

## Lecture 22, Oct. 21

### Order Properties in $\mathbb{Z}$ , $\mathbb{Q}$ and $\mathbb{R}$

**22.1 Theorem. The Completeness Property in  $\mathbb{R}$**  Every non-empty set  $S \subseteq \mathbb{R}$  which is bounded above has a **supremum** (or least upper bound) in  $\mathbb{R}$ . Every non-empty set  $S \subseteq \mathbb{R}$  which is bounded below has a **infimum** (or greatest lower bound) in  $\mathbb{R}$ .

In  $S \subseteq \mathbb{R}$ , we say  $S$  is bounded above in  $\mathbb{R}$  when there exists  $b \in \mathbb{R}$  such that  $b \geq x$  for every  $x \in S$ . Such a number  $b$  is called an **upper bound** for  $S$  in  $\mathbb{R}$ . A **Supremum** for  $S$  is a number  $b \in \mathbb{R}$  such that  $b \geq x$  for every  $x \in S$  and for all  $c \in \mathbb{R}$ , if  $c \geq x$  for every  $x \in S$ , then  $b \leq c$ .

**22.2 Theorem. Density of  $\mathbb{Q}$  in  $\mathbb{R}$**  For all  $a, b \in \mathbb{R}$ , if  $a < b$  then there exists  $c \in \mathbb{Q}$  such that  $a < c < b$ .

**22.3 Theorem. Order Properties in  $\mathbb{Z}$**

1. **Natural numbers are non-negative.**  $\mathbb{N} = \{x \in \mathbb{Z} \mid x \geq 0\}$
2. **Discreteness** for all  $k, n \in \mathbb{Z}$ ,  $k \leq n \leftrightarrow k < n + 1$
3. **Well Ordering Property of  $\mathbb{Z}$  in  $\mathbb{R}$ .** Every nonempty set  $S \subseteq \mathbb{Z}$  which is bounded above in  $\mathbb{R}$  has a maximum element in  $S$ . Every nonempty set  $S \subseteq \mathbb{Z}$  which is bounded below in  $\mathbb{R}$  has a minimum element in  $S$ . In particular, every nonempty set  $S \subseteq \mathbb{N}$  has a minimum number.
4. For every  $x \in \mathbb{R}$ , there exists  $a \in \mathbb{Z}$  such that  $a \leq x$ . For every  $x \in \mathbb{R}$ , there exists  $b \in \mathbb{Z}$  such that  $x \leq b$ .
5. **Floor and Ceiling Property** For every  $x \in \mathbb{R}$  there exists a unique  $n \in \mathbb{Z}$  which we denoted by  $n = \lfloor x \rfloor$ , such that  $n \leq x$  and  $n + 1 > x$ . For every  $x \in \mathbb{R}$  there exists a unique  $m \in \mathbb{Z}$  which we denoted by  $m = \lceil x \rceil$ , such that  $x \leq m$  and  $x > m - 1$ .
6. **Monotone Sequence Property of  $\mathbb{Z}$**  Let  $m \in \mathbb{Z}$  and let  $(x_n)_{n \geq m}$  be a sequence of integers (so each  $x_n \in \mathbb{Z}$ ). If  $x_{n+1} > x_n$  for all  $n \geq m$ , then for all  $b \in \mathbb{R}$ , there exists  $n \geq m$  such that  $x_n > b$ . If  $x_{n+1} < x_n$  for all  $n \geq m$ , then for all  $b \in \mathbb{R}$ , there exists  $n \geq m$  such that  $x_n < b$ .

*Remark.* If  $N$  has a total ordering  $\leq$  and  $N$  has the property that every nonempty set  $S \subseteq N$  has a minimum element, then we say that  $N$  is a well ordering set.

**22.4 Exercise.** 1. Show that for all  $a \in \mathbb{Z}$ , if  $a \neq 0$  then  $|a| \geq 1$

2. Show that the only units in  $\mathbb{Z}$  are  $\pm 1$ . Indeed show that for all  $a, b \in \mathbb{Z}$ , if  $ab = 1$  then  $(a = b = 1$  or  $a = b = -1)$

### Here ends Chapter 2: Rings Fields, Orders and Induction

### Chapter 3: Factorization in $\mathbb{Z}$

**22.5 Definition.** For  $a, b \in \mathbb{Z}$ , we say  $a$  **divides**  $b$ , or  $a$  is a **factor** of  $b$ , or  $b$  is a **multiple** of  $a$ , and we write  $a \mid b$ , when

$$b = ak \text{ for some } k \in \mathbb{Z}$$

**22.6 Theorem.**

1.  $1 \mid a$  for all  $a \in \mathbb{Z}$

2.  $a \mid 1 \leftrightarrow a = \pm 1$
3.  $0 \mid a \leftrightarrow a = 0$
4.  $a \mid 0$  for all  $a \in \mathbb{Z}$
5.  $a \mid b \leftrightarrow |a| \mid |b|$
6. if  $b \neq 0$  and  $a \mid b$  then  $|a| \leq |b|$
7.  $a \mid a$
8. if  $a \mid b$  and  $b \mid a$  then  $a = b$
9. if  $a \mid b$  and  $b \mid c$  then  $a \mid c$
10. if  $a \mid b$  and  $a \mid c$  then

$$\forall x, y \in \mathbb{Z} \quad a \mid (bx + cy)$$

*Proof.*

6. Suppose  $b \neq 0$  and  $a \mid b$ . Choose  $k \in \mathbb{Z}$  so that  $b = ak$ . If  $k = 0$ , then  $b = ak = a0 = 0$ . But  $b \neq 0$ , so  $k \neq 0$ . Since  $k \neq 0$  we have  $|k| \geq 1$ . Since  $b = ak$ , we have  $|b| = |ak| = |a| |k| \geq |a| 1 = |a|$

□