Math 320 Notes, Chapter 3

Instructor: Tony Armas

Spring 2020

1 Rings

We've been doing arithmetic (namely addition and multiplication) on the integers and on congruence classes. We can also perform addition and multiplication on other number systems such as the rational numbers, real numbers, and complex numbers.

Furthermore, we can define similar structures on other sets. We can actually define a general theory for addition and multiplication that we can apply to any system with that structure. So, if we prove results about this general theory, then they will apply to any system that follows the theory.

A system with defined operations of addition and multiplication that follow some basic fundamental properties is called a **ring.**

1.1 Definition and Examples of Rings

Definition A **ring** is a nonempty set R equipped with two operations (usually written as addition and multiplication) that satisfy the following axioms. For all $a, b, c \in R$:

1. If $a \in R$ and $b \in R$, then $a + b \in R$ (closure for addition)

2. $a + (b + c) = (a + b) + c$ (associative addition)

3. $a + b = b + a$ (commutative addition)

4. There is an element 0_R in R such that $a + 0_R = a = 0_R + a$ for every $a \in R$ (additive identity/zero element)

5. For each $a \in R$, there is an element $-a \in R$ such that $a + (-a) = (-a) + a = 0_R$.

6. If $a \in R$ and $b \in R$, then $ab \in R$ (closure for multiplication)

7. $a(bc) = (ab)c$ (associative multiplication)

8. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ (distributive laws)

These are the bare minimum requirements for a set R to be a ring. Notice that multiplication doesn't have to be commutative. Here are some additional properties that a ring may have:

Definition: A **commutative ring** is a ring R that satisfies the following axiom:

9. $ab = ba$ for all $a, b \in R$.

Definition: A **ring with identity** is a ring R that contains an element 1_R satisfying this axiom

Examples:

(1) The typical number systems $\mathbb{Z}, \mathbb{R}, \mathbb{C}, \mathbb{Q}$ are all commutative rings with identity.

(2) We defined $\mathbb{Z}_n$ to also be a commutative ring with identity, for any $n \geq 2$.

(3) $2\,\mathbb{Z} = \{2n : n \in \mathbb{Z}\} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ is a commutative ring, with regular addition and multiplication, since sums and products of even integers are even. However, $1 \notin 2\,\mathbb{Z}$, so $2\,\mathbb{Z}$ does have a multiplicative identity.

We can look at examples of rings that are far less familiar.

Example:

Let $M(\mathbb{R})$ be the set of 2×2 matrices with real entries.

We define addition of matrices by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

and we define multiplication by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} w & x \\ y & z \end{pmatrix} = \begin{pmatrix} aw + by & ax + bz \\ cw + dy & cx + dz \end{pmatrix}$$

Note that multiplication of matrices is **not** commutative. Here is an example of how reversing the order of multiplication produces different elements:

$$\begin{pmatrix} 2 & 3 \\ 0 & -4 \end{pmatrix} \begin{pmatrix} 1 & -5 \\ 6 & 7 \end{pmatrix} = \begin{pmatrix} 20 & 11 \\ -24 & -28 \end{pmatrix}$$

$$\begin{pmatrix} 1 & -5 \\ 6 & 7 \end{pmatrix}\begin{pmatrix} 2 & 3 \\ 0 & -4 \end{pmatrix} = \begin{pmatrix} 2 & 23 \\ 12 & -10 \end{pmatrix}$$

The zero element is the zero matrix:

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

And of course, for a matrix A, then additive inverse is $-A$.

The multiplicative identity is the identity matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

In general, if R is a commutative ring with identity, then $M(R)$, the set of all 2×2 matrices with entries in R, is a ring with identity.

Another example of a ring is the set of all functions $f : \mathbb{R} \to \mathbb{R}$, where we define addition and multiplication by

$$(f+g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x).$$

Since $\mathbb{R}$ is commutative, multiplication of functions is commutative. The additive identity element is the constant function 0, and the multiplicative identity is the constant function 1. You can find two functions that when multiplied together form the zero function.

Definition: An **integral domain** is a commutative ring R with identity $1_R \neq 0_R$ that satisfies the following property: Whenever $a, b \in R$ and $ab = 0_R$, either $a = 0_R$ or $b = 0_R$.

We say $1_R \neq 0_R$ so that we may exclude the zero ring.

