Notes - Commutative Rings
(2025-01-22)

George McNinch

2025-01-22

Ring homomorphisms

If R and S are rings, a function $\phi : R \to S$ is called a *ring homomorphism* provided that

a. ϕ is a homomorphism of *additive groups*, and
b. ϕ preserves multiplication; i.e. for all $x, y \in R$ we have $\phi(xy) = \phi(x)\phi(y)$.
c. $\phi(1_R) = 1_S$.

The *kernel* of the ring homomorphism $\phi : R \to S$ is given by

$$\ker \phi = \phi^{-1}(0) = \{x \in R \mid \phi(x) = 0\};$$

thus $\ker \phi$ is just the kernel of ϕ viewed as a homomorphism of additive groups.

Properties of the kernel:

a. $\ker \phi$ is an additive subgroup of R
b. for every $r \in R$ and every $x \in \ker \phi$ we have $rx \in \ker \phi$.

Ideals of a ring

For simplicity suppose that the ring R (and S) are *commutative* rings.

A subset I of R is an *ideal* provided that

a. I is an additive subgroup of R, and
b. for every $r \in R$ and every $x \in I$ we have $rx \in I$.

We sometimes describe condition b. by saying that "I is closed under multiplication by every element of R".

The proof of the following is immediate from definitions:

Proposition If $\phi : R \to S$ is a ring homomorphism , then $\ker \phi$ is an ideal of R.

Quotient rings

Let R be a commutative ring and I an ideal of R.

Since I is a subgroup of the (abelian) additive group R, we may consider the quotient group R/I. Its elements are (additive) cosets $a + I$ for $a \in R$.

It follows from the definition of cosets that the $a + I = b + I$ if and only if $b - a \in I$.

The additive group can be made into a commutative ring by defining the multiplication as follows:

For $a + I, b + I \in R/I$ (so that $a, b \in R$), the product is given by

$$(a + I)(b + I) = ab + I.$$

In order to make this definition, one must confirm that this rule is well-defined. Namely, if we have equalities $a + I = a' + I$ and $b + I = b' + I$, we need to know that

$$(a + I)(b + I) = (a' + I)(b' + I).$$

Applying the definition, we see that we must confirm that

$$ab = I = a'b' + I.$$

For this, we need to argue that $a'b' - ab \in I$.

Since $a + I = a' + I$, we know that $a' - a = x \in I$ and since $b + I = b' + I$ we know that $b' - b = y \in I$.

Thus $a' = a + x$ and $b' = b + y$. Now we see that

$$a'b' = (a + x)(b + y) = ab + ay + xb + xy$$

Since I is an ideal, we see that $ay, xb, xy \in I$ henc $ay + xb + xy \in I$. Now conclude that $a'b' + I = ab + I$ as required.

It is now straightforward to confirm that the ring axioms hold for the set R/I with these operations.

Proposition If I is an ideal of the commutative ring R, then R/I is a commutative ring with the addition and multiplication just described.

Principal ideals

If R is a commutative ring and $a \in R$, the *principal ideal generated by* a – written Ra or $\langle a \rangle$ – is defined by

$$Ra = \langle a \rangle = \{ra \mid r \in R\}.$$

Proposition For $a \in R$, Ra is an *ideal* of R.

Example Let $n \in \mathbb{Z}_{>0}$ and consider the principal ideal $n\mathbb{Z}$ of the ring $\mathbb{Z}$ generated by $n \in \mathbb{Z}$.

As an additive group, $n\mathbb{Z}$ is the infinite cyclic group generated by n.

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ is the finite commutative ring with n elements; these elements are precisely the *congruence classes* of integers modulo n.

Isomorphism Theorem

Theorem Let R, S be commutative rings with identity and let $\phi : R \to S$ be a ring homomorphism. Assume that ϕ is *surjective* (i.e. *onto*). Then ϕ determines an isomorphism $\overline{\phi} : R/I \to S$ where $I = \ker \phi$, where $\overline{\phi}$ is determined by the rule

$$\overline{\phi}(a + I) = \phi(a) \quad \text{for } a \in R.$$

Outline of proof

First, you must confirm that $\overline{\phi}$ is *well-defined*; i.e. that if $a + I = a' + I$ then $\overline{\phi}(a + I) = \overline{\phi}(a' + I)$.

Next, you must confirm that $\overline{\phi}$ is a ring homomorphism (this is immediate from the definition of ring operations on R/I).

Finally, you must confirm that $\ker \overline{\phi} = \{0\}$, where here 0 refers to the additive identity of the quotient ring R/I. This additive identity is of course the trivial coset $I = 0 + I \in R/I$.

Polynomial ring example

If F is a field and $a \in F$, consider the mapping

$$\Phi : F[T] \to F$$

given by $\Phi(f(T)) = f(a)$. Namely, applying Φ to a polynomial $f(T)$ results in the value $f(a)$ of $f(T)$ at a.

The definition of multiplication in $F[T]$ guarantees that Φ is a ring homomorphism.