Preliminaries and Notation

Sets and Intervals

- An interval with round brackets such as \((a, b)\) means all the numbers between \(a\) and \(b\) not including \(a\) and \(b\). We call this interval an open interval.

- An interval with square brackets such as \([a, b]\) means all the numbers between \(a\) and \(b\) including \(a\) and \(b\). We call this interval a closed interval.

- An interval with one square bracket and one closed bracket is called a clopen interval.

(i) \([a, b)\): means all numbers between \(a\) and \(b\) including \(a\) and not \(b\).
(ii) \((a, b]\) means all the numbers between \(a\) and \(b\) including \(b\) and not \(a\).

General Mathematics Notation

- The symbol \(\forall\) means 'for all'
- The symbol \(\exists\) means 'there exists'
- The symbol \(\in\) means 'in'. We use it to say things like the number number 1 is in the interval \((0, 2)\) and we write it mathematically as \(1 \in (0, 2)\).
- \(\mathbb{R}\) is the set of all real numbers, i.e. all numbers in the interval \((-\infty, \infty)\).
- \(*\) is used to denote a general operation (i.e. it could be multiplication \(\cdot\) or addition \(+\)). Make sure to look at the context. Here we will use \(\cdot\) when we mean multiplication and \(+\) when we mean addition. We will use \(*\) to denote a 'dummy' binary operation (meaning you can replace it with any operation that you want and the statement should hold true).

1.4 Binary Operations

**Definition 1.17** A Binary Operation on a nonempty set \(A\) is a mapping \(f\) from \(A \times A\) to \(A\). We use the following notation

\[ f : A \times A \rightarrow A \]

Examples of binary operations:

- Let \(f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}\) be defined as follows: \(\forall (x, y) \in \mathbb{R} \times \mathbb{R}\)

\[ f(x, y) = x + y \]

- Let \(f : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}\) be defined as follows: \(\forall (x, y) \in \mathbb{R} \times \mathbb{R}\)

\[ f(x, y) = x \cdot y \]
• Let \( f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \) be defined as follows: \( \forall (x, y) \in \mathbb{Z} \times \mathbb{Z} \)
\[
f(x, y) = x \cdot y + 1
\]

**Definition 1.18** We define the following:

- We say a binary operation is **commutative** if the following relation holds:
  \[ x \ast y = y \ast x \]

- We say a binary operation is **associative** if the following relation holds:
  \[ (x \ast y) \ast z = x \ast (y \ast z) \]

**Examples:**

(i) Let \( \ast \) be defined as follows: \( x \ast y = x + y - 1 \). Then, the operation \( \ast \) is commutative and associative since
  \[ x \ast y = x + y - 1 = y + x - 1 = y \ast x \] (commutativity)
  and
  \[ (x \ast y) \ast z = (x + y - 1) \ast z = (x + y - 1) + z - 1 = x - 1 + y + z - 1 = x + (y \ast z) - 1 = x \ast (y \ast z) \] (associativity)

**Definition 1.19** We say a set is **closed** under a binary operation \( \ast \) if
\[
\forall x, y \in B, \quad x \ast y \in B.
\]

For the following definitions let \( A \) be a nonempty set.

**Definition 1.20** We call \( e \in A \) an **identity element** with respect to the binary operation \( \ast \) if the following holds
\[
e \ast x = x \ast e = x
\]
for all \( x \in A \).

**Definition 1.21** Let \( e \) be the identity element of \( A \) with respect to \( \ast \). Let \( a, b \in A \).

(i) **right inverse**: \( b \) is a right inverse of \( a \) if \( a \ast b = e \).

(ii) **left inverse**: \( b \) is a left inverse of \( a \) if \( b \ast a = e \).

(iii) **inverse**: \( b \) is an inverse of \( a \) if \( a \ast b = b \ast a = e \). That is to say that \( b \) is both a right and left inverse of \( a \).

**Definition 1.22** A **permutation** is a one-to-one correspondence from a set to itself. For any nonempty set \( A \) we denote the set of all permutations on \( A \) as \( S(A) \). The set of all mappings from \( A \) to \( A \) is denoted \( M(A) \).

**Definition 1.15** The **composite** mapping \( f \circ g \) where \( f : A \to B \) and \( g : B \to A \) is the mapping from \( A \) to \( C \) defined by
\[
(f \circ g)(x) = f(g(x))
\]

Example: Let \( f : [0, 1] \to [1, 2] \) be defined by \( f(x) = x + 1 \) and let \( g : [1, 2] \to [1, 4] \) be defined by \( g(x) = x^2 \). Then,
\[
(g \circ f)(x) = g(f(x)) = (x + 1)^2
\]
and it maps from \([0, 1]\) to \([1, 4]\).

