Notes 02 Theorems, Proofs Outlines.

Exercises. For each of the following theorems, a sequence of steps has been stated that outline the proof of the theorem. For each step, show why the step follows from the axioms and previous theorems. [As "previous theorems" you may assume what you know about the way integers operate with each other; for example, you may assume that if $a > 0$ and $b < c$ then $ab < ac$ or if $a < 0$ and $b < c$ then $ab > ac$.]

Theorem 2.3. There is no integer between 0 and 1.

Proof. Let $P_1 : 1 \leq 1$ and if n is a positive integer, let $P_n : 1 \leq n$.

Step 1. P_1 is true.

Step 2. $P_n \Rightarrow P_{n+1}$ for all $n > 1$.

Step 3 and conclusion. If $n \in \mathbb{N}$ then $n \geq 1$.

Then (conclusion): There is no positive integer between 0 and 1.

□

Theorem 2.7. [The division algorithm for positive integers.] If each of a and b is a positive integer then there exist unique non-negative integers q and r with $0 \leq r < b$ so that:

$$a = bq + r.$$

Proof. First we prove the existence of r (and q). Let

$$S = \{r \geq 0 | \text{ there is a number } q \geq 0 \text{ so that } a = bq + r\}.$$

Step 1. $q = 0$ and $r = a$ satisfy the definition for $r = a$ to be in the set S.

Step 2. $S \neq \emptyset$ and there is a least element of S.

Step 3. Let $\hat{r}$ denote the least element of S and let $\hat{q}$ be the element that by definition of S gives us $a = b\hat{q} + \hat{r}$. If we assume $\hat{r} \geq b$ then $r' = \hat{r} - b$ and $q' = \hat{q} + 1$ satisfy the condition for $r' \in S$.

Step 4, conclusion 1. Therefore $r' < \hat{r}$ which contradicts the definition of $\hat{r}$; so there exists a number $\hat{r}$ that satisfies the conclusion of the theorem.

Next we prove uniqueness: Suppose that $\hat{r}, \hat{q}$ and r, q are both pairs of non-negative integers such that:

$$\begin{aligned} a &= b\hat{q} + \hat{r} \quad \text{with} \quad 0 \leq \hat{q}; 0 \leq \hat{r} < b \\ a &= bq + r \quad \text{with} \quad 0 \leq q; 0 \leq r < b. \end{aligned}$$

Step 5. If $q < \hat{q}$ then $\hat{r} < r$.

Step 6. If $\hat{r} < r$ then $0 < r - \hat{r} < b$.

Step 7. If $q < \hat{q}$ then this contradicts $r < b$ and $\hat{r} < b$.

Step 8. In a similar way as steps 5-7, we conclude that if $\hat{q} < q$ we have a contradiction.

Step 9, conclusion 2. $\hat{q} = q$.

Step 10. Since $\hat{q} = q$ we can conclude that $\hat{r} = r$.

□

Theorem 2.9. If $a > 0$, $b > 0$ and $a|b$ then $a \leq b$.

Proof.

Step 1. There is an integer q so that $b = qa$.

Step 2. $q \geq 1$.

Step 3. $aq \geq a$.

Step 4 and conclusion. $a \leq b$. □