Exam | Solutions posted
- graded EoW
- HW 2 this week

Today: Relations, Equivalence Classes
We'll look at the notion of relations on a set, a way of comparing two elements of a set.

Def The Cartesian product of two sets A and B denoted $A \times B$

is the set of all ordered pairs where $a \in A$ and $b \in B$.

$A \times B = \{(a, b) \mid a \in A, b \in B\}$

Ex $A = \{1, 2, 3\}$
$B = \{2, 3\}$
$A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3), (3, 2), (3, 3)\}$

Ex $A = \{(x, y, z) \mid z^2 \geq 1, 2, 3\}$
$B = \{1, 2, 3\}$

Def A relation on a set $S$ is a subset $R \subseteq S \times S$. Generally we write:

$x R y \iff (x, y) \in R$

Ex $A = \{1, 2, 3\}$, $R = \{(1, 2), (1, 3), (2, 3)\}$

Suppose we have a set $A$, and a set $R$ which is a subset of $A \times A$.

Does this represent anything we are familiar with?
Example:
A = \{1,2,3,4,5,6\}
R = \{(1,1), (1,2), (1,3), (1,4), (1,5), (1,6),
(2,2), (2,4), (2,6),
(3,3), (3,6),
(4,4),
(5,5),
(6,6)\}

What about R here?

R = \{(x,y) \in A \times A \mid x \neq y\}

Definition:
A directed graph is an ordered pair \( G = (V, E) \)
where \( V \) is a set of vertices (or nodes) and \( E \) is a set of directed pairs of vertices (directed edges).

Digraphs and Relations:

Can use digraphs to express relations.

Example:
A = \{a, b, c, d\}
R = \{(a,a), (a,b), (c,d), (d,c)\}

\( x R y \iff (x \neq y \land x \leq y) \)

Example:
A = \{1, 2, 3, 4, 5, 6\}
\[ R \subseteq A \times A \]

**B is reflexive if** \( \forall x \in A, xRx \)

**Examples**
- \( \text{set } \{1, 2, 3\} \)
- \( \text{set } \{1, 2, 3\} \)

**Non Examples**
- \( \text{set } \{1, 2, 3\} \neq \text{non equality} \)
- \( \text{set } \{1, 2, 3\} \)

**B is symmetric if** \( \forall x, y \in A, (xRy \rightarrow yRx) \)

**Examples**
- \( (xRy \rightarrow yRx) \)

**Non Examples**
- \( \leq \)
- \( N: \{1\} \) (divisibility)

**B is transitive if** \( \forall x, y, z \in B, (xRy \land yRz) \rightarrow xRz \)

**Examples**
- \( \leq \)

**Non Examples**
- \( \neq \)
- \( 1 \neq 2 \land 2 \neq 1 \)
- \( t \neq 1 \)
A relation on a set $A$ is a subset $R \subseteq A \times A$

\[(x, y) \in R\]

**Def** A relation $R$ is called an equivalence relation if

1. $\forall x \in A, xRx$ (reflexive)
2. $\forall x, y \in A, xRy \implies yRx$ (symmetric)
3. $\forall x, y, z \in A, (xRy \land yRz) \implies xRz$ (transitive)

The equivalence class of $x \in A$ (equivalence class is often denoted by $[x]$)

is $[x] = \{y \in A | xRy\} \subseteq A$

**Ex** $A = \{-2, 1, 1, 2, 3\}$

<table>
<thead>
<tr>
<th>Relation</th>
<th>Graph</th>
<th>Equivalence Classes</th>
</tr>
</thead>
<tbody>
<tr>
<td>equal</td>
<td>![Diagram]</td>
<td>${-2, 3}, {1}, {2}$</td>
</tr>
<tr>
<td>nothing</td>
<td>![Diagram]</td>
<td>${-2, 3}, {1}, {2}$</td>
</tr>
</tbody>
</table>
| partly
  (commutative)
| ![Diagram] | $\{-2, 3\}, \{1\}, \{2\}$ |
| same sign      | ![Diagram] | $\{-2, 3\}, \{1\}, \{2\}$ |
Ex

\[ A = P(\{3, \cdot, 3\}) \] where \( P(S) \) is the power set of \( S \)

Def: The power set of a set \( S \) is the set of all subsets of \( S \), including the empty set and \( S \) itself.

We can write the elements of the power set ordered with respect to inclusion as a graph.

