Homework #9 Solutions

p 149, #18 Let $n > 1$. Then $n-1 \in U(n)$ and $(n-1)^2 = n^2-2n+1$ so that $(n-1)^2 \bmod n = 1$. Since $n-1 \neq 1$, this means that $|n-1| = 2$ in $U(n)$. As the order of any element in a group must divide the order of that group, it follows that 2 must divide the order of $U(n)$, i.e. the order of $U(n)$ is even.

p 149, #22 Let $a \in G$, $a \neq e$. Then $\langle a \rangle$ is a nontrivial subgroup of G. Since G has no proper nontrivial subgroup, it must be that $G = \langle a \rangle$. That is, G is cyclic. If G is infinite then $G \cong \mathbb{Z}$, which we know has infinitely many subgroups, and this is a contradiction. Therefore, G must be a finite cyclic group. By the fundamental theorem of cyclic groups, the subgroups of G correspond to the divisors of its order. Since G has no subgroups other than $\{e\}$ and itself, it must be that $|G|$ is divisible only by 1 and itself, i.e. $|G|$ is prime.

p 149, #26

Theorem 1. *Let G be a finite group with even order. Then G has an element of order 2.*

Proof. Since any element and its inverse have the same order, we can pair each element of G with order larger than two with its (distinct) inverse, and hence there must be an even number of elements of G with order greater than two. However, $|G|$ is even and so G has an odd number of nonidentity elements. It follows that G must have an element with order 2. $\square$

The solution to the problem now follows from the theorem.

p 149, #28 Let $H \leq \mathbb{Q}$ and suppose $[\mathbb{Q} : H] = n < \infty$. For any $r \in \mathbb{Q}$ consider the cosets

$$H, r+H, 2r+H, \dots, nr+H.$$

Since H has only n distinct cosets, two of these must be the same. That is, there must be i, j with $0 \leq i < j \leq n$ so that $ia + H = ja + H$, i.e. $a(j-i) \in H$. Since $1 \leq j-i \leq n$, we have proven that for any rational r there is an integer k, $1 \leq k \leq n$, so that $kr \in H$. Let $N = n!$. Since every number between 1 and n divides N, we find that for any $r \in Q$, $Nr \in H$. But if r is rational then so is r/N and so

$$r = N\left(\frac{r}{N}\right) \in H$$

which means $H = \mathbb{Q}$. The conclusion follows.

p 149, #30 Let H be a subgroup of D_n with odd order. Since every flip in D_n has order 2, and 2 does not divide $|H|$, Lagrange's theorem tells us that H can contain no flips. Therefore,

H consists entirely of rotations. But the rotations in D_n form a cyclic subgroup, generated by $R_{360/n}$. So we have

$$H \leq \langle R_{360/n} \rangle$$

and since every subgroup of a cyclic group is cyclic, we conclude that H is cyclic.

p 149, #34 Follows from the theorem proven in #26.

p 150, #36 For convenience we set $\phi_n(a)a^n$ for all $a \in G$. Since G is abelian, for any $x, y \in G$ we have

$$\phi_n(xy) = (xy)^n = x^n y^n = \phi_n(x)\phi_n(y)$$

which shows that ϕ_n is operation preserving. This is the easy part. Now we need to show that ϕ_n is one-to-one and onto. Since G is finite, it suffices to show only that ϕ_n is one-to-one. So suppose that $\phi_n(x) = \phi_n(y)$ for some $x, y \in G$. Then $x^n = y^n$ or, since G is abelian,

$$x^n y^{-n} = (xy^{-1})^n = e.$$

As $(n, |G|) = 1$, problem #19 allows us to conclude that $xy^{-1} = e$, and hence that $x = y$. This proves that ϕ_n is one-to-one and, as noted above, conclude that proof that $\phi_n \in \mathrm{Aut}(G)$.

p 150, #38 Since $H \cap K$ is a subgroup of both H and K, Lagrange's theorem tells us that $|H \cap K|$ must be divide both $|H| = pq$ and $|K| = qr$. As p, q, r are distinct primes, this means that $|H \cap K| = 1$ or q. Appealing to Lagrange's theorem again, we find that this means $[H : H \cap K] = pq$ or p. We must eliminate the first case.

Let $a \in H$. We claim that $H \cap aK = a(H \cap K)$. One inclusion is obvious: we have $a(H \cap K) \subset aK$ and since $a \in H$ we have $a(H \cap K) \subset H$. Hence $a(H \cap K) \subset H \cap aK$. Now for the reverse. Let $h \in H \cap aK$. Then $h = ak$ with $k \in K$ and so $k = a^{-1}h$. Since $a \in H$, we find that $k \in H$, which means that $k \in H \cap K$. Hence, $h = ak \in a(H \cap K)$ proving that $H \cap aK \subset a(H \cap K)$.

The fact that $H \cap aK = a(H \cap K)$ for all $a \in H$ tells us that each left coset of $H \cap K$ in H comes from a left coset of K in G (in fact, a coset of the form aK with $a \in H$). In particular, this means that the number of left cosets of $H \cap K$ in H is less than or equal to the number of cosets of K in G, i.e.

$$[H : H \cap K] \leq [G : K] = \frac{|G|}{|K|} = p.$$

This means that the case $[H : H \cap K] = pq$ is impossible, leaving us to conclude that $[H : H \cap K] = p$. Lagrange's theorem (again!) then gives $|H \cap K| = q$.

Additional Problem. We use the one-step subgroup test. Since $e \in H$, $e = aea^{-1} \in aHa^{-1}$, so that $aHa^{-1} \neq \emptyset$. Furthermore, if $x = ah_1a^{-1}, y = ah_2a^{-1} \in aHa^{-1}$ $(h_1, h_2 \in H)$, then

$$xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1} = (ah_1a^{-1})(ah_2^{-1}a^{-1}) = ah_1h_2^{-1}a^{-1} \in aHa^{-1}$$

since $h_1 h_2^{-1} \in H$. Therefore, aHa^{-1} passes the one-step subgroup test.