

Topic 16 · Sheet A: Questions

Group actions, orbits, fields and linear congruences

Suggested time

About 75 minutes

Total marks

76

Questions

12

Builds on

Topics 1 to 15

How to use this sheet. Work on your own paper. The questions start gently and get harder; questions 11 and 12 are exam style. Marks are a guide to how much working is expected, roughly one minute per mark. You need group actions, the permutation action, orbits and fixed points, fields, the finite fields $\mathbb{Z}/p\mathbb{Z}$ and linear congruences, plus Topics 1 to 15. This is the last sheet, so it draws on the whole module.

Notation. A group action of G on X is written $g \cdot x$, with $e_G \cdot x = x$ and $g \cdot (h \cdot x) = (gh) \cdot x$. In the permutation action of $\text{Sym}(n)$ on X^n , $y = \sigma \cdot x$ means $y_{\sigma(i)} = x_i$ for all $i \in \llbracket n \rrbracket$; equivalently $y_j = x_{\sigma^{-1}(j)}$. The orbit of x is $G \cdot x = \{g \cdot x \mid g \in G\}$, and x is a fixed point when $G \cdot x = \{x\}$. $\Delta(k) = \{(a, b, c) \in \mathbb{N}^3 \mid a + b + c = k\}$. In D_8 , R_θ and M_θ are as on Topic 13.

1

4 marks

Decide whether each rule defines a group action. If not, name the property that fails.

- (a) $(\mathbb{Z}, +)$ acting on $\mathbb{Z}$ by $n \cdot x = x + n$ [1]
- (b) C_2 acting on $\mathbb{R}$ by $[k]_2 \cdot x = (-1)^k x$ [1]
- (c) $(\mathbb{Z}, +)$ acting on $\mathbb{Z}$ by $n \cdot x = nx$ [1]
- (d) D_8 acting on $\{a, b\}$ by $g \cdot x = x$ [1]

2

4 marks

Label the days of the week $X = \{\text{Mon, Tue, Wed, Thu, Fri, Sat, Sun}\}$, and let $(\mathbb{Z}, +)$ act on X by $n \cdot d = \text{the day } n \text{ days after } d$.

- (a) Find $3 \cdot \text{Fri}$. [1]
- (b) Find $10 \cdot \text{Mon}$. [1]
- (c) Find $(-2) \cdot \text{Tue}$. [1]
- (d) Find the orbit of Wed. How many orbits are there? [1]

3

6 marks

- (a) Let $\sigma = (0\ 1\ 3)(2\ 4) \in \text{Sym}(5)$ and $x = (a, b, c, d, e)$. Find $\sigma \cdot x$ using $y_{\sigma(i)} = x_i$. [2]
- (b) Find σ^{-1} , and check your answer to (a) using $y_j = x_{\sigma^{-1}(j)}$. [1]
- (c) In the permutation action of $\text{Sym}(3)$ on X^3 , find $(0\ 1) \cdot (x, y, z)$ and $(0\ 2\ 1) \cdot (x, y, z)$. [2]
- (d) Check that $(0\ 1) \cdot ((1\ 2) \cdot (x, y, z)) = ((0\ 1)(1\ 2)) \cdot (x, y, z)$. [1]

4

6 marks

Let D_8 act on $\mathbb{R}^2$ by its defining action, $g \cdot x = g(x)$.

- (a) Find the orbit of $(0, 0)$. [1]
- (b) Find the orbit of $(1, 0)$. [1]
- (c) Find the orbit of $(1, 1)$. [1]
- (d) Find the orbit of $(2, 1)$. [2]
- (e) For the action of C_2 on $\mathbb{R}$ in question 1(b), describe the orbits and find the fixed points. [1]

5

6 marks

Let $\text{Sym}(3)$ act on $\mathbb{N}^3$ by the permutation action.

