Chapter 4

Integers

The Division Algorithm

Let $\emptyset \neq A \subseteq \mathbb{R}$ and $x \in A$. Then x is the *least element* of A if $x \leq b$, for all $b \in A$.

Let $S \subseteq A$ where $S \neq \emptyset$. Then A is *well-ordered* if every S has a least element.

(Well-Ordering Principle) The set of natural numbers is well-ordered. In other words, any nonempty subset of $\mathbb{N}$ contains a least element.

Lemma 4.0.1. *Let $a, b \in \mathbb{N}$. Then there are unique nonnegative integers q and r with $0 \leq r < b$ such that*

$$a = qb + r.$$

Example 4.0.2. Consider the integers 11 and 5. Then $11 = 2(5) + 1$. Here $a = 11$, $b = 5$, $q = 2$, and $r = 1$. Notice that $0 \leq r < b$.

Problem 4.0.3. *Find integers q and r as in Lemma 4.0.1 for the integers $a = 51$ and $b = 7$.*

Proof. (Proof of Lemma 4.0.1)

Proof of existence

Let $a, b \in \mathbb{N}$. Consider the set

$$B = \{kb \,|\, k \in \{0, 1, 2, \dots\}\}.$$

Then $B \subseteq \mathbb{N}$. Also $0 \in B$ so $\emptyset \neq B$. Moreover, there exists $q \in \mathbb{Z}$ such that $qb \in B$ and $a < qb$ since $a < (a + 1)b \in B$. Let

$$C = \{q \in \mathbb{Z} \,|\, a < qb\}.$$

Then $a+1 \in C$. Since $C \neq \emptyset$ and $C \subseteq \mathbb{Z}$ it follows that C has a least element, say q_0+1 by the Well-ordering principle. Hence

$$\begin{aligned} q_0 b \leq a < (q_0+1)b &\Rightarrow q_0 b \leq a < q_0 b + b \\ &\Rightarrow 0 \leq a - q_0 b < b. \end{aligned}$$

By letting $r = a - q_0 b$ we get that $a = q_0 b + r$ and $0 \leq r < b$ as desired.

Proof of Uniqueness

Assume $a = q_1 b + r_1$ and $a = q_2 b + r_2$ where $0 \leq r_1, r_2 < b$. Then $q_1 b + r_1 = q_2 b + r_2$ which implies $(q_1 - q_2)b = r_2 - r_1$. Since $r_2 - r_1$ is a multiple of b and $r_2 - r_1 < b$ it must be the case that $r_2 - r_1 = 0$ which implies $q_1 - q_2 = 0$. Therefore $r_1 = r_2$ and $q_1 = q_2$.

□