Remark: The Binomial Theorem, which we will discuss is closely related to the power set.

\[ \Rightarrow \] A \( k \)-element subset of some set is a \( k \)-element combination.

\[ \Rightarrow \] The binomial coefficient \( \binom{n}{k} \) or \( nCk \) is the number of subsets with \( k \) elements in a set with \( n \) elements.

\[ \Rightarrow \] # of sets with \( k \) elements of the power set of a set of \( n \) elements.

\[ C(3,0) = 1 \] subset with 0 elements (empty set)

\[ C(3,1) = 3 \] subsets \( \{1\} \) (singletons)

\[ C(3,2) = 3 \] subsets with 2 elements (complement of empty set)

\[ C(3,3) = 1 \] subset of 3 elements (original set)

A combination \( nCk \) or \( C(n,k) \) is given by

\[ \frac{n!}{k!(n-k)!} \]
Let $A$ be the power set of the set $S = \{1, 2, 3\}$.

Two subsets are related if they have the same size (cardinality).

$\Rightarrow$ There is not much to check here, since the relation is built on equality (and equality is reflexive, symmetric, transitive).

Let us look at equivalence classes of $A$ under this relation.

$[\emptyset] = \emptyset \emptyset$

$[\{1\}] = \{1\} \{1\}$

$[\{1, 2\}] = \{1, 2\} \{1, 2\}$

$[\{1, 2, 3\}] = \{1, 2, 3\} \{1, 2, 3\}$

All equivalence classes are singletons.

**Prop**

Suppose $R_1, R_2$ are both equivalence relations (i.e. $R_1, R_2 \subseteq A \times A$).

Then $R = R_1 \cap R_2$ is an equivalence relation.

(we define a new relation)

Since $R_1, R_2 \subseteq A \times A$, we know $R_1 \cap R_2 \subseteq A \times A$ so this is a relation.

**Proof**

1. **Reflexivity**: Suppose $x \in A$, we want to show $xRx \ (x, x) \in R$.

2. **Symmetry**: Suppose $xRy \wedge yRx \Rightarrow (x, y) \in R_1 \wedge (y, x) \in R_2 \Rightarrow (x, x) \in R_1 \cap R_2 \Rightarrow xRx \vee yRx$

3. **Transitivity**: Suppose $xRy \wedge yRz \Rightarrow (x, y) \in R_1 \wedge (y, z) \in R_2 \Rightarrow (x, z) \in R_1 \cap R_2 \Rightarrow xRz \vee yRz$.
Transitive  Suppose \( xRy \) and \( yRz \) \( \quad (\text{and show } xRz) \)

\[
\Rightarrow (x,y) \in R = R_1 \land R_2 \Rightarrow (x,y) \in R_1 \quad \text{and} \quad (y,z) \in R_2
\]

\[
(y,z) \in R_2 \quad \Rightarrow (y,z) \in R_1 \quad \text{and} \quad (y,z) \in R_2
\]

\[
\Rightarrow xR_1 y \quad \text{and} \quad yR_2 z \quad \Rightarrow xR_1 z \quad \Rightarrow (x,z) \in R_1 \quad \Rightarrow (x,z) \in R_1 \land R_2
\]

\[
xR_1 y \quad \text{and} \quad yR_2 z \quad \Rightarrow xR_2 z \quad \Rightarrow (x,z) \in R_2
\]

\[
\Rightarrow xR_2 z \quad \square
\]

Symmetric

\[
xRy \Rightarrow yRx
\]

\[
(x,y) \in R = R_1 \land R_2 \Rightarrow (x,y) \in R_1 \quad \text{and} \quad (x,y) \in R_2
\]

both \( R_1 \) and \( R_2 \) symmetric so

\[
(y,x) \in R_1 \quad \text{and} \quad (y,x) \in R_2
\]

\[
\Rightarrow (y,x) \in R_1 \land R_2 \Rightarrow yRx \quad \square
\]

Proof: \( R_1 \) \( \Rightarrow \) we say that \( a \) is congruent to \( b \) \( \text{mod } n \) \( \iff n \mid (a-b) \)

\[
g \equiv b \text{ (mod n)} \iff n \mid (a-b)
\]

Def: Given \( n \in \mathbb{N} \) and \( a,b \in \mathbb{Z} \), we say that \( a \) is congruent to \( b \) \( \text{mod } n \) \( \iff n \mid (a-b) \)

(\text{or } a \text{ and } b \text{ have the same remainder when divided by } n)

\( n \) is called the module

\[
8 \equiv 3 \text{ mod } 5 \iff 5 \mid 8-3
\]

\[
20 \equiv 4 \text{ mod } 8 \iff 8 \mid 20-4
\]

\[
13 \equiv -1 \text{ mod } 7 \iff 7 \mid 13+1
\]
Proposition \( \equiv (\text{mod } n) \) is an equivalence relation

That is:

