Alg - 3

HW. (1) $A \underset{s}{\sim} B \iff A = TBT^{-1}$ for some invertible $T \in M_{n\times n}(\mathbb{R})$ and $A, B \in M_{n\times n}(\mathbb{R})$. Prove that $\underset{s}{\sim}$ is an equivalence rel on $M_{n\times n}(\mathbb{R})$.

2. Define $x \sim y \iff x - y = n$ for some $n \in \mathbb{Z}$ and $x, y \in \mathbb{R}$, the set of reals. Prove that $\sim$ is an equivalence relation on $\mathbb{R}$.

Note $\mathbb{R}/\sim$ will be identified with $S^1 = T = \{z \in \mathbb{C} : |z| = 1\}$ (where $\sim$ is defined in ~~Hw~~ #3 (2) ④.

$x \sim y \iff x - y = n$ for some $n \in \mathbb{Z}$.

Defn $p \geq 2$ integer is prime iff $p = mn$, $m, n \in \mathbb{N}$ then either $m = 1$ or $n = 1$

(only divisors in $\mathbb{N}$ of p are $1, p$)

Thm $n \in \mathbb{N}$ is either a prime or

Thm $n \in \mathbb{N}$ is either a prime or else $n = p_1 p_2 \cdots p_r$ where $p_1 \cdots p_r$ are primes in $\mathbb{N}$, $r \geq 1$ integer. $p_1 \cdots p_r$ need not be distinct.

Proof. Let $S = \{n \in \mathbb{N} : n$ is not a product of primes$\}$

$S \subseteq \mathbb{N}$. T. show $S = \emptyset$.

Suppose not. Then by WOP there is a smallest $m \in S$: $m \leq n$ $\forall n \in S$

Since $m \in S$, m is not product of primes

So there are $d, e \in \mathbb{N}$ s.t. $1 < d, 1 < e$

s.t. $m = de \cdot e, d \notin S$ as $m > d$ & $m > e$

So $d = t_1 \cdots t_r$, $e = t_1' \cdots t_p'$ where

$t_1, \ldots, t_r, t_1', \ldots t_s'$ are primes

But $m = de = t_1 \cdots t_r t_1' \cdots t_s'$, a product of primes. $\Rightarrow m \notin S$, a contradiction. So $S = \emptyset$

Fundamental Theorem of arithmetic.

Fundamental Theorem of arithmetic

(i) Every $2 \leq n \in \mathbb{N} \Rightarrow n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ where

$p_1 < p_2 < \cdots < p_r$, primes &

$\alpha_i \geq 0$ intgrs $i = 1 \cdots r$

| $n^0 = 1$

(ii) If also $n = q_1^{\beta_1} \cdots q_s^{\beta_s}$

where $q_1 < \cdots < q_s$ are primes

and $\beta_i \geq 0$ intgrs, $i = 1 \cdots s$

then $r = s$ and $p_i = q_i$, $i = 1 \cdots r = s$

These unique α_i, $i = 1 \cdots r$

are called orders of n at p_i.

$$\operatorname{ord}_{p_i}(n) = \alpha_i$$

$n = 8 = 2^3$, $p_1 = 2$, $\alpha_1 = 3$

$\operatorname{ord}_2 8 = 3$

Ex $m, n \in \mathbb{N}$,

Ex $m, n \in \mathbb{N}$

$m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$

$n = p_1^{\beta_1} \cdots p_r^{\beta_r}$ $\alpha_1 \cdots \alpha_r, \beta_1 \cdots \beta_r \geq 0$ integers

$(n, m) = d = p_1^{\min(\alpha_1, \beta_1)} p_2^{\min(\alpha_2, \beta_2)} \cdots p_r^{\min(\alpha_r, \beta_r)}$

$[n, m] = p_1^{\max\{\alpha_1, \beta_1\}} \cdots p_r^{\max\{\alpha_r, \beta_r\}}$

Equivalence relations and congruences

S is a set (always non empty)

Def (1) A relation $\sim$ is a subset of $S \times S = \{(a, b) : a, b \in S\}$, the set of all ordered pairs: $(a, b) = (c, d) \iff a = c$ $b = d$

(2) A relation $\sim$ on S is called an equivalence relation, write $a \sim b$ for $(a, b) \in \sim \subseteq S \times S$ iff

(i) $a \sim a$ (reflexive prop) $\forall a \in S$

(ii) $a \sim b \Rightarrow b \sim a$ (symmetric)

(ii) $a \sim b \Rightarrow b \sim a$ (symmetric) $\forall\, a, b \in S$

(iii) $a \sim b$ and $b \sim c \Rightarrow a \sim c$ (transitive prob)

Ex | $x, y \in \mathbb{Z}$, $n \in \mathbb{N}$, fixed. Define

$x \underset{n}{\sim} y \iff n \mid x-y$

Then $x \underset{n}{\sim} y$ is an equivalence rel on $\mathbb{Z}$.

