MATH 417, HOMEWORK 3

CHARLES ANCEL

Exercise 1.7.6 From Last Week. If an element $\mathbb{Z}_n$ has a multiplicative inverse, is that multiplicative inverse unique? That is, if $[a]$ is invertible, can there be two distinct elements $[b]$ and $[c]$ of $\mathbb{Z}_n$ such that $[a][b] = [1]$ and $[a][c] = [1]$?

Solution

We need to show whether the multiplicative inverse of an element in $\mathbb{Z}_n$ is unique. Specifically, we want to determine if there can be two distinct elements $[b]$ and $[c]$ in $\mathbb{Z}_n$ such that $[a][b] = [1]$ and $[a][c] = [1]$.

Proof.

Assume that $[a]$ is an invertible element in $\mathbb{Z}_n$. Suppose there exist two elements $[b]$ and $[c]$ in $\mathbb{Z}_n$ such that:

$$[a][b] = [1] \quad \text{and} \quad [a][c] = [1].$$

This implies:

$$ab \equiv 1 \pmod{n} \quad \text{and} \quad ac \equiv 1 \pmod{n}.$$

Showing b and c Must Be Congruent Modulo n. Since $[a]$ has a multiplicative inverse, there exists some integer k such that:

$$ab = 1 + kn \quad \text{for some integer } k.$$

Similarly, there exists some integer m such that:

$$ac = 1 + mn \quad \text{for some integer } m.$$

We need to show that $b \equiv c \pmod{n}$.

Starting from the equations $ab \equiv 1 \pmod{n}$ and $ac \equiv 1 \pmod{n}$, we have:

$$ab \equiv ac \pmod{n}.$$

Since $a \in \mathbb{Z}_n$ and a is invertible, there exists an inverse $[a]^{-1}$ such that:

$$[a][a]^{-1} = [1].$$

Multiplying both sides of $ab \equiv ac \pmod{n}$ by $[a]^{-1}$, we get:

$$b \equiv c \pmod{n}.$$

Conclusion. Thus, b and c are congruent modulo n, meaning $[b] = [c]$ in $\mathbb{Z}_n$. Therefore, the multiplicative inverse of $[a]$ in $\mathbb{Z}_n$ is unique.

$\square$

Exercise 2. Let p, q, r be distinct primes, and let $n = pqr$ and $m = (p-1)(q-1)(r-1)$. Show that for any $a \in \mathbb{Z}$ and $h \in \mathbb{N}$ that

$$h \equiv 1 \pmod{m} \text{ implies } a^h \equiv a \pmod{n}$$

Solution

To show that $a^h \equiv a \pmod{n}$ if $h \equiv 1 \pmod{m}$, where $m = (p-1)(q-1)(r-1)$ and $n = pqr$, we will use the properties of modular arithmetic and Euler's theorem.

Proof.

Let $a \in \mathbb{Z}$ and $h \in \mathbb{N}$ such that $h \equiv 1 \pmod{m}$. That is, there exists an integer k such that:

$$h = 1 + km.$$

We need to show that:

$$a^h \equiv a \pmod{n}.$$

Application of Euler's Theorem. Euler's theorem states that if a is coprime to p, q, and r (i.e., $\gcd(a,p) = \gcd(a,q) = \gcd(a,r) = 1$), then:

$$a^{p-1} \equiv 1 \pmod{p}, \quad a^{q-1} \equiv 1 \pmod{q}, \quad a^{r-1} \equiv 1 \pmod{r}.$$

Since $m = (p-1)(q-1)(r-1)$, we know that m is a common multiple of $(p-1)$, $(q-1)$, and $(r-1)$. Therefore:

$$a^m \equiv 1 \pmod{p}, \quad a^m \equiv 1 \pmod{q}, \quad a^m \equiv 1 \pmod{r}.$$

