Math 5111 (Algebra 1)

Lecture #3 $\sim$ September 17, 2020

Rings Part 2:

- Ideals and Quotient Rings
- Isomorphisms
- Homomorphisms

This material represents §1.3.4-1.3.8 from the course notes.

Ideals, I

Our next task is to generalize the idea of modular arithmetic into general rings.

- In $\mathbb{Z}$ and $F[x]$, we defined modular congruences using divisibility, but let us take a broader approach: if I is a subset of R (whose properties we intend to characterize in a moment) let us say that two elements $a, b \in R$ are "congruent modulo I" if $a - b \in I$.
- We would like "congruence modulo I" to be an equivalence relation: this requires $a \equiv a \pmod{I}$, $a \equiv b \pmod{I}$ implies $b \equiv a \pmod{I}$, and $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$ implies $a \equiv c \pmod{I}$.
- It is easy to see that these three conditions require $0 \in I$, that I be closed under additive inverses, and that I be closed under addition. (Thus, I is in fact closed under subtraction.)

Ideals, II

We also want congruences to respect addition and multiplication.

- If $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$, then we want $a + c \equiv b + d \pmod{I}$ and $ac \equiv bd \pmod{I}$.
- In terms of ring elements, this is equivalent to the following: if $b = a + r$ and $d = c + s$ for some $r, s \in I$, then we want $(b + d) - (a + c) = r + s$ to be in I, and we also want $bd - ac = (a + r)(c + s) - ac = as + rc + rs$ to be in I.
- The first condition clearly follows from the requirement that I is closed under addition. It is a bit less obvious how to handle the second condition, but one immediate implication follows by setting $a = c = 0$: namely, that $rs \in I$.
- Thus, I must be closed under $\cdot$, so it must be a subring.
- But more is needed: since $0 \in I$, we can set $r = 0$ to see that $as \in I$, and we can also set $s = 0$ to see that $rc \in I$.

Ideals, III

- So in fact, I must be closed under (left and right) multiplication by *arbitrary* elements of R, in addition to being a subring. It is then easy to see that this condition is also sufficient to ensure that $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$ imply $a + c \equiv b + d \pmod{I}$ and $ac \equiv bd \pmod{I}$.
- Our last task is to define residue classes and then the ring operations: we define the residue class $\overline{a}$ (modulo I) to be the set of ring elements b congruent to a modulo I, which is to say, $\overline{a} = \{a + r \,:\, r \in I\}$.
- Then we take the operations on residue classes to be $\overline{a} + \overline{b} = \overline{a + b}$ and $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$, and by properties of congruences, these operations will be well-defined and the collection of residue classes will form a ring.

Ideals, IV

Now we just have to run through the discussion more formally:

Definition

A subset I of a ring R that is closed under arbitrary left and right multiplication by elements of R is called an ideal of R (or, for emphasis, a two-sided ideal).

- Explicitly, I is an ideal if I contains 0 and for any $x, y \in I$ and any $r \in R$, the elements $x - y$, rx, and xr are all in I.
- There are one-sided notions of ideals as well: a left ideal is closed under arbitrary left multiplication, while a right ideal is closed under arbitrary right multiplication.
- If R is commutative, then left ideals, right ideals, and two-sided ideals are the same.

Ideals, V

Examples:

1. The subrings $n\mathbb{Z}$ are ideals of $\mathbb{Z}$, since they are clearly closed under arbitrary multiplication by elements of $\mathbb{Z}$.
2. If $R = F[x]$ and p is any polynomial, the subring pR of multiples of p is an ideal of $F[x]$, since it is closed under arbitrary multiplication by polynomials in $F[x]$.
3. The subring $\mathbb{Z}$ of $\mathbb{Q}$ is not an ideal of $\mathbb{Q}$, since it is not closed under arbitrary multiplication by elements of $\mathbb{Q}$, since for example if we take $r = \frac{1}{3} \in \mathbb{Q}$ and $x = 4 \in \mathbb{Z}$, the element $rx = \frac{4}{3}$ is not in $\mathbb{Z}$.
4. For any ring R, the subrings $\{0\}$ and R are ideals of R. We refer to $\{0\}$ as the trivial ideal (or the "zero ideal") and refer to any ideal $I \neq R$ as a proper ideal (since it is a proper subset of R).

Ideals, VI

Examples:

5. In the ring $R = \mathbb{Z}[x]$, the set S of polynomials with even constant term is an ideal of R. It is not hard to see that $0 \in S$, that S is closed under subtraction, and that the product of any polynomial with an element of S also has even constant term, so S is closed under arbitrary R-multiplication.
6. The set $S = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ of "even" residue classes is an ideal of $\mathbb{Z}/8\mathbb{Z}$. It is not hard to verify that this set is closed under subtraction and arbitrary R-multiplication.
7. The set $S = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$ is not an ideal of $\mathbb{Z}/7\mathbb{Z}$ since it is not closed under addition. (The problem is that 7 is odd.)
8. The set $S = \{(2a, 3a) : a \in \mathbb{Z}\}$ is not an ideal of $\mathbb{Z} \times \mathbb{Z}$: although it is a subring, it is not closed under arbitrary R-multiplication since for example $(1, 2) \cdot (2, 3) = (2, 6)$ is not in S, even though $(2, 3)$ is.

