MATH 103A, MODERN ALGEBRA I, MT2

Wednesday, November 13th, 2019, 10-10:50am, APM B402A

- Your Name: SOLUTIONS
- ID Number:
- Section: B01 (5:00 PM)     B02 (6:00 PM)

<table>
<thead>
<tr>
<th>Problem #</th>
<th>Points (out of 10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

Total (out of 40):
Problem 1. Let $(G, \cdot)$ be a cyclic group of size 6. Choose a generator $a \in G$.

(a) Find the order of each of its elements:

\[
\begin{array}{cccccc}
   & e & a & a^2 & a^3 & a^4 & a^5 \\
\hline
C \cup & 0 & 1 & 2 & 3 & 4 & 5 \\
\end{array}
\]

163236 resp.

Circle those $x$ above for which $G = \langle x \rangle$ holds.

(b) List the elements of the non-trivial subgroups $\langle a^2 \rangle$ and $\langle a^3 \rangle$.

(c) Is the product $G \times G$ abelian? Is $G \times G$ cyclic? If so find a generator.

\[(a^\circ) \quad \text{ord}(a^n) = \frac{6}{(\text{GCD}(6, n))} \]

<table>
<thead>
<tr>
<th>$n$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>ord($a^n$)</td>
<td>1</td>
<td>6</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>6</td>
</tr>
</tbody>
</table>

--- deduce that only $x = a$ and $x = a^5$ generate $G$.

(b) $\langle a^2 \rangle = \{ e, a^2, a^4 \}$

$\langle a^3 \rangle = \{ e, a^3 \}$

\[\text{The two non-trivial subgroups of } G.\]

(c) $G \times G$ is abelian, but not cyclic.

Cyclic groups are abelian ($a^m \cdot a^n = a^{m+n} = a^n \cdot a^m$), and products of abelian groups are abelian:

\[(a, b) \circ (c, d) = (a \cdot c, b \cdot d) = (c \cdot a, d \cdot b) = (c, d) \circ (a, b).\]

Since $G$ is abelian. continued \[\rightarrow\]
However, $G \times G$ is not cyclic: All its elements have order $\leq 6$ since $\forall a, b \in G$ we have

$$(a, b)^6 = (a^6, b^6) = (e, e) = e_{G \times G}.$$ But $|G \times G| = |G| \cdot |G| = 36 > 6$. 
Problem 2. Recall that $(\mathbb{Z}_7^\times, \cdot)$ is the multiplicative group of invertible residue classes modulo 7.

(a) Check that the residue class $[3]$ generates $\mathbb{Z}_7^\times$. Find its size $|\mathbb{Z}_7^\times|$.

(b) Find the order of each of the elements:

\[ [1] \quad [2] \quad \boxed{[3]} \quad [4] \quad \boxed{[5]} \quad [6]. \]

Circle those $[x]$ above for which $\mathbb{Z}_7^\times = \langle [x] \rangle$ holds.

(c) Find the integer $r$ in the interval $0 \leq r < 7$ satisfying the congruence

\[ 3^{71} \equiv r \pmod{7}. \]

\[ (a) \text{ First, } |\mathbb{Z}_7^\times| = \phi(7) = 7 - 1 = 6 \quad \text{(using 7 is prime). Second, } [3] \text{ is a generator: Working modulo 7, }\]

\[ 3^1 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6 \quad 3^4 \equiv 4 \]

\[ \implies 3^5 \equiv 5 \quad 3^6 \equiv 1 \quad \text{First time we get 1.} \]

This verifies $[3]$ has order 6, so $\mathbb{Z}_7^\times = \langle [3] \rangle$.

