

# P1

MATH 541 HW1 | Harry Luo

Proof:

1. First, prove the relation to be equivalent:

- Reflective:  $a \sim a \Rightarrow f(a) = f(a)$ , TRUE.
- Symmetric:  $a \sim b \Rightarrow f(a) = f(b) \Rightarrow f(b) = f(a) \Rightarrow b \sim a$ , TRUE.
- transitive:  $a \sim b, b \sim c \Rightarrow f(a) = f(b), f(b) = f(c) \Rightarrow f(a) = f(c) \Rightarrow a \sim c$ , TRUE.

2. Then, prove its equivalence classes to be the fibers of  $f$ :

Let  $C$  be the set of equivalence classes of  $A$  under  $\sim$ , and let  $F$  be the set of fibers of  $f$ . We will show that  $C = F$ .

Take an arbitrary element  $a \in A$ . The equivalence class of  $a \in A$  is:

$$\begin{aligned} \{x \in A \mid x \sim a\} &= \{x \in A \mid f(x) = f(a)\} \\ &= f^{-1}\{f(a)\} \end{aligned} \tag{1}$$

which by definition is the fiber of  $f$ .

Since  $a$  was arbitrary, every equivalence class is a fiber of  $f$ , i.e.  $C \subseteq F$ .

Conversely, let  $F'$  be an arbitrary fiber of  $f$  for some  $b \in B$ . Then by definition,

$$\begin{aligned} F' &= f^{-1}\{b\} \\ &= \{x \in A \mid f(x) = b\} \end{aligned} \tag{2}$$

Since  $f$  is surjective,  $\exists a \in A$  s.t.  $f(a) = b$ . Consider the equivalence class of  $a$ :

$$\begin{aligned} \{x \in A \mid x \sim a\} &= \{x \in A \mid f(x) = f(a)\} \\ &= \{x \in A \mid f(x) = b\} \\ &= F'. \end{aligned} \tag{3}$$

Since  $F'$  was arbitrary, every fiber of  $f$  is an equivalence class, i.e.  $F \subseteq C$ . Thus,  $C = F$ . ■

## P2

Prove by contradiction:

1. Consider an arbitrary **column** in the multiplication table of  $G$ . Suppose that the column is *not* a permutation of  $G$ .

Then there would be at least two identical elements in this column, which we denote as  $a$ . This implies that

$$\exists x, y \in G, x \neq y, s.t. xa = ya \quad (4)$$

Applying  $x^{-1}$  from right on both sides:

$$\begin{aligned} x^{-1}xa &= x^{-1}ya \\ a &= x^{-1}ya \\ \Rightarrow x^{-1}y &= e. \end{aligned} \quad (5)$$

Since inverse of an element is unique,  $y = x$ , which is a contradiction.

2. Similarly, consider arbitrary **row** in the multiplication table of  $G$ . Suppose that this row is *not* a permutation of  $G$ , i.e. there are at least two repeating elements, denoted as  $b$ . This implies

$$\exists x, y \in G, x \neq y, s.t. xa = xb. \quad (6)$$

Applying  $a^{-1}$  from left on both sides:

$$\begin{aligned} xaa^{-1} &= xba^{-1} \\ x &= xba^{-1} \\ \Rightarrow ba^{-1} &= e. \end{aligned} \quad (7)$$

Since inverse of an element is unique,  $b = a$ , a contradiction. ■

3. Multiplication tables are special cases of Latin squares. In particular, they hold the property of associativity. This restricts the set of possible Latin squares, because:

The group operation must be associative, meaning for every single combination of three elements,  $a, b, c \in G$ ,  $(ab)c = a(bc)$ .

In a table, this means:

- let entry  $(a, b) := d$  and entry  $(d, c) := e$ , then we must have entry  $(d, c)$  equal to entry  $(a, e)$ .

This is a strong restriction on the possible arrangements of elements in a Latin square, and thus only a small subset of Latin squares can be multiplication tables of groups.

### P3

We check each axiom one by one:

#### Closure: Satisfied.

For any  $a, b \in \mathbb{R}$ ,  $a + b \in \mathbb{R}_{\text{ext}}$ .

If at least one of the numbers is  $\infty$ , the sum is  $\infty \in \mathbb{R}_{\text{ext}}$ .

#### associativity: Satisfied.

We want to show that for any  $a, b, c \in \mathbb{R}_{\text{ext}}$ ,  $(a + b) + c = a + (b + c)$ . We have two cases:

- If all elements are real, then the sum is trivially associative.
- If at least one element is  $\infty$ , then both sides equal  $\infty$ .

#### Identity: Satisfied.

The identity element is  $0 \in \mathbb{R}_{\text{ext}}$ . For any  $a \in \mathbb{R}_{\text{ext}}$ ,  $a + 0 = 0 + a = a$ .

