1 Algebra

Definition 1.1. A number is called an *algebraic number* if it satisfies a polynomial equation

$$c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 = 0$$

where the coefficients $c_0, c_1, \ldots, c_n$ are integers and $c_n \neq 0$ and $n \geq 1$.

Theorem 1.1 (Rational Zeros Theorem)**.** *Suppose $c_0, c_1, \ldots, c_n$ are integers and $r \in \mathbb{Q}$ satisfies the polynomial*

$$c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 = 0$$

where $n \geq 1, c_n \neq 0,$ and $c_0 \neq 0$. Let $r = \frac{m}{d}$, where $m, d \in \mathbb{Z}$ such that $\gcd(m, d) = 1$ and $d \neq 0$. *Then $m \mid c_0$* and *$d \mid c_n$.*

Proof. Let $x = r = m/d$ be a solution to the polynomial. Then,

$$\begin{gathered} c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0 = 0, \\ c_n \left(\frac{m^n}{d^n}\right) + c_{n-1}\left(\frac{m^{n-1}}{d^{n-1}}\right) + \ldots + c_1\left(\frac{m}{d}\right) + c_0 = 0. \\ c_n m^n + c_{n-1}m^{n-1}d + \cdots + c_1 m d^{n-1} + c_0 d^n = 0 \end{gathered}$$

Then rearranging, we see

$$c_0 d^n = -m\left(c_n m^{n-1} + c_{n-1}m^{n-2}d + \cdots c_1 d^{n-1}\right)$$

Since $gcd(m, d) = 1$, we know that $gcd(m, d^n) = 1$, and thus m divides c_0. Now rearranging again, we see

$$c_n m^n = -d\left(c_{n-1}m^{n-1} + \cdots + c_1 m d^{n-2} + c_0 d^{n-1}\right)$$

Thus, d divides c_n.

□

Remark 1.1. The result above states that given a polynomial with integer coefficients, a constant term, and a nonzero leading coefficient, if the polynomial is going to have rational roots, then the numerator of the root will divide the constant and the denominator will divide the leading coefficient. Note that often the leading coefficient is 1 so we typically only ensure the numerator divides the constant. Also note that we are not saying this rational is always a root, we are only saying that if a rational is a root, it has the form described above.

1.1 Divisibility in $\mathbb{Z}$

We start by defining the integers. This ordered set will be our object of study. SAY MORE HERE

Definition 1.2 ($\mathbb{Z}$)**.** The set of integers is any ordered set equipped with two operations $+, \cdot$ that satisfy the following axioms. $\forall a, b, c \in \mathbb{Z}$:

1. If $a, b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$ *[Closure for addition]*
2. $a + (b + c) = (a + b) + c$ *[Associative addition]*
3. $a + b = b + a$ *[Commutative addition]*
4. $a + 0 = a = 0 + a$ *[Additive identity]*
5. For each $a \in \mathbb{Z}$, the equation $a + x = 0$ has a solution in $\mathbb{Z}$.
6. If $a, b \in \mathbb{Z}$, then $ab \in \mathbb{Z}$ *[Closure for multiplication]*
7. $a(bc) = (ab)c$ *[Associative multiplication]*

8. $a(b+c) = ab + ac$ and
   $(a+b)c = ac + bc$ *[Distributive laws]*
9. $ab = ba$ *[Commutative multiplication]*
10. $a \cdot 1 = a = 1 \cdot a$ *[Multiplicative identity]*
11. If $ab = 0$, then $a = 0$ or $b = 0$.

Remark 1.2. The below result is foundational to all of number theory and abstract algebra. It is the idea that given some number a to know how b *fits into* a we will take as many copies or multiples of b. We want to show existence and uniqueness. To show existence, we will show that such an r satisfying the hypothesis exists.
So we will consider numbers of the form $r = a - bq$. So we make a set of this form and show that it is nonempty. Then we will let the unique q, r correspond to the min of the set.

