Homework 6 Solutions to Selected Problems

March 16, 2012

1 Chapter 7, Problem 6 (not graded)

Note that

$$H = \{bn : b \in \mathbb{Z}\}.$$

That is, H is the subgroup of multiples of n. To find cosets, we look for an integer a that is not in H and add it to every element in H to get the coset $a + H$ (remember that the operation in $\mathbb{Z}$ is addition). For example, if $n > 1$, then the coset $1 + H$ is

$$1 + H = \{bn + 1 : b \in \mathbb{Z}\}.$$

Hence $1 + H$ is the set of all integers congruent to 1 mod n. In general, let $0 \leq r < n$. Then every coset of H can be written as

$$r + H = \{bn + r : b \in \mathbb{Z}\}.$$

How do we know that this is all the cosets? We just need to make sure that every integer is in one of these cosets. In this case, we can use the division algorithm: given any integer a, there exists integers b and r with $0 \leq r < n$ such that

$$a = bn + r.$$

Hence $a \in r + H$.

2 Chapter 7, Problem 22 (graded)

Let $g \in H$. We need to show that $g \in K$ in order to prove that $H \subseteq K$. To show that $g \in K$, we can try to write g as a product of elements in K.

We know that there are elements a and b such that

$$aH \subseteq bK.$$

Since $g \in H$, $ag \in aH$ (remember that $aH = \{ah : h \in H\}$). Hence $ag \in bK$. This means that there is an element $k \in K$ such that

$$ag = bk.$$

Be careful: we do not know if $g = k$. We also do not know if a and b are in either H or K, so let us try to get rid of a and b.

2.1 Getting rid of a

Since e, the identity, is an element of H, we have that $ae \in aH$, so $a \in aH$. Since $aH \subseteq bK$, $a \in bK$. This means that there is an element $l \in K$ such that

$$a = bl.$$

Therefore, $ag = (bl)g$, so

$$ag = (bl)g = bk.$$
$$blg = bk.$$

2.2 Getting rid of b

Cancel b by multiplying on the left by b^{-1}:

$$lg = k.$$

Solve for g:

$$g = l^{-1}k.$$

Since $l \in K$ and $k \in K$, $l^{-1}k \in K$, so $g \in K$. Therefore, if $g \in H$, then $g \in K$, so $H \subseteq K$.

3 Chapter 7, Problem 26 (not graded)

If G is cyclic, G would have at least one element of order 25. This is because if $G = \langle a \rangle$, then by Corollary 1 on page 74, $|a| = |\langle a \rangle| = |G| = 25$.

However, if G is not cyclic, it has no element of order 25 (in general if you have a finite group and an element with the same order as the group itself, then the group is cyclic and that element is a generator for the group). In this case, we need to show that $g^5 = e$ for every $g \in G$.

By Corollary 2 on page 142, if $g \in G$, then $|g|$ divides $|G|$. That is, $|g|$ divides 25, so the only possibilities for $|g|$ are 1, 5, and 25. We already eliminated 25 since the group is not cyclic. If $|g| = 1$, the $g = e$, and $e^5 = e$. If $|g| = 5$, then by definition of order, $g^5 = e$ as well. Thus, if G is not cyclic, $g^5 = e$ for every $g \in G$.

4 Chapter 7, Problem 28 (graded)

Since $|G| = 8$, there exists an element $g \in G$ with $g \neq e$. By Corollary 2 on page 142, $|g|$ divides $|G|$, so the only possibilities for $|g|$ are 1, 2, 4, and 8.

$|g|$ cannot be 1 since g is not the identity element.

If $|g| = 2$, then we have found an element of order 2.

If $|g|$ is either 4 or 8, we will have to use Theorem 4.2 on page 75 to find an element of order 2.

If $|g| = 4$, then $|g^2| = \frac{4}{\gcd(4,2)} = \frac{4}{2} = 2$, so g^2 is an element of order 2 in G.

If $|g| = 8$, then $|g^4| = \frac{8}{\gcd(8,4)} = \frac{8}{4} = 2$, so g^4 is an element of order 2 in G.

5 Chapter 8, Problem 14 (graded)

Since $G_1 \approx G_2$ and $H_1 \approx H_2$, we have functions

$$\phi : G_1 \to G_2$$

and

$$\varphi : H_1 \to H_2$$

such that ϕ and φ are isomorphisms: both maps are 1-1, onto, and operation-preserving.

We need to find an isomorphism from $G_1 \oplus H_1$ to $G_2 \oplus H_2$ using ϕ and φ.