Ideals, VII

Proposition (Principal Ideals)

If R is a commutative ring with 1, the set $(a) = \{ra : r \in R\}$ of all R-multiples of a forms a (two-sided) ideal of R, known as the principal ideal generated by a.

Proof:

- Since $0a = 0$ we see $0 \in (a)$. Furthermore, since $ra - sa = (r - s)a$ we see that (a) is closed under subtraction.
- Furthermore, if $t \in R$ then we have $t(ra) = (tr)a$, so since R is commutative, (a) is closed under multiplication by arbitrary elements of R. Thus, (a) is an ideal.

We will remark that in any Euclidean domain (like $\mathbb{Z}$ or $F[x]$), every ideal is principal (an element of minimum norm will generate the ideal).

Quotient Rings, I

Definition

If I is an ideal of the ring R, then we say a is congruent to b modulo I, written $a \equiv b \pmod{I}$, if $a - b \in I$.

- As in $\mathbb{Z}$ and $F[x]$, congruence modulo I is an equivalence relation that respects addition and multiplication (that was the whole point of the discussion last time where I derived the defining property of an ideal.
- The proofs are the same as in $\mathbb{Z}$ and $F[x]$ upon converting "divisibility" into "containment in I".

I will mention also that it is not common to use the language of congruences with ideals. I am only phrasing things this way to underscore the analogies with $\mathbb{Z}/m\mathbb{Z}$ and $F[x]/(p)$.

Quotient Rings, II

Now we observe all of our basic properties of congruences:

Proposition (Ideal Congruences)

Let I be an ideal of R and $a, b, c, d \in R$. Then the following are true:

1. $a \equiv a \pmod{I}$.
2. $a \equiv b \pmod{I}$ *if and only if* $b \equiv a \pmod{I}$.
3. *If* $a \equiv b \pmod{I}$ *and* $b \equiv c \pmod{I}$, *then* $a \equiv c \pmod{I}$.
4. *If* $a \equiv b \pmod{I}$ *and* $c \equiv d \pmod{I}$, *then* $a + c \equiv b + d \pmod{I}$.
5. *If* $a \equiv b \pmod{I}$ *and* $c \equiv d \pmod{I}$, *then* $ac \equiv bd \pmod{I}$.

Proofs: Straightforward from the definition of an ideal.

Quotient Rings, III

Next, residue classes:

Definition

If I is an ideal of the ring R, then for any $a \in R$ we define the residue class of a modulo I to be the set $\overline{a} = a + I = \{a + x : x \in I\}$. This set is also called the coset of I represented by a.

- We will use the notations $\overline{a}$ and $a + I$ interchangeably. (The latter is intended to evoke the idea of "adding" a to the set I.)
- We observe, as with our previous examples of residue classes, that any two residue classes are either disjoint or identical and that they partition R: specifically, $\overline{a} = \overline{b}$ if and only if $a \equiv b \pmod{I}$ if and only if $a - b \in I$.

Quotient Rings, IV

All that remains is to verify that the residue classes form a ring, in the same way as in $\mathbb{Z}$ and $F[x]$:

Theorem (Quotient Rings)

Let I be an ideal of the ring R. Then the collection of residue classes modulo I forms a ring, denoted R/I (read as "R mod I"), under the operations $\overline{a} + \overline{b} = \overline{a+b}$ and $\overline{a} \cdot \overline{b} = \overline{ab}$. (This ring is called the quotient ring of R by I.) If R is commutative then so is R/I, and likewise if R has a 1 then so does R/I.

The notation R/I is intended to emphasize the idea that I represents a single element (namely, $\overline{0}$) in the quotient ring R/I, and the other elements in R/I are "translates" of I. In this way, R/I is the ring obtained from R by "collapsing" or "dividing out" by I, whence the name "quotient ring".

Quotient Rings, V

Proof:

- The proof is essentially bookkeeping, and the only real content is to show that the operations are well-defined: that is, if we choose different elements $a' \in \bar{a}$ and $b' \in \bar{b}$, the residue class of $a' + b'$ is the same as that of $a + b$, and similarly for the product.
- To see this, if $a' \in \bar{a}$ then $a' \equiv a \pmod{I}$, and similarly if $b' \in \bar{b}$ then $b' \equiv b \pmod{I}$.
- Then $a' + b' \equiv a + b \pmod{I}$, so $\overline{a' + b'} = \overline{a + b}$. Likewise, $a'b' \equiv ab \pmod{I}$, so $\overline{a'b'} = \overline{ab}$.
- Thus, the operations are well-defined.