Since $h = 1 + km$, we have:

$$a^h = a^{1+km} = a \cdot (a^m)^k.$$

Using the property $a^m \equiv 1 \pmod{p}$, $a^m \equiv 1 \pmod{q}$, and $a^m \equiv 1 \pmod{r}$:

$$a^h \equiv a \cdot 1^k \equiv a \pmod{p}, \quad a^h \equiv a \cdot 1^k \equiv a \pmod{q}, \quad a^h \equiv a \cdot 1^k \equiv a \pmod{r}.$$

Combining Results. By the Chinese Remainder Theorem (CRT), since p, q, and r are distinct primes, the congruences:

$$a^h \equiv a \pmod{p}, \quad a^h \equiv a \pmod{q}, \quad a^h \equiv a \pmod{r}$$

imply that:

$$a^h \equiv a \pmod{pqr}.$$

Therefore:

$$a^h \equiv a \pmod{n}.$$

Conclusion. For any $a \in \mathbb{Z}$ and $h \in \mathbb{N}$, if $h \equiv 1 \pmod{m}$, then $a^h \equiv a \pmod{n}$, where $n = pqr$ and $m = (p-1)(q-1)(r-1)$.

$\square$

Exercise 1.9.10. Let p be a prime number, $k \in \mathbb{Z}$, and $s \in \mathbb{Z}_{\geq 0}$. Show that

$$(1+kp)^{p^s} \equiv 1 + kp^{s+1} \pmod{p^{s+1}}$$

(Hint: induction on s.)

Solution

We will use mathematical induction on s to prove that

$$(1+kp)^{p^s} \equiv 1 + kp^{s+1} \pmod{p^{s+1}}.$$

Proof.

Base Case $s = 0$. For $s = 0$:

$$(1+kp)^{p^0} = (1+kp)^1 = 1 + kp.$$

We need to show:

$$1 + kp \equiv 1 + kp \pmod{p}.$$

This is trivially true since both sides are identical.

Inductive Step. Assume the statement holds for some $s = n$, that is:

$$(1+kp)^{p^n} \equiv 1 + kp^{n+1} \pmod{p^{n+1}}.$$

We need to show it holds for $s = n+1$, i.e.:

$$(1+kp)^{p^{n+1}} \equiv 1 + kp^{n+2} \pmod{p^{n+2}}.$$

Using the inductive hypothesis:

$$(1+kp)^{p^n} = 1 + kp^{n+1} + p^{n+1}x \quad \text{for some integer } x.$$

Raise both sides to the power p:

$$(1+kp)^{p^{n+1}} = \left[(1+kp)^{p^n}\right]^p.$$

Expanding using the binomial theorem:

$$\left[1 + kp^{n+1} + p^{n+1}x\right]^p = \sum_{i=0}^{p} \binom{p}{i} (1 + kp^{n+1})^{p-i} (p^{n+1}x)^i.$$

Simplify the terms modulo p^{n+2}: - For $i = 0$:

$$\binom{p}{0} (1 + kp^{n+1})^p (p^{n+1}x)^0 = (1 + kp^{n+1})^p.$$

Using the binomial theorem again:

$$(1 + kp^{n+1})^p = 1 + p(kp^{n+1}) + \binom{p}{2} (kp^{n+1})^2 + \cdots \equiv 1 + kp^{n+2} \pmod{p^{n+2}}.$$

- For $i > 0$:

$$\binom{p}{i}(1+kp^{n+1})^{p-i}(p^{n+1}x)^i \equiv 0 \pmod{p^{n+2}}$$

since $p^{n+1}x$ is divisible by p^{n+1} and thus p^{n+2}.

Summing all terms modulo p^{n+2}:

$$(1+kp)^{p^{n+1}} = (1+kp)^{p^n \cdot p} = 1 + kp^{n+2} \pmod{p^{n+2}}.$$

Conclusion. By induction, the statement holds for all $s \geq 0$:

$$(1+kp)^{p^s} \equiv 1 + kp^{s+1} \pmod{p^{s+1}}.$$

$\square$

Exercise 4. Compute the multiplication table for $\Phi(8)$.