Define $\psi : G_1 \oplus H_1 \to G_2 \oplus H_2$ by

$$\psi(g, h) = (\phi(g), \varphi(h)) .$$

5.1 1-1

Let (g_1, h_1) and (g_2, h_2) be elements of $G_1 \oplus H_1$. That is, g_1 and g_2 are in G_1, while h_1 and h_2 are in H_1. Suppose

$$\psi(g_1, h_1) = \psi(g_2, h_2).$$

Then

$$(\phi(g_1), \varphi(h_1)) = (\phi(g_2), \varphi(h_2)) .$$

Therefore,

$$\phi(g_1) = \phi(g_2)$$

and

$$\varphi(h_1) = \varphi(h_2).$$

Since ϕ and φ are 1-1, we can conclude that $g_1 = g_2$ and $h_1 = h_2$. Hence

$$(g_1, h_1) = (g_2, h_2),$$

so ψ is 1-1.

5.2 Onto

Let $(g_2, h_2) \in G_2 \oplus H_2$. In order to show that ψ is onto, we need to find an element in $G_1 \oplus H_1$ that is sent to (g_2, h_2) via ψ. Since $g_2 \in G_2$ and ϕ is onto, there exists $g_1 \in G_1$ such that $\phi(g_1) = g_2$. Similarly, since $h_2 \in H_2$ and φ is onto, there exists $h_1 \in H_1$ such that $\varphi(h_1) = h_2$. Let us check if ψ sends (g_1, h_1) to (g_2, h_2):

$$\psi(g_1, h_1) = (\phi(g_1), \varphi(h_1)) = (g_2, h_2).$$

Therefore, ψ is onto.

5.3 Operation-preserving

Let (g_1, h_1) and (g_2, h_2) be elements of $G_1 \oplus H_1$. Then we need to show that

$$\psi\left((g_1, h_1)(g_2, h_2)\right) = \psi(g_1, h_1)\psi(g_2, h_2).$$

Let us start on the left. We can use the definition of multiplication in an external direct product to write:

$$\psi\left((g_1, h_1)(g_2, h_2)\right) = \psi(g_1 g_2, h_1 h_2).$$

Use the definition of ψ:

$$\psi(g_1 g_2, h_1 h_2) = \left(\phi(g_1 g_2), \varphi(h_1 h_2)\right).$$

ϕ and φ are operation preserving:

$$\left(\phi(g_1 g_2), \varphi(h_1 h_2)\right) = \left(\phi(g_1)\phi(g_2), \varphi(h_1)\varphi(h_2)\right).$$

We use the definition of multiplication in an external direct product to split the ordered pair on the right side into a product of ordered pairs:

$$\left(\phi(g_1)\phi(g_2), \varphi(h_1)\varphi(h_2)\right) = \left(\phi(g_1), \varphi(h_1)\right)\left(\phi(g_2), \varphi(h_2)\right).$$

If you have trouble, remember that the left components must be elements of G_2, while the right components must be elements of H_2. Furthermore, since order matters when multiplying in a group (especially if the group is non-Abelian), $\phi(g_1)$ must be to the left of $\phi(g_2)$, and $\varphi(h_1)$ must be to the left of $\varphi(h_2)$.

Finally, we use the definition of ψ:

$$\left(\phi(g_1), \varphi(h_1)\right)\left(\phi(g_2), \varphi(h_2)\right) = \psi(g_1, h_1)\psi(g_2, h_2).$$

Therefore, ψ is operation-preserving. In conclusion, ψ is an isomorphism, and $G_1 \oplus H_1 \approx G_2 \oplus H_2$.

6 Chapter 8, Problem 16 (not graded)

We can find two subgroups of order 12 by using a direct product of a subgroup $H \leq \mathbb{Z}_{40}$ with a subgroup $K \leq \mathbb{Z}_{30}$. To make sure that the subgroup $H \oplus K$ has order twelve, we need to make sure that $|H| \cdot |K| = 12$. Remember, the order of a finite (sub)group is the number of elements in it. The order of a direct product $H \oplus K$ is the product of the orders of the groups:

$$|H \oplus K| = |H| \cdot |K|$$

6.1 $|H| = 4$ and $|K| = 3$

Let $H = \langle 10 \rangle$ and $K = \langle 10 \rangle$. In $\mathbb{Z}_{40}$, 10 has order 4, while in $\mathbb{Z}_{30}$, 10 has order 3. Hence $|H| = 4$ and $|K| = 3$ (see Corollary 1, page 74), so $|H \oplus K| = |H| \cdot |K| = 4 \cdot 3 = 12$.

