Solutions to Dummit and Foote's *Abstract Algebra*

Written by
James Ha

Contents

1 Introduction to Groups **1**
1.1 Basic Axioms and Examples 1
1.2 Dihedral Groups 10
1.3 Symmetric Groups 13
1.4 Matrix Groups 17
1.5 The Quaternion Group 23
1.6 Homomorphisms and Isomorphisms 24
1.7 Group Actions 32

Chapter 1

Introduction to Groups

1.1 Basic Axioms and Examples

1. (a) This operation is not associative, since $a \star (b \star c) = a - (b - c) = a - b + c \neq a - b - c = (a - b) - c = (a \star b) \star c$.

1. (b) This operation is associative, since $a \star (b \star c) = a + (b + c + bc) + a(b + c + bc) = a + b + c + bc + ab + ac + abc = (a + b + ab) + c + (a + b + ab)c = (a \star b) \star c$.

1. (c) This operation is not associative, since $a \star (b \star c) = \frac{a + \frac{b+c}{5}}{5} = \frac{a}{5} + \frac{b+c}{25} \neq \frac{a+b}{25} + \frac{c}{5} = \frac{\frac{a+b}{5} + c}{5} = (a \star b) \star c$.

1. (d) This operation is associative, since $(a, b) \star ((c, d) \star (e, f)) = (a, b) \star (cf + de, df) = (adf + bcf + bde, bdf) = (ad + bc, bd) \star (e, f) = ((a, b) \star (c, d)) \star (e, f)$.

1. (e) This operation is not associative, since $a \star (b \star c) = \frac{ac}{b} \neq \frac{a}{bc} = (a \star b) \star c$.

2. The operation $a \star b = a - b$ is clearly not commutative since $a - b \neq b - a$ in general.

The operation $a \star b = a + b + ab$ is commutative, since $a \star b = a + b + ab = b + a + ba = b \star a$.

The operation $a \star b = \frac{a+b}{5}$ is commutative, since $a \star b = \frac{a+b}{5} = \frac{b+a}{5} = b \star a$.

The operation $(a, b) \star (c, d) = (ad + bc, bd)$ is commutative, since $(a, b) \star (c, d) = (ad + bc, bd) = (cb + da, db) = (c, d) \star (a, b)$.

Finally, the operation $a \star b = \frac{a}{b}$ is not commutative, since $\frac{a}{b} \neq \frac{b}{a}$ in general.

3. Addition of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is clearly associative, since $\overline{a} + (\overline{b} + \overline{c}) = \overline{a} + \overline{b+c} = \overline{a+b+c} = \overline{a+b} + \overline{c} = (\overline{a} + \overline{b}) + \overline{c}$.

4. Multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is clearly associative, since $\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a} \cdot \overline{bc} = \overline{abc} = \overline{ab} \cdot \overline{c} = (\overline{a} \cdot \overline{b}) \cdot \overline{c}$.

5. We have already shown that multiplication of residue classes in $\mathbb{Z}/n\mathbb{Z}$ is associative, and it is clear that the identity element is $\overline{1}$ if $n > 1$. However, if $n > 1$, then the residue class $\overline{0}$ has no multiplicative inverse, since its product with every other residue class of $\mathbb{Z}/n\mathbb{Z}$ is $\overline{0}$. Therefore, $\mathbb{Z}/n\mathbb{Z}$ is not a group under multiplication of residue classes.

6. (a) Addition of rational numbers is associative, since $\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf+ed}{df} = \frac{adf+bcf+bed}{bdf} = \frac{ad+bc}{bd} + \frac{e}{f} = \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f}$. Now let $\frac{a}{b}$ and $\frac{c}{d}$ be two rational numbers in lowest terms with odd denominators. Their sum $\frac{ad+bc}{bd}$ has an odd denominator as well, since b and d are both odd. Remembering that odd integers can only be divided by other odd integers, we find that the sum $\frac{ad+bc}{bd}$ written in lowest terms must have an odd denominator. The identity element is clearly $\frac{0}{1}$. Finally, noting that every element $\frac{a}{b}$ has an inverse $-\frac{a}{b}$ in the set, we conclude that this set is a group under addition.

6. (b) This set is not closed under addition (e.g., $\frac{1}{2} + \frac{1}{6} = \frac{2}{3}$, which has odd denominator). This set cannot be a group under addition.

6. (c) This set is not closed under addition (e.g., $\frac{9}{10} + \frac{2}{10} = \frac{11}{10} > 1$). This set cannot be a group under addition.

6. (d) This set is not closed under addition (e.g., $\frac{11}{10} + (-\frac{10}{10}) = \frac{1}{10} < 1$). This set cannot be a group under addition.

6. (e) This is the set of integers and half-integers. The sum of two integers is an integer, the sum of two half-integers is an integer, and the sum of an integer and a half-integer is a half-integer, so this set is closed under addition. The identity element is clearly 0. Finally, each element a has an inverse $-a$ in the set. Therefore, this set is a group under addition.