Some examples of integral domains are $\mathbb{Z}$ and $\mathbb{Z}_p$ for p primes. We have seen that $M(\mathbb{R})$ and the ring of functions $\mathbb{R} \to \mathbb{R}$ are not integral domains.

The rational numbers $\mathbb{Q}$ is another example of an integral domain. We say $a/b = c/d$ iff $ad = bc$, so that unreduced are equal to their reduced versions. We define addition and multiplication by

$$a/b + c/d = (ad + bc)/bd, \quad (a/b)(c/d) = (ac)/(bd).$$

Also, $\mathbb{Q}$ has another property that $\mathbb{Z}$ does not have: for any $q \in \mathbb{Q} - \{0\}$, there's an element, which we denote by q^{-1}, such that $qq^{-1} = q^{-1}q = 1$. We call q^{-1} the multiplicative inverse of q.

It's easy to see that every nonzero rational number has such an inverse. If $q = a/b$, and $a, b \neq 0$, then $q^{-1} = b/a$, since $(a/b)(b/a) = (ab)/(ab) = 1$.

A commutative ring with 1_R with the property that every nonzero element has a multiplicative inverse is called a **field**.

The non-commutative version of a field is called a **division ring.**

$\mathbb{R}$ is another example of a field, as is $\mathbb{C}$:

If $z = a + bi \in \mathbb{C}$, then its inverse is $z^{-1} = \frac{a-bi}{a^2+b^2} = \frac{\overline{z}}{|z|^2}$.

Another example: The set of matrices

$$\left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$$

is a field.

Recall that the Cartesian product of two sets A and B, denoted by $A \times B$, is defined to be the set

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

We can define rings of Cartesian products:

Theorem: Let R and S be rings. Define addition and multiplication on the Cartesian product $R \times S$ by

$$(r, s) + (r', s') = (r + r', s + s'), \quad (r, s)(r', s') = (rr', ss').$$

Then, $R \times S$ is a ring. If R and S are **both** commutative, then $R \times S$ is commutative. If R and S have identity elements $1_R, 1_S$ respectively, then $R \times S$ has identity $(1_R, 1_S)$.

Note that the product of two rings $R \times S$ is never an integral domain, even if both R, S are integral domains. Take any nonzero $r \in R, s \in S$. Then,

$$(r, 0)(0, s) = (0, 0).$$

1.1.1 Subrings

Suppose we have a ring R, and a subset $S \subset R$. Is S a ring as well? If so, then we call S a **subring** of R. The following theorem will help answer this question:

Theorem 3.2 Suppose that R is a ring and S is a subset of R such that

(i) S is closed under addition,

(ii) S is closed under multiplication,

(iii) $0_R \in S$,

(iv) If $a \in S$, then $-a \in S$.

Then, S is a subring of R.

1.2 Basic Properties of Rings

1.2.1 Arithmetic in Rings

We did not yet define subtraction in rings. We will do so in terms of addition, multiplication, and the ring axioms:

Theorem 3.3: For any element a in a ring R, the equation $a + x = 0_R$ has a unique solution.

That is, additive inverses are unique.

By the 4th ring axiom, we know that a has an additive inverse u. Now, we need to show uniqueness.

Suppose that v is some other additive inverse, so $a + v = 0_R$. Then,

$$v = v + 0_R = v + (a + (u)) = (v + a) + (u) = (a + v) + (u) = 0_R + (u) = u.$$

So, a has a *unique* additive inverse, which we denote by $-a$. We define subtraction as for $a, b \in R$ by

$$a - b = a + (-b).$$

Theorem 3.4: If $a + b = a + c$ in a ring R, then $b = c$.

Proof: Add $-a$ to both sides and use associativity of addition:

$$
\begin{aligned}
-a + (a+b) &= -a + (a+c)\\
(-a+a)+b &= (-a+a)+c\\
0_R + b &= 0_R + c\\
b &= c.
\end{aligned}
$$

Theorem 3.5: For any elements a, b in a ring R,

(1) $a \cdot 0_R = 0_R \cdot a$. In particular, $0_R \cdot 0_R = 0_R$.

(2) $a(-b) = (-a)b = -ab$.

(3) $-(-a) = a$

(4) $-(a+b) = (-a) + (-b)$

(5) $-(a-b) = b - a$

(6) $(-a)(-b) = ab$

If R has an identity, then

(7) $(-1_R)a = -a$.

