Chapter 22 - Equivalence Relations

These notes also contain material covered in Chapter 21 (Congruence Classes) which is well worth reading.

Relations:

Def^n: Let X be a set. A (binary) relation on X is a subset R of $X \times X$. If $(x,y) \in R$ we say that x is R-related to y or

$$x \, R \, y.$$

↑ usually we just use notation like this, but here we have given the formal definition.

Examples:

- On $\mathbb{R}$ we have the binary relations $\leq$, $\geq$, $<$, $>$, and $=$. Usually we don't think of these as subsets of $\mathbb{R} \times \mathbb{R}$, but we could.

- If X is a non-empty set, then on $P(X)$ we have the binary relations $\subseteq$, $\subset$ and $=$.

Note that if $x R y$, that does not necessarily mean that $y R x$. E.g., $1 \leq 2$ but $2 \not\leq 1$.

Equivalence Relations

Def^n: A relation $\sim$ on a set X is said to be an equivalence relation if it satisfies the following:

(i) Reflexive property: $\forall x \in X,\ x \sim x$.

(ii) Symmetric property:
$\forall x, y \in X,\ x \sim y \Rightarrow y \sim x$.

(iii) Transitive property:
$\forall x, y, z \in X,$
$(x \sim y \text{ and } y \sim z) \Rightarrow x \sim z$.

Examples:

- On $\mathbb{R}$, $=$ is an equivalence relation (clearly), but $\leq$ is not. (not symmetric)

Remark: On any set X, $=$ is an equivalence relation (but not a very interesting one).

- When we define the rational numbers, we are really using an equivalence relation on the set $X = \mathbb{Z} \times \mathbb{N}$.

  Recall that for $a, c \in \mathbb{Z}$ and $b, d \in \mathbb{N}$ we say $\frac{a}{b} = \frac{c}{d}$ if and only if $ad = bc$.

  $\longrightarrow$ $\frac{a}{b} = \frac{c}{d}$ really means $(a,b) \sim (c,d)$ where the equivalence relation $\sim$ is defined by

  $$(a,b) \sim (c,d) \iff ad = bc$$

  clearly reflexive & symmetric

  transitivity: Suppose $(a,b), (c,d), (e,f) \in \mathbb{Z} \times \mathbb{N}$ and $(a,b) \sim (c,d)$ (i.e. $\frac{a}{b} = \frac{c}{d}$) and $(c,d) \sim (e,f)$ (i.e. $\frac{c}{d} = \frac{e}{f}$).

  Then $ad = bc$ and $cf = ed$, so $adf = bcf = bed$ and since $d > 0$ it follows that $af = be$, i.e. $(a,b) \sim (e,f)$ (i.e. $\frac{a}{b} = \frac{e}{f}$) as required.

This $\longrightarrow$ shows that fractions make sense!

- We use the following equivalence relation without thinking.

If I have d dollars and c cents I may record this as $(d,c) \in \mathbb{N} \times \mathbb{N}$.

A very natural equivalence relation is

i.e. (d,c) and (d',c') represent the same total amount of money. →

$(d,c) \sim (d',c')$ if and only if $d' = d+q$ and $c' = c-100q$ for some $q \in \mathbb{Z}$.

Equivalence Classes:

When we are dealing with a set X equipped with an equivalence relation $\sim$ we often want to treat "equivalent" elements of X as "the same" (as we do when we write $\frac{a}{b} = \frac{c}{d}$ for fractions). This is often done mentally (i.e. we keep in mind that equivalent elements should be thought of as being in some sense the same) but there is also a formal way dealing with this.

Def^n: Let $\sim$ be an equivalence relation on a set X. For each $a \in X$ we define the equivalence class of a, denoted $[a]$, by

$$[a] = \{x \in X \mid x \sim a\}.$$

Remarks:

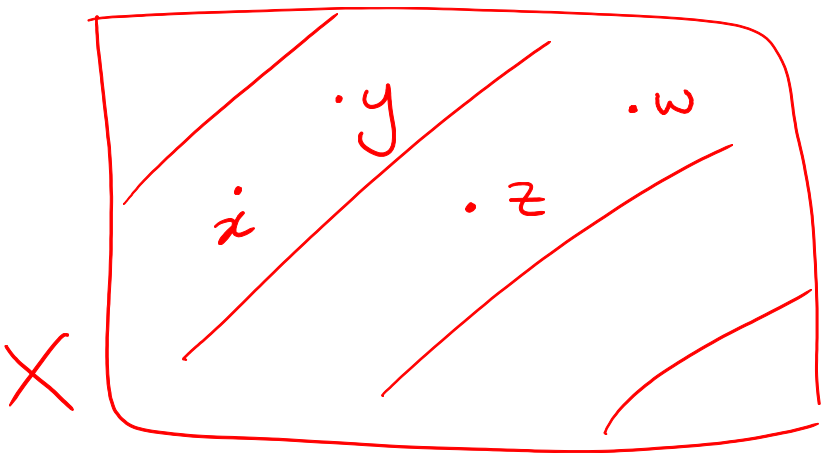
(1) Note that for $a, b \in X$,

$$[a] = [b] \iff a \sim b.$$

(2) Every element of X is in exactly one equivalence classes, so X is a disjoint union of its equivalence classes.

