

Algebra - 2017 Test

These answers have been transcribed from the barely legible handwriting that was given on Canvas. There thus may be errors in the solutions; please check and let me know if something's not quite right.

1. Let G be the set of matrices given by:

$$G = \left\{ \begin{bmatrix} \alpha & \beta \\ 2\beta & \alpha \end{bmatrix} \mid \alpha, \beta \in \mathbb{Z}_3, \alpha^2 + \beta^2 \neq 0 \right\}$$

On G we consider the operation matrix multiplication.

(a) (6 points) Show that G with matrix multiplication forms a group.

Solution:

1. G is closed with respect to multiplication:

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

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

2. Unit element:

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

3. Inverse:

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

because $2(2\beta) = \beta$ if $(\alpha, \beta) \neq (0, 0)$.

(b) (6 points) Let $\mathbb{F} = \mathbb{Z}_3[x] / \langle x^2 + 1 \rangle$. Show that $\phi : G \rightarrow \mathbb{F} \setminus \{0\}$ defined by

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

is a group isomorphism from G to the multiplicative group of the field \mathbb{F} .

Solution: $p(x) = x^2 + 1$ is irreducible ($p(0) = 1, p(1) = 2, p(2) = 2$). Therefore $\mathbb{Z}_3[x] / \langle x^2 + 1 \rangle$ is a field.

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

1.

$$\begin{aligned}\mathbb{F} &= \{ \alpha + \beta x + \langle x^2 + 1 \rangle \mid \alpha, \beta \in \mathbb{Z}_3 \} \\ \mathbb{F} \setminus \{0\} &= \{ \alpha + \beta x + \langle x^2 + 1 \rangle \mid \alpha, \beta \neq (0, 0) \} \\ &\Rightarrow \phi \text{ is surjective.}\end{aligned}$$

2.

$$\begin{aligned}\phi \left(\begin{bmatrix} \alpha_1 & \beta_1 \\ 2\beta_1 & \alpha_1 \end{bmatrix} \right) &= \phi \left(\begin{bmatrix} \alpha_2 & \beta_2 \\ 2\beta_2 & \alpha_2 \end{bmatrix} \right) \\ \Rightarrow \alpha_1 + \beta_1 x &= \alpha_2 + \beta_2 x \\ \Rightarrow \alpha_1 = \alpha_2, \beta_1 &= \beta_2 \\ \Rightarrow \phi &\text{ is injective.}\end{aligned}$$

3.

$$\begin{aligned}\phi \left(\begin{bmatrix} \alpha_1 & \beta_1 \\ 2\beta_1 & \alpha_1 \end{bmatrix} \begin{bmatrix} \alpha_2 & \beta_2 \\ 2\beta_2 & \alpha_2 \end{bmatrix} \right) \\ = \phi \left(\begin{bmatrix} \alpha_1 \alpha_2 + 2\alpha_2 \beta_1 & \alpha_1 \beta_2 + \alpha_2 \beta_1 \\ 2\alpha_1 \beta_2 + 2\alpha_2 \beta_1 & 2\beta_1 \beta_2 + \alpha_1 \alpha_2 \end{bmatrix} \right) \\ = (\alpha_1 \alpha_2 + 2\alpha_2 \beta_2) + (\alpha_1 \beta_2 + \alpha_2 \beta_1)x + \langle x^2 + 1 \rangle \\ \\ (\alpha_1 + \beta_1 x)(\alpha_1 + \beta_2 x) + \langle x^2 + 1 \rangle \\ = \alpha_1 \alpha_2 + (\alpha_1 \beta_2 + \alpha_2 \beta_1)x + \beta_1 \beta_2 x^2 + \langle x^2 + 1 \rangle \\ = (\alpha_1 \alpha_2 + 2\beta_1 \beta_2) + (\alpha_1 \beta_2 + \alpha_2 \beta_1)x + \langle x^2 + 1 \rangle \\ = x^2 + \langle x^2 + 1 \rangle = 2 + \langle x^2 + 1 \rangle\end{aligned}$$

2. Given the permutations:

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

Write α , β and $\beta\alpha$ as:

- (5 points) Product of disjoint cycles.
- (5 points) Product of 2-cycles.
- (4 points) Determine the order of α .