Proof:

(1)

$$a \cdot 0_R + 0_R = a \cdot 0_R = a \cdot (0_R + 0_R) = a \cdot 0_R + a \cdot 0_R.$$

Then, by Theorem 3.4, $a \cdot 0_r = 0_R$. The proof for $0_R \cdot a = 0_R$ is similar.

(2)

$$ab + a(-b) = a[b + (-b)] = a \cdot 0_R = 0_R.$$

This shows that $a(-b)$ is a solution to $ab + x = 0_R$. By Theorem 3.3, there is only one solution to this equation, and $-ab$ is the unique solution, so $-ab = a(-b)$.

(3) $-(-a)$ is the unique solution to the equation $-a + x = 0_R$, but a is also a solution, so $a = -(-a)$.

(4) $-(a+b)$ is the unique solution to $(a+b) + x = 0_R$. We'll show that $(-a) + (-b)$ is also a solution:

$$(a+b) + [(-a) + (-b)] = a + (-a) + b + (-b) = 0_R + 0_R = 0_R.$$

Therefore, by Theorem 3.3, $-(a+b) = (-a) + (-b)$.

(5) $-(a-b)$ is the unique solution to $(a-b)+x=0_R$. We'll show that $b-a$ also solves this:

$$(a-b)+(b-a)=a+(-b)+b+(-a)=a+(-a)+b+(-b)=0_R+0_R=0_R.$$

(6) By (2), $(-a)(-b)=-((-a)b)=-(-ab)$. By (3), $-(-ab)=ab$.

(7) By (2), $(-1_R)a=-(1_R\cdot a)=-a$.

We can also define exponents:

$$a^n=a\cdot a\cdots a \qquad n \text{ factors}$$

For positive integers m,n,

$$a^m a^n=a^{m+n}, \qquad (a^m)^n=a^{mn}.$$

If R has identity, define $a^0=1_R$.

If $a\in R$ and n is a positive integer, then define

$$na=a+a+a+\ldots+a \qquad (n \text{ summands})$$

$$-na=(-a)+(-a)+(-a)+\ldots+(-a) \qquad (n \text{ summands})$$

Lastly, define $0a=0_R$.

Example:

Let $a,b\in R$. Then,

$$(a+b)^2=(a+b)(a+b)=a(a+b)+b(a+b)=a^2+ab+ba+b^2.$$

Be careful, since ab and ba aren't necessarily equal. If R is commutative, then we get the usual

$$(a+b)^2=a^2+2ab+b^2.$$

For a commutative ring, $(a+b)^n$ follows the binomial theorem.

Theorem 3.6: Let S be a nonempty subset of a ring R such that

(1) S is closed under multiplication (if $a, b \in S$, then $a - b \in S$)

(2) S is closed under multiplication.

Proof:

Since S is nonempty, it contains some element a. Since S is closed under subtraction,

$$a - b = 0_R \in S,$$

so property 3 in Theorem 3.2 is satisfied. This tells us that if $x \in R$, then $-x \in R$, since

$$-x = 0_R - x \in R.$$

This satisfies property 4.

If $x, y \in R$, then $-y \in R$, so

$$x + y = x - (-y) \in S,$$

so property 1 is satisfied.

Finally, property two is satisfied by assumption.

1.2.2 Units and Zero Divisors

Definition: An element a in a ring R with identity is called a **unit** if there exists $u \in R$ such that $au = 1_R = ua$. In this case u is called the **multiplicative inverse** of a and is denoted a^{-1}.

Examples:

(1) The only units in $\mathbb{Z}$ are ± 1

(2) Every element of a field is a unit.

(3) For a 2×2 matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

in the ring $M_2(F)$, where F is a field, the **determinant** of A is $\det A = ad - bc$. If $\det A \neq 0_F$, then A is a unit, with multiplicative inverse

$$A^{-1} = (\det A)^{-1} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

Definition: An element $a \in R$ is a **zero divisor** provided that

(1) $a \neq 0_R$,

(2) There exists a nonzero element $c \in R$ such that $ac = 0_R$ or $ca = 0_R$.

Remark: in a noncommutative ring, it's possible to have $ac = 0_R$ and $ca \neq 0_R$.