Theorem 1.2 (Division Algorithm)**.** *Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique $q, r \in \mathbb{Z}$ such that*

$$a = bq + r \text{ and } 0 \leq r < b.$$

Proof. Consider,

$$S = \{a - bx \mid \forall x \in \mathbb{Z}\}$$

We start by showing S is nonempty.
Observe that $|a| \in S$ since we can let $x = 0$ which gives $0 \leq a$, which tells us positive a is in S.
Now let $r = \min S$. We know r exists by the Well Ordering Axiom. Then let $x = q$ correspond to r.
We will now show that $r < b$.
By contradiction, suppose $r > b$. Then this gives us that there is at least one factor of b in r.

$$a = bq + r = b(q+1) + r' \implies r' \in S \text{ and } r' < r$$

which contradicts that $r = \min S$, thus q and r exist.
Now we show uniqueness. Suppose there exists r' and q' such that

$$a = bq + r = bq' + r' \implies r' - r = b(q - q').$$

Since we have that both r and r' are less than b, this gives

$$| r' - r | < b \implies | b(q - q') | < b \implies | q - q' | < 1$$

Then since the difference $q - q'$ is an integer, we have that $q = q' \implies r = r'$. □

Definition 1.3 (Greatest Common Divisor)**.** For any two nonzero integers a and b, the *greatest common divisor* $gcd(a, b)$ is the unique positive integers d such that

1. $d \mid a$ and $d \mid b$
2. If $\exists c \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$, then $c \leq d$.

Remark 1.3. The greatest common divisor between any two integers will prove to be an important topic. When broken down, it is essentially a set of the shared factors of a and b. Why would that be so? Because if d is the greatest magnitude greater than 0 that divides both a and b then every other divisor that is greater than 0 but be *contained* in the magnitude of d. This will be helpful as a sort of relation between the integers and their *intersection with respect to divisibility.*

Theorem 1.3 (Bezout's Identity)**.** *Let a and b be integers, not both 0, and let $d = gcd(a, b)$. Then there exists integers u and v such that*

$$gcd(a, b) = d = au + bv$$

Remark 1.4. *Why would this make sense?* So recall that the *gcd* is the largest *positive* divisor, then it would be plausible that the smallest positive integer linear combination of a and b is largest factor that is shared amongst a and b. That is, through linear combinations, we can remove the multiples and factors of a and b that they dont have in their *intersection*, then the magnitude that remains would be the *gcd*. Also notice the usefulness of this result. This allows us to relate the divisibility structure of a and b to any combination that is made with them. *Why does the gcd have to be the least positive element?* First consider if the smallest positive linear combination was greater than, say, a. Since the *gcd* divides both a and b, the smallest linear combo must be less than both a and b. If the smallest linear combo was smaller than the *gcd* then we would have that factors of a and b combine to something positive but less than the greatest factor they have in common.

Proof. Let $S = \{au + bv \mid u, v \in \mathbb{Z}\}$. We will first show that S contains positive integers. Let $u = a$ and $v = b$, then we have $a^2 + b^2 \in S$. Thus there exists positive integers in S. Let $t = \min S$, which we know exists because $S \subset \mathbb{Z}$ so by well ordering axiom there must exist a least positive element. Define $d = gcd(a, b)$. We want to show that $t = d$. We will start by showing $t \mid a$ and $t \mid b$.

$$\text{By 1.2,} \quad a = tq + r \implies r = a - tq \implies r = a - aqu - bqv \implies r = a(1 - qu) + b(-qv)$$

Thus $r \in S$, but since, by the hypothesis of 1.2 $\quad r < t = \min S$. This implies that

□

Remark 1.5. So we hypothesized that the *gcd* was going to be a linear combination of a and b because it is the greatest factor of them both, so in a way, they can both construct it. We then hypothesized in the proof that the *gcd* is the least positive multiple. So to show that t is the *gcd*, we show that it divides them both and is the greatest such integer to do so. To show that t divides a and b, we show, using 1.2 that the remainder must be in S, but that would mean the remainder is less than t so that gives us what we are looking for.

