Class 21

April 12, 2024

Before we get into the topics of today's lecture, let's clarify some notation. Let R be a commutative ring and let $a \in R$. Then

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

For example, suppose $R = \mathbb{Z}$. Then

$$\langle 3 \rangle = 3\mathbb{Z} = \{3n | n \in \mathbb{Z}\}$$

For another example, consider $R = \mathbb{R}[x]$. Then

$$\langle x^2 - 2 \rangle = \left\{ \left(x^2 - 2\right) p(x) | p(x) \in \mathbb{R}[x] \right\}$$

Let's show $\langle a \rangle$ is an ideal of R. We can use the ideal test! First, suppose $ar_1, ar_2 \in \langle a \rangle$. Then

$$ar_1 - ar_2 = a(r_1 - r_2) \in \langle a \rangle$$

Now, suppose $s \in R$ and $ar \in \langle a \rangle$. Then

$$(ar)s = a(rs) \in \langle a \rangle$$

so $\langle a \rangle$ is an ideal. (Note as R is commutative, it suffices to show right multiplication absorbs. For a non-commutative ring you have to show both sides).

Ring Homomorphisms and Ring Isomorphisms

As with groups, we can show some of the structure of rings are preserved under homomorphisms and isomorphisms. For rings, we have to extend the definition slightly form the definition in groups.

Def

Let R and S be rings. A map $\phi : R \to S$ is a ring homomorphism if

1. $\phi(a+b) = \phi(a) + \phi(b)$
2. $\phi(ab) = \phi(a)\phi(b)$

Ex 1

Suppose $\phi : \mathbb{Z} \to \mathbb{Z}_2$ given by

$$\phi(x) =_2 x^2$$

To show this is a ring homomorphism, let's first show the addition property holds:

$$\phi(a+b) =_2 (a+b)^2 =_2 a^2 + 2ab + b^2 =_2 a^2 + b^2$$

as we are working mod 2, and $2ab$ is a multiple of 2, thus

$$\phi(a+b) =_2 a^2 + b^2 =_2 \phi(a) + \phi(b)$$

Now, for the multiplication property:

$$\phi(ab) =_2 (ab)^2 =_2 a^2b^2 =_2 \phi(a)\phi(b)$$

Ex 2

Let $\phi : \mathbb{R}[x] \to \mathbb{R}$ given by

$$\phi(p(x)) = p(1)$$

This is the map that takes a polynomial and plugs 1 in for x. For convenience, we will let

$$p(x) = \sum_{i=0}^{n} p_i x^i,\ \ q(x) = \sum_{j=0}^{m} q_j x^j$$

and without loss of generality, suppose $p_i = 0, q_j = 0$ for all $i > n, j > m$. First, let's show the addition property:

$$\phi(p(x) + q(x)) = \phi\left(\sum_{i=0}^{n} p_i x^i + \sum_{j=0}^{m} q_j x^j\right) = \phi\left(\sum_{i=0}^{\max\{n,m\}} (p_i + q_i) x^i\right)$$

plugging in $x = 1$:

$$= \sum_{i=0}^{\max\{n,m\}} (p_i + q_i)(1)^i = \sum_{i=0}^{\max\{n,m\}} (p_i + q_i)(1)^i = \sum_{i=0}^{n} p_i (1)^i + \sum_{j=0}^{m} q_j (1)^j = \phi\left(\sum_{i=0}^{n} p_i x^i\right) + \phi\left(\sum_{j=0}^{m} q_j x^j\right) = \phi(p(x)) + \phi(q(x))$$

Now to show multiplication:

$$\phi(p(x)\,q(x)) = \phi\left(\left(\sum_{i=0}^{n} p_i x^i\right)\left(\sum_{j=0}^{m} q_j x^j\right)\right) = \phi\left(\sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} p_j q_{i-j}\right) x^i\right)$$

plugging in $x = 1$

$$= \sum_{i=0}^{n+m}\left(\sum_{j=0}^{i} p_j q_{i-j}\right)(1)^i = \left(\sum_{i=0}^{n} p_i (1)^i\right)\left(\sum_{j=0}^{m} q_j (1)^j\right) = \phi\left(\sum_{i=0}^{n} p_i x^i\right)\phi\left(\sum_{j=0}^{m} q_j x^j\right) = \phi(p(x))\,\phi(q(x))$$

Def

Let $\phi : R \to S$ be a ring homomorphism. If ϕ is also a bijection, then ϕ is a ring isomorphism. If $R = S$, then ϕ is a ring automorphism.

Non Ex 1

Let $\phi : \mathbb{Z}[x] \to \mathbb{Z}[x]$ given by

$$\phi(p(x)) = -p(x)$$

Then ϕ is not a ring isomorphism. To show this, we will consider each property: For the addition property:

$$\phi(p(x) + q(x)) = -(p(x) + q(x)) = -p(x) - q(x) = \phi(p(x)) + \phi(q(x))$$

For the multiplication property:

$$\phi(p(x)\,q(x)) = -(p(x)\,q(x)) \neq (-p(x))(-q(x)) = \phi(p(x))\,\phi(q(x))$$

So the multiplication property will not hold.