Note that composition of maps is associative.
\[
(f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x))) = f(g \circ h)(x) = f \circ (g \circ h)(x)
\]

Let us now define the identity map.
Consider Example 12 from the book. Let \( f \) be defined by

\[
(3) \quad \text{Contrapositive: For this proof method we prove that the negation of the statement holds. To negate a logical statement we do the following:}
\]

\[
\forall x \in A, \quad I_A(x) = x
\]

In addition, for any \( f \in A(A) \) (which means \( f : A \to A \) so that \( f(A) \in A \)) we have the following:

\[
(I_A \circ f)(x) = I_A(f(x)) = f(x)
\]

and

\[
f \circ I_A(x) = f(I_A(x)) = f(x).
\]

Consider Example 12 from the book. Let \( f : Z \to Z \) be defined by \( f(z) = 2z \) and let \( g : Z \to Z \) be defined by

\[
g(z) = \begin{cases} 
\frac{z}{2}, & z \in E \\
4, & z \in O
\end{cases}
\]

Now, since \( f(z) \) is always even, \( (g \circ f)(z) = z \) for all \( z \in Z \). Hence, \( g \circ f = I_Z \) which means that \( g \) is a left inverse of \( f \) (similarly, \( f \) is a right inverse for \( g \)). Now,

\[
f \circ g(z) = \begin{cases} 
z, & z \in E \\
8, & z \in O
\end{cases}
\]

Hence, \( f \circ g \neq I_Z \) so that \( g \) is not a right inverse for \( f \).

1.4.a Proofs

Now, let’s talk a little bit about constructing a proof. Say that you want to prove a statement like ’\( p \) implies \( q \)’ (mathematically we can denote this as \( p \Rightarrow q \)). This may also be stated as ’If \( p \), then \( q \)’. There are a few ways to do this.

1. **Direct proof:** You just assume \( p \) and then argue that \( q \) is true.

2. **Contradiction:** You assume \( p \) is true and that \( q \) is false. Then you argue until you get a contradiction. An example of this type of proof method is as follows: Statement: If \( a, b \in Z \), then \( a^2 - 4b \neq 2 \). We start the proof by supposing the \( q \) portion of the statement is false. Which is to say that if \( a, b \in Z \), then \( a^2 - 4b = 2 \). Thus,

\[
a^2 = 2 + 4b = 2(2b + 1) \Rightarrow a^2 \in E \Rightarrow a \in E
\]

Thus, we can write \( a = 2c \) for some number \( c \). Plug \( 2c \) in for \( a \) in the equation \( a^2 - 4b = 2 \) to get

\[
4c^2 - 4b = 2 \Rightarrow 4(c^2 - b) = 2 \Rightarrow 2(c^2 - b) = 1
\]

Thus, since \( c^2 - b \) is an integer, \( 2(c^2 - b) = 1 \) implies \( 1 \in E \). But, this is false. Hence we have proven the original statement: If \( a, b \in Z \), then \( a^2 - 4b \neq 2 \).

3. **Contrapositive:** For this proof method we prove that the negation of the statement holds. To negate a logical statement we do the following:

\[
(p \Rightarrow q) = (q \Rightarrow p)
\]

So, let us try to prove the following claim: For \( a, b \in Z \), \( a + b \geq 15 \) implies \( a \geq 8 \) or \( b \geq 8 \). Here

\[
a + b \geq 15 \quad \text{is our } p \text{ statement}
\]

and

\[
a \geq 8 \text{ or } b \geq 8 \quad \text{is our } q \text{ statement}
\]

So to form the negation we want to do

\[
(a + b \geq 15 \Rightarrow a \geq 8 \vee b \geq 8) = (a < 8 \wedge b < 8 \Rightarrow a + b < 15)
\]

So, we now try to prove the following statement directly: \( a < 8 \wedge b < 8 \Rightarrow a + b < 15 \).
Proof. Assume that \( a < 8 \) and \( b < 8 \) for \( a, b \in \mathbb{Z} \). Since \( a, b \in \mathbb{Z} \)
\[
a < 8 \quad \text{and} \quad b < 8 \quad \Rightarrow \quad a \leq 7 \quad \text{and} \quad b \leq 7
\]
We can now add the two inequalities \( a \leq 7 \) and \( b \leq 7 \) to get
\[
a + b \leq 14
\]
This implies that \( a + b < 15 \). Hence we have proven that \( a < 8 \land b < 8 \Rightarrow a + b < 15 \) which is equivalent to our original statement.

