# Math 71: Abstract Algebra

Prishita Dharampal

**Problem 1**. Determine whether the following functions $f$ are well-defined:

1. $f : \mathbb{Q} \to \mathbb{Z}$ defined by $f(a/b) = a$
2. $f : \mathbb{Q} \to \mathbb{Q}$ defined by $f(a/b) = a^2/b^2$

*Solution.*

1. $f$ is not well defined.
   $f(1/2) = 1, f(2/4) = 2$ but,
   $1/2 = 2/4$ therefore, $f$ is ambiguous and not well-defined.

2. $f$ is well-defined.
   $f(1/2) = 1/4, f(2/4) = 4/16$ and,
   $4/16 = 1/4$
   thus, $f$ is unambiguous and well-defined.

**Problem 2**. Let $f : A \to B$ be a surjective map of sets. Prove that the relation

$$a \sim b \text{ if and only if } f(a) = f(b)$$

is an equivalence relation whose equivalence classes are the fibers of $f$.

*Solution.*

To see if $\sim$ is an equivalence relation for any $a, b \in A$:

1. $a = a \implies f(a) = f(a), \forall a \in A$. Thus, the relation is reflexive, $a \sim a$.
2. From definition for any $a, b \in A$,
   if $a = b \implies f(a) = f(b) \implies f(b) = f(a)$. Thus, the relation is symmetric, $a \sim b \implies b \sim a$.
3. And by transitivity of $=$, if $f(a) = f(b)$ and $f(b) = f(c)$ then $f(a) = f(c)$. Which also means if $a = b, b = c \implies a = c, \forall a, b, c \in A$. Thus, the relation is transitive, $a \sim b$ and $b \sim c \implies a \sim c$.

Thus the relation $a \sim b$ on set $A$ is an equivalence relation.
If $f(a) = b$ for any $a \in A, b \in B$, then the fiber over b is $f^{-1}(b) = F_b$, such that $F_b \subset A$. $\forall x, y \in F_b$ we know that $f(x) = f(y) = b$. Thus, $x \sim y$.
Thus, all elements in the fiber over $b$ exist in the same equivalence class say, $A_b$.
Moreover, $\forall z \in A_b$, $z \sim x$, then $f(z) = f(x) = b$. Which implies that $z \in F_b$. Thus, there exists a 1-to-1 relationship between the fibers of $f$ and the equivalence classes in $A$.

**Problem 3**. Prove that for any given positive integer $N$, there exist only finitely many integers $n$ with $\varphi(n) = N$, where $\varphi$ denotes Euler's $\varphi$-function. Conclude in particular that $\varphi(n)$ tends to infinity as $n$ tends to infinity.

*Solution.*

For Euler's $\varphi-$function we know that,

1. $\varphi(ab) = \varphi(a)\varphi(b)$, if $(a, b) = 1$.
2. $\varphi(p^a) = p^{a-1}(p-1)$, for a prime $p$, and any $a \geq 1$.

Let $n = q^a b$, where $q$ is the biggest prime factor $n$ has. Then:

$$N = \varphi(n) = \varphi(q^a b)$$
$$N = \varphi(q^a b) = \varphi(q^a)\varphi(b)$$
$$N = q^{a-1}(q-1)\varphi(b)$$

Since we know that $N, \varphi(b) \in \mathbb{Z}^+$, $a \geq 1$, we can say that $q < N$. Thus, there are only a finite possibilities for $1 < q < N$, for any fixed $N$.

We also know that $q^{a-1} \leq N$, hence, $q^{a-1} < N$. So,

1. $n$ can only contain some subset of a finite number of primes,
2. and for each prime in $n$, there can only be a finite number of different powers that it can be raised to.

So only a finite number of $n$ can be generated using $q, a$. Hence, there only exist finitely many integers $n$ with $\varphi(n) = N$.

To see that $\varphi(n)$ tends to infinity, as $n$ tends to infinity, let's consider that set $P = \{p_1, \ldots, p_n\}$ for a finite number of primes. Then we know that for a $n = p_1 p_2 \ldots p_n + 1$, n has a prime divisor p.

$$p \mid n = p \mid (p_1 p_2 \ldots p_n + 1)$$

But $p \notin P$, because if $p \in P$ then:

$$p \mid n = p \mid p_1 p_2 \ldots p_n + p \mid 1$$

and $p \mid 1$ cannot be true (Euler's proof for infinite primes). Thus, there are infinite primes, and as $n \to \infty$, $N$ accumulates more primes and thus also tends to infinity.

**Problem 4**. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \le a \le n$. Prove that if $a$ and $n$ are not relatively prime, there exists an integer $b$ with $1 \le b < n$ such that $ab \equiv 0 \pmod{n}$, and deduce that there cannot be an integer $c$ such that $ac \equiv 1 \pmod{n}$.

