Homework #11 Solutions

p 166, #18 We start by counting the elements in D_m and D_n, respectively, of order 2. If $x \in D_m$ and $|x| = 2$ then either x is a flip or x is a rotation of order 2. The subgroup of rotations in D_m is cyclic of order m, and since m is even there is exactly $\phi(2) = 1$ rotation of order 2. Therefore, D_m contains exactly $m+1$ elements of order 2. On the other hand, $y \in D_n$ can have order 2 only if y is a flip, since the rotations in D_n have order dividing n, which is odd. Therefore there are exactly n elements in D_n of order 2.

We are now in a position to count the elements of order 2 in $D_m \oplus D_n$. Suppose $(x, y) \in D_m \oplus D_n$ and $|(x, y)| = 2$. Since $|(x, y)| = \text{lcm}(|x|, |y|)$, it must be that either $|x| = 2$ and $|y| = 1, 2$ or $|x| = 1$ and $|y| = 2$. In the first case, the preceding paragraph shows that there are $m+1$ choices for x and $n+1$ choices for y, giving a total of $(m+1)(n+1)$ pairs. In the second case $x = e$ and there are n choices for y, yielding another n pairs. Thus, the total number of pairs with order 2 is

$$(m+1)(n+1) + n.$$

p 166, #28 It is not hard to show that $\mathbb{Z}_{12} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{15}$ has no element of order 9, so we won't be able to find a cyclic subgroup of order 9. We therefore look for the next easiest type of subgroup, namely one of the form $H \oplus K \oplus J$ where $H \leq \mathbb{Z}_{12}$, $K \leq \mathbb{Z}_4$ and $J \leq \mathbb{Z}_{15}$. The order of such a subgroup is $|H| \cdot |K| \cdot |J|$. If this is to equal 9, Lagrange's theorem tells us that we need $|H| = 3$, $|K| = 1$ and $|J| = 3$. Since $\mathbb{Z}_{12}, \mathbb{Z}_4$ and $\mathbb{Z}_{15}$ are all cyclic, they have unique subgroups of these orders. That is, we must take $H = \langle 4 \rangle$, $K = \{0\}$ and $J = \langle 5 \rangle$, so our subgroup is

$$\langle 4 \rangle \oplus \{0\} \oplus \langle 5 \rangle$$

p 167, #40 According to Corollary 1 of Theorem 8.2 we have

$$\begin{aligned} \mathbb{Z}_{10} \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_6 \\ &\cong \mathbb{Z}_2 \oplus \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \\ &\cong \mathbb{Z}_{60} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2. \end{aligned}$$

p 167, #44 We have

$$\begin{aligned} 1 &= 8 \cdot 2 \bmod 15 \\ &= 8 \cdot \phi(2, 3) \\ &= \phi(8 \cdot 2 \bmod 3, 8 \cdot 3 \bmod 5) \\ &= \phi(1, 4) \end{aligned}$$

which shows that $(1,4)$ maps to 1.

p 167, #50 Since $165 = 3 \cdot 5 \cdot 11$, the Corollary to Theorem 8.3 gives

$$U(165) \cong U(3) \oplus U(5) \oplus U(11) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{10}.$$

p 167, #52 We begin by observing that

$$\mathrm{Aut}(\mathbb{Z}_{20}) \cong U(20) \cong U(4) \oplus U(5) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4.$$

If $(x,y) \in \mathbb{Z}_2 \oplus \mathbb{Z}_4$ has order 4 then, since $|(x,y)| = \mathrm{lcm}(|x|,|y|)$, x is free and y must have order 4. Since $\mathbb{Z}_4$ has $\phi(4) = 2$ elements of order 4, it follows that $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, and hence $\mathrm{Aut}(\mathbb{Z}_{20})$, has 4 elements of order 4. On the other hand, since $4 \cdot (x,y) = (0,0)$ for every $(x,y) \in \mathbb{Z}_2 \oplus \mathbb{Z}_4$, Lagrange's theorem tells us that the possible orders of elements are 1, 2 or 4. Having counted the order 4 elements, and knowing that only the identity has order 1, we conclude that there must be exactly 3 elements of order 2.

p 168, #58 By the Corollary to Theorem 8.3:

$$U(144) = U(2^4 \cdot 3^2) \cong U(2^4) \oplus U(3^2) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$$

$$U(140) = U(2^2 \cdot 5 \cdot 7) \cong U(2^2) \oplus U(5) \oplus U(7) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_6$$

proving that $U(144) \cong U(140)$.

