◇ ◇ ◇ ◇ MATH 4441/6441: MODERN ALGEBRA I ◇ ◇ ◇ ◇
HOMEWORK SETS AND EXAMS

Yongwei Yao

2025 SPRING SEMESTER
GEORGIA STATE UNIVERSITY

Contents

There are four (4) problems in each homework set. Math 6441 students need to do all 4 problems while Math 4441 students need to do any three (3) problems out the four. If a Math 4441 student submits all 4 problems, then one of the lowest score(s) is dropped. There is a bonus point for Math 4441 students solving all 4 problems correctly/perfectly.

When solving homework problems, make sure that your arguments and computations are rigorous, accurate, and complete. Present your step-by-step work in your solutions/proofs.

There are three (3) PDF files for the homework sets and exams, one with the problems only, one with hints, and one with solutions. Links are available below.

PROBLEMS HINTS SOLUTIONS

$(G,*)\ldots H\leqslant G\ldots|G|=[G:H]\cdot|H|\ldots a^{|G|}=e\ldots\varphi\colon G\to G',\ \varphi(ab)=\varphi(a)\varphi(b)\ldots N\trianglelefteq G\ldots G/N\ldots G/\operatorname{Ker}(\varphi)\cong\operatorname{Im}(\varphi)$

Problem 1.1. Let $A = \{1, 2, 3, 4\}$, $B = \{2, 3, 5, 6, 7\}$ and $C = \{3, 6, 7, 8\}$ be sets.

(1) Compute $(A \setminus B) \cap C$ and $A \setminus (B \cap C)$. Are they equal?
(2) Compute $(A \cap B) \cup C$ and $A \cap (B \cup C)$. Are they equal?

Solution. (1) First, we see

$$A \setminus B = \{1, 4\},$$
$$B \cap C = \{3, 6, 7\}.$$

In light in the computation above, we get

$$(A \setminus B) \cap C = \{1, 4\} \cap \{3, 6, 7, 8\} = \varnothing$$
$$A \setminus (B \cap C) = \{1, 2, 3, 4\} \setminus \{3, 6, 7\} = \{1, 2, 4\}.$$

Thus $(A \setminus B) \cap C \neq A \setminus (B \cap C)$ (in this particular case).

(2) We have

$$A \cap B = \{2, 3\},$$
$$B \cup C = \{2, 3, 5, 6, 7, 8\}.$$

In light in the computation above, we see

$$(A \cap B) \cup C = \{2, 3\} \cup \{3, 6, 7, 8\} = \{2, 3, 6, 7, 8\}$$
$$A \cap (B \cup C) = \{1, 2, 3, 4\} \cap \{2, 3, 5, 6, 7, 8\} = \{2, 3\}.$$

Thus $(A \cap B) \cup C \neq A \cap (B \cup C)$ (in this particular case).

Problem 1.2. Let A, B and C be sets. Prove $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$.

Proof. It suffices to show $x \in A \setminus (B \cup C) \Leftrightarrow x \in (A \setminus B) \cap (A \setminus C)$. Indeed, we have

$$\begin{aligned} x \in A \setminus (B \cup C) &\iff x \in A \text{ and } x \notin B \cup C \\ &\iff x \in A \text{ and } [x \notin B \text{ and } x \notin C] \\ &\iff [x \in A \text{ and } x \notin B] \text{ and } [x \in A \text{ and } x \notin C] \\ &\iff x \in A \setminus B \text{ and } x \in A \setminus C \\ &\iff x \in (A \setminus B) \cap (A \setminus C). \end{aligned}$$

□

Problem 1.3. For each function f_i, determine whether it is injective but not surjective, surjective but not injective, bijective, or neither injective nor surjective. Explain why.

(1) $f_1 \colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}$ with $f_1(x) = x^2$ for all $x \in \mathbb{R}_{\geqslant 0}$, where $\mathbb{R}_{\geqslant 0} = \{x \in \mathbb{R} \mid x \geqslant 0\} = [0, \infty)$.
(2) $f_2 \colon \mathbb{R}_{\geqslant 0} \to \mathbb{R}_{\geqslant 0}$ with $f_2(x) = x^2$ for all $x \in \mathbb{R}_{\geqslant 0}$.
(3) $f_3 \colon \mathbb{R} \to \mathbb{R}_{\geqslant 0}$ with $f_3(x) = x^4$ for all $x \in \mathbb{R}$.
(4) $f_4 \colon \mathbb{R} \to \mathbb{R}$ with $f_4(x) = 10^{x^2}$ for all $x \in \mathbb{R}$. (Here 10^{x^2} stands for $10^{(x^2)}$, not $(10^x)^2$.)

Solution. (1) The function f_1 is injective but not surjective. It is injective (i.e., 1-1) because for if x_1, $x_2 \in \mathbb{R}_{\geqslant 0}$ such that $x_1 \neq x_2$ (meaning x_1, x_2 are distinct non-negative real numbers) then $x_1^2 \neq x_2^2$ hence $f_1(x_1) \neq f_1(x_2)$. The function f_1 is not onto $\mathbb{R}$ since, for $-1 \in \mathbb{R}$, there is no $x \in \mathbb{R}_{\geqslant 0}$ such that $f_1(x) = -1$.

(2) The function f_2 is bijective. This is because for for every $y \in \mathbb{R}_{\geqslant 0}$ (hence $y \geqslant 0$), there exists $\sqrt{y} \in \mathbb{R}_{\geqslant 0}$ such that $f_1(\sqrt{y}) = (\sqrt{y})^2 = y$ and, moreover, $\sqrt{y}$ is the only preimage (in $\mathbb{R}_{\geqslant 0}$, the domain of f_2) of y under f_2.

(3) The function f_3 is surjective but not injective. It is surjective because for every $y \in \mathbb{R}_{\geqslant 0}$ (hence $y \geqslant 0$), there exists $\sqrt[4]{y} \in \mathbb{R}$ such that $f_3(\sqrt[4]{y}) = (\sqrt[4]{y})^4 = y$. It is not injective since $f_3(1) = 1 = f_3(-1)$ while $1 \neq -1$.

(4) The function f_4 is neither injective nor surjective. It is not injective since $f_4(-2) = 10^4 = f_4(2)$ while $-2 \neq 2$. To see why f_4 is not surjective, just notice that there is no $x \in \mathbb{R}$ such that $f_4(x) = -13$.

Problem 1.4. Let A, B and C be sets.

(1) Find a concrete example of A, B and C such that $(A \cup B) \cap C \subsetneq A \cup (B \cap C)$.
(2) Prove $(A \cup B) \cap C \subseteq A \cup (B \cap C)$.

