5a. (i) $\mathcal{G}$ is closed with respect to multiplication:

$$\begin{bmatrix} \alpha_1 & \beta_1 \\ 2\beta_1 & \alpha_1 \end{bmatrix}\begin{bmatrix} \alpha_2 & \beta_2 \\ 2\beta_2 & \alpha_2 \end{bmatrix} = \begin{bmatrix} \alpha_1\alpha_2 + 2\alpha_2\beta_2 & \alpha_1\beta_2 + \alpha_2\beta_1 \\ 2\beta_1\alpha_2 + 2\alpha_1\beta_2 & 2\beta_1\beta_2 + \alpha_1\alpha_2 \end{bmatrix}$$

$\in \mathcal{G}$.

Moreover, the product is symmetric in $((\alpha_1,\beta_1),(\alpha_2,\beta_2))$, therefore the operation is commutative

(ii) Unit element:

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in \mathcal{G}.$$

(iii)

$$\begin{bmatrix} \alpha & \beta \\ 2\beta & \alpha \end{bmatrix}^{-1} = \underbrace{\begin{bmatrix} \alpha & 2\beta \\ \beta & \alpha \end{bmatrix}}_{\in \mathcal{G}} \cdot \frac{1}{\alpha^2+\beta^2} \quad (\alpha^2+\beta^2)^{-1}$$

Text

because $2(2\beta)=\beta$

$\alpha^2+\beta^2 \neq 0$ if ~~$\alpha \neq 0 \neq \beta$~~ $(\alpha,\beta)\neq(0,0)$

α	β	$\alpha^2+\beta^2$
0	1	1
1	0	1
1	1	2
1	2	2
2	0	1
2	1	2
2	2	2
~~0~~ 1	~~1~~ 0	1

(i)' $(\alpha,\beta)\neq(0,0) \Leftrightarrow$

$$\det\begin{bmatrix} \alpha & \beta \\ 2\beta & \alpha \end{bmatrix} \neq 0$$

$\det(A_1 \cdot A_2) = \det(A_1)\cdot\det(A_2)$

$\Rightarrow A_1A_2 \in \mathcal{G}$.

(iv) Associativity is always satisfied for matrix multiplication.

(b) $p(x)=x^2+1$ is irreducible ($p(0)=1, p(1)=2, p(2)=2$)

$\Rightarrow$ $\mathbb{Z}_3[x]/\langle x^2+1\rangle$ is a field.

define

$$\varphi\left(\begin{bmatrix}\alpha & \beta \\ 2\beta & \alpha\end{bmatrix}\right) = \alpha+\beta x + \langle x^2+1\rangle$$

(i) $\mathbb{F} = \{\alpha+\beta x+\langle x^2+1\rangle \mid \alpha,\beta\in\mathbb{Z}_3\}$.

$\mathbb{F}\setminus\{0\} = \{\alpha+\beta x+\langle x^2+1\rangle \mid \alpha,\beta \neq (0,0)\}$.

$\Rightarrow$ φ is surjective.

(ii) $\varphi\left(\begin{bmatrix}\alpha_1 & \beta_1 \\ 2\beta_1 & \alpha_1\end{bmatrix}\right) = \varphi\left(\begin{bmatrix}\alpha_2 & \beta_2 \\ 2\beta_2 & \beta_2\end{bmatrix}\right)$

$\Rightarrow$ $\alpha_1+\beta_1 x = \alpha_2+\beta_2 x$

$\Rightarrow$ $\alpha_1=\alpha_2,\ \beta_1=\beta_2$

$\Rightarrow$ φ is injective

(iii) $\varphi\left(\begin{bmatrix}\alpha_1 & \beta_1 \\ 2\beta_1 & \alpha_1\end{bmatrix}\begin{bmatrix}\alpha_2 & \beta_2 \\ 2\beta_2 & \alpha_2\end{bmatrix}\right)$

$$=\varphi\left(\begin{bmatrix}\alpha_1\alpha_2+2\alpha_2\beta_2 & \alpha_1\beta_2+\alpha_2\beta_1 \\ 2\alpha_1\beta_2+2\alpha_2\beta_1 & 2\beta_1\beta_2+\alpha_1\alpha_2\end{bmatrix}\right)$$

$$= (\alpha_1\alpha_2+2\alpha_2\beta_2) + (\alpha_1\beta_2+\alpha_2\beta_1)x + \langle x^2+1\rangle$$

$$(\alpha_1+\beta_1 x)(\alpha_2+\beta_2 x)+\langle x^2+1\rangle = \alpha_1\alpha_2 + (\alpha_1\beta_2+\alpha_2\beta_1)x + \beta_1\beta_2 x^2 + \langle x^2+1\rangle$$

$$= (\alpha_1\alpha_2+2\beta_1\beta_2) + (\alpha_1\beta_2+\alpha_2\beta_1)x + \langle x^2+1\rangle$$

