Name: Rajat Rajesh shetty Assignment-7
CWID: 10477484

① Find the smith normal form of the Matrix

$$\begin{bmatrix} 1 & 2 & 1 \\ 3 & 4 & 0 \\ 2 & 1 & -1 \end{bmatrix}$$

show all steps!

$$\Rightarrow \begin{bmatrix} 1 & 2 & 1 \\ 3 & 4 & 0 \\ 2 & 1 & -1 \end{bmatrix} \xrightarrow{r_2-3r_1} \begin{pmatrix} 1 & 2 & 1 \\ 0 & -2 & -3 \\ 2 & 1 & -1 \end{pmatrix}$$

$$\xrightarrow{r_3-2r_1} \begin{pmatrix} 1 & 2 & 1 \\ 0 & -2 & -3 \\ 0 & -3 & -3 \end{pmatrix} \xrightarrow{r_2\cdot(-1)} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 3 \\ 0 & -3 & -3 \end{pmatrix}$$

$1-2\cdot 2$
$=-3$
$1-2(1)$
$=-3$

$$\xrightarrow{r_3\cdot(-1)} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 2 & 3 \\ 0 & 3 & 3 \end{pmatrix} \xrightarrow{r_2-r_3} \begin{pmatrix} 1 & 2 & 1 \\ 0 & -1 & 0 \\ 0 & 3 & 3 \end{pmatrix} \xrightarrow{r_2(-1)} \begin{pmatrix} 1 & 2 & 1 \\ 0 & 1 & 0 \\ 0 & 3 & 3 \end{pmatrix}$$

$$\xrightarrow{r_1-2r_2} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 3 & 3 \end{pmatrix} \xrightarrow{r_3-3r_2} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix} \xrightarrow{C_3-C_1} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

$$\Rightarrow \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

soln //

(2) Consider the set $Hom(\mathbb{Z}^n, \mathbb{Z}_2)$ of homomorphisms from $\mathbb{Z}^n$ to $\mathbb{Z}_2$ has 2^n elements. Fix the standard free basis $\{e_1 \dots e_n\}$ for $\mathbb{Z}^n$.

(a) Consider any homomorphism $\varphi: \mathbb{Z}^n \to \mathbb{Z}_2$. Let $b_i = \varphi(e_i)$ for $i = 1 \dots n$. Let $v = (\alpha_1 \dots \alpha_n) \in \mathbb{Z}^n$ s.t. $\varphi(v)$ is uniquely defined by $b_1 \dots b_n$ ie, find a formula for $\varphi(v)$.

(b) P.T for any $b_1 \dots b_n \in \{0,1\}$ there exists a homomorphism φ satisfying $b_i = \varphi(e_i)$ for every $i = 1, \dots, n$.

(c) Conclusion. There are 2^n choices of $b_1 \dots b_n \in \{0,1\}$. each choice defines a unique homomorphism. Hence, there are 2^n homomorphisms.

$\Rightarrow$ a)

assume: $v = \alpha_1 e_1 + \dots + \alpha_n e_n \quad (\alpha_i \in \mathbb{Z})$

$$\therefore \varphi(v) = \varphi(\alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n)$$
$$= \varphi(\alpha_1 e_1) + \dots + \varphi(\alpha_n e_n) \quad \text{(By property of Homomorphism)}$$
$$= \varphi(\alpha_1)\varphi(e_1) + \dots + \varphi(\alpha_n)\varphi(e_n)$$
$$= \alpha_1 b_1 + \dots + \alpha_n b_n \quad [\because \alpha_i \in \mathbb{Z} \text{ (scalar) } \& \ \varphi(e_i) = b_i]$$

thus the formula of $\varphi(v)$ which is uniquely represented.

b) suppose $b_1, b_2 \dots b_n \in \{0,1\}$.

since every no in $\mathbb{Z}$ can be written as

$b = \alpha_1 b_1 + \alpha_2 b_2 + \dots + \alpha_n b_n \ ; \ \alpha_i \in \mathbb{Z}$

so assume: $\varphi(v) = b$ ie. $\varphi(v_i) = \alpha_i b_i$ for $i = n$.

As, $\alpha_i \in \mathbb{Z}$ so we can write $\varphi(v_i) = \varphi(\alpha_i) b_i$

so there exists an identity e_i for $\varphi(e_i) = b_i$

so $\varphi(v_i) = \varphi(\alpha_i)\varphi(e_i) = \alpha_i \varphi(e_i) = \varphi(\alpha_i e_i)$

$\because \alpha_i \in \mathbb{Z}$, so $\varphi(\alpha_i e_i) = \varphi(\alpha_i)\varphi(e_i)$

ie, φ is an homomorphism.

Hence there exists a homomorphism φ.

ST $\varphi(e_i) = b_i$

This completes the proof.

(c) since $\mathbb{Z}^n$ contains n elements & $\mathbb{Z}^2$ contains 2 elements.

Since homomorphism is unique

Since homomorphism & 2^n choices so total no of homomorphism is 2^n.

7.3 Suppose that G is an abelian group generated by x_1 & x_2. Using a quantum algo we learn x_1 & x_2 are subject to the following relations:

$$r_1 = 6x_1 + 10x_2 = 0$$
$$r_2 = 16x_1 - 2x_2 = 0$$
$$r_3 = -4x_1 + 18x_2 = 0$$

Assuming that this sets of relation is complete express G as a direct product of cyclic groups.

