Department of Mathematics, METU, MATH 116 - BASIC ALGEBRAIC STRUCTURES

# FIRST MIDTERM

31st March 2016. Duration : 100 minutes. Three questions : 20 + 10 , 10 + 10 + 10 + 10 , 10 + 10 + 10

| STUDENT NUMBER | NAME, FAMILY NAME | Q1 | Q2 | Q3 | TOTAL |
|---|---|---|---|---|---|
| | | | | | |

Solutions

1. Consider the binary operation $\star$ on $\mathbb{Z}$ defined for each $x, y \in \mathbb{Z}$ by

$$x \star y = x + y - 3$$

(A) Prove that $\mathbb{Z}$ constitutes a group with respect to the binary operation $\star$.
(B) Let $\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}$ be the map defined for each $x \in \mathbb{Z}$ by

$$\varphi(x) = x - 3\,.$$

Prove that $\varphi$ is an isomorphism from the group on $\mathbb{Z}$ with respect to $\star$ to the group on $\mathbb{Z}$ with the ordinary addition.

---

(A) $*$ is

Associative : $x * (y * z) = x + (y * z) - 3 = x + (y + z - 3) - 3$
$= (x + y - 3) + z - 3 = (x * y) * z$

With identity $= 3$ : $x * 3 = x + 3 - 3 = x$
$3 * x = 3 + x - 3 = x$

& inverses : The inverse of $x \in \mathbb{Z}$ is $6 - x$ : Indeed
$x * (6 - x) = x + 6 - x - 3 = 3$
$(6 - x) * x = 6 - x + x - 3 = 3$

(B) $\varphi$ is a bijection ; indeed $\varphi^{-1}(y) = y + 3$.
To see that it is an isomorphism, observe that

$\varphi(x * y) = x * y - 3 = x + y - 3 - 3$
$= (x - 3) + (y - 3)$
$= \varphi(x) + \varphi(y)$.

**2.** Consider the group $U_9$ of invertible elements of $\mathbb{Z}_9$ with respect to multiplication modulo 9.

(A) Make a list of the elements of $U_9$.
(B) Construct the multiplication table of $U_9$.
(C) Determine whether $U_9$ is a cyclic group.
(D) Find <u>all</u> subgroups of $U_9$.

---

(A) Invertible elements of $\mathbb{Z}_9$ are those $[n]$ with $(n,9)=1$. ($n$ for brevity!)

Hence $U_9 = \{1, 2, 4, 5, 7, 8\}$. Alternatively: $1^{-1}=1$, $2^{-1}=5$, $4^{-1}=7$, $8^{-1}=8$ by direct checking.

(B)

| | 1 | 2 | 4 | 5 | 7 | 8 |
|---|---|---|---|---|---|---|
| 1 | 1 | 2 | 4 | 5 | 7 | 8 |
| 2 | 2 | 4 | 8 | 1 | 5 | 7 |
| 4 | 4 | 8 | 7 | 2 | 1 | 5 |
| 5 | 5 | 1 | 2 | 7 | 8 | 4 |
| 7 | 7 | 5 | 1 | 8 | 4 | 2 |
| 8 | 8 | 7 | 5 | 4 | 2 | 1 |

(C) Yes, $U_9$ is cyclic.

Indeed

$$U_9 = \langle 2 \rangle = \{\underset{=1}{2^0}, \underset{=2}{2^1}, \underset{=4}{2^2}, \underset{=8}{2^3}, \underset{=7}{2^4}, \underset{=5}{2^5}\} \simeq \mathbb{Z}_6$$

(D) Since $U_9$ is cyclic, all its subgroups are cyclic.
The trivial subgroups: $\underset{=\langle 1 \rangle}{\{1\}}$ & $\underset{=\langle 2 \rangle = \langle 5 \rangle}{U_9}$

$$\langle 4 \rangle = \langle 7 \rangle = \{1, 4, \underset{=4^2}{7}\}$$

$$\langle 8 \rangle = \{1, 8\}$$

**3.** For an arbitrary group $G$, and an element $x \in G$, let

$$\mathrm{C}(x) = \left\{ y \in G \;\middle|\; xy = yx \right\}$$

(A) Prove that $\mathrm{C}(x)$ is a subgroup of $G$.
(B) Show that $\mathrm{C}(x) = \mathrm{C}(x^{-1})$ for any $x \in G$.
(C) Let $G = \mathrm{S}_3 = \left\{ I, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2 \right\}$ be the group of permutations of the set $\{1, 2, 3\}$ where

$$\sigma = (2\,3) = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad \rho = (1\,2\,3) = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}$$

Make a list of the elements of $\mathrm{C}(\sigma\rho)$. (If you wish you may use the facts that $\sigma\rho = \rho^2\sigma$ and $\rho\sigma = \sigma\rho^2$.)

---

(A) If $a, b \in C(x)$, then $abx = axb = xab$ hence $ab \in C(x)$.
Thus, $C(x)$ is closed with respect to the binary operation.

$e \in C(x)$ as $ex = x = xe$

If $a \in C(x)$ then $ax = xa$ hence $axa^{-1} = x$ hence $xa^{-1} = a^{-1}x$

showing that $a^{-1} \in C(x)$, too.

It follows that $C(x)$ is a subgroup of $G$.

(B) $a \in C(x)$ iff $ax = xa$ iff $x^{-1}ax = a$ iff $x^{-1}a = ax^{-1}$
iff $a \in C(x^{-1})$. This being true for arbitrary $a \in C(x)$
we conclude that $C(x) = C(x^{-1})$.

(C) $\rho(\sigma\rho) = \sigma\rho^2\rho = \sigma \neq \sigma\rho^2 = (\sigma\rho)\rho$

$\rho^2(\sigma\rho) = \sigma\rho\rho = \sigma\rho^2 \neq \sigma = (\sigma\rho)\rho^2$

$\sigma(\sigma\rho) = \rho \neq \rho^2 = \sigma^2\rho^2 = (\sigma\rho)\sigma$

$\sigma\rho(\sigma\rho) = (\sigma\rho)\sigma\rho$ obviously

$\sigma\rho^2(\sigma\rho) = \sigma^2\rho^2 = \rho^2 \neq \rho = \sigma^2\rho^4 = (\sigma\rho)\sigma\rho^2$

$\therefore$ $C(\sigma\rho) = \{e, \sigma\rho\}$