MATH 415

Modern Algebra I

Lecture 33: Homomorphisms of rings (continued).

Homomorphism of rings

Definition. Let R and R' be rings. A function $f : R \to R'$ is called a **homomorphism of rings** if $f(r_1 + r_2) = f(r_1) + f(r_2)$ and $f(r_1 r_2) = f(r_1)f(r_2)$ for all $r_1, r_2 \in R$.

Properties of homomorphisms:

- If H' is a subring of R', then $f^{-1}(H')$ is a subring of R.
- If I' is a two-sided (resp. left, right) ideal in R', then $f^{-1}(I')$ is a two-sided (resp. left, right) ideal in R.
- The kernel $\mathrm{Ker}(f) = f^{-1}(0)$ is a two-sided ideal in R.
- If H is a subring of R, then $f(H)$ is a subring of R'.
- If I is a two-sided (resp. left, right) ideal in R, then $f(I)$ is a two-sided (resp. left, right) ideal in $f(R)$, but may not be an ideal in R'.

Examples of homomorphisms

- Trivial homomorphism.

Given any rings R and R', let $f(r) = 0_{R'}$ for all $r \in R$, where $0_{R'}$ is the zero element in R'. Then $f : R \to R'$ is a homomorphism of rings.

- Residue modulo n of an integer.

For any $k \in \mathbb{Z}$ let $f(k)$ be the remainder of k after division by n. Then $f : \mathbb{Z} \to \mathbb{Z}_n$ is a homomorphism of rings.

- Homomorphisms of $\mathbb{Z}$.

Let R be any ring and i be any idempotent element in R. Then there exists a unique homomorphism $f : \mathbb{Z} \to R$ such that $f(1) = i$. It can be defined inductively: $f(1) = i$, $f(k+1) = f(k) + i$ for all $k \geq 1$, $f(0) = 0$ and $f(-k) = -f(k)$ for all $k \geq 1$.

Suppose $f : R \to R'$ is a homomorphism of rings. It induces homomorphisms of certain rings built from R and R'.

- Rings of functions.

Given a nonempty set S, let $\mathcal{F}(S, R)$ be the ring of all functions $h : S \to R$. A homomorphism $\phi : \mathcal{F}(S, R) \to \mathcal{F}(S, R')$ is given by $\phi(h) = f \circ h$.

- Rings of polynomials.

A homomorphism $\phi : R[x] \to R'[x]$ is given by
$\phi(a_0 + a_1x + a_2x^2 + \cdots + a_nx^n) =$
$f(a_0) + f(a_1)x + f(a_2)x^2 + \cdots + f(a_n)x^n$.

- Rings of matrices.

Let $\mathcal{M}_{n,n}(R)$ be the ring of all $n\times n$ matrices with entries from R. A homomorphism $\phi : \mathcal{M}_{n,n}(R) \to \mathcal{M}_{n,n}(R')$ is given by $\phi\big((a_{ij})_{1\leq i,j\leq n}\big) = (f(a_{ij}))_{1\leq i,j\leq n}$.

Given a nonempty set S and a ring R, let $\mathcal{F}(S, R)$ be the ring of all functions $h : S \to R$.

- Evaluation at a point.

Let us fix a point $x_0 \in S$ and define a function $\phi : \mathcal{F}(S, R) \to R$ by $\phi(h) = h(x_0)$. Then ϕ is a homomorphism of rings.

- Restriction to a subset.

Let S_0 be a nonempty subset of S. A homomorphism $\phi : \mathcal{F}(S, R) \to \mathcal{F}(S_0, R)$ is given by $\phi(h) = h|_{S_0}$.

- Extension to a larger set.

Let S_1 be a set that contains S. For any function $h : S \to R$ let $\phi(h) = h_1$, where the function $h_1 : S_1 \to R$ is defined by $h_1(x) = h(x)$ if $x \in S$ and $h_1(x) = 0$ otherwise. Then $\phi : \mathcal{F}(S, R) \to \mathcal{F}(S_1, R)$ is a homomorphism of rings.

