1 MATH 340: Rings and Fields

1.1 Introduction

Definition 1.1 (Binary Operation)**.** An **internal binary operation** defined on a set S is a mapping $f : S \times S \to S$.

In this document, we will refer to these simply as **binary operations**.

The following are examples of binary operations:

1. Addition on the set of nonnegative integers $\mathbb{Z}_{\geq 0}$.
2. Subtraction on the set of integers $\mathbb{Z}$.
3. Multiplication on the set of $n \times n$ matrices with real number entries $\mathbb{R}^{n \times n}$.

The following are not binary operations:

1. Subtraction on the set of nonnegative integers $\mathbb{Z}_{\geq 0}$, because $0 - 1 = -1$ is not in $\mathbb{Z}_{\geq 0}$.
2. Division on the set of rational numbers $\mathbb{Q}$, because $1/0$ is not defined.

Definition 1.2 (Ring)**.** A **ring** is a set R with two binary operations—addition $(+)$ and multiplication $(\cdot)$—satisfying the following **ring axioms**:

1. Addition is associative, meaning $(a + b) + c = a + (b + c)$ for all $a, b, c \in R$.
2. Addition is commutative, meaning $a + b = b + a$ for all $a, b \in R$.
3. There is an identity element with respect to addition, meaning there exists $0 \in R$ satisfying $a + 0 = a$ and $0 + a = a$ for all $a \in R$.
4. Every element has an inverse with respect to addition, meaning that for all $a \in R$, there exists $b \in R$ satisfying $a + b = 0$ and $b + a = 0$.
5. Multiplication is associative, meaning $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
6. There is an identity element with respect to multiplication, meaning there exists $1 \in R$ satisfying $a \cdot 1 = a$ and $1 \cdot a = a$ for all $a \in R$.
7. Multiplication is distributive over addition, meaning $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in R$.

The following are examples of rings.

1. The set of integers $\mathbb{Z}$ with addition and multiplication defined conventionally.
2. The set of $n \times n$ matrices with entries from a ring R, along with the addition and multiplication operations copied from R.

By convention, the addition operation of a ring is denoted $(+)$, and the multiplication operation of a ring is denoted $(\cdot)$. Furthermore, adding an additive inverse is usually written as "subtraction", meaning $a + (-b) \equiv a - b$, and the multiplication operation is usually written without $(\cdot)$, meaning $a \cdot b \equiv ab$. We will adopt all of these these conventions. To provide alternative notation, a ring is generally described $(R, +, \cdot)$, meaning the underlying set is R, the addition operation is $(+)$, and the multiplication operation is $(\cdot)$.

Some texts do not require condition (6) to hold, that is, their rings do not necessarily an identity element with respect to multiplication. See this Wikipedia article for more information. As a subjective opinion, this seems to be somewhat of a stylistic choice: if there is no multiplicative identity, then we cannot take the product of an arbitrary collection of elements, because this would be undefined if the collection is empty. On the other hand, sometimes it simply does not make sense to force the existence of a multiplicative identity. This may not be the best example, but later we will define a special type of "subring" called an ideal, which should not be defined as requiring a multiplicative identity.

Definition 1.3 (Commutative ring)**.** A **commutative ring** is a ring R with the additional property that the multiplication operation is commutative, meaning $ab = ba$ for all $a, b \in R$.

Proposition 1.1. *Let R be a ring, then R has exactly one additive identity.*

Proof. By definition, we know that R has at least one additive identity, so we will show it has at most one. Let $a, b \in R$ be two additive identities, and see that $a+b = b$ because a is an additive identity. But also, we see that $a+b = a$, because b is an additive identity, so it follows that $a = b$. This means every additive identity is the same, so there is at most one. □

Proposition 1.2. *Let R be a ring, then R has exactly one multiplicative identity.*

Proof. Refer to the proof of the uniqueness of the additive identity, and replace addition with multiplication. □

Since we now know that rings contain exactly one additive and multiplicative identity, we can (and will) denote these values with 0 and 1 respectively.