Example: In $\mathbb{Z}_6$, the matrix

$$\begin{pmatrix} 4 & 1 \\ 2 & 5 \end{pmatrix}$$

is a zero divisor:

$$\begin{pmatrix} 4 & 1 \\ 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 6 & 6 \\ 12 & 12 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

An integral domain contains no zero divisors.

Theorem 3.7: Cancellation is valid in any integral domain R: If $a \neq 0_R$ and $ab = ac$ in R, then $b = c$.

Proof:

$$ab - ac = a(b - c).$$

Since $a \neq 0_R$ and R is an integral domain, $b - c = 0 \Rightarrow b = c$.

Theorem 3.8: Every field F is an integral domain.

Proof: Suppose $a \in F$ is nonzero, and $ab = 0_F$. Multiply both sides by a^{-1}:

$$a^{-1}(ab) = 1_F \cdot b = b = a^{-1} 0_F = 0_F.$$

Theorem 3.9: Every finite integral domain R is a field.

Proof: We can list the nonzero elements of R:

$$1_R, x_1, x_2, \ldots, x_n.$$

Multiply every element of this list by x_1:

$$x_1, x_1^2, x_1x_2, x_1x_3, \ldots, x_1x_n.$$

Since R is an integral domain, $x_1x_i \neq x_1x_j$ for all $1 \leq i, j \leq n$. So, this list contains $n+1$ distinct nonzero elements of R. Since there are only $n+1$ distinct nonzero elements of R, this list contains all of the elements of R, so 1_R shows up somewhere, i.e. $x_1x_i = 1$ for some i.

1.3 Isomorphisms and Homomorphisms

We can relabel the numbers 1-12 with the Roman numerals I, II, III, IV, V, VI, VII, VIII, IX, X.

This section concerns the ideal of "relabeling," but with rings. We will show that two rings can share the same properties, and are "essentially the same" except for how they're written.

For example, consider the subring $R = \{0, 2, 4, 6, 8\}$ of $\mathbb{Z}_{10}$

Write out the addition and multiplication tables for R. We can see that it is a field with identity element 6:

$+$	0	6	2	8	4
0	0	6	2	8	4
6	6	2	8	4	0
2	2	8	4	0	6
8	8	4	0	6	2
4	4	0	6	2	8

$\cdot$	0	6	2	8	4
0	0	0	0	0	0
6	0	6	2	8	4
2	0	2	4	6	8
8	0	8	6	4	2
4	0	4	8	2	6

Now, we'll show that this is actually the addition and multiplication table for the field $\mathbb{Z}_5$.

Leave the 0 alone, but replace 6 with 1, leave 2 alone, 8 with 3, and leave 4 alone. This gives us

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

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

This tells us that $\mathbb{Z}_5$ and R are exactly the same rings, except for the way the elements are labeled. They have the same number of elements, and their ring structures (i.e. the way their addition and multiplication behave) are the same.

When two rings are essentially the same in this way, we say they are **isomorphic.** For small finite rings, we can just write out the multiplication and addition tables and just re-label elements accordingly. But how do we show that larger rings are isomorphic to each other?

The basic idea for two rings R and S to be isomorphic:

(1) The elements of S are just a re-labeling of the elements of R.

(2) The multiplication and addition of R works the same as the multiplication and addition of S.

(1) tells us that there is a function $f : R \to S$ that assigns to each $r \in R$ and element $s \in S$, i.e. $f(r) = s$, so f *re-labels* the element r as s.

In our previous example we had a function $f : R \to \mathbb{Z}_5$ where

$$f(0) = 0, f(6) = 1, f(2) = 2, f(8) = 3, f(4) = 4.$$

This function must have the following properties:

(1) Distinct elements of R must have distinct labels.

That is, if $r \neq r'$ in R, then $f(r) \neq f(r')$.

So, f must be one-to-one/injective.

(2) Every element of S must be the label for some element in R.

So for every $s \in S$, there exists $r \in R$ such that $f(r) = s$.

So, f must be onto/surjective.