*Solution.*

Given that $a, n$ are not relatively prime, there exists a gcd $d > 1$ such that:

$$\begin{aligned} a(\text{mod d}) &\equiv n(\text{mod d}) \equiv 0 \\ n &= n'd, n' < n \\ a &= a'd, a' < a, n \\ a &= a'd \text{ (multiplying both sides by n')} \\ an' &= a'dn' = ab \\ ab &\equiv 0 \text{ (mod n)} \end{aligned}$$

i.e. an integer $b$ exists such that $1 \le b < n$.

Assuming $ac \equiv 1$ (mod n):

$$\begin{aligned} ac &\equiv 1 \text{ (mod n)} \\ acb &\equiv 1b \text{ (mod n)} \\ (ab)c &\equiv b \text{ (mod n), integers are commutative} \\ 0c &\equiv b \text{ (mod n)}, ab \equiv 0 (\text{mod n}) \\ 0 &\equiv b \text{ (mod n)} \end{aligned}$$

This implies $b \ge n$ but from the first proof, $b < n$. Thus, this is a contraction and $c$ cannot exist if $a, n$ are not co-prime.

**Problem 5**. Let $n \in \mathbb{Z}$, $n > 1$, and let $a \in \mathbb{Z}$ with $1 \leq a \leq n$. Prove that if $a$ and $n$ are relatively prime, there exists an integer $c$ such that $ac \equiv 1 \pmod{n}$. [use the fact that the g.c.d. of two integers is a $\mathbb{Z}$-linear combination of the integers]

*Solution.*

Given that $a, n$ are relatively prime, the gcd $d = 1$.

$$\begin{aligned} d &= ax + ny, \text{ where } x, y \in \mathbb{Z} \\ 1 &= ax + ny \\ -ny &= ax - 1 \\ 0 &\equiv ax - 1 \text{ (mod n)} \\ 1 &\equiv ax \text{ (mod n)} \end{aligned}$$

Thus, an integer $x$ or $c$ exists such that $ac \equiv 1$ (mod n) if $a$ and $n$ are co-prime.

**Problem 6**. Conclude from the previous two exercises that $(\mathbb{Z}/n\mathbb{Z})^\times$ is the set of elements $\bar{a}$ of $\mathbb{Z}/n\mathbb{Z}$ with $(a, n) = 1$ and hence prove Proposition 4. Verify this directly in the case $n = 12$.

*Solution.*

From the above two solutions we know:

1. $(a, n) = 1 \implies \exists c, ac \equiv 1,$ (mod n)
2. $(a, n) > 1 \implies \nexists c, ac \equiv 1,$ (mod n)

Hence $\forall a, n : (a, n) > 1$, there exists no multiplicative inverse for $a \in \mathbb{Z}/n\mathbb{Z}$ because there exists no $c < n : ac \equiv 1$ (mod n). However, for co-prime $a, n$, a $c < n : ac \equiv 1$ (mod n) exists. Thus the latter set has multiplicative inverses. It is also closed under multiplication because $\forall a, b \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1 \& (b, n) = 1 \implies (ab, n) = 1$.
(The other 2 axioms - associativity and identity element = 1 are inherited from $\mathbb{Z}$).
Thus, $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} : (a, n) = 1\}$, where $\bar{a}$ is the equivalence class for all $a$ such that $ac \equiv 1$ (mod n).

**Problem 7**. Determine which of the following sets are groups under addition:

1. The set of rational numbers (including $0 = 0/l$) in lowest terms whose denominators are odd.
2. The set of rational s(including $0 = 0/l$) in lowest terms whose denominators are even.
3. The set of rational numbers of absolute value $< 1$.
4. The set of rational numbers of absolute value $\geq 1$ together with 0.
5. The set of rational numbers with denominators equal to 1 or 2.
6. The set of rational numbers with denominators equal to 1, 2 or 3.

*Solution.*

1. The set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are odd.
   Let this set be called $A$. Let's see if the axioms hold for this set under addition: $\forall \frac{a}{b}, \frac{c}{d} \in A$
   (a) Associativity: inherited from $\mathbb{Q}$.
   (b) Closure: $\frac{a}{b} + \frac{c}{d} = \frac{a+c}{bd}$, if b, d are odd, then bd is odd.
   (c) Identity: $\frac{a}{b} + 0/1 = \frac{a}{b} = 0/1 + \frac{a}{b}$
   (d) Inverse element: $\frac{a}{b} + (-\frac{a}{b}) = 0/1$, if b is odd then -b is also odd.

   Thus, this set is a group under addition.