p 191, #4 H is *not* normal in $GL(2,\mathbb{R})$ since

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in H \text{ , } B = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in GL(2,\mathbb{R})$$

and

$$BAB^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 2 \end{pmatrix}$$

which does not belong to H.

p 191, #10 Let $G = \langle a \rangle$ be a cyclic group and let $H \triangleleft G$. If $gH \in G/H$ then $g = a^n$ for some $n \in \mathbb{Z}$ so that

$$gH = a^n H = (aH)^n \in \langle aH \rangle.$$

This shows that $G/H = \langle aH \rangle$ and is hence cyclic.

p 191, #12 Let G be an abelian group and let $H \triangleleft G$. For any $aH, bH \in G/H$ we have, since G is abelian,

$$(aH)(bH) = (ab)H = (ba)H = (bH)(aH)$$

which proves that G/H is abelian as well.

p 191, #14 Since $\langle 8\rangle = \{0, 8, 16\}$ and

$$\begin{aligned} 2 \cdot 14 \bmod 24 &= 4 \\ 3 \cdot 14 \bmod 24 &= 18 \\ 4 \cdot 14 \bmod 24 &= 8 \end{aligned}$$

we see that the coset $14 + \langle 8\rangle$ has order 4 in $\mathbb{Z}_{24}/\langle 8\rangle$.

p 192, #18 Since 15 has order 4 in $\mathbb{Z}_{60}$, Lagrange's theorem tells us that

$$|\mathbb{Z}_{60}/\langle 15\rangle| = [\mathbb{Z}_{60} : \langle 15\rangle] = \frac{|\mathbb{Z}_{60}|}{|\langle 15\rangle|} = \frac{60}{4} = 15.$$

p 192, #22 We start by noting that $\langle (2,2)\rangle = \{(2m, 2m) \,|\, m \in \mathbb{Z}\}$ so that $n \cdot (1,0) = (n,0) \notin \langle (2,2)\rangle$ for every $n \in \mathbb{Z}^+$. From this it follows that $(1,0) + \langle (2,2)\rangle$ must have infinite order in $(\mathbb{Z} \oplus \mathbb{Z})/\langle (2,2)\rangle$ and hence that this group has infinite order. If $(\mathbb{Z} \oplus \mathbb{Z})/\langle (2,2)\rangle$ were cyclic, it would have to be isomorphic to $\mathbb{Z}$, the only infinite cyclic group. However, $\mathbb{Z}$ has no elements of order 2, whereas $(1,1) + \langle (2,2)\rangle$ is an element of $(\mathbb{Z} \oplus \mathbb{Z})/\langle (2,2)\rangle$ with order 2. Consequently, $(\mathbb{Z} \oplus \mathbb{Z})/\langle (2,2)\rangle$ is *not* isomorphic to $\mathbb{Z}$ and so is not cyclic.

p 192, #26 Using the Cayley table for G on page 90 we find that the 4 cosets of H are

$$\begin{aligned} H &= \{e, a^2\} \\ aH &= \{a, a^3\} \\ bH &= \{b, ba^2\} \\ baH &= \{ba, ba^3\}. \end{aligned}$$

Moreover, according to the same Cayley table we have

$$\begin{aligned} (aH)^2 &= a^2H = H \\ (bH)^2 &= b^2H = a^2H = H \end{aligned}$$

so that G/H has at least 2 distinct elements of order 2. Since $\mathbb{Z}_4$ has only a single element of order 2, it must be that $G/H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

p 192, #28 The four cosets in G/H are

$$\begin{aligned} H &= \{(0,0), (2,0), (0,2), (2,2)\} \\ (1,1) + H &= \{(1,1), (3,1), (1,3), (3,3)\} \\ (1,2) + H &= \{(1,2), (3,2), (1,0), (3,0)\} \\ (2,1) + H &= \{(2,1), (0,1), (2,3), (0,3)\} \end{aligned}$$

which all have order 2. Therefore $G/H \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. The cosets in G/K are

$$\begin{aligned}
K &= \{(0,0),(1,2),(2,0),(3,2)\} \\
(1,1)+K &= \{(1,1),(2,3),(3,1),(0,3)\} \\
(1,3)+K &= \{(1,3),(2,1),(3,3),(0,1)\} \\
(2,2)+K &= \{(2,2),(3,0),(0,2),(1,0)\}
\end{aligned}$$

and since $(1,1)+K$ clearly has order 4, it must be that $G/K \cong \mathbb{Z}_4$.

p 193, #42 We prove only the generalization, which is the following.