Solution:

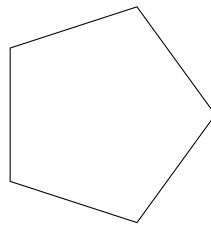
$$\begin{aligned}\alpha &= (12345)(678) \\ &= (15)(14)(13)(12)(68)(67)\end{aligned}$$

$$\begin{aligned}\beta &= (1)(23847)(56) \\ &= (12)(21)(27)(24)(28)(23)(56)\end{aligned}$$

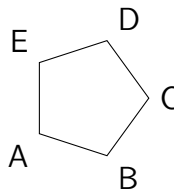
$$\begin{aligned}\beta\alpha &= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 7 & 6 & 1 & 2 & 4 & 5 \end{bmatrix} \\ &= (13746285) \\ &= (15)(18)(12)(16)(14)(17)(13)\end{aligned}$$

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

3. (10 points) Use Burnside's theorem to determine the number of different ways in which the edges of a regular pentagon (see figure), made of copper wire, can be colored using two colors.



Solution: The group of transformations (permutations) that leaves the pentagon invariant is D_5 .



D_5 has 5 rotations ($R_0, R_{72}, R_{144}, R_{216}, R_{288}$) and 5 reflections: R_A, R_B, R_C, R_D, R_E .

$$|S| = 2^5.$$

$$|\text{fix}(R_0)| = |S| = 2^5$$

$$|\text{fix}(R_{72})| = \cdots = |\text{fix}(R_{288})| = 2$$

$$|\text{fix}(R_A)| = \cdots = |\text{fix}(R_E)| = 2^3$$

$((AE, AB), (BC, DE), (CD))$ must have the same color for R_A)

The total number of fixes is $2^5 + 4 \cdot 2 + 5 \cdot 2^3 = 32 + 8 + 40 = 80$. So the total number of different configurations is $\frac{80}{|D_5|} = 8$.

4. (a) (3 points) Let $a(x) = x^2 + a_1x + a_0 \in \mathbb{Z}_2[x]$. Determine all values of $a_0, a_1 \in \mathbb{Z}_2$ for

which $a(x)$ is irreducible.

Solution: $a(x)$ irreducible $\Leftrightarrow a(0) \neq 0 \neq a(1)$

$$\begin{aligned}a(0) = a_0 &\Rightarrow a_0 = 1 \\ \Rightarrow a(1) = 1 + a_1 + 1 = a_1 &\Rightarrow a_1 = 1 \\ \Rightarrow a(x) = x^2 + x + 1\end{aligned}$$

(b) (4 points) Let $p(x) = x^4 + x^3 + x^2 + x + 1 \in \mathbb{Z}_2[x]$.

Prove that $p(x)$ is irreducible.

Solution: $p(x)$ irreducible $\Leftrightarrow p(x) \neq m(x)n(x)$

If $\deg m(x) = 1$ then $p(0) = 0$ or $p(1) = 1$.

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

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

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

Conclusion: $p(x)$ is irreducible.

(c) (3 points) Let $\mathbb{F} = \mathbb{Z}_2[x] / \langle p(x) \rangle$.

Is \mathbb{F} a field?

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

(d) (4 points) What is the number of elements of \mathbb{F} ?

Solution:

$$\begin{aligned}\mathbb{Z}_2[x] / \langle p(x) \rangle &= \{m_0 + m_1x + m_2x^2 + m_3x^3 + \langle p(x) \rangle \mid m_i \in \mathbb{Z}_2, i = 0, 1, 2, 3\} \\ \Rightarrow |\mathbb{F}| &= 2^4 = 16\end{aligned}$$

Question:	1	2	3	4	Total
Points:	12	14	10	14	50
Score:					