Quotient Rings, VI

Proof (continued):

- Now we just observe that the ring axioms are essentially inherited from R.
- For the ring axioms [R1]-[R6], we observe that associativity, commutativity, and the distributive laws follow immediately from the corresponding properties in R: the additive identity in R/I is $\overline{0}$ and the additive inverse of $\overline{a}$ is $\overline{-a}$.
- For example, for [R2] we have $\overline{a} + \overline{b} = \overline{a + b} = \overline{b + a} = \overline{b} + \overline{a}$.
- Finally, if R is commutative then so will be the multiplication of the residue classes, and if R has a 1 then the residue class $\overline{1}$ is easily seen to be a multiplicative identity in R/I.

Quotient Rings, VII

This general description of "quotient rings" generalizes the two examples we have previously discussed: $\mathbb{Z}/m\mathbb{Z}$ and $F[x]/p$.

- To be explicit, $\mathbb{Z}/m\mathbb{Z}$ is the quotient of $\mathbb{Z}$ by the ideal $m\mathbb{Z}$, while $F[x]/p$ is the quotient of the polynomial ring $F[x]$ by the principal ideal (p) consisting of all multiples of p.
- It is not hard to see that the integer congruence $a \equiv b \pmod{m}$, originally defined as being equivalent to the statement $m|(b-a)$, is the same as the congruence $a \equiv b \pmod{I}$ where I is the ideal $m\mathbb{Z}$, since $b - a \in m\mathbb{Z}$ precisely when $b - a$ is a multiple of m.

Quotient Rings, VIII

First, the trivial examples:

Example: If R is any ring, the quotient ring of R by the zero ideal, namely $R/0$, has the same structure as R itself.

- Explicitly, if $I = 0$, then $a + I = \{a\}$ for all $a \in R$, so the operations in R/I are exactly the same as in R itself.

Example: If R is any ring, the quotient ring of R by itself, namely R/R, has the same structure as the trivial ring $\{0\}$.

- Explicitly, if $I = R$, then $a + I = R$ for all $a \in R$, so there is only one residue class in R/R, meaning that R/R must be the trivial ring.

Quotient Rings, IX

Example: In $R = \mathbb{Z}[x]$, with I consisting of all multiples of $x^2 + 1$, describe the structure of the quotient ring R/I.

- It is easy to see that I is an ideal of R, since it is a subring that is closed under arbitrary multiplication by elements of R.
- From our discussion of polynomial rings, we know that the residue classes in R/I are represented uniquely by residue classes of the form $\overline{a + bx}$ where $a, b \in \mathbb{Z}$. Note that in this quotient ring, we have $\overline{x}^2 + \overline{1} = \overline{0}$, which is to say, $\overline{x}^2 = -\overline{1}$.
- The addition in this quotient ring is given by $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$ while the multiplication is given by $\overline{a + bx} \cdot \overline{c + dx} = \overline{(ac - bd) + (ad + bc)x}$, which follows from the distributive law and the fact that $\overline{x}^2 = -\overline{1}$.

The operations in this ring are the same as those in the Gaussian integer ring $\mathbb{Z}[i]$, except with $\overline{x}$ in place of i.

Quotient Rings, X

Example: In $R = \mathbb{Z}/8\mathbb{Z}$, with $I = \{0, 4\}$, describe the structure of the quotient ring R/I.

- Note that I is the principal ideal generated by 4.
- Since each residue class contains 2 elements, and R has 8 elements in total, there are four residue classes. With this observation in hand, it is not hard to give a list: $\overline{0} = I = \{0, 4\}$, $\overline{1} = 1 + I = \{1, 5\}$, $\overline{2} = 2 + I = \{2, 6\}$, and $\overline{3} = 3 + I = \{3, 7\}$.
- Notice, for example, that in the quotient ring R/I, we have $\overline{1} + \overline{3} = \overline{0}$, $\overline{2} \cdot \overline{2} = \overline{0}$, and $\overline{2} \cdot \overline{3} = \overline{2}$: indeed, we can see that the structure of R/I is exactly the same as $\mathbb{Z}/4\mathbb{Z}$ (the labelings of the elements are even the same).

Quotient Rings, XI

Example: In the polynomial ring $R = \mathbb{Z}[x]$, with I consisting of the polynomials with even constant term (i.e., the polynomials of the form $2a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ for integers a_i), describe the structure of the quotient ring R/I.

- We observe that there are only two residue classes, namely $\overline{0}$ and $\overline{1}$: to see this observe that $p(x) \in \overline{0}$ when the constant term of p is even, and $p(x) \in \overline{1}$ when the constant term of p is odd.
- Then one can verify that the structure of this quotient ring is "the same" as $\mathbb{Z}/2\mathbb{Z}$ (with, for example, $\overline{1} + \overline{1} = \overline{0}$).