Solution/Proof. (1) Let $A = B = \{1\}$ and $C = \varnothing$, for example. Then

$$B \cap C = \varnothing \quad \text{and} \quad A \cup B = \{1\}.$$

Consequently, we see

$$A \cup (B \cap C) = \{1\} \cup \varnothing = \{1\} \quad \text{and} \quad (A \cup B) \cap C = \{1\} \cap \varnothing = \varnothing,$$

which illustrates $(A \cup B) \cap C \subsetneq A \cup (B \cap C)$ (for these specific sets A, B and C). (`However, one should not conclude that the statement` $(A \cup B) \cap C \subsetneq A \cup (B \cap C)$ `holds for all sets` A, B `and` C `--- just consider the case when` $A = \varnothing$ `for example.`)

(2) It suffices to show $x \in (A \cup B) \cap C \Rightarrow x \in A \cup (B \cap C)$. Indeed, we have

$$\begin{aligned}
x \in (A \cup B) \cap C &\iff x \in A \cup B \text{ and } x \in C \\
&\iff [x \in A \text{ or } x \in B] \text{ and } x \in C \\
&\iff [x \in A \text{ and } x \in C] \text{ or } [x \in B \text{ and } x \in C] \\
&\overset{*}{\Longrightarrow} x \in A \text{ or } [x \in B \text{ and } x \in C] \\
&\iff x \in A \text{ or } x \in B \cap C \\
&\iff x \in A \cup (B \cap C).
\end{aligned}$$

Note the implication $\overset{*}{\Longrightarrow}$ in the above argument—the reverse implication fails in general (cf. part (1) above). This completes the proof of $(A \cup B) \cap C \subseteq A \cup (B \cap C)$, as required. $\square$

Problem 2.1. Let $X = \{a, b\}$, $Y = \{1, 2\}$ and $Z = \{x, y, z\}$.

(1) Find all functions from X to Y.
(2) Find all injective functions from X to Y, if they exist.
(3) Write down all surjective functions from Y to Z, if they exist.
(4) Write down all **non**-injective functions from Y to Z, if they exist.

Solution. (1) The functions from X to Y are listed as follows

$$f_1\colon\ a \mapsto 1,\ b \mapsto 1; \qquad f_2\colon\ a \mapsto 1,\ b \mapsto 2;$$
$$f_3\colon\ a \mapsto 2,\ b \mapsto 1; \qquad f_4\colon\ a \mapsto 2,\ b \mapsto 2.$$

Since $|X| = 2$ and $|Y| = 2$, there are altogether $|Y|^{|X|} = 2^2 = 4$ functions from X to Y.

(2) In light of part (1) above, there are 2 injective functions from X to Y. They are

$$f_2\colon\ a \mapsto 1,\ b \mapsto 2; \qquad \text{and} \qquad f_3\colon\ a \mapsto 2,\ b \mapsto 1.$$

(3) There exists no surjective function from Y to Z, since $|Y| = 2 < 3 = |Z|$.

(4) There are three **non**-injective functions from Y to Z, which are listed below

$$g_1\colon\ 1 \mapsto x,\ 2 \mapsto x; \qquad g_2\colon\ 1 \mapsto y,\ 2 \mapsto y; \qquad g_2\colon\ 1 \mapsto z,\ 2 \mapsto z.$$

Problem 2.2. Let S_3 denote the set of all bijective functions from $X = \{1, 2, 3\}$ to itself. Let $\varphi \in S_3$ and $\psi \in S_3$ be defined as follows

$$\varphi\colon\ 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3 \qquad \text{and} \qquad \psi\colon\ 1 \mapsto 3,\ 2 \mapsto 1,\ 3 \mapsto 2.$$

(1) Determine $\varphi \circ \psi$ and $\psi \circ \varphi$ explicitly. Are they equal?
(2) Determine φ^{-1} and ψ^{-1} explicitly.
(3) Determine φ^2 and φ^3 explicitly. Is anyone of the two equal to I_X?
(4) Determine ψ^2 and ψ^3 explicitly. Is anyone of the two equal to I_X?

Solution. (1) By direct computation, we see

$$\varphi \circ \psi\colon\ 1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 1 \qquad \text{and} \qquad \psi \circ \varphi\colon\ 1 \mapsto 1,\ 2 \mapsto 3,\ 3 \mapsto 2.$$

In particular, $\varphi \circ \psi \neq \psi \circ \varphi$.

(2) It is straightforward to see that

$$\varphi^{-1}\colon\ 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3 \qquad \text{and} \qquad \psi^{-1}\colon\ 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1.$$

(`Notice that` $\varphi^{-1} = \varphi$.)

(3) It is straightforward to see

$$\varphi^2\colon\ 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 3 \qquad \text{and} \qquad \varphi^3\colon\ 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3.$$

In particular, $\varphi^2 = I_X$. (`Also note that` $\varphi^3 = \varphi = \varphi^{-1}$.)

(4) It is straightforward to see

$$\psi^2\colon\ 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1 \qquad \text{and} \qquad \psi^3\colon\ 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 3.$$

In particular, $\psi^3 = I_X$. (`Also note that` $\psi^2 = \psi^{-1}$.)

Problem 2.3. Let $f\colon X \to Y$ and $g\colon Y \to Z$ be functions, in which X, Y and Z are non-empty sets.

(1) If both f and g are surjective (i.e., onto), prove that $g \circ f$ is surjective.
(2) **Disprove**: If $g \circ f$ is surjective (i.e., onto), then both f and g are surjective.

Proof. (1) Assume that f and g are surjective (i.e., onto); and let $z \in Z$ (be arbitrary). Since g is surjective (by assumption), there exists $y \in Y$ such that

$$g(y) = z.$$

Now, since f is surjective (by assumption), there exists $x \in X$ such that

$$f(x) = y.$$

Combining the above, we see $g(f(x)) = g(y) = z$, which simply says

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

Thus for every $z \in Z$ there exists $x \in X$ such that $g \circ f(x) = z$. Therefore $g \circ f$ is onto.

(2) Let $X = \{1\}$, $Y = \{a, b\}$ and $Z = \{2\}$. Define $f\colon X \to Y$ and $g\colon Y \to Z$ as follows

$$f\colon\ 1 \mapsto a; \qquad\qquad g\colon\ a \mapsto 2,\ b \mapsto 2.$$

Then the composite function $g \circ f\colon X \to Z$ is determined as follows

$$g \circ f\colon\ 1 \mapsto 2 \quad \text{as} \quad g \circ f(1) = g(f(1)) = g(a) = 2.$$

It is clear that $g \circ f$ is surjective (in fact, bijective), but f is not surjective. □

Problem 2.4. Let f, f_1, $f_2\colon X \to Y$ and g, g_1, $g_2\colon Y \to Z$ be functions, in which X, Y and Z are (non-empty) sets.

(1) Prove that if g is 1–1 (i.e., injective) and $g \circ f_1 = g \circ f_2$, then $f_1 = f_2$.
(2) **Disprove** the statement: If $g_1 \circ f = g_2 \circ f$ then $g_1 = g_2$.

Proof/Solution. (1) Assume that g is 1–1 and $g \circ f_1 = g \circ f_2$. To prove $f_1 = f_2$, let $x \in X$ be an arbitrary element of X. (We must show $f_1(x) = f_2(x)$.) Since $g \circ f_1 = g \circ f_2$, we see

$$g \circ f_1(x) = g \circ f_2(x),$$

which simply means

$$g(f_1(x)) = g(f_2(x)).$$

Now, because g is 1–1 by assumption, the above equation forces

$$f_1(x) = f_2(x)$$

In summary, we see $f_1(x) = f_2(x)$ for all $x \in X$, which proves $f_1 = f_2$ as required. □

(2) We disprove the statement with a counterexample as follows: Let $X = \{1\}$, $Y = \{a, b\}$ and $Z = \{2, 3\}$. Define $f\colon X \to Y$ and $g_1, g_2\colon Y \to Z$ as follows

$$f\colon\ 1 \mapsto a; \qquad g_1\colon\ a \mapsto 2,\ b \mapsto 2; \qquad g_2\colon\ a \mapsto 2,\ b \mapsto 3.$$

Then it is easy to see that

$$g_1 \circ f(1) = g_1(f(1)) = g_1(a) = 2 = g_2(a) = g_2(f(1)) = g_2 \circ f(1).$$

Consequently, $g_1 \circ f$ and $g_2 \circ f$ are the same function from $X = \{1\}$ to $Z = \{2, 3\}$. In short, $g_1 \circ f = g_2 \circ f$. But $g_1 \neq g_2$ because $g_1(b) \neq g_2(b)$.

