Section 2: Rings and Fields

HW p. 10 # 1-9 at the end of the notes

In this section, we discuss the basics of rings and fields.

Rings

Definition 2.1: A *ring* $< R, +, \cdot >$ is a non-empty set R with two binary operations + and $\cdot$, normally called addition and multiplication, defined on R such that R is closed under + and $\cdot$, that is for $a, b \in R$, $a + b \in R$ and $a \cdot b \in R$, and where the following axioms are satisfied for all $a, b, c \in R$:

1. R_1: $< R, + >$ is an abelian group, that is
   a. $(a+b)+c = a+(b+c)$ (Associatively under + is satisfied)
   b. For each $a \in R$, there exists an identity $0 \in R$ were
      $a + 0 = 0 + a = a$ (R has an additive Identity)
   c. For each $a \in R$, there exists an $-a \in R$ where
      $a + (-a) = (-a) + a = 0$ (Each element in R has an additive inverse)
   d. $a + b = b + a$ (Addition is commutative)
2. R_2: $(ab)c = a(bc)$ (Associativity under $\cdot$ is satisfied)
3. R_3: $a(b+c) = ab + ac$ (Left and Right Distributive laws are satisfied)
   $(a+b)c = ac + bc$

Definition 2.2: A *commutative ring* is a ring R that satisfies $ab = ba$ for all $a, b \in R$ (it is commutative under multiplication). Note that rings are always by condition 1 commutative under addition.

Definition 2.3: A *ring with unity* is a ring with the multiplicative identity, that is, there exists $1 \in R$ where $a \cdot 1 = 1 \cdot a = a$ for all $a \in R$.

$Z = \{\ldots, -3, -2, -1, 0, 1, 2, 3, 4, \ldots\}$

Examples of Rings

Example 1: Show that the integers $< Z, +, \cdot >$ represents a ring.

Solution: The integers $< Z, +, \cdot >$ represents a ring. For $a, b \in Z$, it is known that Z is closed under + and $\cdot$, that is $a + b \in Z$ and $a \cdot b \in Z$. For $a, b, c \in Z$, we must next show it satisfied the 3 properties for a ring.

1. $R_1 : < Z, + >$ is known to be an an abelian group, that is
   a. $(a+b)+c = a+(b+c)$ (Z is known to be associative under +)
   b. For each $a \in Z$, there exists an identity zero given by $0 \in Z$ were
      $a + 0 = 0 + a = a$ (0 is the known additive identity element in the integers)
   c. For each $a \in Z$, there exists an $-a \in Z$ where
      $a + (-a) = (-a) + a = 0$ (Each element in Z has an additive inverse obtained by negating the element)
   d. $a + b = b + a$ (Z is known to be commutative under +)
2. $R_2 : (ab)c = a(bc)$ (Z is known to be associative under $\cdot$)
3. $R_3 : a(b+c) = ab + ac$ (Left and Right Distributive laws are known to hold in the
   $(a+b)c = ac + bc$ integers.)

∎

Notes:

i. Z is a commutative ring since the integers are known to be commutative under multiplication, that is $ab = ba$ for all $a, b \in Z$.

ii. Z has unity 1 since $1 \cdot a = a \cdot 1 = a$ for all $a \in Z$.

Example

$2Z = \{\ldots, -6, -4, -2, 0, 2, 4, 6, 8, \ldots\}$ (multiples of 2 even integers)

integer multiples of 3

Example 2: Show that $3Z = \{\ldots, -12, -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$ is a ring. Is $3Z$ a commutative ring? Does it have unity?

Solution: Let $a, b, c \in 3\mathbb{Z}$

Then $a = 3l$, $b = 3m$, $c = 3n$, $l, m, n \in \mathbb{Z}$

Note: $3\mathbb{Z}$ is closed under $+$: $a + b = 3l + 3m = 3(l+m) \in 3\mathbb{Z}$

is closed under $\bullet$: $ab = (3l)(3m) = 3(3lm) \in 3\mathbb{Z}$

R_1: i) Assoc: $(a+b)+c = a+(b+c)$ Integers are known to be assoc under $+$

ii) Additive Identity: If $0 \in 3\mathbb{Z}$, and $0 + a = a + 0 = a$ for all $a \in 3\mathbb{Z}$

iii) Additive Inverse: If $a \in 3\mathbb{Z}$, $-a = -3l = 3(-l) \in 3\mathbb{Z}$

and $a + (-a) = (-a) + a = 0$

iv.) Comm under $+$: $a + b = b + a$ (known for integer $+$)

R_2: Assoc under $\bullet$ $(ab)c = a(bc)$ Integer mult is known to be assoc

R_3: Distributive Law: $a(b+c) = ab + ac$, $(a+b)c = ac + bc$ $\Big\}$ known fact for the integers

Hence $3\mathbb{Z}$ is is a ring!

