Introduction to Algebra (I) Homework 1

B13902022 賴昱錡

2025 年 9 月 16 日

1

(a)

By some calculation as belows, $i = 2, 3, 6$ satisfies the given condition that $f_i(f_i(x)) = x$ asides from $i = 1$.

$$
\begin{aligned}
f_2(f_2(x)) &= 1 - (1 - x) = x \\
f_3(f_3(x)) &= \frac{1}{\frac{1}{x}} = x \\
f_6(f_6(x)) &= \frac{\frac{x}{x-1}}{\frac{x}{x-1} - 1} = x
\end{aligned}
$$

(b)

By some observation, $f_1(x)$ satisfies the condition $f_i(x) = x$, $f_2(x), f_3(x), f_6(x)$ satisfies $f_i(f_i(x)) = x$, and $f_4(x), f_5(x)$ satisfies the condition $f_i(f_i(f_i(x))) = x$.

For set S, we can do the same operation several times to form original permutation. The 1st method is doing (1) for one time, the 2nd method is doing (12), (23) or (13) for 2 times, and the 3rd method is doing (123) or (132) for 3 times.

Thus, considering the counts of composition and the operations, we can correspond $f_2(x)$ to (12), $f_3(x)$ to (23), $f_6(x)$ to (13). Also $f_1(x)$ to (1), and $f_(4)$ to (123), and $f_5(x)$ to (132).

(c)

For $i, j \in 2, 3, 6,\ i \neq j$, considering all possible compositions, thus, $f_i(f_j(x)) \neq f_j(f_i(x))$ is true.

$$
\begin{aligned}
f_2(f_3(x)) &= 1 - \frac{1}{x} \\
f_3(f_2(x)) &= \frac{1}{1-x} \\
f_2(f_6(x)) &= 1 - \frac{x}{x-1} \\
f_6(f_2(x)) &= \frac{1-x}{-x} \\
f_3(f_6(x)) &= \frac{x-1}{x} \\
f_6(f_3(x)) = \frac{\frac{1}{x}}{\frac{1}{x}-1} &= \frac{1}{1-x}
\end{aligned}
$$

Similarily, consider their corresponding element in S, we have: (In my correspondence, if f_i corresponds to operation a, f_j corresponds to operation b, then $f_i(f_j(x))$ corresponds to doing a then b $(a \to b)$)

- $(12) \to (13)$ results in (132).
- $(13) \to (12)$ results in (123).
- $(12) \to (23)$ results in (123).
- $(23) \to (12)$ results in (132).
- $(13) \to (23)$ results in (132).
- $(23) \to (13)$ results in (123).

The corresponding element in S also satisfies the given condition.

(d)

By 1(b), $f_1(x)$ is corresponding to (1), and $f_4(x)$ to (123), and $f_5(x)$ to (132).

2

(a)

The elements satisfying the condition when $n = 5$ include $1, 2, 3$. For $x = 1$, we can choose $y = 1$. For $x = 2$, we can choose $y = 3$. For $x = 3$, we can choose $y = 2$. For $x = 4$, we can choose $y = 4$. There are 4 elements satisfying the condition.

(b)

For $n = 6$:

- $x = 1, y = 1 \Rightarrow 1 * 1 \equiv 1 \pmod 6$
- $x = 5, y = 5 \Rightarrow 5 * 5 \equiv 1 \pmod 6$

(c)

For $n = 8$:

- $x = 1, y = 1 \Rightarrow 1 \equiv 1 \pmod 8$
- $x = 3, y = 3 \Rightarrow 9 \equiv 1 \pmod 8$
- $x = 5, y = 5 \Rightarrow 25 \equiv 1 \pmod 8$
- $x = 7, y = 7 \Rightarrow 49 \equiv 1 \pmod 8$

(d)

For $n = 13$:

- $x = 1, y = 1 \Rightarrow 1 \equiv 1 \pmod{13}$
- $x = 2, y = 7 \Rightarrow 14 \equiv 1 \pmod{13}$
- $x = 3, y = 9 \Rightarrow 27 \equiv 1 \pmod{13}$
- $x = 4, y = 10 \Rightarrow 40 \equiv 1 \pmod{13}$
- $x = 5, y = 8 \Rightarrow 40 \equiv 1 \pmod{13}$
- $x = 6, y = 11 \Rightarrow 66 \equiv 1 \pmod{13}$
- $x = 7, y = 2 \Rightarrow 14 \equiv 1 \pmod{13}$
- $x = 8, y = 5 \Rightarrow 40 \equiv 1 \pmod{13}$
- $x = 9, y = 3 \Rightarrow 27 \equiv 1 \pmod{13}$
- $x = 10, y = 4 \Rightarrow 40 \equiv 1 \pmod{13}$
- $x = 11, y = 6 \Rightarrow 66 \equiv 1 \pmod{13}$
- $x = 12, y = 12 \Rightarrow 144 \equiv 1 \pmod{13}$