Proposition 1. *Let G be a group and let $n \in \mathbb{Z}^+$. If G has a unique subgroup of order n then that subgroup is normal in G.*

Proof. Let H be the unique subgroup of G of order n. For any $x \in G$, xHx^{-1} is also a subgroup of G with order n. Therefore it must be that $xHx^{-1} = H$. Since $x \in G$ was arbitrary, this proves that H is normal in G. □

p 193, #44 We prove only the generalization, which is the following.

Proposition 2. *If G is a finite group then $[G : Z(G)]$ is 1 or is composite.*

Proof. Assume, for the sake of contradiction, that $[G : Z(G)]$ is prime. Then $G/Z(G)$ is a group of prime order and is therefore cyclic. Theorem 9.3 then implies that G is abelian, which means that $G = Z(G)$ and so $[G : Z(G)] = 1$, which is a contradiction. □

p 193, #46 Let $aH \in G/H$. If aH has finite order then there is an $n \in Z^+$ so that

$$a^n H = (aH)^n = H,$$

i.e. $a^n \in H$. But every element of H has finite order and so there is an $m \in \mathbb{Z}^+$ so that

$$a^{nm} = (a^n)^m = e$$

which implies, since $mn \geq 1$, that a has finite order. That is, $a \in H$ so that aH is the trivial coset H. We have therefore shown that the only element of G/H with finite order is the identity, which is equivalent to the desired conclusion.

p 195, #70 We begin with the following general result.

Proposition 3. *Let G be a group and $H \triangleleft G$. For any $g \in G$ the set*

$$K = \bigcup_{i \in \mathbb{Z}} g^i H$$

is a subgroup of G.

Proof 1. We use the one-step subgroup test. We begin by noting that $K \neq \emptyset$ since $H \subset K$ and $H \neq \emptyset$. If $x, y \in K$ then there exist $h_1, h_2 \in H$ and $i, j \in \mathbb{Z}$ so that $x = g^i h_1$ and $y = g^j h_2$. Since $H \triangleleft G$, $g^{-j}H = Hg^{-j}$, and so $h_1 h_2^{-1} g^{-j} = g^{-j} h_3$ for some $h_3 \in H$. Thus

$$xy^{-1} = g^i h_1 h_2^{-1} g^{-j} = g^i g^{-j} h_3 = g^{i-j} h_3 \in K$$

proving that K passes the one-step subgroup test. □

Proof 2. Let $\gamma : G \to G/H$ be the natural homomorphism. Since the kernel of γ is H and $\gamma(g^i) = g^i H = (gH)^i$, $\gamma^{-1}((gH)^i) = g^i H$ by Theorem 10.1. Thus

$$K = \bigcup_{i \in \mathbb{Z}} g^i H = \bigcup_{i \in \mathbb{Z}} \gamma^{-1}((gH)^i) = \gamma^{-1}\left(\bigcup_{i \in \mathbb{Z}} \{(gH)^i\}\right) = \gamma^{-1}(\langle gH \rangle)$$

which shows that K is a subgroup of G by Theorem 10.2. □

The conclusion of the problem now follows easily. Since gH has order 3, the cosets H, gH and $g^2 H$ are distinct, and any other coset of the form $g^i H$ is one of these. Therefore

$$\bigcup_{i \in \mathbb{Z}} g^i H = H \cup gH \cup g^2 H$$

and the latter set contains exactly 12 elements since $|H| = 4$. The proposition tells us this set is a subgroup of G, so we're finished.

p 210, #6 Let $f, g \in G$. The linearity of differentiation assures us that $\int f + \int g$ is an antiderivative of $f + g$, i.e.

$$\left(\int f + \int g\right)' = \left(\int f\right)' + \left(\int g\right)' = f + g.$$

Furthermore, since $(\int f)(0) = (\int g)(0) = 0$ we have

$$\left(\int f + \int g\right)(0) = \left(\int f\right)(0) + \left(\int g\right)(0) = 0 + 0 = 0$$

so that $\int f + \int g$ passes through the point $(0, 0)$. It follows from the definition of $\int$ that $\int f + \int g = \int (f + g)$, proving that the map $f \mapsto \int f$ is indeed a homomorphism.