Now, let’s talk about proving an ‘if and only if’ statement (note that we can abbreviate ‘if and only if’ as ‘iff’. First, when we make the statement ‘\( p \iff q \)’ we mean both ‘if \( p \), then \( q \)’ and ‘if \( q \), then \( p \)’ must hold. So, as is stated in the book, to prove the statement ‘\( p \iff q \)’ we must prove the following two statements:

1. (\( p \iff q \)): This is the ‘if’ part of the proof and it is often referred to as the sufficient condition. Here, we assume \( q \) is true and we prove that \( p \) must then be true.
2. (\( p \iff q \)): This is the ‘only if’ part of the proof and it is often referred to as the necessary condition. Here, we assume \( p \) is true and then we prove that \( q \) must hold.

1.6. Equivalence Relations

Definition 1.35 (Relation) A binary relation on a nonempty set \( A \) is a set \( R \) of pairs \((x, y)\) for \( x \in A \) and \( y \in A \). Note that \( R \subseteq A \times A \). If two elements \( x \) and \( y \) are related, i.e. \((x, y) \in R\), then we write \( xRy \).

The symbol \( \sim \) is often also used to denote a relation. Using this notation we write \( x \sim y \). We will use the \( \sim \) notation to denote the actual relation (so when we want to say \( x \) is related to \( y \), we write \( x \sim y \)) and we will use \( R \) to denote the set of ordered pairs. Namely,
\[
R := \{(x, y) | x \in A, y \in A \text{ and } x \sim y\}.
\]

To clarify this definition, let us take an example.

Example 1
Let \( A \) be the set of integers between 1 and 5. Consider the relation defined by \( a \) is related to \( b \) if \( a \mod b = 2 \).

Then, we may construct the set \( R \). In the set \( A \), we have the following:

- \( 1 \mod 2 = 1 \), \( 1 \mod 3 = 1 \), \( 1 \mod 4 = 1 \), and \( 1 \mod 5 = 1 \).
- \( 2 \mod 1 = 0 \), \( 2 \mod 3 = 2 \), \( 2 \mod 4 = 2 \), and \( 2 \mod 5 = 2 \).
- \( 3 \mod 1 = 0 \), \( 3 \mod 2 = 1 \), \( 3 \mod 4 = 3 \), and \( 3 \mod 5 = 3 \).
- \( 4 \mod 1 = 0 \), \( 4 \mod 2 = 0 \), \( 4 \mod 3 = 1 \), \( 4 \mod 5 = 4 \).
- \( 5 \mod 1 = 0 \), \( 5 \mod 2 = 1 \), \( 5 \mod 3 = 2 \), \( 5 \mod 4 = 1 \).

Hence,
\[
R = \{(x, y) | x \in A, y \in A \text{ and } x \sim y\} = \{(2, 3), (2, 4), (2, 5), (5, 3)\}.
\]

Definition 1.36 (Equivalence Relation) A relation \( \sim \) on \( A \) is an equivalence relation on \( A \) if the following are satisfied for all \( x, y, z \in A \):

(i) \( x \sim x \), \( \forall x \in A \). (reflexive)
(ii) \( x \sim y \Rightarrow y \sim x \). (symmetric)
(iii) \( x \sim y \text{ and } y \sim z \Rightarrow x \sim z \). (transitive)

Note that the relation in example (1) is not an equivalence relation since \( 2 \sim 3 \) but \( 3 \not\sim 2 \), i.e. the relation is not reflexive, \( \sim \) means ‘not related to’.
Example 2
Consider the set of all integers, \( \mathbb{Z} \). We define \( \sim \) to be 'congruence modulo 4'. This is to say that a number \( x \) is congruent modulo 4 iff \( x - y \) is a multiple of 4, i.e. \( (x - y) \mod 4 = 0 \). We write \( x \equiv y \pmod{4} \). Note that for \( (x - y) \mod 4 \) to be zero this means that 4 divides \( x - y \) some number of times (let us say \( k \) times) with zero remainder. We can write this as \( 4|(x - y) = k \) remainder 0. Hence, \( (x - y) \) is a multiple of 4. Specifically, \( (x - y) = 4k \).

We can show that the relation \( x \equiv y \pmod{4} \) in the set of integers \( \mathbb{Z} \) is an equivalence relation by checking the three properties in the definition above. Let \( x, y \) and \( z \) be arbitrary integers in \( \mathbb{Z} \).

- (reflexive): We want to show that \( x \equiv x \pmod{4} \). Equivalently, we must show that \( x - x = 4k \) for some \( k \).
  
  
  \[
  x - x = 0 = 4 \cdot 0
  \]

  Hence, \( x - x = 4k \) for \( k = 0 \) which implies that \( x \equiv x \pmod{4} \).