Ring Isomorphisms, I

Our next task is to describe what it means to say that two rings have the same structure. Consider $R = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$:

$+$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(0,0)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(0,0)$	$(0,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(0,1)$	$(0,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(1,0)$	$(1,1)$	$(0,0)$

$\cdot$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$	$(0,0)$
$(1,1)$	$(0,0)$	$(1,1)$	$(1,0)$	$(0,1)$
$(1,0)$	$(0,0)$	$(1,0)$	$(1,0)$	$(0,0)$
$(0,1)$	$(0,0)$	$(0,1)$	$(0,0)$	$(0,1)$

and also $S = \mathbb{F}_2[x]/(x^2 + x)$:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	x	0
$x+1$	0	$x+1$	0	$x+1$

If we relabel $(0,0)$ as 0, $(1,1)$ as 1, $(1,0)$ as x, and $(0,1)$ as $x+1$, the first pair of tables becomes the second set of tables.

Ring Isomorphisms, II

Also compare $\mathbb{Z}/6\mathbb{Z}$ to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\cdot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$+$	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,0)	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(1,1)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)	(0,0)
(0,2)	(0,2)	(1,0)	(0,1)	(1,2)	(0,0)	(1,1)
(1,0)	(1,0)	(0,1)	(1,2)	(0,0)	(1,1)	(0,2)
(0,1)	(0,1)	(1,2)	(0,0)	(1,1)	(0,2)	(1,0)
(1,2)	(1,2)	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)

$\cdot$	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)	(0,0)
(1,1)	(0,0)	(1,1)	(0,2)	(1,0)	(0,1)	(1,2)
(0,2)	(0,0)	(0,2)	(0,1)	(0,0)	(0,2)	(0,1)
(1,0)	(0,0)	(1,0)	(0,0)	(1,0)	(0,0)	(1,0)
(0,1)	(0,0)	(0,1)	(0,2)	(0,0)	(0,1)	(0,2)
(1,2)	(0,0)	(1,2)	(0,1)	(1,0)	(0,2)	(1,1)

Ring Isomorphisms, III

In both cases, after relabeling the elements appropriately, we can see that the addition and multiplication structures of the two rings are exactly the same.

- Let us formalize this idea: a general such "relabeling" is a function $\varphi : R \to S$ with the property that φ is a bijection (so that each element of R is "labeled" with a unique element of S and vice versa) and that φ respects the ring operations.
- Explicitly, we require $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ and $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$ for all $r_1, r_2 \in R$.

Ring Isomorphisms, IV

Definition

Let R and S be rings. A ring isomorphism φ from R to S is a bijection $\varphi : R \to S$ such that $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ and $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$ for all elements r_1 and r_2 in R.

We remark here that in both of the conditions $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ and $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$, the operations on the left are performed in R while the operations on the right are performed in S.

Note: Isomorphisms arise in a variety of contexts (e.g., isomorphisms of vector spaces, isomorphisms of groups, etc.), and in some cases the rings we are considering may carry additional structure. We will simply say "isomorphism" when the particular type of isomorphism is clear from the context.

Ring Isomorphisms, V

Example: For $R = \mathbb{Z}/6\mathbb{Z}$ and $S = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, the map $\varphi : R \to S$ defined via $\varphi(n \bmod 6) = (n \bmod 2, n \bmod 3)$ is an isomorphism.

- Note that "reducing" a residue class in $\mathbb{Z}/6\mathbb{Z}$ modulo 2 or modulo 3 makes sense because 2 and 3 both divide 6, so φ is well-defined.
- We can then appeal to the calculations jammed onto the slide (or make an appeal to the Chinese remainder theorem) to see that φ is a bijection and that $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ and $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$ for any residue classes $r_1, r_2 \in \mathbb{Z}/6\mathbb{Z}$.

Ring Isomorphisms, VI

Example: For $S = \left\{ \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \in M_{2\times 2}(\mathbb{R}) : a, b \in \mathbb{R} \right\}$, the map $\varphi : \mathbb{C} \to S$ defined via $\varphi(a+bi) = \begin{bmatrix} a & b \\ -b & a \end{bmatrix}$ is an isomorphism.

- First, φ is a bijection since it has a two-sided inverse; namely, the map $\varphi^{-1} : S \to \mathbb{C}$ defined by $\varphi^{-1}\left(\begin{bmatrix} a & b \\ -b & a \end{bmatrix}\right) = a+bi$.
- Furthermore, if $z = a+bi$ and $w = c+di$, then φ respects addition and multiplication: $\varphi(z+w) = \varphi((a+c)+(b+d)i)$ $= \begin{bmatrix} a+c & b+d \\ -(b+d) & a+c \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} + \begin{bmatrix} c & d \\ -d & c \end{bmatrix} =$ $\varphi(z) + \varphi(w)$ and $\varphi(zw) = \varphi((ac-bd)+(ad+bc)i) =$ $\begin{bmatrix} ac-bd & ad+bc \\ -(ad+bc) & ac-bd \end{bmatrix} = \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} =$ $\varphi(z) \cdot \varphi(w)$.

Ring Isomorphisms, VII

Definition

If there is an isomorphism $\varphi : R \to S$, we say R and S are isomorphic, and write $R \cong S$.

