Solutions

Name:____

No calculators, phones or any other devices may be present during the exam. Show work to receive full credit. There are 5 problems.

1. Consider the following set of 4×4 matrices:

$$G = \left\{ \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbb{Z},\ \ b \text{ is even} \right\}$$

   (a) Prove that G, with the operation of matrix multiplication, is a group.

   (b) Is the group G abelian? Explain.

(a) • Associativity holds by associativity of matrix multiplication

• Closed under the operation:

$$A, B \in G \quad \overset{A}{\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}} \overset{B}{\begin{pmatrix} 1 & a' & b' & c' \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}} = \overset{AB}{\begin{pmatrix} 1 & a+a' & b+b' & c+c' \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}}$$

note $a, b, c, a', b', c' \in \mathbb{Z} \Rightarrow a+a', b+b', c+c' \in \mathbb{Z}$

and b, b' even $\Rightarrow b+b'$ even, so $AB \in G$

• Letting $a=b=c=0$ shows that G has the identity matrix

• The inverse of A as above is $\begin{pmatrix} 1 & -a & -b & -c \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

Note $a, b, c \in \mathbb{Z}$, b even $\Rightarrow -a, -b, -c \in \mathbb{Z}$ and $-b$ is even $\Rightarrow A^{-1} \in G$.

$\Rightarrow G$ is a group.

(b) G is abelian. The expression for AB above is same as for BA.

2. Let G be any group. Let $a, b \in G$, and let $x \in G$ be some unknown. Suppose

$$x^3 = ab, \qquad x^4 = aba. \quad (*) \tag{1}$$

(a) Solve for an expression of x in terms of a and b. Show all steps.
Describe the solutions to (1) in the following cases:

(b) $G = (\mathbb{Z}_7^\times, \times)$ and $a \equiv 2 \pmod 7$, $b \equiv 3 \pmod 7$.

(c) $G = S_3$ and $a = (12)$, $b = e$.

(a) $x^3 = ab \Rightarrow x^{-3} = (ab)^{-1} = b^{-1}a^{-1} \quad (**)$

$x = x^{-3}x^4 \underset{(**)}{=} (b^{-1}a^{-1})x^4 \underset{(*)}{=} (b^{-1}a^{-1})(aba) = \cancel{b^{-1}}\cancel{a^{-1}}\cancel{a}\cancel{b}a = a$

$\Rightarrow \boxed{x = a}$

(b) By (a), any solution must satisfy $x \equiv a \equiv 2 \pmod 7$.

But then $x^3 \equiv 2^3 \equiv 8 \equiv 1 \not\equiv 6 \equiv (2)(3) \equiv ab \pmod 7$,

So there are $\boxed{\text{no solutions}}$.

(c) By (a), any solution must satisfy $x = (12)$.

Check: $x^3 = (12)^3 = (12) = (12)e = ab$ ✓

$x^4 = (12)^4 = e = (12)e(12) = aba$ ✓

So $\boxed{x = (12)}$ is the solution

3. (a) Consider the following elements of $GL_2(\mathbb{R})$:

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \qquad B = \begin{pmatrix} 0 & 1/2 \\ 2 & 0 \end{pmatrix}$$

Compute the orders of the elements A, B and AB.

(b) For any abelian group G, prove that the subset H of G consisting of elements of finite order is a subgroup of G.

(c) Is part (b) true if G is non-abelian? Explain.

(a) $A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I$, $A^3 = A^2A = (-I)A = -A$

$A^4 = A^2A^2 = (-I)(-I) = I \Rightarrow \boxed{\operatorname{ord}(A) = 4}$

$B^2 = \begin{pmatrix} 0 & \frac{1}{2} \\ 2 & 0 \end{pmatrix}\begin{pmatrix} 0 & \frac{1}{2} \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \Rightarrow \boxed{\operatorname{ord}(B) = 2}$

$AB = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & \frac{1}{2} \\ 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & -\frac{1}{2} \end{pmatrix} \quad (AB)^n = \begin{pmatrix} 2^n & 0 \\ 0 & (-\frac{1}{2})^n \end{pmatrix} \Rightarrow \boxed{\operatorname{ord}(AB) = \infty}$

(b) Let $H = \{a \in G \mid \operatorname{ord}(a) < \infty\} \subset G$.

$H \neq \emptyset$ since $\operatorname{ord}(e) = 1 < \infty \Rightarrow e \in H$.