6. (f) This set is not closed under addition (e.g., $\frac{1}{2}+\frac{1}{3}=\frac{5}{6}$, which does not have denominator 1, 2, or 3). This set cannot be a group under addition.

7. The operation $\star$ is well-defined due to the fact that addition, subtraction, and the greatest integer function are well-defined. It is also obvious that for any $x, y \in \mathbb{R}$, $x \star y \in [0,1)$, so G is closed under $\star$. It is not hard to see that for $x, y \in \mathbb{R}$, $[x+y] = [x] + [y] + [x - [x] + y - [y]]$. Then the operation $\star$ is associative, since

$$\begin{aligned}
a \star (b \star c) &= a \star (b + c - [b+c]) \\
&= a + b + c - [b+c] - [a + b + c - [b+c]] \\
&= a + b + c - [b+c] - [a+b+c] + [[b+c]] - [a + b + c - [a+b+c] - [b+c] + [[b+c]]] \\
&= a + b + c - [a+b+c] \\
&= a + b + c - [a+b] - [a+b+c] + [a+b] - [a + b + c - [a+b+c] - [a+b] + [a+b]] \\
&= a + b + c - [a+b] - [a+b+c-[a+b]] \\
&= (a + b - [a+b]) \star c \\
&= (a \star b) \star c
\end{aligned}$$

The identity element is clearly 0, since for any $g \in G$, $g \star 0 = g + 0 - [g+0] = g - [g] = g$. Since 0 is the identity, it is its own inverse. If $g > 0$, the inverse of g is $1 - g$, since $g \star (1-g) = g + 1 - g - [g + 1 - g] = 1 - [1] = 0$. Note that since $0 < g < 1$, $0 > -g > -1$ and therefore, $1 > 1 - g > 0$, so $1 - g \in G$. Therefore, G is a group under $\star$. Finally, note that G is an abelian group under $\star$, since $a \star b = a + b - [a+b] = b + a - [b+a] = b \star a$.

8. (a) Since multiplication in $\mathbb{C}$ is associative, we need only show that G is closed under multiplication, that there exists an identity element, and that every element has an inverse in G. If $z_1, z_2 \in G$, then there exist $n_1, n_2 \in \mathbb{Z}$ such that $z_1^{n_1} = z_2^{n_2} = 1$. Then note that for the product $z_1 z_2$, $(z_1 z_2)^{n_1 n_2} = z_1^{n_1 n_2} z_2^{n_1 n_2} = 1^{n_2} 1^{n_1} = 1$ and therefore, $z_1 z_2 \in G$. Hence, G is closed under multiplication. The identity element is clearly 1 and it is its own inverse. For any other element $z \in G$, we can show that $z^{n-1} \in G$, since $(z^{n-1})^n = z^{(n-1)n} = (z^n)^{n-1} = 1^{n-1} = 1$. It is easy to see that z and z^{n-1} are each other's inverses. Therefore, G is a group under multiplication.

8. (b) G is not a group under addition because it does not contain 0 and thus, does not have an identity element.

9. (a) We are given that addition in $\mathbb{R}$ is associative. Observe that G is closed under addition since for $a_1 + b_1\sqrt{2}, a_2 + b_2\sqrt{2} \in G$, we have $a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2} = (a_1 + a_2) + (b_1 + b_2)\sqrt{2}$, which is an element of G because $\mathbb{Q}$ is closed under addition. The identity element $0 + 0\sqrt{2} = 0$ is clearly in G. Finally, every

element $a + b\sqrt{2}$ has an inverse $-a - b\sqrt{2} \in G$, since if $a, b \in \mathbb{Q}$, then $-a, -b \in \mathbb{Q}$ as well. Therefore G is a group under addition.

9. (b) We are given that multiplication in $\mathbb{R}$ is associative. The product of any two non-zero elements $a_1 + b_1\sqrt{2}$ and $a_2 + b_2\sqrt{2}$ is $(a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2}$. The product is non-zero and is clearly an element of G, since $\mathbb{Q}$ is closed under addition and multiplication. Thus the non-zero elements of G are closed under multiplication. The multiplicative identity $1 + 0\sqrt{2} = 1$ is clearly a non-zero element of G. Finally, each non-zero element $a + b\sqrt{2}$ has an inverse $\frac{a-b\sqrt{2}}{a^2-2b^2}$, which is clearly a non-zero element of G. Therefore, the non-zero elements of G form a group under multiplication.

10. Let G be a finite group and M be the multiplication table of G. If G is abelian, then for any two elements $g_i, g_j \in G$, $g_ig_j = g_jg_i$. Consequently, $M_{ij} = M_{ji}$, and M is therefore a symmetric matrix.

Now suppose that G's multiplication table M is a symmetric matrix. Then for any i, j, $M_{ij} = g_ig_j = g_jg_i = M_{ji}$. Since $g_ig_j = g_jg_i$ for any i, j, we find that G is an abelian group.