Problem 3.1. Consider integers 24, 60, 67 and 97.

(1) List **all** (positive and negative) common divisors of 24 and 60. Determine $\gcd(24, 60)$.
(2) Express $\gcd(67, 97)$ as a linear combination of 67 and 97 (with integer coefficients).

Solution. (1) The common divisors of 24 and 60 are $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12$, the greatest of which is 12. Thus, by definition, $\gcd(24, 60) = 12$.

(2) By the Euclidean Algorithm, we have

$$(*) \qquad \begin{aligned} 97 &= 1 \cdot 67 + 30 \\ 67 &= 2 \cdot 30 + 7 \\ 30 &= 4 \cdot 7 + 2 \\ 7 &= 3 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0, \end{aligned}$$

which implies $\gcd(67, 97) = 1$.

To express $\gcd(67, 97) = 1$ in the form of $67m + 97n$ (with m, $n \in \mathbb{Z}$), we make use of the equations in $(*)$ above to get

$$\begin{aligned} 1 = 7 - 3 \cdot 2 &= 7 - 3(30 - 4 \cdot 7) = 13 \cdot 7 - 3 \cdot 30 \\ &= 13(67 - 2 \cdot 30) - 3 \cdot 30 = 13 \cdot 67 - 29 \cdot 30 \\ &= 13 \cdot 67 - 29(97 - 1 \cdot 67) = 42 \cdot 67 - 29 \cdot 97. \end{aligned}$$

In summary, $\gcd(67, 97) = 1 = (42)67 + (-29)97$ as required. (`Such linear combinations are not unique. Your solutions could be different.`)

Problem 3.2. Let $x = 3 - i$, $y = 4 + 2i$ and $z = -3 - \sqrt{3}i$.

(1) Compute $x + y$ and $x - y$.
(2) Compute xy and x/y.
(3) Write z in polar form $z = r(\cos\theta + i\sin\theta)$ with $0 \leqslant r \in \mathbb{R}$ and $0 \leqslant \theta < 2\pi$.
(4) Compute z^{33}. Is z^{33} in $\mathbb{R}$? Show your reasoning/computation.

Solution. (1) We compute $x + y$ and $x - y$ as follows:

$$x + y = (3 + 4) + (-1 + 2)i = 7 + i \quad \text{and} \quad x - y = (3 - 4) + (-1 - 2)i = -1 - 3i.$$

(2) We compute xy and x/y as follows:

$$\begin{aligned} xy &= (3 - i)(4 + 2i) = (12 + 2) + (6 - 4)i = 14 + 2i, \qquad \text{and} \\ \frac{x}{y} &= \frac{3 - i}{4 + 2i} = \frac{(3 - i)(4 - 2i)}{(4 + 2i)(4 - 2i)} = \frac{(12 - 2) + (-6 - 4)i}{4^2 + 2^2} = \frac{10 - 10i}{20} = \frac{1}{2} - \frac{1}{2}i. \end{aligned}$$

(3) First, $r = |z| = \sqrt{(-3)^2 + (-\sqrt{3})^2} = \sqrt{12} = 2\sqrt{3}$. To figure out θ, we see that

$$\cos\theta = \frac{-3}{2\sqrt{3}} = -\frac{\sqrt{3}}{2} \qquad \text{and} \qquad \sin\theta = \frac{-\sqrt{3}}{2\sqrt{3}} = -\frac{1}{2}.$$

Consequently, $\theta = \frac{7\pi}{6}$. (Note that the point $(-3, -\sqrt{3})$ is located in the third quadrant of the x-y coordinate plane.) In summary, $z = 2\sqrt{3}\big(\cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6}\big)$.

(4) We claim that $z^{33} = 2^{33}3^{16}\sqrt{3}\,i \notin \mathbb{R}$. Indeed, by De Moivre's formula, we have

$$\begin{aligned} z^{33} &= \Big(2\sqrt{3}\big(\cos\tfrac{7\pi}{6} + i\sin\tfrac{7\pi}{6}\big)\Big)^{33} = (2\sqrt{3})^{33}\Big(\cos\tfrac{33\cdot 7\pi}{6} + i\sin\tfrac{33\cdot 7\pi}{6}\Big) \\ &= (2\sqrt{3})^{33}\Big(\cos\tfrac{77\pi}{2} + i\sin\tfrac{77\pi}{2}\Big) = (2\sqrt{3})^{33}\Big(\cos\big(38\pi + \tfrac{\pi}{2}\big) + i\sin\big(38\pi + \tfrac{\pi}{2}\big)\Big) \\ &= 2^{33}3^{16}\sqrt{3}\Big(\cos\tfrac{\pi}{2} + i\sin\tfrac{\pi}{2}\Big) = 2^{33}3^{16}\sqrt{3}(0+i) = 2^{33}3^{16}\sqrt{3}\,i \notin \mathbb{R}. \end{aligned}$$

Problem 3.3. Let $D = \{13^i \mid i \in \mathbb{Z}\}$, the set consisting of all powers of 13 (of all integer exponents). (For example, 13^{-18}, 13^0, $13^{451} \in D$.) For all m, $n \in D$, let $m * n = mn$, the (ordinary) product of m and n. Determine whether statements (1)–(4) are true or false **with justification**. Also answer (5).

(1) For all a, $b \in D$, it holds that $a * b \in D$.
(2) For all a, b, $c \in D$, it holds that $(a * b) * c = a * (b * c)$.
(3) There exists a (fixed) element $e \in D$ such that $e * a = a = a * e$ for all $a \in D$.
(4) For every $a \in D$, there exists $a' \in D$ such that $a' * a = e = a * a'$.
(5) $(D, *)$ is $\boxed{\text{an abelian group}}$ a non-abelian group not a group (choose one)

Solution. (1) True. For all a, $b \in D$, we see $a = 13^i$ and $b = 13^j$ for some i, $j \in \mathbb{Z}$ and hence $a * b = ab = 13^i 13^j = 13^{i+j}$ which is in D since $i + j \in \mathbb{Z}$.

(2) True. This is because multiplication (among complex numbers) is associative.

(3) True. Indeed, $1 \in D$ (since $1 = 13^0$) and 1 satisfies

$$1a = a = a1 \quad \text{i.e.,} \quad 1 * a = a = a * 1 \quad \text{for all} \quad a \in D.$$

Thus, 1 is the identity element of D under the operation $*$. (That is, $e = 1$.)