If we require that the antiderivative $\int f$ pass through any point (a, b) with $b \neq 0$ then the map is *never* a homomorphism. To see this, note that for any $f \in G$ we have

$$\left(\int f\right)(a) = b$$

and

$$\left(\int f + \int f\right)(a) = \left(\int f\right)(a) + \left(\int f\right)(a) = 2b \neq b = \left(\int (f + f)\right)(a)$$

demonstrating that $\int (f + f) \neq \int f + \int f$.

p 211, #10 Let $x, y \in G$. To show that $\phi(xy) = \phi(x)\phi(y)$ we consider 4 possible cases.
Case 1: x and y are both rotations. Then xy is also a rotation and so

$$\phi(x)\phi(y) = 1 \cdot 1 = 1 = \phi(xy).$$

Case 2: x is a rotation and y is a reflection. Then xy is also a reflection and so

$$\phi(x)\phi(y) = 1 \cdot -1 = -1 = \phi(xy).$$

Case 3: x is a reflection and y is a rotation. Then, as above, xy is a reflection and so

$$\phi(x)\phi(y) = -1 \cdot 1 = 1 = \phi(xy).$$

Case 4: x and y are both reflections. Then xy is a rotation and so

$$\phi(x)\phi(y) = -1 \cdot -1 = 1 = \phi(xy).$$

Since $\phi(xy) = \phi(x)\phi(y)$ in each case, we conclude that ϕ is a homomorphism.

It's clear from the definition of ϕ that $\ker\phi$ consists of all of the rotations in G, i.e. $\ker\phi = G \cap \langle R_{360/n} \rangle$, where $G \leq D_n$. Note that this proves that for any subgroup G of a dihedral group, the set of rotations in G is a normal subgroup of G.

p 211, #14 This function is not a homomorphism because it fails to preserve the respective group operations. To be specific, if we denote the function by ϕ, we have

$$\phi(6 + 6) = \phi(0) = 0$$

and

$$\phi(6) + \phi(6) = 18 + 18 \bmod 10 = 6.$$

That is, $\phi(6 + 6) \neq \phi(6) + \phi(6)$.

p 212, #24a Since $\phi(7) = 6$ and $43 \cdot 6 \bmod 50 = 1$ we have

$$\phi(1) = \phi(43 \cdot 7) = 43\phi(7) = 43 \cdot 6 \bmod 15 = 3$$

from which it follows that

$$\phi(x) = x\phi(1) = 3x.$$

p 212, #36 The whole point here is that every element of $\mathbb{Z} \oplus \mathbb{Z}$ can be written as a $\mathbb{Z}$-linear combination of $(3, 2)$ and $(2, 1)$. This is because, given any $(u, v) \in \mathbb{Z} \oplus \mathbb{Z}$, the equation $x(3, 2) + y(2, 1) = (u, v)$ is the same as the vector equation

$$x \begin{pmatrix} 3 \\ 2 \end{pmatrix} + y \begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$$

which is the same as the matrix equation

$$\begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} u \\ v \end{pmatrix}$$

and the latter has the solution

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 2 & 1 \end{pmatrix}^{-1} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 2 & -3 \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} -u+2v \\ 2u-3v \end{pmatrix}$$

which is a vector with integer entries since $u, v \in \mathbb{Z}$. From this computation it follows that

$$\phi((u,v)) = \phi(x(3,2) + y(2,1)) = x\phi(3,2) + y\phi(2,1) = (-u+2v)a + (2u-3v)b.$$

In particular

$$\phi(4,4) = (-4+8)a + (8-12)b = 4a - 4b.$$

p 213, #52 We will use the one-step subgroup test to prove that H is indeed a subgroup of G. First of all, $H \neq \emptyset$ since $\alpha(e) = e = \beta(e)$ implies that $e \in H$. Now, if $a, b \in H$ then

$$\alpha(ab^{-1}) = \alpha(a)\alpha(b^{-1}) = \alpha(a)\alpha(b)^{-1} = \beta(a)\beta(b)^{-1} = \beta(a)\beta(b^{-1}) = \beta(ab^{-1})$$

implying that $ab^{-1} \in H$. Therefore H is a subgroup of G.