Groups and Symmetry HW6 Solutions

November 4, 2014

Exercise 1. 7.1

Proof. Check that the set forms a group and find that it is cyclic (it is generated by 2). Example (iv) of chapter 7 shows that any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$, so in this case this cyclic group of 6 elements must be $\mathbb{Z}_6$. Or you can write down an explicit isomorphism. □

Exercise 2. 7.2

Proof. As always, first check that this set actually forms a group under multiplication mod 20. Although this group has 8 elements it is not isomorphic to $\mathbb{Z}_8$ because there is no one element that generates the entire group. To see this, calculate the order of each of the elements $1, 3, 7, 9, 11, 13, 17, 19$ to find that they are $1, 4, 4, 2, 2, 4, 4, 2$ respectively. □

Exercise 3. 7.4

Proof. Let s be the reflection of the triangle about the axis through a vertex and the opposite side, and let r be the rotation clockwise by $2\pi/3$. Then define the mapping ϕ by sending s to (12) and r to (123) is an explicit isomorphism. Since s and r generate all of D_3, we can extend the definition of ϕ to any element of D_3. More explicitly, ϕ maps the six elements of D_3, e, r, r^2, s, rs, r^2s to $e, (123), (132), (12), (13), (23)$. This is a bijection, and check that this is indeed a homomorphism (i.e. respects the group structures). Our choice to send s to (12) can be viewed as labeling the vertices of the triangle such that s is the reflection about the axis through the vertex 3 and the midpoint of the edge connecting 1 and 2. At this point, there is still a choice to be made as to whether the vertices are labelled $3, 2, 1$ when read clockwise, or $3, 1, 2$. Choosing to send r to (123) fixes this choice as a clockwise $3, 1, 2$ labeling.

The same reasoning applies for if choose to send s to (23) or (13), both leading to two other possibilities as to where to send r depending on the clockwise labeling. Therefore, there are a total of $3 \cdot 2 = 6$ explicit isomorphisms between D_3 and S_3. □

Exercise 4. 7.5

Proof. Let $\phi : G \to G$ be defined by $\phi(x) = x^{-1}$. Since every element of a group has an inverse, this map is always a bijection. For it to be an isomorphism we must check that it satisfies the homomorphism property. Thus, ϕ is an isomorphism if and only if for all $x, y \in G$, $\phi(x)\phi(y) = \phi(xy)$, but this is true if and only if for all $x, y \in G$

$$\begin{aligned}\phi(x)\phi(y) &= \phi(xy) \\ &= (xy)^{-1} \\ &= y^{-1}x^{-1} \\ &= \phi(y)\phi(x),\end{aligned}$$

(i.e. if and only if for all $x, y \in G$, $\phi(x)\phi(y) = \phi(y)\phi(x)$). But since ϕ is a bijection of G with G, this holds if and only if G is abelian. □

Exercise 5. 7.8

Proof. Consider the group of integers $\mathbb{Z}$ under addition and its proper subgroup $2 \cdot \mathbb{Z}$. Define the map $\phi : \mathbb{Z} \to \mathbb{Z}$ by $\phi(n) = 2 \cdot n$. This is a bijection because every even integer $2x$ satisfies $\phi(x) = 2x$, and if $2x = \phi(x) = \phi(y) = 2y$ then $x = y$. The map ϕ is a homomorphism because $\phi(x+y) = 2(x+y) = 2x+2y = \phi(x) + \phi(y)$ for all $x, y \in \mathbb{Z}$. □

Exercise 6. 7.9

Proof. Suppose that x generates G, so that any element of G is of the form x^n for some integer n. Then once we know the image of x under ϕ, we know all of ϕ because $\phi(x^n) = \phi(x)^n$. Since ϕ is an isomorphism, and in particular surjective, every element of G can be written as $\phi(x^n) = \phi(x)^n$ for some integer n, so $\phi(x)$ also generates G.

To summarize, an isomorphism of G is completely determined once the image of a generator is determined, and in particular the image of this generator must also be a generator. Consider the generator 1 in $\mathbb{Z}$. Once we define where $\phi : \mathbb{Z} \to \mathbb{Z}$ maps 1, we have completely determined ϕ by the rule $\phi(n) = n \cdot \phi(1)$. The image, $\phi(1)$, must also be a generator, but there are only two generators of $\mathbb{Z}$, namely 1 and -1. Therefore, there are two isomorphisms of $\mathbb{Z}$, the identity isomorphism, and the one that sends every integer n to $-n$. We can even phrase this result as, "the group of isomorphisms of $\mathbb{Z}$ with itself is isomorphic to $\mathbb{Z}_2$."

