## Abstract Algebra – Worksheet 5

**Some notational conventions:**

- From now on, "the group $\mathbb{Z}_n$" will be taken to mean the set $\{0, 1, 2 \ldots n - 1\}$ with operation addition mod $n$.
- For groups such as $\mathbb{Z}_n$, where it is natural to use additive notation, we replace our multiplicative expressions by the additive analogues, as follows:
  - for $n$ an integer, in place of $a^n$ write $na$
  - in place of $a^{-1}$ write $-a$
  - write "0" for the identity.

1. A *subgroup* $H$ of a group $G$ is a nonempty subset of $G$ which is itself a group under the operation of $G$. Find a nontrivial (i.e. not the whole group or just the identity) subgroup for each of the following, and show that your subset really is a subgroup:
   (a) The set $\mathbb{Z}$ of integers under addition.
   (b) The set $D_4$ of symmetries of the square.
2. You may have noticed in the previous problem that a subset of a known group inherits certain group properties automatically. To make the process more efficient, prove the **Two-Step Subgroup Test**: Let $G$ be a group and $H$ a nonempty subset of $G$. Then $H$ is a subgroup of $G$ if
   (i) for any $a$ and $b$ in $H$, $ab$ is in $H$, AND
   (ii) for any $a$ in $H$, $a^{-1}$ is in $H$.

   (So your work is to show that given (i) and (ii), $H$ is closed under the operation of $G$ and the three axioms in the definition of a group hold for $H$.)
3. Prove that the set $\{1, 2, ..., n - 1\}$ is a group under multiplication modulo $n$ if and only if $n$ is prime.

**Definition.**

(i) The *order* of a group $G$, denoted $|G|$, is the number of elements in $G$ (finite or infinite).

(ii) The *order* of an element $g$ in a group $G$ is the smallest positive integer $n$ such that $g^n = e$. (In an additive group, this would be $ng = 0$, where $ng$ means $g + g + ... + g$ with $n$ terms.) If no such integer $n$ exists, we say that $g$ has *infinite order*. The order of an element $g$ is denoted $|g|$.

4. Find the order of each of the following groups as well as the order of each element in the group: $\mathbb{Z}_5$, $\mathbb{Z}_6$, $D_3$, $D_4$.