Exam 1 Solutions

① A **group** is a set with a binary operation such that the binary operation is associative, has an identity, and every element of the set has an inverse in the set.

$(\mathbb{Z}, +)$ is a group since adding two integers yields an integer, integer addition is associative, 0 is the identity, and the inverse of $a \in \mathbb{Z}$ is $-a \in \mathbb{Z}$.

Although $(\mathbb{Z}, \cdot)$ is a binary operation since the product of 2 integers is an integer, it is not a group since the element $2 \in \mathbb{Z}$ has no inverse in $\mathbb{Z}$.

② The **order** of g is the smallest positive integer n such that $g^n = e$ (if it exists). If no such n exists, g has infinite order.

If $g^n = e$, this does not mean that $|g| = n$; it only means that $|g| \mid n$.

③ $Z(G) = \{ z \in G \mid zg = gz \ \forall g \in G \}$ is a subgroup of G.

Proof Note that $eg = ge = g \ \forall g \in G$, so $e \in Z(G)$ and $Z(G)$ is nonempty.

Suppose $z_1, z_2 \in Z(G)$. Then $z_1 g = g z_1$ and $z_2 g = g z_2 \ \forall g \in G$.

For any $g \in G$, we have

$$(z_1 z_2) g = z_1 (z_2 g) = z_1 (g z_2) = (z_1 g) z_2 = (g z_1) z_2 = g (z_1 z_2).$$

Thus, $z_1 z_2 \in Z(G)$.

If $z \in Z(G)$, then $zg = gz \Rightarrow g = z^{-1} g z \Rightarrow g z^{-1} = z^{-1} g \ \forall g \in G$, so $z^{-1} \in Z(G)$. Thus, $Z(G) \leq G$ by the subgroup test. ▨

④ A group G is abelian iff $(ab)^{-1} = a^{-1} b^{-1} \ \forall a, b \in G$.

Proof Suppose first that G is abelian. Let $a, b \in G$. By the Shoes-Socks Property, $(ab)^{-1} = b^{-1} a^{-1}$, but since G is abelian, $b^{-1} a^{-1} = a^{-1} b^{-1}$.

Thus $(ab)^{-1} = a^{-1} b^{-1}$.

Conversely, suppose that $(ab)^{-1} = a^{-1} b^{-1} \ \forall a, b \in G$. Let $a, b \in G$.

Then $(ab)(ab)^{-1} = (ab)(a^{-1} b^{-1}) = e \Rightarrow a b a^{-1} = b \Rightarrow ab = ba$.

Thus, G is abelian. ▨

⑤ $S = \mathbb{R}^3 \setminus \{\langle 0,0,0\rangle\}$, $\hat{x} \sim \hat{y}$ if $\exists\, \lambda \in \mathbb{R}^*$ s.t. $\hat{y} = \lambda \hat{x}$. Then $\sim$ is an equivalence relation on S.

Proof Let $\hat{x} \in S$. Then $\hat{x} = 1 \cdot \hat{x}$ and $1 \in \mathbb{R}^*$, so $\hat{x} \sim \hat{x}$ and $\sim$ is reflexive.

Suppose $\hat{x}, \hat{y} \in S$ and $\hat{x} \sim \hat{y}$. Then $\exists\, \lambda \in \mathbb{R}^*$ s.t. $\hat{y} = \lambda \hat{x}$. Since $\lambda \neq 0$, we have $\hat{x} = \frac{1}{\lambda} \hat{y}$ with $\frac{1}{\lambda} \in \mathbb{R}^*$. Thus, $\hat{y} \sim \hat{x}$ and $\sim$ is symmetric.

Suppose $\hat{x}, \hat{y}, \hat{z} \in S$ with $\hat{x} \sim \hat{y}$ and $\hat{y} \sim \hat{z}$. Then $\exists\, \lambda, \mu \in \mathbb{R}^*$ s.t. $\hat{y} = \lambda \hat{x}$ and $\hat{z} = \mu \hat{y}$. Then $\hat{z} = \mu(\lambda \hat{x}) = (\mu\lambda)\hat{x}$. Since $\mu\lambda \in \mathbb{R}^*$, we have $\hat{x} \sim \hat{z}$, so $\sim$ is transitive. Thus, $\sim$ is an equivalence relation on S. ▨

The equivalence class of $\hat{x}$ is the set of nonzero vectors in $\mathbb{R}^3$ that are parallel to $\hat{x}$.

⑥ $G = \mathbb{Z}_{36}$.

The generators of G are elements $\bar{j} \in \mathbb{Z}_{36}$ s.t. $\gcd(j, 36) = 1$.

These are: $\bar{1}, \bar{5}, \bar{7}, \overline{11}, \overline{13}, \overline{17}, \overline{19}, \overline{23}, \overline{25}, \overline{29}, \overline{31}, \overline{35}$.

The # of subgroups of G is the # of positive divisors of $|G| = 36$.

These are $1, 2, 3, 4, 6, 9, 12, 18$, and 36, so G has $\boxed{9}$ subgroups.

Since $\bar{1}$ generates G, a generator for the subgroup of order K is $\frac{n}{K} \cdot \bar{1} = \overline{\frac{36}{K}}$.

Order of subgroup	Generator
1	$\bar{0} = \overline{36}$
2	$\overline{18} = \overline{\frac{36}{2}}$
3	$\overline{12} = \overline{36/3}$ etc.
4	$\bar{9}$
6	$\bar{6}$
9	$\bar{4}$
12	$\bar{3}$
18	$\bar{2}$
36	$\bar{1}$

The # of elements of G of order 9 is $\phi(9) = \boxed{6}$.

$[\{1, 2, 4, 5, 7, 8\}]$