(e)

For $n = 30$:

- $x = 1, y = 1 \Rightarrow 1 \equiv 1 \pmod{30}$
- $x = 7, y = 13 \Rightarrow 91 \equiv 1 \pmod{30}$
- $x = 11, y = 11 \Rightarrow 121 \equiv 1 \pmod{30}$
- $x = 13, y = 7 \Rightarrow 91 \equiv 1 \pmod{30}$
- $x = 17, y = 23 \Rightarrow 391 \equiv 1 \pmod{30}$
- $x = 19, y = 19 \Rightarrow 361 \equiv 1 \pmod{30}$
- $x = 23, y = 17 \Rightarrow 391 \equiv 1 \pmod{30}$
- $x = 29, y = 29 \Rightarrow 841 \equiv 1 \pmod{30}$

3

(a)

We have to prove that ”There exists integer a, b such that $ax + bn = 1$.” is **necessary and sufficient** for $x \in \mathbb{Z}/n\mathbb{Z}^\times$ (Here $x \in \mathbb{Z}/n\mathbb{Z}$).

For any $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, by definition, there exists integer $a \in [1, n-1]$ (Because $a \in \mathbb{Z}/n\mathbb{Z}$, the condition $a = 0$ is impossible for $ax \equiv 1 \pmod{n}$), such that $ax \equiv 1 \pmod{n}$, so ax can be written as the form $ax = -bn + 1, b \in \mathbb{Z}, b = \frac{ax-1}{-n}$. Thus, there exists integer a, b such that $ax + bn = 1$, and the **necessity** of ”There exists integer a, b such that $ax + bn = 1$.” has been proven.

If there exists integer a, b such that $ax + bn = 1$, integer a can be written as the form $a = un + v, u \in \mathbb{Z}, v \in \mathbb{Z}/n\mathbb{Z}$ (By basic division). Make a substitution:

$$\begin{aligned} (un + v)x + bn &= 1 \\ vx = -unx - bn + 1 &= n(-ux - b) + 1 \end{aligned}$$

We can observe that $vx \equiv 1 \pmod{n}$, thus, $x \in (\mathbb{Z}/n\mathbb{Z})^\times$, and the sufficiency has been proven.

In conclusion, ”There exists integer a, b such that $ax+bn = 1$.” is **necessary and sufficient** for $x \in \mathbb{Z}/n\mathbb{Z}^\times$ (Here $x \in \mathbb{Z}/n\mathbb{Z}$).

(b)

In (b), we need to prove that "n is prime" is **necessary and sufficient** for $(\mathbb{Z}/n\mathbb{Z})^\times$ having $n-1$ elements.

Before proving the sufficiency, we have to prove the theorem called **Bézout's Identity**:

Also, for simplicity, (a, b) means $\gcd(a, b)$ in the following proof.

> Let $a, b \in \mathbb{Z}, ab \neq 0$
>
> $d = \gcd(a, b)$ be the greatest common divisor of a and b.
>
> Then $\exists x, y \in \mathbb{Z}$ such that $ax + by = d$. Also, d is the smallest positive integer combination of a and b.

Proof:

Given any two non-zero integer a, b, Let set $S = \{ax + by : x, y \in \mathbb{Z} \wedge ax + by > 0\}$

It's trivial that S is not an empty set (For example, $a > 0, x = 1, y = 0$ or $a < 0, x = 1, y = 0$, $ax + by \in S$, thus, S is not an empty set). Since all elements in S are positive integers, by well ordering principle, S contains a least element d. And write it as the form $d = au + bv$, where u and v are integers.

Consider a's euclidean division: $a = qd + r, q \in \mathbb{Z}, 0 \leq r < d$, we have:

$$r = a - qd = a - q(au + bv) = a(1 - qu) - bqv$$

Because both $1 - qu$ and qv are integers, $r \in S \cup \{0\}$ (because $0 \leq r < d$). Also, d is the least element in S, this implies that r is not belonging to S, it must be 0. Thus, $d|a$. Similarily, $d|b$.

Consider arbitrary common divisor c of a, b, $\exists s, t$ such that $a = cs, b = ct$. So, $d = au + bv = c(us + vt)$, because $us + vt \in \mathbb{Z}$, we know $c|d \wedge c \leq d$.