$= \cancel{\varphi(\alpha_1+\beta_1 x).}$ ($x^2+\langle x^2+1\rangle = 2+\langle x^2+1\rangle$.)

2. $\alpha = (1\,2\,3\,4\,5)(6\,7\,8)$

$= (1\,5)(1\,4)(1\,3)(1\,2)\cdot(6\,8)(6\,7)$

$\beta = (1)(2\,3\,8\,4\,7)(5\,6)$

$= (1\,2)(2\,1)(2\,7)(2\,4)(2\,8)(2\,3)(5\,6)$

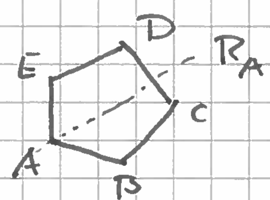
$$\beta\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 7 & 6 & 1 & 2 & 4 & 5 \end{bmatrix}$$

$= (1\,3\,7\,4\,6\,2\,8\,5)$

$= (1\,5)(1\,8)(1\,2)(1\,6)(1\,4)(1\,7)(1\,3)$

(c) $|\alpha| = \mathrm{lcm}(5,3) = 15$

7. Group of transformation (permutations) that leaves pentagon invariant is D_5:



D_5: 5 rotations:

$R_0, R_{72}, R_{144}, R_{216}, R_{288}$

5 reflections:

R_A, R_B, R_C, R_D, R_E

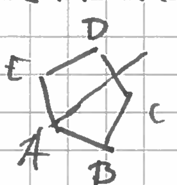
all edges same color

$|S| = 2^5$

$|Fix(R_0)| = |S| = 2^5$ $\quad |Fix(R_{72})| = \ldots = |Fix(R_{288})| = 2$

$|Fix(R_A)| = |Fix(R_B)| = |Fix(R_C)| = |Fix(R_D)| = |Fix(R_E)|$

$= 2^3$



$$\left.\begin{array}{lll} AE, AB & \text{same color:} & 2 \\ BC, DE & \text{"} \quad \text{"} & : 2 \\ DC & \text{ind.} & : 2 \end{array}\right\} 2^3$$

Total number of fixes:

$$2^5 + 4.2 + 5.2^3 = 32 + 8 + 40 = 80$$

$\Rightarrow$ Different configurations $\dfrac{80}{|D_5|} = 8.$

8.(a) $a(x)$ irreducible $\Leftrightarrow$ $a(0) \neq 0 \neq a(1)$

$a(0) = a_0 \Rightarrow a_0 = 1$

$\Rightarrow a(1) = 1 + a_1 + \cancel{0}1 = a_1 \Rightarrow a_1 = 1$

$\Rightarrow a(x) = x^2 + x + 1$

(b) $p(x)$ irreducible $\Leftrightarrow$ $p(x) \neq m(x)n(x)$

if $\deg m(x) = 1$ then $p(0) = 0$ or $p(1) = 1$:

$p(0) = 1$, $p(1) = 1$

$\Rightarrow$ $m(x)$ and $n(x)$ are irreducible factors of degree 2

$\overset{(a)}{\Longrightarrow}$ $m(x) = n(x) = a(x) = x^2 + x + 1$

$(x^2 + x + 1)^2 = x^4 + x^2 + 1 \neq p(x)$

Conclusion $p(x)$ is irreducible

(c) $p(x)$ irr. $\Rightarrow$ $\langle p(x) \rangle$ maximal

$\Rightarrow$ $\mathbb{Z}_2[x]/\langle p(x) \rangle$ is a field

(d) $\mathbb{Z}_2[x]/\langle p(x) \rangle = \{ m_0 + m_1 x + m_2 x^2 + m_3 x^3 + \langle p(x) \rangle \mid m_i \in \mathbb{Z}_2, i = 0,1,2,3 \}.$

$\Rightarrow |\mathbb{F}| = 2^4 = 16.$