t. $f(b) = 1$.

$$\Rightarrow ab = 1$$

$$\Rightarrow a \text{ is a unit}$$

$\therefore D$ is a field. ■

Example:

Let p be prime. Then \mathbb{Z}_p is an integral domain $\Rightarrow \mathbb{Z}_p$ is a field.

Recall: R is a ring, $a \in R, n \in \mathbb{N}$.

$$\bullet \ n \cdot a = \underbrace{a + a + \cdots + a}_n$$

- $(-n)a = \underbrace{-a - a - \cdots - a}_n$
- $0 \cdot a = 0$

Example:

1. In $M_2(\mathbb{R})$,

$$3 \cdot \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 3 \\ 3 & 3 \end{bmatrix}.$$

2. In \mathbb{Z}_6 : $\underbrace{2}_{\in \mathbb{Z}} \cdot \underbrace{3}_{\in \mathbb{Z}_6} = 3 +_6 3 = 0$.

Remark:

If R is a ring and $a, b \in R, m, n \in \mathbb{Z}$, then

1. $(m + n) \cdot a = m \cdot a + n \cdot a$
2. $m(a + b) = ma + mb$
3. $(mn)a = m(na)$
4. $m(ab) = (ma)b = a(mb)$
5. $(ma)(nb) = (mn)(ab)$

Characteristic of a Ring

Definition:

The characteristic of a ring R is the least positive integer n such that $\forall a \in R, n \cdot a = 0$. If no such integer exists, R is said to be of characteristic 0.

Example:

1. $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$. $\text{char}(\mathbb{Z}_6) = 6$.
2. $\text{char}(\mathbb{Z}) = 0$.
3. $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ are of characteristic 0.

Theorem 2.21:

Let R be a ring with unity 1.

1. If 1 has infinite order, then $\text{char}(R) = 0$.
2. If 1 has order n , then $\text{char}(R) = n$.

Proof. (Exercise)

Example:

1. $\text{char}(\mathbb{Z}_n) = n$
2. $\text{char}(M_2(\mathbb{R})) = 0$

Theorem 2.22:

The characteristic of an integral domain is 0 or prime.

Proof. (Exercise)

Ideals and Factor Rings (Part I)

Ideals

Definition:

A subring I of a ring R is called an ideal of R if $\forall r \in R, \forall a \in I, ra \in I$ and $ar \in I$.

Example:

1. Let R be a ring. Then, $\{0\}$ (*trivial ideal*) and R (*improper ideal*) are ideals of R .

Ideal I s.t. $I \neq R$ is a *proper ideal* of R .

2. $n\mathbb{Z} \subseteq \mathbb{Z}$ ($n \in \mathbb{Z}^+$) $n\mathbb{Z}$ is an ideal of \mathbb{Z} .

(\because) Let $r \in \mathbb{Z}, x \in n\mathbb{Z} \implies x = nk$ for some $k \in \mathbb{Z}$. $xr = rx = r(nk) = (rn)k = (nr)k \in n\mathbb{Z}$.

$\therefore n\mathbb{Z}$ is an ideal of \mathbb{Z} .

Ideal Subring Test (Theorem 2.23):

Let R be a ring and $\emptyset \neq I \subseteq R$. Then, I is an ideal if and only if the following hold:

1. $\forall a, b \in I, a - b \in I$,
2. $\forall r \in R, a \in I, ra \in I$ and $ar \in I$.

Principal Ideal

Let R be a commutative ring with unity. Fix $a \in R$. Consider $\{ar \mid r \in R\} =: \langle a \rangle = I$

- $a \cdot 1 = a \in I$ so $I \neq \emptyset$.
- Let $x, y \in I \implies x = ar_1, y = ar_2$ for some $r_1, r_2 \in R$.

$$x - y = ar_1 - ar_2 = a \underbrace{(r_1 - r_2)}_{\in R} \in I.$$

- Let $r \in R, x \in I \implies x = ar_1$ for some $r_1 \in R$.

$$xr = rx = r(ar_1) = (ra)r_1 = (ar)r_1 = a(rr_1) \in I.$$

$\therefore I$ is an ideal of R .

I is called the *principal ideal generated by a* , denoted (a) or $\langle a \rangle$.

Example:

1. \mathbb{Z} . Let $n \in \mathbb{Z}$. The principal ideal of \mathbb{Z} generated by n

$$\langle n \rangle = \{n \cdot k \mid k \in \mathbb{Z}\} = n\mathbb{Z}$$

Factor Rings

Concept:

Consider S , subring of R . $\langle S, + \rangle$ is a(n) (abelian) subgroup of the abelian group $\langle R, + \rangle$. So, $S \trianglelefteq R$.

$R/S = \{r + S \mid r \in R\}$ is an abelian group under addition of left cosets.

(*) Define multiplication of left cosets as follows:

$$(r_1 + S)(r_2 + S) = (r_1 r_2) + S$$

Note: It is not well-defined on some cases.

Lemma 2.24:

Let R be a ring and I an ideal of R . Then, multiplication of left cosets of I is a well-defined operation on the set $R/I = \{a + I \mid a \in R\}$.

Proof. Suppose $a + I = c + I$ and $b + I = d + I$ for some $a, b, c, d \in R$.

