Name: Halla Daás, ID: 94836

50/53

Exam I

Ayman Badawi

QUESTION 1. (8 points) Consider $(Z_{24}, +)$. Note that $+$ means addition (mod 24).

(i) Find a subgroup, say D, of Z_{24} with exactly 6 elements.

We find an element $a \in Z_{24}$ s.t $|a| = 6$

$a = 4$. $(4^6 = 0)$.

$D = \{4, 4^2, 4^3, 4^4, 4^5, 4^6 = 0\}$

$= \{4, 8, 12, 16, 20, 0\}$ ✓ 4/4

(ii) Let D as in (i). Find all distinct left cosets of D.

$|Z_{24}| = 24$, $|D| = 6$. There are $\frac{24}{6} = 4$ distinct left cosets

1) $e + D = \{4, 8, 12, 16, 20, 0\}$

2) $1 + D = \{5, 9, 13, 17, 21, 1\}$

3) $2 + D = \{6, 10, 14, 18, 22, 2\}$

4) $3 + D = \{7, 11, 15, 19, 23, 3\}$ ✓ 4/4

QUESTION 2. (10 points)

(1) Let $(G, *)$ be a group and $a \in G$ such that $ord(a) = |a| = m < \infty$. Assume that $a^n = e$ for some positive integer n. Prove that $m \mid n$ (note $m \mid n$ means m is a factor of n).

Since $|a| = m$ and $a^n = e$, it is clear that $n \geq m$ (m is the smallest positive integer $k \geq 1$ where $a^k = e$).

Then $n = mq + r$, $q \geq 1$, $0 \leq r < m$

$e = a^n = a^{mq+r} = a^{mq} * a^r = (a^m)^q * a^r = e^q * a^r = e * a^r = a^r$

We have: $a^r = e$.

Since $r < m$ and m is the smallest integer $k \geq 1$ where $a^k = e$, then

$0 \leq r < 1 \Rightarrow r$ has to be 0. $\therefore n = mq \Rightarrow m \mid n$

6/6

(2) Let $(G, *)$ be a group with 11 elements and $a \in G$. Prove that $a = b^5$ for some $b \in G$, where $b = a^k$ for some integer k.

$n = 11$.

Since $\gcd(5, 11) = 1$,

$1 = 5K + 11n$.

$a^1 = a^{5K+11n} = \underbrace{a^{11n}}_{(a^{11})^n = e^n = e} * a^{5K} = a^{5K}$

$\Rightarrow a = (a^k)^5 = b^5$

so $b = a^k$ done

4/4

We can see that $1 = 5(-2) + 11(1)$, so $k = -2$

extra: so $b = a^{-2}$. ✓

QUESTION 3. (12 points)

(i) Let $(G,*)$ be a group and $a \in G$ such that $|a| = 15$. Prove that $D = \{a, a^2, ..., a^{15} = e\}$ is a subgroup of G.

Since D is a finite subset of G, we prove that $D < G$ by closure. Let $a^i, a^j \in D$ s.t $1 \le i,j \le 15$, then:

$a^i * a^j = a^{i+j}$.

If $i+j \le 15$, then it's clear that $a^{i+j} \in D$.

If $i+j > 15$, then $i+j = 15q + r$, $q \ge 1$, $0 \le r < 15$

so $a^{i+j} = a^{15q+r} = a^{15q} * a^r = (a^{15})^q * a^r = e * a^r = a^r$.

If $r = 0$, $a^r = e \in D$. If $r > 0$, (and $r < 15$), then $a^r \in D$ $(1 \le r < 15)$ $\therefore$ D is closed, D ≤ G

6/6

(ii) Is it possible that $|G| = 35$? Explain briefly.

Since $D < G$ & $|D| = 15$, we know by Lagrange's Theorem that $15 \mid |G|$. Assume $|G| = 35$, $15 \mid 35$? is a contradiction $(15 \nmid 35)$ so $|G| \ne 35$.

N/A

(iii) Let F be a subgroup of D (D is as in (i)) with 5 elements. Find F.

We let $a^k \in D$ s.t $|a^k| = 5$.

