Jan21

Thursday, January 21, 2021 1:18 PM

Announcement No HW Due tomorrow.

HW 1: Released tomorrow (1-22)
Due Friday 1-29 @ Noon
on Gradescope.

Last Time:

S, T sets $\quad f: S \longrightarrow T$

f injective $\Longleftrightarrow$ it has a left inverse.

Injective: If $f(x) = f(y)$ then $x = y$.

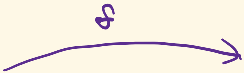
Left Inverse: $g: T \longrightarrow S$ s.t.

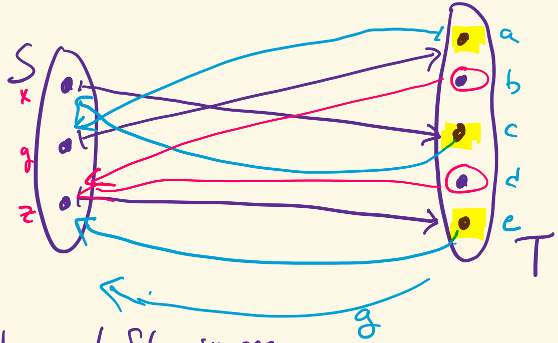
$g(f(x)) = x$ i.e. $g \circ f = \mathrm{id}_S$.

We proved $\Longleftarrow$

Study $\Longrightarrow$ by looking @ an example.

Example





Want a left inverse

g should undo f.

My hand is forced for $g(a), g(c), g(e)$

b & d can go anywhere.

Easily check $g \circ f = id_S$.

$g(f(x)) = g(c) = x$:)

Remark

- Make clear relationship between injectivity & left inverses
- Argument for general case similar.
- Philosophy: Work out a simple example & observe main idea of general case.

Important Structure on Sets:

Equivalence Relations.

Example

Call $x, y \in \mathbb{Z}$ related (or similar) if have same parity (EX/ same as $x - y$ even) (i.e. both even or both odd) write $x \sim y$

Observe $\sim$ like $=$

✓ • $x \sim x$

✓ • $x \sim y$ then $y \sim x$

✓ • $x \sim y$ $y \sim z$ then $x \sim z$

Define as a certain $\mathcal{U} \subseteq \mathbb{Z} \times \mathbb{Z}$

$$\underset{\{(x,y) \mid x \sim y\}}{\underset{\shortparallel}{\mathcal{U}}}$$

Def^n An equivalence relation on a set S is a subset $\mathcal{U} \subseteq S \times S$ satisfying.

① (Reflexivity) $(x, x) \in \mathcal{U}$
$x \sim x$

② (Symmetric) $(x, y) \in \mathcal{U}$ then $(y, x) \in \mathcal{U}$
$x \sim y$ then $y \sim x$

③ (Transitivity) $(x, y) \in \mathcal{U}$ and $(y, z) \in \mathcal{U}$ then $(x, z) \in \mathcal{U}$.

$x \sim y$ & $y \sim z \implies x \sim z$

Notation If $\mathcal{U} \subseteq S \times S$ is an equivalence relation
$(x,y) \in \mathcal{U} \iff x \sim y$

Related Notion: Partitions of Set

Def^n S a set. $\{X_i\}$ a collection of subsets of S. $(X_i \subseteq S)$

We call $\{X_i\}$ a partition of S if.

→ a) Each $X_i \neq \emptyset$ (nonempty)

→ b) $\bigcup_i X_i = S$ (union is S)

→ c) If $i \neq j$ then $X_i \cap X_j = \emptyset$.

Example $S = \mathbb{Z}$.

X_1 = odd numbers

→ X_2 = even numbers.

a) ✓ odd & evens exist

b) Every number is even or odd.

c) No number is both even & odd.

Observe

$\sim$ from example above

$\iff$ "in same box" of our partition.

