Midterm 1 Practice: Solutions

1. (a) Give the definition of an isomorphism of binary structures.

Solution. Let $(S, \star)$ and $(S', \star')$ be two binary structures. An **isomorphism** is a one-to-one and onto (or injective and surjective, or bijective) function $\phi : S \to S'$ such that $\phi(x \star y) = \phi(x) \star' \phi(y)$ for all $x, y \in S$.

(b) Is $\phi : \mathrm{GL}_2(\mathbb{R}) \to \mathbb{R}^\times$ given by $\phi(A) = \det A$ an isomorphism of the binary structures $(\mathrm{GL}_2(\mathbb{R}), \times)$ and $(\mathbb{R}^\times, \times)$?

Solution. This is not an isomorphism because it is not one-to-one. The matrices $A = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $B = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$ have $\det A = \det B$, but $A \neq B$.

2. (a) Let G be a group. Give the definition of a subgroup of G.

Solution. A **subgroup** H of a group G is a subset of G that

- is closed under the binary operation in G, i.e. for any $a, b \in H$, $ab \in H$,
- contains the identity element $e \in G$, i.e. $e \in H$, and
- for any $a \in H$, $a^{-1} \in H$.

(b) Is $S = \{A \in \mathrm{GL}_2(\mathbb{R}) \mid \det A = 2\}$ a subgroup of $\mathrm{GL}_2(\mathbb{R})$?

Solution. This is not a subgroup because it does not contain the identity matrix ($\det I = 1$). (It is also not a subgroup because it is not closed under matrix multiplication and it does not contain inverses.)

(c) Is $(S = \{2^n \mid n \in \mathbb{Z}\}$ a subgroup of $(\mathbb{Q}^\times, \times)$?

Solution. This is a subgroup. It is closed under the binary operation $\times$ because, if $2^n \in S$ and $2^m \in S$, then $2^n \times 2^m = 2^{n+m} \in S$. It contains the identity of $\mathbb{Q}^\times$ because $1 = 2^0 \in S$. Finally, if $2^n \in S$, $2^{-n} = (2^n)^{-1} \in S$, so S contains inverses.

(d) Find all subgroups of the group $\mathbb{Z}_5$ and give all generators for each subgroup.

Solution. In class, we showed that subgroups of the finite cyclic group $\mathbb{Z}_n$ correspond to the divisors of n, and two elements a and b generate the same subgroup if and only if $\gcd(a, n) = \gcd(b, n)$. The only divisors of 5 are 1 and 5, so the only subgroups of $\mathbb{Z}_5$ are $\langle 1 \rangle$ and $\langle 0 \rangle$. The generators of $\langle 1 \rangle$ are 1, 2, 3, 4 and the only generator of $\langle 0 \rangle$ is 0.

(e) Find all subgroups of the group $\mathbb{Z}_9$ and give all generators for each subgroup.

Solution. Using the same argument as above, the divisors of 9 are $1, 3, 9$, so the subgroups are $\langle 1 \rangle$, $\langle 3 \rangle$ and $\langle 0 \rangle$. The generators of $\langle 1 \rangle$ are 1,2,4,5,7,8, the generators of $\langle 3 \rangle$ are 3 or 6, and the only generator of $\langle 0 \rangle$ is 0.

3. (a) Give the definition of an abelian group.

Solution. A group G is **abelian** if its binary operation is commutative. (Alternative: a group is abelian if, for all $a, b \in G$, $ab = ba$.)

(b) If $(G, \cdot)$ is an abelian group with identity e, show that $H = \{x \in G \mid x^2 = e\}$ is a subgroup of G.

Solution. We first need to show that H is closed under the operation $\cdot$. If $x \in H$ and $y \in H$, we must show $xy \in H$, which means $(xy)^2 = e$. But,

$$\begin{aligned}(xy)^2 &= xyxy \\ &= xyyx \text{ because } G \text{ is abelian} \\ &= xx \text{ because } y^2 = e \\ &= e \text{ because } x^2 = e.\end{aligned}$$

Therefore, H is closed. H contains the identity of G because $e^2 = e$, and H contains inverses because, if $x \in H$, $x^2 = e$, so $x^{-1} = x$.

4. (a) Give the definition of a cyclic group.

Solution. A group G is **cyclic** if there is some element a that generates G, i.e. $G = \langle a \rangle$.

(b) If G is a cyclic group and $\phi : G \to G'$ is an isomorphism of G with another group G', prove that G' is also cyclic.

Solution. Because G is cyclic, there is an element $a \in G$ such that $G = \langle a \rangle$. To show G' is cyclic, we must show there is an element $b \in G'$ such that $G' = \langle b \rangle$. We claim that $b = \phi(a)$. By the homomorphism property, for any $n \in \mathbb{Z}$, $\phi(a^n) = \phi(a)^n$. To show that $G' = \langle \phi(a) \rangle$, we must show that any element $z \in G'$ is of the form $z = \phi(a)^r$ for some integer r. But, ϕ is onto, so there is an element $x \in G$ such that $\phi(x) = z$. Because G is cyclic, $x = a^r$ for some $r \in G$. Therefore, $z = \phi(x) = \phi(a^r) = \phi(a)^r$, so G' is cyclic generated by $\phi(a)$.