MATH 415

Modern Algebra I

Lecture 22:
Homomorphisms of rings (continued).
Prime and maximal ideals.

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'.

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.

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 set 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:

- 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.

Prime ideals

Definition. A (two-sided) ideal I in a ring R is called **prime** if for any elements $x, y \in R$ we have

$$xy \in I \implies x \in I \text{ or } y \in I.$$

Example. In the ring $\mathbb{Z}$, every nontrivial proper ideal is of the form $n\mathbb{Z}$, where $n > 1$. This ideal is prime if and only if n is a prime number.

The entire ring R is always a prime ideal of itself. The trivial ideal $\{0\}$ is prime if and only if the ring R has no divisors of zero.

Theorem The ideal I is prime in the ring R if and only if the factor ring R/I has no divisors of zero.

Proof ("if"). Suppose $xy \in I$ while $x, y \in R \setminus I$. Then $x + I \neq 0 + I$ and $y + I \neq 0 + I$ while $(x + I)(y + I) = xy + I = I$ so that $x + I$ and $y + I$ are divisors of zero in R/I.

Maximal ideals

Definition. A (two-sided) ideal I in a ring R is called **maximal** if $I \neq R$ and for any ideal J satisfying $I \subset J \subset R$, we have $J = I$ or $J = R$.

Example. In the ring $\mathbb{Z}$, every nontrivial proper ideal is of the form $n\mathbb{Z}$, where $n > 1$. This ideal is contained in an ideal $m\mathbb{Z}$ if and only if m divides n. It follows that the ideal $n\mathbb{Z}$ is maximal if and only if it is prime.

Theorem A proper ideal I in the ring R is maximal if and only if the factor ring R/I has no (two-sided) ideals other than the trivial ideal and itself.

Theorem A proper ideal I in the ring R is maximal if and only if the factor ring R/I has no (two-sided) ideals other than the trivial ideal and itself.

Proof. Consider a map $\phi : R \to R/I$ given by $\phi(x) = x + I$ for all $x \in R$. This map is a homomorphism of rings.

Suppose R/I has a nontrivial proper ideal J'. Then $J = \phi^{-1}(J')$ is an ideal in R such that $I \subset J \subset R$. Since the map ϕ is onto, it follows that $J \neq I$ and $J \neq R$. In particular, the ideal I is not maximal.

Conversely, assume that there is an ideal J in R such that $I \subset J \subset R$ while $J \neq I$ and $J \neq R$. Then $J' = \phi(J)$ is an ideal in $\phi(R) = R/I$. The ideal J' is nontrivial since J is not contained in the kernel $\mathrm{Ker}(\phi) = I$. Since $I \subset J$, it follows that $\phi(J) = J'$ is disjoint from $\phi(R \setminus J)$. In particular, J' is a proper ideal in R/I.

Theorem Suppose R is a commutative ring with unity. Then R has no (two-sided) ideals other than the trivial ideal and itself if and only if R is a field.

Proof. Assume R is a field and let I be a nontrivial ideal in R. Take any nonzero element $a \in I$. Since R is a field, this element admits a multiplicative inverse a^{-1}. Then for any $x \in R$ we have $x = 1x = (aa^{-1})x = a(a^{-1}x) \in I$. That is, $I = R$.

Now assume R is not a field. Then there is a nonzero element $a \in R$ that does not admit a multiplicative inverse. Hence $aR = \{ax \mid x \in R\}$, which is an ideal in R, does not contain the unity 1. In particular, aR is a proper ideal. It is nontrivial since $a = a \cdot 1 \in aR$.

Corollary 1 Suppose R is a commutative ring with unity. Then a proper ideal $I \subset R$ is maximal if and only if the factor ring R/I is a field.

Corollary 2 Suppose R is a commutative ring with unity. Then any maximal ideal in R is prime.

Remark. If the ring R is not commutative then the corollaries (and the preceding theorem) may fail. For example, in the ring $\mathcal{M}_{n,n}(\mathbb{R})$ of $n \times n$ matrices with real entries ($n \geq 2$), the trivial ideal is maximal but not prime. Note that this ring does have one-sided proper nontrivial ideals.

