Name: ______________________

This is an open book/library/notes/web take-home exam, but you are not to collaborate. Your instructor is the only human source you are allowed to consult. Be sure to cite all outside sources you use.

Please submit your solution to each problem on a separate page, and staple this sheet on top of your exam.

This exam is due at 8:40 a.m. in class on October 10, 2018.

Problem	1	2	3	4	5	Total
Points	30	10	15	20	25	100
Score						

1. (a) Let G be the group of matrices

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a, b, c \in \mathbb{Z}/3\mathbb{Z},\ a \neq 0 \neq c \right\}.$$

Determine whether G is isomorphic to any of the groups A_4, D_{12}, or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, that is, the alternating group of degree 4, the dihedral group of order 12, or the direct product of a cyclic group of order 2 and a cyclic of order 6.

(b) Prove or disprove: $S_4 \cong D_{24}$.

(c) Prove or disprove: $D_{16} \cong \mathbb{Z}/2\mathbb{Z} \times D_8$.

2. Let G be a group of order 105. Suppose that G acts transitively on a set X. What are the possible cardinalities of the set X?

3. Let H be a normal subgroup of a finite group G, and assume that $|H| = p$ is the smallest prime number dividing $|G|$. Show that $H \leq Z(G)$, the center of G.
(Hint: Consider the action of G on H via conjugation, that is, g sends h to ghg^{-1}. Also note that the identity e in H is fixed under this action by every g in G.)

4. Let H_1 and H_2 be normal subgroups of a group G.

(a) Prove or disprove that $H_1 \cong H_2$ implies $G/H_1 \cong G/H_2$.

(b) Prove or disprove that $G/H_1 \cong G/H_2$ implies $H_1 \cong H_2$.

5. Consider the integers $\mathbb{Z}/n\mathbb{Z}$ modulo n as a ring with usual $\times$ and $+$ operations, and make the Cartesian product $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z}$ into a ring with componentwise $\times$ and $+$ operations.

(a) For $n := n_1 \cdots n_t$, show that the map

$$\begin{aligned} f\colon \mathbb{Z}/n\mathbb{Z} &\to \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z} \\ \bar{r} &\mapsto (\bar{r}, \ldots, \bar{r}) \end{aligned}$$

is both well-defined, and a ring homomorphism, that is, $f(ab) = f(a)f(b)$ and $f(a+b) = f(a) + f(b)$ for all a, b in $\mathbb{Z}/n\mathbb{Z}$. Here $\bar{r}$ on the left means "r mod n," but in the i-th component on the right it means "r mod n_i."

(b) Show that, in addition, if one has $\gcd(n_i, n_j) = 1$ for $i \neq j$ then the above map f is injective, and hence bijective (so a ring isomorphism).

(c) Use this to show that if n has prime factorization $n = p_1^{e_1} \cdots p_t^{e_t}$ with p_i primes and $e_i \geq 1$, then the Euler phi function defined by $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$ has the formula

$$\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_t^{e_t}) = (p_1^{e_1} - p_1^{e_1 - 1}) \cdots (p_t^{e_t} - p_t^{e_t - 1}).$$

(d) Recall that Fermats Little Theorem says any integer x satisfies $x^p \equiv x \bmod p$ when p is prime. Prove the following generalization: If n is squarefree in the sense that $n = p_1 \cdots p_t$ for distinct primes p_i, then every integer x satisfies $x^{\varphi(n)+1} \equiv x \bmod n$.

(e) Show that the result in part (d) is false whenever n is not squarefree, that is, for each nonsquarefree n, show how to exhibit some integer x for which $x^{\varphi(n)+1} \not\equiv x \bmod n$.