Section 26. Homomorphisms and Factor Rings (continued).

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 $a, b \in R$.

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 $-a \in S$.

Alternatively, to check a subset S is a subring, we can check
(1) $(S, +)$ is additive subgroup.
(2) S is closed under $\cdot$.

Example. Is the set S of all upper triangular matrices with real number entries a subring of $M_3(\mathbb{R})$?

Since the sum and the multiplication of two upper triangular matrices are upper triangular, so S is closed under $+$ and $\cdot$. The zero matrix is upper triangular, A is upper triangular implies that $-A$ is also upper triangular, so S is a subring of $M_3(\mathbb{R})$.

Example. Determine if the given subsets of $M_2(\mathbb{R})$ are subrings:

$$S_1 = \{\begin{pmatrix} a & b \\ -b, & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$$

$$S_2 = \{\begin{pmatrix} a & 2b \\ -b, & a \end{pmatrix} \mid a, b \in \mathbb{R}\}$$

S_1 is a subring, S_2 is not.

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.

This theorem is similar to Theorem 13.12 for group homomorphisms. There is also an analog for linear maps between vector spaces.

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

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

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

A ring homomorphism ϕ is also a group homomorphism from the additive group $(R, +)$ to additive group $(R', +)$, so all the theorems for group homomorphism apply.

Theorem 26.5. Let $\phi : R \to R'$ be a ring homomorphism, $H = Ker(\phi)$, $b \in R'$, then $\phi^{-1}(b)$ is either an empty set or $\phi^{-1}(b) = a + H$ for any $a \in R$ with $\phi(a) = b$.

This theorem is a direct consequence of Theorem 13.15.

Example. For the homomorphism $\phi : \mathbb{Z} \to \mathbb{Z}_n$, $\phi(a) = a \mod n$,
$Ker(\phi) = n\mathbb{Z}$.
$\phi^{-1}(a) = a + n\mathbb{Z}$

Example. For the ring homomorphism $\phi : C[0,7] \to \mathbb{R}$, $\phi(f) = f(3)$,
$Ker(\phi) = \{f(x) \in C[0,7] \,|\, f(3) = 0\}$.
$\phi^{-1}(5) = x + 2 + Ker(\phi)$.

Definition 26.10. An additive subgroup N of a ring R satisfying the properties that

$$an \in N, na \in N, \quad \text{for all } a \in R, n \in N$$

is called an **ideal** of R.

The condition in the definition can be written as

$$aN \subseteq N, Na \subseteq N \ \text{ for all } a \in R.$$

Example. In ring $\mathbb{Z}$, for every integer n, $n\mathbb{Z}$ is an ideal of $\mathbb{Z}$.

Corollary 26.14. Let N be an ideal of a ring R, let R/N be the set of additive cosets $a+N$ $(a \in R)$, then the following $+$ and multiplication on R/N are well-defined

$$(a+N)+(b+N)=(a+b)+N, \ \ (a+N)\cdot(b+N)=ab+N.$$

And $(R/N,+,\cdot)$ is a ring.

The ring R/N is called the **factor ring** (or **quotient ring**) **of** R **by** N.

Example. $R = \mathbb{Z}$, $N = n\mathbb{Z}$ is an ideal of $\mathbb{Z}$, where n is fixed positive integer, then $R/N = \mathbb{Z}/n\mathbb{Z}$ is $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, the integer ring modulo n.

Theorem 26.16. Let N be an ideal of a ring R. Then $\gamma : R \to R/N$ given by

$$\gamma(a) = a + N$$

is a ring homomorphism with kernel N.

This Theorem is an anlogue of Theorem 14.9.

Theorem 26.17. (**Fundamental Homomorphism Theorem; Analogue of Theorem 14.11.** Let $\phi : R \to R'$ be a ring homomorphism with kernel N. Then $\phi(R)$ is a ring, and the map

$$\mu : R/N \to \phi(R) \text{ given by } \mu(a+N) = \phi(a)$$

is well-defined and is an isomorphism of rings.

In our syllabus, there is a topic in linear algebra about Jordan canonical forms. I will post a note in Canvas. This topic will NOT be assessed in the final exam.

The end

Good Luck, Keep Safe!