(4) True. Let $a \in D$, so that $a = 13^i$ with $i \in \mathbb{Z}$. There exists $a' = 13^{-i} \in D$ satisfying

$$13^{-i}13^i = 1 = 13^i 13^{-i} \quad \text{i.e.,} \quad a' * a = e = a * a'.$$

(5) In light of (1)–(4), we see $(D, *)$ is a group by definition. Under ordinary multiplication, we have $a * b = ab = ba = b * a$ for all a, $b \in D$. Thus $(D, *)$ is an abelian group.

Problem 3.4. Let a, b, $c \in \mathbb{Z}$, i.e., a, b, c are all integers.

(1) Give a concrete example of a, b, $c \in \mathbb{Z}$ such that $a \mid c$ and $b \mid c$, but $(ab) \nmid c$.
(2) Prove that if $\gcd(a, b) = 1$, $a \mid c$ and $b \mid c$ then $(ab) \mid c$.

Solution/Proof. (1) With $a = b = c = 2$, for example, we have $a \mid c$ and $b \mid c$, but $(ab) \nmid c$.

(2) Assume $\gcd(a, b) = 1$, $a \mid c$ and $b \mid c$. Note that, quite generally, $\gcd(a, b)$ is a linear combination of a and b. In our case, as $\gcd(a, b) = 1$, there exist $r, s \in \mathbb{Z}$ such that $1 = ra + sb$. Multiplying both sides of $1 = ra + sb$ by c, we get

$$(*) \qquad c = rac + sbc.$$

Since $a \mid c$ and $b \mid c$, there exist $m, n \in \mathbb{Z}$ such that $c = ma$ and $c = nb$. Continuing with equation $(*)$ above, we get

$$(**) \qquad c = rac + sbc = ra(nb) + sb(ma) = rnab + smab = (rn + sm)(ab).$$

Note that $rn + sm$ is an integer. So the equation $(**)$ establishes $(ab) \mid c$ as required. □

Problem 4.1. For all x, $y \in \mathbb{Z}$, let $x*y = |x|+y$. (For example, $(-1)*(-2) = -1 = 1*(-2)$.) Determine whether (1)–(4) are true or false with justification. And then answer (5).

(1) For all a, $b \in \mathbb{Z}$, it holds that $a * b \in \mathbb{Z}$.
(2) For all a, b, $c \in \mathbb{Z}$, it holds that $(a * b) * c = a * (b * c)$.
(3) There exists a (fixed) element $e \in \mathbb{Z}$ such that $e * a = a$ for all $a \in \mathbb{Z}$.
(4) For every $a \in \mathbb{Z}$, there exists $a' \in \mathbb{Z}$ such that $a' * a = e$.
(5) $(\mathbb{Z}, *)$ is an abelian group a non-abelian group $\boxed{\text{not a group}}$ (choose one)

Solution. (1) True. For all a, $b \in \mathbb{Z}$, we have $a * b = |a| + b \in \mathbb{Z}$.

(2) False. For example, when $a = 1$, $b = -2$ and $c = 3$, we have

$$(1 * (-2)) * 3 = (-1) * 3 = 4 \neq 6 = 1 * 5 = 1 * ((-2) * 3).$$

(3) True. This is because $0 \in \mathbb{Z}$ and 0 satisfies

$$0 * a = |0| + a = 0 + a = a \quad \text{for all} \quad a \in \mathbb{Z}.$$

In other words, 0 is the identity element of $\mathbb{Z}$ under the operation $*$. (That is, $e = 0$.)

(4) False. For example, take $a = 13 \in \mathbb{Z}$. Then for all $b \in \mathbb{Z}$,

$$b * 13 = |b| + 13 \geqslant 13 \quad \text{implying} \quad b * 13 \neq 0 = e.$$

In other words, there exists no $a' \in \mathbb{Z}$ such that $a' * 13 = e$.

(5) In light of (1)–(4), we see that $(\mathbb{Z}, *)$ is not a group, by definition.

Problem 4.2. Let G be a group of order 2 (meaning $|G| = 2$). Say $G = \{e, a\}$, in which e and a denote the two distinct elements of G with e being the identity element of G.

(1) Fill in each of the blanks with a or e: $ee = \boxed{}$, $ea = \boxed{}$, $ae = \boxed{}$ and $aa = \boxed{}$. Justify your claims rigorously.
(2) Determine whether G is abelian. Justify your claim rigorously.

Solution/Proof. (1) We claim that $ee = \boxed{e}$, $ea = \boxed{a}$, $ae = \boxed{a}$ and $aa = \boxed{e}$. We give detailed justifications as follows:

- The equation $ee = e$ follows from definition (i.e., $ex = x$ for all $x \in G$).
- The equation $ea = a$ follows from definition (i.e., $ex = x$ for all $x \in G$).
- The equation $ae = a$ follows from a property of group (i.e., $xe = x$ for all $x \in G$).
- Since $aa \in G$, either $aa = a$ or $aa = e$. If it should happen that $aa = a$, we would have $aa = ea$; then by the concellation property, we would get $a = e$, which is not possible. Thus $aa \neq a$. So we must have $aa = e$. (Alternatively, there exists $a^{-1} \in G$ such that $a^{-1}a = e$. So either $a^{-1} = e$ or $a^{-1} = a$. Note that $a^{-1} \neq e$, since $ea = a \neq e$. Thus $a^{-1} = a$, which implies $aa = e$.)

(2) We verify $xy = yx$ for all x, $y \in G$ by exhaustion as follows:

$$aa = aa, \quad ee = ee, \quad \text{and} \quad ea = a = ae.$$

Therefore G is abelian. (This shows that all group of order 2 are abelian.) □

Problem 4.3. Let $(G, *)$ be a group, and a, b, c, $d \in G$. Fill in each of the blanks (?) with an expression involving a, b, c, d, a^{-1}, b^{-1}, c^{-1}, d^{-1} such that the equation holds. (Note that ab is short for $a * b$, and $c(?)db$ short for $c * (?) * d * b$, etcetera.)

(1) $a(?)dc = abc$.
(2) $(?)abd = dc^{-1}d$.
(3) $ba^{-1}(?)d^{-1}bc = abc$.

Solution. We provide answers as follows:

(1) $a(bd^{-1})dc = abc$.
(2) $(dc^{-1}b^{-1}a^{-1})abd = dc^{-1}d$.
(3) $ba^{-1}(ab^{-1}ad)d^{-1}bc = abc$.

For example, to solve (3), we have

$$\begin{aligned} ba^{-1}xd^{-1}bc = abc &\iff ba^{-1}xd^{-1} = a \\ &\iff ba^{-1}x = ad \\ &\iff a^{-1}x = b^{-1}ad \iff x = ab^{-1}ad. \end{aligned}$$

Problem 4.4. Let $D = \mathbb{Q} \setminus \{0\}$, the set of all non-zero rational numbers. For all x, $y \in D$, define $x*y = 4xy$, the ordinary product of 4, x and y. (For example, $(2)*(3) = 4(2)(3) = 24$.)

(1) Determine whether $(D, *)$ is a group.
(2) Justify your claim in (1) carefully.

Solution/Proof. (1) We claim that $(D, *)$ is a group. In fact, it is abelian.