Isomorphic rings share the same structure, except that the elements and operations are labeled differently.

Most of the examples of ring isomorphisms we will give are moderately artificial, for the simple reason that we do not have a large number of different rings to work with, and most of them do look fairly different from one another.

Ring Isomorphisms, VIII

Proposition (Properties of Isomorphisms)

If R, S, T are any rings, the following hold:

1. *The identity map $I : R \to R$ is an isomorphism.*
2. *If $\varphi : R \to S$ is an isomorphism, then so is $\varphi^{-1} : S \to R$.*
3. *If $\varphi : R \to S$, $\psi : S \to T$ are isomorphisms, so is $\psi\varphi : R \to T$.*
4. *If $\varphi : R \to S$ is an isomorphism, then $\varphi(0_R) = 0_S$, and if R has a 1, then so does S, and $\varphi(1_R) = 1_S$.*
5. *If $\varphi : R \to S$ is an isomorphism, then $r \in R$ is a unit in R if and only if $\varphi(r) \in S$ is a unit in S; if so, $\varphi(r)^{-1} = \varphi(r^{-1})$.*
6. *If $\varphi : R \to S$ is an isomorphism, R is a field iff S is a field.*

Ring Isomorphisms, VIII

Proofs:

1. The identity map $I : R \to R$ is an isomorphism.
   - I is clearly a bijection and respects the ring operations.
2. If $\varphi : R \to S$ is an isomorphism, then so is $\varphi^{-1} : S \to R$.
   - φ^{-1} is a bijection. If $\varphi^{-1}(s_1) = r_1$ and $\varphi^{-1}(s_2) = r_2$, then $\varphi(r_1) = s_1$ and $\varphi(r_2) = s_2$.
   - Thus, $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2) = s_1 + s_2$, meaning that $\varphi^{-1}(s_1 + s_2) = r_1 + r_2 = \varphi^{-1}(s_1) + \varphi^{-1}(s_2)$, and likewise for multiplication.
3. If $\varphi : R \to S$, $\psi : S \to T$ are isomorphisms, so is $\psi\varphi : R \to T$.
   - $\psi\varphi$ is a bijection. Also, $(\psi\varphi)(r_1 + r_2) = \psi(\varphi(r_1 + r_2)) = \psi(\varphi(r_1) + \varphi(r_2)) = \psi\varphi(r_1) + \psi\varphi(r_2)$, and likewise for multiplication.

Ring Isomorphisms, IX

Proofs (continued):

4. If $\varphi : R \to S$ is an isomorphism, then $\varphi(0_R) = 0_S$, and if R has a 1, then so does S, and $\varphi(1_R) = 1_S$.
   - Let $s \in S$ and define $r = \varphi^{-1}(s)$. Then $s + \varphi(0_R) = \varphi(r) + \varphi(0_R) = \varphi(r + 0_R) = \varphi(r) = s$, so $\varphi(0_R)$ is an additive identity in S.
   - The same idea works if R has a 1.
5. If $\varphi : R \to S$ is an isomorphism, then $r \in R$ is a unit in R if and only if $\varphi(r) \in S$ is a unit in S; if so, $\varphi(r)^{-1} = \varphi(r^{-1})$.
   - If $r \in R$ is a unit in R with inverse t, we have $1_R = rt$, so $1_S = \varphi(1_R) = \varphi(rt) = \varphi(r)\varphi(t)$ so $\varphi(r)$ is a unit in S with inverse $\varphi(t)$. The converse is equivalent, by (2).
6. If $\varphi : R \to S$ is an isomorphism, R is a field iff S is a field.
   - Every nonzero $r \in R$ is a unit iff every nonzero $s \in S$ is a unit by (5), and clearly R is commutative iff S is.

Ring Homomorphisms, I

We next give a brief discussion of maps that respect the ring operations without the requirement that they be bijections.

Definition

A function $\varphi : R \to S$ is a ring homomorphism if $\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$ and $\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$ for all elements r_1 and r_2 in R.

Note of course that any isomorphism is a homomorphism, but the reverse is not typically true.

Ring Homomorphisms, II

Examples:

1. Let R be a commutative ring and $a \in R$. The "evaluation at a map" $\varphi_a : R[x] \to R$ defined by $\varphi_a(p) = p(a)$ is a ring homomorphism.
   - Note $\varphi_a(p+q) = (p+q)(a) = p(a) + q(a) = \varphi_a(p) + \varphi_a(q)$ by the definition of polynomial addition.
   - Likewise, we have $\varphi_a(r_b x^b \cdot r_c x^c) = r_b r_c a^{b+c} = (r_b a^b)(r_c a^c) = \varphi_a(r_b x^b)\varphi_a(r_c x^c)$ because R is commutative. Then $\varphi_a(pq) = \varphi_a(p)\varphi_a(q)$ for any polynomials p, q by the distributive law.

More generally, the evaluation map is also a homomorphism on general rings of functions.

