Visual Algebra

Lecture 8.4: Ring homomorphisms

Dr. Matthew Macauley

School of Mathematical & Statistical Sciences
Clemson University
South Carolina, USA
http://www.math.clemson.edu/~macaule/

Group theory

- normal subgroups are characterized by being invariant under conjugation:

$$H \leq G \text{ is normal} \quad \text{iff} \quad ghg^{-1} \in H \text{ for all } g \in G,\ h \in H.$$

- The quotient G/N exists iff N is a normal: $N \trianglelefteq G$.
- A homomorphism is a structure-preserving map: $f(x * y) = f(x) * f(y)$.
- The kernel of a homomorphism is normal: $\mathrm{Ker}(\phi) \trianglelefteq G$.
- If $N \trianglelefteq G$, there is a natural quotient $\pi\colon G \to G/N$, $\pi(g) = gN$.
- There are four isomorphism theorems.

Ring theory

- (left) ideals of rings are characterized by being invariant under (left) multiplication:

$$I \subseteq R \text{ is a (left) ideal} \quad \text{iff} \quad rx \in I \text{ for all } r \in R,\ x \in I.$$

- The quotient ring R/I exists iff I is a two-sided ideal: $I \trianglelefteq R$.
- A homomorphism is structure-preserving: $f(x+y) = f(x)+f(y)$, $f(xy) = f(x)f(y)$.
- The kernel of a homomorphism is a two-sided ideal: $\mathrm{Ker}(\phi) \trianglelefteq R$.
- If $I \trianglelefteq R$, there is a natural quotient $\pi\colon R \to R/I$, $\pi(r) = r + I$.
- There are four isomorphism theorems.

A familiar example

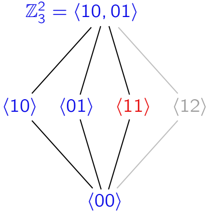
Consider the ring $R = \mathbb{Z}_3^2 = \{ab \mid a, b \in \mathbb{Z}_3\}$.

We know that the following map is a group homomorphism:

$$\phi \colon \mathbb{Z}_3^2 \to \mathbb{Z}_3, \qquad \phi(ab) = b.$$

The table below (right) shows it's also a ring homomorphism.

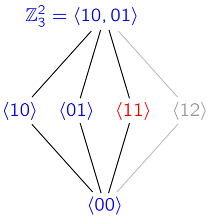
Do you see why $\langle 10 \rangle$ is an ideal?



+	00	10	20	01	11	21	02	12	22
00	00	10	20	01	11	21	02	12	22
10	10	-0	00	11	-1	01	12	-2	02
20	20	00	10	21	01	11	22	02	12
01	01	11	21	02	12	22	00	10	20
11	11	-1	01	12	-2	02	10	-0	00
21	21	01	11	22	02	12	20	00	10
02	02	12	22	00	10	20	01	11	21
12	12	-2	02	10	-0	00	11	-1	01
22	22	02	12	20	00	10	21	01	11

×	00	10	20	01	11	21	02	12	22
00	00	00	00	00	00	00	00	00	00
10	00	-0	20	00	-0	20	00	-0	20
20	00	20	10	00	20	10	00	20	10
01	00	00	00	01	01	01	02	02	02
11	00	-0	20	01	-1	21	02	-2	22
21	00	20	10	01	21	11	02	22	12
02	00	00	00	02	02	02	01	01	01
12	00	-0	20	02	-2	22	01	-1	21
22	00	20	10	02	22	12	01	21	11

Different types of substructures



Let's consider two other subgroups of $R = \mathbb{Z}_3^2$.

- The subgroup $\langle 11 \rangle$ is a subring but not an ideal.
- The subgroup $\langle 12 \rangle$ is a not even a subring.

$\times$	00	11	22	12	21	10	20	01	02
00	00	00	00	00	00	00	00	00	00
11	00	11	22	12	21	10	20	01	02
22	00	22	11	21	12	20	10	02	01
12	00	12	21	11	22	10	20	01	02
21	00	21	12	22	11	20	10	02	01
10	00	10	20	10	20	10	20	00	00
20	00	20	10	20	10	20	10	00	00
01	00	01	02	02	01	00	00	01	02
02	00	02	01	01	02	00	00	02	01

$\times$	00	12	21	10	22	01	11	20	02
00	00	00	00	00	00	00	00	00	00
12	00	11	22	10	21	02	12	20	01
21	00	22	11	20	12	01	21	10	02
10	00	10	20	10	20	00	10	20	00
22	00	21	12	20	11	02	22	10	01
01	00	02	01	00	02	01	01	00	02
11	00	12	21	10	22	01	11	20	02
20	00	20	10	20	10	00	20	10	00
02	00	01	02	00	01	02	02	00	01

Quotient rings

Since an ideal I of R is an additive subgroup (and hence normal):

- $R/I = \{x + I \mid x \in R\}$ is the set of cosets of I in R;
- R/I is a quotient group; with the binary operation (addition) defined as

$$(x + I) + (y + I) := x + y + I.$$

It turns out that if I is also a two-sided ideal, then we can make R/I into a ring.