11. The orders of the elements are $|\overline{0}| = 1$, $|\overline{1}| = 12$, $|\overline{2}| = 6$, $|\overline{3}| = 4$, $|\overline{4}| = 3$, $|\overline{5}| = 12$, $|\overline{6}| = 2$, $|\overline{7}| = 12$, $|\overline{8}| = 3$, $|\overline{9}| = 4$, $|\overline{10}| = 6$, $|\overline{11}| = 12$.

12. The orders are $|\overline{1}| = 1$, $|\overline{-1}| = 2$, $|\overline{5}| = 2$, $|\overline{7}| = 2$, $|\overline{-7}| = 2$, $|\overline{13}| = 1$.

13. The orders are $|\overline{1}| = 36$, $|\overline{2}| = 18$, $|\overline{6}| = 6$, $|\overline{9}| = 4$, $|\overline{10}| = 18$, $|\overline{12}| = 3$, $|\overline{-1}| = 36$, $|\overline{-10}| = 18$, $|\overline{-18}| = 2$.

14. The orders are $|\overline{1}| = 1$, $|\overline{-1}| = 2$, $|\overline{5}| = 6$, $|\overline{13}| = 3$, $|\overline{-13}| = 6$, $|\overline{17}| = 2$.

15. This is clearly true for any single element $a_1 \in G$. Now assume that it holds true for the product of any n elements $a_1, ..., a_n \in G$. Consider the product $(a_1...a_{n+1})$ of $n + 1$ elements of G. We may write $(a_1...a_{n+1}) = (a_1...a_n)a_{n+1}$. Since $(a_1...a_n)$ is a product of n elements of G, its inverse satisfies $(a_1...a_n)^{-1} = a_n^{-1}...a_1^{-1}$. Multiplying, we obtain $(a_1...a_n)^{-1}(a_1...a_n)a_{n+1} = a_{n+1}$. The inverse of this product is simply a_{n+1}^{-1}: $a_{n+1}^{-1}a_{n+1} = a_{n+1}^{-1}(a_1...a_n)^{-1}a_1...a_{n+1} = a_{n+1}^{-1}...a_1^{-1}a_1...a_{n+1} = 1$. Since the product of $a_{n+1}^{-1}...a_1^{-1}$ and $a_1...a_{n+1}$ is the identity, we find that $a_{n+1}^{-1}...a_1^{-1} = (a_1...a_{n+1})^{-1}$. By induction on n, we have the claim.

16. Let $x \in G$ and suppose $x^2 = 1$. Then by definition of the order of x, $1 \leq |x| \leq 2$. That is to say, $|x|$ is either 1 or 2.

Now, suppose that $|x|$ is either 1 or 2. This means that either $x = 1$ or $x^2 = 1$. But if $x = 1$, then $x^2 = 1^2 = 1$. So either way, $x^2 = 1$.

17. Let $x \in G$ and suppose $|x| = n$ for some $n \in \mathbb{Z}^+$. Then $x^n = x \cdot x^{n-1} = 1$. x^{n-1} is clearly an element of G, since G must be closed under its group operation. Since the product of x^{n-1} and x is the identity, we must have $x^{-1} = x^{n-1}$.

18. Let $x, y \in G$. If $xy = yx$, then left multiplication of y^{-1} yields $y^{-1}xy = x$. Similarly, if $y^{-1}xy = x$, then left multiplication of y yields $xy = yx$.

If $y^{-1}xy = x$, then left multiplication of x^{-1} yields $x^{-1}y^{-1}xy = 1$. Similarly, if $x^{-1}y^{-1}xy = 1$, then left multiplication of x yields $y^{-1}xy = x$. Hence, the claim.

19. (a) Let $x \in G$ and $a, b \in \mathbb{Z}^+$. Then $x^{a+b} = \prod_{i=1}^{a+b} x = \prod_{i=1}^{a} x \prod_{i=1}^{b} x = x^a x^b$. Furthermore, $(x^a)^b = \prod_{i=1}^{b} x^a = \prod_{i=1}^{ab} x = x^{ab}$. That is to say, these are consequences of the generalized associative law.

19. (b) This is really just a consequence of exercise 15, but we can prove it by induction if you want. This is clearly true for $a = 1$, since $(x)^{-1} = x^{-1}$. Suppose it is true for all $a \leq n$. Consider $a = n + 1$, where we may write $x^{n+1} = x^n \cdot x$. Applying $(x^n)^{-1} = x^{-n}$, we obtain $x^{-n}x^{n+1} = x^{-n} \cdot x^n \cdot x = x$. To this, we may apply x^{-1}, yielding $x^{-1} \cdot x^{-n} \cdot x^{n+1} = x^{-1} \cdot x^{-n} \cdot x^n \cdot x = x^{-1} \cdot x = 1$. This implies that $x^{-1} \cdot x^{-n} = x^{-(n+1)}$ is the inverse of x^{n+1} (i.e., $x^{-(n+1)} = (x^{n+1})^{-1}$). By induction on n, we have the claim.