Ring Homomorphisms, III

Examples (continued):

2. Let R and S be any rings. The zero map $Z : R \to S$ given by $Z(r) = 0_S$ for every $r \in R$ is a ring homomorphism.
3. If S is a subring of R, the map $\iota : S \to R$ given by $\iota(s) = s$ is a ring homomorphism. This map is called the inclusion map, since it simply reflects the set inclusion of S inside R.
4. The function $f : \mathbb{Z} \to \mathbb{Z}$ given by $f(n) = 2n$ is not a ring homomorphism. Explicitly, although it satisfies $f(m+n) = 2(m+n) = f(m) + f(n)$, it is not multiplicative since $f(1 \cdot 1) = 2$ while $f(1) \cdot f(1) = 4$.
5. The function $f : \mathbb{R} \to \mathbb{R}$ given by $f(x) = x^2$ is not a ring homomorphism. Explicitly, although it satisfies $f(xy) = (xy)^2 = f(x)f(y)$, it is not additive since $f(1+1) = 4$ while $f(1) + f(1) = 2$.

Ring Homomorphisms, IV

Examples (continued):

6. Determine whether the map $\varphi : (\mathbb{Z}/15\mathbb{Z}) \to (\mathbb{Z}/15\mathbb{Z})$ given by $\varphi(a) = 10a$ is a ring homomorphism.
   - Note $\varphi(a+b) = 10(a+b) = 10a + 10b = \varphi(a) + \varphi(b)$.
   - Also, $\varphi(ab) = 10ab = 100ab = (10a)(10b) = \varphi(a)\varphi(b)$, since $10 \equiv 100 \pmod{15}$.
   - Therefore, φ is a homomorphism.
7. Let R be the ring of infinitely differentiable real-valued functions on $\mathbb{R}$. Determine whether the derivative map $D : R \to R$ given by $D(f) = f'$ is a ring homomorphism.
   - We have $D(f+g) = (f+g)' = f' + g' = D(f) + D(g)$, so D is additive. However, D does not respect ring multiplication, since for example $D(x \cdot x^2) = 3x^2$ while $D(x) \cdot D(x^2) = 2x$. Therefore, φ is not a homomorphism.

Ring Homomorphisms, V

Examples (continued):

8. Let R be any ring. Determine whether the map $\varphi : R \to R \times R$ given by $\varphi(r) = (r, r)$ is a ring homomorphism.

   - We have $\varphi(r+s) = (r+s, r+s) = (r, r) + (s, s) = \varphi(r) + \varphi(s)$.
   - Likewise, $\varphi(rs) = (rs, rs) = (r, r)(s, s) = \varphi(r)\varphi(s)$, so φ is a homomorphism.
   - This particular map shows up frequently in topology and algebraic geometry (it is the famous "diagonal morphism").

Ring Homomorphisms, VI

Examples (continued):

9. The map $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $\varphi(a) = \overline{a}$, so that φ maps the integer a to its associated residue class $\overline{a}$ modulo m, is a ring homomorphism.
10. In essentially the same way, the reduction modulo p map inside $F[x]$ is also a homomorphism.

Ring Homomorphisms, VII

Many properties of isomorphisms also apply to homomorphisms.

Proposition (Properties of Homomorphisms)

If R, S, T are any rings, the following hold:

1. *If $\varphi : R \to S$, $\psi : S \to T$ are homomorphisms, so is $\psi\varphi : R \to T$.*
2. *If $\varphi : R \to S$ is a homomorphism, then $\varphi(0_R) = 0_S$, $\varphi(-r) = -\varphi(r)$ for every $r \in R$, and $\varphi(r_1 - r_2) = \varphi(r_1) - \varphi(r_2)$ for every $r_1, r_2 \in R$.*
3. *If $\varphi : R \to S$ is a surjective homomorphism and R has a 1, then S also has a 1 and $\varphi(1_R) = 1_S$. Also, for any unit $u \in R$, the value $\varphi(u)$ is a unit in S with inverse $\varphi(u^{-1})$.*

Proofs: Essentially the same as the proofs for isomorphisms.

Kernel and Image, I

Definition

If $\varphi : R \to S$ is a ring homomorphism, the kernel of φ, denoted $\ker \varphi$*, is the set of elements in R mapped to 0_S by φ. In other words,* $\ker \varphi = \{r \in R : \varphi(r) = 0\}$.

- The kernel measures how close φ is to being the zero map: if the kernel is large, then φ sends many elements to zero, while if the kernel is small, φ sends few elements to zero.
- Example: The kernel of the reduction homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ with $\varphi(a) = \overline{a}$ is the subring $m\mathbb{Z}$.
- Example: The kernel of the evaluation map $\varphi_a : F[x] \to F$ given by $\varphi_a(p) = p(a)$ is the set of polynomials in $F[x]$ with $p(a) = 0$, which is (equivalently) the set of polynomials divisible by $x - a$.