(WTS: $(a + I)(b + I) = (c + I)(d + I) \implies ab + I = cd + I \implies -ab + cd \in I$)

$$\begin{aligned} a + I = c + I &\iff -a + c \in I \\ &\iff -a + c = x, \exists x \in I \\ &\implies c = a + x \end{aligned}$$

$$\begin{aligned} b + I = d + I &\iff -b + d \in I \\ &\iff -b + d = y, \exists y \in I \\ &\implies d = b + y \end{aligned}$$

Now,

$$\begin{aligned} cd &= (a + x)(b + y) \\ &= a(b + y) + x(b + y) \\ &= ab + ay + xb + xy \\ &\implies -ab + cd = \underbrace{\underbrace{a}_{R} \underbrace{y}_{I}}_I + \underbrace{\underbrace{x}_{I} \underbrace{b}_{R}}_I + \underbrace{\underbrace{xy}_{I}}_I \in I \end{aligned}$$

\therefore multiplication of left cosets is well-defined. ■

Theorem 2.25:

Let I be an ideal of a ring R . Then, R/I is a ring under addition and multiplication of left cosets

Proof. Note that addition and multiplication of left cosets are binary operators in R/I

\mathcal{R}_1 : R/I is an abelian group under addition of left cosets.

\mathcal{R}_2 : Let $a + I, b + I, c + I \in R/I$.

$$\begin{aligned}(a + I)[(b + I)(c + I)] &= (a + I)(bc + I) \\ &= a(bc) + I \\ &= (ab)c + I \\ &= (ab + I)(c + I) = [(a + I)(b + I)](c + I)\end{aligned}$$

\mathcal{R}_3 : Let $a + I, b + I, c + I \in R/I$.

$$\begin{aligned}(a + I)[(b + I) + (c + I)] &= (a + I)[(b + c) + I] \\ &= a(b + c) + I \\ &= (ab + ac) + I \\ &= (ab + I) + (ac + I) \\ [(a + I) + (b + I)](c + I) &= [(a + b) + I](c + I) \\ &= (a + b)c + I \\ &= (ac + bc) + I \\ &= (ac + I) + (bc + I)\end{aligned}$$

$\therefore R/I$ is a ring under addition and multiplication of left cosets. ■

Remark:

R/I is called the factor ring or *quotient ring* of R *modulo* I .

Remarks:

1. If R is commutative, then R/I is commutative.
2. If R has unity 1, then R/I has unity $1 + I$.

Examples:

- $\mathbb{Z}/3\mathbb{Z} = \{3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\}$

+	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$3\mathbb{Z}$	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$1 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$3\mathbb{Z}$
$2 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$

·	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$3\mathbb{Z}$	$3\mathbb{Z}$	$3\mathbb{Z}$	$3\mathbb{Z}$
$1 + 3\mathbb{Z}$	$3\mathbb{Z}$	$1 + 3\mathbb{Z}$	$2 + 3\mathbb{Z}$
$2 + 3\mathbb{Z}$	$3\mathbb{Z}$	$2 + 3\mathbb{Z}$	$1 + 3\mathbb{Z}$

$\mathbb{Z}/3\mathbb{Z}$ is commutative and has unity $1 + 3\mathbb{Z}$. $(1 + 3\mathbb{Z})^{-1} = 1 + 3\mathbb{Z}$, $(2 + 3\mathbb{Z})^{-1} = 2 + 3\mathbb{Z}$

$\therefore \mathbb{Z}/3\mathbb{Z}$ is a field.

- Consider $8\mathbb{Z} \subseteq 2\mathbb{Z}$. $8\mathbb{Z}$ is an ideal of $2\mathbb{Z}$. (Theorem 2.23)

(a) $2\mathbb{Z}/8\mathbb{Z} = \{8\mathbb{Z}, 2 + 8\mathbb{Z}, 4 + 8\mathbb{Z}, 6 + 8\mathbb{Z}\}$

(b)

+	$8\mathbb{Z}$	$2 + 8\mathbb{Z}$	$4 + 8\mathbb{Z}$	$6 + 8\mathbb{Z}$
$8\mathbb{Z}$	$8\mathbb{Z}$	$2 + 8\mathbb{Z}$	$4 + 8\mathbb{Z}$	$6 + 8\mathbb{Z}$
$2 + 8\mathbb{Z}$	$2 + 8\mathbb{Z}$	$4 + 8\mathbb{Z}$	$6 + 8\mathbb{Z}$	$8\mathbb{Z}$
$4 + 8\mathbb{Z}$	$4 + 8\mathbb{Z}$	$6 + 8\mathbb{Z}$	$8\mathbb{Z}$	$2 + 8\mathbb{Z}$
$6 + 8\mathbb{Z}$	$6 + 8\mathbb{Z}$	$8\mathbb{Z}$	$2 + 8\mathbb{Z}$	$4 + 8\mathbb{Z}$

\cdot	$8\mathbb{Z}$	$2 + 8\mathbb{Z}$	$4 + 8\mathbb{Z}$	$6 + 8\mathbb{Z}$
$8\mathbb{Z}$	$8\mathbb{Z}$	$8\mathbb{Z}$	$8\mathbb{Z}$	$8\mathbb{Z}$
$2 + 8\mathbb{Z}$	$8\mathbb{Z}$	$4 + 8\mathbb{Z}$	$8\mathbb{Z}$	$4 + 8\mathbb{Z}$
$4 + 8\mathbb{Z}$	$8\mathbb{Z}$	$8\mathbb{Z}$	$8\mathbb{Z}$	$8\mathbb{Z}$
$6 + 8\mathbb{Z}$	$8\mathbb{Z}$	$4 + 8\mathbb{Z}$	$8\mathbb{Z}$	$4 + 8\mathbb{Z}$

(c) $2\mathbb{Z}/8\mathbb{Z}$ is not an integral domain.