19. (c) Since x^{-1} is also an element of G, we already have the proof for the case where a and b are both negative. It is also obvious that the equations hold if at least one of $a = 0$, $b = 0$, or $a = b = 0$.

For the case where a and b are of opposite sign, simply note that $1 \cdot x = x = x \cdot 1$ so that we may insert arbitrary numbers of factors xx^{-1} or $x^{-1}x$ into the expansion of any power of x. Then $x^{a+b} = x^a x^{-a} x^{a+b} = x^a x^b$ (i.e., it is a consequence of the generalized associative law). The equation $(x^a)^b = x^{ab}$ in this case is just a consequence of part (b) above or the generalized associative law for $b < 0$ or $a < 0$, respectively.

20. For $x \in G$ let $|x| = n$. Then $x^n = 1 = x^{-n}x^n$. It follows that $x^{-n} = 1$. Furthermore, no positive integer $k < n$ exists such that $x^{-k} = 1$, for if there were

such a k, then $x^k = x^k \cdot 1 = x^k \cdot x^{-k} = 1$. Since $|x| > k$, this is a contradiction. Therefore, $|x^{-1}| = n$. For a proof of the converse, simply switch x and x^{-1} above.

21. Let G be a finite group, and consider $x \in G$ such that $|x| = n$, where n is odd. Since, n is odd, there exists $j \in \mathbb{Z}$ such that $j \geq 0$ and $n = 2j + 1$. We have $x^{2j+2} = x^{2j+1} \cdot x = 1 \cdot x = x$. Writing $k = j + 1$ and noting that $k \geq 1$, we have the claim.

22. First, we show that $(g^{-1}xg)^n = g^{-1}x^n g$. The claim is clearly true for $n = 1$. Suppose it holds for all $n \leq k$. Then for $n = k + 1$, we have $(g^{-1}xg)^{k+1} = (g^{-1}xg)^k g^{-1}xg = g^{-1}x^k gg^{-1}xg = g^{-1}x^k xg = g^{-1}x^{k+1}g$. By induction on k, we have the claim.

Now, note that $(g^{-1}xg)^{|x|} = g^{-1}x^{|x|}g = g^{-1}g = 1$, so that $|g^{-1}xg| \leq |x|$. Suppose that there exists $k < |x|$ such that $(g^{-1}xg)^k = 1$. Then $1 = gg^{-1} = g(g^{-1}xg)^k g^{-1} = gg^{-1}x^k gg^{-1} = x^k$. This is a contradiction, so no such k exists and $|g^{-1}xg| = |x|$.

In this proof, x and g were any two elements of G, so consider $x = ab$ and $g = a$, where $a, b \in G$. We find that $|ba| = |a^{-1}aba| = |g^{-1}xg| = |x| = |ab|$.

23. This is obvious. If $|x| = n$ and $n = st$, for $n, s, t \in \mathbb{Z}^+$, then $(x^s)^t = x^{st} = 1$. There cannot be any positive integer $k < t$ such that $(x^s)^k = 1$ because that would imply that $|x| \neq n$. Therefore $|x^s| = t$.

24. Let a and b be commuting elements of G. Clearly the equation holds for $n = 1$. Now suppose it holds for $n \leq k$ and consider $(ab)^{k+1}$. We have $(ab)^{k+1} = (ab)^k ab = a^k b^k ab = a^k ab^k b = a^{k+1}b^{k+1}$, where we used the fact that a and b commute to obtain the second-to-last equality. By induction on k, we have the claim for $n \in \mathbb{Z}^+$. The equation obviously holds for $n = 0$ as well, since $(ab)^0 = 1 = 1 \cdot 1 = a^0 b^0$.

For $n < 0$, we simply need to show that if $ab = ba$, then $a^{-1}b^{-1} = b^{-1}a^{-1}$. It is easy to see that $(ab)^{-1} = b^{-1}a^{-1}$ and $(ba)^{-1} = a^{-1}b^{-1}$. If $ab = ba$, then $1 = (ab)^{-1}ab = (ab)^{-1}ba$. It follows from the uniqueness of $(ba)^{-1}$ that $b^{-1}a^{-1} = (ab)^{-1} = (ba)^{-1} = a^{-1}b^{-1}$. Since a^{-1} and b^{-1} commute, the proof above can be applied to them and therefore, $(ab)^n = a^n b^n$, $\forall n \in \mathbb{Z}$.

25. Suppose $x^2 = 1$, $\forall x \in G$. Consider any two elements $a, b \in G$, and note that their product ab is also an element of G. Therefore, $(ab)^2 = abab = 1$. However, $abba = 1$ also, so $abab = abba$. Multiplying on the left by ba, we find that $ab = ba$. Therefore, G is an abelian group.

26. We are given that H is closed under $\star$ and closed under inverses. Then for any $h \in H$ the product $hh^{-1} = 1$ must also be in H, so H contains the identity element. Since $\star$ is associative in G, it must also be associative in H. Therefore, H is a group under $\star$.