Proposition 1.1. *Let $a, b, x, y \in \mathbb{Z}$. Then*

$$ax + by = c \iff gcd(a, b) \mid c.$$

Proof. Suppose $ax + by = c$ and let $d = gcd(a, b)$. Then

$$\exists k, l \in \mathbb{Z} \text{ such that } c = dkx + dly \implies d \mid c.$$

Conversely, assume $d = gcd(a, b) \mid c$. That is, $\exists k \in \mathbb{Z}$ such that $dk = c$. Then

$$c = dk = a(kx) + b(ky) \implies \exists u, v \in \mathbb{Z},\ c = au + bv.$$

This concludes the proof. □

Proposition 1.2. *Let $a, b, c \in \mathbb{Z}$. If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.*

Proof. Suppose $a \mid bc$ and $gcd(a, b) = 1$. Then $\exists k \in \mathbb{Z}$ such that $ak = bc$. Also by 1.3,

$$\exists u, v \in \mathbb{Z} \text{ such that } 1 = au + bv$$

$$\implies c = acu + bcv \implies c = ac + akv.$$

Thus $a \mid c$. □

Remark 1.6. This proposition is insightful to how the *gcd* will be used often. Notice we have that a divides a product but it shares no factors with b, who is also in the product. Thus the only factors it must share with the product must be with c. So we would expect to have that a divides c.

Exercise 1.1. *Let $a, b, c \in \mathbb{Z}$. Suppose $\gcd(a, b) = 1$. If $a|c$ and $b|c$, then $ab|c$.*

Exercise 1.2. *Let $a, b, c \in \mathbb{Z}$. Then $\forall t \in \mathbb{Z}$ all of the following hold*

1. $\gcd(a, b) = \gcd(a, b + at)$
2. $\gcd(ta, tb) = t \gcd(a, b) \quad$ for $t > 0$

3. $\gcd(a, \gcd(b, c)) = gcd(gcd(a, b), c)$

4. $\gcd(a, c) = 1 \implies \gcd(ab, c) = \gcd(b, c)$

Exercise 1.3. *Let $a, b, c \in \mathbb{Z}$. If $\gcd(a, c) = 1$ and $\gcd(b, c) = 1$, then $\gcd(ab, c) = 1$*

Exercise 1.4. *A positive integer is divisible by 3 $\iff$ the sum of its digits is divisible by 3.*

Theorem 1.4. *Let $p \in \mathbb{Z}$ with $p \neq 0, 1, -1$. Then p is prime if and only if p has the following property*

$$\text{whenever } p \mid bc, \text{ then } p \mid b \text{ or } p \mid c$$

Remark 1.7. This is obvious in comparison to 1.2 since a prime is coprime to every integer. Thus we will lean on that proof heavily.

Proof. Suppose p is prime and consider $p \mid bc$. Since p is prime, if $p \mid b$ then the theorem is proved, if $p \nmid b$ then since p is prime, $gcd(p, b) = 1$. By 1.2 this gives us that $p \mid b$ or $p \mid c$.
Conversely, by the contrapositive, suppose p is not prime. Then if $p \mid bc$ then to have $p \mid b$ or $p \mid c$ we would need that $gcd(p, b) = 1$, $\forall b \in \mathbb{Z}$. But this would mean that p is prime.
□

Theorem 1.5 (Fundamental Theoerem of Arithmetic)**.** *Every integer $n \neq 0, 1, -1$ has a unique prime factorization.*

Proof. First we will show existence of the factorization.
Let $S = \{n \in \mathbb{N} \mid n > 1 \text{ and } \nexists \text{ primes } p_1 p_2 \cdots p_n \text{ such that } p_1 p_2 \cdots p_n = n\}$. Then assume, by contradiction, that S is nonempty. Then by the well ordering axiom, let $n = \min S$. Since n is not prime, $\exists a, b \in \mathbb{Z}$ such that $ab = n$. Then this means $a \mid n$ and $b \mid n$. Since $a, b \leq n$, we have that a and b have prime factorizations. Thus n has a prime factorization. This proves the existence of a prime factorization for all integers.
Now we will show that this factorization is unique.
By □

Exercise 1.5. *If $n > 1$ has no positive prime faster less than or equal to $\sqrt{n}$, then s is prime.*

Exercise 1.6. $a|b \iff a^n|b^n$

1.2 Congruence and Congruence Classes

Remark 1.8. The concepts below intend to study the structure that arithmetic and divisibility have among the integers. We do this by making our object of focus the remainder that an integer leaves after being divided. If some integer a leaves behind the same remainder as some other integer b when divided by n, then their difference $a - b$ is divisible by n. If we use their unique representation from 1.2, then

$$a - b = nq_1 + r - nq_2 - r = n(q_1 - q_2)$$

Why do we care about the divisibility structure? We will soon see that what we see as divisibility among numbers can actually be abstracted and shown to be an example of a more general concept. The concepts discussed later will show that the properties we find out about the integers actually are very similar properties that the more general elements share with each other.