Ring Homomorphism

Definition:

A ring homomorphism from a ring R to a ring R' is a mapping ϕ from R to R' that preserves both ring operations, that is,

$$\forall a, b \in R, \phi(a + b) = \phi(a) + \phi(b) \text{ and } \phi(ab) = \phi(a)\phi(b).$$

Remarks:

Let $\phi : R \rightarrow R'$ be a ring homomorphism.

1. If ϕ is one-to-one, we call ϕ a ring monomorphism.
2. If ϕ is onto, we call ϕ a ring epimorphism.
3. If ϕ is a bijection, then ϕ is called a ring isomorphism.
4. If ϕ is bijective and $R' = R$, then ϕ is called a ring automorphism.

Definition:

Two rings R and R' are said to be isomorphic, written $R \cong R'$, if there exists an isomorphism from R to R' .

Remarks:

If $\phi : R \rightarrow R'$ is a ring homomorphism, then $\phi : \langle R, + \rangle \rightarrow \langle R', + \rangle$ is a group homomorphism. In particular,

1. If 0 and $0'$ are the zero elements of R and R' , then $\phi(0) = 0'$.
2. If $a \in R$, then $\phi(-a) = -\phi(a)$.
3. If $a \in R$ and $n \in \mathbb{Z}$, then $\phi(na) = n\phi(a)$.

Properties of Ring Homomorphisms (Theorem 2.26):

1. If $a \in R$ and $n \in \mathbb{N}$, then $\phi(an) = [\phi(a)]n$.
2. If S is a subring of R , then $\phi(S) = \{\phi(a) \mid a \in S\}$ is a subring of R' .
3. If R is commutative, then $\phi(R)$ is commutative.
4. If I is an ideal of R , then $\phi(I)$ is an ideal of the ring $\phi(R)$ (but not necessarily of R').
5. If S' is a subring of R' , then $\phi^{-1}(S') = \{a \in R \mid \phi(a) \in S'\}$ is a subring of R .
6. Let R be a ring with unity 1_R .
 1. Then $\phi(R)$ is a ring with unity $\phi(1_R)$.
 2. If a is a unit in R , then $\phi(a)$ is a unit in the ring $\phi(R)$ with $[\phi(a)]^{-1} = \phi(a^{-1})$.

Proof. (Exercise!)

5. Suppose S' is a subring of R' . Show: $\phi^{-1}(S')$ is a subring of R .

Note that $\langle S', + \rangle$ is a subgroup of $\langle R', + \rangle$. Since ϕ is a group homomorphism, $\langle \phi^{-1}(S'), + \rangle$ is a subgroup of $\langle R, + \rangle$.

It remains to be shown that $\phi^{-1}(S')$ is closed under multiplication.

Let $x, y \in \phi^{-1}(S')$. WTS: $xy \in \phi^{-1}(S')$, i.e. $\phi(xy) \in \phi^{-1}(S')$.

Now, $x, y \in \phi^{-1}(S') \Rightarrow \phi(x), \phi(y) \in S' \Rightarrow \phi(xy) = \phi(x)\phi(y) \in S'$

Since S' is a subring of R' . Thus $xy \in \phi^{-1}(S')$. $\therefore \phi^{-1}(S')$ is a subring of R .

Examples:

1. Consider the map $\phi : \mathbb{Z} \rightarrow 2\mathbb{Z}$ given by $\phi(k) = 2k$.

Let $a, b \in \mathbb{Z}$. Then

- $\phi(a + b) = 2(a + b) = 2a + 2b = \phi(a) + \phi(b)$
- $\phi(ab) = 2ab$ but $\phi(a)\phi(b) = (2a)(2b) = 4ab$

Thus ϕ is not ring homomorphism.

2. Consider the map $\phi : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ given by $\phi(x) = (x, 0)$. Then ϕ is a ring homomorphism. (Why?)

$\phi(\mathbb{Z}) = \{(x, 0) \mid x \in \mathbb{Z}\}$ is a commutative ring with unity (unity in $\phi(\mathbb{Z})$ is $\phi(1) = (1, 0)$). The units of $\phi(\mathbb{Z})$ are $\phi(1) = (1, 0)$ and $\phi(-1) = (-1, 0)$.

Kernel of a Homomorphism

Definition:

Let R, R' be rings with $0'$, the zero element in R' . Let $\phi : R \rightarrow R'$ be a ring homomorphism. The kernel of ϕ is the set

$$\ker \phi := \{a \in R \mid \phi(a) = 0'\} = \phi^{-1}(\{0'\})$$

Remarks:

1. ϕ is one-to-one if and only if $\ker \phi = \{0\}$.
2. ϕ is a ring isomorphism if and only if ϕ is onto and $\ker \phi = \{0\}$.
3. If $a \in R$ and $\phi(a) = a'$ then

$$\phi^{-1}(a') = \{r \in R \mid \phi(r) = a'\} = a + \ker \phi$$

The Kernel is an Ideal (Theorem 2.27):

Let $\phi : R \rightarrow R'$ be a ring homomorphism. Then $\ker \phi$ is an ideal of R .

