Algebra I

Dhyan Laad
2024ADPS0875G

1 Preliminaries

1.1 The Natural Numbers

We start by covering a few basic and useful properties of the natural numbers, which in this text does not include 0. Stated below is an axiom reffered to as the *well ordering principle* (WOP).

Every nonempty subset of the natural numbers has a least element.

Note that the WOP holds trivially for any finite extension to $\mathbb{N}$. Now from it, it is possible to prove the *principle of mathematical induction* (PMI).

Theorem 1.1 (Principle of Mathematical Induction). *For a set $S \subseteq \mathbb{N}$, if*

(a) $1 \in S$, *and*

(b) *for every* $k \in \mathbb{N}$, $k \in S \Rightarrow k + 1 \in S$,

then $S = \mathbb{N}$.

Proof. Assume for contradiction that $S \neq \mathbb{N}$. This implies that there must exist natural numbers not in S. Define

$$C = \mathbb{N} \setminus S.$$

By construction, C is nonempty, which means by the WOP, C must have a least element m.

Since $1 \in S$ and $m \in C$, $m \neq 1$, which means that $m > 1$. This means that $m - 1$ is a natural number, and since m is the smallest element of C, $m - 1$ must be in S. By (b), since $m - 1 \in S$, it must be the case that $m \in S$ ($\Rightarrow\!\Leftarrow$). Since m cannot be in both S and C, the assumption that $S \neq \mathbb{N}$ must be false. □

This theorem is sometimes referred to as *weak induction*. Ironically, *strong induction* follows from the standard PMI.

Theorem 1.2 (Principle of Strong Induction). *For a set $S \subseteq \mathbb{N}$, if*

(a) $1 \in S$, *and*

(b) *for every* $k \in \mathbb{N}$, $\{1, 2, \ldots, k\} \subseteq S \Rightarrow k + 1 \in S$, *then* $S = \mathbb{N}$.

It is also possible to axiomatize the PMI and derive the WOP from it. The proof is done by proving the contrapositive statement: if a set S has no least element, then S is empty.

Definition 1.3. Let $a, b \in \mathbb{Z}$. We say that a *divides* b if there exists $c \in \mathbb{Z}$ such that

$$b = ac$$

and symbolically write $a \mid b$.

Now for another fundamental result in elementary number theory.

Theorem 1.4 (Division Lemma). *For any $a \in \mathbb{Z}$ and $b \in \mathbb{N}$, there exist unique integers q and r such that*

$$a = bq + r$$

where $0 \leq r < b$.

Proof. Define the set

$$S = \{a - xb : x \in \mathbb{Z} \text{ and } a - xb \geq 0\}.$$

Set $x = -|a|$. Then,

$$a - xb = a - (-|a|)b = a + |a|b \geq a + |a| \geq 0.$$

Therefore, S is nonempty. Since S is also a subset of $\mathbb{N}$, by an extension of the WOP to admit 0, S has a least element $r \geq 0$. Thus,

$$r = a - qb$$

for some $q \in \mathbb{Z}$. We now assert that $r < b$.

Assume for contradiction that $r \geq b$. Then,

$$r - b = (a - qb) - b = a - (q + 1)b \geq 0.$$

This means that $r - b$ is an element of S ($\Rightarrow\!\Leftarrow$), which contradicts the fact that r is the least element of S. Therefore, $r < b$.

We also prove the uniqueness of q and r by contradiction. Assume that there exist integers q' and r' different from q and r respectively such that

$$a = qb + r = q'b + r'$$

with $0 \leq r, r' < b$. Rearranging the above expression, we have

$$(q - q')b = r' - r \Rightarrow |q - q'||b| = |r' - r|.$$

Now,

$$q \neq q' \Rightarrow |q - q'| \geq 1 \Rightarrow |r' - r| \geq |b| \qquad (\Rightarrow\!\Leftarrow)$$

which contradicts our assumed bounds on r and r'. As such, q and r must be unique. $\square$

Definition 1.5. The *greatest common divisor* (gcd) of two nonzero integers a and b is the unique positive integer d such that

(a) $d \mid a$ and $d \mid b$, and

(b) if $c \mid a$ and $c \mid b$ for some $c \in \mathbb{Z}$, then $c \mid d$.

Symbolically, $d = (a, b)$.

Equivalently, the gcd of two integers a and b is the largest integer that divides them. The *Euclidean algorithm* (described below) employs the division lemma to find the gcd of two arbitrary integers, along with a proof of termination.

Theorem 1.6 (Euclidean Algorithm). *Let $a \in \mathbb{Z}$ and $b \in \mathbb{N}$. There exist integers q_i and r_i for $i \in 1 : k$ such that*

$$
\begin{aligned}
a &= bq_1 + r_1, && 0 \le r_1 < b, \\
b &= r_1 q_2 + r_2, && 0 \le r_2 < r_1, \\
&\vdots && \vdots \\
r_{k-2} &= r_{k-1} q_k + r_k, && 0 \le r_k < r_{k-1}, \\
r_{k-1} &= r_k q_{k+1}.
\end{aligned}
$$

Then $(a, b) = r_k$.

Step 1. Divide a by b to obtain

$$a = bq_1 + r_1, \quad 0 \le r_1 < b.$$

Step 2. If $r_1 = 0$, then $(a, b) = b$. Otherwise, divide b by r_1 to get

$$b = r_1 q_2 + r_2, \quad 0 \le r_2 < r_1.$$

Step 3. Continue dividing the previous divisor by the remainder until a remainder of 0 is obtained.

Conclusion. The last nonzero remainder r_k is (a, b).

