Abstract Algebra
Judson, Thomas J.

Notes by:
Clay Curry

2 The Integers

2.1 Induction

Definition: First Principle of Mathematical Induction

Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer n_0. If for all integers k with $k \geq n_0$, $S(k)$ implies that $S(k+1)$ is true, then $S(n)$ is true for all integers n greater than or equal to n_0.

Definition: Second Principle of Mathematical Induction

Let $S(n)$ be a statement about integers for $n \in \mathbb{N}$ and suppose $S(n_0)$ is true for some integer n_0. If $S(n_0), S(n_0+1), \ldots, S(k)$ imply that $S(k+1)$ for $k \geq n_0$, then the statement $S(n)$ is true for all integers $n \geq n_0$.

Definition: Principle of Well-Ordering

Every non-empty subset of the natural numbers contains a least element.

Theorem:

The Principle of Mathematical Induction implies that 1 is the least natural number

Proof: □

Theorem:

The Principle of Mathematical Induction implies the Principle of Well-Ordering. That is, every nonempty subset of $\mathbb{N}$ contains a least element.

Proof: □

2.2 The Division Algorithm

An application of the Principle of Well-Ordering that is often-used is the division algorithm.

Theorem: Division Algorithm

Let a and b be integers, with $b \geq 0$. Then there exists unique integers q and r such that

$$a = bq + r$$

where $0 \leq r < b$.

Proof: *existence of q and r.* Consider the set,

$$R = \{a - bx : x \in \mathbb{Z} \wedge a - bx \geq 0\}$$

If $0 \in R$, then $b|a$, and we can let $q = a/b$ and $r = 0$. If $0 \notin R$, then the WOP guarentees the existence of a smallest element in a set R iff $R \subseteq \mathbb{N}$ and $R \neq \emptyset$. Since $a - xb \in \mathbb{Z}$ and $a - xb > 0$, clearly $R \subset N$ the first condition of the WOP is satisfied. To show that $R \neq \emptyset$, consider the two cases:

Case 1: $a \geq 0$. By letting $x = 0$, clearly $a \in R$.

Case 2: $a < 0$. By letting $x = 2a$ and substituting $a - bx = a - b(2a) = a(1 - 2b)$, we have the product of two negative integers a and $(1-2b)$, when $b > 1$ (which is being claimed), hence $a - bx \in R$.

Because $R \subset \mathbb{N}$ and $R \neq \emptyset$, the WOP guarentees that there exists a least element $r = a - bq$. $\square$