(2) To show $(D, *)$ is a group, we need to verify that $(D, *)$ is closed under $*$, is associative, has a (left) identity, and every element of D has a (left) inverse. We verify the conditions one by one as follows:

(i) For all a, $b \in D$ so that a, $b \in \mathbb{Q} \setminus \{0\}$, it is clear that $4ab$ is a non-zero rational number; this means $a * b \in D$. This shows D is closed under $*$.
(ii) For all a, b, $c \in D$, we see $(a * b) * c = (4ab) * c = 4(4ab)c = 16abc$ while $a * (b * c) = a * (4bc) = 4(a(4bc)) = 16abc$. This shows $(a * b) * c = a * (b * c)$.
(iii) We claim that the identity of $(D, *)$ is $e = \frac{1}{4}$, which is in D. Indeed, for all $a \in D$,
$$\tfrac{1}{4} * a = 4(\tfrac{1}{4})a = 1a = a.$$
(iv) We claim that, for all $a \in D$, the inverse of a in $(D, *)$ is $\frac{1}{16a}$, which is in D. Indeed, it is straightforward to see $\frac{1}{16a}$ is a non-zero rational number (i.e., $\frac{1}{16a} \in D$) and
$$\tfrac{1}{16a} * a = 4(\tfrac{1}{16a})a = \tfrac{4a}{16a} = \tfrac{1}{4} = e.$$

Consequently, we see $(D, *)$ is a group by definition. (`In fact, it is easy to see` $a*b = b*a$ `for all` a, $b \in D$`; so` $(D, *)$ `is an abelian group.`) □

Sets: Problems 1.1, 1.2, 1.4.

Functions: Problems 1.3, 2.1, 2.2, 2.3, 2.4.

About S_n (e.g., with $n = 3$): Problem 2.2.

Integers, complex numbers: Problems 3.1, 3.2, 3.4.

Definition of groups: Problems 3.3, 4.1, 4.4.

Properties of groups: Problems 4.2, 4.3.

Lecture notes and textbooks: All we have covered, **including properties of groups**.

Note: The above list is not intended to be complete. The problems in the actual test may vary in difficulty as well as in content. Going over, understanding, and digesting the problems listed above will definitely help. However, simply memorizing the solutions of the problems may not help you as much.

You are strongly encouraged to practice more problems (than the ones listed above) on your own.

Solutions

have been withdrawn

from the site

PROBLEMS HINTS SOLUTIONS

Problem 5.1. Let G be a group and let a, b be (fixed) elements of G such that $ab^{-1} = b^{-1}a$. Prove the following equations.

(1) $ab = ba$.
(2) $a^{-1}b = ba^{-1}$.

Proof. We have

$$\begin{aligned} ab^{-1} = b^{-1}a &\implies b(b^{-1}a)b = b(ab^{-1})b \\ &\implies ab = ba, && \text{which is (1)} \\ &\implies a^{-1}(ab)a^{-1} = a^{-1}(ba)a^{-1} \\ &\implies ba^{-1} = a^{-1}b, && \text{which is (2).} \end{aligned}$$

Here is **another way** to prove the equations: From $ab^{-1} = b^{-1}a$, we obtain

$$b(b^{-1}a)b = b(ab^{-1})b, \qquad (b^{-1}a)^{-1} = (ab^{-1})^{-1},$$

which yield equations (1) $ab = ba$, (2) $a^{-1}b = ba^{-1}$ respectively. □

Problem 5.2. Let G be a group of order 3. Say $G = \{e, a, b\}$, in which e, a and b are the three distinct elements of G with e the identity element. (Compare with Problem 4.2.)

(1) Fill in each of the blanks with a, b or e: $ab = \boxed{}$ and $ba = \boxed{}$. Explain why.
(2) Prove that G is abelian. That is, every group of order 3 is abelian.
(3) Fill in each of the blanks with a, b or e: $a^2 = \boxed{}$ and $b^2 = \boxed{}$. Prove your claims.

Solution/Proof. (1) We claim that $ab = \boxed{e}$ and $ba = \boxed{e}$.

To see why $ab = e$, note that ab could only possibly be a, b, or e. If $ab = a$, then we would have $ab = ae$ and hence $b = e$ (by cancellation), which is not the case. If $ab = b$, then we would have $ab = eb$ and hence $a = e$ (by cancellation), which is not the case. Therefore we must have $ab = e$, as claimed. Since $ab = e$, we conclude $ba = e$.

(2) By exhaustion, we show $xy = yx$ for all x, $y \in G$ and hence G is abelian as follows

$$aa = aa, \quad bb = bb, \quad ee = ee, \quad ae = a = ea, \quad be = b = eb, \quad \text{and} \quad ab \overset{(1)}{=} e \overset{(1)}{=} ba.$$

(3) We claim that $a^2 = \boxed{b}$ and $b^2 = \boxed{a}$. To see why $a^2 = b$, note that if $a^2 = a$, i.e., $aa = a$, then we would have $aa = ae$ and hence $a = e$ (by cancellation), which is not the case. If $aa = e$, then we would have $aa = e \overset{(1)}{=} ab$, which would imply $a = b$ (by cancellation), which is not the case. Thus $a^2 = b$.

Similarly, if $bb = b$, then we would have $b = e$, which is not the case. If $bb = e$, then we would have $bb = e \overset{(1)}{=} ab$, which would imply $a = b$, which is not the case. Thus it is forced that $bb = a$, as claimed. (Alternatively, we see $b^2 = (a^{-1})^2 = (a^2)^{-1} = b^{-1} = a$.) □

Remark. The solution of Problem 5.2 not only shows that every group of order 3 is abelian, it also describes the structure/operation of all groups of order 3 completely and explicitly.

Problem 5.3. Let G be a group, a, $b \in G$ and m, $n \in \mathbb{Z}$.

(1) Prove that if $a^5 = b^5$ and $a^7 = b^7$ then $a = b$.

(2) Prove that if $a^m = b^m$, $a^n = b^n$ and $\gcd(m, n) = 1$ then $a = b$.

Proof. (1) Observe that $5(3) + 7(-2) = 1$. Consequently, we see

$$\begin{aligned} a = a^1 = a^{5(3)+7(-2)} = a^{5(3)}a^{7(-2)} &= (a^5)^3(a^7)^{-2} \\ &= (b^5)^3(b^7)^{-2} = b^{5(3)}b^{7(-2)} = b^{5(3)+7(-2)} = b^1 = b, \end{aligned}$$

which proves $a = b$ as required. (See the general proof in (2) below.)

(2) Since $\gcd(m, n) = 1$, there exist s, $t \in \mathbb{Z}$ such that $ms + nt = 1$. Consequently,

$$\begin{aligned} a = a^1 = a^{ms+nt} = a^{ms}a^{nt} &= (a^m)^s(a^n)^t \\ &= (b^m)^s(b^n)^t = b^{ms}b^{nt} = b^{ms+nt} = b^1 = b, \end{aligned}$$

which proves $a = b$ as required. □

Problem 5.4. Let G be a group such that $(ab)^4 = a^4b^4$, $(ab)^5 = a^5b^5$ and $(ab)^6 = a^6b^6$ for all a, $b \in G$. Prove that G is abelian.

Proof. Let a, $b \in G$ be arbitrary elements. (It suffices to show $ab = ba$.)

