Groups and Symmetry HW4 Solutions

October 3, 2014

Exercise 1. 5.7

Proof. The identity of G has order 1, so is contained in H. If $a \in G$ has finite order n, then $a^n = e$, so $(a^{-1})^n = (a^n)^{-1} = e^{-1} = e$. Thus, the inverse of an element of H has finite order, so is also in H. Now suppose that $a, b \in H$, i.e. both have finite orders n and m respectively. Then let $k = \max(n, m)$. Since G is abelian $(ab)^k = a^k b^k$, which is equal to the identity since k is at least as big as the order of both a and b. Therefore, if a and b are in H, then so is ab. Thus, H is a subgroup of G. $\square$

Exercise 2. 5.10

Proof. The elements of $\mathbb{Z}_{12}$ that generate the group are $1, 5, 7, 11$. The elements of $\mathbb{Z}_5$ that generate the group are $1, 2, 3, 4$. The elements of $\mathbb{Z}_9$ that generate the group are $1, 2, 4, 5, 7, 8$. To prove these statements show that the order of each of the elements listed is the order of the group. And remember to show that the order of any other element has order strictly less than the order of the group. In doing so you will discover the general rule. The general result that this suggests is that an element a of $\mathbb{Z}_n$ generates the group if and only if $\gcd(a, n) = 1$. (Also, see exercise 4.2 from HW3.) $\square$

Exercise 3. 5.12

Proof. The identity element is $0 = 0 \cdot a + 0 \cdot b$, so is contained in H. The inverse of any element $\lambda \cdot a + \mu \cdot b \in H$ is $-\lambda \cdot a + (-\mu) \cdot b$, which is also in H. The sum of any two elements $(\lambda_1 a + \mu_1 b), (\lambda_2 a + \mu_2 b) \in H$ is $(\lambda_1 a + \mu_1 b) + (\lambda_2 a + \mu_2 b) = ((\lambda_1 + \lambda_2)a + (\mu_1 + \mu_2)b)$, which is also in H.

Let d be the smallest positive number in the set $\lambda a + \mu b$ with λ and μ integers. Let $d = \lambda_1 a + \mu_1 b$. Since $1 \cdot a + 0 \cdot b = a$ and $0 \cdot a + 1 \cdot b = b$ are in the group H, $d \leq a$ and $d \leq b$. Since $\gcd(a, b)$ divides a and b, for any λ, μ, $\gcd(a, b)$ divides the sum $\lambda a + \mu b$. Then in particular, $\gcd(a, b)$ divides d, so $d = l \cdot \gcd(a, b)$ for some positive integer l. If d divides both a and b, then it can't be strictly larger than $\gcd(a, b)$, in which case $l = 1$, $d = \gcd(a, b)$, and we are done. So we must prove that d divides both a and b.

Since $d \leq a$, the division algorithm says that there exist positive integers q

and r such that $a = qd + r$ where $0 \leq r < d$, $0 < q$. Rearranging gives $d = \frac{a-r}{q}$. Plug this in to $d = \lambda_1 a + \mu_1 b$ to get $\frac{a-r}{q} = \lambda_1 a + \mu_1 b$, which implies $r = (1 - q\lambda_1)a + (-q\mu_1)b$. If $r > 0$ then r is a positive member of H that is strictly smaller than d, which cannot happen. Therefore, r must have been equal to 0. The same reasoning applies for b. Thus, d must divide a and b, so $d = \gcd(a, b)$. □

Exercise 4. 10.1

Proof. If $G \times H$ is cyclic then there exists an element $(g, h) \in G \times H$ such that for any other element $(g', h') \in G \times H$ there exists a power n such that $(g^n, h^n) = (g', h')$. Then in particular this says that for any $g' \in G$ there exists an n such that $g^n = g'$, so g generates G. Likewise, h generates H. □

Exercise 5. 10.4

Proof. First prove that given three groups G, H, K that $G \times H \times K$ makes sense without parentheses. In other words, $G \times (H \times K)$ is the same as $(G \times H) \times K$. To do so, just check that $\phi : G \times (H \times K) \to (G \times H) \times K$ defined by $(g, (h, k)) \mapsto ((g, h), k)$ is an isomorphism of groups.