- (symmetric): Assume that \( x \equiv y \pmod{4} \). We want to show that \( y \equiv x \pmod{4} \).

  \[
  x \equiv y \pmod{4} \implies (x - y) = 4k \text{ for some } k \implies (y - x) = 4(-k) \implies y \equiv x \pmod{4}.
  \]

- (transitive): Assume that \( x \equiv y \pmod{4} \) and \( y \equiv z \pmod{4} \). We want to show \( x \equiv z \pmod{4} \).

  \[
  x \equiv y \pmod{4} \implies (x - y) = 4k \text{ for some } k
  \]

  \[
  y \equiv z \pmod{4} \implies (y - z) = 4j \text{ for some } j
  \]

  So, we have

  \[
  (x - y) - (y - z) = 4k - 4j \implies x - z = 4(k - j)
  \]

  Hence, \( x \equiv z \pmod{4} \). Since \( x \equiv y \pmod{4} \) in the set of integers \( \mathbb{Z} \) satisfies the three properties of an equivalence relation, it is an equivalence relation.

One nice application of equivalence relations is to define quotient sets. We may define an equivalence class with respect to an element in a set \( A \). Again, let \( \sim \) be an equivalence relation. Then, for an element \( x \in A \), we define the equivalence class of \( x \) as the following:

\[
[x] = \{ y \in A | x \sim y \}.
\]

In the context of the above example, for a particular integer \( a \in \mathbb{Z} \)

\[
[a] = \{ x \in \mathbb{Z} | a \equiv x \pmod{4} \}
\]

We call the quotient set the set of all equivalence classes. We denote it by \( A/\sim \). As an example, consider the 'congruence modulo 2' relation on the integers. That is \( x \equiv y \pmod{2} \) or \( (x - y) = 2k \) for some integer \( k \). Then, the equivalence class of any even number (say 2) is the set of all even numbers. And, the equivalence class of any odd number (say 3) is the set of all odd numbers. So, \( \mathbb{Z}/\sim \) where \( \sim \) is the 'congruence modulo 2' equivalence relation is the set

\[
\mathbb{Z}/\sim = \{ [2], [3] \}
\]

where \([2]\) is the equivalence class of all even numbers and \([3]\) is the equivalence class of all odd numbers.

2. Integers

2.1 Postulates for the Integers

(1) Addition postulates: Note that \( (\mathbb{Z}, +) \) forms an abelian group. Hence, the addition postulates are just the properties of an abelian group.

(a) Closure: \( \mathbb{Z} \) is closed under +.

(b) Associativity: addition is associative.

(c) Identity element: 0 is the identity element for \( (\mathbb{Z}, +) \).
(d) Inverse: For \( a \in \mathbb{Z} \), \(-a\) is the additive inverse since \( a + (-a) = 0 \).
(e) Commutative: \( a + b = b + a \).

(2) **Multiplicative postulates:** Note that \((\mathbb{Z}, \cdot)\) forms a commutative **monoid.** A commutative monoid has all the properties of an abelian group except for the inverse.

(a) Closure: \( \mathbb{Z} \) is closed under \( \cdot \).
(b) Associativity: multiplication is associative.
(c) \( 1 \) is the identity element: \( z \cdot 1 = z \).
(d) Multiplication is commutative.

(3) **Distribution Law:** Multiplication distributes over addition.

(i) (left distributive law): \( x \cdot (y + z) = x \cdot y + x \cdot z \)

(4) **Positive Integers:** \( \mathbb{Z}^+ \subset \mathbb{Z} \) where \( \mathbb{Z}^+ \) denotes the set of positive integers (it does not contain 0). \( \mathbb{Z}^+ \) has the following properties:

(a) \( \mathbb{Z}^+ \) is closed under addition.
(b) \( \mathbb{Z}^+ \) is closed under multiplication.
(c) **Law of Trichotomy:** For \( x \in \mathbb{Z} \) one and only one of the following is true:
   (i) \( x \in \mathbb{Z}^+ \)
   (ii) \( x = 0 \)
   (iii) \( -x \in \mathbb{Z}^+ \).

(5) **Induction Postulate:** If \( S \subset \mathbb{Z}^+ \) such that \( 1 \in S \) and \( x \in S \Rightarrow x + 1 \in S \), then \( S = \mathbb{Z}^+ \).

**Note:** Since \( \mathbb{Z} \) satisfies postulates (1)-(3), \( \mathbb{Z} \) forms a **commutative ring.** We may prove that the integers also satisfy something called the right distributive law.

**Theorem 2.1** The equality

\[(y + z) \cdot x = y \cdot x + z \cdot x\]

(right distributive law)

holds for all \( x, y, z \in \mathbb{Z} \).