Proof. Let $0'$ be the zero element of R' . Since $\{0'\}$ is a subring of R' , then $\phi^{-1}(\{0'\}) = \ker \phi$ is a subring of R (by Theorem 2.26).

Let $a \in \ker \phi$ and $r \in R$. (WTS: ar and ra are in $\ker \phi$)

$$\phi(ar) = \phi(a)\phi(r) = 0' \cdot \phi(r) = 0'$$

Since $\phi(ar) = 0'$, then $ar \in \ker \phi$.

Using a similar argument, we can show that $ra \in \ker \phi$.

$\therefore \ker \phi$ is an ideal of R .

First Isomorphism Theorem for Rings (Theorem 2.28):

Let $\phi : R \rightarrow R'$ be a ring homomorphism. Then

$$\mu : R / \ker \phi \rightarrow \phi(R)$$

given by $\mu(a + \ker \phi) = \phi(a)$ is a ring isomorphism. In particular, $R / \ker \phi \cong \phi(R)$ (as rings).

Proof. It follows from the First Isomorphism Theorem for Groups that μ is a group isomorphism. (WTS: μ preserves multiplication.)

Let $a + \ker \phi, b + \ker \phi \in R / \ker \phi$. Then,

$$\begin{aligned}\mu[(a + \ker \phi)(b + \ker \phi)] &= \mu(ab + \ker \phi) \\ &= \phi(ab) = \phi(a)\phi(b) \\ &= \mu(a + \ker \phi)\mu(b + \ker \phi)\end{aligned}$$

$\therefore \mu$ is a ring isomorphism.

Remark:

The isomorphism μ is called the *natural* or *canonical isomorphism* from $R / \ker \phi$ to $\phi(R)$.

Examples:

1. Let $\phi : \mathbb{Z} \rightarrow \mathbb{Z}_n$ be the mapping such that $\phi(m) =$ the remainder when m is divided by n . Then ϕ is a ring epimorphism. (Verify this!)

$$\ker \phi = n\mathbb{Z}$$

By the FITR,

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z} / \ker \phi \cong \phi(\mathbb{Z}) = \mathbb{Z}_n$$

Thus,

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n \text{ as rings.}$$

2. Consider the ring homomorphism $\phi : \mathbb{Z} \rightarrow \mathbb{Z} \times \mathbb{Z}$ where $\phi(x) = (x, 0)$.

$$\ker \phi = \{0\}$$

By the FITR,

$$\mathbb{Z}/\{0\} = \mathbb{Z} / \ker \phi \cong \phi(\mathbb{Z}) = \{(x, 0) \mid x \in \mathbb{Z}\}$$

Noting that $\mathbb{Z}/\{0\} \cong \mathbb{Z}$, we get

$$\mathbb{Z} \cong \{(x, 0) \mid x \in \mathbb{Z}\}$$

Canonical Isomorphism from R to R/I (Theorem 2.29):

Let I be an ideal of a ring R . Then $\gamma : R \rightarrow R/I$ given by $\gamma(a) = a + I$ is a ring homomorphism with $\ker \gamma = I$.

Proof. It follows from Theorem 2.12 that γ is a group homomorphism with $\ker \gamma = I$. (WTS: γ preserves multiplication.)

Let $a, b \in R$. Then $\gamma(ab) = ab + I = (a + I)(b + I) = \gamma(a)\gamma(b)$.

$\therefore \gamma$ is a ring homomorphism.

Ideals and Factor Rings (Part II)

Concept:

Given: R , a commutative ring with unity.

I , ideal of $R \implies R/I$ is a commutative ring with unity

- *Question 1:* If R is a field, what are the possible factor rings R/I ?
- *Question 2:* When is the factor ring R/I a field?
- *Question 3:* When is the factor ring R/I an integral domain?

Ideals of a Field (Theorem 2.30):

Let R be a ring with unity 1 and let I be an ideal of R . If I contains a unit of R then $I = R$.

Proof. Suppose $u \in I$ is a unit of R . Then $\exists u^{-1} \in R$ such that $1 = u^{-1}u \in I$ since I is an ideal of R . Thus $1 \in I$.

Clearly $I \subseteq R$. (NTS: $R \subseteq I$). Let $r \in R$. Now, $r = r \cdot 1 \in I$ since I is an ideal of R . Thus $R \subseteq I$ and so $I = R$.

Corollary 2.31:

A field has no proper nontrivial ideals. That is, the only ideals of a field F are $\{0\}$ or F itself.

Proof. Let F be a field and I an ideal of F . Note that either I is trivial (that is $I = \{0\}$) or I is nontrivial. Suppose $I \neq \{0\}$. Let $0 \neq a \in I \subseteq F$. Thus a is a unit of F . Hence $I = F$.

Remark:

Let F be a field and I an ideal of F . Then either $I = \{0\}$ or $I = F$. Then the factor rings F/I are

- $F/\{0\} \cong F$
- $F/F \cong \{0\}$

Maximal Ideals

Definition:

A proper ideal M of a ring R is said to be maximal if whenever J is an ideal of R such that $M \subseteq J \subseteq R$, either $J = M$ or $J = R$.

Examples:

$3\mathbb{Z}$ and $4\mathbb{Z}$ are ideals of \mathbb{Z} .