Definition 1.4 (Congruence $\pmod n$)**.** Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then a is congruent to b modulo n if $n \mid a - b$. This is denoted $a \equiv b \pmod n$

Theorem 1.6 (Congruence $\in$ Equivalence Relations)**.** *Let n be a positive integer, then $\forall a, b, c \in \mathbb{Z}$,*

1. $a \equiv a \pmod n$

2. *If* $a \equiv b \pmod n$, *then* $b \equiv a \pmod n$

3. *If* $a \equiv b \pmod n$ *and* $b \equiv c \pmod n$, *then* $a \equiv c \pmod n$.

Proof. The proof of (1) and (2) is straightforward after seeing the proof of (3). If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$ then we can write

$$\begin{aligned} \exists k, l \in \mathbb{Z} : \quad & a - b = nk \quad \text{and} \quad b - c = nl \\ \implies \quad & b = a - nk \quad \text{and} \quad b = c + nl \\ \implies \quad & a - c = n(k + l). \end{aligned}$$

Thus $a \equiv c \pmod{n}$.

□

Proposition 1.3 (Modulo Arithmetic)**.** *If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then*

1. $a + c \equiv b + d \pmod{n}$
2. $ac \equiv bd \pmod{n}$

Proof. (1) : Since $a \equiv b$ and $c \equiv d$ we have, by definition, $a - b = nk$ and $c - d = nl$. Adding these, we obtain $(a + c) - (b + d) = n(k + l) \implies a + c \equiv b + d$.
(2) : So we want $ac \equiv bd$, or equivalently, we want to find $k \in \mathbb{Z}$ such that $ac - bd = nk$. Then to use the hypothesis we do,

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = c(nk) + b(nl) = n(ck + bl).$$

Thus, $ac \equiv bd \pmod{n}$.

□

Definition 1.5 (Congruence Class)**.** Let $a, n \in \mathbb{Z}$ be integers with $n > 0$. The *congruence class* of a modulo n (denoted $[a]$) is the set of all integers that are congruent to a modulo n, that is,

$$[a] = \{b \mid b \in \mathbb{Z} \quad \text{and} \quad b \equiv a \pmod{n}\}.$$

Recall $b \equiv a \pmod{n}$ means that $b - a = kn$ for some integer k or, equivalently, that $b = a + kn$. Thus

$$[a] = \{b \mid b \equiv a \pmod{n}\} = \{b \mid b = a + kn \text{ with } k \in \mathbb{Z}\} = \{a + kn \mid k \in \mathbb{Z}\}$$

Theorem 1.7 (Congruence Class Equality)**.** *$a \equiv c \pmod{n}$ if and only if $[a] = [c]$.*

Proof. Suppose $a \equiv c$, we want to show that $[a] \subset [c]$ and $[c] \subset [a]$, so also suppose that $x \in [a]$. Then by definition of $[a]$, $x \in [a] \implies x \equiv a$, then by transitivity, we have that $x \equiv a$ and $a \equiv c \implies x \equiv c \implies x \in [c]$. Suppose instead that $x \in [c]$. Then again by transitivity we obtain that $x \in [a]$.
Suppose $[a] = [c]$. Then by definition of $[a]$, $a \equiv a$ but since $[a] = [c]$, we have that $a \equiv a \implies a \in [c] \implies a \equiv c$. □

Corollary 1.1. *Two congruence classes modulo n are either disjoint or identical.*

Proof. If $[a]$ and $[c]$ are disjoint, there is nothing to prove. Suppose that $[a] \cap [c]$ is nonempty. Then there is an integer b with $b \in [a]$ and $b \in [c]$. Then, by the definition of congruence class, $b \equiv a \pmod{n}$ and $b \equiv c \pmod{n}$. Therefore, by symmetry and transitivity, $a \equiv c \pmod{n}$. Then by 1.7 we have that, $[a] = [c]$. □