To show H is a subgroup it suffices to show:

$a, b \in H \Rightarrow ab^{-1} \in H$.

$a, b \in H \Rightarrow \operatorname{ord}(a) = m < \infty$, $\operatorname{ord}(b) = n < \infty$.

$\Rightarrow (ab^{-1})^{mn} \underset{G \text{ abelian}}{=} a^m (b^n)^{-1} = ee^{-1} = e \Rightarrow \operatorname{ord}(ab^{-1}) \leq mn < \infty$

$\Rightarrow ab^{-1} \in H$.

(c) $\boxed{\text{No.}}$

Part (a) gives $A, B \in GL_2(\mathbb{R})$ where $\operatorname{ord}(A), \operatorname{ord}(B) < \infty$ but $\operatorname{ord}(AB) = \infty$.

4. Compute the following expressions. State any theorems used.

(a) $6^{81} \pmod{19}$

(b) $5^{61} \pmod{28}$

(c) $(4126)(123)$

(d) $\sigma^{10!}$ where $\sigma = (5612)(34)(1234)(1532)(98754)(12)$ is in S_9

(a) 19 is prime Fermat: $x^{19} \equiv x \pmod{19}$

$6^{81} \equiv 6^{19\cdot 4+5} \equiv (6^{19})^4 6^5 \equiv 6^4 6^5 \pmod{19}$

$6^2 \equiv 36 \equiv 17 \equiv -2, \quad 6^4 = (6^2)^2 \equiv (-2)^2 \equiv 4$

$\Rightarrow 6^{81} \equiv 6^4 6^5 \equiv 6^4 6^4 6^1 \equiv (4)(4)(6) \equiv (-3)(6) \equiv -18 \equiv \boxed{1 \pmod{19}}$

(b) Euler: $x^{\phi(n)} \equiv 1 \pmod{n}$, if $\gcd(x,n)=1$.

$\phi(28) = |\mathbb{Z}_{28}^{\times}| = |\{1,3,5,9,11,13,15,17,19,23,25,27\}| = 12$

$\Rightarrow 5^{12} \equiv 1 \pmod{28}$

$\Rightarrow 5^{61} \equiv 5^{12\cdot 5+1} \equiv (5^{12})^5 5^1 \equiv (1)^5 5 \equiv \boxed{5 \pmod{28}}$

(c) $(4126)(123) = \boxed{(164)(23)}$

$1 \mapsto 2 \mapsto 6$ $\quad$ $2 \mapsto 3$

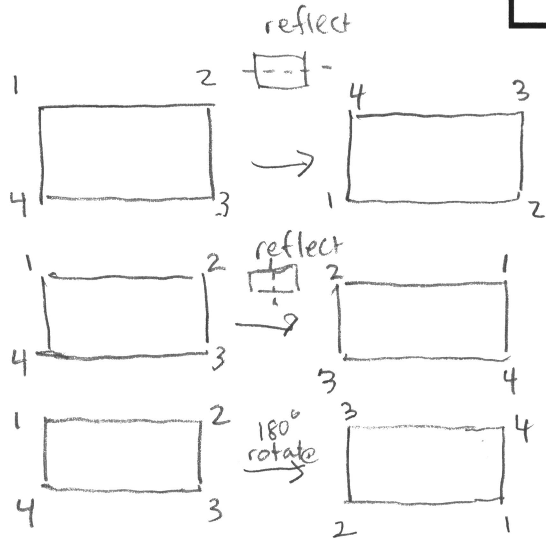
$6 \mapsto 4$ $\quad$ $3 \mapsto 1 \mapsto 2$

$4 \mapsto 1$

(d) Recall for a finite group G, $a^{|G|} = e$ for all $a \in G$.

$|S_9| = 9!$ and $10! = (10)(9!)$. So $\sigma^{10!} = (\sigma^{9!})^{10} = (\sigma^{|S_9|})^{10} = e^{10} = \boxed{e}$

5. Describe the symmetry group of the picture below. By labelling the vertices, identify this group with a set of permutations. Is the group abelian?



$(14)(23)$

$(12)(34)$

$(13)(24)$

and of course the identity e

The group is $\{e, (14)(23), (12)(34), (13)(24)\}$

Yes, it's abelian.

$$\big((14)(23)\big)\big((12)(34)\big) = (14)(23)(12)(34) = (13)(24)$$

$$\big((12)(34)\big)\big((14)(23)\big) = (12)(34)(14)(23) = (13)(24)$$

Other cases similar.