27. Let $H = \{x^n \mid n \in \mathbb{Z}\}$, where $x \in G$. It is easy to see that H is closed under the group operation of G, since $x^k \cdot x^\ell = x^{k+\ell}$ for $k, \ell \in \mathbb{Z}$. It is also closed under inverses, since $(x^k)^{-1} = x^{-k}$ is in H for all $k \in \mathbb{Z}$. The identity element $x^0 = 1$ is clearly an element of H. Finally, the group operation of G is associative on G so it must also be associative on H. Therefore, H is a subgroup of G.

28. (a)

$$\begin{aligned}(a_1, b_1)[(a_2, b_2)(a_3, b_3)] &= (a_1, b_1)(a_2 \star a_3, b_2 \diamond b_3) \\ &= (a_1 \star (a_2 \star a_3), b_1 \diamond (b_2 \diamond b_3)) \\ &= ((a_1 \star a_2) \star a_3, (b_1 \diamond b_2) \diamond b_3) \\ &= (a_1 \star a_2, b_1 \diamond b_2)(a_3, b_3) \\ &= [(a_1, b_1)(a_2, b_2)](a_3, b_3)\end{aligned}$$

28. (b) For any element $(a, b) \in A \times B$, we have $(a, b)(1, 1) = (a \star 1, b \diamond 1) = (a, b)$ and similarly for $(1, 1)(a, b)$. Therefore, $(1, 1)$ is the identity.

28. (c) For any element $(a, b) \in A \times B$, we have $(a^{-1}, b^{-1})(a, b) = (a^{-1} \star a, b^{-1} \diamond b) = (1, 1)$ and similarly for $(a, b)(a^{-1}, b^{-1})$. Therefore (a^{-1}, b^{-1}) is the inverse of (a, b).

29. Let $A \times B$ be an abelian group. Then for any $(a_1, b_1), (a_2, b_2) \in A \times B$, we have $(a_1 \star a_2, b_1 \diamond b_2) = (a_1, b_1)(a_2, b_2) = (a_2, b_2)(a_1, b_1) = (a_2 \star a_1, b_2 \diamond b_1)$. Since $a_1 \star a_2 = a_2 \star a_1$ and $b_1 \diamond b_2 = b_2 \diamond b_1$ for any $a_1, a_2 \in A$ and $b_1, b_2 \in B$, both A and B are abelian.

Now suppose both A and B are abelian. Then for any $a_1, a_2 \in A$ and $b_1, b_2 \in B$, we have $a_1 \star a_2 = a_2 \star a_1$ and $b_1 \diamond b_2 = b_2 \diamond b_1$. Now consider any two elements $(a_1, b_1), (a_2, b_2) \in A \times B$. Their product is $(a_1, b_1)(a_2, b_2) = (a_1 \star a_2, b_1 \diamond b_2) = (a_2 \star a_1, b_2 \diamond b_1) = (a_2, b_2)(a_1, b_1)$. Therefore, $A \times B$ is an abelian group.

30. For any two elements of the form $(a, 1)$ and $(1, b)$ in $A \times B$, we have $(a, 1)(1, b) = (a \star 1, 1 \diamond b) = (1 \star a, b \diamond 1) = (1, b)(a, 1)$, so they commute. Furthermore, $(a, 1)(1, b) = (1 \star a, b \diamond 1) = (a, b)$. The order of (a, b) is the smallest positive integer n such that $(a, b)^n = (a, 1)^n (1, b)^n = (a^n, 1)(1, b^n) = (1, 1)$. It follows from the definition of

$|a|$ and $|b|$ that $|a|$ and $|b|$ must divide all integers n satisfying $(a,b)^n = (1,1)$ (see exercise 35 if you are not convinced). The smallest positive integer n such that $|a|$ and $|b|$ both divide n is by definition the least common multiple of $|a|$ and $|b|$. Thus, $|(a,b)|$ is the least common multiple of $|a|$ and $|b|$.

31. Let G be a finite group of even order. Let $t(G) = \{g \in G \mid g \neq g^{-1}\}$. Note that for any element $x \in t(G)$, we necessarily have $x^{-1} \in t(G)$. Pairing each element with its inverse, we find that the order of $t(G)$ must be even. It follows that the order of $G - t(G)$ is also even. Since 1 is its own inverse, it must be in $G - t(G)$, which implies that there exists at least one other element of $G - t(G)$. This element y must be its own inverse as well, meaning $y^2 = 1$ or $|y| = 2$. So, G must contain an element of order 2.

32. Let $x \in G$ and $|x| = n$, for $n < \infty$. Suppose there exist integers $k, \ell < n$ such that $k \neq \ell$ and $x^k = x^\ell$. Assume without loss of generality that $k > \ell$. Then it follows that $x^{k-\ell} = 1$. Since $k - \ell \in \mathbb{Z}^+$ and $k - \ell < n$, this would imply that $|x| \neq n$. This is a contradiction, so the elements $1, x, ..., x^{n-1}$ must be distinct. Since G is a group, all distinct powers of x are elements of G. We may conclude that $|x| \leq |G|$.

