Practice Exam 1

① Let S be a set and let R be a relation on the set S. We say that R is symmetric if for every pair $a, b \in S$ satisfying aRb, we also have bRa.

Let $S = \mathbb{Z}$ and define R_1 to be the relation aR_1b if $2 \mid a-b$ (equivalence mod 2). Then aR_1b implies $a-b = 2m$ for some $m \in \mathbb{Z} \Rightarrow$ $b-a = 2(-m)$ for $-m \in \mathbb{Z}$, so $2 \mid b-a$ and bR_1a. Thus, R_1 is symmetric.

Define R_2 to be the relation aR_2b if $a < b$. Then R_2 is not symmetric since $1 R_2 2$ but $2 \not R_2 1$.

② A group is a set with a binary operation such that the operation is associative, has an identity, and every element of the set has an inverse in the set. The set $\mathbb{Z}$ under the operation of addition is a group: adding any two integers yields an integer, $a + (b+c) = (a+b)+c \ \forall a,b,c \in \mathbb{Z}$, the identity element is 0, and the inverse of $a \in \mathbb{Z}$ is $-a$. However, the set $\mathbb{Z}$ under the operation of multiplication is not a group since $2 \in \mathbb{Z}$ has no inverse in $\mathbb{Z}$.

③ Subgroups of D_4 of order 2 are:

$\{R_0, R_{180}\}$, $\{R_0, H\}$, $\{R_0, V\}$, $\{R_0, D\}$, and $\{R_0, D'\}$.

④ Find two elements $a, b \in \mathbb{Z}/17\mathbb{Z}$ s.t. $a^2 = \overline{-1} = b^2$.

Certainly $\overline{4}^2 = \overline{4}\cdot\overline{4} = \overline{4\cdot 4} = \overline{16} = \overline{-1}$, so $a = \overline{4}$. Consider $a^{-1} = \overline{13}$. Then $\overline{13}^2 = \overline{13}\cdot\overline{13} = \overline{13\cdot 13} = \overline{169} = \overline{-1}$ since $17 \mid 169-(-1) = 170$. So $a = \overline{4}$, $b = \overline{13}$.

⑤ Let G be a group and $a \in G$. Let $C = \{g \in G \mid ag = ga\}$. Prove that $C \leq G$.

Proof Note that $ae = ea = a$, so $e \in C$, and C is nonempty. Suppose $g, h \in C$. Then $ag = ga$ and $ah = ha$. Thus, we have

$$a(gh) = (ag)h = (ga)h = g(ah) = g(ha) = (gh)a \Rightarrow gh \in C.$$

Suppose $g \in C$, so that $ag = ga$. Then multiplying on the right + left by g^{-1} gives $a = gag^{-1} \Rightarrow g^{-1}a = ag^{-1}$. Thus $g^{-1} \in C$. Hence $C \leq G$. ▨

⑥ Let $G = (\mathbb{Z}, +)$ and $\mathbb{N} = \{0, 1, 2, \dots\} \subseteq \mathbb{Z}$. Then $\mathbb{N}$ is not a subgroup of $\mathbb{Z}$ because 1 has no inverse in $\mathbb{N}$ $(-1 \notin \mathbb{N})$.