(3) By (1), the equivalence classes encode the equivalence relation.

→ **Picture:**



$x \sim y$

$x \not\sim z$

$z \sim w$

Def^n: Let $\sim$ be an equivalence relation on the set X. We define the quotient of X by the equivalence relation $\sim$, denoted $X/\sim$, to be the set of all equivalence classes

$$X/\sim \;=\; \{[a] \mid a \in X\}.$$

"X mod $\sim$"

Sets of the form $X/\sim$ are extremely common in mathematics. One reason (among many) is the following proposition.

Proposition 22.3.4: Let $f: X \to Y$ be a surjection. Define an equivalence relation on X by $x_1 \sim x_2 \iff f(x_1) = f(x_2)$. Then the map f induces a bijection $X/\sim \to Y$ by $[x] \mapsto f(x)$.

$\hat{f}$

Proof: Exercise. □

Diagram:

$$\begin{array}{ccc} a \in X & & \\ \downarrow & \searrow^{f} & \\ [a] \in X/\sim & \xrightarrow{\hat{f}} & Y \end{array}$$

we say that f factors through $X/\sim$

Example: Congruence Classes

Let $m \in \mathbb{N}$ and consider the binary relation on $\mathbb{Z}$ defined by

$$a \sim_m b \iff a \equiv b \bmod m.$$

We have already seen that $\sim_m$ is reflexive, symmetric and transitive (Chapter 19).

Notation:

- The equivalence class of $a \in \mathbb{Z}$ with respect to $\sim_m$ is denoted $[a]_m$.

  So, e.g., $[5]_4 = [1]_4$, $[12]_7 = [5]_7$, $[4]_2 = [0]_2$.

- The quotient of $\mathbb{Z}$ by $\sim_m$ is denoted $\mathbb{Z}_m$ (or sometimes $\mathbb{Z}/m\mathbb{Z}$).

> Note that
> $$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\}.$$

When the meaning is clear from the context we may just write

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}.$$

But for this class you should stick with the $[\cdot]_m$ notation.

Remark: For $m \in \mathbb{N}$ and $a, b \in \mathbb{Z}$,

$$[a]_m = [b]_m \iff a \equiv b \bmod m.$$

Modular Arithmetic Revisited:

From Chapter 19 we have:

Proposition (Modular Arithmetic):
Let $m \in \mathbb{N}$ and $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ s.t. $[a_1]_m = [a_2]_m$ and $[b_1]_m = [b_2]_m$.

Then

(i) $[a_1 + b_1]_m = [a_2 + b_2]_m$;

(ii) $[a_1 - b_1]_m = [a_2 - b_2]_m$;

(iii) $[a_1 b_1]_m = [a_2 b_2]_m$.

It follows that there is a well defined way to add and multiply congruence classes modulo m. We define:

$$[a]_m + [b]_m = [a+b]_m ;$$
$$[a]_m - [b]_m = [a-b]_m ;$$
$$[a]_m [b_m]_m = [ab]_m$$

for any $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$.

Examples:

- $[3]_5 + [4]_5 = [7]_5 = [2]_5$
- $[2]_7 - [5]_7 = [-3]_7 = [4]_7$
- $[2]_4 [3]_4 = [6]_4 = [2]_4$

multiplication

Addition Table for $\mathbb{Z}_4$:

$+$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[1]_4$	$[1]_4$	$[2]_4$	$[3]_4$	$[0]_4$
$[2]_4$	$[2]_4$	$[3]_4$	$[0]_4$	$[1]_4$
$[3]_4$	$[3]_4$	$[0]_4$	$[1]_4$	$[2]_4$

Multiplication Table for $\mathbb{Z}_4$:

$\times$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$	$[0]_4$
$[1]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[2]_4$	$[0]_4$	$[2]_4$	$[0]_4$	$[2]_4$
$[3]_4$	$[0]_4$	$[3]_4$	$[2]_4$	$[3]_4$

Remarks:

- Note that $[2]_4[2]_4 = [0]_4$.
- Note also that there is no congruence class $[x]_4$ s.t. $[2]_4[x]_4 = [1]_4$.

→ These things don't happen in usual arithmetic. They also don't happen in modular arithmetic when we work modulo a prime.

In general, $\mathbb{Z}_m$ only has the properties of a (commutative) ring. But for p prime $\mathbb{Z}_p$ is a field, like $\mathbb{R}$ or $\mathbb{Q}$.

Addition Table for $\mathbb{Z}_5$:

$+$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[1]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$
$[2]_5$	$[2]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$
$[3]_5$	$[3]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$
$[4]_5$	$[4]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$

Multiplication Table for $\mathbb{Z}_5$:

$\times$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$	$[0]_5$
$[1]_5$	$[0]_5$	$[1]_5$	$[2]_5$	$[3]_5$	$[4]_5$
$[2]_5$	$[0]_5$	$[2]_5$	$[4]_5$	$[1]_5$	$[3]_5$
$[3]_5$	$[0]_5$	$[3]_5$	$[1]_5$	$[4]_5$	$[2]_5$
$[4]_5$	$[0]_5$	$[4]_5$	$[3]_5$	$[2]_5$	$[1]_5$

Note that the entries are all distinct in each row and in each column (besides the first row and first column), unlike for $\mathbb{Z}_4$.