Exercise 1.7. *Let $n > 1$ be an integer and consider congruence modulo n.*

1. *If a is any integer and r is the remainder when a is divided by n, then $[a] = [r]$.*
2. *There are exactly n distinct congruence classes, namely, $[0], [1], [2], \ldots, [n - 1]$.*

Proof. (1) : Suppose a is an integer and r is the remainder when a is divided by n, then from 1.2 we have, $a = nk + r$ or $a - r = nk \implies a \equiv r \implies [a] = [r]$. Where the last implication used 1.7.
(2) : From (1) we know that any given integer will be the same congruence class as its remainder r where $0 \leq r < n$, thus there are $n - 1$ such possible remainders. We also have from 1.1 that each class is disjoint, thus there are $n - 1$ possible equivalence classes.

□

Definition 1.6. The set of all congruences classes modulo n is denoted $\mathbb{Z}_n$.
Note that an element of $\mathbb{Z}_n$ is a class, the set of integers that it is congruent to, not a single integer.

Exercise 1.8. *If a, b are integers such that $a \equiv b \pmod{p}$ for every positive prime p, then $a = b$.*

Remark 1.9. We will continue to study division in the integers at this abstracted level by using the concept that equivalence is defined by having the same remainder when divided by a number. The congruence class $\mathbb{Z}_n$ is a set consisting of other sets. These other sets are the sets of integers that are congruent modulo n, and the numbers that are congruent modulo n are the ones that have the same remainder when divided by n. Now we can define relations between classes more effectively.

Theorem 1.8. *If $[a] = [b]$ and $[c] = [d]$ in $\mathbb{Z}_n$, then*

$$[a + c] = [b + d] \quad \text{and} \quad [ac] = [bd].$$

Proof. From 1.7 we have that $a \equiv b$ and $c \equiv d$. Then from 1.3 we have

$$a + c \equiv b + d \quad \text{and} \quad ac \equiv bd$$

Then from 1.7 again we have $[a + c] = [b + d]$ and $[ac] = [bd]$. □ □

Definition 1.7 (Operations in $\mathbb{Z}_n$)**.** We define addition $+$ and multiplication $\cdot$ in $\mathbb{Z}_n$ by

$$[a] \oplus [c] = [a + c] \quad \text{and} \quad [a] \odot [c] = [ac].$$

Proposition 1.4. *For any classes $[a], [b], [c]$ in $\mathbb{Z}_n$,*

1. *If $[a] \in \mathbb{Z}_n$ and $[b] \in \mathbb{Z}_n$, then $[a] \oplus [b] \in \mathbb{Z}_n$.*
2. $[a] \oplus ([b] \oplus [c]) = ([a] \oplus [b]) \oplus [c]$.
3. $[a] \oplus [b] = [b] \oplus [a]$.
4. $[a] \oplus [0] = [a] = [0] \oplus [a]$.
5. *For each $[a]$ in $\mathbb{Z}_n$, the equation $[a] \oplus x = [0]$ has a solution in $\mathbb{Z}_n$.*
6. *If $[a] \in \mathbb{Z}_n$ and $[b] \in \mathbb{Z}_n$, then $[a] \odot [b] \in \mathbb{Z}_n$.*
7. $[a] \odot ([b] \odot [c]) = ([a] \odot [b]) \odot [c]$.
8. $[a] \odot ([b] \oplus [c]) = [a] \odot [b] \oplus [a] \odot [c]$ *and*
   $([a] \oplus [b]) \odot [c] = [a] \odot [c] \oplus [b] \odot [c]$.
9. $[a] \odot [b] = [b] \odot [a]$.
10. $[a] \odot [1] = [a] = [1] \odot [a]$.

Remark 1.10 (Change of Notation)**.** From now on, to denote an element in $\mathbb{Z}_n$ we will just denote it by its integer form. That is, when we say we are *in* $\mathbb{Z}_n$, then we will write $[a]_n$ as a. This is just for notational convenience, nothing has changed.

Remark 1.11. After some work with the integers modulo n, we start to notice a pattern, when the integers are modulo a prime number, the $\mathbb{Z}_n$ product of nonzero elements is always nonzero. So the distinction is that when $a \neq 0$ the equation $ax = 1$ has a solution in $\mathbb{Z}$ if and only if $a = 1$ or $a = -1$, but for the multiplication in $\mathbb{Z}_p$ where p is a prime, the equation always has a solution.