Proposition 1.3. *Let R be a ring, and $a \in R$. Then a has exactly one additive inverse.*

Proof. By definition, we know that a has at least one additive inverse, so we show it has at most one. Suppose $b, c \in R$ are both additive inverses of a, and see the following:

$$\begin{aligned} a+b=0 \text{ and } a+c=0 &\implies b+(a+b)=b+(a+c) && (1)\\ &\iff (b+a)+b=(b+a)+c && (2)\\ &\iff 0+b=0+c && (3)\\ &\iff b=c && (4) \end{aligned}$$

This means every additive inverse of a is the same, so there is at most one. □

Let R be a ring, and $a \in R$. Since we now know the additive inverse of a is unique, we can (and will) denote this value with $-a$.

Proposition 1.4. *Let R be a ring, and $a \in R$. Then $0a = 0$.*

Proof. See that

$$\begin{aligned} (0+0)a=0a &\iff 0a+0a=0a && (5)\\ &\iff 0a+0a-(0a)=0a-(0a) && (6)\\ &\iff 0a=0 && (7) \end{aligned}$$

□

Proposition 1.5. *Let R be a ring, and $a, b \in R$. Then $(-a)b = -(ab) = a(-b)$.*

Proof. For the first equality, we use multiplication by zero to see that

$$\begin{aligned} 0b=0 &\iff ((-a)+a)b=0 && (8)\\ &\iff (-a)b+ab=0 && (9)\\ &\iff (-a)b+ab-(ab)=0-(ab) && (10)\\ &\iff (-a)b=-(ab) && (11) \end{aligned}$$

For the second equality, we use the same approach to see that

$$\begin{aligned} a0=0 &\iff a((-b)+b)=0 && (12)\\ &\iff a(-b)+ab=0 && (13)\\ &\iff a(-b)+ab-(ab)=0-(ab) && (14)\\ &\iff a(-b)=-(ab) && (15) \end{aligned}$$

□

From these last two proofs, we see that it is allowed to "cancel out" identical addition terms from both sides of an equation. This is due to the associativity and commutativity of addition, along with the existence of an additive identity for every element. Keep this in mind as, in the future, we may not explicitly write the subtraction on both sides.

Definition 1.4 (Zero divisor)**.** Let R be a ring, and $a \in R$. Then a is a **left zero divisor** if there exists nonzero $b \in R$ such that $ab = 0$, a **right zero divisor** if there exists nonzero $c \in R$ such that $ca = 0$, and a **zero divisor** if it is either a left zero divisor or a right zero divisor.

Proposition 1.6. *Let R be a ring, and $a \in R$. Then a is a left zero divisor if and only if there exists $b, c \in R$ satisfying $b \neq c$ and $ab = ac$.*

Proof. Suppose a is a left zero divisor, so there exists nonzero $b \in R$ such that $ab = 0$. Set $c = 0$ and see that $b \neq c$ and $ab = ac$.

Suppose there exists $b, c \in R$ satisfying $b \neq c$ and $ab = ac$. We see that $ab = ac \iff ab - ac = 0 \iff a(b - c) = 0$, but since $b \neq c \iff b - c \neq 0$, this means a is a left zero divisor. □

Definition 1.5 (Integral domain)**.** An **integral domain** is a commutative ring R with the additional property that $ab = 0 \implies a = 0$ or $b = 0$ for all $a, b \in R$. This is equivalent to saying that R has no nonzero zero divisors.

Definition 1.6 (Unit)**.** Let R be a ring, and $a \in R$. Then a is a **unit** if there exists $b \in R$ such that $ab = 1$ and $ba = 1$.

Proposition 1.7. *Let R be a ring, and $a \in R$ a unit. Then a has exactly one multiplicative inverse.*

Proof. Refer to the proof of the uniqueness of the additive inverse, and replace addition with multiplication and 0 with 1. □

Let R be a ring, and $a \in R$ a unit. Since we now know the multiplicative inverse of a is unique, we can (and will) denote this value with a^{-1}.