From theorem 10.1 of this chapter we know that $\mathbb{Z}_3 \times \mathbb{Z}_2$ is really the cyclic group $\mathbb{Z}_6$ because 2 and 3 are relatively prime. Then

$$\begin{aligned} \mathbb{Z}_3 \times V &= \mathbb{Z}_3 \times (\mathbb{Z}_2 \times \mathbb{Z}_2) \\ &\cong (\mathbb{Z}_3 \times \mathbb{Z}_2) \times \mathbb{Z}_2 \\ &\cong \mathbb{Z}_6 \times \mathbb{Z}_2. \end{aligned}$$

□

Exercise 6. 10.5

Proof. The identity element (e, e) is contained in the diagonal. Given an element (g, g) in the diagonal, the inverse (g^{-1}, g^{-1}) is in the diagonal. Given two elements (g, g) and (h, h) in the diagonal, their product $(g, g)(h, h) = (gh, gh)$ is in the diagonal. Thus, the diagonal $\Delta = \{(x, x) \mid x \in G\}$ forms a subgroup of $G \times G$. Consider the homomorphism $\phi : G \to \Delta$ defined by $g \mapsto (g, g)$. This is a group homomorphism because $\phi(gh) = (gh, gh) = (g, g)(h, h) = \phi(g)\phi(h)$ for any two elements $g, h \in G$. The image of ϕ is all of Δ because for any $(g, g) \in \Delta$, $\phi(g) = (g, g)$. Finally, ϕ is one-to-one because if $(g, g) = \phi(g) = \phi(h) = (h, h)$ then $g = h$. Thus, ϕ is an isomorphism of groups. □

Exercise 7. 10.6

Proof. The element (e_G, e_H) is contained in $A \times B$ because $e_G \in A$ and $e_H \in B$ because A and B are themselves subgroups of G and H respectively. Similarly for any $(a, b) \in A \times B$ the inverse $(a, b)^{-1} = (a^{-1}, b^{-1}) \in A \times B$ because A and B are subgroups. And for any two elements $(a, b), (a', b') \in A \times B$ we have that

$aa' \in A$ and $bb' \in B$, so $(aa', bb') \in A \times B$.

A subgroup that does not occur in this way is the diagonal subgroup (from the previous question), $\Delta = \{(n, n) \mid n \in \mathbb{Z}\}$. $\square$

Exercise 8. 10.7

Proof. These groups are all distinct, despite all having the same order. There may be many different ways to prove this.

The group $\mathbb{Z}_{24}$ is cyclic so for it to be isomorphic to some other group G, it must be that G is cyclic. But none of the other groups on the list are cyclic. To see this note that since 12 and 2 are not relatively prime, $\mathbb{Z}_{12} \times \mathbb{Z}_2$ is not cyclic. Furthermore, any dihedral group D_n is not even abelian, so $D_{12}, D_4 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \times D_6$ are all nonabelian because they contain a copy of a dihedral group as a subgroup. Recall that A_4 is the symmetry group of the tetrahedron not including reflections (exercises in chapter 1) and that it is nonabelian. Since S_4 and $A_4 \times \mathbb{Z}_2$ both contain A_4 as a subgroup, they are both nonabelian. To sum up thus far, $\mathbb{Z}_{24}$ is the only cyclic group, so it is in its own isomorphism class in our list. Out of the remaining groups, $\mathbb{Z}_{12} \times \mathbb{Z}_2$ is the only abelian group, so it is in its own isomorphism class as well.

Now we are left with $D_4 \times \mathbb{Z}_3, D_{12}, A_4 \times \mathbb{Z}_2, \mathbb{Z}_2 \times D_6$, and S_4. Let's count the number of elements of order 2 in each group. Recalling exercise 4.1 from HW2, the group D_{12} has 13 elements of order 2.

Similarly, D_6 has 7 elements of order 2, which implies $\mathbb{Z}_2 \times D_6$ has 15 elements of order 2 (these are $(0, d)$, $(1, d)$, and $(1, e)$ where d is order 2 in D_6).

The group D_4 has 5 elements of order 2, and since $\mathbb{Z}_3$ has no elements of order 2, the group $D_4 \times \mathbb{Z}_3$ has 5 elements of order 2. The group A_4 has the three elements $(12)(34), (13)(24), (14)(23)$ of order 2 (which if you recall the exercises of chapter 1 correspond to the rotation of the tetrahedron about the axis through opposite edges). Thus, the group $A_4 \times \mathbb{Z}_2$ has 7 elements of order 2.

Finally, S_4 can be checked directly to have the following 9 elements of order 2,

$$(12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23).$$

Thus, each group has a different number of elements of order 2, so they cannot possibly be isomorphic. $\square$

Exercise 9. 10.10

Proof. For any groups A, B, the products $A \times B$ and $B \times A$ are isomorphic via the obvious isomorphism $(a, b) \mapsto (b, a)$. Thus, $G \times \mathbb{Z}$ is the same as $\mathbb{Z} \times G$.