Proof. All of the remainders are nonnegative integers:

$$b > r_1 > r_2 > \cdots > r_{k-1} > r_k > 0.$$

By the WOP, $\mathbb{N}$ cannot contain an infinite strictly decreasing sequence, which means the algorithm must terminate after a finite number of steps, with the last remainder being 0. □

Now for a final result on the properties of natural numbers

Theorem 1.7 (Bézout's Lemma). *Let a and b be nonzero integers. Then, there exist integers x and y such that*

$$ax + by = (a, b).$$

Furthermore, (a, b) is the smallest positive integer that can be written in this form.

Proof. Define the set

$$S = \{ax + by : x, y \in \mathbb{Z} \text{ and } ax + by > 0\}.$$

If $a > 0$, then $a \cdot 1 + b \cdot 0 = a \in S$ and if $a < 0$, then $a \cdot (-1) + b \cdot 0 = -a \in S$. If $a = 0$, then b can be similarly picked to match the sign of y for the linear combination to be positive, which means the set is nonempty.

Since the set is nonempty, by the WOP let d be the least element in S. As such, there exist integers x_0 and y_0 such that

$$d = ax_0 + by_0. \tag{$*$}$$

Now, by the division lemma, we know that there exist integers q and r such that

$$a = dq + r \tag{$**$}$$

where $0 \leq r < d$. From $(*)$ and $(**)$, we have

$$r = a - dq = a - (ax_0 + by_0)q \Rightarrow r = a(1 - x_0 q) + b(-y_0 q).$$

Now note that r must be 0, since if it were not, then it would be an element of S, which is not possible since $r < d$, which contradicts the fact that d is the least element of S. Since $r = 0$, it follows that $a = dq \Rightarrow d \mid a$, and by the same flow of thought, $d \mid b$.

Let c be an arbitrary divisor of a and b, i.e. there exist integers k and ℓ such that $a = ck$ and $b = c\ell$. To show that $d = (a, b)$, c must also divide d.

$$d = ax_0 + by_0 = (ck)x_0 + (c\ell)y_0 = c(kx_0 + \ell y_0) \Rightarrow c \mid d.$$

□

1.2 Relations

Definition 1.8. Let X be a set. A relation R on X is a subset of the Cartesian product

$$X \times X = \{(x, y) : x, y \in X\}.$$

If $(x, y) \in R$, we say that x *is related to* y *by* R. Symbolically

$$xRy,$$

and if there is no ambiguity in the relation, then it is common to write $x \sim y$.

We now discuss a few proprties that a relation may possess.

Definition 1.9. Let X be a set and $\sim$ be a relation on X. The relation is

(a) *reflexive* if $x \sim x$ for all $x \in X$,

(b) *symmetric* if $x \sim y \Rightarrow y \sim x$ for all $x, y \in X$, and

(c) *transitive* if $x \sim y$ and $y \sim z$ imply that $x \sim z$ for all $x, y, z \in X$.

Definition 1.10. A relation that is reflexive, symmetric, and transitive is said to be an *equivalence relation.*

Now consider a fundamental equivalence relation.

Example 1.11. Let $n \in \mathbb{N}$ with $n \geq 2$. Define a relation $\sim$ on $\mathbb{Z}$ by

$$x \sim y \Leftrightarrow x \text{ and } y \text{ give the same remainder when divided by } n,$$

or symbolically

$$x \sim y \Leftrightarrow n \mid (x - y).$$

Reflexivity. For any $x \in \mathbb{Z}$, we have that $x - x = 0$, and since $n \mid 0$, it follows that $x \sim x$.

Symmetry. If $x \sim y$, then $n \mid (x-y) \Rightarrow x-y = nk$ for some $k \in \mathbb{Z}$. Now, $y-x = n(-k) \Rightarrow n \mid (y - x)$, and as such $y \sim x$.

Transitivity. If $x \sim y$ and $y \sim z$, then there exist integers k and ℓ such that $x - y = nk$ and $y - z = n\ell$. Therefore $x - z = (x - y) + (y - z) = n(k + \ell) \Rightarrow n \mid (x - z)$.

Definition 1.12. Let $\sim$ be an equivalence relation on a set X. For $x \in X$, the *equivalence class of* x is defined by

$$[x] = \{y \in X : x \sim y\}.$$

The set of all equivalence classes is denoted by

$$X/{\sim} = \{[x] : x \in X\}.$$

Definition 1.13. A *partition* of a set X is a collection of nonempty disjoint subsets of X whose union is X.

Theorem 1.14. *The equivalence classes of an equivalence relation on a set X form a partition of X. Conversely, given a partition of X, there exists an equivalence relation whose equivalence classes are exactly the elements of the partition.*

Proof. ($\Rightarrow$) Suppose $\sim$ is an equivalence relation on X. Since $\sim$ is reflexive, $x \in [x]$ for every $x \in X$, which means that all equivalence classes are nonempty. Furthermore, for any $x \in X$, it holds that $x \in [x]$, which means that

$$\bigcup_{x \in X} [x] = X.$$

To show that the equivalence classes are disjoint, assume for contradiction that there exist unique $[x]$ and $[y]$ such that $[x] \cap [y] \neq \varnothing$. Therefore, there exists an element z of X common to both $[x]$ and $[y]$, i.e. $z \sim x$ and $z \sim y$. By symmetry and transitivity, $x \sim y \Rightarrow [x] = [y]$ ($\Rightarrow\Leftarrow$) which contradicts the assumption that $[x] \neq [y]$. As such, equivalence classes are disjoint.

($\Leftarrow$) Given a partition of S, define $a \sim b$ iff a and b are in the same subset. Reflexivity, symmetry, and transitivity trivially hold. $\square$