**Proof.** Let \( x, y, z \) be arbitrary elements in \( \mathbb{Z} \). Then, since \( \mathbb{Z} \) is closed under addition, \( y + z \in \mathbb{Z} \). We also have that multiplication is commutative so that

\[(y + z) \cdot x = x \cdot (y + z)\]

Since \((\mathbb{Z}, +, \cdot)\) satisfies the left distributive law, we have

\[(y + z) \cdot x = x \cdot (y + z) = x \cdot y + x \cdot z = y \cdot x + z \cdot x\]

where the last equality holds because multiplication is commutative. Hence, we have shown that

\[(y + z) \cdot x = y \cdot x + z \cdot x.\]

Now, we state a lemma such that will be used to prove a theorem.

**Lemma 2.3 (Cancellation Law for Addition)**
If \( a, b, c \in \mathbb{Z} \) and \( a + b = a + c \), then \( b = c \).
Proof. We prove this lemma directly. Let $a, b, c$ be integers and suppose that $a + b = a + c$. Since $(\mathbb{Z}, +, \cdot)$ is a commutative ring, it contains the additive inverse of every element in $\mathbb{Z}$. Hence, $-a \in \mathbb{Z}$. We may use the other postulates of the integers to get the following implications:

\[
\begin{align*}
    a + b &= a + c \\
    \Rightarrow (-a) + (a + b) &= (-a) + (a + c) \\
    \Rightarrow (-a + a) + b &= (-a + a) + c \\
    \Rightarrow 0 + b &= 0 + c \\
    \Rightarrow b &= c
\end{align*}
\] (by postulate 1-b)

(by postulate 1-d)

(by postulate 1-c)

Now, we state the theorem we are interested in proving.

**Theorem 2.2 (Additive Inverse of a Product)** For arbitrary $x, y \in \mathbb{Z}$,

\[( -x ) \cdot y = -(x \cdot y) \]

Proof.

\[
\begin{align*}
    x \cdot y + (-x) \cdot y &= (x + (-x)) \cdot y \\
    &= 0 \cdot y \\
    &= 0 \cdot y + 0 \\
    &= 0 \cdot y + 0 \cdot y + (-0 \cdot y) \\
    &= 0 + 0 \cdot y + (-0 \cdot y) \\
    &= 0 \cdot y + (-0 \cdot y) \\
    &= 0
\end{align*}
\] (by theorem 2.1)

(by postulate 1-d)

(by postulate 1-c)

(by postulate 1-d)

Hence, $x \cdot y + (-x) \cdot y = 0$. So, we know that $x \cdot y + (-x) \cdot y = 0$ by postulate 1-d. And, we have shown that $x \cdot y + (-x) \cdot y = 0$. Thus, $x \cdot y + (-x) \cdot y = x \cdot y + (-x) \cdot y$. So, by the lemma, $(-x) \cdot y = -(x \cdot y)$. □

**Definition 2.4 (Order Relation $<$)** For $x, y \in \mathbb{Z}$

\[x < y \iff y - x \in \mathbb{Z}^+\]

where $y - x = y + (-x)$.

Since we have an order relation $<$ meaning 'less than', we can state the well ordering axiom.

**Well ordering axiom:** Every nonempty subset of the set of nonnegative integers contains a smallest element.

The well ordering axiom does not hold on the set of all integers $\mathbb{Z}$, i.e. there is no smallest negative integer.

We may now define 'powers' of elements in $\mathbb{Z}$.

**Definition (powers)** Let $x \in \mathbb{Z}$. $x^n := x \cdot \cdots \cdot x$. Note that this is well defined since we take $x^1 = x$ and inductively we define $x^{k+1} = x^k \cdot x$.

**Definition (multiples)** Let $x \in \mathbb{Z}$. Then we define $1x = x$ and $(k + 1)x = kx + x$. 

---

7
2.2 Mathematical Induction

Often we want to prove a statement $P_n$ for every $n \in \mathbb{Z}^+$. Logically the way we can think about induction is that if $P_1$ is true and if $P_k$ is true implies that $P_{k+1}$ is true for arbitrary $k \in \mathbb{Z}^+$, $P_n$ must be true for all $n \in \mathbb{Z}^+$.

**Proof by Mathematical Induction** We want to prove $P_n$ is true for all $n \in \mathbb{Z}^+$. We take the following three steps:

1. Verify the statement for $n = 1$.
2. (inductive assumption or hypothesis): Assume the statement holds for $n = k$.
3. Under the assumption in 2., prove the statement hold for $n = k + 1$.

Let us take an example to get the gist of proof by induction.