(b) Now, $\text{ord } [3]^n = \frac{6}{\text{GCD}(6,n)}$. Let $n = 0, 1, 2, \ldots, 5$:


\[ \begin{array}{cccccc}
 1 & 3 & 6 & 3 & 6 & 2 \\
 (n=0) & (n=2) & (n=1) & (n=4) & (n=5) & (n=3)
\end{array} \]

Only $[3]$ and $[5]$ are generators of $\mathbb{Z}_7^\times$. continued →
(c) Since $3^6 \equiv 1 \pmod{7}$ we try to divide 71 by 6 using the division algorithm:

$$71 = 11 \cdot 6 + 5$$

Thus, modulo 7,

$$3^{71} \equiv (3^6)^{11} \cdot 3^5 \equiv 3^5 \equiv 5 \pmod{7}$$

$\implies$ Answer is $[r = 5]$. \[ \uparrow \text{ as we found in (a).} \]
Problem 3. Let \( D_4 \) be the dihedral group of symmetries of a square centered at the origin. Introduce

\[
r = \text{rotation by } \frac{\pi}{2} \text{ in the counterclockwise direction},
\]

\[
s = \text{reflection across the horizontal axis}.
\]

Recall the relations \( r^4 = s^2 = e \) and \( rs = sr^{-1} \).\(^*\)

(a) Give its cardinality \( |D_4| \). Is \( D_4 \) an abelian group?

(b) Describe geometrically what the transformation \( rs \) does to a point in the plane: If \( rs \) is a rotation give the angle, if \( rs \) is a reflection give the axis.

(c) Identify the element \( rsr^{-1} \) on the list below. Justify your answer.

\[
e, r, r^2 \bigcirc s, sr, sr^2, sr^3
\]

(a) \( D_4 \) consists of 4 rotations \( \{e, r, r^2, r^3\} \) and 4 reflections \( \{s, sr, sr^2, sr^3\} \). Therefore, \( |D_4| = 8 \).

\( D_4 \) is non-abelian: Otherwise, cancellation law:

\[
rs = rs = sr^{-1} \quad \Rightarrow \quad r = r^{-1} \Rightarrow r^2 = e
\]

- assuming \( r, s \) commute.

(b) Let \( e_1 = (1,0) \) and \( e_2 = (0,1) \) be the standard basis for the plane \( \mathbb{R}^2 \)

\[
e_1 \xrightarrow{s} e_1 \xrightarrow{r} e_2
\]

\[
e_2 \xrightarrow{s} -e_2 \xrightarrow{r} e_1
\]

shows \( rs \) interchanges \( e_1 \) and \( e_2 \).
*Conclusion:* The transformation 

takes

a vector \((x', y')\) to \((x, y)\).

I.e., \(rs = \text{reflection across the axis with angle } \frac{\pi}{4}\). 

\((x = y')\)

\(r^4 = e\).

\(s^2 = e\).

\(r^2 = s\).

\((c)\) \(srs^{-1} = srs = ssr^{-1} = r^{-1} = r^3\)

So \(srs^{-1} = r^3\) .
Problem 4. Let $\alpha \in S_7$ be the permutation given by $\alpha = (1352)(5137)$.

(a) Express $\alpha$ in array form. That is, fill in the blank boxes below.

\[\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \square & \square & \square & \square & \square & \square & \square \end{pmatrix}\]

\[5 1 7 4 3 6 2\]

(b) Is $\alpha$ a cycle? If not, find its decomposition into disjoint cycles.

(c) Compute $\operatorname{ord}(\alpha)$ and $\operatorname{sign}(\alpha)$. Does $\alpha$ belong to $A_7$?

(a) For example $1 \xrightarrow{(5137)} 3 \xrightarrow{(1352)} 5$.

\[\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 7 & 4 & 3 & 6 & 2 \end{pmatrix}\]

(b) $\alpha$ takes $1 \rightarrow 5 \rightarrow 3 \rightarrow 7 \rightarrow 2 \rightarrow 1$

(and fixes 4 and 6). So yes, $\alpha$ is a $5$-cycle:

\[\alpha = (15372)\]

(c) $\operatorname{ord}(\alpha) = 5$ and $\operatorname{sign}(\alpha) = (-1)^{5-1} = 1$

(it's a 5-cycle) - in other words $\alpha$ is even, i.e. it does belong to $A_7$:

\[\alpha \in A_7\]