

- (1) (7.16) Recall that for any integer $n > 1$, $\phi(n)$ denotes the number of integers less than n , which are relatively prime to n . Prove that if a is any number relatively prime to n , then $a^{\phi(n)} \pmod n = 1$.

Proof: First observe that $\phi(n) = |U(n)|$ by the definition of $U(n)$. Since a is relatively prime to n , we can view $a \in U(n)$ (after reducing mod n). By a corollary to Lagrange, we know that

$$a^{|G|} = a^{|U(n)|} = a^{\phi(n)} = 1.$$

Hence $a^{\phi(n)} \pmod n = 1$.

- (2) (7.18) Show that the order of $U(n)$ is even when $n > 2$.

Proof: The number $n - 1$ is always relatively prime to n (if not, then some number divides both n and $n - 1$ and hence it divides 1). Thus $n - 1 \in U(n)$. Also $(n - 1)^2 = n^2 - 2n + 1 = 1 \pmod n$. Hence $n - 1$ has order 1 or 2. If $n > 2$, it cannot be the identity element of $U(n)$, so it has order two. Thus $U(n)$ always has an element of order 2 when $n > 2$. Thus 2 must divide $U(n)$ by Lagrange - Done.

- (3) (7.22) Suppose that G is a group with more than one element and G has no proper, non-trivial subgroups. Prove that $|G|$ is prime. (Do not assume that G is finite.)

Proof: First assume that G is infinite. Let $a \in G$, with $a \neq e$. Then a must generate all of G , i.e., G is an infinite cyclic group. However, then $\langle a^2 \rangle$ is a proper subgroup of G - contradiction. Thus G is finite.

Again let $a \in G$, with $a \neq e$. Let $H = \langle a \rangle$. By assumption, $H = G$, and so G is cyclic. Recall an old theorem that says that if G is a finite cyclic group and if d divides $|G|$, then G has a subgroup of order d . Therefore, since our group G has no subgroups, $|G|$ has no divisors except 1 and $|G|$. Thus $|G|$ is prime.

- (4) (7.30) Prove that every subgroup of D_n of odd order is cyclic.

Proof: Let H be a subgroup of D_n of odd order. Observe that there are two types of elements in D_n , rotations and reflections. However, all reflections have order 2. Thus by Lagrange, none of these elements can be in H . Hence H is a subset of the collection of all rotations. But the set of all rotations in D_n is a subgroup of D_n . In fact, it is a cyclic subgroup generated by the element $\mathcal{R}_{2\pi/n}$. Since any subgroup of a cyclic group is cyclic, we conclude that H is cyclic.

- (5) (8.20) The group $S_3 \oplus Z_2$ is isomorphic to one of the following groups: $Z_{12}, Z_6 \oplus Z_2, A_4, D_6$. Determine which one.

Proof: We do this by a process of elimination. Clearly $G = S_3 \oplus Z_2$ is not isomorphic to either Z_{12} or $Z_6 \oplus Z_2$, since G is nonabelian, while the latter two groups are abelian (being the direct product of abelian groups.)

Next, note that $(123) \in S_3$ has order 3, while Z_2 has an element of order 2. Thus $((123), 1) \in G$ has order $\text{lcm}(3, 2) = 6$. We show that $A_4 \subset S_4$ has no element of order 6. By looking at products of disjoint cycles, we see that S_4 can have elements of order 1, 2, 3, or 4 (and this last is by taking a 4-cycle, which is not in A_4 in any case). Thus A_4 cannot have an element of order 6. Therefore, G is not isomorphic to A_4 . So by elimination, G is isomorphic to D_6 . (Note that we have not actually proven that the two groups are isomorphic, we are just taking the books word for it.)