**Example 3**

Prove

\[ 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \]

**Proof.** Let’s go through the three steps above.

(a) Check for $n = 1$:

\[ \frac{1(1+1)}{2} = \frac{2}{2} = 1 \]

(b) Assume $n = k$ holds:

\[ 1 + 2 + \cdots + k = \frac{k(k+1)}{2} \quad \text{(Induction Hypothesis)} \]

(c) Show $n = k + 1$ holds: So, we must show that

\[ 1 + 2 + \cdots + (k+1) = \frac{(k+1)(k+1+1)}{2} = \frac{(k+1)(k+2)}{2} \]

\[ 1 + 2 + \cdots + k + (k + 1) = \frac{k(k + 1)}{2} + k + 1 = \frac{2(k + 1)}{2} = \frac{k(k + 1) + 2(k + 1)}{2} = \frac{(k + 1)(k + 2)}{2} \]

Since we showed the three steps,

\[ 1 + 2 + \cdots + n = \frac{n(n+1)}{2} \]

holds for all $n \in \mathbb{Z}^+$.

**Theorem 2.6 (Least Positive Integer)** The integer 1 is the least positive integer, i.e. $1 \leq n$ for all $n \in \mathbb{Z}^+$.

**Proof.** Let $S$ be the set of all positive integers greater than or equal to 1, i.e.

\[ S := \{ n \in \mathbb{Z} | 1 \leq n \} \]

Now, we want to use induction to show that $S$ contains all the positive integers. If we can show this, then we have shown that all positive integers satisfy the inequality $1 \leq n$ and hence 1 is the least positive integer.
1. Check for \( n = 1 \): \( 1 \in S \) since \( 1 \leq 1 \).

2. Assume for \( n = k \): assume that \( 1 \leq k \) holds.

3. Show for \( n = k + 1 \) that \( 1 \leq k + 1 \): By definition 2.4, we know that \( x < y \Leftrightarrow y - x \in \mathbb{Z}^+ \). So,
   \[
   1 - 0 = 1 + (-0) = 1 \in \mathbb{Z}^+
   \]
   Hence, \( 0 < 1 \). Now, \( 0 < 1 \) implies that \( k < k + 1 \) since
   \[
   k + 1 - (k + 0) = k + 1 - k = 1 \in \mathbb{Z}^+
   \]
   so again by definition 2.4 \( k < k + 1 \). By the induction hypothesis in 2. above we have \( 1 \leq k \). We just showed that \( k < k + 1 \). Hence,
   \[
   1 \leq k < k + 1 \implies 1 \leq k + 1
   \]
   Thus, \( k \in S \) implies \( k + 1 \in S \).

Using induction we have shown that all the positive integers are contained in \( S \). Therefore, 1 is the least positive integer. \( \square \)

2.3 Divisibility

**Definition 2.8 (Divisor, Multiple)** Let \( a, b \in \mathbb{Z} \). We say \( a \) divides \( b \) if there is an integer \( c \) such that
   \[
   b = ac
   \]
   We often denote ‘\( a \) divides \( b \)’ as \( a \mid b \). We may also say that \( b \) is a multiple of \( a \), \( a \) is a factor of \( b \), or that \( a \) is a divisor of \( b \).

**Theorem 2.10 (Division Algorithm)** Let \( a, b \in \mathbb{Z} \) such that \( b > 0 \). Then, \( \exists \) unique integers \( q \) and \( r \) such that
   \[
   a = bq + r \quad \text{with} \quad 0 \leq r < b
   \]
   We call \( q \) the quotient and we call \( r \) the remainder. Another form of the theorem conclusion is
   \[
   \frac{a}{b} = q + \frac{r}{b}
   \]

**Proof.** We prove this theorem in two parts. We first prove existence and then we prove uniqueness.

- (existence): We must show that there exists \( q \) and \( r \) such that \( a = bq + r \) with \( 0 \leq r < b \). Consider \( a, b \in \mathbb{Z} \) such that \( b > 0 \). Let \( S \) be the set defined by
  \[
  S := \{ x \in \mathbb{Z} | x = a - bn, n \in \mathbb{Z} \}
  \]
  Let \( S' := \{ x \in S | x \geq 0 \} \). The set \( S' \neq 0 \) since if \( a = 0 \), then \( b \in S' \) with \( n = -1 \) and if \( a \neq 0 \), then \( a + 2b|a| \in S' \) with \( n = -2|a| \). Now, if \( 0 \in S' \), we have \( 0 = a - bq \) for some \( q \). Hence, \( a = bq + 0 \) so that \( r = 0 \). If \( 0 \notin S' \), then \( S' \) contains a least element \( r \) by the well ordering axiom. Since \( r \in S' \) we can write it as \( r = a - bq \) for some \( q \in \mathbb{Z} \). Hence, \( a = bq + r \) with \( r \geq 0 \). Now,
  \[
  r - b = a - bq - b = a - b(q + 1)
  \]
  so that \( r - b \in S \). Since \( r \) is the least element in \( S' \) and \( b > 0 \) so that \( r - b < r \), we must have that \( r - b < 0 \) because \( S' \) contains all nonnegative integers in \( S \). Hence, \( r < b \). Thus, we have
  \[
  a = bq + r \quad \text{with} \quad 0 \leq r < b
  \]
  And we are done.