Consider the map $\phi : G \to \mathbb{Z} \times G$ defined by

$$(a_1, a_2, a_3, a_4 \ldots) \mapsto (a_1, (a_2, a_3, a_4, \ldots)) .$$

This map is certainly well-defined. It is a homomorphism because

$$\begin{aligned}
\phi((a_1, a_2, a_3, a_4 \ldots) + (b_1, b_2, b_3, b_4 \ldots)) &= \phi((a_1 + b_1, a_2 + b_2, a_3 + b_3, a_4 + b_4 \ldots)) \\
&= (a_1 + b_1, (a_2 + b_2, a_3 + b_3, a_4 + b_4, \ldots)) \\
&= (a_1 + b_1, (a_2, a_3, a_4, \ldots) + (b_2, b_3, b_4, \ldots)) \\
&= (a_1, (a_2, a_3, a_4, \ldots)) + (b_1, (b_2, b_3, b_4, \ldots)) \\
&= \phi((a_1, a_2, a_3, a_4 \ldots)) + \phi((b_1, b_2, b_3, b_4 \ldots)).
\end{aligned}$$

It is one-to-one because if $(a_1, (a_2, a_3, \ldots)) = (b_1, (b_2, b_3, \ldots))$, then certainly $(a_1, a_2, a_3, \ldots) = (b_1, b_2, b_3, \ldots)$. Finally it is surjective because any element $(a_1, (a_2, a_3, \ldots))$ in $\mathbb{Z} \times G$ gets mapped to by $(a_1, a_2, a_3, \ldots)$ in G.

Now consider the map $\psi : G \to G \times G$ defined by $(a_1, a_2, a_3, a_4, \ldots) \mapsto ((a_1, a_3, a_5, \ldots), (a_2, a_4, a_6, \ldots))$. Again check that this is a homomorphism, that it is surjective, and injective. Checking these is similar to what we just did with $G \times \mathbb{Z}$. $\square$

Exercise 10. 10.12

Proof. Let $G = \{e, g_1, g_2, g_3\}$ where the g_i are distinct and not equal to the identity. If $G = \{e, g_1, g_2, g_3\}$ is not cyclic, then the order of each element has to be strictly less than 4. The element e has order 1, while none of the elements g_1, g_2, g_3 can have order 1 because if g_i has order 1 then $g_i = e$. But we are assuming that G is a group of 4 elements. Thus, each g_i can have order 2 or 3.

We claim that the order of each element g_1, g_2, g_3 is two. To get a contradiction, suppose that one of them, say g_1 has order 3. Then $g_1^2 \neq e$, so g_1^2 is equal to either g_2 or g_3. Without loss of generality, suppose that $g_1^2 = g_2$. Then $e = g_1^3 = g_1 g_1^2 = g_1 g_2$, so g_2 is the inverse of g_1 and vice versa. Recall that for any group, multiplication by an element on the left is a bijection of the group with itself. In other words, multiplying on the left by g_1 must permute the 4 elements of G. So far, we have

$$\begin{aligned}
g_1 \cdot e &= g_1, \\
g_1 \cdot g_1 &= g_2, \\
g_1 \cdot g_2 &= e,
\end{aligned}$$

thus for g_1 to permute the elements, it must be that $g_1 \cdot g_3 = g_3$. But this implies that $g_1 = e$, which is a contradiction. Since we would arrive at this same contradiction no matter which g_i we assumed to have order 3, it follows that each g_i has order 2. (In Chapter 11, we will see that the order of an element always divides the order of the group. In this case the order of the group is 4, so we would have been able to directly conclude that order of every nonidentity element is 2.)

With this information we can fill in a portion of the multiplication table for our group G.

	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e		
g_2	g_2		e	
g_3	g_3			e

Now consider the product g_1g_2. Since the row corresponding to g_1 has to permute the elements of G, this product g_1g_2 can be either g_2 or g_3. If $g_1g_2 = g_2$, then by taking inverse $g_1 = e$, which cannot happen. Thus, $g_1g_2 = g_3$. By similar reasoning we can fill in all of the remaining spots in the table to get.

	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3	e	g_1
g_3	g_3	g_2	g_1	e

This is precisely the group table for the Klein four groups $\mathbb{Z}_2 \times \mathbb{Z}_2$ under the homomorphism $g_1 \mapsto (1, 0)$, $g_2 \mapsto (0, 1)$, $g_3 \mapsto (1, 1)$. $\square$