By assumption we have $(ab)^6 = a^6b^6$, which expands to $abababababab = aaaaaabbbbbb$. By cancellation, we get $bababababa = aaaaabbbbb$, i.e., $(ba)^5 = a^5b^5$. Thus $(ba)^5 = a^5b^5 \overset{\clubsuit}{=} (ab)^5$, in which the equation $\clubsuit$ is part of the assumption. In short, we have

$$(\dagger) \qquad (ab)^5 = (ba)^5.$$

Similarly, $(ab)^5 = a^5b^5$ expands to $abababababab = aaaaabbbbb$, which gives $bababababa = aaaaabbbb$ by concellation. Thus $(ba)^4 = a^4b^4 \overset{\spadesuit}{=} (ab)^4$, in which $\spadesuit$ is given. In short,

$$(\ddagger) \qquad (ab)^4 = (ba)^4 \quad \text{or equivalently} \quad (ba)^4 = (ab)^4.$$

Combining (†) and (‡), we see

$$(ab)^4(ab) = (ab)^5 \overset{(\dagger)}{=} (ba)^5 = (ba)^4(ba) \overset{(\ddagger)}{=} (ab)^4(ba).$$

That is,

$$(ab)^4(ab) = (ab)^4(ba),$$

which implies

$$ab = ba$$

by cancellation (by cancelling $(ab)^4$ from the left, to be specific).

In summary, we have verified $ab = ba$ for all a, $b \in G$. This establishes that G is an abelian group, as required. □

Problem 6.1. Let $A = \mathbb{C} \setminus \{0\}$. Consider the group $(A,\ \cdot\ )$ under the usual multiplication. Also consider φ defined by $1 \mapsto 3$, $2 \mapsto 4$, $3 \mapsto 2$, $4 \mapsto 1$, which is in the group $(S_4, \circ)$.

(1) Determine the order of 3, considered as an element of $(A,\ \cdot\ )$.
(2) Determine the order of $\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4})$ as an element of $(A,\ \cdot\ )$.
(3) Determine $\mathrm{o}(\varphi)$.
(4) Compute φ^{1234} in the format of $1 \mapsto \boxed{?}$, $2 \mapsto \boxed{?}$, $3 \mapsto \boxed{?}$, $4 \mapsto \boxed{?}$.

Solution. (1) Note that the identity of $(A,\ \cdot\ )$ is 1. By direct computation, we see

$$3^1 \neq 1, \quad 3^2 = 9 \neq 1, \quad \text{and more generally} \quad \underbrace{3 \cdot 3 \cdots 3}_{n \text{ terms}} = 3^n \neq 1 \text{ for all } n \geqslant 1.$$

Consequently, $\mathrm{o}(3) = \infty$ in $(A,\ \cdot\ )$.

(2) By De Moivre's formula, we see (details skipped)

$$\big(\cos(\tfrac{\pi}{4}) + i\sin(\tfrac{\pi}{4})\big)^n \neq 1 \text{ for } n = 1, \ldots, 7, \quad \text{and} \quad \big(\cos(\tfrac{\pi}{4}) + i\sin(\tfrac{\pi}{4})\big)^8 = 1.$$

Thus $\mathrm{o}\big(\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4})\big) = 8$ in $(A,\ \cdot\ )$.

(3) The identity of $(S_4, \circ)$ is $e\colon 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 3,\ 4 \mapsto 4$. By direct computation (details skipped), we see

$$\varphi^1 \neq e, \quad \varphi^2 \neq e, \quad \varphi^3 \neq e \quad \text{and} \quad \varphi^4 = e.$$

Therefore $\mathrm{o}(\varphi) = 4$ in $(S_4, \circ)$.

(4) Observing $1234 = 4(308) + 2$, we see

$$\varphi^{1234} = \varphi^{4(308)+2} = (\varphi^4)^{308}\varphi^2 = \varphi^2.$$

By computing φ^2 directly, we see $\varphi^{1234}\colon 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 4,\ 4 \mapsto 3$.

Problem 6.2. Let G be a group such that $x^2 = e$ for all $x \in G$.

(1) True or false: $x^{-1} = x$ for all $x \in G$. Justify.
(2) Prove that G is abelian.

Proof. (1) True. For all $x \in G$, the assumption $x^2 = e$ (i.e., $xx = e$) clearly implies $x^{-1} = x$.

(2) Let $x,\ y \in G$. (We must show $xy = yx$.) **One proof goes as follows**:

$$xy = xey = x(xy)^2y = x(xy)(xy)y = (xx)yx(yy) = x^2yxy^2 = eyxe = yx.$$

Alternatively, note that $xy = (xy)^{-1}$, $x = x^{-1}$ and $y = y^{-1}$ by part (1) above. Thus

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx.$$

In summary, we see $xy = yx$ for all $x,\ y \in G$, showing that G is abelian. □

Problem 6.3. Let G be an **abelian** group, $a \in G$ a **fixed** element of G, and n a **fixed** integer. Define $f\colon G \to G$ by $f(x) = x^n$ for all $x \in G$.

(1) Determine whether f is a group homomorphism, with justification.
(2) Prove that $f(a) = a$ **if** $a^{n-1} = e$.
(3) Prove that $f(a) = a$ **only if** $a^{n-1} = e$ (i.e., $a^{n-1} = e$ if $f(a) = a$.)

Solution/Proof. (1) Yes, f is a group homomorphism. Indeed, for all x, $y \in G$, we have

$$f(xy) = (xy)^n \overset{*}{=} x^n y^n = f(x)f(y) \quad \text{as required.}$$

Note that the equality $\overset{*}{=}$ holds because G is abelian.

(2) If $a^{n-1} = e$, then we see

$$a^n = a^{n-1}a = ea = a, \quad \text{that is,} \quad f(a) = a.$$

(3) If $f(a) = a$, then by the construction of f, we see $a^n = a$ and therefore

$$a^{n-1}a = a = ea, \quad \text{which implies} \quad a^{n-1} = e \quad \text{by cancellation.}$$

Alternatively, proofs of (2) and (3) can be combined as follows

$$f(a) = a \iff a^n = a \iff a^{n-1}a = ea \iff a^{n-1} = e. \qquad \square$$

Problem 6.4. Let G be a group and let a, $g \in G$ be **fixed** elements. Define $h\colon G \to G$ by $h(x) = g^{-1}xg$ for all $x \in G$.

(1) Determine whether h is a group homomorphism, with justification.
(2) Prove that $h(a) = a$ **if** $ag = ga$.
(3) Prove that $h(a) = a$ **only if** $ag = ga$ (i.e., $ag = ga$ if $h(a) = a$.)

Solution/Proof. (1) Yes, h is a group homomorphism. Indeed, for all x, $y \in G$, we have

$$h(x)h(y) = (g^{-1}xg)(g^{-1}yg) = g^{-1}x(g^{-1}g)yg = g^{-1}xeyg = g^{-1}xyg = g^{-1}(xy)g = h(xy).$$

(2) If $ag = ga$, then (by associativity)

$$h(a) = g^{-1}ag = g^{-1}(ag) = g^{-1}(ga) = (g^{-1}g)a = ea = a.$$

(3) If $h(a) = a$, i.e., $g^{-1}ag = a$, then (by associativity)

$$ga = g(g^{-1}ag) = (g^{-1}g)ag = ag \quad \text{as required.}$$

Alternatively, proofs of (2) and (3) can be combined as follows

$$ag = ga \iff g^{-1}ag = g^{-1}ga \iff g^{-1}ag = a \iff h(a) = a. \qquad \square$$

Problem 7.1. Let $\varphi\colon G \to G'$ be a group homomorphism, in which G and G' are groups. Let $a \in G$ such that $\mathrm{o}(a) < \infty$. (Denote the identity elements of G and G' by e and e' respectively.)