Kernel and Image, II

Definition

If $\varphi : R \to S$ is a ring homomorphism, the image of φ, denoted $\operatorname{im} \varphi$, is the set of elements in S of the form $\varphi(r)$ for some $r \in R$.

- In the context of general functions, the image is often called the range of φ. We use the word "image" to emphasize the fact that it has additional structure.
- Intuitively, the image measures how close φ is to being surjective: indeed (by definition) φ is surjective if and only if $\operatorname{im} \varphi = S$.

Kernel and Image, III

The kernel and image have additional ring structure:

Proposition

Let $\varphi : R \to S$ be a ring homomorphism. Then

1. *The image $\operatorname{im}\varphi$ is a subring of S.*
2. *The kernel $\ker\varphi$ is an ideal of R.*
3. *The kernel is zero (i.e., $\ker\varphi = \{0\}$) if and only if φ is injective.*
4. *The map φ is an isomorphism if and only if $\ker\varphi = \{0\}$ and $\operatorname{im}\varphi = S$.*

Proofs: Straightforward from the definitions.

Ideals and Homomorphisms, I

Homomorphisms and quotient rings are deeply related.

- To begin, observe that if $\varphi : R \to S$ is a ring homomorphism, then the kernel of φ is an ideal of R. Thus, we can use homomorphisms to construct new ideals.
- Equally importantly, we can also do the reverse: we can use ideals to construct homomorphisms.
- As noted earlier, the map $\varphi : R \to R/I$ associating a ring element to its residue class (i.e., with $\varphi(a) = \overline{a}$) is a ring homomorphism.
- Furthermore, the kernel of this map φ is, by definition, the set of elements in R with $\varphi(r) = \overline{0}$, which is to say, the set of elements $r \in I$.
- Thus, we see that kernels of homomorphisms and ideals are precisely the same things!

Ideals and Homomorphisms, II

We can summarize these observations as follows:

Proposition (Projection Homomorphisms)

If I is an ideal of R, then the map $\varphi : R \to R/I$ defined by $\varphi(a) = \overline{a} = a + I$ is a surjective ring homomorphism called the projection homomorphism from R to R/I.

Proof:

- We have $\varphi(a+b) = \overline{a+b} = \overline{a} + \overline{b} = \varphi(a) + \varphi(b)$ and $\varphi(a \cdot b) = \overline{a \cdot b} = \overline{a} \cdot \overline{b} = \varphi(a) \cdot \varphi(b)$, so φ is a homomorphism.
- Furthermore, φ is surjective, essentially by definition: any residue class in R/I is of the form $\overline{a}$ for some $a \in R$, and then $\varphi(a) = \overline{a}$.

Ideals and Homomorphisms, III

Next, we ask: if $\varphi : R \to S$ is a homomorphism with kernel I, what can we say about the structure of R/I?

- For example, if $R = \mathbb{Q}[x]$ and $\varphi : R \to \mathbb{R}$ is defined by $\varphi(p) = p(0)$, then it is easy to see that φ is a homomorphism.
- Furthermore, the kernel of φ is the ideal I of $\mathbb{Q}[x]$ consisting of the polynomials divisible by x, while the image of φ is the set of rational numbers.
- Then it is easy to see (from our description of the kernel) that R/I is precisely the same as R/xR, and from the division algorithm for polynomials we know that the residue classes are represented by the polynomials of degree 0 in $\mathbb{Q}[x]$; namely, the constant polynomials $\overline{c}$ for $c \in \mathbb{Q}$.

Ideals and Homomorphisms, IV

- But now notice that the structure of R/I (namely, of $\mathbb{Q}$) is exactly the same as the structure as the image of φ.
- More formally, these two rings are isomorphic, with an isomorphism given by identifying a residue class $\overline{c}$ with the rational number c.
- This relabeling can, equivalently, be thought of as being done via the homomorphism φ: we associate the residue class $\overline{c}$ in R/I with the rational number $\varphi(\overline{c}) = c$.
- In other words: φ gives an isomorphism between $R/\ker\varphi$ and the image $\operatorname{im}\varphi$.

Ideals and Homomorphisms, V

The example we just discussed leads to a general result:

Theorem (First Isomorphism Theorem)

If $\varphi : R \to S$ is a homomorphism of rings, then $R/\ker\varphi$ is isomorphic to $\operatorname{im}\varphi$.

- Intuitively, φ is a surjective homomorphism $\varphi : R \to \operatorname{im}\varphi$ (this is simply the definition of the image).
- To turn this map into an isomorphism, we must "collapse" its kernel to a single element: this is precisely what the quotient ring $R/\ker\varphi$ represents.

Ideals and Homomorphisms, VI

Proof:

- Let $I = \ker \varphi$. We use φ to construct a map $\psi : R/I \to \operatorname{im} \varphi$, and then show that it is injective and surjective.
- The map is defined as follows: for any residue class $\overline{r} \in R/I$, we define $\psi(\overline{r}) = \varphi(r)$.
- We must verify that this map ψ is well-defined, so suppose that r' is some other representative of the residue class $\overline{r}$: then $r' - r \in I$, so $\varphi(r' - r) = 0$ and thus $\varphi(r') = \varphi(r)$.
- Thus, $\psi(\overline{r'}) = \varphi(r') = \varphi(r) = \psi(\overline{r})$, so the map ψ is well-defined.

