Lecture notes for Abstract Algebra I: Lecture 19

1 Rings homomorphisms and ideals

In the study of groups, a homomorphism is a map that preserves the operation of the group. Similarly, a homomorphism between rings preserves the operations of addition and multiplication in the ring. More specifically, if R and S are rings, then **a ring homomorphism** is a map $\varphi\colon R \longrightarrow S$ satisfying

$$\varphi(a+b) = \varphi(a) + \varphi(b) \qquad \text{and} \qquad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

for all $a, b \in R$. If $\varphi\colon R \longrightarrow S$ is a one-to-one and onto homomorphism, then φ is called an **isomorphism of rings**. The set of elements that a ring homomorphism maps to 0 plays a fundamental role in the theory of rings. For any ring homomorphism $\varphi\colon R \longrightarrow S$, we define the kernel of a ring homomorphism to be the set

$$\ker\varphi = \{r \in R \,|\, \varphi(r) = 0\}$$

Example 1. For any integer n we can define a ring homomorphism $\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$ by $a \mapsto a(\bmod n)$. This is indeed a ring homomorphism, since

$$\begin{aligned}\varphi(a+b) &= (a+b)(\bmod n)\\ &= a(\bmod n) + b(\bmod n)\\ &= \varphi(a) + \varphi(b)\end{aligned}$$

and

$$\begin{aligned}\varphi(a \cdot b) &= (a \cdot b)(\bmod n)\\ &= a(\bmod n) \cdot b(\bmod n)\\ &= \varphi(a) \cdot \varphi(b)\end{aligned}$$

The kernel of $\varphi\colon \mathbb{Z} \longrightarrow \mathbb{Z}_n$ is $\ker(\varphi) = n\mathbb{Z}$.

Proposition 2. *Let $\varphi\colon R \longrightarrow S$ be a ring homomorphism.*

1. *If R is a commutative ring, then $\varphi(R)$ is a commutative ring.*
2. *$\varphi(0) = 0$.*
3. *Let 1_R and 1_S be the identities for R and S, respectively. If φ is onto, then $\varphi(1_R) = 1_S$.*
4. *If R is a field and $\varphi(R) \neq 0$, then $\varphi(R)$ is a field as well.*

In group theory we found that normal subgroups play a special role. These subgroups have nice characteristics that make them more interesting to study than arbitrary subgroups. In ring theory the objects corresponding to normal subgroups are a special class of subrings called **ideals**.

Definition 3. An ideal in a ring R is a subring I of R such that if a is in I and r is in R, then both ar and ra are in I; that is, $rI \subset I$ and $Ir \subset I$ for all $r \in R$.

$$I \textbf{ ideal} \Leftrightarrow r - s \in I \quad \forall r, s \in I \quad \text{and} \quad ar, ra \in I \quad \forall a \in I, r \in R.$$

Remark 4. Given a ring homomorphism $\varphi \colon R \longrightarrow S$, the kernel $\ker(\varphi)$ is an ideal of R. We can check

(1) $x, y \in \ker(\varphi) \Rightarrow \varphi(x), \varphi(y) = 0 \Rightarrow \varphi(x-y) = \varphi(x) - \varphi(y) = 0 \Rightarrow x - y \in \ker(\varphi)$.

(2) $x \in \ker(\varphi), r \in R \Rightarrow \varphi(rx) = \varphi(r)\varphi(x) = \varphi(r) \cdot 0 = 0 \Rightarrow rx \in \ker(\varphi)$.

(2) $x \in \ker(\varphi), r \in R \Rightarrow \varphi(xr) = \varphi(x)\varphi(r) = 0 \cdot \varphi(r) = 0 \Rightarrow xr \in \ker(\varphi)$.

Example 5. If a is an element in a commutative ring R with identity, the set

$$\langle a \rangle = \{ar \,|\, r \in R\}$$

is nonempty since both $0 = a0$ and $a = a1$ are in $\langle a \rangle$. The sum of two elements in $\langle a \rangle$ is again in $\langle a \rangle$ since $ar + ar' = a(r + r')$. The inverse of ar is $-ar = a(-r) \in \langle a \rangle$. Finally, if we multiply an element $ar \in \langle a \rangle$ by an arbitrary element $s \in R$, we have $s(ar) = a(sr) \in \langle a \rangle$. Therefore, $\langle a \rangle$ satisfies the definition of an ideal. If R is a commutative ring with identity, then an ideal of the form $\langle a \rangle$ is called a **principal ideal** or **principal ideal generated by a**.

Proposition 6. *In the ring $\mathbb{Z}$, all ideals are principal. The ring $\mathbb{Z}$ is what is called **A principal ideal domain (PID)**.*

Proof. The ideal $\{0\}$ is clearly principal. If $I \subset \mathbb{Z}$ is a non-zero ideal, take smallest positive number $a \in I$. Any other element $b \in I$ will be expressed as

$$b = aq + r \quad \text{with} \quad r \in I \ \text{ with } \ 0 \leq r < a$$

By the way we have selected the a it most be $r = 0$ and $I = \langle a \rangle$. □

The importance of the concept of ideal is given by the following result.

Theorem 7. *Let I be an ideal of R. The factor group R/I is a ring with multiplication defined by*

$$(r + I)(s + I) = rs + I.$$

Proof. We already know that R/I is an abelian group under addition. Let $r + I$ and $s + I$ be two classes in R/I. We must show that the product $(r + I)(s + I) = rs + I$ is independent of the choice of coset; that is, if we choose elements r' and s' in $r + I$ and $s + I$ respectively, then the product $r's'$ must be in $rs + I$. Since $r' \in r + I$, there must be $a \in I$ such that $r' = r + a$. In the same way, there must be $b \in I$ such that $s' = s + b$. We calculate

$$r's' = (r + a)(s + b) = rs + as + rb + ab$$

and the element $as + rb + ab \in I$ since I is an ideal; consequently, $r's' \in rs + I$. We still need to verify he associative law for multiplication and the distributive laws. $\square$

Definition 8. The ring R/I is called the **factor or quotient ring** of R by I.

Example 9. For $R = \mathbb{Z}$ and $n \in \mathbb{Z}$, the ideal $\langle n \rangle$ in R has quotient

$$R/\langle n \rangle = \mathbb{Z}_n.$$

In general, we have the isomorphism theorems from group theory:

Theorem 10. *If $\varphi\colon R \longrightarrow S$ is a surjective ring homomorphism, then*

$$R/\ker(\varphi) \cong S.$$

Theorem 11. *If I is an ideal in R and R' is a subring, then $R' \cap I$ is an ideal in R' and*

$$R'/(R' \cap I) \cong (R' + I)/I.$$

Theorem 12. *If $I \subset J \subset R$ are ideals in R, then*

$$J/I \cong R/I \,/\, R/J.$$