#### Inverse: NOT satisfied.

Assume not, then for  $\infty \in \mathbb{R}_{\text{ext}}$ ,  $\exists a \in \mathbb{R}_{\text{ext}} \text{ s.t. } a + \infty = 0$ . This is a contradiction, since  $a + \infty = \infty$  for any  $a \in \mathbb{R}_{\text{ext}}$ .

Therefore,  $(\mathbb{R}_{\text{ext}}, +)$  is not a group. ■

**P4**

$$G = \{z \in \mathbb{C} \mid z^n = 1 \text{ for some } n \in \mathbb{Z}^+\} \quad (8)$$

**a. Prove that G is a group under multiplication.**

We check for each axiom:

**Closure:**

let  $a, b \in G$ , then  $a^{n_1} = 1, b^{n_2} = 1$ , for some  $n_1, n_2 \in \mathbb{Z}^+$ . Need to show that  $ab \in G \Leftrightarrow (ab)^k = 1$  for some  $k \in \mathbb{Z}^+$ .

Take  $k = n_1 n_2$ , then

$$(ab)^k = a^{n_1 n_2} b^{n_1 n_2} = 1^{n_2} 1^{n_1} = 1. \quad (9)$$

Exists such  $k$ , and so  $ab \in G$ , i.e. closure is satisfied.

**Assoc.**

Trivially satisfied, as  $G \subset \mathbb{C}$ , each element is a complex number, and multiplication of complex numbers is associative.

**Identity.**

Trivially satisfied, as  $1 \in G$  (take  $n = 1$ ), and for any  $a \in G$ ,  $a1 = 1a = a$ .

**Inverse.**

Consider arbitrary  $a \in G$ . Exists  $n \in \mathbb{Z}^+$  s.t.  $a^n = 1$ . Rewriting,

$$a^{n-1}a = 1 \Rightarrow a^{n-1} = a^{-1}. \quad (10)$$

Since  $(z^{n-1})^n = (z^n)^{n-1} = 1, z^{n-1} \in G$ .

Therefore,  $(G, \times)$  is a group. ■

**b.  $(G, +)$  is not a group.**

Assume identity exists, then for any  $a \in G$ ,

$$e + a = a + e = a. \quad (11)$$

Since  $a, e \in \mathbb{C}$ , the identity must be 0. However,  $0 \notin G$ , since  $0^n = 0$  for any  $n \in \mathbb{Z}^+$ , a contradiction. Thus the identity axiom is failed. ■

## P5

We check the four axioms:

### Closure:

As given in the problem,  $H$  is closed under  $\star$ .

### Associativity:

Since  $H \subset G$  and  $\star$  is associative on  $G$ ,  $\star$  is also associative on  $H$ .

### Inverse:

We are given that  $H$  is closed under inverse, and so the inverse axiom is satisfied.

### Identity:

Since  $H$  is nonempty, take arbitrary  $h \in H$ . Since  $H$  is closed under inverse,  $h^{-1} \in H$ . Now, we have:

$$h \star h^{-1} = h^{-1} \star h := e. \quad (12)$$

This identity element must exist in  $H$  by closure of  $H$  under  $\star$ . Thus, the identity axiom is satisfied.

## P6

$(A, \star)$  and  $(B, \diamond)$  are groups.  $A \times B := \{(a, b) \mid a \in A, b \in B\}$  with operation:  $(a, b)(c, d) = (a \star c, b \diamond d)$  for all  $(a, b), (c, d) \in A \times B$ .

### 1. Check group axioms:

#### Closure:

Take arbitrary  $(a_1, b_1)$  and  $(a_2, b_2) \in A \times B$ . Then,

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2). \quad (13)$$

Since  $A$  and  $B$  are groups,  $a_1 \star a_2 \in A$  and  $b_1 \diamond b_2 \in B$ . Thus,  $(a_1 \star a_2, b_1 \diamond b_2) \in A \times B$ , i.e. closure is satisfied.

#### Associativity:

Take arbitrary  $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$ . Then,

$$\begin{aligned} [(a_1, b_1)(a_2, b_2)](a_3, b_3) &= (a_1 \star a_2, b_1 \diamond b_2)(a_3, b_3) \\ &= ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) \\ &= (a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)) \\ &= (a_1, b_1)(a_2 \star a_3, b_2 \diamond b_3) \\ &= (a_1, b_1)[(a_2, b_2)(a_3, b_3)]. \end{aligned} \quad (14)$$

and so associativity is satisfied.

#### Identity:

Take arbitrary  $(a, b) \in A \times B$ . Let  $e_A$  and  $e_B$  be the identity elements of  $A$  and  $B$  respectively. Then,

$$(a, b)(e_A, e_B) = (a \star e_A, b \diamond e_B) = (a, b) \quad (15)$$

and similarly,  $(e_A, e_B)(a, b) = (e_A \star a, e_B \diamond b) = (a, b)$ . Thus, the identity axiom is satisfied with identity element  $(e_A, e_B)$ .

