

HOMEWORK 8
Math 109 - Dr. Chow
UCSD Winter 2003

5. In example 4, does there exist a member of Y that does not have an inverse with respect to composition? Prove your answer.

Example 4 has Y as the set of all functions from the nonempty set X onto X , and the operation is \circ . So the question becomes: "Does there exist a function $f : X \rightarrow X$ which is onto which has no inverse function?" If X is a finite set, the answer is no. Every onto function $f : X \rightarrow X$ would also be a one-to-one function, which means $f(x)$ has an inverse function $f^{-1} : X \rightarrow X$ such that $f^{-1} \circ f(x) = x$ and $f \circ f^{-1}(x) = x$.

If X is infinite, however, then there are functions which are onto but not one-to-one. For example, let $X = \mathbb{N}$. Define $f : \mathbb{N} \rightarrow \mathbb{N}$ by

$$f(n) = \begin{cases} \frac{n}{2} & \text{if } n \text{ is even} \\ \frac{n+1}{2} & \text{if } n \text{ is odd} \end{cases}$$

Then f is onto since for every natural number m , $f(2m) = m$. But it is not one-to-one because $f(1) = 1$ and $f(2) = 1$. Therefore, it cannot have an inverse function under \circ .

11. Complete the following table in such a way that $*$ is commutative and has an identity element, and each element has an inverse with respect to $*$.

$*$	a	b	c	d
a	d	b		
b	c	a		
c			a	
d				

Since $*$ is commutative, the Cayley table of $*$ must be symmetric across the diagonal. Hence, we can fill in

$*$	a	b	c	d
a	d	c	b	
b	c	a		
c	b		a	
d				

Now one of the four elements must be the identity, that is, when we combine any other element with the identity, we get the original element back. Looking through our list, a cannot be the identity, since $a * a \neq a$. Likewise, b and c cannot be the identity since $b * b \neq b$ and $c * c \neq c$. Therefore, d must be the identity. In that case, we know $d * a = a * d = a$, $d * b = b * d = b$, $d * c = c * d = c$, and $d * d = d$. So we can fill in the last row and last column of the table:

$*$	a	b	c	d
a	d	c	b	a
b	c	a		b
c	b		a	c
d	a	b	c	d

Finally, b must have an inverse, that is, there must be an element x such that $b * x = x * b$ is the identity element, which we've shown to be d . Since $b * a \neq d$, $b * b \neq d$, $b * c \neq d$, we must have $b * d = d * b = d$. Finally, we can complete the table:

*	a	b	c	d
a	d	c	b	a
b	c	a	d	b
c	b	d	a	c
d	a	b	c	d

14a. Prove that the operation \odot on \mathbb{Z}_n is commutative.

Since the integers are commutative, we know that $a \cdot b = b \cdot a$ as integers. So for all $[a], [b] \in \mathbb{Z}_n$, $[a] \odot [b] = [a \cdot b] = [b \cdot a] = [b] \odot [a]$. Hence, \odot is commutative.

14b. Prove that the operation \oplus on \mathbb{Z}_n is associative.

Since the integers are associative under $+$, we know $(a+b)+c = a+(b+c)$ as integers. So for all $[a], [b], [c] \in \mathbb{Z}_n$, $([a] \oplus [b]) \oplus [c] = ([a+b]) \oplus [c] = [(a+b)+c] = [a+(b+c)] = [a] \oplus ([b+c]) = [a] \oplus ([b] \oplus [c])$.

14c. Prove that the operation \odot on \mathbb{Z}_n is associative.

Since the integers are associative under \cdot , we know $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ as integers. So for all $[a], [b], [c] \in \mathbb{Z}_n$, $([a] \odot [b]) \odot [c] = ([a \cdot b]) \odot [c] = [(a \cdot b) \cdot c] = [a \cdot (b \cdot c)] = [a] \odot ([b \cdot c]) = [a] \odot ([b] \odot [c])$.

20. If $[a] \in \mathbb{Z}_n$ and $[a] \neq [0]$, then $[a]$ is a **divisor of zero** in \mathbb{Z}_n if there is a nonzero element $[b]$ of \mathbb{Z}_n such that $[a] \odot [b] = [0]$. Characterize those integers a such that the element $[a]$ of \mathbb{Z}_n is a divisor of zero in \mathbb{Z}_n .

Let's look at an example, $\mathbb{Z}_6 = \{[0], [1], [2], [3], [4], [5]\}$. $[0]$ is not a divisor of zero, since a divisor of zero is required to be nonzero. $[1]$ is not a divisor of zero, since if $[b] \neq [0]$, $[1] \odot [b] = [b] \neq [0]$. $[2]$ is a divisor of zero, since $[2] \odot [3] = [2 \cdot 3] = [6] = [0]$ in \mathbb{Z}_6 . Using the same equation, $[3]$ is a divisor of zero. $[4]$ is a divisor of zero also, since $[4] \odot [3] = [12] = [0]$. Finally, going through all the possibilities for $[b]$ in $[5] \odot [b]$ shows that $[5]$ is not a divisor of zero. So the complete list of divisors of zero are $\{[2], [3], [4]\}$. It appears that the a 's that are not relatively prime to 6 are divisors of zero. So that is what our characterization is:

Characterization 1. Let $[a] \in \mathbb{Z}_n$ and $[a] \neq [0]$. Then $[a]$ is divisor of zero in \mathbb{Z}_n if and only if a and n are not relatively prime.

PROOF: (\Leftarrow) Suppose that a and n are not relatively prime. Then $d = \gcd(a, n) > 1$. Let $b = \frac{n}{d}$. Since $d > 1$, $1 \leq b < n$, so $[b] \neq [0]$. Furthermore, $[a] \odot [b] = [a \cdot b] = [a \cdot \frac{n}{d}] = [\frac{a}{d} \cdot n]$. Since d is a common divisor of a and n , $a = kd$ for some integer k . Hence, $[a] \odot [b] = [k \cdot n] = [0]$ in \mathbb{Z}_n . Since $[b] \neq [0]$, we conclude that $[a]$ is a divisor of zero.

(\Rightarrow) We prove by contradiction. Assume that $[a]$ is a divisor of zero but a and n are relatively prime. By the first assumption, there exists a $[b] \neq [0]$ such that $[a] \odot [b] = [0]$. Since $\gcd(a, n) = 1$, there exist integers r and s such that $ar + ns = 1$. Multiplying both sides by b , we have $abr + nbs = b$. Then $[b] = [abr + nbs] = [abr] \oplus [nbs] = ([ab] \odot [r]) \oplus [0] = [0] \odot [r] = [0]$. But this is a contradiction with the assumption that $[b] \neq [0]$. Hence, a and n must not be relatively prime. \square