$\Rightarrow$

$$r_1 = 6x_1 + 10x_2 = 0$$
$$r_2 = 14x_1 - 2x_2 = 0$$
$$r_3 = -4x_1 + 18x_2 = 0$$

$$\begin{pmatrix} 6 & 10 \\ 14 & -2 \\ -4 & 18 \end{pmatrix} \xrightarrow{r_1 \to r_1 + r_3} \begin{pmatrix} 2 & 28 \\ 14 & -2 \\ -4 & 18 \end{pmatrix} \xrightarrow{r_3 \to r_3 + 2r_1} \begin{pmatrix} 2 & 28 \\ 14 & -2 \\ 0 & 74 \end{pmatrix}$$

$6-4 = 2$, $10+18 = 28$, $-4+2(2) = 0$, $18+2(28)$

$$\xrightarrow{r_2 \to r_2 - 7r_1} \begin{pmatrix} 2 & 28 \\ 0 & 198 \\ 0 & 74 \end{pmatrix} \xrightarrow{C_2 \to C_2 - 14C_1} \begin{pmatrix} 2 & 0 \\ 0 & 198 \\ 0 & 74 \end{pmatrix} \xrightarrow{r_2 \to r_2 - 2r_3} \begin{pmatrix} 2 & 0 \\ 0 & 50 \\ 0 & 74 \end{pmatrix}$$

$$\xrightarrow{r_3 \to r_3 - r_2} \begin{pmatrix} 2 & 0 \\ 0 & 50 \\ 0 & 24 \end{pmatrix} \xrightarrow{r_2 \to r_2 - r_3} \begin{pmatrix} 2 & 0 \\ 0 & 26 \\ 0 & 24 \end{pmatrix} \xrightarrow{r_2 \to r_2 - r_3} \begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 24 \end{pmatrix} \xrightarrow[-12r_2]{r_3 \to r_3} \begin{pmatrix} 2 & 0 \\ 0 & 2 \\ 0 & 0 \end{pmatrix}$$

so $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

7.4 Suppose that G is an albelian group generated by x_1, x_2, x_3. Using a quantum algorithm we learn that x_1, x_2, x_3 are subject to the following relations:

$$r_1 = 2x_1 + 4x_2 - 4x_3 = 0$$
$$r_2 = -4x_1 + 2x_2 + 8x_3 = 0.$$

Assuming that this set of relation is complete express G as a direct product of cyclic group.

$\Rightarrow$ $r_1 = 2x_1 + 4x_2 - 4x_3 = 0$

$r_2 = -4x_1 + 2x_2 + 8x_3 = 0.$

$$\begin{pmatrix} 2 & 4 & -4 \\ -4 & 2 & 8 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_3 \to C_3 - 2C_1} \begin{pmatrix} 2 & 4 & 0 \\ -4 & 2 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{R_2 \to R_2 + 2R_1} \begin{pmatrix} 2 & 4 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$-4 + 2 \cdot 2 = 0$ $\quad$ $2 + 2(4) = 10$

$$\xrightarrow{C_1 \leftrightarrow C_2} \begin{pmatrix} 4 & 2 & 0 \\ 10 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_1 \to C_1 - 2C_2} \begin{pmatrix} 0 & 2 & 0 \\ 10 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \xrightarrow{C_1 \leftrightarrow C_2} \begin{pmatrix} 2 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

so, $G \simeq \mathbb{Z}_2 \cdot \mathbb{Z}_{10} \cdot \mathbb{Z}$

I.5 which of the following rings are fields? if R is a ring, then find inverses of all nontrivial elements or a formula to compute the inverse. If R is not a ring, then find a nontrivial elements that has no inverse.

(a) $(\mathbb{Z}_5, +\cdot)$

(b) $(\mathbb{Z}_6, +\cdot)$

(c) $\{a+b\sqrt{5} \mid a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$ with the ausual addition & multiplication

⇒(a) $(\mathbb{Z}_5, +\cdot)$ is a field.

Clearly, $(\mathbb{Z}_5, +, \cdot)$ is commutative ring.

unity = 1

$(1)^{-1} = 1$ $\quad (2)^{-1} = 4 \quad 3^{-1} = 3 \quad 4^{-1} = 2.$

every nontrivial element is unit.

$\therefore \Rightarrow (\mathbb{Z}_5, +, \cdot)$ is field

(b) $(\mathbb{Z}_6, +\cdot)$

as $2 \cdot 3 = 0$ in $\mathbb{Z}_6$.

$\mathbb{Z}_6$ has 0 divisors.

2, 3, 4 are not unit.

thus $(\mathbb{Z}_6, +\cdot)$ is not field

(c) $\{a+b\sqrt{5} \mid a, b \in \mathbb{Q}\}$

$\{a+b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ is commutative

unity = 1

$(a+b\sqrt{5})(a-b\sqrt{5}) = a^2 - 5b^2$

$$\frac{1}{a+b\sqrt{5}} = \frac{a-b\sqrt{5}}{a^2-5b^2}$$

every non~~[illegible]~~ element is unit.

zero/non trivial

$\Rightarrow \{a+b\sqrt{5} \mid a.b\in\mathbb{Q}\}$ is field with $(+,\cdot)$