Practice Problems MTH 461 Spring 2026

$H \neq \emptyset$, $H \subset G$.

1. H is a subgroup $\Leftrightarrow$ $ab^{-1} \in H$ for all $a, b \in H$

"$\Rightarrow$": Suppose H is a subgroup.
Let $a, b \in H$. Then $b^{-1} \in H$
and $ab^{-1} \in H$, since H is closed under inverses
and multiplication.

"$\Leftarrow$": Suppose $ab^{-1} \in H$ for all $a, b \in H$.
Let's show H is a subgroup.

- $e \in H$? Let $a \in H$ ($H \neq \emptyset$). Then $aa^{-1} = e \in H$. ✓
- $a \in H \Rightarrow a^{-1} \in H$? Apply the assumption to e, a to get $ea^{-1} = a^{-1} \in H$. ✓
- $a, b \in H \Rightarrow ab \in H$? Apply assumption to a, b^{-1} ✓

2. Let G be a group. Let $a, b \in G$, $x \in G$ unknown.

$$x^3 = e, \quad x^2 b = ba$$

(a) Solve for x:

$$X^3 = e \xRightarrow[\text{by } x^{-1}]{\text{mult.}} X^2 = X^{-1}$$

$$X^2 b = ba \underset{\substack{\uparrow \\ \text{substitute} \\ x^2 = x^{-1}}}{\Rightarrow} X^{-1} b = ba \underset{\substack{\uparrow \\ \text{mult. on} \\ \text{right by } b^{-1}}}{\Rightarrow} X^{-1} = bab^{-1} \underset{\text{invert}}{\Rightarrow} x = ba^{-1}b^{-1}$$

(b) Suppose $G = \mathbb{Z}_5^\times$ $a \equiv 4$, $b \equiv 3$. Solve for x.

a^{-1} of $a \equiv 4 \equiv -1$ is a itself.

b^{-1} of $b \equiv 3$ is $2 \pmod 5$.

$\Rightarrow x \equiv (3)(-1)(2) \equiv -6 \equiv -1 \equiv 4 \pmod 5$.

However, $x^3 \equiv (-1)^3 \equiv -1 \not\equiv 1$ so there are no solutions.

(Quick solution: Lagrange $\Rightarrow$ ord(x) divides $|\mathbb{Z}_5^\times| = 4$ and $x^3 \equiv 1$, $x \not\equiv 1$ would imply ord$(x) = 3$.)

$\boxed{3}$ S_n is nonabelian $\Leftrightarrow n \geq 3$.

$n \geq 3 \Rightarrow S_n$ nonabelian: take $(12), (23) \in S_n$

$$(12)(23) = (123) \neq (132) = (23)(12)$$

$S_1 = \{e\}$, $S_2 = \{e, (12)\}$ are abelian.

$\boxed{4}$ $G = \left\{ \underbrace{\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}}_{A} \;\middle|\; a, b, c \in \mathbb{R} \right\}$, operation = multipl.

Heisenberg Group

(a) G is a group:

let's show it's a subgroup of $GL_2(\mathbb{R})$.

$\det A = 1$, so $G \subset GL_2(\mathbb{R})$.

- identity? Yes, let $a = b = c = 0$. ✓
- $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a' & b' \\ 0 & 1 & c' \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & a+a' & b' + ac' + b \\ 0 & 1 & c + c' \\ 0 & 0 & 1 \end{pmatrix}$

  so G is closed under the operation. ✓
- the inverse of $\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ is $\begin{pmatrix} 1 & -a & ac - b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$. ✓

(b) G abelian? No. Example:

$$\underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{A} \underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{B} = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\neq$$

$$\underbrace{\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}}_{B} \underbrace{\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}}_{A} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

5 List left/right cosets:

a) $3\mathbb{Z} \subset \mathbb{Z}$. $\mathbb{Z}$ abelian so left cosets = right cosets.

$$0 + 3\mathbb{Z}, \quad 1 + 3\mathbb{Z}, \quad 2 + 3\mathbb{Z}$$
$$\quad \| \qquad\qquad \| \qquad\qquad \|$$
$$0 \pmod 3 \quad 1 \pmod 3 \quad 2 \pmod 3$$

b) $A_4 \subset S_4$. Even / odd perms. (Here left cosets = right)

c) $\langle 8 \rangle \subset \mathbb{Z}_{24}$. Abelian again.

$\langle 8 \rangle = \{0, 8, 16\}$.

$\langle 8 \rangle + 1 = \{1, 9, 17\}$. $\quad \langle 8 \rangle + 2 = \{2, 10, 18\}$

$\langle 8 \rangle + 3 = \{3, 11, 19\}$. $\quad \langle 8 \rangle + 4 = \{4, 12, 20\}$

$\langle 8 \rangle + 5 = \{5, 13, 21\}$. $\quad \langle 8 \rangle + 6 = \{6, 14, 22\}$.

$\langle 8 \rangle + 7 = \{7, 15, 23\}$. (Note Lagrange $\Rightarrow \# = \dfrac{|\mathbb{Z}_{24}|}{|\langle 8 \rangle|} = 8$.)

