

18.1. homomorphisms.

Definition 18.12. A **ring homomorphism** is a mapping $\phi : R \rightarrow S$ between two rings R and S so that

- (1) ϕ is a homomorphism of additive group.

$$\phi(x + y) = \phi(x) + \phi(y) \quad \forall x, y \in R$$

- (2) ϕ takes multiplication in R to multiplication in S :

$$\phi(xy) = \phi(x)\phi(y)$$

I will say ϕ is **multiplicative** for short.

The **kernel** of ϕ is defined to be

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

A ring homomorphism always takes 0 to 0. Why?

However, it might not take unity to unity. For example, take the mapping:

$$\phi : \mathbb{Z}_2 \rightarrow \mathbb{Z}_6$$

given by $\phi(0) = 0$ and $\phi(1) = 3$. This is a homomorphism of additive groups since the order of 3 in \mathbb{Z}_6 is 2. It is also multiplicative since $3 \cdot 3 = 3$ in \mathbb{Z}_6 . Thus 3 is **idempotent** in \mathbb{Z}_6 (a solution of the equation $x^2 = x$).

Show that, if R has unity and $\phi : R \rightarrow S$ is a ring homomorphism, then ϕ takes unity to an idempotent of S .

The kernel of ϕ is an additive subgroup of R . Why?

Definition 18.13. An **isomorphism of rings** is a ring homomorphism $\phi : R \rightarrow S$ which is also a bijection. Then R, S are said to be isomorphic as rings. Any property shared by isomorphic rings is called a **structural property of the ring**.

Which of the following are structural properties of rings?

- (1) R is commutative.
- (2) R is a ring with unity.
- (3) R has no zero divisors.
- (4) R is finite.

18.2. products.

Definition 18.14. The **product** of rings R_1, R_2, \dots, R_n is the Cartesian product of the underlying sets

$$\prod_{i=1}^n R_i = R_1 \times R_2 \times \cdots \times R_n$$

with addition and multiplication defined coordinate wise:

$$(a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n)$$

$$(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$$

The projection mapping $p_j : \prod R_i \rightarrow R_j$ is a ring homomorphism for each j . Why is that?

Example 18.15. \mathbb{Z}_6 is ring isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_3$. The isomorphism is given by $\phi(n) = (n, n)$ where n is reduced modulo 2 in the first coordinate and reduced modulo 3 in the second coordinate.

When can you tell that a ring is a product?

One sign is that a product has many zero divisors since

$$(r, 0)(0, s) = (0, 0) \in R \times S$$

So, a ring without zero divisors cannot be a product of two smaller rings.

18.3. integer multiplication. If a is an element of a ring R and n is any integer then we can define

$$n \cdot a \in R$$

as follows. First $0 \cdot a := 0$. For $n \geq 1$ the idea is:

$$n \cdot a = \underbrace{a + a + \dots + a}_{n \text{ times}}$$

However, the rigorous definition is:

$$(n + 1) \cdot a := n \cdot a + a$$

starting with $n = 0$ which we already defined ($0 \cdot a = 0$). For negative integers $n = -k$, $k > 0$ we define

$$(-k) \cdot a = -(k \cdot a)$$

This is the additive inverse of $k \cdot a$.

Problem: Show that, if $\phi : R \rightarrow S$ is a ring homomorphism then

$$\phi(n \cdot a) = n \cdot \phi(a)$$

for all $a \in R, n \in \mathbb{Z}$.

Definition 18.16. The **characteristic** of a ring R is the smallest positive integer n so that $n \cdot a = 0$ for all $a \in R$. If no such integer exists then the characteristic of R is defined to be 0.

For example, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic zero and \mathbb{Z}_n has characteristic n . What is the characteristic of $\mathbb{Z}_n \times \mathbb{Z}_m$?

Lemma 18.17. $0a = 0$

Proof. Let $x = 0a$. We want to show that $x = 0$. We use distributivity:

$$x = 0a = (0 + 0)a = 0a + 0a = x + x$$

Subtract x from both sides to get $x = 0$. Why can we subtract x ? \square

Theorem 18.18. *If R is a ring with unity then*

$$n \cdot a = (n \cdot 1)a$$

Proof. First take $n \geq 0$. We do induction.