- (uniqueness): We show uniqueness by contradiction. We assume that \( q \) and \( r \) are not unique. That is to says there exists \( q_1, q_2, r_1, r_2 \) such that for \( a, b \in \mathbb{Z} \)
  \[
  a = bq_1 + r_1 \quad \text{and} \quad a = bq_2 + r_2
  \]
where \(0 \leq r_1 < b\) and \(0 \leq r_2 < b\). Without loss of generality we may assume \(r_1 < r_2\) so that we have
\[
0 \leq r_2 - r_1 \leq r_2 < b.
\]
We also have
\[
0 \leq r_2 - r_1 = (a - bq_2) - (a - bq_1) = b(q_1 - q_2)
\]
so that along with \(0 \leq r_2 - r_1 \leq r_2 < b\) we have
\[
0 \leq r_2 - r_1 = b(q_1 - q_2) < b
\]
But, the last inequality only holds when \(q_1 - q_2 \leq 0\) since \(b > 0\). Thus, \(0 \leq b(q_1 - q_2) \leq 0\) which implies that \(q_1 - q_2 = 0\). Further, this implies that \(r_1 = r_2\). So, \(q\) and \(r\) are in fact unique.

\[\square\]

### 2.4 Prime Factors and Greatest Common Divisor

**Definition 2.11 (Greatest Common Divisor or gcd)** An integer \(d\) is a **greatest common divisor** (gcd) of \(a\) and \(b\) if the following hold:

1. \(d \in \mathbb{Z}^+\)
2. \(d | a\) and \(d | b\) (i.e. \(a = dq_1\) and \(b = dq_2\))
3. \(c | a\) and \(c | b\) imply \(c | d\). (\(a = cq_3\) and \(b = cq_4\), then \(d = cq_5\)).

**Theorem 2.12 (gcd)** Let \(a, b \in \mathbb{Z}\) and let at least one of them be nonzero. Then, there exists a gcd \(d\) of \(a\) and \(b\). Moreover, we can write \(d\) as
\[
d = am + bn
\]
for \(m, n \in \mathbb{Z}\) and \(d\) is the smallest positive integer that can be written in this form.

**Proof.** If \(b = 0\) so that \(a \neq 0\) or equivalently \(|a| > 0\). Then, \(d = |a|\) is a gcd for \(a\) and \(b\) since \(d = |a| \in \mathbb{Z}^+\), \(a = |a| \cdot (-1)\) if \(a < 0\) or \(a = |a| \cdot 1\) if \(a > 0\) so that \(d|a\). Similarly, \(b = |a| \cdot 0\) so that \(d|b\). Also, \(c|a\) and \(c|b\) imply \(c|d\) since \(a = cq_1\) and \(b = cq_2\) imply \(d = |a| = |cq_1|\) which implies that \(c|d\). Thus, either \(d = a \cdot 1 + b \cdot 0\) or \(d = a \cdot (-1) + b \cdot 0\).

The case when \(a = 0\) so that \(b \neq 0\) is symmetric to the case described above.

Now, we consider the case when \(a \neq 0\) and \(b \neq 0\). Let \(S\) be defined as follows:
\[
S := \{ z \in \mathbb{Z} | z = ax + by \text{ for some } x, y \in \mathbb{Z} \}
\]
and define
\[
S^+ := \{ z \in S | z > 0 \}
\]
The set \(S\) contains \(b = a \cdot 0 + b \cdot 1\) and \(-b = a \cdot 0 + b \cdot (-1)\) so \(S^+ \neq \emptyset\). By the well ordering axiom, \(S^+\) has a least element \(d\) and since \(d \in S^+\), \(d\) is positive and we write \(d = am + bn\). Now, what is left to show is that \(d\) is a gcd of \(a\) and \(b\). First, we already have that \(d \in \mathbb{Z}^+\). By theorem 2.10 (division algorithm), since \(d > 0\) and \(a, d \in \mathbb{Z}\), there exists integers \(q\) and \(r\) such that
\[
a = dq + r \quad \text{with} \quad 0 \leq r < d
\]
Hence,
\[
r = a - dq = a - (am + bn)q = a(1 - mq) + b(-mq)
\]
which shows that \(r \in S\). Since \(0 \leq r < d\) and since \(d\) is the least element in \(S^+\), it must be the case that \(r = 0\). Hence,
\[
0 = a - dq \Rightarrow a = dq \Rightarrow d|a
\]
We may make a similar argument to show that \( d \mid b \). Now, we check that last point. That is we must show that if \( c \mid a \) and \( c \mid b \) then \( c \mid d \).