(1) Prove that $\mathrm{o}(\varphi(a)) < \infty$.

(2) Prove that $\mathrm{o}(\varphi(a)) \mid \mathrm{o}(a)$.

Proof. Denote $\mathrm{o}(a) = k$, which is a positive integer by the assumption that $\mathrm{o}(a) < \infty$. Observe that, in particular, $a^k = e$. Since $\varphi\colon G \to G'$ be a group homomorphism, we see

$$[\varphi(a)]^k = \varphi(a^k) = \varphi(e) = e'.$$

(1) Knowing $[\varphi(a)]^k = e'$ with k being a positive integer, we see $\mathrm{o}(\varphi(a)) < \infty$.

(2) Knowing $[\varphi(a)]^k = e'$ with $k \in \mathbb{Z}$ (with $\mathrm{o}(\varphi(a)) < \infty$ by part (1) above), we see $\mathrm{o}(\varphi(a)) \mid k$ (by a theorem covered in class), which simply says $\mathrm{o}(\varphi(a)) \mid \mathrm{o}(a)$ as required. □

Problem 7.2. Consider the group $(S_3, \circ)$ under composition, which consists of the following

$$f_1\colon\ 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 3; \qquad f_2\colon\ 1 \mapsto 1,\ 2 \mapsto 3,\ 3 \mapsto 2; \qquad f_3\colon\ 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3;$$
$$f_4\colon\ 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1; \qquad f_5\colon\ 1 \mapsto 3,\ 2 \mapsto 1,\ 3 \mapsto 2; \qquad f_6\colon\ 1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 1.$$

$H = \{x \in G \mid x^2 = f_1\}$ and $K = \{x^3 \mid x \in S_3\}$.

(1) Determine whether H is a subgroup of S_3.

(2) Determine whether K is a subgroup of S_3.

Solution. (1) Direct computation (details omitted) reveals

$$f_1^2 = f_1, \qquad f_2^2 = f_1, \qquad f_3^2 = f_1, \qquad f_4^2 \neq f_1, \qquad f_5^2 \neq f_1, \qquad f_6^2 = f_1.$$

Consequently,

$$H = \{f_1,\ f_2,\ f_3,\ f_6\}.$$

Now, observe that H is not closed under the operation of S_3; for example, we have

$$f_2 \in H \quad \text{and} \quad f_3 \in H, \qquad \text{but} \quad f_2 f_3 = f_5 \notin H.$$

Therefore, H is not a subgroup of S_3.

(2) We have (details omitted)

$$\begin{aligned} K &= \{f_1^3,\ f_2^3,\ f_3^3,\ f_4^3,\ f_5^3,\ f_6^3\} \\ &= \{f_1,\ f_2,\ f_3,\ f_6\} = H. \end{aligned}$$

Therefore, K is not a subgroup of S_3, as shown in (1) above.

Problem 7.3. Let G be an abelian group, $H = \{x \in G \mid x^9 = e\}$. Prove $H \leqslant G$, that is, prove that H is a subgroup of G.

Proof. Note that, for $x \in G$, the construction of H says that $x \in H$ if and only if $x^9 = e$.

Firstly, as the identity element $e \in G$ satisfies $e^9 = e$, we see $e \in H$.

Secondly, let $x,\ y \in H$. (We need to show $xy \in H$.) Note that $x,\ y \in H$ simply means $x^9 = e$ and $y^9 = e$. Now, in light of G being abelian, we see

$$(xy)^9 = x^9 y^9 = ee = e, \quad \text{showing} \quad xy \in H.$$

Finally, let $x \in H$, which simply means $x^9 = e$. (We need to show $x^{-1} \in H$.) We see

$$(x^{-1})^9 = x^{-9} = (x^9)^{-1} = e^{-1} = e, \quad \text{showing} \quad x^{-1} \in H.$$

This proves that H is a subgroup of G, i.e., $H \leqslant G$. □

Problem 7.4. Let G be an abelian group, $H = \{a^4 \mid a \in G\}$ and $K = \{a^{52} \mid a \in G\}$.

(1) Prove $H \leqslant G$, that is, prove that H is a subgroup of G.
(2) Prove $K \subseteq H$, that is, prove that K is a subset of H.

Proof. (1) Note that, for an element $x \in G$, $x \in H$ if and only if $x = a^4$ for some $a \in G$.

Firstly, as the identity element $e \in G$ can be written as $e = e^4$, we see $e \in H$.

Secondly, let $x, y \in H$. (We must show $xy \in H$.) Note that $x, y \in H$ simply means $x = a^4$ and $y = b^4$ for some $a, b \in G$. Now, in light of G being abelian, we see

$$xy = a^4b^4 = (ab)^4 \text{ with } ab \in G, \quad \text{showing} \quad xy \in H.$$

Finally, let $x \in H$; so that $x = a^4$ for some $a \in G$. (We must show $x^{-1} \in H$.) We see

$$x^{-1} = (a^4)^{-1} = a^{-4} = (a^{-1})^4 \text{ with } a^{-1} \in G, \quad \text{showing} \quad x^{-1} \in H.$$

This proves that H is a subgroup of G, i.e., $H \leqslant G$.

(2) Let $z \in K$; so that $z = c^{52}$ for some $c \in G$. Then we see

$$z = c^{52} = (c^{13})^4 \text{ with } c^{13} \in G, \quad \text{showing} \quad z \in H.$$

In summary, every $z \in K$ satisfies $z \in H$. This proves $K \subseteq H$, as required. □

Problem 8.1. Consider the group $(S_3, \circ)$ under composition, which consists of the following

$f_1\colon\ 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 3;$ $\quad f_2\colon\ 1 \mapsto 1,\ 2 \mapsto 3,\ 3 \mapsto 2;$ $\quad f_3\colon\ 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3;$
$f_4\colon\ 1 \mapsto 2,\ 2 \mapsto 3,\ 3 \mapsto 1;$ $\quad f_5\colon\ 1 \mapsto 3,\ 2 \mapsto 1,\ 3 \mapsto 2;$ $\quad f_6\colon\ 1 \mapsto 3,\ 2 \mapsto 2,\ 3 \mapsto 1.$

Find as many (distinct) subgroups of S_3 as possible. You will receive 1 point per correct subgroup and -1 point per incorrect choice.

Solution. Note that the identity element of the group S_3 is $e = f_1$. We list six (6) distinct subgroups of S_3 as follows.

$$H_1 = \{f_1\},\ H_2 = \{f_1, f_2\},\ H_3 = \{f_1, f_3\},\ H_4 = \{f_1, f_6\},\ H_5 = \{f_1, f_4, f_5\},\ H_6 = S_3.$$

Alternatively, the above six (6) distinct subgroups of S_3 can be described as

$$H_1 = [f_1],\ H_2 = [f_2],\ H_3 = [f_3],\ H_4 = [f_6],\ H_5 = [f_4] = [f_5] \text{ and } H_6 = S_3.$$

(In fact, H_1, H_2, H_3, H_4, H_5 and H_6 exhaust **all** the subgroups of $(S_3, \circ)$.)