(2) $A, B \in M_{n\times n}(\mathbb{R})$. $A \underset{s}{\sim} B$ (A is similar to B) iff $A = TBT^{-1}$ for some invertible $T \in M_{n\times n}(\mathbb{R})$

Then $\underset{s}{\sim}$ is an equivalence rel on $M_{n\times n}(\mathbb{R})$

(3) $A, B \in M_{n\times n}(\mathbb{C})$, $A \underset{U}{\sim} B$ (unitary equivalence) iff $A = UBU^{-1}$ for some $U \in M_{n\times n}(\mathbb{C})$ unitary: $U^{-1} = U^* = \overline{U}^t$,

prove $U \in M_{n\times n}$ ...

$= \overline{U^t}$

$= \bar{U}^t$

Let S be a set & $\sim$ be an equivalence relation on S. For each $x \in S$ let $C_x = [x] = \{y \in S : y \sim x\}$, & is called the equivalence class of x.

Thm (1) $C_x \neq \phi$ ✓

(2) $C_x \cap C_y = \phi$ or if $C_x \cap C_y \neq \phi$ then $C_x = C_y$

(3) $\{C_x\}_{x \in S}$ is a partition of S

Def. $\{A_\alpha\}_{\alpha \in I \neq \phi}$ of subsets of S is a partition of S iff

(1) $A_\alpha \neq \phi \quad \forall \alpha \in I$

(1) $A_\alpha \neq \phi \quad \forall \alpha \in I$

(2) $A_\alpha \cap A_\beta = \phi$ for $\alpha \neq \beta$

(3) $S = \bigvee_{\alpha \in I} A_\alpha$

Proof of thm. Since $x \sim x$

$\Rightarrow x \in C_x \Rightarrow C_x \neq \phi$. proving (1)

(2) Let $x, y \in S$. If $C_x \cap C_y = \phi$, done

(nothing to prove) Suppose $C_x \cap C_y \neq \phi$

then to show $C_x = C_y$?.

$C_x \subseteq C_y$ and $C_y \subseteq C_x$.

Since $C_x \cap C_y \neq \phi$, $\exists\ z \in C_x \cap C_y$

$z \in C_x$ and $z \in C_y$

$\Downarrow$ $\Downarrow$

$z \sim x$ $\quad$ $z \sim y$.

$\Downarrow$

$x \sim z$ by symmetry $\wedge$ $z \sim y$

$\Rightarrow x \sim y$ by transitivity proof

$a \in C_x$. Want to prove $a \in C_y$

$a \in C_x \Rightarrow a \sim x$, and $x \sim y$

$\Rightarrow a \sim y$ by transitive proof

$\Rightarrow a \in C_y$. Similarly.

Show that $C_y \subseteq C_x$. proves

$C_y = C_x$.

(3) $\bigcup_{x \in S} C_x = S$

Since $C_x \subseteq S$ for each x

$\bigcup_{x \in S} C_x \subseteq S$. If $a \in S$

$\Downarrow$ $a \in C \subseteq \bigcup C_x$

then $a \in C_a \subseteq \bigcup_{x \in S} C_x$

$\Rightarrow S \subseteq \bigcup_{x \in S} C_x$

prove $S = \bigcup_{x \in S} C_x$

Notation The set $S/\sim = \{[x] : x \in S\}$

$= \{C_x : x \in S\}$

called called the quotient set.

Thm $\sim_n$ is an equivalence relation on $\mathbb{Z}$

where $x \sim_n y \iff n \mid x-y$

Proof (1) $x \sim_n x \iff n \mid x-x=0$

as $0 = 0 \cdot n$.

(2) Suppose $x \sim_n y$. $x-y = qn$

for $q \in \mathbb{Z}$

Now $y-x = -(x-y)$

$= -(qn)$

$= (-q)n$

$\Rightarrow n \mid y-x$. (symmetric proof)

(3) Suppose $x \underset{n}{\sim} y \wedge y \underset{n}{\sim} z$, for $x, y, z \in \mathbb{Z}$

then $x-y = q_1 n$ and $y-z = q_2 n$

for $q_1, q_2 \in \mathbb{Z}$

$x-z = x-y+y-z = q_1 n + q_2 n$

$= (q_1+q_2)n$

$\Rightarrow n \mid x-z \Rightarrow$ transitivity.

$[x] = [x]_n = \{ y \in \mathbb{Z} : y \underset{n}{\sim} x \}$

(1) $x \underset{n}{\sim} y$, $a \underset{n}{\sim} b \Rightarrow$ (i) $x+a \underset{n}{\sim} y+b$

(ii) $xa \underset{n}{\sim} y \cdot b$

$$\mathbb{Z}/\sim_n = \{[x]_n : x \in \mathbb{Z}\}$$

$[x]_n \oplus_n [y]_n = [x+y]_n$ — sum

$[x] \otimes_n [y]_n = [xy]_n$ — product

x is congruent to y mod n, write

$x = y \bmod n \iff x \sim_n y$ i.e.

$n \mid x-y$.