PMath 347 Groups and Rings

Homework # 1

Fall 2017, Rahim Moosa

Due on Friday September 22.

1. Fix $n \geq 3$ and let $r, s \in D_{2n}$ be the rotation and reflection symmetries discussed in class (or see §1.3 of D&F). Prove that

(a) $s \neq r^i$ for any $i \geq 0$, and

(b) $sr^i = r^{-i}s$ for any $i \geq 0$

2. Define the *order* of an element of a group, $a \in G$, to be the least positive integer n such that $a^n = 1$, if such an n exists. If no positive power of a is the identity then we say that a is of *infinite order*. The order of a is denoted by $|a|$.

Prove that $|ab| = |ba|$ for all $a, b \in G$.

3. Suppose G is a group and consider the function $\phi : G \to G$ given by $\phi(g) = g^2$. Prove that ϕ is a homomorphism if and only if G is abelian.

In the following two questions $\mathbb{Z}_n := \{0, 1, \ldots, n-1\}$ *equipped with both addition and multiplication modulo* n*. That is,* $a \oplus b$ *is the remainder of* $a + b$ *when divided by* n*, and* $a \otimes b$ *is the remainder of* ab *when divided by* n*. For these questions you may use basic facts about arithmetic, from MATH 135 for example.*

4. Let $n \geq 2$ and $\mathbb{Z}_n^\times := \{a \in \mathbb{Z} : 0 \leq a < n, \gcd(a, n) = 1\}$. Prove that $\mathbb{Z}_n^\times$ with multiplication modulo n is a group.

5. Fix integers n, m, both ≥ 2, and such that n divides m. Prove that there exists a nontrivial group homomorphism $\phi : \mathbb{Z}_m \to \mathbb{Z}_n$.