Problem 8.2. Consider the group $(G, \circ)$ under composition, which consists of the following

$f_1\colon\ 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 3,\ 4 \mapsto 4;$ $\quad f_2\colon\ 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 4,\ 4 \mapsto 3;$
$f_3\colon\ 1 \mapsto 2,\ 2 \mapsto 1,\ 3 \mapsto 3,\ 4 \mapsto 4;$ $\quad f_4\colon\ 1 \mapsto 1,\ 2 \mapsto 2,\ 3 \mapsto 4,\ 4 \mapsto 3.$

Find as many (distinct) subgroups of $(G, \circ)$ as possible. You will receive 1 point per correct subgroup and -1 point per incorrect choice. (Note that $(G, \circ)$ is a subgroup of $(S_4, \circ)$.)

Solution. Note that the identity element of the group G is $e = f_1$. We list five (5) distinct subgroups of G as follows.

$$H_1 = \{f_1\},\ H_2 = \{f_1, f_2\},\ H_3 = \{f_1, f_3\},\ H_4 = \{f_1, f_4\},\ H_5 = G.$$

Alternatively, the above five (5) distinct subgroups of G can be described as

$$H_1 = [f_1],\ H_2 = [f_2],\ H_3 = [f_3],\ H_4 = [f_4],\ H_5 = G.$$

(In fact, H_1, H_2, H_3, H_4 and H_5 exhaust **all** the subgroups of $(G, \circ)$.)

Problem 8.3. Let G be a group of order 30, i.e., $|G| = 30$, and let x, $y \in G$.

(1) If $x \in G$ satisfies $x^{24} = e$ and $x^9 \neq e$, determine all the possible value(s) of $\mathrm{o}(x)$.
(2) If $y^{20} = e$, $y^8 \neq e$ and $y^{15} \neq e$, then determine all the possible value(s) of $\mathrm{o}(y)$.
(3) Is it possible to ever have $z \in G$ such that $z^{45} = e$ and $z^{105} \neq e$? Why or why not?

Solution. (1) As $|G| = 30$, we see $\mathrm{o}(x)$ divides 30 by Lagrange's theorem. Also, $x^{24} = e$ implies that $\mathrm{o}(x)$ divides 24. Thus, $\mathrm{o}(x)$ must be a positive common divisor of 30 and 24, which are 1, 2, 3 and 6 precisely. Consequently, $\mathrm{o}(x)$ must be one of the following: 1, 2, 3 or 6. That is, $\mathrm{o}(x) \in \{1, 2, 3, 6\}$.

Moreover, $x^9 \neq e$ implies that $\mathrm{o}(x)$ is *not* a divisor of 9. That is, $\mathrm{o}(x) \notin \{1, 3, 9\}$.

Combining the above information, we see $\mathrm{o}(x) \in \{1, 2, 3, 6\} \setminus \{1, 3, 9\} = \{2, 6\}$. That is, $\mathrm{o}(x)$ could only possibly be 2 or 6.

(2) The assumption $y^{20} = e$ and $|G| = 30$ implies that $\mathrm{o}(y)$ must be a positive common divisor of 20 and 30. That is, $\mathrm{o}(y) \in \{1, 2, 5, 10\}$.

Moreover, $y^8 \neq e$ implies that $\mathrm{o}(y)$ is *not* a divisor of 8. That is, $\mathrm{o}(y) \notin \{1, 2, 4, 8\}$.

Similarly, $y^{15} \neq e$ implies that $\mathrm{o}(y)$ is *not* a divisor of 15. That is, $\mathrm{o}(y) \notin \{1, 3, 5, 15\}$.

Combining the above, we see $\mathrm{o}(y) \in \{1, 2, 5, 10\} \setminus (\{1, 2, 4, 8\} \cup \{1, 3, 5, 15\}) = \{1, 2, 5, 10\} \setminus \{1, 2, 3, 4, 5, 8, 15\} = \{10\}$. That is, $\mathrm{o}(y) = 10$, precisely.

(3) It is **not possible** to have $z \in G$ with $|G| = 30$ such that $z^{45} = e$ and $z^{105} \neq e$. Suppose, on the contrary, such z exists. Then $\mathrm{o}(z)$ must be a positive common divisor of 30 and 45 but *not* a divisor of 105. But this is not possible because the positive common divisors of 30 and 45 are 1, 3, 5 and 15 precisely, all of which are divisors of 105. This contradiction shows that there is no $z \in G$ (with $|G| = 30$) such that $z^{45} = e$ and $z^{105} \neq e$.

Problem 8.4. Prove that every group of order 4 is abelian as follows: Let G be any group of order 4, i.e., $|G| = 4$.

(1) Suppose there exists $a \in G$ such that $\mathrm{o}(a) = 4$. Prove that G is abelian.
(2) Suppose that no elements of G have order 4. Prove $x^2 = e$ for all $x \in G$.
(3) Suppose that no elements of G have order 4. Prove that G is abelian.

Proof. (1) Since $|[a]| = \mathrm{o}(a) = 4 = |G|$ (together with $[a] \leqslant G$), we see

$$G = \{e, a, a^2, a^3\} = [a], \quad \text{which implies } G \text{ is cyclic.}$$

Since G is cyclic, G is abelian. (It is proved in class that every cyclic group is abelian.)

(2) Let $x \in G$ be an arbitrary element of G, so $\mathrm{o}(x) \neq 4$. We have $\mathrm{o}(x) \mid 4$ by Lagrange's theorem. (Note that the positive divisors of 4 are precisely 1, 2 and 4.) Since $\mathrm{o}(x) \neq 4$, we see $\mathrm{o}(x) = 1$ or 2, which (necessarily and invariably) yields $x^2 = e$. (Indeed, if $\mathrm{o}(x) = 1$, then $x = e$ and hence $x^2 = e$; if $\mathrm{o}(x) = 2$, then $x^2 = e$.)

(3) For every x, $y \in G$, we have $x^2 = y^2 = (xy)^2 = e$ and hence

$$xy = xey = x(xy)^2y = xxyxyy = x^2yxy^2 = eyxe = yx,$$

which shows G is abelian. (This argument has been given in Problem 6.2.)

Note that (1) and (3) exhaust all the possibilities for groups of order 4; and in each case we are able to prove that G is abelian. **Thus every group of oder 4 is abelian.** □

Materials covered earlier: Midterm I; Homework Sets 1, 2, 3, 4.

Basic properties, direct calculations: Problems 5.1, 5.2, 5.3, 6.1, 6.2, 7.4, 8.1, 8.3, 8.4, etcetera.

Abelian groups: Problems 5.2, 5.4, 6.2, 8.4.

Orders of elements: Problems 6.1, 7.1, 8.3, 8.4.

Homomorphisms: Problems 6.3, 6.4, 7.1.

Subgroups, the subgroup criterion: Problems 5.3, 7.2, 7.3, 7.4, 8.1, 8.2.

Lagrange's theorem: Problems 8.3, 8.4.

Lecture notes and textbooks: All we have covered.

Note: The above list is not intended to be complete. The problems in the actual test may vary in difficulty as well as in content. Going over, understanding, and digesting the problems listed above will definitely help. However, simply memorizing the solutions of the problems may not help you as much.

You are strongly encouraged to practice more problems (than the ones listed above) on your own.