33. (a) Let $x \in G$ and $|x| = n$, with $n < \infty$. Suppose that n is odd and that $x^i = x^{-i}$ for some $i \in \{1, 2, ..., n-1\}$. This would mean that $x^{2i} = 1$. By definition of $|x|$, it must be true that $2i \geq n$. It is clear that for x^k to be equal to 1, we must have $n|k$ (see exercise 35 if you are not convinced). Since $2i < 2n$, we require that $2i = n$. But this is impossible because n is odd! Therefore, no such i exists.

33. (b) Let x, n, i be defined as above. Suppose now that $n = 2k$ for some $k \in \mathbb{Z}$, and that there exists $1 \leq i < n$ such that $x^i = x^{-i}$. Then we would have $x^{2i} = 1$ and $2i \geq n$. Since $2i < 2n$, it must be that $2i = n = 2k$ (i.e., $i = k$).

Now suppose that $n = 2k$ and consider $i = k$. $x^{2k} = x^{2i} = 1$ so $x^i = x^{-i}x^{2i} = x^{-i} \cdot 1 = x^{-i}$.

34. Let $|x| = \infty$ for $x \in G$. Suppose that there are two integral powers x^j, x^k of x such that $j \neq k$ but $x^j = x^k$. Assume without loss of generality that $j > k$. Then it must be that $x^{j-k} = 1$. But by definition of $|x|$, since $0 < j - k < \infty$, we would have $|x| \neq \infty$. This is a contradiction, so all powers of x must be distinct.

35. Let $|x| = n$ for $x \in G$ and consider x^k for $k \in \mathbb{Z}$. The division algorithm states that for any $k, n \in \mathbb{Z}$ with $n > 0$, there exist $q, r \in \mathbb{Z}$ such that $k = qn + r$, with

$0 \leq r < n$. Then we may write $x^k = x^{qn+r} = x^{qn}x^r = (x^n)^q x^r = x^r$. Therefore, all integral powers of x are equal to one of the elements of $\{1, x, ..., x^{n-1}\}$.

36. Let $G = \{1, a, b, c\}$ with identity element 1, and assume that G has no elements of order 4. Consider the product ab. Because neither a nor b are the identity, we must have $ab = 1$ or $ab = c$. Suppose $ab = 1$. Then $a^2 \neq 1$ since the cancellation laws would imply that $a = b$. It follows that $|a| = 3$ so that $a^2 = a^2 \cdot ab = a^3 \cdot b = b$. Now consider the product ac. Similarly to ab, we must have $ac = 1$ or $ac = b$. However, $ac \neq 1$ or $b = c$ by the cancellation law, and $ac \neq b$ or $a = c$ by the cancellation law. We must conclude that $ac \notin G$, which is absurd. Therefore, $ab = c$. If $a^2 = b$, then necessarily, $a^3 = 1$. But then $c = ab = a^3 = 1$, so we must have $a^2 = 1$, and thus, $ac = b$. Using similar reasoning, we find that $bc = a$, $b^2 = 1$, $c^2 = 1$. By the proof of exercise 25, G is abelian. This is clearly the only possible structure for G, so the group table is unique.

1.2 Dihedral Groups

1. (a) The six elements of D_6 are $1, r, r^2, s, sr, sr^2$. We have $|r| = |r^2| = 3$, $|1| = 1$, and $|s| = |sr| = |sr^2| = 2$. Note that because $(sr)^2 = 1$ and $(sr^i)^2 = sr^isr^i = sr^{i-1}sr^{-1}r^i = sr^{i-1}sr^{i-1} = (sr^{i-1})^2$ for all positive integers i, $|sr^i| = 2$ for all positive integers i.

1. (b) The eight elements of D_8 are $1, r, r^2, r^3, s, sr, sr^2, sr^3$. We have $|1| = 1$, $|r| = |r^3| = 4$, $|r^2| = 2$, and $|s| = |sr| = |sr^2| = |sr^3| = 2$.

1. (c) The ten elements of D_{10} are $1, r, r^2, r^3, r^4, s, sr, sr^2, sr^3, sr^4$. We have $|1| = 1$, $|r| = |r^2| = |r^3| = |r^4| = 5$, and $|s| = |sr| = |sr^2| = |sr^3| = |sr^4| = 2$.

2. Let x be any element of D_{2n} that is not a power of r. Then $x = sr^k$ for some integer $0 \leq k < n$. Therefore, $rx = rsr^k = sr^{-1}r^k = sr^{k-1} = sr^kr^{-1} = xr^{-1}$.

