Group Theory

Week 3 Exercises

Topics : Bezout's Lemma, Fermat's and Orbit-Stabilizer Theorem, Burnside's Lemma

Awez

1 Solutions

Solution (Q1.3.1). Addition modulo n is a binary operation on $\mathbb{Z}_n$ since it maps every element in $\mathbb{Z}_n \times \mathbb{Z}_n$ to a unique element in $\mathbb{Z}_n$. It's because by Euclid's division lemma $a+b$ can be written as $qn+r$, $r \in \mathbb{Z}_n$ and this r is unique, thus $a+b \equiv r \mod n$ and we have a unique mapping. This operation also nakes $\mathbb{Z}_n$ into a group since

1. It's associative,

$$\begin{aligned} a \cdot (b \cdot c) &= a + ((b+c) \mod n) \mod n && (1)\\ &= (a+b+c) \mod n && (2)\\ &= ((a+b) \mod n + c) \mod n && (3)\\ &= (a \cdot b) \cdot c. && (4) \end{aligned}$$

2. We have an identity $e = 0$ such that $a \cdot e = e \cdot a = a$ since $a + 0 = 0 + a \equiv a \mod n$.
3. For every $a \in \mathbb{R}_n$ we have $a' = (n-a) \mod n$ since we have $a \cdot a' = a' \cdot a = e \equiv 0 \mod n$.

Solution (Q1.3.2). So let the given set of numbers be $S = \{x | x \in \mathbb{R}_n \ \gcd(x,n) = 1\}$ and the given operation be '$\cdot$'. First, the operation is a function from $S \times S \to S$ since $\forall x, y \in S, xy \mod n \in S$. This belongs to S as $\gcd(x,n) = 1$ and $\gcd(y,n) = 1 \implies \gcd(xy, 1) = 1$ and it's unique because of Euclid's division lemma. Moreover

1. It's associative,

$$\begin{aligned} (a \cdot b) \cdot c &= ab \mod n \cdot c && (5)\\ &= ((ab \mod n)c) \mod n && (6)\\ &= (abc) \mod n && (7)\\ &= (a(bc \mod n)) \mod n && (8)\\ &= a \cdot (b \cdot c) && (9) \end{aligned}$$

2. There's an identity $e = 1 \in S$, since $\gcd(1,n) = 1$ and

$$a \cdot 1 = 1 \cdot a = a \mod n = a \tag{10}$$

3. For each $a \in S$, using Bezout's lemma since $\gcd(a,n) = 1$ there exists an x such that $ax \equiv 1 \mod n$. Then $x \mod n$ is the inverse of a. Since $a \cdot x = x \cdot a = 1 \mod n$.

This S is known as $\mathbb{Z}^*$.

Solution (Q2.2). To prove that the example 2.2 is a valid group action, we need to verify the two group action properties:

1. For any $g, h \in G$ and $s \in S$, we must show that $(gh) \cdot s = g \cdot (h \cdot s)$.

$$\begin{aligned} (gh) \cdot s &= (gh)(s) && (11)\\ &= g(h(s)) && (12)\\ &= g \cdot (h \cdot s), && (13) \end{aligned}$$

which holds since g and h are elements of the group G, and $\cdot$ denotes the action on S.

2. For every $s \in S$, we must show that $e \cdot s = s$, where e is the identity in G.

$$e \cdot s = e(s) = s, \tag{14}$$

by the definition of the group action, where e acts as an identity on S.

Hence, the example 2.2 is a valid group action.

Solution (Q2.3). To prove Burnside's Lemma, let G be a finite group acting on a finite set S. We need to count the orbits of G on S in two ways:

1. First, by considering the number of fixed points of each group element $g \in G$. Define $|S^g|$ as the number of elements of S fixed by g. Then the total number of fixed points across all elements is

$$\sum_{g \in G} |S^g|. \tag{15}$$

2. Next, count the elements in each orbit. Each orbit contains exactly $|G|/|G_s|$ elements, where G_s is the stabiliser of $s \in S$. Thus, the number of orbits is

$$\frac{1}{|G|} \sum_{g \in G} |S^g|, \tag{16}$$

which proves Burnside's Lemma.

Solution (Q2.4). We are asked to prove that the relation $\sim$ defined by $s \sim t$ if and only if there exists a $g \in G$ such that $g \cdot s = t$ is an equivalence relation.

1. **Reflexivity:** For all $s \in S$, we have $e \cdot s = s$ where e is the identity element in G. Thus, $s \sim s$.
2. **Symmetry:** If $s \sim t$, then there exists $g \in G$ such that $g \cdot s = t$. Since G is a group, the inverse g^{-1} exists, and $g^{-1} \cdot t = s$. Thus, $t \sim s$.
3. **Transitivity:** If $s \sim t$ and $t \sim u$, then there exist $g, h \in G$ such that $g \cdot s = t$ and $h \cdot t = u$. Thus, $h(g \cdot s) = u$, which means $(hg) \cdot s = u$, so $s \sim u$.

Hence, $\sim$ is an equivalence relation.