Theorem 1.9. *If $p > 1$ is an integer, then the following are equivalent:*

1. *p is prime.*
2. *For any $a \neq 0$ in $\mathbb{Z}_p$, the equation $ax = 1$ has a solution in $\mathbb{Z}_p$.*
3. *Whenever $bc = 0$ in $\mathbb{Z}_p$, then $b = 0$ or $c = 0$.*

Corollary 1.2. *Let a and n be integers with $n > 1$. Then*
The equation $[a]x = [1]$ has a solution in $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$ in $\mathbb{Z}$.

Definition 1.8 (Units)**.** For any $a \in \mathbb{Z}_n$, if $\exists b \in \mathbb{Z}_n$ such that $ab = 1$, then a is a *unit*. In this case, we say b is the *inverse* of a.

Definition 1.9 (Zero Divisors)**.** Suppose $a \in \mathbb{Z}_n$ and $a \neq 0$. If $\exists c \in \mathbb{Z}_n$ such that $c \neq 0$ and $ac = 0$.

Exercise 1.9. *Let $n > 1$ be an integer and let a, b be integers. Define $d = \gcd(a, n)$. Consider the linear congruence*

$$[a]x = [b] \quad \text{in } \mathbb{Z}_n.$$

1. *Show that the congruence has at least one solution if and only if $d \mid b$. Conclude that no solution exists when $d \nmid b$.*

2. *Assume $d \mid b$. Use Bézout's identity to find integers u, v such that*

$$au + nv = d.$$

Show that

$$x = \left[\frac{b}{d}u\right]$$

is a solution in $\mathbb{Z}_n$.

3. *Prove that every solution is of the form*

$$x = \left[\frac{b}{d}u + k\frac{n}{d}\right], \quad k \in \{0, 1, \ldots, d-1\}.$$

Show that these d solutions are pairwise distinct.

4. *Conclude that if $d \mid b$, there are exactly d distinct solutions, and otherwise, there are none. Explain how this fully classifies solutions to linear congruences.*

5. *Solve the congruences:*

$$13x = 9 \quad \text{in } \mathbb{Z}_{24}, \quad \text{and} \quad 25x = 10 \quad \text{in } \mathbb{Z}_{65}.$$

6. *Show that if $\gcd(a, n) = 1$, then $[a]$ is invertible in $\mathbb{Z}_n$, ensuring a unique solution to $[a]x = [b]$. Relate this to computing the inverse of $[a]$ in $\mathbb{Z}_n$.*

1.3 Rings

We now generalize the properties we have found consistent across the number-like systems we have studied.

Definition 1.10 (Ring)**.** A ring is a nonempty set R equipped with two operations $+, \cdot$ that satisfy the following axioms. $\forall a, b, c \in R$:

1. If $a \in R$ and $b \in R$, then $a + b \in R$. [Closure under Addition]
2. $a + (b + c) = (a + b) + c$ [Associativity of Addition]
3. $a + b = b + a$ [Commutativity of Addition]
4. There exists an element $0_R \in R$ such that $a + 0_R = a = 0_R + a, \ \forall a \in R$ [Additive identity]
5. For each $a \in R$, $a + x = 0_R$ has a solution in R, that is, $x \in R$ [Additive Inverse]
6. If $a \in R$ and $b \in R$, then $ab \in R$ [Closure under Multiplication]
7. $a(bc) = (ab)c$ [Associativity of Multiplication]
8. $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$ [Distributive Law]

Definition 1.11 (Commutative Ring)**.** A commutative ring is a ring R that satisfies the additional axiom: commutative multiplication

$$ab = ba \quad \forall a, b \in R.$$

Definition 1.12 (Multiplicative Identity)**.** A ring with indentity is a ring R that contains an element 1_R that satisfies the additional axiom: multiplicative identity

$$a1_R = a = 1_R a \quad \forall a \in R.$$

Definition 1.13 (Integral Domain)**.** An integral domain is a commutative ring R with identity $1_R \neq 0_R$ that satisfies the additional axiom

$$\text{Whenever } a, b \in R \text{ and } ab = 0_R, \text{ then } a = 0_R \text{ or } b = 0_R.$$

Definition 1.14 (Field)**.** A field is a commutative ring R with identity $1_R \neq 0_R$ that satisfies the axiom

$$\text{For each } a \neq 0_R \in R, \quad ax = 1_R \text{ has a solution in } R$$

Remark 1.12. Note that these operations don't have to adhere to what we think of as addition and multiplication of two numbers....