- Note that $4\mathbb{Z} \subset 2\mathbb{Z} \subset \mathbb{Z}$. Thus $4\mathbb{Z}$ is not a maximal ideal of \mathbb{Z} .
- Suppose $n\mathbb{Z}$ is an ideal of \mathbb{Z} such that $3\mathbb{Z} \subseteq n\mathbb{Z} \subseteq \mathbb{Z}$. Since $3 \in 3\mathbb{Z} \subseteq n\mathbb{Z}$, then $n \mid 3$. Hence $n = 3$ or $n = 1$. So $n\mathbb{Z} = 3\mathbb{Z}$ or $n\mathbb{Z} = \mathbb{Z}$. Thus $3\mathbb{Z}$ is a maximal ideal of \mathbb{Z} .

Remarks:

Let R be a ring.

1. The only ideal that properly contains a maximal ideal of R is R .
2. A maximal ideal of R may not be unique. That is, R may have more than one maximal ideal. (e.g. $2\mathbb{Z}$ and $5\mathbb{Z}$ are both maximal ideals of \mathbb{Z})

Examples:

The ideals of \mathbb{Z}_{12} :

- \mathbb{Z}_{12}
- $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$
- $\langle 3 \rangle = \{0, 3, 6, 9\}$
- $\langle 4 \rangle = \{0, 4, 8\}$
- $\langle 6 \rangle = \{0, 6\}$
- $\{0\}$

Is $\langle 4 \rangle$ a maximal ideal of \mathbb{Z}_{12} ?

Is $\langle 4 \rangle$ a maximal ideal of $\langle 2 \rangle$?

What are the maximal ideals of \mathbb{Z}_{12} ?

Factor Rings from Maximal Ideals are Fields (Theorem 2.32):

Let R be a commutative ring with unity and let I be an ideal of R . Then

$$R/I \text{ is a field} \iff I \text{ is a maximal ideal of } R.$$

Proof. (\implies) Suppose R/I is a field. Let J be an ideal of R such that $I \subseteq J \subseteq R$.
(NTS: Either $J = I$ or $J = R$).

Suppose $J \neq I$. Then $\exists b \in J/I \implies I \neq b + I \in R/I \implies b + I$ is a unit in $R/I \implies \exists (a + I) \in R/I$ such that $(b + I)(a + I) = 1 + I \implies -ba + 1 \in I \subset J$.

Thus $1 = ba + (-ba + 1) \in J \implies J = R$.

$\therefore I$ is a maximal ideal of R .

(\impliedby) Suppose I is a maximal ideal of R . Since R is commutative with unity, then so is R/I . Note also that $I \neq R$ since I is maximal and so $1 \notin I$. Thus $1 + I \neq I$.

(NTS: Every nonzero element of R/I is a unit.)

Let $a + I$ be a nonzero element in R/I (i.e. $a \in R$ but $a \notin I$).

Form $J := \{ra + b \mid r \in R, b \in I\}$. Claim: J is an ideal of R . If $x \in I$ then $x = 0 \cdot a + x \in J \implies I \subseteq J \subseteq R \implies J = I \vee J = R$. However, $a \notin I$ but $a = 1 \cdot a + 0 \in J \implies J \neq I$. Thus $J = R$.

Now, $1 \in R = J \implies 1 = ra + b$ for some $r \in R, b \in I$

$$\begin{aligned}
&\Rightarrow -ra + 1 = b \in I \\
&\Rightarrow ra + I = 1 + I \\
&\Rightarrow (r + I)(a + I) = (a + I)(r + I) = 1 + I \\
&\Rightarrow a + I \text{ is a unit.}
\end{aligned}$$

$\therefore R/I$ is a field.

Proof of claim that J is an ideal of R :

Claim: $J = \{ra + b \mid r \in R, b \in I\}$ is an ideal of R .

Proof:

- J is nonempty: $0 = 0 \cdot a + 0 \in J \Rightarrow J \neq \emptyset$
- If $x, y \in J$, show that $x - y \in J$. (Exercise!)
- If $s \in R$ and $x \in J$, show that $sx \in J$ and $xs \in J$.

$\because x \in J \Rightarrow x = ra + b$ for some $r \in R, b \in I$. So $sx = s(ra + b) = (sr)a + sb \in J$.

Note that R is commutative so $xs = sx \in J$. ■

Application of Theorem 2.32:

Consider the ideals $3\mathbb{Z}$ and $4\mathbb{Z}$ of \mathbb{Z} .

- $\mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}_3$ is a field, thus $3\mathbb{Z}$ is a maximal ideal of \mathbb{Z} .
- $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$ is not a field, thus $4\mathbb{Z}$ is not a maximal ideal of \mathbb{Z} .

Remark:

$n\mathbb{Z}$ is a maximal ideal of \mathbb{Z} if and only if n is prime.

Converse of Corollary 2.31 holds (Corollary 2.33):

A commutative ring with unity is a field if and only if it has no proper nontrivial ideals.

Proof.

(\Rightarrow) Follows from Corollary 2.31.

(\Leftarrow) Suppose a commutative ring R with unity has no proper nontrivial ideals. Then $\{0\}$ is a maximal ideal. Thus $R \cong R/\{0\}$ is a field.

Prime Ideals

Definition:

A proper ideal P of a commutative ring R is said to be prime if whenever $a, b \in R$ such that $ab \in P$ then either $a \in P$ or $b \in P$.