3. The outline of this proof was given in exercise 1.(a) for my convenience. Elements of D_{2n} that are not powers of r are elements of the form sr^k for $0 \leq k < n$. It is easy to see that $s^2 = (sr)^2 = 1$ using the given relations. Suppose that for all $j < k$, $|sr^j| = 2$. Then we have $(sr^k)^2 = sr^ksr^k = sr^{k-1}rsr^k = sr^{k-1}sr^{-1}r^k = (sr^{k-1})^2 = 1$. Induction on k gives the desired result.

It is also easy to see that s, sr generate D_{2n}, since $s \cdot sr = r$, so that $r^k = (s \cdot sr)^k$ and $sr^k = s(s \cdot sr)^k$ for all integers k.

4. Because $|r| = n$, all powers r^j of r with $0 \leq j < n$ are distinct. It follows that $|r^k| = 2$, since r^k cannot possibly be the identity. It is obvious that z commutes with all powers of r. To see that z commutes with s, note that $(sz)^2 = 1$ by exercise 3. However, $(sz)(zs) = s(zz)s = ss = 1 = (sz)(sz)$, so by the cancellation law, $zs = sz$. From there, it follows that z commutes with all elements sr^j that are not powers of r, since $zsr^j = szr^j = sr^jz$.

It is easy to see that no other distinct power of r commutes with s (except, of course, the identity). It follows from the fact that $r^js = sr^{-j} = sr^{n-j}$, which we can prove by induction. The relation $rs = sr^{-1}$ holds. Suppose that $r^is = sr^{-i}$ for all $i < j$. Then $r^js = r^{j-1}rs = r^{j-1}sr^{-1} = sr^{-j+1}r^{-1} = sr^{-j}$, and by induction on j, we have the claim. Since $j \neq n - j$ unless $j = k$, no other distinct power of r commutes with s. Furthermore, sr^j for any integer j does not commute with r, since $rsr^j = sr^{-1}r^j = sr^{j-1} \neq sr^jr$. Therefore, z is the only non-identity element of D_{2n} that commutes with all others.

5. From exercise 4, we know that elements sr^j never commute with all elements of D_{2n}. Further, for a distinct non-identity power r^j (we can restrict attention to $0 < j < n$) of r to commute with s, we require $2j = n$. Since n is odd, this is impossible and no non-identity power of r commutes with s. It is clear, then, that the only element commuting with all others is the identity, which does so by definition.

6. Let $x, y \in G$ such that $|x| = |y| = 2$. Let $t = xy$. Then note that $(yx)t = yxxy = 1$ so that $t^{-1} = yx$. Thus, $tx = (xy)x = x(yx) = xt^{-1}$.

7. We have already shown that a, b generate D_{2n}. The relation $a^2 = 1$ is identical to $s^2 = 1$ and $(ab)^n = 1$ is the relation $r^n = 1$. From the relations $b^2 = 1$ and $a^2 = 1$, we have $(ab)^{-1} = ba$, so that $a(ab)^{-1} = ab^2(ab)^{-1} = ab^3a = aba$. This is exactly the relation $sr^{-1} = rs$. So the relations for s, r follow from those of a, b. To show the converse, note that if $rs = sr^{-1}$, then $(sr)^2 = srsr = ssr^{-1}r = 1$, which is exactly the equation $b^2 = 1$.

8. The cyclic subgroup generated by r has order n, since there are only n distinct powers of r.

9. Consider two adjacent vertices 1, and 2. There are four positions that 1 can be sent to via rotation. For each of those positions, 2 can be sent to any of three positions. There are thus 12 positions that the adjacent vertices can be sent to and $|G| = 12$.

10. Consider two adjacent vertices 1 and 2. There are 8 positions that 1 can be sent to, and for each of these, there are 3 possible positions that vertex 2 can be sent to, so $|G| = 3 \cdot 8 = 24$.

11. Consider two adjacent vertices 1 and 2. There are 6 positions that 1 can be sent to, and for each of these, there are 4 possible positions that 2 can be sent to, so $|G| = 6 \cdot 4 = 24$.

12. Labeling two adjacent vertices 1 and 2, note that there are 20 positions that we can send 1 to, and for each of these, there are 3 positions that we can send 2 to. Therefore, $|G| = 20 \cdot 3 = 60$.

13. Labeling two adjacent vertices 1 and 2, there are 12 positions that 1 can be sent to, and for each of these, there are 5 possible positions for 2. Therefore, $|G| = 12 \cdot 5 = 60$.

14. As noted earlier in this chapter, $\{1\}$ is a set of generators for $\mathbb{Z}$ under addition.

15. $\{\overline{1}\}$ is a generating set for $\mathbb{Z}/n\mathbb{Z}$ under addition. The generator $\overline{1}$ satisfies the relation $\overline{1}^n = \overline{0}$.

