Group Theory
Report

Awez

1 Groups, Subgroups, Homomorphisms

Solution (Q2.4.1). $f(x) = x$ and $g(x) = x$, even though f and g are surjective $f \cdot g$ is not.

Solution (Q2.4.2). Let S be the set of functions from $[0, 1]$ to $[2, 3]$. For a function to be a binary operation on set T, it's domain is defined to be $T \times T$ and it should return a value from T, but when we take two functions from S, their composition might not be in S, it might not even be defined, for example take $f, g : [0, 1] \to [2, 3]$ and $f(x) = x + 2$ then $g(f(x))$ is not even defined, hence composition is not a binary operation.

Solution (Q2.4.3). No, because a binary operation on set S is a function with domain $S \times S$, but here it's not defined $\forall (a, b) \in S$, for eg. (b, a).

Solution (Q3.3.1).

1. Identity is 0, for $x \in \mathbb{Z}$, $-x$ is it's inverse.
2. Identity is the identity matrix I, for an invertible matrix A, inverse is A^{-1}.
3. Identity is $f(x) = x$, inverse is $f^{-1}(x)$.
4. Identity is $\phi(x, y) = (x, y)$, inverse is $\phi^{-1}(x, y)$, for a symmetry $\phi(x, y)$.

Solution (Q3.3.2). Since for a group G, identity $e \in G$ is such that $\forall a \in G$, $a \cdot e = e \cdot a = a$, suppose e and f both are identities, then

$$\begin{aligned} e \cdot f &= f && (1)\\ &= e && (2)\\ \implies e &= f. && (3) \end{aligned}$$

Hence proved that identity is unique.

Solution (Q3.3.3). In a group G, a' is said to be the inverse of a iff $a \cdot a' = a' \cdot a = e$ where e is identity. Suppose we have two identities a_1 and a_2 of a, then

$$\begin{aligned} a_1 \cdot a \cdot a_2 &= (a_1 \cdot a)a_2 && (4)\\ &= e \cdot a_2 && (5)\\ &= a_2 && (6)\\ a_1 \cdot a \cdot a_2 &= a_1 \cdot (a \cdot a_2) && (7)\\ &= a_1 \cdot e && (8)\\ &= a_1 \implies a_1 = a_2. && (9) \end{aligned}$$

Hence proved that inverse of any $a \in G$ is unique.

Solution (Q3.3.4). Since there exists unique inverse a' of a,

$$\begin{aligned} a \cdot b &= a \cdot c && (10)\\ \implies a' \cdot a \cdot b &= a' \cdot a \cdot c && (11)\\ \implies e \cdot b &= e \cdot c && (12)\\ \implies b &= c. && (13) \end{aligned}$$

Hence proved.

Note: In the following solutions, to prove H (a subset of G) can form a subgroup of G, which is a group itself I've just proved H is closed and it contains identity, i.e for $a, b \in H, a \cdot b \in H$. This is sufficient since all $a, b \in H$ satisfy the other three conditions required for H to be a group since they are already in G which is a group. First, $a \cdot (b \cdot c) = (a \cdot b) \cdot c, \forall a, b, c \in H$ which is true since a, b, c are also in group G. The other two are true since H does contain the identity.

Solution (Q4.4.1). Since H is a subgroup of G, by definition H has same operation as G, hence $\forall a \in H$, $a \in G$. Since H is a group, it also has an identity, let it be $e' \in H$. Now $\forall a \in H, a \cdot e' = e' \cdot a = e'$, but $\forall a \in G, a \cdot e = e \cdot a = e$, since they're the same operation, cancellation gives $e = e'$. Hence $e \in H$.

Solution (Q4.4.2). Assuming addition under integers, the set of odd integers isn't a subgroup, it isn't even a group since two odd numbers upon adding don't give an odd number. Whereas the set of even numbers is a subgroup, since it's a group, under the same operation as of integers. The set $\{kn \mid k \in \mathbb{Z}\}$ are all subgroups for each $n \in \mathbb{Z}$ of integers.

Solution (Q4.4.3). Any subgroup H of G containing all the elements of set S must have atleast all the elements of S, since H is closed under it's operation. Thus the smallest possible subgroup of G containing all the elements of S can be S.

Solution (Q4.4.4). $H \cap K$ is a subgroup of G because let $a, b \in H \cap K$, then $a \cdot b$ is also in H, similarly $a \cdot b$ is also in K. Thus $a \cdot b \in H \cap K$. Thus $H \cap K$ forms a group and is a subgroup of G. $H \cup K$ is not a subgroup of G because if $a \in H - K \subseteq H$ and $b \in K - H \subseteq K$ then we can't even guarantee $a \cdot b$ is in $H \cup K$ thus it's not even a group in first place. With similar arguments we can prove $T = \cap_{i \in I} H_i$ is a subgroup of G by taking $a, b \in T$. Since a,b belong to each of H_i, $a \cdot b$ also belongs to each of H_i thus is in T. There for T is a group with same operator as G and thus a subgroup of G.

Solution (Q5.3.1).