Note: $3\mathbb{Z}$ is commutative: $a \cdot b = b \cdot a$ (known fact for integers)

Note: $3\mathbb{Z}$ does not have a unity element $(1 \notin 3\mathbb{Z})$

Definition 2.4: The Cartesian product of the groups $G_1, G_2, \dots, G_n$ is the set $(a_1, a_2, \dots, a_n)$, where $a_i \in G_i$ for $i = 1, 2, \dots, n$. We denote the Cartesian product by

$$G_1 \times G_2 \times \cdots \times G_n = \prod_{i=1}^{n} G_i .$$

Recall that a group G is a non-empty set that is closed under a binary operation * that satisfy the following 3 axioms

1. Associativity: For all $a, b, c \in G$, $(a*b)*c = a*(b*c)$.
2. Identity: For any $a \in G$, there exists an $e \in G$ where $a*e = e*a = a$.
3. Inverse: For each $a \in G$, there exists an element $a^{-1} \in G$ where $a*a^{-1} = a^{-1}*a = e$.

Fact: The Cartesian product $G_1 \times G_2 \times \cdots \times G_n$ forms a group under the binary operation $(a_1, a_2, \dots, a_n)(b_1, b_2, \dots, b_n) = (a_1 b_1, a_2 b_2, \dots, a_n b_n)$, $a_i, b_i \in G_i$.

Proof: Note that G is closed. This is true because, since each G_i is a group, each G_i is closed and $a_i b_i \in G_i$ for any $a_i, b_i \in G_i$. Hence

$$(a_1 b_1, a_2 b_2, \dots, a_n b_n) \in G_1 \times G_2 \times \cdots \times G_n \text{ since } a_i b_i \in G_i$$

We next prove the 3 group properties.

1. Associativity: Let $x, y, z \in G_1 \times G_2 \times \cdots \times G_n$. Then $x = (a_1, a_2, \dots, a_n)$, $y = (b_1, b_2, \dots, b_n)$, and $z = (c_1, c_2, \dots, c_n)$ where $a_i, b_i, c_i \in G_i$. It can be show that both $(xy)z$ and $x(yz)$ equal $(a_1 b_1 c_1, a_2 b_2 c_2, \dots, a_n b_n c_n)$. Hence, $G_1 \times G_2 \times \cdots \times G_n$ is associative.
2. Identity: The identity is given by $e = (e_1, e_2, \dots, e_n)$, where each e_i is the identity for the group G_i. Note that for $x = (a_1, a_2, \dots, a_n)$, we have

   $$xe = (a_1, a_2, \dots, a_n)(e_1, e_2, \dots, e_n) = (a_1 e_1, a_2 e_2, \dots, a_n e_n) = (a_1, a_2, \dots, a_n) = x .$$

   Similarly, we can show $ex = x$.
3. Inverse. For each $a_i \in G_i$, $a_i^{-1} \in G_i$ since G_i is a group. Hence, the inverse of $x = (a_1, a_2, \dots, a_n)$ is $x^{-1} = (a_1^{-1}, a_2^{-1}, \dots, a_n^{-1})$. Note that

   $$xx^{-1} = (a_1, a_2, \dots, a_n)(a_1^{-1}, a_2^{-1}, \dots, a_n^{-1}) = (a_1 a_1^{-1}, a_2 a_2^{-1}, \dots, a_n a_n^{-1}) = (e_1, e_2, \dots, e_n) = e$$

   Similarly, $x^{-1}x = e$.

Hence, by definition, $G_1 \times G_2 \times \cdots \times G_n$ is a group. ∎

Page 5

Tuesday, August 18, 2020 5:52 PM

Example 3: Show $4Z \times Z$ is a ring under addition and multiplication.