Examples:

1. Consider $6\mathbb{Z}$. Note that $2 \cdot 3 \in 6\mathbb{Z}$ but neither 2 nor 3 are in $6\mathbb{Z}$. Thus $6\mathbb{Z}$ is not a prime ideal of \mathbb{Z} .

2. Consider the trivial ideal $\{0\} \in \mathbb{Z}_{12}$. Is $\{0\}$ a prime ideal of \mathbb{Z}_{12} ?
 3. $\{0\}$ is a prime ideal of an integral domain D .
- \therefore Let $a, b \in D$ such that $ab \in \{0\} \implies ab = 0 \implies a = 0$ or $b = 0 \implies a \in \{0\}$ or $b \in \{0\}$.

Factor Rings from Prime Ideals (Theorem 2.34):

Let R be a commutative ring with unity and let I be an ideal of R . Then

$$R/I \text{ is an integral domain} \iff I \text{ is a prime ideal of } R.$$

Proof.

(\implies) Suppose R/I is an integral domain. Let $a, b \in R$ such that $ab \in I$. Then $ab + I = I \implies (a + I)(b + I) = I$. Since R/I is an integral domain, either $a + I = I$ or $b + I = I$, which means that either $a \in I$ or $b \in I$.

(\impliedby) Suppose I is a prime ideal of R . Since R is a commutative ring with unity 1, then so is R/I . Note also that $I \neq R$ since I is prime and so $1 \notin I$. Thus $1 + I \neq I$. (NTS: R/I has no zero divisors.)

Let $a + I, b + I \in R/I$ such that $(a + I)(b + I) = I$. Then, $ab + I = I \implies ab \in I$. Since I is prime, then either $a \in I$ or $b \in I \implies a + I = I$ or $b + I = I$.

$\therefore R/I$ is an integral domain.

Applications of Theorem 2.34:

1. $\mathbb{Z}/4\mathbb{Z} \cong \mathbb{Z}_4$ is not an integral domain. Thus $4\mathbb{Z}$ is not a prime ideal of \mathbb{Z} . Indeed $2 \cdot 2 \in 4\mathbb{Z}$ but $2 \notin 4\mathbb{Z}$.

Remark: $n\mathbb{Z}$ is a prime ideal of \mathbb{Z} if and only if n is prime.

2. Let $I = \{(x, 0) \mid x \in \mathbb{Z}\} \subseteq \mathbb{Z} \times \mathbb{Z}$. Then I is an ideal of $\mathbb{Z} \times \mathbb{Z}$. (Exercise!)

Suppose $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}$ such that $(a, b)(c, d) = (ac, bd) \in I$. Then $bd = 0 \implies b = 0$ or $d = 0 \implies (a, b) \in I$ or $(c, d) \in I$. Hence I is prime. Thus $(\mathbb{Z} \times \mathbb{Z})/I$ is an integral domain.

(Exercise:) Use FITR (First Isomorphism Theorem for Rings) to show that $(\mathbb{Z} \times \mathbb{Z})/I \cong \mathbb{Z}$.

Maximal Ideals are Prime Ideals (Corollary 2.35):

Every maximal ideal of a commutative ring R with unity is a prime ideal of R .

Proof. Let I be a maximal ideal of R . By Theorem 2.32, R/I is a field. Hence R/I is an integral domain. Thus I is a prime ideal of R . ■

Remarks:

1. The converse of Corollary 2.35 does not hold. That is, a prime ideal of a commutative ring R with unity may not be a maximal ideal of R .

e.g., $I = \{(x, 0) \mid x \in \mathbb{Z}\}$ is a prime ideal of $\mathbb{Z} \times \mathbb{Z}$ which is not a maximal ideal of $\mathbb{Z} \times \mathbb{Z}$.
(Why?)

2. Corollary 2.35 does not hold if R has no unity.

e.g. $2\mathbb{Z}$ has no unity and $4\mathbb{Z}$ is a maximal ideal of $2\mathbb{Z}$ but $4\mathbb{Z}$ is not a prime ideal of $2\mathbb{Z}$.
(Why?)

Field of Quotients of Integral Domains and Prime Fields

R with unity contains a homomorphic image of \mathbb{Z} (Lemma 2.36):

Let R be a ring with unity 1. The mapping $\phi : \mathbb{Z} \rightarrow R$ given by $\phi(m) = m \cdot 1$ is a ring homomorphism.

Proof. Let $m, n \in \mathbb{Z}$. Then

$$\begin{aligned}\phi(m + n) &= (m + n) \cdot 1 = m \cdot 1 + n \cdot 1 = \phi(m) + \phi(n) \\ \phi(mn) &= (mn) \cdot 1 = (mn) \cdot 1 \cdot 1 = (m \cdot 1)(n \cdot 1) = \phi(m)\phi(n)\end{aligned}$$

Remark:

Note that $\phi(\mathbb{Z})$ is a subring of R .

The Characteristic of Rings with Unity

$\text{char } R$ = smallest positive integer n such that $n \cdot a = 0$ for all $a \in R$.

If no such positive integer exists, then $\text{char } R = 0$.

Recall: R , a ring with unity 1

- $\text{char } R = n \iff |1| = n$ in the group $\langle R, + \rangle$
- $\text{char } R = 0 \iff 1$ has infinite order in the group $\langle R, + \rangle$

Structure of R based on its Characteristic (Theorem 2.37)

Let R be a ring with unity.