$|a^k| = \frac{15}{\gcd(k,15)} = 5$. $\gcd(k,15) = 3$ so $k = 3$

$\therefore F = \{a^3, (a^3)^2, (a^3)^3, (a^3)^4, (a^3)^5 = e\}$

4/4

QUESTION 4. (8 points) (1) Let $b \in G$ such that $|b| = 36$. Find $|b^9|$, $|b^8|$, $|b^{22}|$, $|b^{-1}|$, and $|(b^{22})^{-1}|$. $* \; |a^k| = \frac{|a|}{\gcd(k,|a|)}$

$|b^9| = \frac{36}{9} = 4$ $|b^{-1}| = |b| = 36$

$|b^8| = \frac{36}{4} = 9$ $|(b^{22})^{-1}| = |b^{22}| = 18$

$|b^{22}| = \frac{36}{22} = 18$

5/5

Let $a \in G, a \ne e$. We know $|a| \mid P$. Since $a \ne e$ and P is Prime, we have $|a| = P$. Hence $\{a, a^2, a^3, ..., a^P = e\} = G$. Let $x, y \in G$. Then $x = a^i$, $y = a^j$ $\Rightarrow x * y = a^i * a^j = a^j * a^i = y * x$.

. (2) Let $(G,*)$ be a group such that $|G| = p$, for some prime integer p. Prove that G is abelain.

$a * b = b * a \; \forall a, b \in G$

1/3

Since p is prime, and as a consequence of Lagrange, we know that $\forall a \in G$, $|a| = 1$ or $|a| = p$. $|a| = 1$ if $a = e$ and $|a| = p$ if $a \ne e$.

(We also know that $(a*b)^m = a^m * b^m$ iff G is abelian.)

Let $a, b \in G$.

Since G is closed, $a*b \in G$. Then $|a*b| = 1$ or p. If order $= 1$,

$\Rightarrow (a*b)^1 = e$ so $b = a^{-1}$. Then $a*b = e = b*a$

Since $|a| = p$

* If order $= p$, then $(a*b)^p = e$

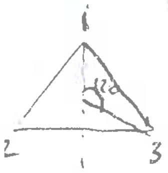
but we know $a^p = e$ and $b^p = e$ so $(a*b)^p = a^p * b^p = e$ $\therefore$ G is abelian

QUESTION 5. (6 points) (1) Let G be a group with n elements and let $a \in G$. Prove that $a^n = e$ for every $a \in G$.

Let $|a| = m$, then we know that $D = \{a, a^2, \dots, a^m\}$ is a subgroup of G. By Lagrange, $|D| \mid |G|$ so $m \mid n$.
$\Rightarrow n = mk$, $k \in N^*$. Then $a^n = a^{mk} = (a^m)^k = e^k = e$.

3/3

L_1



(2) Consider the symmetric group D_3. Find $L_1 \circ R_{120}$ and $R_{120} \circ L_1$.

$L_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$L_1 \circ R_{120} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

3/3

$R_{120} \circ L_1 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

QUESTION 6. (9 points) Let $G = (Z_{15}, +) \oplus (Z_{11}^*, \cdot)$.

(i) Find $|G|$

$= |Z_{15}| \times |Z_{11}^*| = 15 \times 10 = 150$ 1.5/1.5

(ii) Let m be the maximum order of an element in G. Find m. 1.5/1.5

We know that $m = LCM[\underset{max}{|a|}, \underset{max}{|b|}]$ for some $a \in (Z_{15}, +)$ & $b \in Z_{11}^*$.

max $|a| = |1| = 15$ and max $|b| = 10$ (since 11 is prime, $\exists\, b \in Z_{11}$ s.t $|b| = 10$)

Then $m = LCM(15, 10) = 30$

(iii) Find $|(4, 2)|$.

Let $|(4,2)| = m$. Then $(4^m, 2^m) = (0, 1)$. $\Rightarrow |4| \mid m$ and $|2| \mid m$

$|4| = 15$, $|2| = 10$, $m = LCM(15, 10) = 30$. 1.5/1.5

(iv) Find $(8, 10)^{-1}$.

$(8, 10)^{-1} = (8^{-1}, 10^{-1}) = (7, 10)$ 1.5/1.5

$10 \cdot x = 1$

(v) Find a subgroup H of G with 6 elements.

Let $(x, y) \in G$ s.t $|(x,y)| = 6$. Then $LCM(|x|, |y|) = 6$

Let $|x| = 3$, $|y| = 2$. (since $|x| \mid 15$ and $|y| \mid 10$)

Then $x = 5$, $y = 10$

Then $H = \{(5,10), (5,10)^2, (5,10)^3, (5,10)^4, (5,10)^5, (5,10)^6 = e\}$

3/3