$(n = 0)$ $0 \cdot a = 0$ is equal to $(0 \cdot 1)a = 0a = 0$ (by the Lemma).

$(n + 1)$ Suppose we know that $n \cdot a = (n \cdot 1)a$. Then we want to know the same for $n + 1$:

$$(n + 1) \cdot a := n \cdot a + a = (n \cdot 1)a + a = (n \cdot 1 + 1)a = ((n + 1) \cdot 1)a$$

So the theorem holds for all $n \geq 0$.

Now suppose n is negative. So, $n = -k$, $k > 0$. Then

$$(-k) \cdot a := -(k \cdot a) = -(k \cdot 1)a = (-k \cdot 1)a$$

by the second lemma which is below. \square

Lemma 18.19. $(-a)b = a(-b) = -ab$ for all a, b in any ring R .

Proof. By distributivity and the first lemma we have:

$$0 = 0b = (a + (-a))b = ab + (-a)b$$

So, $(-a)b$ is the additive inverse of ab . The other identity $a(-b) = -ab$ is similar. \square

Definition 18.20. A **field** is a commutative ring with unity $1 \neq 0$ in which every nonzero element is a unit. In particular, F has no zero divisors.

If F is a field then the nonzero elements form a multiplicative group F^\times . A nonexample is: \mathbb{Z}_{nm} is not a field for $n, m \geq 2$ since n and m are zero divisors: $(n)(m) = 0$ in \mathbb{Z}_{nm} .

Theorem 18.21. *The characteristic of a field F is either 0 or a prime number.*

Lemma 18.22. *If R is a ring with unity then the characteristic of R is the smallest positive integer n so that $n \cdot 1 = 0$ (or $\text{char } R = 0$ if no such n exists).*

Proof of Theorem. Suppose not. Then the characteristic of F is nm where $n, m \geq 2$. By the lemma, $nm \cdot 1 = 0$ but $a = n \cdot 1$ and $b = m \cdot 1$ are nonzero. But,

$$ab = (n \cdot 1)b = n \cdot b = n \cdot (m \cdot 1)$$

$$= \underbrace{(1 + \cdots + 1)}_m + \cdots + \underbrace{(1 + \cdots + 1)}_m = nm \cdot 1 = 0$$

So, a, b are zero divisors. So, F is not a field. \square

19. INTEGRAL DOMAINS

Definition 19.1. An **integral domain** (or **simply domain**) is defined to be a commutative ring with unity and no zero divisors.

For example, \mathbb{Z} , $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\}$ are integral domains as is any subring of \mathbb{C} .

Definition 19.2. A **subring** of a ring R is a subset $S \subseteq R$ so that

- (1) S is an additive subgroup of R (nonempty and closed under subtraction)
- (2) S is closed under multiplication in R .

Every field is an integral domain by definition and every subring of a field is an integral domain. For finite rings, the converse is true:

Theorem 19.3. Every finite integral domain is a field.

But first we need a lemma.

Lemma 19.4. Cancellation holds in a commutative ring iff it is an integral domain:

$$ax = ay, a \neq 0 \Rightarrow x = y$$

Proof. Suppose that R is a domain. Then $ax = ay$ implies

$$0 = ax - ay = a(x - y) \Rightarrow a = 0 \text{ or } x - y = 0$$

Since $a \neq 0$ we have $x - y = 0$ or $x = y$. So, cancellation holds in a domain. Conversely suppose that cancellation does not hold. Then $ax = ay$ for some $a \neq 0$ and $x \neq y$. But then

$$a(x - y) = 0$$

shows that R is not an integral domain. \square

Proof of theorem. Take any $a \neq 0$ in a finite integral domain D . Then multiplication by a gives a mapping

$$f : D \rightarrow D, \quad f(x) = ax$$

which is 1-1 (by cancellation) and therefore onto (D being finite). So, $f(x) = ax = 1$ for some $x \in D$ and $x = a^{-1}$. \square