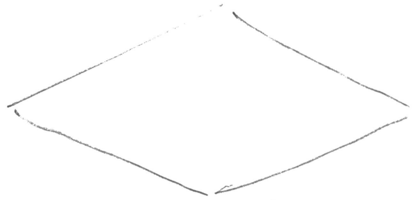
d) $H = \{e, (123), (132)\} \subset S_4$.

Lagrange: $[S_4 : H] = \dfrac{|S_4|}{|H|} = \dfrac{24}{3} = 8$.

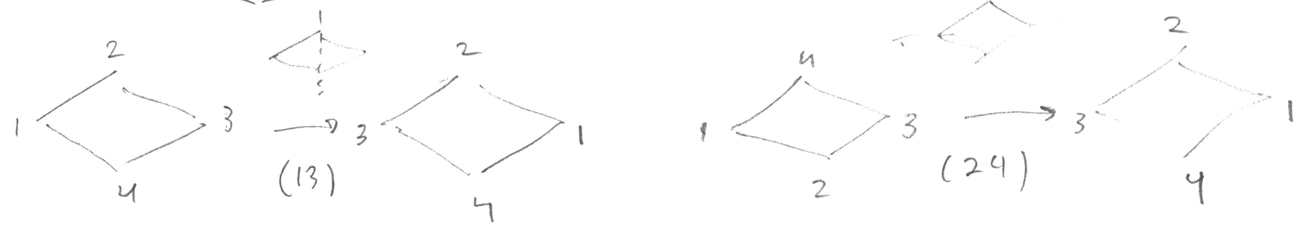
$H(12) = \{(12), (13), (23)\}$

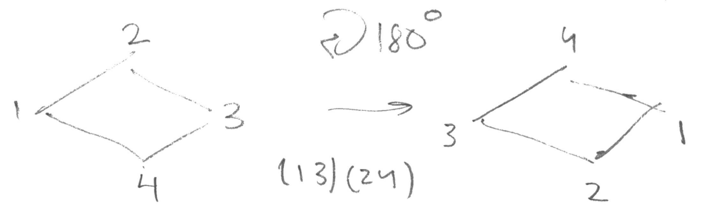
$H(14) = \{(14), (1423), (1432)\}$ etc.

$\boxed{6}$



(a)
(b)





, identity e

$G = \{\text{symmetries of } \diamond\}$ $\quad |G| = 4$

$\cong$ as a subgp of S_4 $\quad \{e, (13), (24), (13)(24)\}$

(c) not a subgp of A_4, since $(13), (24)$ odd.

$\boxed{7}$ Use Fermat's Little thm to show:

$p = 4n+3$ prime $\Rightarrow$ no solutions to $x^2 \equiv -1 \pmod p$

Recall Fermat: $x^p \equiv x \pmod p$.

Suppose $x^2 \equiv -1$ Then $x^p \equiv x^{4n+3} = (x^2)^{2n+1} \cdot (x)$

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

With Fermat, get $x \equiv -x \underset{\text{mult. by } x}{\Rightarrow} -1 \equiv 1 \pmod p \Rightarrow p = 2$, impossible

$\boxed{8}$ a) $(142)(231) = (234)$, order $= 3$, parity $=$ even

$(54123)(24) = (12)(354)$, order $= 6$, parity $=$ odd

b) $H = \{e, (12), (34), (12)(34), (45), (12)(45)\} \subset S_5$ a subgp?

$(34)(45) = (345) \notin H$, so $\underline{\text{NO}}$.

c) possible orders of elements in A_5?

(123) — 3

(1235) — 5

$(12)(34)$ — 2

e — 1

$1, 2, 3, 5$

$\boxed{9}$ $7^{81} \pmod{30}$? $\mathbb{Z}_{30}^{\times} = \{1, 7, 11, 13, 17, 19, 23, 29\}$

$\phi(30) = |\mathbb{Z}_{30}^{\times}| = 8$

Euler $\Rightarrow$ $7^8 \equiv 1 \pmod{30} \Rightarrow 7^{80} = (7^8)^{10} \equiv 1 \pmod{30}$

$\Rightarrow 7^{81} \equiv 7 \pmod{30}$.

10. G finite cyclic, $|G|=n$, $G=\langle a\rangle$.

Show: if $b=a^k$, $\gcd(k,n)=1 \Rightarrow G=\langle b\rangle$.

Recall $G=\langle a\rangle \Leftrightarrow |G|=\text{ord}(a)$.

So $\text{ord}(a)=n$.

Need to show $\text{ord}(b)=n$.

Suppose $\text{ord}(b)=m<n$.

$$\Rightarrow b^m=(a^k)^m=a^{km}=e$$

$km \geq \text{ord}(a)=n$, divide km by n:

$$km=nd+r, \qquad 0\leq r<n$$

$$\Rightarrow e=a^{km}=a^{nd+r}=\underbrace{(a^n)}_{e}{}^d a^r=a^r$$

$\Rightarrow a^r=e$ and $0\leq r<n$

If $r>0$, this contradicts $\text{ord}(a)=n$.

If $r=0$, $km=nd$ $\quad \gcd(km,n)\overset{k \text{ rel. prime } n}{=}\gcd(m,n)<n$

$\gcd(nd,n)=n$, contradiction

$\square$