Ex 2

Suppose $\phi : \mathbb{Q}[x] / \langle x^2 - 2 \rangle \to \mathbb{Q}[\sqrt{2}]$ given by

$$\phi\left(ax + b + \langle x^2 - 2 \rangle\right) = a\sqrt{2} + b$$

Then ϕ is a ring isomorphism. To show this, we can start by showing the addition and multiplication properties:

$$\phi\left(\left(ax + b + \langle x^2 - 2 \rangle\right) + \left(cx + d + \langle x^2 - 2 \rangle\right)\right) = \phi\left((a + c)x + (b + d)\right) = (a + c)\sqrt{2} + (b + d)$$

$$= a\sqrt{2} + b + c\sqrt{2} + d = \phi\left(ax + b + \langle x^2 - 2 \rangle\right) + \phi\left(cx + d + \langle x^2 - 2 \rangle\right)$$

Now for the multiplication property:

$$\phi\left(\left(ax + b + \langle x^2 - 2 \rangle\right)\left(cx + d + \langle x^2 - 2 \rangle\right)\right) = \phi\left(acx^2 + (a + d)x + bd + \langle x^2 - 2 \rangle\right)$$

But as we have quotiented $\mathbb{Q}[x]$ by $\langle x^2 - 2 \rangle$, then

$$acx^2 + (a + d)x + bd + \langle x^2 - 2 \rangle = acx^2 + (a + d)x + bd - ac\left(x^2 - 2\right) + \langle x^2 - 2 \rangle = (a + d)x + bd + 2ac + \langle x^2 - 2 \rangle$$

Thus

$$\phi\left(\left(ax + b + \langle x^2 - 2 \rangle\right)\left(cx + d + \langle x^2 - 2 \rangle\right)\right) = \phi\left((a + d)x + bd + 2ac + \langle x^2 - 2 \rangle\right)$$

$$= (a + d)\sqrt{2} + bd + 2ac = \left(a\sqrt{2} + b\right)\left(c\sqrt{2} + d\right) = \phi(ax + b)\,\phi(cx + d)$$

Now, let's show we have a bijection. For onto, suppose $a\sqrt{2} + b \in \mathbb{Q}[x]$. Then $\phi\left(ax + b + \langle x^2 - 2 \rangle\right) = a\sqrt{2} + b$, so ϕ is onto. Now, suppose

$$\phi\left(ax + b + \langle x^2 - 2 \rangle\right) = \phi\left(cx + d + \langle x^2 - 2 \rangle\right)$$

Then

$$a\sqrt{2} + b = c\sqrt{2} + d$$

thus $a = c$ and $b = d$, so

$$ax + b + \langle x^2 - 2 \rangle = cx + d + \langle x^2 - 2 \rangle$$

and ϕ is one-to-one. As all of the conditions are satisfied, then ϕ is a ring isomorphism.

Properties of Ring Isomorphisms

Let R, S be rings and $\phi : R \to S$ be a ring isomorphism. Further, let

1. Ring Isomorphisms form an equivalence relation.
2. The composition of ring isomorphisms are a ring isomorphism.
3. $\phi(0) = 0$
4. If R is a ring with unity, then $\phi(1) = 1$.
5. $\phi(-a) = -a$
6. If R is a ring with unity and a is a unit, then $\phi\left(a^{-1}\right) = \phi(a)^{-1}$.
7. R is a commutative ring if and only if S is a commutative ring.
8. a is a zero divisor in R if and only if $\phi(a)$ is a zero divisor in S.
9. R is an integral domain if and only if S is an integral domain.
10. R is a field if and only if S is a field.

Pf

Properties 1 and 2 will be left as exercises for a future assignment.

3)

Consider $\phi(0) = \phi(0+0) = \phi(0) + \phi(0)$. Then subtracting $\phi(0)$ from both sides, we get

$$0 = \phi(0) - \phi(0) = \phi(0) + \phi(0) - \phi(0) = \phi(0)$$

4)

Consider $a \in R$:

$$\phi(a) = \phi(1a) = \phi(1)\phi(a)$$

So $\phi(1) = 1$.

5)

Consider

$$0 = \phi(0) = \phi(a-a) = \phi(a) + \phi(-a)$$

so $-\phi(a) = \phi(-a)$.

6)

Suppose a is a unit in R. Then

$$1 = \phi(1) = \phi\left(aa^{-1}\right) = \phi(a)\phi\left(a^{-1}\right)$$

So $\phi(a)^{-1} = \phi\left(a^{-1}\right)$

7)

First, suppose R is a commutative ring. Then

$$\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$$

for all $a, b \in R$. As ϕ is onto, this implies $\phi(a)\phi(b) = \phi(b)\phi(a)$ for all $\phi(a), \phi(b) \in S$. Now, suppose S is a commutative ring. Let $a, b \in R$. Then

$$\phi(ab) = \phi(a)\phi(b) = \phi(b)\phi(a) = \phi(ba)$$

and as ϕ is one-to-one, then $ab = ba$.

8)

Suppose a is a zero divisor in R. Then $\exists b \in R$ such that $ab = 0$ and $a, b \neq 0$. Thus

$$0 = \phi(0) = \phi(ab) = \phi(a)\phi(b)$$

But as ϕ is one-to-one and $a, b \neq 0$, then $\phi(a), \phi(b) \neq 0$. Thus $\phi(a)$ is a zero divisor. Now, suppose $\phi(a)$ is a zero divisor in S. Then $\exists \phi(b) \neq 0$ such that

$$\phi(0) = 0 = \phi(a)\phi(b) = \phi(ab)$$

but as ϕ is one-to-one, $0 = ab$ and as $\phi(a), \phi(b)$ are both non-zero, then so are a, b and thus a is a zero divisor.

9)

This follows by **4)** (which implies that both rings will have an identity), **7)** (which implies both rings will be commutative), and **8)**, (which ensures each ring will have no zero divisors).

10)

This follows by **4)** (which implies that both rings will have an identity), **6)** (which ensures every nonzero element of both rings are units),and **7)** (which implies both rings will be commutative).