Proposition 1.8. *Let R be a ring, and $a \in R$. Then a cannot be both a unit and a zero divisor.*

Proof. Towards a contradiction, suppose a is both a unit and a zero divisor. Without loss of generality, assume a is a left zero divisor, so there exists nonzero $b \in R$ such that $ab = 0$. Since a is a unit, there exists $c \in R$ such that $ca = 1$. Now we see that $ab = 0 \iff cab = c0 \iff b = 0$, but b is nonzero, a contradiction. □

Definition 1.7 (Zero ring)**.** A **zero ring** is a ring containing a single element. This kind of ring is "zero" because the single element must be the additive identity, denoted by 0.

Definition 1.8 (Field)**.** A **field** is a nonzero commutative ring R with the additional property that every nonzero element is a unit.

Definition 1.9 (Characteristic)**.** The **characteristic** of a ring R is the least positive integer c satisfying $\underbrace{1+\cdots+1}_{c \text{ times}} = 0$. If such an integer does not exist, then the characteristic is 0.

Proposition 1.9. *Let R be a ring with characteristic c. If c is a composite number, then R has zero divisors.*

Proof. Since c is composite, there exists $m, n \in \mathbb{Z}_{\geq 0}$ satisfying $c = mn$ and $m, n < c$. Let $r = \underbrace{1+\cdots+1}_{m \text{ times}} \in R$ and $s = \underbrace{1+\cdots+1}_{n \text{ times}} \in R$, which are both nonzero by minimality of c. Now distributivity gives us

$$rs = (\underbrace{1+\cdots+1}_{m \text{ times}})(\underbrace{1+\cdots+1}_{n \text{ times}}) = \underbrace{1+\cdots+1}_{c \text{ times}} = 0,$$

so r and s are zero divisors in R. □

Theorem 1.1 (Euler)**.** *Let R be a commutative ring, and $R^\times$ the set of units in R. If $n \coloneqq |R^\times|$ is finite, then $a^n = 1$ for all $a \in R^\times$.*

Proof. Let $\phi : R^\times \to R^\times$ be a mapping defined by $r \mapsto ar$. Since ϕ is a mapping between equally sized finite sets, we will show that it is injective, which would imply that it is bijective. See that $\phi(r) = \phi(s) \iff ar = as \iff (a^{-1})ar = (a^{-1})as \iff r = s$.

Now we know that ϕ is a bijection, which means $R^\times = \phi(R^\times)$. The theorem follows from the following equality of products:

$$\prod_{r \in R^\times} \phi(r) = \prod_{r \in R^\times} r \iff \prod_{r \in R^\times} ar = \prod_{r \in R^\times} r \tag{16}$$

$$\iff a^n \prod_{r \in R^\times} r = \prod_{r \in R^\times} r \tag{17}$$

$$\iff a^n = 1 \tag{18}$$

□

We note that the commutativity of multiplication is required for this proof, otherwise we couldn't pull out a factor of a from each factor on the left hand side. However Euler's theorem also holds for noncommutative rings, although we are currently unable to confirm this.

Proposition 1.10. *Let R be a ring, and $a \in R$ not a zero divisor. If n is a positive integer, then a^n is not a zero divisor.*

Proof. For a contradiction, suppose there exists a positive integer n for which a^n is a zero divisor. Let n be the least such positive integer and, by definition, there exists a nonzero $b \in R$ such that $a^n b = 0$. By the minimality of n, we note that a^{n-1} is not a zero divisor, so $a^{n-1}b$ is nonzero. But $a^n b = a(a^{n-1}b) = 0$ implies a is a zero divisor, a contradiction. □

Proposition 1.11. *Let R be a ring whose underlying set is finite, and $a \in R$. Then a is either a zero divisor or a unit.*

Proof. Suppose a is not a zero divisor, and we will show that a is a unit. Consider the sequence $a, a^2, a^3, \ldots$ which, since a is not a zero divisor, only contains nonzero elements. Since R is finite but the sequence is infinite, some element in the sequence must repeat, so there exists positive integers n, k satisfying $a^n = a^{n+k}$. This means $a^n \cdot 1 = a^n \cdot a^k$ and, since a^n is not a zero divisor, we can cancel out to see that $a^k = 1$. This means a^{k-1} is a multiplicative inverse of a, so a is a unit. □