Since d is greater than all divisors, $d = \gcd(a, b)$, it's also the least element in S by previous definition.

To prove the sufficiency of n being prime, assume n is prime. Then for every $x \in (\mathbb{Z}/n\mathbb{Z}), x \neq 0$ we have $(x, n) = 1$. By Bézout's Identity, there exists integers a, b such that $ax + bn = 1$. This implies $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ by 3(a). Thus, there are $n - 1$ elements in $(\mathbb{Z}/n\mathbb{Z})^\times$ (Since except for 0, $(\mathbb{Z}/n\mathbb{Z})$ contains $n - 1$ elements).

To prove the necessity of n being prime, assume there are $n - 1$ elements in $(\mathbb{Z}/n\mathbb{Z})^\times$, the group has all integers on the interval $[1, n - 1]$. And this implies that there exists integer a and b such that $ax + bn = 1$ by 3(a). (choose arbitrary $x \in (\mathbb{Z}/n\mathbb{Z})^\times$)

Let $\gcd(x, n) = k \neq n, x = ku, n = kv,\ u, v \in \mathbb{Z}$. Pluggin it in $ax + bn = 1$ we get $k(ua + vb) = 1$, since $ua + vb \in \mathbb{Z}$, $k \neq 1$ is impossible. So, $(x, n) = 1$. Because all integers on $[1, n - 1]$ is coprime to n, n is a prime number obviously. Here the necessity is proved.

In conclusion, "n is prime" is **necessary and sufficient** for $(\mathbb{Z}/n\mathbb{Z})^\times$ having $n-1$ elements. Thus, $(\mathbb{Z}/n\mathbb{Z})^\times$ has $n - 1$ elements if and only if n is prime.

4

(a)

Suppose e and e' are identity elements of group $(G, *)$, by the definition of group, $\forall g \in G$, there are:

$$g * e = e * g = g,\ g * e' = e' * g = g$$

Thus, $e = e * e' = e' * e = e'$, the identity element of a group is unique.

Suppose h and h' are the inverse element of an element $x \in G$, and e is the identity element of group $(G, *)$, by the definition:

$$x * h = h * x = e,\ x * h' = h' * x = e$$

And $h * (x * h') = (h * x) * h' = e * h' = h'$, thus, the inverse for every $x \in G$ is unique.

(b)

We can consider four cases: a group having 1,2,3 and 4 elements (obviously an empty set is not a group due to the lack of identity and inverse).

Any group with only one element (Let it be $\{x\}$) trivially follows the commutative rule, since the order doesn't matter:

$$x * x = x \Rightarrow x = x^{-1} = e$$

A group G with 2 elements must be in the form $\{e, a\}$ (By definition, group must has one unique identity element), where e is the identity and a is a non-identity element. (In the case $a^{-1} = a, e^{-1} = e$). By the definition, $a * e = e * a = a$. Thus, every group with 2 elements is abelian.

Similarily, a group G with 3 elements must be in the form $\{e, a, b\}$ ($a \neq b \neq e$, e is the identity), since $a \neq e, b \neq e, ab \in G$, we have:

$$a * b = e$$

a and b are inverse to each other, $a * b = b * a$. This is the only non-trival case, $a * e = e * a$ and $b * e = e * b$ are true by definition. Thus, every group with 3 elements is also abelian group.

Similarily, a group G with 4 elements must be in the form $\{e, a, b, c\}$ ($a \neq b \neq c \neq e$, e is the identity). Assume that the group is **not** an abelian group, that is, there exists one pair of non-identity elements (Without loss of generosity, let the pair be a and b) such that $a * b \neq b * a$.

$a * b \neq a, a * b \neq b$ since the identity is unique. Also, $a * b \neq e$, because $a * b = e$ implies $b * a = e$ as well. To make $a * b \in G$, the only possibility is $a * b = c$.

Consider $b * a$, it is not equal to a, b and e because of the same reason mentioned in last paragraph. But $b * a \in G$ by the definition of group, the only possibility is $b * a = a * b = c$, which creates a contradiction. Thus, any group with 4 elements are abelian.

After proving as above, we can have the conclusion that if G has at most four elements, for all $x, y \in G$, we have $x * y = y * x$.

(c)

If every element $x \in G$ satisfies $x * x = e$, then $x = x^{-1}$. So:

$$\begin{aligned} x * y &= x^{-1} * y^{-1} \\ &= (y * x)^{-1} \\ &= y * x \end{aligned}$$

Obviously, for all $x, y \in G$ we have $x * y = y * x$.