Plan

- Review of Last Lecture
- Section 21. The Field of Quotients of an Integral Domain
- Section 26. Homomorphisms and Factor Rings

Review of Last Lecture

In the ring

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

The 0-divisors are $k \neq 0$ that are **not** relatively prime to n.

$$G_n = \{k \in \mathbb{Z}_n \mid k \neq 0, k \text{ is relatively primes to } n\}$$

Theorem 20.6. The set G_n forms a group under the multiplication modulo n.

Example. In $\mathbb{Z}_{14} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13\}$, the 0-divisors are $2, 4, 6, 7, 8, 10, 12$.

$$G_{14} = \{1, 3, 5, 9, 11, 13\}$$

The order of G_n is equal to the Euler's phi function $\phi(n)$: $|G_n| = \phi(n)$.

$\phi(n)$ is the number positive integers k with $1 \leq k < n$ that are relatively prime to n.

(1) $\phi(mn) = \phi(m)\phi(n)$ for m, n relatively primes.

(2) $\phi(p^k) = p^k - p^{k-1}$.

Theorem 20.8. (Euler's Theorem) If a is an integer relatively prime to n, then $a^{\phi(n)} - 1$ is divisible by n.

In the special case that $n = p$ is a prime, a is not a multiple of p, then Euler's theorem is Fermat's theorem:

Theorem 20.1. If p is a prime, a is not a multiple of p, then $a^{p-1} - 1$ is a multiple of p.

Example. $\phi(15) = \phi(3)\phi(5) = (3-1)(5-1) = 8.$
49 is relatively prime to 15, by Euler's theorem

$49^8 - 1$ is a multiple of 15.

Recall the definition of an integral domain:

Definition 19.6. A ring D is called an **integral domain** if it satisfies the following three conditions
(1) D is a commutative ring.
(2) D has a unity 1, $1 \neq 0$.
(3) D has no 0-divisors.

Every field is an integral domain (Theorem 19.9). The converse is not correct: $\mathbb{Z}$ is an integral domain but not a field.

The main result of this section is that every integral domain is contained in a field as a subring. The smallest field that contains a given integral domain D is called the **field of quotients of D**.

For the integral domain $\mathbb{Z}$, its field of quotients is $\mathbb{Q}$, each element in $\mathbb{Q}$ can be written as $\frac{n}{m}$ for some $m, n \in \mathbb{Z}$ and $m \neq 0$.

This motivates the following construction:

Let D be an integral domain. Let

$$S = \{(a, b) \mid a, b \in D, b \neq 0\}$$

(a, b) and (c, d) are equivalent if $ad = bc$. We write $(a, b) \sim (c, d)$ if they are equivalent.

Here the idea is that we think a pair (a, b) as $\frac{a}{b}$.

Let F denote the set of equivalence classes of S.
We define addition $+$ and multiplication $\cdot$ on F by:

$$(a, b) + (c, d) = (ad + bc, db), \quad (a, b) \cdot (c, d) = (ac, bd)$$

We can prove that $+$ and $\cdot$ are well-defined and $(F, +, \cdot)$ is a field.

F is called the field of quotients of D. D can be embedded into F as a subring by $a \in D \mapsto (a, 1)$.

We recall the definition of homomorphism between rings.

Definition 26.1 A map ϕ from ring R to ring R' is a (ring) **homomorphism** if

$$\phi(a+b)=\phi(a)+\phi(b), \quad \phi(ab)=\phi(a)\phi(b)$$

for all $a, b \in R$.

Example. Let $R_1, \ldots, R_n$ be rings, $R_1 \times \cdots \times R_n$ be the direct product ring. For each i, the map $\pi_i : R_1 \times \cdots \times R_n \to R_i$ defined by

$$\pi_i(a_1, \ldots, a_n) = a_i$$

is a homomorphism.

Example. The map $\phi : C[0,7] \to \mathbb{R}$, $\phi(f) = f(3)$, is a homomorphism. ϕ is called the evaluation homomorphism at 3.

If R is a ring, a subset $S \subseteq R$ is a **subring** of R if S is closed under $+$ and $\cdot$ and $(S, +, \cdot)$ is a ring.

To check a subset S is a subring, we only need to check the following:
(1) S is closed under $+$.
(2) S is closed under $\cdot$.
(3) $0 \in S$ and $a \in S$ implies $-a \in S$.

Theorem 26.3. Let $\phi : R \to R'$ be a ring homomorphism. Then
(1) $\phi(0) = 0'$.
(2) $\phi(-a) = -\phi(a)$ for all $a \in R$.
(3) If $S \subseteq R$ is subring, then $\phi(S)$ is a subring of R'.
(4) If $S' \subseteq R'$ is subring, then $\phi^{-1}(S')$ is a subring of R.

Definition. Let $\phi : R \to R'$ be a ring homomorphism, the subring

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

is called the **kernel** of ϕ, and is denoted by $Ker(\phi)$.

Example. For the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_n$, $\phi(a) = a \mod n$, $Ker(\phi) = n\mathbb{Z}$.

Example. For the ring homomorphism $\phi : C[0,7] \to \mathbb{R}$, $\phi(f) = f(3)$, $Ker(\phi) = \{f(x) \in C[0,7] \mid f(3) = 0\}$.

About Quiz.

The symbols $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*$ will be denoted by

$$\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}, \mathbf{Q}^*, \mathbf{R}^*, \mathbf{C}^*$$

Sample problem. Let $\mathbf{C}^*$ be the multiplicative group of non-zero complex numbers. Let A , B , C be subgroups of $\mathbf{C}^*$ given as follows:
A $=$ the set of numbers of form 2^n, n is an integer
B $=$ the set of all 100th roots of unity
C $=$ the set of all positive real numbers
Determine if A, B, C are cyclic groups

(1) A , B , C are all cyclic groups.
(2) A, B are cyclic groups, but C is not
(3) A, C are cyclic groups, but B is not
(4) B , C are cyclic groups, but A is not

The end