Proposition

If $I \subseteq R$ is a (two-sided) ideal, then R/I is a ring (called a quotient ring), where multiplication is defined by

$$(x + I)(y + I) := xy + I.$$

Proof

We need to show this is well-defined. Suppose $x + I = r + I$ and $y + I = s + I$. This means that $x - r \in I$ and $y - s \in I$.

It suffices to show that $xy + I = rs + I$, or equivalently, $xy - rs \in I$:

$$xy - rs = xy - ry + ry - rs = \underbrace{(x - r)}_{\in I} y + r \underbrace{(y - s)}_{\in I} \in I\,.$$

Ring homomorphisms

Definition

A ring homomorphism is a function $f\colon R \to S$ satisfying

$$f(x+y) = f(x) + f(y) \qquad \text{and} \qquad f(xy) = f(x)f(y) \quad \text{for all } x, y \in R.$$

A ring isomorphism is a homomorphism that is bijective.

The kernel is the set $\mathrm{Ker}(f) := \{x \in R \mid f(x) = 0\}$.

Examples

1. The ring homomorphism $\phi\colon \mathbb{Z} \to \mathbb{Z}_n$ sending $k \mapsto k \pmod{n}$ has $\mathrm{Ker}(\phi) = n\mathbb{Z}$.
2. For a fixed real number $\alpha \in \mathbb{R}$, the "evaluation function"

   $$\phi\colon \mathbb{R}[x] \longrightarrow \mathbb{R}\,, \qquad \phi\colon p(x) \longmapsto p(\alpha)$$

   is a homomorphism. The kernel consists of all polynomials that have α as a root.
3. For any ideal $I \trianglelefteq R$, the canonical quotient map is the homomorphism

   $$\pi\colon R \longrightarrow R/I, \qquad r \longmapsto r + I.$$

4. The following quotient, for ideal $I = (x^2 + x + 1)$ in $\mathbb{F}_2[x]$, defines the finite field $\mathbb{F}_4$:

   $$\phi\colon \mathbb{F}_2[x] \longrightarrow \mathbb{F}_2[x]/I, \qquad f(x) \longmapsto f(x) + I.$$

Isomoprhism theorem prerequisites

Proposition

The kernel of a ring homomorphism $\phi\colon R \to S$ is a two-sided ideal.

Proof

We know that $\mathrm{Ker}(\phi)$ is an additive subgroup of R. We must show that it's an ideal.

Left ideal: Let $k \in \mathrm{Ker}(\phi)$ and $r \in R$. Then

$$\phi(rk) = \phi(r)\phi(k) = \phi(r) \cdot 0 = 0 \quad \Longrightarrow \quad rk \in \mathrm{Ker}(\phi). \qquad \checkmark$$

Showing that $\mathrm{Ker}(\phi)$ is a right ideal is analogous. $\square$

Proposition

The sum $S + I = \{s + i \mid s \in S,\ i \in I\}$ of a sum and an ideal is a subring of R.

Proof

$S + I$ is an additive subgroup, and it's closed under multiplication because

$$s_1, s_2 \in S,\ i_1, i_2 \in I \quad \Longrightarrow \quad (s_1 + i_1)(s_2 + i_2) = \underbrace{s_1 s_2}_{\in S} + \underbrace{s_1 i_2 + i_1 s_2 + i_1 i_2}_{\in I} \in S + I. \qquad \square$$

Basic properties of ring homomorphisms

Proposition

A ring homomorphism $\phi\colon R \to S$ is **one-to-one** if and only if $\mathrm{Ker}(\phi) = \{0\}$.

Proof

"$\Rightarrow$" Suppose ϕ is 1-to-1, and let $r \in \mathrm{Ker}(\phi)$. Then $\phi(0) = 0 = \phi(r)$, so $r = 0$. ✓

"$\Leftarrow$" Suppose $\mathrm{Ker}(\phi) = \{0\}$, and say $\phi(x) = \phi(y)$.

Then $0 = \phi(x) - \phi(y) = \phi(x - y) \;\Rightarrow\; x - y \in \mathrm{Ker}(\phi) \;\Rightarrow\; x - y = 0$. ✓

Proposition

Every nontrivial homomorphism $\phi\colon F \to R$ from a field is **one-to-one**.

Proof

Every non-zero element of a field is a unit.

If an ideal I contains a unit, then $I = R$.

Thus, if $\mathrm{Ker}(\phi) \lneq R$, then $\mathrm{Ker}(\phi) = \{0\}$, and hence ϕ is injective. $\square$

The isomorphism theorems for rings

All of the isomorphism theorems for groups have analogues for rings.

- Fundamental homomorphism theorem: "*All homomorphic images are quotients*"
- Correspondence theorem: Characterizes "*subrings and ideals of quotients*"
- Fraction theorem: Characterizes "*quotients of quotients*"
- Diamond theorem: Characterizes "*duality of subquotients*"

We'll state and prove these in the next lecture.

We'll also see a number of visuals that illustrate them.

These will be analogous to the visuals that we saw for the group isomorphism theorems.

This is one reason why it's important to not abandon finite rings.