\[
c \mid a \Rightarrow a = ck \quad \text{and} \quad c \mid b \Rightarrow b = cj
\]

Thus,

\[
d = am + bn = ckm + cjn = c(km + jn)
\]

so that \( c \mid d \). We have shown that \( d \) satisfies 1-3 of definition 2.11 so that we may conclude that \( d \) is a gcd of \( a \) and \( b \).

\[\square\]

### 2.7 Introduction to Coding Theory

#### 3. Groups

Now, we may define a group.

**Definition (Group)** A group \((G,\ast)\) is a set \(G\) together with a binary operation \(\ast\) such that the following hold:

(i) **Closure**: \(\forall a, b \in G \ a \ast b \in G\).

(ii) **Associativity**: \(\forall a, b, c \in G\) \((a \ast b) \ast c = a \ast (b \ast c)\).

(iii) **Identity element**: \(\exists e \in G\) such that \(\forall a \in G\), \(a \ast e = e \ast a = a\).

(iv) **Inverse Element**: For each \(a \in G\), \(\exists a^{-1} \in G\) such that \(a \ast a^{-1} = a^{-1} \ast a = e\).

We sometimes denote the group as \((G, \ast)\) or \(G_{\ast}\).

**Definition (Commutative Group or Abelian Group)** A commutative (abelian) group is a set \(G\) with operation \(\ast\) such that \((G, \ast)\) is a group (see definition above, i.e. all the properties above hold) and the following holds:

\[
\forall a, b \in G, \quad a \ast b = b \ast a.
\]

Some examples of groups:

(i) The set of all non-zero rational numbers (denoted as \(\mathbb{Q}\backslash\{0\}\) which means the rational numbers \(\mathbb{Q}\) with the zero element removed) is an abelian group under the operation \(\cdot\) (multiplication). We denote this group as \((\mathbb{Q}\backslash\{0\}, \cdot)\).

- \(1\) is the identity element: \(r \cdot 1 = r\).
- \(r^{-1}\) is the inverse of \(r \in \mathbb{Q}\backslash\{0\}\).

(ii) \(\mathbb{Q}\) under addition forms an abelian group.

- (commutativity): \(a + b = b + a\).
- (inverse): \(a \in \mathbb{Q}\) \(-a \in \mathbb{Q}\)
- (identity): \(a + 0 = a\).
- (closure): \(a + b \in \mathbb{Q}\).
- (associativity): \((a + b) + c \in \mathbb{Q}\) and \(a + (b + c) \in \mathbb{Q}\).

(iii) \(\mathbb{Z}\) is not a group under multiplication. \(2 \in \mathbb{Z}\) but \(2^{-1} = \frac{1}{2} \notin \mathbb{Z}\).

(iv) (Cyclic group): A cyclic group is a group whose elements are generated by a single element, i.e. the elements are powers of a single element. Consider a cyclic group \((G, \ast)\). \(a\) is the generator for this group if for each element \(g \in G\) we can write \(g = a^k\) for some \(k \in \mathbb{Z}\). For notation, we mean the following \(a^{-1} = a^{-1} \cdot a^{-1} \cdot a^{-1}\). \(a^3 = a \cdot a \cdot a\). As an example, consider the multiplicative group
$\mathbb{Z}_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and let the operation be multiplication, $\cdot$. Then, we claim that 2 is a generator for this group.

$2^1 \pmod{11} = 2$, $2^2 \pmod{11} = 4( \mod{11} ) = 4$, $2^3 \pmod{11} = 8( \mod{11} ) = 8$,

$2^4 = 16( \mod{11} ) = 5$, $2^5 \pmod{11} = 32( \mod{11} ) = 10$, $2^6 \pmod{11} = 64( \mod{11} ) = 9$,

$2^7 \pmod{11} = 128( \mod{11} ) = 7$, $2^8 \pmod{11} = 256( \mod{11} ) = 3$,

$2^9 \pmod{11} = 512( \mod{11} ) = 6$, $2^{10} \pmod{11} = 1024( \mod{11} ) = 1$