When a function f satisfies these two properties, we say that f is a **bijection.**

The function also has to translate the addition and multiplication properly, so if $a+b=c$ in R, then $f(a)+f(b)$ should be $f(c)$ in S, and since $a+b=c$, we need $f(a+b)=f(c)$. Putting this together, we want

$$f(a+b)=f(a)+f(b).$$

Similarly, if $ab=c$, we want $f(a)f(b)=f(c)$, and since $ab=c$, $f(ab)=f(c)$, so

$$f(ab)=f(a)f(b).$$

Definition: A ring R is **isomorphic** to a ring $S(\ R\cong S)$ if there is a function $f:R\to S$ such that

(i) f is one-to one/injective

(ii) f is surjective ($\forall s\in S, \exists r\in R$ s.t. $f(r)=s$)

(iii) $f(a+b)=f(a)+f(b)$ and $f(ab)=f(a)f(b)$ for all $a,b\in R$ (homomorphism property)

In this case, we call f an **isomorphism.**

Examples:

(1)

$$\mathbb{C}\cong\left\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a,b\in\mathbb{R}\right\}$$

(2) $f:\mathbb{C}\to\mathbb{C}$ given by $z\mapsto\overline{z}$ is an isomorphism.

(3) identity map $\iota_R : R\to R$ is an isomorphism.

Note: $R\cong S$ if and only if $S\cong R$.

If $R\cong S$, we have an isomorphism $f:R\to S$. To show that $S\cong R$, we need another isomorphism $S\to R$. Here's how to find it: if f is an isomorphism, then it's a bijection, so it has an inverse $g:S\to R$ such that $g\circ f:R\to R$ is just ι_R, and $f\circ g:S\to S$ is just ι_S. Check that g is an isomorphism.

1.4 Homomorphisms

Definition: Let S and R be rings. A function $f : R \to S$ is a **homomorphism** if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$.

A homomorphism just satisfies property (iii) of the earlier definition, but it may not necessarily be onto or one-to-one.

Examples: (1) zero map $z : R \to S$. (neither injective nor surjective)

(2) $\mathbb{Z} \to \mathbb{Z}_n$ where $a \mapsto a \mod n$. (surjective but not injective)

Theorem 3.10 Let $f : R \to S$ be a homomorphism of rings. Then

(1) $f(0_R) = 0_s$ (homomorphisms map 0 to 0)

(2) $f(-a) = -f(a)$ for all $a \in R$

(3) $f(a-b) = f(a) - f(b)$ for all $a, b \in R$

If R is a ring with idenity and R is surjective, then

(4) S is a ring with identity $f(1_R)$

(5) Wheneverуu is a unit in R, then $f(u)$ is a unit in S and $f(u)^{-1} = f(u^{-1})$

Proof:

(1) easy

(2)

$$0_S = f(0_R) = f(a-a) = f(a) + f(-a) \Rightarrow f(-a) = -f(a)$$

by uniqueness of additive inverses.

(3) follows by (2)

(4) Let $s \in S$ Since f is surjective, $s = f(r)$ for some $r \in R$. Then,

$$f(1_R)s = f(1_R)f(r) = f(1_R \cdot r) = f(r) = s.$$

(5)

$$1_S = f(1_R) = f(uu^{-1}) = f(u)f(u^{-1}).$$

Corollary 3.11 If $f : R \to S$ is a homomorphism of rings, then the image of f is a subring of S.

Proof: easy

Example:

Show that $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

$\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q$ is $n = pq$ and $(p, q) = 1$.

To show two rings R and S are **not** isomorphic, the process is tricky. You have to show that there does not exist an isomorphism.

A common way to do this is to show that they don't have the same **structural properties**. That involves showing some difference in the underlying sets and/or some difference in how their operations behave.

Examples:

(1) do the rings have the same number of elements? Is one finite and the other infinite?

(2) Are both rings commutative?

(3) Are they both integral domains? fields?

(4) How many zero divisors do the rings have?

Examples: (1) $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic. Every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ is its own additive inverse. This is not true in $\mathbb{Z}_4$.

(1) $\mathbb{Z}$ not isomorphic to $\mathbb{Q}$

(2) $\mathbb{Q}$ not isomorphic to $\mathbb{R}$ (square roots)

Suppose $f : R \to S$ is an isomorphism and $a, b, c, \ldots$ in R have a property. If $f(a), f(b), f(c), \ldots$ still have that property, then we say the property is **preserved by isomorphism.**

zero elements, identity, and inverses are preserved by isomoprhism

commutativity is preserved by isomorphism.