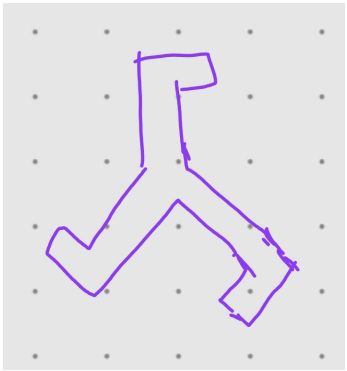

Figure 1: The group of symmetries associated with this are identity, rotation about center by $120°$, by $240°$

Solution (Q6.4.1). Let U and V be groups with operations $\cdot_U$ and $\cdot_V$ respectively and $a \in U$ and a' be it's inverse. Let the function $\phi : U \to V$ be a homomorphism. Then

$$\phi(a \cdot_U a') = \phi(a) \cdot_V \phi(a') \tag{14}$$
$$\phi(e_U) = \phi(a) \cdot_V \phi(a') \tag{15}$$
$$e_V = \phi(a) \cdot_V \phi(a') \tag{16}$$
$$\tag{17}$$

since we know that $\phi(e_U) = e_V$ where e is identity. Similarly we can show that

$$e_V = \phi(a') \cdot_V \phi(a) \tag{18}$$
$$\implies \phi(a) \cdot_V \phi(a') = e_V = \phi(a') \cdot_V \phi(a) \tag{19}$$
$$\implies \phi(a') = (\phi(a))' \tag{20}$$

Thus, homomorphism takes inverse of an element (a) to inverse of it's image.

Solution (Q6.4.2). Let $a, b \in K$. Then $\phi(a) = \phi(b) = e_V$. Also

$$\phi(a \cdot_U b) = \phi(a) \cdot_V \phi(b) \tag{21}$$
$$= e_V \tag{22}$$
$$\implies a \cdot b \in K \tag{23}$$

Thus, K is a group under same operation as of U thus is a subgroup of U.

Solution (Q6.4.3). Let $a, b \in H$, i.e $\exists a_0, b_0 \in U$ such that $\phi(a_0) = a$ and $\phi(b_0) = b$. Then

$$\phi(a_0 \cdot_U b_0) = \phi(a_0) \cdot_V \phi(b_0) \tag{24}$$
$$= a \cdot_V b \tag{25}$$
$$\implies \exists c_0 \in U(a_0 \cdot_U b_0) \text{ such that } \phi(c_0) = a \cdot_V b \tag{26}$$
$$\implies a \cdot_V b \in V \tag{27}$$

Thus, K forms a subgroup of V, known as image of ϕ.

2 Topics : Cosets, Lagrange's Theorem, p$^{\text{th}}$ roots of unity

Solution (Q1).
- Let number of elements in G be n.
- Since n is prime, $n \geq 2$, and there exists atleast one element which is not identity (e), let it be u.
- If the order of u is p, the subgroup generated by u is $\{e, u, u^2, \ldots, u^{p-1}\}$.
- Clearly size of this subgroup (p) is atleast 2.
- By Lagrange's theorem size of a subgroup divides the size of the group.
- But size of G (n) is a prime, so if p divides n and $p \geq 2$ then $p = n$.
- G has an element which generates a subgroup covering entirety of G, hence G is cyclic.
- Thus, any group with prime number of elements is cyclic.

Solution (Q2).
- Yes, consider G which is infinite and H which contains just e, the identity, which in itself forms a subgroup.
- Then G has infinite number of cosets $\{\{a\}|a \in G\}$.
- Another example is, consider $\mathbb{R}^{*}$[1] under multiplication as G and H as $\{-1, 1\}$ then each $a \in G, a > 0$ forms the left coset $aH = \{-a, a\}$ which is unique.
- Thus there are infinite left cosets of G with respect to finite H.

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

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,

$$a \cdot (b \cdot c) = a + ((b + c) \mod n) \mod n \tag{28}$$
$$= (a + b + c) \mod n \tag{29}$$
$$= ((a + b) \mod n + c) \mod n \tag{30}$$
$$= (a \cdot b) \cdot c. \tag{31}$$

[1] $\mathbb{R}^*$ is just $\mathbb{R} - \{0\}$

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,

$$\begin{aligned}(a \cdot b) \cdot c &= ab \mod n \cdot c && (32)\\ &= ((ab \mod n)c) \mod n && (33)\\ &= (abc) \mod n && (34)\\ &= (a(bc \mod n)) \mod n && (35)\\ &= a \cdot (b \cdot c) && (36)\end{aligned}$$

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

$$a \cdot 1 = 1 \cdot a = a \mod n = a \tag{37}$$

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 $(gh) \cdot s = g \cdot (h \cdot s)$.

$$\begin{aligned}(gh) \cdot s &= (gh)(s) && (38)\\ &= g(h(s)) && (39)\\ &= g \cdot (h \cdot s), && (40)\end{aligned}$$

   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.

$$e \cdot s = e(s) = s, \tag{41}$$

   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

$$\sum_{g \in G} |S^g|. \tag{42}$$

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

$$\frac{1}{|G|} \sum_{g \in G} |S^g|, \tag{43}$$

   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.