4 Z X Z

1st coord is an integer multiple of 4

2nd coord is an integer

Solution: Let $a, b, c \in 4Z \times Z$. Then $a = (4s_1, t_1)$, $b = (4s_2, t_2)$, and $c = (4s_3, t_3)$ where $s_1, t_1, s_2, t_2, s_3, t_3 \in Z$. Note that $4Z \times Z$ is closed under + and $\cdot$ since

$$a + b = (4s_1, t_1) + (4s_2, t_2) = (4s_1 + 4s_2, t_1 + t_2) = (4(s_1 + s_2), t_1 + t_2) \in 4Z \times Z \ .$$

and

$$a \cdot b = (4s_1, t_1) \cdot (4s_2, t_2) = (16s_1s_2, t_1t_2) = (4(4s_1s_2), t_1t_2) \in 4Z \times Z \, .$$

We now demonstrate that this set satisfies the 3 properties for a ring,

R_1: $4Z \times Z$ is an abelian group under + since

i) $4Z \times Z$ is associative under + since

$$\begin{aligned}(a+b)+c &= [(4s_1, t_1) + (4s_2, t_2)] + (4s_3, t_3) \\ &= (4s_1 + 4s_2, t_1 + t_2) + (4s_3, t_3) \\ &= (4s_1 + 4s_2 + 4s_3, t_1 + t_2 + t_3) \\ &= (4s_1, t_1) + (4s_2 + 4s_3, t_2 + t_3) \\ &= (4s_1, t_1) + [(4s_2, t_2) + (4s_3, t_3)] \\ &= a + (b + c)\end{aligned}$$

ii) $\mathbf{0} = (0, 0) \in 4Z \times Z$ serves as the identity under + since

$$a + 0 = (4s_1, t_1) + (0,0) = (4s_1 + 0, t_1 + 0) = (4s_1, t_1) = (0 + 4s_1, 0 + t_1) = (0,0) + (4s_1, t_1) = 0 + a$$

iii) For $a = (4s_1, t_1)$, then $-a = (-4s_1, -t_1) \in 4Z \times Z$ serves as the additive inverse since

$$\begin{aligned}a + (-a) &= (4s_1, t_1) + (-4s_1, -t_1) = (4s_1 - 4s_1, t_1 - t_1) \\ &= (0,0) \\ &= (-4s_1 + 4s_1, -t_1 + t_1) \\ &= (-4s_1, -t_1) + (4s_1, t_1) \\ &= (-a) + a\end{aligned}$$

iv) $4Z \times Z$ is abelian under + since

$$a + b = (4s_1, t_1) + (4s_2, t_2) = (4s_1 + 4s_2, t_1 + t_2) = (4s_2 + 4s_1, t_2 + t_1) = (4s_2, t_2) + (4s_1, t_1) = b + a$$

Page 6

Tuesday, August 18, 2020 5:52 PM

R_2 : $4Z \times Z$ is associative under multiplication.

$$\begin{aligned}(ab)c &= [(4s_1,t_1)(4s_2,t_2)](4s_3,t_3)\\ &= (4s_1 4s_2, t_1 t_2)(4s_3,t_3)\\ &= (4s_1 4s_2 4s_3, t_1 t_2 t_3)\\ &= (4s_1,t_1)(4s_2 4s_3, t_2 t_3)\\ &= (4s_1,t_1)[(4s_2,t_2)(4s_3,t_3)]\\ &= a(bc)\end{aligned}$$

R_3 : The distributive laws hold. For example,

$$\begin{aligned}a(b+c) &= (4s_1,t_1)[(4s_2,t_2)+(4s_3,t_3)]\\ &= (4s_1,t_1)(4s_2+4s_3, t_2+t_3)\\ &= (4s_1(4s_2+4s_3), t_1(t_2+t_3))\\ &= (4s_1 4s_2 + 4s_1 4s_3, t_1 t_2 + t_1 t_3)\\ &= (4s_1 4s_2, t_1 t_2) + (4s_1 4s_3, t_1 t_3)\\ &= (4s_1,t_1)(4s_2,t_2) + (4s_1,t_1)(4s_3,t_3)\\ &= ab + ac\end{aligned}$$

A similar argument can be used to show $(a+b)c = ac + bc$

Since all of the properties hold, $4Z \times Z$ is a ring.

$4Z \times Z$ is commutative under $\bullet$

$Z \times Z$	$4Z \times Z$
unity element is $(1,1)$	does not have a unity element
$a(1,1) = (4s_1,t_1)\cdot(1,1)$	$(1,1) \notin 4Z \times Z$
$= (4s_1\cdot 1, t_1\cdot 1)$	$1 \notin 4Z$
$= (4s_1, t_1)$	
$= a$	

Recall! $Z_m = \{0, 1, 2, \ldots, m-1\}$ all possible remainders modulo m

Example 4: Compute (-4, 7) (2, 8) in $Z_3 \times Z_9$.