Fact There is a bijection ← def a bijective function.

$$\left\{\begin{array}{c}\text{equivalence}\\ \text{relations}\\ \text{on } S\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{partitions}\\ \text{on}\\ S\end{array}\right\}$$

$$\xmapsto{\quad\text{How?}\quad}$$

Def$^{\underline{n}}$

Let $\sim$ be an equivalence relation on S. Let $a \in S$. The equivalence class of a is

$$\underset{\uparrow}{[a]} = \underset{\uparrow}{\overline{a}} = \{ b \in S \mid a \sim b \} \subseteq S$$

various notations

Ex/ $S = \mathbb{Z}$ $\quad\sim$ was sharing parity.

$$\left.\begin{array}{l}[2] = \text{even numbers}\\ [7] = \text{odd numbers}\end{array}\right\} \begin{array}{c}\text{recover the}\\ \text{partition}\\ \text{of } \mathbb{Z}.\end{array}$$

Prop

1) Let $\sim$ be an equivalence relation on a set S. Then the equivalence classes of $\sim$ form a partition of S.

2) Let $\{X_i\}$ be a partition of S.
The X_i are equivalence classes of
a unique equivalence Relation on S.

Proof HW.

Do a tiny bit.

①. Have these equivalence classes of $\sim$.
Show they are a partition.

(a) $[a]$ is nonempty.

Know $a \sim a$ (reflexive)

So $a \in [a]$ ✓ $\cancel{\emptyset}$

Algebraic Properties of $\mathbb{Z}$

Have $+ : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$

$\times : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$. satisfy.

	⊕	⊗
Associative	① $a+(b+c)=(a+b)+c$	①' $a\times(b\times c)=(a\times b)\times c$
Identity	② $a+0=0+a=a$	②' $a\times 1=1\times a=a$
Inverse	③ $a+(-a)=(-a)+a=0$	
Commutative	④ $a+b=b+a$	④' $a\times b=b\times a$

Distributive ⑤ $a\times(b+c)=a\times b+a\times c$

§ Divisibility

Defⁿ $a, b \in \mathbb{Z}$. We say a divides b $(a \mid b)$ if $\exists\ k \in \mathbb{Z}$ s.t. $ak = b$

Ex $3 \mid 21$ b/c $3 \cdot \underset{\uparrow k}{7} = 21$

$3 \nmid 22$. No such k exists.

Exercise

$a \mid b$ and $a \mid c$. Then $a \mid (b+c)$

$a \mid b$ then $a \mid bc$ any c.

Defⁿ (Greatest Common Divisor)

$a, b \in \mathbb{Z}$ $\gcd(a,b)$ is a $g \in \mathbb{Z}$ s.t.

① $g \mid a$ and $g \mid b$. (common divisor)

② If $d \mid a$ & $d \mid b$ then $d \leq g$.

Ex $\gcd(12, 15) = 3$

Defⁿ / Prop (Long Division)

Let $a, b \in \mathbb{Z} \setminus \{0\}$. Exists unique q, r

↑ quotient

s.t. ① $a = b\underline{q} + \underline{r}$

② $0 \leq r < |b|$

↑ remainder (or residue)

Ex

$$\begin{array}{r} 3 \quad R\,2 \\ 7\,\overline{)\,23} \\ -21 \\ \hline 2 \end{array}$$

$$\boxed{23 = 7\cdot 3 + 2}$$

Proof Exercise.

Hint: Consider the set $\{a-bq \mid q\in\mathbb{Z}\}$

Theorem (Euclidean Algorithm)

$a,b\in\mathbb{Z}\setminus\{0\}$. Iterate long division as follows.

$$a = bq_0 + r_0 \leftarrow$$

smaller $\downarrow$

$$b = r_0\cdot q_1 + r_1 \leftarrow$$

$$r_0 = r_1\cdot q_2 + r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + \underline{\underline{r_n}} \leftarrow$$

$$r_{n-1} = q_{n+1}\cdot r_n + 0$$

Then $\gcd(a,b) = r_n$

Pf/ Exercise.