Solution

Finding Elements of $\mathbb{Z}_8^*$. The set $\mathbb{Z}_8^*$ (the group of units modulo 8) consists of the integers less than 8 that are coprime to 8. An integer a is coprime to 8 if $\gcd(a, 8) = 1$.

We check each integer from 1 to 7:

- $\gcd(1, 8) = 1 \implies 1 \in \mathbb{Z}_8^*$
- $\gcd(2, 8) = 2 \implies 2 \notin \mathbb{Z}_8^*$
- $\gcd(3, 8) = 1 \implies 3 \in \mathbb{Z}_8^*$
- $\gcd(4, 8) = 4 \implies 4 \notin \mathbb{Z}_8^*$
- $\gcd(5, 8) = 1 \implies 5 \in \mathbb{Z}_8^*$
- $\gcd(6, 8) = 2 \implies 6 \notin \mathbb{Z}_8^*$
- $\gcd(7, 8) = 1 \implies 7 \in \mathbb{Z}_8^*$

Thus, the elements of $\mathbb{Z}_8^*$ are:

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\}.$$

Multiplication Table for $\mathbb{Z}_8^*$. We compute the products of these elements modulo 8:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	$9 \equiv 1$	$15 \equiv 7$	$21 \equiv 5$
5	5	$15 \equiv 7$	$25 \equiv 1$	$35 \equiv 3$
7	7	$21 \equiv 5$	$35 \equiv 3$	$49 \equiv 1$

The multiplication table for $\mathbb{Z}_8^*$ is:

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Exercise 5. Let G be the set of all functions $\mathbb{N} \to \mathbb{N}$.

- **a.** Show that $(G, \circ)$, where $f, g \mapsto f \circ g$ is the operation of composition of functions, is a monoid, but not a group.
- **b.** Give an example of elements $f, g \in G$ such that $f \circ g = \mathrm{id}$, but $g \circ f \neq \mathrm{id}$. (So an element in a monoid with a "one-sided inverse" might not have an actual inverse.)

Solution

a. Showing that $(G, \circ)$ is a Monoid but not a Group.

Proof.

To show that $(G, \circ)$ is a monoid, we need to verify two properties: associativity and the existence of an identity element.

Associativity. Let $f, g, h \in G$. We need to show that function composition is associative:

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

For any $x \in \mathbb{N}$:

$$f \circ (g \circ h)(x) = f(g(h(x))) = (f \circ g)(h(x)) = (f \circ g) \circ h(x).$$

Since this holds for all $x \in \mathbb{N}$, function composition is associative.

Identity Element. The identity function $\mathrm{id} \in G$ is defined by:

$$\mathrm{id}(x) = x \quad \text{for all } x \in \mathbb{N}.$$

We need to show that id is the identity element for function composition:

$$f \circ \mathrm{id} = f \quad \text{and} \quad \mathrm{id} \circ f = f.$$

For any $x \in \mathbb{N}$:

$$f \circ \mathrm{id}(x) = f(\mathrm{id}(x)) = f(x),$$
$$\mathrm{id} \circ f(x) = \mathrm{id}(f(x)) = f(x).$$

Since these hold for all $f \in G$, id is the identity element.

Not a Group. To show that $(G, \circ)$ is not a group, we need to show that there exists at least one element in G that does not have an inverse.

Consider the function $f \in G$ defined by:

$$f(x) = x + 1.$$

Assume there exists $g \in G$ such that $f \circ g = \mathrm{id}$ and $g \circ f = \mathrm{id}$. For $f \circ g = \mathrm{id}$, we need:

$$f(g(x)) = x \implies g(x) + 1 = x \implies g(x) = x - 1.$$

For $g \circ f = \mathrm{id}$, we need:

$$g(f(x)) = x \implies g(x + 1) = x \implies (x + 1) - 1 = x.$$

However, $g(x) = x - 1$ is not a valid function from $\mathbb{N}$ to $\mathbb{N}$ because it maps 0 to -1, which is not in $\mathbb{N}$. Therefore, f does not have an inverse in G.

