Math 345 – PS#3 Solutions
Summer 2, 2012

p.60, #36. Prove that the generators of $\mathbb{Z}_n$ *are the congruence classes* $[r]$ *such that* $1 \leq r < n$ *and* $\gcd(r,n) = 1$.
Proof. First note that $\mathbb{Z}_n = \langle [1] \rangle$ since $[r] = r[1]$. Let $[r] \in \mathbb{Z}_n \smallsetminus [0]$; then $[r] = r[1]$. By Theorem 4.6, $|[r]| = n/d$, where $\gcd(r,n) = d$. But $[r]$ is a generator if and only if $|[r]| = n$ if and only if $d = 1$.

p.60, #38. Prove that the order of an element in a cyclic group G *must divide the order of the group.*
Proof. Let $a \in G$. Then $|a| = |\langle a \rangle|$. By Lagrange's Theorem 6.5, $|\langle a \rangle| \mid |G|$. Therefore $|a| \mid |G|$.

p.76, #27. Let G *be a group and let* $g \in G$. *Prove that the function* $\lambda_g : G \to G$ *defined by* $\lambda_g(a) = ga$ *is a permutation of* G.
Proof. To show that λ_g is injective, assume that $\lambda_g(a) = \lambda_g(b)$. Evaluating both sides gives $ga = gb$ so that $a = b$ by left cancellation. Hence λ_g is injective. To show that λ_g is surjective, let $b \in G$; then $g^{-1}b \in G$ since G has inverses and the closure property holds in G. But$(g^{-1}b) = g(g^{-1}b) = (gg^{-1})b = eb = b$. Therefore λ_g is surjective.

p.76, #29. Recall that the ***center*** *of a group* G *is the subgroup* $Z(G) = \{g \in G \mid gx = xg \text{ for all } x \in G\}$. Find the center of D_8. What about the center of D_{10}? What is the center of D_n?
Solution. First note that any two rotations in D_n commute: Let r be the rotation of $2\pi/n$ in D_n. Then the rotations in D_n are $\{r, r^2, \ldots r^{n-1}, r^n = id\}$ and $r^m r^n = r^{m+n} = r^{n+m} = r^n r^m$ for all m, n. Let s be the reflection in D_n that fixes vertex 1; then the reflections in D_n are $\{s, sr, sr^2, \ldots, sr^{n-1}\}$. Note that $r^i(sr^j) = r^i(sr^j ss) = r^i(srs)^j s = r^i(r^{-1})^j s = r^i r^{-j} s = r^{i-j}s$ and $(sr^j)r^i = sr^{i+j}ss = r^{-i-j}s$. Thus $r^i(sr^j) = (sr^j)r^i$ iff $i - j \equiv -i - j \pmod{n}$ iff $2i \equiv 0 \pmod{n}$. Thus $Z(D_{2n}) = \{id, r^n\}$ and $Z(D_{2n+1}) = \{id\}$. In particular, $Z(D_8) = \{id, r^4\}$ and $Z(D_{10}) = \{id, r^5\}$.

p. , #11. Let H be a subgroup of a group G. Prove that

a. If $x \in H$, then $Hx = H$.
b. If $g_1, g_2 \in G$ and $g_1 \in g_2 H$, then $g_2 H \subseteq g_1 H$.
c. If $g_1, g_2 \in G$ and $g_1^{-1} g_2 \in H$, then $Hg_2^{-1} \subseteq Hg_1^{-1}$.
d. If $g_1, g_2 \in G$ and $Hg_1^{-1} = Hg_2^{-1}$, then $g_1^{-1} g_2 \in H$.

Proof. (a) Let $a \in Hx$. Then there exists some $h \in H$ such that $a = hx$. But $x \in H$, so $a = hx \in H$ by closure. Therefore $Hx \subseteq H$. Let $b \in H$. Then $b = b(x^{-1}x) = (bx^{-1})x$. But $x^{-1} \in H$ since H is a subgroup containing x, and $bx^{-1} \in H$ by closure. Hence $b = (bx^{-1})x \in Hx$ and $H \subseteq Hx$.
(b) Let $x \in g_2 H$. Then there exists $h \in H$ such that $x = g_2 h$. Since $g_1 \in g_2 H$, there exists $h' \in H$ such that $g_1 = g_2 h'$ and $g_2 = g_1 (h')^{-1}$. Thus $x = g_2 h = \left(g_1 (h')^{-1}\right) h = g_1 \left((h')^{-1} h\right) \in g_1 H$. Therefore $g_2 H \subseteq g_1 H$.
(c) Let $x \in Hg_2^{-1}$. Then there exists $h \in H$ such that $x = hg_2^{-1}$. Since $g_1^{-1} g_2 \in H$, there exists $h' \in H$ such that $g_1^{-1} g_2 = h'$ and $g_2^{-1} = (h')^{-1} g_1^{-1}$. Thus $x = hg_2^{-1} = h\left((h')^{-1} g_1^{-1}\right) = \left(h (h')^{-1}\right) g_1^{-1} \in Hg_1^{-1}$. Therefore $Hg_2^{-1} \subseteq Hg_1^{-1}$.
(d) Let $x \in Hg_1^{-1} = Hg_2^{-1}$. Then there exist $h, h' \in H$ such that $x = hg_1^{-1} = h' g_2^{-1}$. Hence $g_1^{-1} g_2 = h^{-1} h' \in H$.