MATH 415

Modern Algebra I

Lecture 22: Homomorphisms of rings.

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 $r_1, r_2 \in R$.

That is, f is a homomorphism of the binary structure $(R, +)$ to $(R', +)$ and, simultaneously, a homomorphism of the binary structure $(R, \cdot)$ to $(R', \cdot)$. In particular, f is a homomorphism of additive groups, which implies the following properties:

- $f(0) = 0$,
- $f(-r) = -f(r)$ for all $r \in R$,
- if H is an additive subgroup of R then $f(H)$ is an additive subgroup of R',
- if H' is an additive subgroup of R' then $f^{-1}(H')$ is an additive subgroup of R,
- $f^{-1}(0)$ is an additive subgroup of R, called the **kernel** of f and denoted $\mathrm{Ker}(f)$.

More properties of homomorphisms

Let $f : R \to R'$ be a homomorphism of rings.

- If H is a subring of R, then $f(H)$ is a subring of R'.

We already know that $f(H)$ is an additive subgroup of R'. It remains to show that it is closed under multiplication in R'. Let $r_1', r_2' \in f(H)$. Then $r_1' = f(r_1)$ and $r_2' = f(r_2)$ for some $r_1, r_2 \in H$. Hence $r_1' r_2' = f(r_1)f(r_2) = f(r_1 r_2)$, which is in $f(H)$ since H is closed under multiplication in R.

- If H' is a subring of R', then $f^{-1}(H')$ is a subring of R.

We already know that $f^{-1}(H')$ is an additive subgroup of R. It remains to show that it is closed under multiplication in R. Let $r_1, r_2 \in f^{-1}(H')$, that is, $f(r_1), f(r_2) \in H'$. Then $f(r_1 r_2) = f(r_1)f(r_2)$ is in H' since H' is closed under multiplication in R'. Hence $r_1 r_2 \in f^{-1}(H')$.

More properties of homomorphisms

- If H' is a left ideal in R', then $f^{-1}(H')$ is a left ideal in R.

We already know that $f^{-1}(H')$ is a subring of R. It remains to show that $r \in R$ and $a \in f^{-1}(H')$ imply $ra \in f^{-1}(H')$. We have $f(a) \in H'$. Then $f(ra) = f(r)f(a)$ is in H' since H' is a left ideal in R'. In other words, $ra \in f^{-1}(H')$.

- If H' is a right ideal in R', then $f^{-1}(H')$ is a right ideal in R.

- If H' is a two-sided ideal in R', then $f^{-1}(H')$ is a two-sided ideal in R.

- The kernel $\mathrm{Ker}(f)$ is a two-sided ideal in R.

Indeed, $\mathrm{Ker}(f)$ is the pre-image of the trivial ideal $\{0\}$ in R'.

More properties of homomorphisms

- If an element $a \in R$ is idempotent in R (that is, $a^2 = a$) then $f(a)$ is idempotent in R'.

Indeed, $(f(a))^2 = f(a^2) = f(a)$.

- If 1_R is the unity in R then $f(1_R)$ is the unity in $f(R)$.

Let $r' \in f(R)$. Then $r' = f(r)$ for some $r \in R$. We obtain $r'f(1_R) = f(r)f(1_R) = f(r \cdot 1_R) = f(r) = r'$ and $f(1_R)r' = f(1_R)f(r) = f(1_R \cdot r) = f(r) = r'$.

- If 1_R is the unity in R and R' is a domain with unity, then either $f(1_R)$ is the unity in R' or else the homomorphism f is identically zero.

If $f(1_R) = 0$ then f is identically zero: $f(r) = f(r \cdot 1_R) = f(r)f(1_R) = f(r) \cdot 0 = 0$ for all $r \in R$. Otherwise $f(1_R)$ is a nonzero idempotent element. We know that in a domain with unity, the only idempotent elements are the zero and the unity.

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.

- Change of the modulus.

Let d be a divisor of an integer $n \geq 1$. Then for any $k \in \mathbb{Z}$ the remainder after division of k by n uniquely determines the remainder after division of k by d. This gives rise to a map $f : \mathbb{Z}_n \to \mathbb{Z}_d$, which is a homomorphism of rings.

Examples of homomorphisms

- General homomorphisms of $\mathbb{Z}$.

Let R be any ring and r be any idempotent element in R: $r^2 = r$. Then there exists a unique homomorphism of rings $f : \mathbb{Z} \to R$ such that $f(1) = r$. It can be defined inductively: $f(1) = r$, $f(k+1) = f(k) + r$ for all $k \geq 1$, $f(0) = 0$ and $f(-k) = -f(k)$ for all $k \geq 1$.

- General homomorphisms of $\mathbb{Z}_n$.

Let R be any ring and $r \in R$ be any idempotent element such that its order in the additive group of R divides n. Then there exists a unique homomorphism $f : \mathbb{Z}_n \to R$ such that $f(1) = r$.

- Complex conjugate.

For any complex number $z = x + yi$ let $f(z) = \bar{z} = x - yi$. Then f is a homomorphism of the ring $\mathbb{C}$ onto itself.

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 $\phi\big((a_{ij})_{1 \le i,j \le n}\big) = (f(a_{ij}))_{1 \le i,j \le n}$.

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 $R_0 \neq \{0\}$ of a ring R with unity does not contain the unity 1_R of R, it may still have its own unity $1_{R_0} \neq 0$. 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 $R/\operatorname{Ker}(f)$ 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 $K = \operatorname{Ker}(f)$, 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. • $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(k) = k \bmod n$.

We have $\operatorname{Ker}(f) = n\mathbb{Z}$ and $f(\mathbb{Z}) = \mathbb{Z}_n$. Hence the factor ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$.

Matrix model of complex numbers

Consider a function $\phi : \mathbb{C} \to \mathcal{M}_{2,2}(\mathbb{R})$ given by

$$\phi(x+iy) = \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

for all $x, y \in \mathbb{R}$. Then ϕ is a homomorphism of rings.

Indeed, for any real numbers x, y, x' and y' we have $(x+iy)+(x'+iy') = (x+x')+i(y+y')$ and

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} + \begin{pmatrix} x' & -y' \\ y' & x' \end{pmatrix} = \begin{pmatrix} x+x' & -(y+y') \\ y+y' & x+x' \end{pmatrix}.$$

Further, $(x+iy)(x'+iy') = (xx'-yy')+i(xy'+yx')$ and

$$\begin{pmatrix} x & -y \\ y & x \end{pmatrix} \begin{pmatrix} x' & -y' \\ y' & x' \end{pmatrix} = \begin{pmatrix} xx'-yy' & -(xy'+yx') \\ xy'+yx' & xx'-yy' \end{pmatrix}.$$

The kernel $\mathrm{Ker}(\phi)$ is clearly trivial. It follows that the ring $\mathbb{C}$ is isomorphic to $\phi(\mathbb{C})$. In particular, $\phi(\mathbb{C})$ is a field.