Similarly, list the generators of $\mathbb{Z}_{12}$, which are $1, 5, 7, 11$ (see exercise $5, 10$). Then the generator 1 can be mapped to $1, 5, 7$, or 11. In this case, the group of isomorphisms of $\mathbb{Z}_{12}$ with itself is isomorphic to the Klein group. Do you see why? □

Exercise 7. 9.1

Proof. (a) Yes. The identity is in this set, the product of two diagonal matrices is diagonal, and the inverse of a diagonal matrix

$$\begin{pmatrix} x_1 & 0 & \dots & 0 \\ 0 & x_2 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \dots & x_n \end{pmatrix} \text{ is } \begin{pmatrix} 1/x_1 & 0 & \dots & 0 \\ 0 & 1/x_2 & \dots & 0 \\ & & \ddots & \\ 0 & 0 & \dots & 1/x_n \end{pmatrix}.$$

(b) No, the product of two symmetric matrices need not be symmetric. In fact, $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ is a symmetric matrix, but has determinant 0, so is not even invertible.

(c) No. The inverse of a matrix may not have integer entries. For example $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ is invertible, but its inverse is $\begin{pmatrix} 1/2 & 0 \\ 0 & 1 \end{pmatrix}$.

(d) Yes, check the axioms for a group.

□

Exercise 8. 9.2

Proof. The determinant of such a matrix is $ac - b \cdot 0 = ac \neq 0$, so the matrices in this set are invertible. In particular, the inverse of $\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$ is $\begin{pmatrix} 1/a & -b/ac \\ 0 & 1/c \end{pmatrix}$, which is contained in this set of matrices. The identity matrix is also in this set of matrices. Finally, check that the product of two such matrices is again such a matrix. □

Exercise 9. 9.3

Proof. The identity matrix has determinant 1 so is contained in this set. If A, B are two matrices with integer entries such that $\det(A) = \pm 1$ and $\det(B) = \pm 1$, then $\det(AB) = \det(A)\det(B) = \pm 1$. The only thing left to check is that if A is in the set, then so is the inverse A^{-1}.

Let A be an integer matrix such that $\det(A)$ is 1 or -1. Recall the following formula for the inverse, $A^{-1} = \frac{1}{det(A)}(\text{adjugate of } A)$, where the adjugate of a matrix A is the transpose of the cofactor matrix of A. If A contains only integer entries then each of its cofactors is an integer, so the cofactor matrix and the adjugate contain only integer entries. Therefore, the inverse $A^{-1} = \frac{1}{det(A)}(adjA)$ has integer entries since $det(A) = \pm 1$. Furthermore, $\pm 1 = \det(I) = \det(AA^{-1}) = \det(A)\det(A^{-1})$ implies that $\det(A^{-1}) = \pm 1$, so the inverse A^{-1} is contained in this set of matrices. Therefore, this set forms a group under matrix multiplication. □

Exercise 10. 9.5

Proof. Each one of these four relations is a result of multiplying the two matrices and applying the four cosine and sine formulas

$$\cos(\theta)\cos(\phi) \pm \sin(\theta)\sin(\phi) = \cos(\theta \mp \phi)$$
$$\sin(\theta)\cos(\phi) \pm \sin(\phi)\cos(\theta) = \sin(\theta \pm \phi)$$

(note the relative plus-minus signs).

Geometrically, $A_\theta A_\phi = A_{\theta+\phi}$ says that an anticlockwise rotation through ϕ followed by an anticlockwise rotation through θ is the same as performing a single anticlockwise rotation through angle $\theta + \phi$. The relation $A_\theta B_\phi = B_{\theta+\phi}$ says that performing a reflection in the line at angle $\phi/2$ to the positive x-axis followed by an anticlockwise rotation through angle θ is the same as performing a single reflection in the line at angle $(\theta + \phi)/2$. Similarly, rotating by ϕ and then reflection in the line at angle $\theta/2$ is the same as a single reflection in the line at angle $(\theta - \phi)/2$. Finally, a reflection in the line with angle $\phi/2$ followed by a reflection in the line $\theta/2$ is the same as a single rotation through angle $\theta - \phi$. Note that the angles are understood $\mod 2\pi$. Can you see directly from geometry why these relations must be true? □