Hint: If $a=bq+r$ then show.

$$\longrightarrow \gcd(a,b) = \gcd(b,r) \qquad \varnothing$$

Corollary (Extended Euclidean Algorithm)

$a,b\in\mathbb{Z}$. Then $\exists\ u,v\in\mathbb{Z}$ s.t.

$$\gcd(a,b) = au + bv.$$

Proof $a, b \neq 0.$

Run Euc. Alg.

$$\gcd(a,b) = r_n = r_{n-2} - q_n r_{n-1}$$

Solve $r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$

Solve $r_{n-2} = --$

$$\vdots$$
$$\downarrow$$

Solve $r_0 = a - b q_0.$

Plug in all the way back up ∅

Example $\gcd(35, 20)$

$$35 = 20 \cdot 1 + 15$$
$$20 = 15 \cdot 1 + \boxed{5} \longleftarrow \gcd(35, 20) = 5$$
$$15 = 5 \cdot 3 + 0$$

$5 = 20 - 15 \cdot 1$ $\quad 20 - (35 - 20 \cdot 1) \cdot 1$

$15 = 35 - 20 \cdot 1$ $\quad$ ↰ plug in $\quad \boxed{= 2 \cdot 20 - 35}$

Primes

Defn An integer $p > 1$ is prime if its only positive divisors are 1 & p itself.

Euclid's Lemma

$a, b \in \mathbb{Z}$. p a prime.

If $p | ab$ the $p | a$ or $p | b$.

Rmk Primality important.

$15 | 3 \cdot 5$ but $15 | 3$ or 5.

Proof $g = \gcd(a, p)$

Then $g = 1$ or $g = p$.

↑ we win. b/c $p | a$.

Let $g = 1$

EEA $\exists\, u, v$ s.t.

$au + pv = 1$ mult by b

$abu + pbv = b$.

$p | ab \implies p | abu$.

$p | p \implies p | pbv$ $\implies p / (\underbrace{abu + pbv}_{= b})$:)

Inductive Euclid's Lemma

p prime. $p | a_1 a_2 \cdots a_n$.

Then $p | a_i$ for some i.

Pf/ Base Case

Obvious for $n = 1$ ($p | a \Rightarrow p | a$)

Inductive Step

Assume true for n-1 ← (Inductive Hypothesis)

Show true for n.

$$p \mid (a_1 \cdots a_n) \rightsquigarrow p \mid (a_1 \cdots a_{n-1}) \cdot a_n.$$

Euclid's Lemma $p \mid a_1 \cdots a_{n-1}$ or $p \mid a_n$

$\Downarrow$ induction — ↑ we win.

$p \mid a_i$ some $i = 1, \ldots, n-1$

$\varnothing$

Theorem (Fundamental Theorem of Algebra)

Let $a > 1$ be an integer. The a can be written as a product of primes

$$a = p_1 p_2 \cdots p_t$$

Such a factorization is unique up to reordering

Rmk Allowing repeats.

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}$$ ↙ uniqueness?

Proof

Existence: ✓

Suppose $S = \{ z > 1 \mid z \text{ doesn't have a prime factorization} \}$.

There exist a smallest such z_1 cannot be prime.

$\exists\, 1 < z_1, z_2 < z$ s.t. $z = z_1 z_2$.

Then $z_1 = p_1 \cdots p_t$

$z_2 = q_1 \cdots q_\ell$.

$$\Longrightarrow z = z_1 z_2 = p_1 \cdots p_t q_1 \cdots q_\ell.$$

2) Uniqueness

$$\boxed{a = p_1 \cdots p_t = q_1 q_2 \cdots q_\ell}$$

WLOG ↙

Assume also without loss of generality that $\ell \geq t$.

$p_1 \mid q_1 q_2 \cdots q_\ell$ Ind Euclid

$\Longrightarrow p_1 \mid q_i$ some i.

$\Longrightarrow p_1 = q_i$ Reordering the q_i

assume $p_1 = q_1$,

So cancel them..

$$p_2 p_3 \cdots p_t = q_2 q_3 \cdots q_\ell.$$

Same way $p_2 = q_2$, $p_3 = q_3$, ...

$$1 = q_{t+1} \cdots q_\ell$$

↑ These must be all 1

But they are prime.

So $\ell \not> t$ so $\ell = t$.

The primes paired up

So we win