- (a) List the ten points of $\Delta(3)$. [2]
- (b) Check that $(0\ 1\ 2) \cdot (2, 1, 0)$ lies in $\Delta(3)$. [1]
- (c) Find the orbits of $\text{Sym}(3)$ on $\Delta(3)$. [2]
- (d) Which points of $\Delta(3)$ are fixed points? [1]

6

6 marks

- (a) Does the left action of C_4 on itself have any fixed points? [1]
- (b) Let $H = \{0, 4, 8\}$ act on C_{12} by $h \cdot g = h + g$. Find the orbits. [2]
- (c) Find the orbit of 0 under the canonical action of $\text{Sym}(4)$ on $\llbracket 4 \rrbracket$. [1]
- (d) Let $H = \{\epsilon, (0\ 1)(2\ 3)\}$ act on $\llbracket 4 \rrbracket$ by $\sigma \cdot x = \sigma(x)$. Find the orbits. [1]
- (e) Let $K = \langle (0\ 1\ 2) \rangle$ act on $\llbracket 4 \rrbracket$ in the same way. Find the orbits and the fixed points. [1]

7

6 marks

Decide whether each is a field, with its usual addition and multiplication. If not, give a reason.

- (a) $\mathbb{N}$ [1]
- (b) $\mathbb{Z}$ [1]
- (c) $\mathbb{Q}$ [1]
- (d) $\mathbb{Z}/6\mathbb{Z}$ [1]

- (e) $\mathbb{Z}/7\mathbb{Z}$ [1]
 (f) $\mathbb{Z}/2\mathbb{Z}$ [1]

8

6 marks

- (a) By trial and error, find the inverses of $[2]_{11}$, $[3]_{11}$ and $[7]_{11}$ in $\mathbb{Z}/11\mathbb{Z}$. [3]
 (b) Use the fast and backwards euclidean algorithms on $a = 19$, $b = 7$ to find the inverse of $[7]_{19}$. [2]
 (c) In $\mathbb{Z}/7\mathbb{Z}$, write -1 as $[k]_7$ with $k \in \llbracket 7 \rrbracket$, and check that $(-1) \cdot (-1) = 1$. [1]

9

7 marks

Solve each linear congruence, by multiplying by an inverse. Give the answer as a congruence class.

- (a) $4x \equiv 1 \pmod{7}$ [1]
 (b) $3x \equiv 5 \pmod{7}$ [1]
 (c) $5x \equiv 3 \pmod{11}$ [2]
 (d) $7x \equiv 4 \pmod{13}$, checking your answer [3]

10

7 marks

When $\gcd(a, n) \neq 1$, there may be several solutions or none. Check every $x \in \llbracket n \rrbracket$.

- (a) Solve $4x \equiv 2 \pmod{6}$. [2]
 (b) Show that $4x \equiv 3 \pmod{6}$ has no solutions. [2]
 (c) Solve $9x \equiv 6 \pmod{15}$, and write the solutions as a single class modulo 5. [3]

11

9 marks

Exam style. Let $\text{Sym}(3)$ act on $\mathbb{N}^3$ by the permutation action.

- (a) Count the points of $\Delta(6)$. [2]
 (b) Find the orbits of $\text{Sym}(3)$ on $\Delta(6)$. Give one point of each orbit and the size of the orbit. [4]
 (c) Check that the orbit sizes add up to your answer to (a), and explain why they must. [2]
 (d) Find the fixed points. [1]

12

9 marks

Exam style. Consider the congruence $17x \equiv 5 \pmod{43}$.

- (a) Explain why the fact that $\mathbb{Z}/p\mathbb{Z}$ is a field for prime p guarantees exactly one solution class. [1]
 (b) Run the fast euclidean algorithm on $a = 43$, $b = 17$. [2]
 (c) Run the backwards algorithm to find c and d with $43d - 17c = 1$, giving the table of C_n and D_n . [3]

- (d) Hence find the inverse of $[17]_{43}$. [1]
- (e) Solve the congruence, and check your answer. [2]

End of questions. Worked answers and the mark scheme are in the matching answers PDF.