Last time: reviewed equivalence relations and partitions.

2. Showed: equivalence relation defines a partition.
   A partition defines an equivalence relation.
   Didn't prove equiv. relation $\leftrightarrow$ partition by equiv. classes.
   Is a bijection between equiv. relations and partitions.
   (But it's true and not that hard to check...)

3. (a) $a \equiv b \mod n \iff (\exists k \in \mathbb{Z} \mid (b-a) = kn)$ is an equivalence relation.

(b) $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n = \{ \{0\}, \{1\}, \ldots, \{n-1\} \}$

has a well-defined $+ : \mathbb{Z}/n \times \mathbb{Z}/n \rightarrow \mathbb{Z}/n$
and $\circ : \mathbb{Z}/n \times \mathbb{Z}/n \rightarrow \mathbb{Z}/n$

Fact: These new $+$ and $\circ$ have the usual properties of $+$ and $\circ$ for numbers: commutativity, associativity, $\circ$ distributes over $+$.

Application:

\[ a_k a_{k-1} \ldots a_2 a_1 a_0 = a_k 10^k + a_{k-1} 10^{k-1} + \ldots + a_0 10^0 \]

is divisible by $9 \iff 9 \mid (a_k + \ldots + a_0)$.

Reason:

$10 \equiv 1 \mod 9 \implies 10^2 \equiv 1^2 \mod 9 \implies \ldots \implies 10^k \equiv 1^k \mod 9$

\[ \Rightarrow a_k 10^k + \ldots + a_0 10^0 \equiv (a_k + a_{k-1} + \ldots + a_0) \mod 9 \]

$9 \mid n \iff n \equiv 0 \mod 9.$
**Groups**

**Def.** A binary operation on a set $S$ is a map/function $*: S \times S \to S$.

**Ex.** $+ : \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n$ are binary operations.

*Note. One usually writes $x*y$ instead of $*(x,y)$.*

**Def.** A binary operation $*: S \times S \to S$ is associative if $\forall x, y, z \in S$

$$x * (y * z) = (x * y) * z$$

**Ex.** $+: \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n$ is associative.

$\cdot : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}, (a, b) \mapsto a - b$

is not associative.

$$a - (b - c) \neq (a - b) - c.$$

**Def.** A binary operation $+: S \times S \to S$ is **commutative** if $\forall \ x, \ y \in S$

$$x + y = y + x.$$

**Ex.** $+$ is not commutative.

**Exa.** $S = M_n(\mathbb{R}) = n \times n$ matrices with real entries.

$$M_n(\mathbb{R}) = \{ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} : a_{ij} \in \mathbb{R} \}$$

Matrix multiplication $*: M_n(\mathbb{R}) \times M_n(\mathbb{R}) \to M_n(\mathbb{R})$

$$(a_{ij})(b_{jk}) = \left( \sum_{i} a_{ij} b_{jk} \right)$$

is associative but not commutative.

$$(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix})(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) = (\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}) \text{ while}$$

$$(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix})(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}) = (\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}).$$
Example \[ \text{Cross product } \times : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}^3 \]

is neither associative nor commutative

\[
\begin{align*}
& \mathbf{i} \times (\mathbf{i} \times \mathbf{j}) = \mathbf{i} \times \mathbf{k} = -\mathbf{j} \quad \text{not associative} \\
& (\mathbf{i} \times \mathbf{j}) \times \mathbf{i} = \mathbf{k} \times \mathbf{i} = \mathbf{j} \quad \text{not commutative} \\
& \mathbf{i} \times \mathbf{j} = -\mathbf{j} \times \mathbf{i}
\end{align*}
\]

Def \[ A \text{ group is a set } G \text{ together with a binary operation } \ast : G \times G \to G \text{ and a distinguished element } e \in G \text{ so that } \forall a,b,c \in G \]

1) \( \ast \) associative: \( (a \ast (b \ast c)) = (a \ast b) \ast c \)

2) \( a \ast e = a = e \ast a \) \( \forall a \in G \)

3) \( \forall a \in G, \exists b \in G \) s.t. \( a + b = e \) and \( b + a = e \).

(b is called an inverse of \( a \))

Ex \( (\mathbb{Z}, +, 0) \) is a group.

NonEx \( (\mathbb{Z}, \ast, 1) \) is not a group:

while multiplication \( \ast \) is associative

\( \forall n \in \mathbb{Z} \) s.t. \( n \ast 0 = 1 \).
Proposition 5.1: In any group, inverses are unique.

If \((G, \cdot, e)\) is a group, \(a \cdot c \in G\)

\[
\begin{align*}
ad & \quad a \cdot b = e = b \cdot a \\
a \cdot c = e = c \cdot a & \quad \text{for some } b, c \in G \\
\text{then } & \quad b = c.
\end{align*}
\]

Proof

\[
(c \cdot a) \cdot b = e \cdot b = b.
\]

On the other hand

\[
(c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot e = c,
\]

\[
\therefore \quad b = c.
\]

Proposition 5.1: \(\Rightarrow\) If \(G\) is a group, then \(\sigma\) is a map \(\text{Inv}: G \to G\), \(\text{Inv}(a) = \text{unique } b \in G \quad a \cdot b = e = b \cdot a\).

Usual notation: \(a^{-1} := \text{inv}(a)\).

\(\exists \quad -a = \text{inv}(a)\) \quad \text{if the group operation is written as +}

\[\begin{array}{c}
(\mathbb{Z}/n, +, 10) \text{ is a group and} \\
\text{inv}([k]) = [n-k] + [k] \in \mathbb{Z}/n.
\end{array}\]

Since \([k] + [n-k] = [k + (n-k)] = [n] = 0] .

\[\begin{array}{c}
\text{Ex}\quad \text{Complex numbers } \mathbb{C} \text{ with } 0 \in \mathbb{C} \text{ and +} \\
a \text{ a group,} \\
\mathbb{C} \text{ with } 1 \in \mathbb{C} \text{ and } \cdot = \text{complex multiplication} \\
\text{is not a group: 0 doesn't have an inverse,} \\
\mathbb{C}^* = \{z \in \mathbb{C} \mid z \neq 0\} \text{ is a group under } \cdot
\end{array}\]