2. The set of rational numbers (including $0 = 0/1$) in lowest terms whose denominators are even.
   For $\frac{1}{2} \in$ the set. $\frac{1}{2} + \frac{1}{2} = \frac{2}{2} = 1$(lowest terms). And 1 is not in the set, hence this set does not have closure and is not a group under addition.

3. The set of rational numbers of absolute value $< 1$.
   Let $x$ be any element in this set. For the value of $x = 0.9$, $x + x = 1.8$ which is not $< 1$ and thus not a member of the set (the set is not closed under addition). Hence this set is not a group under addition.

4. The set of rational numbers of absolute value $\geq 1$ together with 0.
   For $x, y \in$ this set, let $x = -1.4$, $y = 1 \implies x + y = -.4$ and $\mid -0.4 \mid = 0.4$ which is not $\geq 1$ and thus not a member of the set (the set is not closed under addition). Hence this set is not a group under addition.

5. The set of rational numbers with denominators equal to 1 or 2.
   For any $\frac{a}{b}, \frac{c}{d} \in$ the set,

   (a) Associativity: Inherited from $\mathbb{Q}$.

   (b) Closure: $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$ but both $b, d \in \{1, 2\}$ so $bd \in \{0, 1\}$. Hence the set is closed under addition.

   (c) Identity: $\frac{a}{b} + 0/1 = \frac{a}{b} = 0/1 + \frac{a}{b}$.

   (d) Inverse element: $\frac{a}{b} + (-\frac{a}{b}) = 0/1$, if $b \in \{1, 2\}$ then $-b \in \{-1, -2\}$.

   Thus, the set is a group under addition.

6. The set of rational numbers with denominators equal to 1, 2, 3.
   $\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd}$, both $b, d \in \{1, 2, 3\}$ which means that $bd \in \{1, 2, 3, 6\}$. Because the result of the sum can have 6 as a denominator the set is not closed under addition.

**Problem 8**. Prove that $(a_1a_2\cdots a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}\cdots a_2^{-1}a_1^{-1}$ for all $a_1, a_2, \ldots, a_n \in G$.

*Solution.*

$$(a_1a_2...a_n)^{-1}(a_1a_2...a_n) = e$$
$$(a_1a_2...a_n)^{-1}(a_1a_2...a_{n-1}a_n)a_n^{-1} = a_n^{-1}$$
$$(a_1a_2...a_n)^{-1}(a_1a_2...a_{n-1})a_{n-1}^{-1} = a_n^{-1}a_{n-1}^{-1}$$

after doing this n times, we get

$$(a_1a_2...a_n)^{-1} = a_n^{-1}a_{n-1}^{-1}...a_2a_1$$

Thus proved.

**Problem 9**. Let $x$ be an element of $G$. Prove that $x^2 = 1$ if and only if $|x|$ is either 1 or 2.

*Solution.*

We know that the order of an element in a group is the minimum postive number of times it needs to be operated on with itself to get the identity element. Given $x^2 = 1 = e$, we can see that $\mid x \mid \leq 2$. So $\mid x \mid \in \{1, 2\}$. Hence proved.

**Problem 10**. Let $x$ be an element of $G$. Prove that if $|x| = n$ for some positive integer $n$ then $x^{-1} = x^{n-1}$.

*Solution.*

Given $\mid x \mid = n$:

$$x^n = e$$
$$x^nx^{-1} = ex^{-1}$$
$$x^{n-1} = x^{-1}$$

Hence proved.

**Problem 11**. If $x$ and $g$ are elements of the group $G$, prove that $|x| = |g^{-1}xg|$. Deduce that $|ab| = |ba|$ for all $a$, $b \in G$

*Solution.*

Let the order of $g^{-1}xg$ be $n$.

$$\begin{aligned}
e &= (g^{-1}xg)^n \\
e &= \underbrace{(g^{-1}xg)(g^{-1}xg)...(g^{-1}xg)}_{n \text{ times}} \\
e &= \underbrace{g^{-1}x(gg^{-1})x(g...g^{-1})xg}_{n \text{ times}} \\
e &= g^{-1}x^n g \\
g^{-1}g &= g^{-1}x^n g \\
gg^{-1}g &= gg^{-1}x^n g \\
gg^{-1} &= x^n gg^{-1} \\
e &= x^n \implies \mid x \mid = n = \mid g^{-1}xg \mid
\end{aligned}$$

Using,

$$\begin{aligned}
n &= \mid x \mid = \mid g^{-1}xg \mid \\
e &= x^n = (g^{-1}xg)^n \\
x^n &= g^{-1}x^n g \text{ (shown above)} \\
gx^n &= gg^{-1}x^n g \\
gx^n &= x^n g \implies \mid gx^n \mid = \mid x^n g \mid
\end{aligned}$$

Thus, $\mid ab \mid = \mid ba \mid \forall a, b \in G$.

