Last time: discussed consequences of order axioms for \( \mathbb{Z} \).

In particular we proved "cancellation law" for \( \mathbb{Z} \):

\[
\text{if } ab = ac \text{ and } a \neq 0, \text{ then } b = c.
\]

Remark: Commutative rings with 1 that satisfy the cancellation law are called integral domains.

2) Stated well-ordering principle for \( \mathbb{Z} \):

If \( \emptyset \neq A \subseteq \mathbb{Z} \), then \( A \) has a least element.

Note least elements are unique:

if \( a_1, a_2 \) are two least elements then

\[
a_1 \leq a_2 \text{ and } a_2 \leq a_1,
\]

hence \( a_1 = a_2 \) (this uses trichotomy!)

3) Proved:

(i) well-ordering \( \Rightarrow \emptyset \neq A \subseteq \mathbb{Z} \) s.t. \( 0 < a < 1 \)

(ii) well-ordering \( \Rightarrow \) induction principle:

if \( A \subseteq \mathbb{Z} \) with (a) \( 0 \in A \) and (b) \( \forall k \in A, k+1 \in A \)

then \( A = \mathbb{Z} \).

Example: Prove by induction that:

\[
1 + 2 + \ldots + n = \frac{n(n+1)}{2} \quad \text{for all } n \in \mathbb{N}.
\]

Solution: Let \( A = \{ n \in \mathbb{N} \mid 1 + 2 + \ldots + n = \frac{n(n+1)}{2} \} \).

Then \( 1 \frac{(1+1)}{2} = 1 \Rightarrow 1 \in A \).

If \( k \in A \) then

\[
1 + 2 + \ldots + k + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2} = (k+1) \left( \frac{k}{2} + 1 \right) = \frac{(k+1)(k+1+1)}{2}.
\]

\( \Rightarrow k+1 \in A \).

\[
\therefore A = \mathbb{N}, \text{ i.e. } \forall n \in \mathbb{N} \quad 1 + 2 + \ldots + n = \frac{n(n+1)}{2}.
\]
Recall. A relation $R$ on a set $X$ is a subset of $X \times X$. We write $a \sim b \iff (a, b) \in R$.

- $R$ is an equivalence relation if
  1. $a \sim a$ for all $a \in X$ (reflexivity)
  2. $a \sim b \Rightarrow b \sim a$ (symmetry)
  3. $(a \sim b$ and $b \sim c) \Rightarrow a \sim c$ (transitivity)

Given an equivalence relation $\sim$ on $X$ we define the equivalence class of $a \in X$ to be the set

$$[a] = C(a) := \{ b \in X \mid b \sim a \}$$

(compare with Theorem 1.6.13 p. 17)

**Theorem 5.1** Let $\sim$ be an equivalence relation on $X$

1. $\forall a \in X, a \in C(a)$

2. $a \sim b \iff C(a) = C(b)$

3. $C(a) \cap C(b) \neq \emptyset \Rightarrow C(a) = C(b)$.  

4. $X = \bigcup_{a \in X} C(a)$

**Example** $X = \mathbb{Z}$ and $a \sim b \iff a - b$ is even.  

$\sim$ is an equivalence relation (see Example 1.6.5; we'll come back to it). Then $C(0)$ = even integers  

$C(1)$ = odd integers  

and $\mathbb{Z} = C(0) \cup C(1)$.

**Proof of Theorem 5.1**

1. Since $a \sim a$, $a \in C(a)$.

2. Suppose $a \sim b$. If $c \in C(a)$, then $c \sim a$.

   Hence, since $c \sim a$ and $a \sim b$, $c \sim b \Rightarrow c \in C(b)$

   $\Rightarrow C(a) \subseteq C(b)$. Similarly, $C(b) \subseteq C(a)$
Therefore \( a \uparrow b \Rightarrow C(a) = C(b) \).

Conversely, suppose \( C(a) = C(b) \). Then, since \( a \in C(a) \) and \( b \in C(b) \), we have \( a \approx C(a) = C(b) \), \( a \approx C(b) \). \( \Rightarrow \) \( a \uparrow b \).

(2) Suppose \( C(a) \cap C(b) \neq \emptyset \). Then \( x \in C(a) \cap C(b) \). Hence \( x \approx a \) and \( x \approx b \).

Note \( x \approx a \Rightarrow x \approx a \uparrow x \). On the other hand, \( a \approx x \) and \( x \approx b \Rightarrow a \uparrow b \).

By (2) \( a \uparrow b \Rightarrow C(a) = C(b) \).

\[ \therefore \text{if } C(a) \cap C(b) \neq \emptyset, \text{ then } C(a) = C(b). \]

Back to divisibility:

16.6 Definition let \( a, b \in \mathbb{Z} \). \( a \) divides \( b \) if \( b = ac \) for some \( c \in \mathbb{Z} \).

We write \( a \mid b \) if \( a \) divides \( b \).

Facts 16.7

1. \( a \mid a \)

2. \( a \mid b \Rightarrow a \mid (-b) \)

3. If \( a \mid b \) and \( b \mid c \), then \( a \mid c \).

Proof

1. \( a = a \cdot 1 \) hence \( a \mid a \).

2. \( a \mid b \Rightarrow b = ce \) for some \( c \in \mathbb{Z} \)

\[ \Rightarrow -b = (-1) \cdot b = (-1) (c) \cdot a \]

\[ = a \mid (-b) \]

3. Since \( a \mid b \), then \( b = ak \) for some \( k \in \mathbb{Z} \)

Since \( b \mid c \), \( c = lb \) for some \( l \in \mathbb{Z} \)

\[ \Rightarrow c = lb = (lk) a \Rightarrow a \mid c. \]
Back to Example 1.6.5: Fix $n \in \mathbb{N}$, $n \geq 1$.

Define $a \sim b \iff n \mid (a - b)$

Claim. $\sim$ is an equivalence relation.

Proof.

1. Reflexivity: $a - a = 0 = 0 \cdot n$ implies $n \mid a - a \Rightarrow a \sim a$.

2. Symmetry: $a \sim b \Rightarrow b - a = -(a - b) = k \cdot n$ for some $k \in \mathbb{Z}$

3. Transitivity

   $a \sim b \text{ and } b \sim c \Rightarrow a \sim c$.

   Since $a - c = (a - b) + (b - c) = k \cdot n + l \cdot n = (k + l) \cdot n$ implies $n \mid a - c \Rightarrow a \sim c$.

Equivalence classes of $\sim$ (really $\sim_n$, $n \geq 2$)

**Ex. $n = 2$**

$C(0) = \{ n \in \mathbb{Z} \mid n \sim 0 = 2n \in \mathbb{Z} \mid 2 \mid n \}$ even integers

$C(1) = \{ n \in \mathbb{Z} \mid n = 2n \mid 2 \mid (n - 1) \}$

$= \{ n \in \mathbb{Z} \mid n = 2k + 1, k \in \mathbb{Z} \}$ odd integers

Since $2\mathbb{Z} \cup (2\mathbb{Z} + 1) = \mathbb{Z}$, this is it.

**Ex. $n = 3$**. We get $C(0) = 3\mathbb{Z}$

$C(1) = 3\mathbb{Z} + 1$

$C(2) = 3\mathbb{Z} + 2$

Since $\mathbb{Z} = 3\mathbb{Z} \cup (3\mathbb{Z} + 1) \cup (3\mathbb{Z} + 2)$

there are no more equivalence classes.