Lecture 7.3: Ring homomorphisms

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4120, Modern Algebra

Motivation (spoilers!)

Many of the big ideas from group homomorphisms carry over to ring homomorphisms.

Group theory

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

Ring theory

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

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 $f\colon R \to S$ is the set $\operatorname{Ker} f := \{x \in R : f(x) = 0\}$.

Examples

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

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

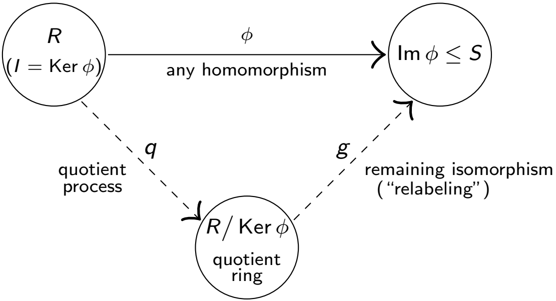
   is a homomorphism. The kernel consists of all polynomials that have α as a root.
3. The following is a homomorphism, for the ideal $I = (x^2 + x + 1)$ in $\mathbb{Z}_2[x]$:

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

The isomorphism theorems for rings

Fundamental homomorphism theorem

If $\phi\colon R \to S$ is a ring homomorphism, then $\operatorname{Ker}\phi$ is an ideal and $\operatorname{Im}(\phi) \cong R/\operatorname{Ker}(\phi)$.



Proof (HW)

The statement holds for the underlying additive group R. Thus, it remains to show that $\operatorname{Ker}\phi$ is a (two-sided) ideal, and the following map is a ring homomorphism:

$$g\colon R/I \longrightarrow \operatorname{Im}\phi\,, \qquad g(x+I) = \phi(x)\,.$$

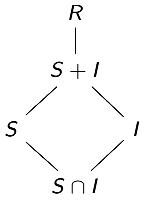
The second isomorphism theorem for rings

Suppose S is a subring and I an ideal of R. Then

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

(ii) The following quotient rings are isomorphic:

$$(S+I)/I \cong S/(S\cap I)\,.$$



Proof (sketch)

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

$$s_1,s_2\in S,\ i_1,i_2\in I \quad\Longrightarrow\quad (s_1+i_1)(s_2+i_2)=\underbrace{s_1s_2}_{\in S}+\underbrace{s_1i_2+i_1s_2+i_1i_2}_{\in I}\in S+I.$$

Showing $S\cap I$ is an ideal of S is straightforward (homework exercise).

We already know that $(S+I)/I\cong S/(S\cap I)$ as additive groups.

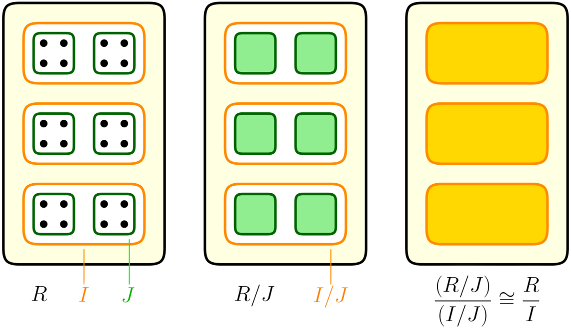
One explicit isomorphism is $\phi\colon s+(S\cap I)\mapsto s+I$. It is easy to check that $\phi\colon 1\mapsto 1$ and ϕ preserves products. □

The third isomorphism theorem for rings

Freshman theorem

Suppose R is a ring with ideals $J \subseteq I$. Then I/J is an ideal of R/J and

$$(R/J)/(I/J) \cong R/I\,.$$

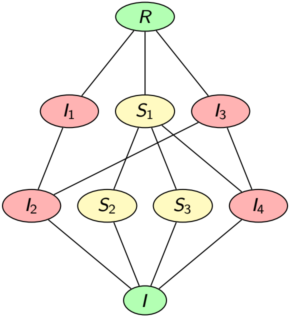


(Thanks to Zach Teitler of Boise State for the concept and graphic!)

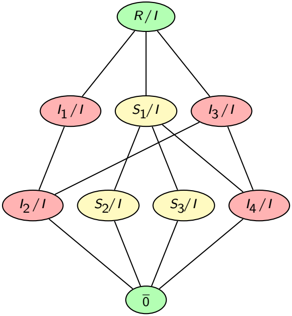
The fourth isomorphism theorem for rings

Correspondence theorem

Let I be an ideal of R. There is a bijective correspondence between subrings (& ideals) of R/I and subrings (& ideals) of R that contain I. In particular, every ideal of R/I has the form J/I, for some ideal J satisfying $I \subseteq J \subseteq R$.



subrings & ideals that contain I



subrings & ideals of R/I

Maximal ideals

Definition

An ideal I of R is maximal if $I \neq R$ and if $I \subseteq J \subseteq R$ holds for some ideal J, then $J = I$ or $J = R$.

A ring R is simple if its only (two-sided) ideals are 0 and R.

Examples

1. If $n \neq 0$, then the ideal $M = (n)$ of $R = \mathbb{Z}$ is maximal if and only if n is prime.
2. Let $R = \mathbb{Q}[x]$ be the set of all polynomials over $\mathbb{Q}$. The ideal $M = (x)$ consisting of all polynomials with constant term zero is a maximal ideal.

   Elements in the quotient ring $\mathbb{Q}[x]/(x)$ have the form $f(x) + M = a_0 + M$.
3. Let $R = \mathbb{Z}_2[x]$, the polynomials over $\mathbb{Z}_2$. The ideal $M = (x^2 + x + 1)$ is maximal, and $R/M \cong \mathbb{F}_4$, the (unique) finite field of order 4.

In all three examples above, the quotient R/M is a field.

Maximal ideals

Theorem

Let R be a commutative ring with 1. The following are equivalent for an ideal $I \subseteq R$.

(i) I is a maximal ideal;

(ii) R/I is simple;

(iii) R/I is a field.

Proof

The equivalence (i)$\Leftrightarrow$(ii) is immediate from the Correspondence Theorem.

For (ii)$\Leftrightarrow$(iii), we'll show that an *arbitrary* ring R is simple iff R is a field.

"$\Rightarrow$": Assume R is simple. Then $(a) = R$ for any nonzero $a \in R$.

Thus, $1 \in (a)$, so $1 = ba$ for some $b \in R$, so $a \in U(R)$ and R is a field. ✓

"$\Leftarrow$": Let $I \subseteq R$ be a nonzero ideal of a field R. Take any nonzero $a \in I$.

Then $a^{-1}a \in I$, and so $1 \in I$, which means $I = R$. ✓ □

Prime ideals

Definition

Let R be a commutative ring. An ideal $P \subset R$ is prime if $ab \in P$ implies either $a \in P$ or $b \in P$.

Note that $p \in \mathbb{N}$ is a prime number iff $p = ab$ implies either $a = p$ or $b = p$.

Examples

1. The ideal (n) of $\mathbb{Z}$ is a prime ideal iff n is a prime number (possibly $n = 0$).
2. In the polynomial ring $\mathbb{Z}[x]$, the ideal $I = (2, x)$ is a prime ideal. It consists of all polynomials whose constant coefficient is even.

Theorem

An ideal $P \subseteq R$ is prime iff R/P is an integral domain.

The proof is straightforward (HW). Since fields are integral domains, the following is immediate:

Corollary

In a commutative ring, every maximal ideal is prime.