**Problem 12**. Suppose $x \in G$ and $|x| = n < \infty$. If $n = st$ for some positive integers $s$ and $t$, prove that $|x^s| = t$

*Solution.*

Given $\mid x \mid= n$ and $n < \infty$:

$$
\begin{aligned}
e &= x^n \\
e &= x^{st} \\
e &= \underbrace{\underbrace{xx...x}_{s \text{ times}} \ \underbrace{xx...x}_{s \text{ times}} \ ... \ \underbrace{xx...x}_{s \text{ times}}}_{t \text{ times}} \\
e &= (x^s)^t \\
\mid x^s \mid &= t
\end{aligned}
$$

Hence proved.

**Problem 13**. Prove that if $x^2 = 1$ for all $x \in G$ then $G$ is abelian.

*Solution.*

If $x^2 = 1, \forall x \in G$ then,

$$
\begin{aligned}
(ab)^2 &= 1 \\
abab &= 1 \\
ababb^{-1} &= b^{-1} \\
aba &= b^{-1} \\
abaa^{-1} &= b^{-1}a^{-1} \\
ab &= b^{-1}a^{-1}
\end{aligned}
$$

but,

$$
\begin{aligned}
kk &= kk^{-1} \\
k &= k^{-1}
\end{aligned}
$$

so,

$$
\begin{aligned}
ab &= b^{-1}a^{-1} \\
ab &= ba
\end{aligned}
$$

Thus, $G$ is abelian.

**Problem 14**. Prove that any finite group $G$ of even order contains an element of order 2. [Let $t(G)$ be the set $\{g \in G \mid g \neq g^{-1}\}$. Show that $t(G)$ has an even number of elements and every nonidentity element of $G|t(G)$ has order 2.]

*Solution.*

Let $t(G) = \{g \in G \mid g \neq g^{-1}\}$. i.e. the set $t(G)$ includes the elements of the group that aren't their own inverses. And because for each $a \in G$ there exists a $a^{-1} \in G$ that is it's inverse, we can pair up elements of $t(G)$ in $(a, a^{-1})$ pairs. Thus we can see that $\mid t(G) \mid= 2n, n \in \mathbb{N}$.
Moreover, we know that the set $G \mid t(G)$ is not empty because $e \notin t(G)$ but $e \in G$. And because $\mid G \mid= 2m$ and $\mid t(G) \mid= 2n$ for any $m, n \in \mathbb{N}$ we know that there exist at least two elements in $\mid (G \mid t(G)) \mid$.
And for any $a \in G \mid t(G)$, $a = a^{-1} \implies aa^{-1} = e \implies \mid a \mid= 2$.
Thus, any finite group $G$ of even order contains an element of order 2.

**Problem 15**. Let $G$ be a group and $g \in G$.

1. Prove that if $ga = a$ for any single $a \in G$ (or that $ag = a$ for any single $a \in G$) then $g$ is the identity element.

2. Prove that if $gg = g$ then $g$ is the identity element.

3. Give an example of a group $G$ and an element $g \in G$ such that $g^3 = g$ but that $g$ is not an identity element.

*Solution.*

1. Given $ga = a, \forall a \in G$:

$$\begin{aligned} gaa^{-1} &= aa^{-1} \\ gaa^{-1} &= e \\ ge &= e \\ g &= e \end{aligned}$$

   Thus, g is the identity element.

2. Given $gg = g$

$$\begin{aligned} gg &= g \\ ggg^{-1} &= gg{-}1 \\ ge &= e \\ g &= e \end{aligned}$$

   Thus, g is the identity element.

3. If $G$ is the group $(\mathbb{Z} \setminus \{0\}, *)$, then for $g = -1$, $g^3 = g$ but $g$ is not an identity element.

**Problem 15**. The set of invertible $n \times n$ real matrices is a group $\mathrm{GL}_n(\mathbb{R})$ with the operation of matrix multiplication, called the real general linear group. Consider the following elements of $\mathrm{GL}_2(\mathbb{R})$:

$$A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Show that $A$ and $B$ have finite order (compute their orders) but that $AB$ has infinite order. This shows that the order of a product is not necessarily the product of the orders! (Though see Problem Set 1 for an instance when this does hold.)

*Solution.*

For $A = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$,

$$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$
$$\left|\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\right| = 3$$

For $B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$,

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$$
$$\left|\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right| = 4$$

$$\begin{aligned} AB &= \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \end{aligned}$$

For $AB = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$ ,

$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ -2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -3 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -4 & 1 \end{pmatrix}$$

It seems like for calculating $AB^n$ the resulting matrix is $= \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix}$, thus $AB^n$ can never produce the identity matrix, and $\mid AB \mid = \infty$.