#### Inverse:

Take arbitrary  $(a, b) \in A \times B$ . Let  $a^{-1}$  and  $b^{-1}$  be the inverses of  $a$  and  $b$  in  $A$  and  $B$  respectively. Then,

$$(a, b)(a^{-1}, b^{-1}) = (a \star a^{-1}, b \diamond b^{-1}) = (e_A, e_B). \quad (16)$$

Similarly,  $(a^{-1}, b^{-1})(a, b) = (e_A, e_B)$  and so the inverse axiom is satisfied. ■

### 2. Prove that $A \times B$ is abelian iff both $(A, \star)$ and $(B, \diamond)$ are abelian.

$\Rightarrow$ : Assume  $A \times B$  is abelian, then for any  $a_1, a_2 \in A$  and  $b_1, b_2 \in B$ , we have:

$$(a_1, b_1)(a_2, b_2) = (a_2, b_2)(a_1, b_1). \quad (17)$$

LHS:

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2). \quad (18)$$

RHS:

$$(a_2, b_2)(a_1, b_1) = (a_2 \star a_1, b_2 \diamond b_1). \quad (19)$$

Thus  $a_1 \star a_2 = a_2 \star a_1$  and  $b_1 \diamond b_2 = b_2 \diamond b_1$ , and so  $A$  and  $B$  are abelian.

$\Leftarrow$ : Assume both  $(A, \star)$  and  $(B, \diamond)$  are abelian, then for any  $a_1, a_2 \in A$  and  $b_1, b_2 \in B$ , we have:

$$(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2) = (a_2 \star a_1, b_2 \diamond b_1) = (a_2, b_2)(a_1, b_1). \quad (20)$$

This shows that  $A \times B$  is abelian. ■

## P7

**1. Prove that**  $xy = yx$  iff  $y^{-1}xy = x$  iff  $x^{-1}y^{-1}xy = 1$ .

- Start from left.

Suppose  $xy = yx$ , applying  $y^{-1}$  on both sides gives  $y^{-1}xy = y^{-1}yx = x$ .

Conversely, suppose  $y^{-1}xy = x$ , then  $yy^{-1}xy = yx \Rightarrow xy = yx$ . The first equivalence is proved.

- Now suppose  $y^{-1}xy = x$ . Applying  $x^{-1}$  on both sides gives  $x^{-1}y^{-1}xy = x^{-1}x = 1$ .

Conversely, suppose  $x^{-1}y^{-1}xy = 1$ . Applying  $x$  on both sides gives  $xx^{-1}y^{-1}xy = x \Rightarrow y^{-1}xy = x$ . The second equivalence is proved, thus completing the proof. ■

**2. Prove further that**  $|yxy^{-1}| = |x|$ .

Let  $|x| = n$  and  $|yxy^{-1}| = m$

- First, prove that  $m \leq n$ : Since  $x^n = e$ , expanding  $(yxy^{-1})$ :

$$\begin{aligned} yxy^{-1}yxy^{-1}\dots yxy^{-1}(n \times) &= yx^n y^{-1} \\ &= yey^{-1} \\ &= e. \end{aligned} \tag{21}$$

And so  $m$  divides  $n$ , i.e.  $m \leq n$ .

- Then, prove that  $n \leq m$ : Since  $(yxy^{-1})^m = e$ , expanding  $(yxy^{-1})^m$  in the same way gives

$$yx^m y^{-1} = e \Rightarrow y^{-1}x^m y^{-1}y = e \Rightarrow x^m = e \tag{22}$$

and so  $n$  divides  $m$ , i.e.  $n \leq m$ .

Thus we have  $m = n$ , i.e.  $|yxy^{-1}| = |x|$ . ■

**3. Prove that**  $|xy| = |yx| \forall x, y \in G$ .

From part 2, we know that for any  $g, h \in G$ ,  $|g| = |hgh^{-1}|$ . Now let  $g = xy$  and  $h = x^{-1}$ , then we can show:

$$|xy| = |x^{-1}(xy)(x^{-1})^{-1}| = |x^{-1}xyx| = |yx| \tag{23}$$

Thus  $|xy| = |yx| \forall x, y \in G$ . ■

**P8**

As hinted,  $t(G) = \{g \in G \mid g \neq g^{-1}\}$ . Consider any  $g \in t(G)$ , then  $g^{-1} \in t(G)$  as well.

This implies that  $g$  and  $g^{-1}$  are distinct, and so  $t(G)$  is composed of pairs of elements, and so  $|t(G)|$  is even.

Since  $|G|$  is also even,  $|G| - |t(G)|$  is even.

Now,  $G - t(G)$  is nonempty since the identity  $e \notin t(G)$ . Thus exists

$$a \neq e \text{ s.t. } a \in G - t(G). \quad (24)$$

We chose  $a \notin t(G)$ , then  $a = a^{-1}$  so that  $a^2 = e, a \neq e$ . This implies that  $a$  is an element of order 2. ■