1. $\text{char } R = n > 1 \implies R$ contains a subring isomorphic to \mathbb{Z}_n
2. $\text{char } R = 0 \implies R$ contains a subring isomorphic to \mathbb{Z}

Proof. Consider the ring homomorphism $\phi : \mathbb{Z} \rightarrow R$ given by $\phi(m) = m \cdot 1$.

By the FITR, $\mathbb{Z}/\ker \phi \cong \phi(\mathbb{Z})$.

Note that $\ker \phi = \{m \in \mathbb{Z} \mid \phi(m) = 0\} = \{m \in \mathbb{Z} \mid m \cdot 1 = 0\}$.

- Suppose $\text{char } R = n > 1$. So $|1| = n$. That is, $n \cdot 1 = 0$ and

$$m \cdot 1 = 0 \iff n \mid m \iff m \in n\mathbb{Z}.$$

Thus $\ker \phi = n\mathbb{Z}$. Hence by FITR,

$$\phi(\mathbb{Z}) \cong \mathbb{Z}/\ker \phi = \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n.$$

- Suppose $\text{char } R = 0$. Then 1 has infinite order. Thus $m \cdot 1 = 0 \iff m = 0$. Thus $\ker \phi = \{0\}$. Hence by FITR,

$$\phi(\mathbb{Z}) \cong \mathbb{Z}/\ker \phi = \mathbb{Z}/\{0\} \cong \mathbb{Z}.$$

Examples:

Consider the ring $R = M_2(\mathbb{R})$ with unity $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Note that the order of $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is infinite. (Why?)

Hence $\text{char } M_2(\mathbb{R}) = 0$.

Thus $M_2(\mathbb{R})$ has a subring isomorphic to \mathbb{Z} by Theorem 2.37. This subring is $\phi(\mathbb{Z})$ where $\phi : \mathbb{Z} \rightarrow M_2(\mathbb{R})$ is given by

$$\phi(m) = m \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} m & 0 \\ 0 & m \end{bmatrix}$$

Thus

$$\phi(\mathbb{Z}) = \{\phi(m) \mid m \in \mathbb{Z}\} = \left\{ \begin{bmatrix} m & 0 \\ 0 & m \end{bmatrix} \mid m \in \mathbb{Z} \right\} \cong \mathbb{Z}$$

Field of Quotients of an Integral Domain

Consider the integral domain \mathbb{Z} .

Note that \mathbb{Z} is not a field. But \mathbb{Z} is a subring of the field \mathbb{Q} .

- *Question:* Given any integral domain D , is there a field F that contains D ? If so, what is the smallest field that will contain D ?

Construction of \mathbb{Q} from \mathbb{Z} :

$$\mathbb{Z}'' \subset \{(a, b) \mid a, b \in \mathbb{Z}, b \neq 0\} \longrightarrow \mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$$

$$(a, b) + (c, d) = (ad + bc, bd) \longrightarrow \frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$$(a, b)(c, d) = (ac, bd) \longrightarrow \left(\frac{a}{b}\right)\left(\frac{c}{d}\right) = \frac{ac}{bd}$$

$$(1, 2), (2, 4), (3, 6) \cdots \longrightarrow \frac{1}{2}$$

$$(a, b) \sim (c, d) \iff ad = bc \longrightarrow \frac{a}{b} = \frac{c}{d} \iff ad = bc$$

Theorem 2.38:

Let D be an integral domain. Then there exists a field that contains a subring which is isomorphic to D .

Proof. Consider $S = \{(a, b) \mid a, b \in D, b \neq 0\} \subset D \times D$.

Define the relation on S by $(a, b) \sim (c, d) \iff ad = bc$.

Claim 1: \sim is an equivalence relation on S . (Exercise!) Denote the equivalence class of (a, b) by $[a, b]$.

Note that $[a, b] = [c, d] \iff ad = bc$

Let $F := \{[a, b] \mid (a, b) \in S\}$

Define the following operations on F :

$$\text{addition : } [a, b] + [c, d] = [ad + bc, bd]$$

$$\text{multiplication : } [a, b] \cdot [c, d] = [ac, bd]$$

Claim 2: The defined operations are well-defined binary operations on F . (Exercise!)

Claim 3:

- a. If $0 \neq b \in D$ then $[0, b] = [0, 1]$.
- b. If $0 \neq k \in D$ and $[a, b] \in F$ then $[ka, kb] = [a, b]$.
- c. If $0 \neq a \in D$ then $[a, a] = [1, 1]$

(Exercise!)

We now show that F is a field.

F is a ring:

$\mathcal{R}_1: \langle F, + \rangle$ is an abelian group.

- $+$ is commutative: Let $[a, b], [c, d] \in F$.

$$[a, b] + [c, d] = [ad + bc, bd] = [cb + da, db] = [c, d] + [a, b]$$

- $+$ is associative: (Exercise!)
- additive identity: Consider $[0, 1] \in F$. For any $[a, b] \in F$,

$$[0, 1] + [a, b] = [a, b] + [0, 1] = [a \cdot 1 + b \cdot 0, b \cdot 1] = [a, b]$$

- additive inverse: Let $[a, b] \in F$. Its additive inverse is $[-a, b]$ since

$$[a, b] + [-a, b] = [-a, b] + [a, b] = [-ab + ab, b^2] = [0, b^2] = [0, 1]$$

\mathcal{R}_2 : Multiplication is associative. (Exercise!)