1) \( \forall a \in \mathbb{Z}, a \equiv a (\text{mod } n) \) (reflexivity)

2) \( \forall a, b \in \mathbb{Z}, a \equiv b (\text{mod } n) \Rightarrow b \equiv a (\text{mod } n) \) (symmetric)

3) \( \forall a, b, c \in \mathbb{Z}, a \equiv b (\text{mod } n) \land b \equiv c (\text{mod } n) \Rightarrow a \equiv c (\text{mod } n) \) (transitive)

Thus, the following statements are equivalent:

- \( i) \ a \equiv b (\text{mod } n) \)
- \( ii) \ n \mid (a-b) \)
- \( iii) \ a-b = nt \) for some \( t \in \mathbb{Z} \)
- \( iv) \ a = b + nt \) for some \( t \in \mathbb{Z} \)

Reflexive: since \( a-a = 0 \in \mathbb{Z} \) then \( a \equiv a (\text{mod } n) \)

Symmetric: let \( a, b \in \mathbb{Z} \) s.t. \( a \equiv b (\text{mod } n) \). Then \( a-b = nt \) for some \( t \in \mathbb{Z} \).

\[ \Rightarrow \text{multiply both sides by } -1 \Rightarrow b-a = n(-t) \]

Since \((\mathbb{Z}, +)\) a group then \(-t \in \mathbb{Z}\) and so \( b \equiv a (\text{mod } n) \)

Transitive: suppose \( a \equiv b (\text{mod } n) \) and \( b \equiv c (\text{mod } n) \). Then \( a-b = nt \) for some \( t \in \mathbb{Z} \)

\[ b-c = nt' \]

\[ \Rightarrow a-c = n(t+t') \Rightarrow t+t' \in \mathbb{Z} \Rightarrow a \equiv c (\text{mod } n) \]
**Def** The equivalence classes for the equivalence relation \( \equiv \) are called **congruence classes**. They are a partition of \( \mathbb{Z} \).

The set of all congruence classes is denoted \( \mathbb{Z}_n \).

**Def** \( a \equiv b \pmod{n} \) \( \iff \) \( n \mid a-b \)

For \( x \in \mathbb{Z} \) (fixed \( x \)), define the equivalence class of \( x \) with \( \equiv \) \( \equiv \pmod{n} \)

by \( [x] = \{ a \in \mathbb{Z} \mid a \equiv x \pmod{n} \} \)

**Ex** \( n=3 \) \( x=0 \), \( [0] = \{ a \in \mathbb{Z} \mid a \equiv 0 \pmod{3} \} \)

all \( a \) in \( \mathbb{Z} \), \( a \equiv 0 \pmod{3} \)

\( \Rightarrow a = 3k \)

\( \Rightarrow 3 \mid a-0 \Rightarrow 3 \mid a \)

**Ex** equivalence

class of \( 1 \)

\( [1] = \{ a \in \mathbb{Z} \mid a \equiv 1 \pmod{3} \} \)

\( \Rightarrow \{ 1, 4, 7, 10, \ldots \} \)

\( 3 \mid 1-1, 3 \mid 4-1, 3 \mid 7-1, -2, -5 \)

\( 3 \mid -2-1, 3 \mid -5-1 \)

\( [2] = \{ a \in \mathbb{Z} \mid a \equiv 2 \pmod{3} \} \)

\( \Rightarrow \{ 2, 5, 8, 11, \ldots \} \)

\( 3 \mid a-2 \)

We can find all of the integers in one of these three sets. None of these sets overlap.

\( \Rightarrow \) These sets partition the integers.
Fact: There are exactly \( n \) equivalence classes modulo \( n \):
\([0], [1], [2], \ldots, [n-1]\)

Every integer is in one of these equivalence classes.

**Def.** Fix \( n \), the set of least residues is given by
\([0, 1, \ldots, n-1]\)

Every element in this set of least residues is attached to one of these equivalence classes.

**Claim.** For all \( a \in \mathbb{Z} \), \( a \equiv a \pmod{n} \) is congruent to exactly one of the least residues modulo \( n \).

\[\implies\] if you are talking about arithmec modulo \( n \), you only need to talk about the numbers \( 0, \ldots, n-1 \).

**Proof:** Use division algorithm \( a = qn + r \) with \( 0 \leq r \leq n-1 \)

\[\implies a - r = nq\]
\[\implies n \mid (a - r)\]
\[\implies a \equiv r \pmod{n}\]

\[\implies a = k \cdot n - \text{other number between 0 and } n-1\]

in other words one of these least residues. Note \( qr \) in division algorth is unique \( \implies n = \text{exactly 1} \)