Proposition 1.5. *Let R and S be rings. Define addition and multiplication on the Cartesian product $R \times S$ by*

$$(r, s) + (r', s') = (r + r', s + s') \quad \text{and} \quad (r, s)(r', s') = (rr', ss').$$

Then $R \times S$ is a ring. If R and S are both commutative, then so is $R \times S$. If both R and S have an identity, then so does $R \times S$.

Theorem 1.10 (Subring)**.** *Suppose that R is a ring and that S is a subset of R such that:*

1. *S is closed under addition (if $a, b \in S$, then $a + b \in S$);*
2. *S is closed under multiplication (if $a, b \in S$, then $ab \in S$);*
3. *$0_R \in S$;*
4. *If $a \in S$, then the solution of the equation $a + x = 0_R$ is in S.*

Then S is a subring of R.

Proof. In order for S to be a subring of R, we only need to check that the axioms for rings hold. Additonally, we need that the additive identity of S is the same one that is in R. We need only check that axioms, from definition (1.10), 1,6,4, and 5 hold since axioms 2,3,7, and 8 hold for all elements of R. □

Theorem 1.11. *For any element a in a ring R, the equation $a + x = 0_R$ has a unique solution.*

Theorem 1.12. *If $a + b = a + c$ in a ring R, then $b = c$.*

Proposition 1.6. *For any elements a and b of a ring R,*

1. *$a \cdot 0_R = 0_R = 0_R \cdot a$. In particular, $0_R \cdot 0_R = 0_R$.*
2. *$a(-b) = -ab \quad$ and $\quad (-a)b = -ab$.*
3. *$-(-a) = a$.*
4. *$-(a + b) = (-a) + (-b)$.*
5. *$-(a - b) = -a + b$.*
6. *$(-a)(-b) = ab$.*

If R has an identity, then

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

Proposition 1.7 (Subring)**.** *Let S be a nonempty subset of a ring R such that:*

1. *S is closed under subtraction (if $a, b \in S$, then $a - b \in S$);*
2. *S is closed under multiplication (if $a, b \in S$, then $ab \in S$).*

Then S is a subring of R.

Definition 1.15. 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, the element u is called the (multiplicative) inverse of a and is denoted a^{-1}. Note that we already defined this in 1.8.

Definition 1.16. An element a in a ring 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 $ca = 0_R$.

Note that we already defined this in 1.9.

Theorem 1.13. *Cancellation is valid in any integral domain R: If $a \neq 0_R$ and $ab = ac$ in R, then $b = c$.*

Theorem 1.14. *Every field F is an integral domain.*

Theorem 1.15. *Every finite integral domain R is a field.*

Definition 1.17 (Isomorphism)**.** A ring R is isomorphic to a ring S (in symbols, $R \cong S$) if there is a function $f : R \to S$ such that all of the below hold:

1. f is injective;
2. f is surjective;
3. $f(a + b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$ for all $a, b \in R$.

In this case, the function f is called an **isomorphism**.

Definition 1.18 (Homomorphism)**.** Let R and S be rings. A function $f : R \to S$ is said to be a **homomorphism** if

$$f(a + b) = f(a) + f(b) \quad \text{and} \quad f(ab) = f(a)f(b) \quad \text{for all } a, b \in R.$$

Theorem 1.16. *Let $f : R \to S$ be a homomorphism of rings. Then*

1. *$f(0_R) = 0_S$.*
2. *$f(-a) = -f(a)$ for every $a \in R$.*
3. *$f(a - b) = f(a) - f(b)$ for all $a, b \in R$.*

If R is a ring with identity and f is surjective, then

4. *S is a ring with identity $f(1_R)$.*
5. *Whenever u is a unit in R, then $f(u)$ is a unit in S and $f(u)^{-1} = f(u^{-1})$.*

Corollary 1.3. *If $f : R \to S$ is a homomorphism of rings, then the image of f is a subring of S.*