Ideals and Homomorphisms, VII

Proof (continued):

- Next, ψ is a homomorphism, since $\psi(\overline{r}+\overline{s}) = \varphi(r+s) = \varphi(r)+\varphi(s) = \psi(\overline{r})+\psi(\overline{s})$ and likewise $\psi(\overline{r}\cdot\overline{s}) = \varphi(r\cdot s) = \varphi(r)\cdot\varphi(s) = \psi(\overline{r})\cdot\psi(\overline{s})$.
- Furthermore we see that $\psi(\overline{r}) = 0$ precisely when $\varphi(r) = 0$, which is to say $r \in \ker(\varphi)$, so that $\overline{r} = \overline{0}$. Thus, the only element in $\ker\psi$ is $\overline{0}$, so ψ is injective.
- Finally, if s is any element of $\operatorname{im}\varphi$, then by definition there is some $r \in R$ with $\varphi(r) = s$: then $\psi(\overline{r}) = s$, meaning that ψ is surjective.
- Since ψ is a homomorphism that is both injective and surjective, it is an isomorphism.

Ideals and Homomorphisms, VIII

The main utility of the first isomorphism theorem is that we can use it to construct isomorphisms of rings.

- In order to show that R/I is isomorphic to a ring S, we search for a surjective homomorphism $\varphi : R \to S$ whose kernel is I.
- The idea above is quite simple, but it is surprisingly powerful.

Ideals and Homomorphisms, IX

Example: If R is any commutative ring, show that $R[x]/(x)$ is isomorphic to R.

- Let $\varphi : R[x] \to R$ be the "evaluation at 0" homomorphism $\varphi(p) = p(0)$. This map is clearly surjective since for any $r \in R$ we have $\varphi(r) = r$.
- Furthermore, the kernel of this homomorphism is precisely the collection of polynomials $p(x) = a_0 + a_1x + \cdots + a_nx^n$ with $p(0) = 0$, which is easily seen to be the ideal $I = (x)$ consisting of polynomials divisible by x.
- Thus, by the first isomorphism theorem, for $I = (x)$ we have $R[x]/I \cong R$.

Ideals and Homomorphisms, X

Example: Show that $\mathbb{Z}/12\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.

- We seek a surjective homomorphism $\varphi : \mathbb{Z} \to (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$ whose kernel is $12\mathbb{Z}$.
- Once this idea is suggested, it is not hard to come up with a candidate, namely, $\varphi(a) = (a \bmod 3, a \bmod 4)$.
- It is easy to verify that map is a homomorphism (since the individual maps of reduction mod 3 and reduction mod 4 are homomorphisms) and it is likewise fairly easy to see that the map is surjective by checking that the images of 0, 1, ... , 11 represent all of the elements in $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.
- Finally, the kernel of the map consists of all integers a with $\varphi(a) = (0, 0)$, which is not hard to see is precisely $12\mathbb{Z}$.
- Therefore, by the first isomorphism theorem applied to φ, we conclude that $\mathbb{Z}/12\mathbb{Z}$ is isomorphic to $(\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.

Ideals and Homomorphisms, XI

We can use the first isomorphism theorem to establish several other related theorems collectively known as the "isomorphism theorems", which characterize how isomorphisms relate to the various ring operations.

- We will skip the proofs of these theorems, since we will not actually use them at any point. (They are in the notes, if you want to work through them.)
- But the idea for each proof is to invoke the first isomorphism theorem in an appropriate way.
- I included them here mostly because it seems odd to refer to the first isomorphism theorem without also including the second, third, and fourth isomorphism theorems.

Ideals and Homomorphisms, XII

Theorem (Second Isomorphism Theorem)

If A is a subring of R and B is an ideal of R, then $A + B = \{a + b : a \in A, b \in B\}$ is a subring of A, $A \cap B$ is an ideal of A, and $(A + B)/B$ is isomorphic to $A/(A \cap B)$.

Theorem (Third Isomorphism Theorem)

If I and J are ideals of R with $I \subseteq J$, then J/I is an ideal of R/I and $(R/I)/(J/I)$ is isomorphic to R/J.

Theorem (Fourth/Lattice Isomorphism Theorem)

If I is an ideal of R, then there is an inclusion-preserving bijection between subrings A of R containing I and the subrings $\overline{A} = A/I$ of R/I. Furthermore, a subring A of R containing I is an ideal of R if and only if A/I is an ideal of R/I.

Summary

We constructed quotient rings and discussed several examples.

We discussed ring isomorphisms and homomorphisms.

We discussed the relationships between ideals and homomorphisms.

Next lecture: Fields and field extensions.