\mathcal{R}_3 : Left and Right Distributive Laws: (Exercise!) (Hint: You may need to use Claim 3(b).)

F is commutative: Given $[a, b], [c, d] \in F$,

$$[a, b][c, d] = [ac, bd] = [ca, db] = [c, d][a, b]$$

F has unity: unity in F is $[1, 1]$ since $[a, b][1, 1] = [1, 1][a, b] = [a, b] \forall [a, b] \in F$.

Clearly, $[1, 1] \neq [0, 1]$. ($\because 1 \cdot 16 = 1 \cdot 0$.)

F is a division ring: Let $[a, b] \in F$ such that $[a, b] \neq [0, 1]$. Then $a \cdot 1 \neq b \cdot 0 \implies a \neq 0 \implies [b, a] \in F$. Note that $[a, b][b, a] = [ab, ba] = [ab, ab] = [1, 1]$. Thus $[a, b]^{-1} = [b, a]$.

$\therefore F$ is a field under the operations addition and multiplication as defined.

Lastly, we show that F contains a subring which is isomorphic to D .

Consider $\phi : D \rightarrow F$ given by $\phi(a) = [a, 1]$. Let $a, b \in D$. Then $\phi(a) + \phi(b) = [a, 1] + [b, 1] = [a + b, 1] = \phi(a + b)$ and $\phi(a)\phi(b) = [a, 1][b, 1] = [ab, 1] = \phi(ab)$

Thus, ϕ is a ring homomorphism.

Note that $\ker \phi = \{a \in D \mid \phi(a) = [0, 1]\} = \{a \in D \mid [a, 1] = [0, 1]\}$. But $[a, 1] = [0, 1] \iff a \cdot 1 = 1 \cdot 0 \iff a = 0$. Thus $\ker \phi = \{0\}$. So by the FITR,

$$\phi(D) \cong D / \ker \phi = D / \{0\} \cong D$$

$\therefore D$ is isomorphic to $\phi(D) = \{[a, 1] \mid a \in D\}$ which is a subring of F .

Remarks:

1. The field F in Theorem 2.38 is called the field of quotients of D .
2. We say that the integral domain D is embedded in its field of quotients F and we write $D \hookrightarrow F$.

Example:

1. \mathbb{Q} is the field of quotients of \mathbb{Z} .

Theorem 2.39:

Let D be an integral domain and F its field of quotients. Suppose K is a field that contains D . Then K contains a subfield L such that $D \subseteq L \subseteq K$ and L is isomorphic to F .

Remark:

The field of quotients F of D is the smallest field that contains D and is unique (up to isomorphism).

Proof. Let $[a, b] \in F$. Then $a, b \in D$ and $b \neq 0$. Thus $a, b \in K$ and b is a unit in K .

Define $\phi : F \rightarrow K$ given by $\phi([a, b]) = ab^{-1}$. Then ϕ is a well-defined monomorphism. (Exercise!)

Set $L = \phi(F)$. By FITR,

$$L = \phi(F) \cong F / \ker \phi = F / \{0\} \cong F$$

Thus L is a subfield of K which is isomorphic to F . For every $a \in D$, $a = a \cdot 1 = a \cdot 1 - 1 = \phi([a, 1])$. Thus $D \subseteq L \subseteq K$.

Prime Subfield of a Field

Recall: The characteristic of an integral domain is either 0 or prime p .

Theorem 2.40:

Let F be a field.

1. F is of prime characteristic $p \implies F$ contains a subfield isomorphic to \mathbb{Z}_p
2. F is of characteristic 0 $\implies F$ contains a subfield isomorphic to \mathbb{Q} .

Proof.

1. Since $\text{char } F = p$, F contains a subring S isomorphic to \mathbb{Z}_p .

Since p is prime, \mathbb{Z}_p is a field. Thus S is a subfield of F isomorphic to \mathbb{Z}_p .

2. If $\text{char } F$ is 0, then F contains a subring S isomorphic to \mathbb{Z} . So S is an integral domain contained in the field F . By Theorem 2.39, F contains a subfield L which is isomorphic to the field of quotients F_S of S .

Since $S \cong \mathbb{Z}$, $F_S \cong \mathbb{Q}$. Thus $L \cong \mathbb{Q}$.

Definition:

The subfield of a field F that is isomorphic to either \mathbb{Z}_p or \mathbb{Q} is called a prime subfield of F .

Remark:

A prime subfield of F is the smallest subfield of F . Equivalently, every subfield of F must contain the prime subfield of F .

Examples:

1. Identify the prime subfield of the field $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.
2. Suppose F is a field with 81 elements. The prime subfield of F is isomorphic to which field?

Solution:

1. The unity in $\mathbb{Q}(\sqrt{2})$ is 1. Since order of 1 is infinite $\implies \text{char } \mathbb{Q}(\sqrt{2}) = 0$. Thus the prime subfield of $\mathbb{Q}(\sqrt{2})$ is \mathbb{Q} .
2. Note: order of $\langle F, + \rangle$ is 81.

$$\text{order of } 1 = \text{char } F = p \text{ for some prime } p \implies p \text{ divides } 81 = 3^4 \implies p = 3$$

Thus the prime subfield of F is isomorphic to \mathbb{Z}_3 .