Solution:

$$(-4,7)\bullet(2,8) = (-4\cdot 2, 7\cdot 8)$$

$$= (-8, 56)$$

mod 3, mod 9

$$\boxed{(1, 2)}$$

express answer in $Z_3 \times Z_9$

mod 3, mod 9

$-8 \bmod 3 = 1$

$56 \bmod 9 = 2$

Note: The set of $m \times n$ matrices with entries in a ring R is an example of a non-commutative ring since matrix multiplication is known not to be commutative.

Theorem 2.5: If R is a ring with additive identity of 0, then for any $a, b \in R$, we have

1. $0a = a0 = 0$.
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$

Proof:

1.

■

2. We show that $a(-b) = -(ab)$.

Now, $\quad a(-b) + ab = a(-b + b) = a(0) = 0$.

Then, adding $-(ab)$ to both sides gives

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

Similarly, it can be shown that $(-a)b = -(ab)$.

■

3. Using property 2, we can show that

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

■

Page 8

Tuesday, August 18, 2020 5:52 PM

Units

Definition 2.6: Let R be a ring with unity $1 \neq 0$. An element $u \in R$ is a unit of R if it has a multiplicative inverse in R. That is, for $u \in R$, there exists an element $u^{-1} \in R$ where $u \cdot u^{-1} = u^{-1} \cdot u = 1 \in R$. If every non-zero element of R is a unit, then R is a division ring. A field is a commutative division ring.

Examples of Fields

The real numbers $\mathbb{R}$ and rational numbers Q under the operations of addition + and multiplication $\cdot$ are fields. However, the integers Z under addition + and multiplication $\cdot$ is not a field since the only non-zero elements that are units is -1 and 1. For example, the integer 2 has no multiplicative inverse since $\frac{1}{2} \notin Z$.

Example 5: Describe all units of the ring Z.

Solution: only units are -1 and 1 of $\mathbb{Z}$

$(1)(1) = 1$ multiplicative inverses are themselves which are integers

$(-1)(-1) = 1$ ∎

Example 6: Describe all units of the ring $\mathbb{R}$. (real #'s)

Solution: All nonzero reals are units since

$a \in \mathbb{R}$, $(a)\left(\frac{1}{a}\right) = 1$, $a^{-1} = \frac{1}{a}$ is mult inverse of a, $a \neq 0$ ∎

Example 7: Describe all units of the ring $Z \times Z$.

Solution: Note: Unity element is $(1,1)$

$(1,1)(1,1) = (1,1)$ ∎

$(-1,-1)\cdot(-1,-1) = (1,1)$

$(-1,1)\cdot(-1,1) = (1,1)$

$(1,-1)\cdot(1,-1) = (1,1)$

$\boxed{\text{4 units are } (1,1), (-1,-1), (-1,1), (1,-1)}$

Tuesday, August 18, 2020 5:52 PM

Recall Integers mod m: $Z_m = \{0, 1, 2, 3, \ldots, m-1\}$

Fact: For Z_m, $x \in Z_m$ is a unit only when $\gcd(x, m) = 1$.

Example 8: Find all of the units for the ring Z_{10}.

Solution: $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

$\boxed{\text{units are: } 1, 3, 7, 9}$

$1 = \gcd(1,10) = \gcd(3,10) = \gcd(7,10) = \gcd(9,10)$

$(3)(\overset{?}{7}) \bmod 10 = 1$ ∎

$3^{-1} = 7$ since $(3)(7) \bmod 10 = 21 \bmod 10 = 1$

Example 9: Find all of the units for the ring Z_7.

Solution:

$Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ 7 is prime

units are $1, 2, 3, 4, 5, 6$ since (all non-zero elements)

$1 = \gcd(1,7) = \gcd(2,7) = \gcd(3,7)$

$= \gcd(4,7) = \gcd(5,7) = \gcd(6,7)$ ∎

why is 2 not a unit in Z_{10}

$(2)(\overset{?}{\ }) \bmod 10 = 1$

no solution! $\gcd(2,10) = 2 \neq 1$

Note: If p is a prime, then $Z_p = \{0, 1, 2, 3, \ldots p-1\}$ is a field since all non-zero elements are units.