Ideals in the ring of polynomials

Theorem Let $\mathbb{F}$ be a field. Then any ideal in the ring $\mathbb{F}[x]$ is of the form

$$p(x)\mathbb{F}[x] = \{p(x)q(x) \mid q(x) \in \mathbb{F}[x]\}$$

for some polynomial $p(x) \in \mathbb{F}[x]$.

Theorem Let $\mathbb{F}$ be a field and $p(x) \in \mathbb{F}[x]$ be a polynomial of positive degree. Then the following conditions are equivalent:

- $p(x)$ is irreducible over $\mathbb{F}$,
- the ideal $p(x)\mathbb{F}[x]$ is prime,
- the ideal $p(x)\mathbb{F}[x]$ is maximal,
- the factor ring $\mathbb{F}[x]/p(x)\mathbb{F}[x]$ is a field.

Examples. • $\mathbb{F} = \mathbb{R}$, $p(x) = x^2 + 1$.

The polynomial $p(x) = x^2 + 1$ is irreducible over $\mathbb{R}$. Hence the factor ring $\mathbb{R}[x]/I$, where $I = (x^2 + 1)\mathbb{R}[x]$, is a field. Any element of $\mathbb{R}[x]/I$ is a coset $q(x) + I$. It consists of all polynomials in $\mathbb{R}[x]$ leaving a particular remainder when divided by $p(x)$. Therefore it is uniquely represented as $a + bx + I$ for some $a, b \in \mathbb{R}$. We obtain that

$$(a + bx + I) + (a' + b'x + I) = (a + a') + (b + b')x + I,$$
$$\begin{aligned}(a + bx + I)(a' + b'x + I) &= aa' + (ab' + ba')x + bb'x^2 + I \\ &= (aa' - bb') + (ab' + ba')x + bb'(x^2 + 1) + I \\ &= (aa' - bb') + (ab' + ba')x + I.\end{aligned}$$

It follows that a map $\phi : \mathbb{C} \to \mathbb{R}[x]/I$ given for all $a, b \in \mathbb{R}$ by $\phi(a + bi) = a + bx + I$ is an isomorphism of rings. Thus $\mathbb{R}[x]/I$ is a model of complex numbers. Note that the imaginary unit i corresponds to $x + I$, the coset of the monomial x.

- $\mathbb{F} = \mathbb{Z}_2,\ p(x) = x^2 + x + 1.$

We have $p(0) = p(1) = 1 \neq 0$ so that p has no zeros in $\mathbb{Z}_2$. Since $\deg(p) \leq 3$, it follows that the polynomial $p(x)$ is irreducible over $\mathbb{Z}_2$. Therefore $\mathbb{Z}_2[x]/(x^2 + x + 1)\mathbb{Z}_2[x]$ is a field. This factor ring consists of 4 elements: 0, 1, α and $\alpha + 1$, where $\alpha = x + p(x)\mathbb{Z}_2[x]$. Observe that α and $\alpha + 1$ are zeros of the polynomial p.

- $\mathbb{F} = \mathbb{Z}_2,\ p(x) = x^3 + x + 1.$

There are two polynomials of degree 3 irreducible over $\mathbb{Z}_2$: $p(x) = x^3 + x + 1$ and $q(x) = p(x - 1) = x^3 + x^2 + 1$. In particular, the factor ring $\mathbb{Z}_2[x]/(x^3 + x + 1)\mathbb{Z}_2[x]$ is a field. It consists of 8 elements: 0, 1, β, $\beta + 1$, β^2, $\beta^2 + 1$, $\beta^2 + \beta$ and $\beta^2 + \beta + 1$, where $\beta = x + p(x)\mathbb{Z}_2[x]$. Observe that β, β^2 and $\beta^2 + \beta$ are zeros of the polynomial p while $\beta + 1$, $\beta^2 + 1$ and $\beta^2 + \beta + 1$ are zeros of the polynomial q.