Notes

September 10, 2014

assignment

2.2 #16

prove f is onto iff there exists $g : B \to A$ such that $f \circ g = f(g(x)) = 1_B$

proof

Assume f is onto then $\forall b \in B\ \exists x_b \in A$ such that $f(x_b) = b$.

For every $b \in B$ choose $x_b \in A$

define $g : B \to A, g(b) = x_b$, then $(f \circ f)(b) = f(g(b)) = f(x_b) = b$

other way

prove that for every $b \in B$ there exists $x \in A$ such that $f(x) = b$

we have $b = f(g(b))$. $g(b) = x$. almost a tautology. done

2.2 #18

LOOK HERE

Let A be a

last time

equivalence relations

example

let $f : S \to T$. on S we define the equivalence relation as follows: $x, y \in S$ then $x \sim_f y$ iff $f(x) = f(y)$.

two elements are related iff they have the same image. if f is injective then $[f] = f$. constant function has one equivalence class.

proposition

there exists a one to one (bijection) from the set of equivalence classes $S/\sim_f$ and $f(s)$. $\bar{f} : S/\sim_f \to f(S)$. Namelly $[x] \to f(x)$.

question? does $[x] = [y]$ imply that $f(x) = f(y)$? in this case, $[x] = [y] \Rightarrow x \sim_f y \Rightarrow f(x) = f(y)$ so f is a well defined function. (well defined is redundant, but places proper emphasis)

surjectivity of $\bar{f}$ is clear. what about injectivity? if $f(x) = f(y) \to x \sim_f y \to [x] = [y]$

1.4 integers modulo n

$n > 1, n \in \mathbb{Z}$. on $\mathbb{Z}$ we define the equiv relation $\equiv$ as $a \equiv b \mod n$ if and only if $n|(a-b)$.

$\mathbb{Z}_n = \mathbb{Z}/\equiv \rightarrow$ set of equiv classes. $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$

alternate notation is $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots, n \bar{-} 1\}$.

define operations on $\mathbb{Z}_n$ as follows:

addition: $[a] + [b] = [a+b]$

multiplication: $[a] \cdot [b] = [a \cdot b]$

$[a] = [a'], [b] = [b'] \rightarrow [a+b] = [a'+b']$.

$n|(a-a'), n|(b-b') \rightarrow n|((a+b)-(a'+b'))$

similarly for multiplication.

$[a] = [a'], [b] = [b'] \rightarrow [a \cdot b] = [a' \cdot b']$.

proposition

these operation satisfy associative, commutative, distributive

definition: Let $[a]_n \in \mathbb{Z}_n$. If there exists $[b]_n \in \mathbb{Z}$ such that $[b] \neq 0, [a][b] = [0]$. We say that $[a]$ is a zero-divisor in $\mathbb{Z}_n$

example

$\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5], [6]\}$. zero divisors are $\{[0], [2], [3], [4]\}$

multiplicative inverse

if $[a][b] = 1$ for some $[b] \in \mathbb{Z}_n$ we say that $[a]$ is an invertible element of $\mathbb{Z}_n$ and $[b]$ is a multiplicative inverse of $[a]$.

$\mathbb{Z}_6$ invertible elements:$\{[1][5]\}$ because $[5][5] = 1$ (25 mod 6 is 1)

lets take $[a] \in \mathbb{Z}$ then $[a]$ is invertible iff $\gcd(a, n) = 1$.

proof

assume $(a, n) = 1$ then $a\alpha + n\beta = 1$ with $\alpha, \beta \in \mathbb{Z}$.Then $[1] = [a][\alpha] + [n][\beta]$ $[n] = [0]$

assume $[a]$ is invertible. then there exists $[b]$ such that $[a][b] = 1, n|(ab-1)$. $ab - 1 = nk, (a, n) = 1$