Remark. Since H and K are cyclic and $\gcd(4, 3) = 1$, by Theorem 8.2, page 158, $H \oplus K$ is cyclic.

6.2 $|H| = 2$ and $|K| = 6$

Let $H = \langle 20 \rangle$ and $K = \langle 5 \rangle$. In $\mathbb{Z}_{40}$, 20 has order 2, while in $\mathbb{Z}_{30}$, 5 has order 6. Hence $|H| = 2$ and $|K| = 6$, so $|H \oplus K| = |H| \cdot |K| = 2 \cdot 6 = 12$.

Remark. Although H and K are cyclic, since $\gcd(2, 6) \neq 1$, by Theorem 8.2, $H \oplus K$ is not cyclic.

7 Chapter 8, Problem 26 (graded)

Before searching for a subgroup, let us discuss how to check if a subgroup H of $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ is NOT a direct product. First, look for two elements (a, b) and (c, d) in H. Second, check if both (a, d) and (c, b) are in H. If not, then H is not a direct product. The reason this works is because a direct product is a Cartesian product, and in a Cartesian product, you can mix components to get other elements. For example,

$$\mathbb{Z}_4 \oplus \mathbb{Z}_2 = \{(0,0), (1,0), (2,0), (3,0), (0,1), (1,1), (2,1), (3,1)\}.$$

Note that $(1, 0)$ and$(2, 1)$ are in $\mathbb{Z}_4 \oplus \mathbb{Z}_2$, and so are $(1, 1)$ and $(2, 0)$.

In contrast, consider the subgroup $\langle (2, 1) \rangle$:

$$\langle (2,1) \rangle = \{(0,0), (2,1)\}.$$

Note that $(0, 0)$ and$(2, 1)$ are in $\langle (2, 1) \rangle$, but $(0, 1)$ and $(2, 0)$ are not in $\langle (2, 1) \rangle$. Therefore, $\langle (2, 1) \rangle$ is not a Cartesian product, so it cannot be a direct product.

Remark. The test demonstrated in this solution is not effective at checking if a (sub)group is a direct product!

8 Chapter 8, Problem 74 (graded)

We will use the RSA scheme with $n = p \cdot q = 37 \cdot 73 = 2701$ and $r = 5$ (in general r must be coprime to $\operatorname{lcm}(37 - 1, 73 - 1) = \operatorname{lcm}(36, 72) = 72$). To encode "RM," we translate the letters into numbers using their position in the alphabet:

$$RM = 1813.$$

Next, we compute $(1813)^r = (1813)^5$ and reduce it modulo 2701:

$$(1813)^5 = 1850 \bmod 2701.$$

Thus, the encoded message is 1850.

Details

To compute and reduce $(1813)^5$ mod 2701 without having to work with large powers of a four-digit number, we can use the fact that

$$(1813)^5 = \left((1813)^2\right)^2 \cdot (1813).$$

This will allow us to work with smaller powers. We will reduce modulo 2701 along the way to keep the numbers fairly small.

$(1813)^2$:

$(1813)^2 = 3,286,969$. To reduce this, we can divide it by 2701 and round down:

$$\frac{3,286,969}{2701} \simeq 1216.$$

Thus, $3,286,969 = (1216)(2701) + r_2$ where $0 \leq r_2 < 2701$. Hence $r_2 = 2553$, and

$$(1813)^2 = 2553 \bmod 2701.$$

$(1813)^4$:

Now, $(1813)^4 = \left((1813)^2\right)^2 = (2553)^2$ mod 2701. We repeat the above process: $(2553)^2 = 6,517,809$, and

$$\frac{6,517,809}{2701} \simeq 2413.$$

$6,517,809 = (2413)(2701) + r_4$ where $0 \leq r_4 < 2701$. Hence $r_4 = 296$, and

$$(1813)^4 = 296 \bmod 2701.$$

$(1813)^5$:

Finally, $(1813)^5 = (1813)^4 \cdot (1813) = 296 \cdot 1813$ mod 2701. $296 \cdot 1813 = 536,648$, and

$$\frac{536,648}{2701} \simeq 198.$$

Thus, $536,648 = (198)(2701) + r_5$ where $0 \leq r_5 < 2701$. Hence $r_5 = 1850$, and

$$(1813)^5 = 1850 \bmod 2701.$$