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)

Problem #	Points (out of 10)
1	
2	
3	
4	

Total (out of 40):

Problem 1. Let $(G, *)$ be a cyclic group of size 6. Choose a generator $a \in G$.

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

e $\quad a \quad$ a^2 $\quad a^3 \quad$ a^4 $\quad a^5.$ 1 6 3 2 3 6 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) $\mathrm{ord}(a^n) = \dfrac{6}{\mathrm{GCD}(6,n)}$. Let $n = 0, 1, 2, \ldots, 5$:

n	0	1	2	3	4	5
$\mathrm{ord}(a^n)$	1	6	3	2	3	6

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

(b) $\langle a^2 \rangle = \{e, a^2, a^4\}$
$\langle a^3 \rangle = \{e, a^3\}$
The two non-trivial subgroups of G.

(c) $G \times G$ is abelian, but not cyclic.
Cyclic groups are abelian ($a^m * a^n = a^{m+n} = a^n * a^m$), and products of abelian groups are abelian:

$$(a,b) \bullet (c,d) = (a*c, b*d) = (c*a, d*b) = (c,d) \bullet (a,b).$$

— since G is abelian.

continued →

– However, $G \times G$ is <u>not</u> cyclic: All its elements have order ≤ 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 $(\mathbb{Z}_7^\times, \bullet)$ 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:

$$[1] \quad [2] \quad [3] \quad [4] \quad [5] \quad [6].$$

1 3 6 3 6 2 resp.

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

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

$$3^{71} \equiv r \pmod 7.$$

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

$3^1 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6 \quad 3^4 \equiv 4$

$3^5 \equiv 5 \quad 3^6 \equiv 1$ First time we get 1.

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

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

$[1]=[3]^0$	$[2]=[3]^2$	$[3]=[3]^1$	$[4]=[3]^4$	$[5]=[3]^5$	$[6]=[3]^3$
1	3	6	3	6	2
$(n=0)$	$(n=2)$	$(n=1)$	$(n=4)$	$(n=5)$	$(n=3)$

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:

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

in the range $[0,6)$.

Thus, modulo 7,

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

as we found in (a).

$\Rightarrow$ Answer is $\boxed{r=5}$.

Problem 3. Let D_4 be the dihedral group of symmetries of a square centered at the origin. Introduce

r=rotation by $\frac{\pi}{2}$ in the counterclockwise direction,

s=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 srs^{-1} on the list below. Justify your answer.

$$e \quad r \quad r^2 \quad r^3 \quad s \quad sr \quad sr^2 \quad sr^3$$

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

- D_4 is <u>non</u>-abelian: Otherwise,

$$sr = rs = sr^{-1} \overset{\text{cancellation law.}}{\Longrightarrow} r = r^{-1} \Rightarrow r^2 = e$$

- assuming r, s commute.

"commutation relation" (*)

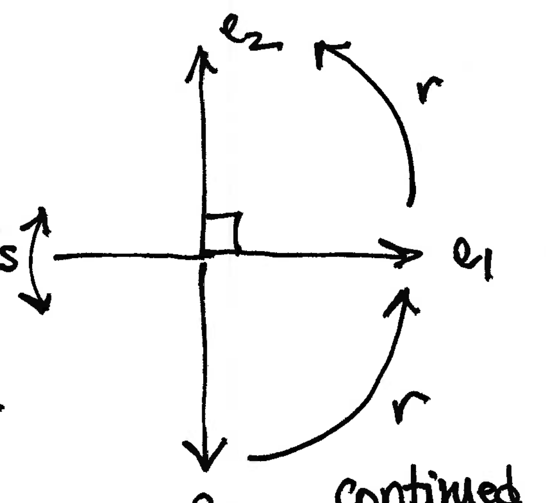
BUT r has order 4. (contradiction)

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

$$e_1 \overset{s}{\longmapsto} e_1 \overset{r}{\longmapsto} e_2$$

$$e_2 \longmapsto -e_2 \longmapsto e_1$$

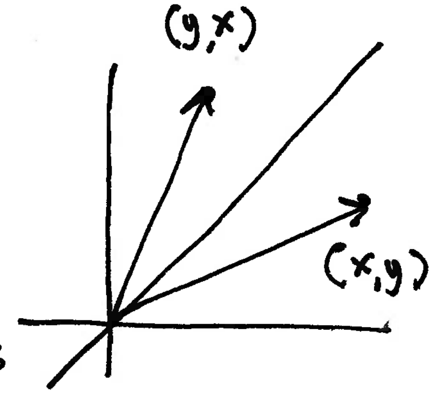
Shows rs <u>interchanges</u> e_1 and e_2



continued

★ <u>CONCLUSION</u>: The transformation rs takes a vector $\begin{pmatrix} x \\ y \end{pmatrix}$ to $\begin{pmatrix} y \\ x \end{pmatrix}$.

I.e., $rs =$ reflection across the <u>axis</u> with angle $\frac{\pi}{4}$.
$(x=y)$



(c) $$srs^{-1} \underset{s^2=e}{=} srs \underset{rs=sr^{-1}}{=} ssr^{-1} \underset{s^2=e}{=} r^{-1} \underset{r^4=e.}{=} r^3$$

so $\boxed{srs^{-1} = r^3}$.

Problem 4. Let $\alpha \in S_7$ be the permutation given by $\alpha = (1352)(5137)$.

(a) Express α 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 α a cycle? If not, find its decomposition into disjoint cycles.

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

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

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

(b) α takes $1 \mapsto 5 \mapsto 3 \mapsto 7 \mapsto 2 \mapsto 1$ (and fixes 4 and 6). So yes, α is a 5-cycle:

$$\boxed{\alpha = (15372)}.$$

(c) $\operatorname{ord}(\alpha) = \boxed{5}$ (it's a 5-cycle) and $\operatorname{sign}(\alpha) = (-1)^{5-1} = \boxed{1}$ — in other words α is even, i.e. it does belong to A_7:

$$\boxed{\alpha \in A_7}.$$