Section 2.8 Exercises
Hertein's Topics In Algebra

Spencer T. Parkin

March 11, 2016

Problem 16

Let $\phi(n)$ be the Euler ϕ-function. If $a > 1$ is an integer, prove that $n|\phi(a^n - 1)$.

Consider the group U_m with $m = 2^n - 1$. Since $|U_m| = \phi(m)$, if we can exhibit an element of U_m with order n, then the result goes through by Lagrange's Theorem. Notice that

$$(a^{n-1})a + (-1)(a^n - 1) = 1.$$

This shows that $\gcd(a, a^n - 1) = 1$; and therefore, $a \in U_m$. Then clearly, we have

$$a^n \equiv 1 \pmod{m},$$

so $|a|$ divides n. But since $a^k - 1 < a^n - 1 = m$ for all $0 \leq k < n$, we must have $|a| = n$. Now by Lagrange's Theorem, the order of the cyclic subgroup generated by a, which is n, must divide $\phi(m)$.

Problem 17

Let G be a group and Z the center of G. If T is any automorphism of G, prove that $T(Z) \subseteq Z$.

Let $z \in Z(G)$, and $x = T(z)$. Now for any $g \in G$, let $g' \in G$ be the pre-image of g with respect to T. We then see that

$$xg = T(z)T(g') = T(zg') = T(g'z) = T(g')T(z) = gx,$$

showing that x commutes with any $g \in G$; so $x \in Z(G)$.