Thus, $(G, \circ)$ is a monoid but not a group.

□

b. Example of One-Sided Inverse.

Proof.

Consider the functions $f, g \in G$ defined by:

$$f(x) = \begin{cases} 0 & \text{if } x = 0, \\ x - 1 & \text{if } x > 0. \end{cases}$$

$$g(x) = x + 1.$$

We show that $f \circ g = \text{id}$ but $g \circ f \neq \text{id}$.

Verification. For $f \circ g$:

$$(f \circ g)(x) = f(g(x)) = f(x+1) = (x+1) - 1 = x \quad \text{for all } x \in \mathbb{N}.$$

Thus:

$$f \circ g = \text{id}.$$

For $g \circ f$:

$$(g \circ f)(x) = g(f(x)) = g\left(\begin{cases} 0 & \text{if } x = 0, \\ x - 1 & \text{if } x > 0. \end{cases}\right) = \begin{cases} g(0) = 1 & \text{if } x = 0, \\ g(x-1) = x & \text{if } x > 0. \end{cases}$$

Thus:

$$g \circ f(0) = 1 \neq 0 \quad \text{and} \quad g \circ f(x) = x \quad \text{for } x > 0.$$

Conclusion. We have $f \circ g = \text{id}$ but $g \circ f \neq \text{id}$. This demonstrates that an element in a monoid with a one-sided inverse might not have an actual inverse.

□

Exercise 2.1.10. Show that any group with four elements must have a nonidentity element whose square is the identity. That is, some nonidentity element must be its own inverse. (See description of problem in Goodman for hints.)

Solution

Let G be a group with four elements. We need to show that there is a nonidentity element $a \in G$ such that $a^2 = e$, where e is the identity element in G.

Structure of Group G

Let the elements of G be $\{e, a, b, c\}$, where e is the identity element.

Case 1: All Nonidentity Elements Are Their Own Inverse.

- Suppose $a^2 = e$, $b^2 = e$, and $c^2 = e$.
- In this case, each nonidentity element is its own inverse.
- Hence, there is nothing more to show.

Case 2: Some Element Does Not Have Its Square Equal to the Identity.

- Suppose $a^2 \neq e$.
- Then $a \neq a^{-1}$, so the inverse a^{-1} must be one of the other nonidentity elements. Without loss of generality, let $b = a^{-1}$.
$$b = a^{-1} \quad \text{and} \quad a = b^{-1}.$$
- We then have:
$$a^2 = ab = e \quad \text{and} \quad b^2 = ba = e.$$

Determine the Structure of c

- The element c must also satisfy $c = c^{-1}$. We must check the possible squares of c:
  - If $c \neq e$ and $c \neq a$ and $c \neq b$, it implies $c^2 = e$.
  - For c, we check the possibility of it forming any additional elements, but since G is closed and there are only 4 elements, c must be either a or b already included in G, or its own inverse.

Verification with Concrete Examples

Cyclic Group $\mathbb{Z}_4$.

- The elements are $\{0, 1, 2, 3\}$ with addition modulo 4.
- The elements 1 and 3 are their own inverses because:
$$1 + 1 = 2 \equiv 0 \pmod 4, \quad 3 + 1 = 4 \equiv 0 \pmod 4.$$

Klein Four-Group V_4.

- The elements are $\{e, r_1, r_2, r_3\}$, where each r_i (nonidentity) has its square equal to e.

Conclusion

In both possible cases, at least one nonidentity element of the group G has its square equal to the identity element. Therefore, any group with four elements must have a non-identity element that is its own inverse.