HOMEWORK 3 SOLUTIONS TO SELECTED PROBLEMS

Chapter 2, Problem 10. First, be aware that the two subsets of D_4 are not the same. H is basically the "square elements" of D_4: elements which equal x^2 for some $x \in D_4$. K is the set of elements whose square is the identity element, namely R_0.

However, we can use a table to help us. On the left, we have the elements of D_4. On the right, we have the squares of each element. For example, $(R_{90})^2 = R_{180}$.

x	x^2
R_0	R_0
R_{90}	R_{180}
R_{180}	R_0
R_{270}	R_{180}
H	R_0
V	R_0
D	R_0
D'	R_0

Thus, H would be all the elements that appear on the right side of the table, and K would be the elements on the left side whose square is R_0.

$$H = \{R_0, R_{180}\}$$

$$K = \{R_0, R_{180}, H, V, D, D'\}$$

Chapter 2, Problem 18. Let a be an element of some group G. To prove that a and $(a^{-1})^{-1}$ are equal, we can try the cancellation property. The key is to find some element $b \in G$ such that

$$ba = b(a^{-1})^{-1}$$

and we would apply the cancellation property to cancel the b on both sides.

One element we can try is $b = a^{-1}$. Since a^{-1} is the group inverse of a,

$$a^{-1}a = e$$

where e is the group identity. But what about $a^{-1}(a^{-1})^{-1}$? By definition, $(a^{-1})^{-1}$ is the inverse of a^{-1}. Here, we really need to remember that a^{-1} is an element of G as well. Thus,

$$a^{-1}(a^{-1})^{-1} = e$$

and so

$$a^{-1}a = a^{-1}(a^{-1})^{-1}$$

and we can cancel a^{-1} from both sides:

$$a = (a^{-1})^{-1}$$

Chapter 2, Problem 26. Suppose

$$(ab)^2 = a^2b^2$$

How do we show $ab = ba$ from this? Let us expand both sides, using the fact that $a^2 = aa$:

$$abab = aabb$$

We can use the cancellation property to simplify both sides. Cancel a on the left from both sides:

$$bab = abb$$

Cancel b on the right from both sides:

$$ba = ab$$

Chapter 3, Problem 4. Let G be a group, e be its identity element, and $a \in G$. In order to prove that a and a^{-1} have the same order in G, we need to consider two cases.

Remark. If $a = e$, then $a^{-1} = e$ as well (notice that $ee = e$, so the identity element is its own inverse). In this case, a and a^{-1} have order one. However, if a is not the identity element, its order is strictly greater than one. In the rest of this problem, we will assume $a \neq e$.

Case 1: a has finite order. Say a has order $n < \infty$. That is,

(1) $a^n = e$
(2) $a^m \neq e$ for $1 \leq m < n$

In order to show that a^{-1} has order n, we need to prove two things:

(1) $(a^{-1})^n = e$
(2) $(a^{-1})^m \neq e$ for $1 \leq m < n$

By applying a generalization of theorem 2.4 (page 50), we have

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

Since a has order n, this equals $e^{-1} = e$. Thus,

$$(a^{-1})^n = e$$

Now suppose $m < n$. Then

$$(a^{-1})^m = (a^m)^{-1}$$

Could this be the identity element e? No, because if $(a^m)^{-1} = e$, then by taking inverses of both sides, we get $a^m = e^{-1} = e$, contradicting the fact that a has order $n > m$. Thus,

$$(a^{-1})^m = (a^m)^{-1} \neq e$$

Therefore, a^{-1} has the same order as a, namely n.

Case 2: a has infinite order. In other words, $a^m \neq e$ for any positive integer m (less than infinity). Thus, we only need to prove that $(a^{-1})^m \neq e$ for any positive integer m. The proof is similar to the second half of the finite case:

$$(a^{-1})^m = (a^m)^{-1}$$

Could this be the identity element e? No, because if $(a^m)^{-1} = e$, then by taking inverses of both sides, we get $a^m = e^{-1} = e$, contradicting the fact that a has infinite order. Thus, for any positive integer m,

$$(a^{-1})^m = (a^m)^{-1} \neq e$$

Therefore, a^{-1} has infinite order as well.

Prove that if gcd$(a, n) = 1$ and b mod $n = a$ mod n, then gcd $(b, n) = 1$.

To prove this statement, we need to translate all the information so we can fit them together. We can take all three pieces of information and turn them into equations involving a, b, n, and possibly other integers.

First, we can take "b mod $n = a$ mod n" and use the definition of equivalence mod n to write the equation

$$a = qn + b$$

where q is some integer. Meanwhile, we can use the fact that the gcd is a linear combination to determine that since $\gcd(a, n) = 1$, there exist integers s and t such that

$$as + nt = 1$$

Our goal is to find integers u and v so that

$$bu + nv = 1$$

This would prove that gcd $(b, n) = 1$.

Since

$$a = qn + b$$

we can substitute for a in the equation

$$as + nt = 1$$

to get

$$(qn + b)\, s + nt = 1$$

How does this help? Let us expand the left hand side and group terms by whether they are multiplied by n or not:

$$bs + n\,(q + t) = 1$$

In other words, if we let $u = s$ and $v = q + t$, then

$$bu + nv = 1$$

Therefore, gcd $(b, n) = 1$.