Another example

Let $\mathbb{Z}[i] = \{m + in \mid m, n \in \mathbb{Z}\}$ be the ring of Gaussian integers. Consider a map $\phi : \mathbb{Z}[i] \to \mathbb{Z}_2$ given by

$$\phi(m + in) = (m + n) \bmod 2.$$

Then ϕ is a homomorphism of rings.

Indeed, let $z_1 = m_1 + in_1$ and $z_2 = m_2 + in_2$ be two Gaussian integers. Then $z_1 + z_2 = (m_1 + m_2) + i(n_1 + n_2)$ and $z_1 z_2 = (m_1 n_1 - m_2 n_2) + i(m_1 n_2 + m_2 n_1)$. Observe that

$$(m_1 + m_2) + (n_1 + n_2) = (m_1 + n_1) + (m_2 + n_2),$$

which implies that $\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$. Further,

$$\begin{aligned}(m_1 n_1 - m_2 n_2) + (m_1 n_2 + m_2 n_1) = \\ &= (m_1 n_1 + m_2 n_2 + m_1 n_2 + m_2 n_1) - 2m_2 n_2 \\ &= (m_1 + n_1)(m_2 + n_2) - 2m_2 n_2,\end{aligned}$$

which implies that $\phi(z_1 z_2) = \phi(z_1)\phi(z_2)$.

- $\phi : \mathbb{Z}[i] \to \mathbb{Z}_2, \;\; \phi(m + in) = (m + n) \bmod 2.$

The kernel $\mathrm{Ker}(\phi)$ consists of all numbers of the form $m + ni$, where m and n are integers of the same parity (both even or both wrong). Since ϕ is a homomorphism of rings, we conclude that $\mathrm{Ker}(\phi)$ is an ideal in $\mathbb{Z}[i]$. In particular, it is a ring. However $\mathrm{Ker}(\phi)$ is not a ring with unity since it does not contain 1.

Remark. In general, if a subring R_0 of a ring R with unity does not contain the unity 1_R of R, it may still have its own unity 1_{R_0}. But this is never the case if R is a domain (and hence satisfies cancellation laws). Indeed, we would have $1_{R_0} 1_{R_0} = 1_{R_0} = 1_R 1_{R_0}$ and, after cancellation, $1_{R_0} = 1_R$.

It is known that every ideal in $\mathbb{Z}[i]$ is principal. In this particular case, we have $\mathrm{Ker}(\phi) = (1 + i)\mathbb{Z}[i]$. Indeed, if $m + in \in \mathrm{Ker}(\phi)$, then $n = m + 2k$ for some integer k. Hence $m + in = m + i(m + 2k) = m(1 + i) + k(2i)$
$= m(1 + i) + k(1 + i)^2 = (1 + i)(m + k + ki)$.

Isomorphism of rings

Definition. Let R and R' be rings. A function $f : R \to R'$ is called an **isomorphism of rings** if it is bijective and a homomorphism of rings.

A ring R is said to be **isomorphic** to a ring R' if there exists an isomorphism of rings $f : R \to R'$.

Theorem Isomorphism is an equivalence relation on the collection of all rings.

Theorem The following properties of rings are preserved under isomorphisms:

- commutativity,
- having the unity,
- having divisors of zero,
- being an integral domain,
- being a field.

Fundamental Theorem on Homomorphisms

Theorem Given a homomorphism $f : R \to R'$, the factor ring $R/\mathrm{Ker}(f)$ is isomorphic to $f(R)$.

Proof. The factor ring is also a factor group. We know from group theory that an isomorphism of additive groups is given by $\phi(r + K) = f(r)$ for any $r \in R$, where $K = \mathrm{Ker}(f)$, the kernel of f. It remains to check that

$$\phi((r_1 + K)(r_2 + K)) = \phi(r_1 + K)\phi(r_2 + K)$$

for all $r_1, r_2 \in R$. Indeed, $\phi((r_1 + K)(r_2 + K)) = \phi(r_1 r_2 + K)$ $= f(r_1 r_2) = f(r_1)f(r_2) = \phi(r_1 + K)\phi(r_2 + K)$.

Example:

- Factor ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$.