Math 3340
Spring 2021
Lecture #5

17 Feb 2021
Lecture #5

Equivalence classes and $\mathbb{Z}_n$

$$\left\{ \begin{array}{l} a \sim a \\ a \sim b \Rightarrow b \sim a \\ a \sim b, b \sim c \Rightarrow a \sim c \end{array} \right\}$$

$R = \{(a,b) \in S \times S : a \sim b\}$

Fix $n \in \mathbb{Z}_{>0}$ (ie: positive integer)

Define an equivalence relation on $\mathbb{Z}$

$$R_n \subseteq \mathbb{Z} \times \mathbb{Z}$$

or

$$a \equiv b \pmod{n}$$

or: $(a \equiv b \ (n))$.

- $(a,b) \in R_n$ if $n \mid b-a$

  (ie: $\exists\ q \in \mathbb{Z}$ s.t. $qn = b-a$).

- $a \equiv b \pmod{n}$ if $n \mid b-a$.

Prop R_n is an equivalence relation on $\mathbb{Z}$:

ie:
① $(a,a) \in R_n$

② $(a,b) \in R_n \Rightarrow (b,a) \in R_n$

③ $(a,b) \in R_n, (b,c) \in R_n \Rightarrow (a,c) \in R_n$

proof ①, ②: do these yourself.

③ $(a,b) \in R_n$ ie: $b-a = q_1 n$ some $q_1 \in \mathbb{Z}$

$(b,c) \in R_n$ ie: $c-b = q_2 n$ some $q_2 \in \mathbb{Z}$

$\therefore \quad c-a = (q_1+q_2)n$

(therefore) $\therefore$ $c-a$ is div. by n

$\therefore (a,c) \in R_n$

notation ① if $a \in \mathbb{Z}$, $[a]_n$ = equiv. class containing a

(of $\equiv \pmod n$)

$= \{b \in \mathbb{Z} : b \sim a\}$

② $\mathbb{Z}_n := \mathbb{Z}/\equiv_n$ = set of equivalence classes.

General factoid

situation: S = set, $\sim$ an equiv. relation on S.

for $x \in S$, let $[x] = \{y \in S : y \sim x\}$.

and $S/\sim$ is the set of all equivalence classes.

then for $x, y \in S$, either

(a) $[x] = [y]$ (in this case $x \sim y$)

or (b) $[x] \cap [y] = \phi$ (case $x \not\sim y$).

* look at the def. of partition of a set S (section. 2.2).

$\{[x] : x \in S\}$ is a partition of S.

proof Suppose $z \in [x] \cap [y]$

then $z \in [x]$, $z \in [y]$

so $z \sim x$, $z \sim y$

$\therefore x \sim y$

But if $x \sim y$, then $[x] = [y]$:

if $z \in [x]$ that means: $z \sim x$ $\therefore z \sim y$

$\therefore z \in [y]$.

$\therefore [x] \subseteq [y]$.

similarly: if $z \in [y]$,

then $z \in [x]$, for same reason

$\therefore [y] \subseteq [x]$.

$\therefore [x] = [y]$.

$\therefore$ either (a) or (b) holds, not both

example Let $n = 4$, what are the equivalence classes of $\equiv \pmod 4$? What is $\mathbb{Z}_4$?

$$[0]_4 = \{ 4k : k \in \mathbb{Z} \}$$

$$[1]_4 = \{ 4k+1 : k \in \mathbb{Z} \}$$

$$[2]_4 = \{ 4k+2 : k \in \mathbb{Z} \}$$

$$[3]_4 = \{ 4k+3 : k \in \mathbb{Z} \}.$$

$$[-1]_4 = [3]_4.$$

$$[0]_4 \cup [1]_4 \cup [2]_4 \cup [3]_4 = \mathbb{Z}$$

partition of $\mathbb{Z}$.

Assume this (from chapter 1):

17 Feb 2021
Lecture #5
5

Division algorithm

Let $n > 0$ be a positive integers,
Let $m \in \mathbb{Z}$.
then $\exists!$ $q, r \in \mathbb{Z}$ s.t

"q = quotient"
"r = remainder"

(a) $m = qn + r$

(b) $0 \leq r \leq n-1$

$0 \leq r \leq n-1$

notation: $m \bmod n = r$

$-1 \bmod 4 = 3$

Example
fix $n > 0$

$h : \mathbb{Z}_n \longrightarrow \{0, 1, 2, \ldots, n-1\}$

$[a]_n \longmapsto a \bmod n$

note: $\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\}$.

need to check: if $[a]_n = [b]_n$, then

$a \bmod n = b \bmod n$.

if $b \in [a]_n$

then want to prove: $a \bmod n = b \bmod n$.

why? $a = q_1 n + r_1$ $\quad 0 \le r_1, r_2 \le n-1$

$b = q_2 n + r_2$ $\quad r_1 = a \bmod n$

$r_2 = b \bmod n$.

$b \in [a]_n$ means $n \mid b-a$.

$$b - a = (q_2 - q_1) n + r_2 - r_1$$

$\therefore r_2 - r_1 = 0$ $\quad \therefore r_1 = r_2$ $\quad \therefore h$ is well defined.

prop $h : \mathbb{Z}_n \longrightarrow \{0, 1, \ldots, n-1\}$

is a bijection.

proof do this yourself.

Groups!

Def Let G = a set. A binary operation on G is a function $* : G \times G \longrightarrow G$

have, for $a, b \in G$, $*(a,b) \in G$

instead we write: $a * b = *(a,b) \in G$.

examples sets: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{N} = \{0,1,2,\ldots\}$

binary op's: $+$ ✓, $\cdot$ ✓, $-$, $\div$

$-$: not on $\mathbb{N}$ (it is a binary op on the rest)

$\div$: not for any of these!

$\div$ is a binary operation on $\mathbb{Q}_{>0}$

Def A **group** $(G,*)$ is a set G together with a binary operation $* : G \times G \to G$ satisfying:

① $*$ is **associative**: $\forall a,b,c \in G$

$$a * (b * c) = (a * b) * c$$

② $\exists\, e \in G$ s.t. $\forall a \in G$ ("identity")

$$e * a = a * e = a$$

③ $\forall a \in G, \exists\, a' \in G$ s.t. ("inverse")

$$a * a' = a' * a = e.$$

notation: a' is called the inverse of a

denoted by a^{-1}