Math 300, Lecture 18, Siddhartha Sahi

1 Well ordering property and divisibility

1.1 Well ordering

Definition 1 Let \( S \) be a subset of \( \mathbb{Z} \); if all elements of \( S \) are \( \geq l \), then we say \( l \) is a lower bound for \( S \). Formally this means

\[
\forall n \in S \Rightarrow n \geq l.
\]

(1)

If \( S \) has a lower bound then we say \( S \) is bounded below.

Example 2 \( \mathbb{N} \) is bounded below; any integer \( l \leq 1 \) is a lower bound for \( \mathbb{N} \).

The set \( 2\mathbb{Z} = \{-\cdots, -4, -2, 0, 2, 4, \cdots\} \) is not bounded below.

As is clear from the above example, a set can have several lower bounds. However as we show below, at most one of the lower bounds can belong to \( S \).

Lemma 3 Suppose \( l, m \) are lower bounds for \( S \subseteq \mathbb{Z} \). If \( l, m \in S \), then \( l = m \).

Proof. Let \( S \) be a subset of \( \mathbb{Z} \). Suppose \( l, m \) are lower bounds of \( S \) and \( l, m \in S \). By definition of lower bound we get \( l \geq m \) and \( m \geq l \). Therefore \( m = l \).

Definition 4 If \( l \) is a lower bound for \( S \) and \( l \in S \), then we say \( l \) is the smallest element of \( S \).

Note that the empty set \( \emptyset \) is bounded below, but it has no smallest element. Indeed every integer is a lower bound for \( \emptyset \) since the antecedent in (1) is false and so the conditional is true; but \( S \) does not have a smallest element, in fact it has no elements at all. The well ordering principle basically asserts that this is the only such example. Before stating and proving this result we note the following:

Remark 5 If \( S \) is a subset of \( \mathbb{Z} \), then \( S = \emptyset \) if \( n \notin S \) for all integers \( n \).

Theorem 6 If \( S \subseteq \mathbb{Z} \) is bounded below and \( S \) has no smallest element then \( S = \emptyset \).
Proof. Let $S$ be a subset of $\mathbb{Z}$. Suppose $S$ is bounded below and $S$ has no smallest element.

Since $S$ is bounded below $S$ has a lower bound, $l$, say. Thus all elements of $S$ are $\geq l$ and by the above remark to prove $S = \emptyset$ we have to show

$$n \notin S \text{ for all integers } n \geq l. \quad (2)$$

We will prove (2) using PCI.

Suppose $l \in S$. Since $l$ is a lower bound of $S$ this means that $l$ is the smallest element of $S$. However this contradicts the assumption that $S$ has no smallest element. Therefore $l \notin S$.

Now let $k$ be an integer $\geq l$, and suppose that none of the integers $l, l + 1, \ldots, k$ belong to $S$. This means that all elements of $S$ are $\geq k + 1$. Thus $k + 1$ is a lower bound of $S$. As in the previous paragraph, we conclude that $k + 1 \notin S$.

By PCI we conclude $n \notin S$ for all $n \geq l$. This proves (2) and therefore the theorem. $\blacksquare$

The well ordering principle is the following equivalent result.

**Theorem 7 (WOP)** Suppose $S \subseteq \mathbb{Z}$ is bounded below and $S \neq \emptyset$, then $S$ has a smallest element.

**Proof.** Left as an exercise. $\blacksquare$

1.2 Division with remainder

In elementary school you must have considered the following kind of arithmetic problem. How many times 3 go into 17 and what is the remainder? The answer is of course "5 times with remainder 2." Of course the remainder is given by the formula

$$2 = 17 - 3 \times 5$$

but why does 3 go into 17 precisely 5 times, and not 4 times or 6 times? The reason is that 5 is the unique integer $q$ such that

$$3(q + 1) > 17 \geq 3q. \quad (3)$$

Once you understand (3), you can also answer the following question. How many times 3 go into $-17$? The answer is "$-6$ times with remainder 1", and not "$-5$ times with remainder 2".

We can use the WOP to prove that this can be done in general.

**Theorem 8** If $n$ is an integer and $d$ is a natural number, then there is a unique integer $q$ such that

$$d(q + 1) > n \geq dq.$$
**Proof.** Let \( n \in \mathbb{Z} \) and let \( d \in \mathbb{N} \). Let \( S \subseteq \mathbb{Z} \) be defined as follows

\[
S = \{ m \in \mathbb{Z} \mid dm > n \}
\]

We leave it as an exercise to show that \( S \) is bounded below and nonempty.

Therefore by the WOP, \( S \) has a unique smallest element \( l \). Then \( l \in S \) but \( (l-1) \notin S \), otherwise \( l \) would not be the smallest element of \( S \). Therefore we get

\[
dl > n \geq d(l - 1)
\]

Let \( q = l - 1 \), then \( q \) satisfies the conditions of theorem.

We leave the uniqueness of \( q \) as an exercise as well. ■

**1.3 Exercises**

1. Prove Theorem 7 [Hint: Argue by contradiction.]

\[
\text{Let } n \in \mathbb{Z}, d \in \mathbb{N}, S = \{ m \in \mathbb{Z} \mid dm > n \} \text{ as in the proof of Theorem 8.}
\]

2. Prove that \( S \neq \emptyset \). [Hint: Show that \( |n| + 1 \in S \)]

3. Prove \( S \) is bounded below [Hint: Show that \(-|n| \) is a lower bound for \( S \).]

4. Prove uniqueness in Theorem 8 by showing that \( p, q \) are integers such that \( d(q + 1) > n \geq dq \) and \( d(p + 1) > n \geq dp \) then \( p = q \). [Hint: Show that \( p > q \) and \( p < q \) both lead to contradictions.]

**Remark 9** In problems dealing with the absolute value \( |n| \), as in the hints for 2, 3 above, it is useful to write \( k = |n| \) so that \( k \geq 0 \), and consider separately the cases \( n \geq 0 \) and \( n < 0 \). In the former case we have \( n = k \), while in the latter case we have \( n = -k \).