Exercises

1. Determine if the following sets under the usual operations of addition and multiplication represent that of a ring. If it is a ring, state whether the ring is commutative, whether it has a unity element, and whether it is a field. If it is not a ring, indicate why it is not.
   a. Z under usual addition and multiplication.
   b. $\mathbb{R}$ under usual addition and multiplication. (real #'s)
   c. $Z \times Z$ under usual addition and multiplication by components.
   d. The set $M_2(\mathbb{R})$ of invertible 2×2 matrices with real entries under usual addition and multiplication.
   e. $Z \times 2Z$ under usual addition and multiplication by components.
   f. Z^+ under usual subtraction and multiplication.

$Z^+ = \{1, 2, 3, 4, 5, 6, 7, \dots\}$

Not a ring: Not closed under subtraction

take $3 - 5 = -2 \notin Z^+$

2. Compute the following products in the given ring.
   a. (10)(8) in Z_{12}
   b. (8)(5) in Z_{15}
   c. (-10)(4) in Z_{26}
   d. (2, 3)(3, 5) in $Z_5 \times Z_9$
   e. (-5, 3)(4, -7) in $Z_6 \times Z_{11}$

$(-10)(4) = -40 \bmod 26 \boxed{= 12}$

3. Describe the units of the given rings.
   a. Z
   b. $Z \times Z$
   c. Q
   d. Z_5
   e. Z_8

Assume

$x^2 - y^2 = (x+y)(x-y)$

Goal to prove commutative is to show $xy = yx$

$x^2 - y^2 = \underline{(x+y)(x-y)}$

expand this side by Distributive Law and then work with equation

4. Show that $x^2 - y^2 = (x+y)(x-y)$ for all x, y in a ring R if and only if R is commutative.

5. Let $(R, +)$ be an abelian group. Show that $(R, +, \cdot)$ is a ring if we define $ab = 0$ for all $a, b \in R$.

6. Show for the ring Z_2, that the expansion $(x+y)^2 = x^2 + y^2$ is true.

$Z_2 = \{0, 1\}$

integers mod 2

$(x+y)^2 \leftarrow$ expand in normal way but reduce coeft's modulo 2 and see what you get

7. Show for the ring Z_p, where p is prime, that the expansion $(x+y)^p = x^p + y^p$ is true. Hint: Note that for a commutative ring, the binomial expansion

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}a^n,$$

where $\binom{n}{r} = \frac{n!}{r!(n-r)!}$, is true.

8. Show that the multiplicative inverse of a unit in a ring with unity is unique.

9. An element of a ring R is idempotent if $a^2 = a$.
   a. Show that the set of all idempotent elements of a commutative ring is closed under multiplication.
   b. Find all idempotents in the ring $Z_6 \times Z_{12}$.
   c. Show that if A is an $n \times n$ matrix such that AB is invertible, then the $n \times n$ matrix $B(AB)^{-1}A$ is an idempotent in the ring of $n \times n$ matrices.

If Neil is idempotent
$(\text{Neil})^2 = \text{Neil}$

To show closure under multiplication
Take two idempotent elements
a and b
Then $a^2 = a$ $b^2 = b$
To prove closure, show ab is idempotent
You must show $(ab)^2 = ab$

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

b.) $Z_6 = \{0,1,2,3,4,5\}$ | $Z_{12} = \{0,1,2,3,4,5,6,7,8,9,10,11\}$

Idempotents

Z_6

$0^2 = 0 \bmod 6 = 0$
$1^2 = 1 \bmod 6 = 1$
$2^2 = 4 \bmod 6 = 4 \neq 2$ X
$3^2 = 9 \bmod 6 = 3$
$4^2 = 16 \bmod 6 = 4$
$5^2 = 25 \bmod 6 = 1$ X

Z_{12}

$0^2 = 0 \bmod 12 = 0$
$1^2 = 1^2 \bmod 12 = 1$
X $2^2 = 4 \bmod 12 = 4 \neq 2$
X $3^2 = 9 \bmod 12 = 9 \neq 3$
$4^2 = 16 \bmod 12 = 4$
⋮
$11^2 = 121 \bmod 12 =$

form all combinations of idempotents elements of Z_6 and $Z12$ into idempotent coordinates in $Z_6 \times Z_{12}$
↑ 1st coord ↑ 2nd coord

$Z_6 \times Z_{12}$
$(\ ,\ )$ (Z_6 ↓, Z_{12} ↓)

$(3,4)$ is Idempotent in $Z_6 \times Z_{12}$

$$(3,4)^2 = (3,4)(3,4) = (9, 16) = (3, 4)$$

($9 \bmod 6$, $16 \bmod 12$)