16. If we identify $x_1 = r$ and $y_1 = s$, then $x_1^2 = 1$ is the relation $r^2 = 1$ and $y_1^2 = 1$ is the relation $s^2 = 1$ of D_4. The relation $(x_1y_1)^2 = 1$ allows us to write $x_1y_1x_1y_1 = 1 = x_1y_1y_1x_1$, from which it follows that $x_1y_1 = y_1x_1$. Since $x_1 = x_1^{-1}$, we have $x_1y_1 = y_1x_1^{-1}$, which is the relation $rs = sr^{-1}$ of D_4. It is easy to see that the relations of x_1, y_1 also follow from those of r, s. Hence this group is D_4.

17. (a) Let $n = 3k$. From the relation $xy = yx^2$, we have $x = yx^2y = yxyx^2 = y^2x^4 = x^4$. Thus, $|x| \leq 3$ and since $|y| = 2$, $|G| \leq 6$. If $n = 3k$, there are no further relations satisfied by the powers of x. So, $|x| = 3$ and $|G| = 6$. If we write $x = r$, and $y = s$, we recover the relations $r^3 = s^2 = 1$ of D_6. In addition, the relation $x^3 = x \cdot x^2 = 1$ reveals that $x^2 = x^{-1}$ so that the relation $xy = yx^2$ is the relation $rs = sr^{-1}$ of D_6.

17. (b) If $(3, n) = 1$, then there exist $q, r \in \mathbb{Z}$ with $0 < r < 3$ such that $n = 3q + r$. As before, we have $x^3 = 1$, but now, we also have $x^n = x^{3q}x^r = x^r = 1$. It follows that $x^3 = x^{3-r} = x^r = 1$ and therefore, $x = 1$. There are then only two distinct elements $1, y$ in X_{2n} so $|X_{2n}| = 2$.

18. (a) If $v^3 = 1$, then applying the inverse v^{-1} gives the relation $v^2 = v^{-1}$.

18. (b) The product v^2u^3v may be written $v^2u^3v = v^2u^2 \cdot uv = uv \cdot uv = uv \cdot v^2u^2 = uv^3u^2 = u^3$. Making use of part (a), we have $v^{-1}u^3v = u^3$ or $u^3v = vu^3$.

18. (c) Since $u^4 = 1$, it is easy to see that $u^9 = u$. Applying v, we have $vu^9 = vu$, but since v commutes with u^3, $vu = vu^9 = v \cdot u^3 \cdot u^3 \cdot u^3 = u^3 \cdot v \cdot u^3 \cdot u^3 = u^6 \cdot v \cdot u^3 = u^9v = uv$. So, u commutes with v.

18. (d) $vu = uv = v^2u^2 = vuvu$. The cancellation law then implies that $uv = vu = 1$.

18. (e) Since $u^4 = v^3 = 1$, we have $u^4v^3 = 1$. But, $u^4v^3 = u(uv)^3 = u$, so $u = 1$. If $u = 1$, then $uv = v = 1$. Thus, $Y = \{1\}$.

1.3 Symmetric Groups

1. The cycle decompositions are $\sigma = (1\ 3\ 5)(2\ 4)$, $\tau = (1\ 5)(2\ 3)$, $\sigma^2 = (1\ 5\ 3)$, $\sigma\tau = (2\ 5\ 3\ 4)$, $\tau\sigma = (1\ 2\ 4\ 3)$, $\tau^2\sigma = \sigma = (1\ 3\ 5)(2\ 4)$.

2. The cycle decompositions are $\sigma = (1\ 13\ 5\ 10)(3\ 15\ 8)(4\ 14\ 11\ 7\ 12\ 9)$, $\tau = (1\ 14)(2\ 9\ 15\ 13\ 4)(3\ 10)(5\ 12\ 7)(8\ 11)$, $\sigma^2 = (1\ 5)(3\ 8\ 15)(4\ 11\ 12)(7\ 9\ 14)(10\ 13)$, $\sigma\tau = (1\ 11\ 3)(2\ 4)(5\ 9\ 8\ 7\ 10\ 15)(13\ 14)$, $\tau\sigma = (1\ 4)(2\ 9)(3\ 13\ 12\ 15\ 11\ 5)(8\ 10\ 14)$, $\tau^2\sigma = (1\ 2\ 15\ 8\ 3\ 4\ 14\ 11\ 12\ 13\ 7\ 5\ 10)$.

3. For the permutations of exercise 1, we have $|\sigma| = 6$, $|\tau| = 2$, $|\sigma^2| = 3$, $|\sigma\tau| = 4$, $|\tau\sigma| = 4$, $|\tau^2\sigma| = 6$.

For the permutations of exercise 2, we have $|\sigma| = 12$, $|\tau| = 30$, $|\sigma^2| = 6$, $|\sigma\tau| = 6$, $|\tau\sigma| = 6$, $|\tau^2\sigma| = 13$.

4. (a) Let the elements of S_3 be labeled as they are on pg. 31. Then we have $|\sigma_1| = 1$, $|\sigma_2| = |\sigma_3| = |\sigma_4| = 2$, $|\sigma_5| = |\sigma_6| = 3$.

4. (b) $|1| = 1$, $|(1\ 2)| = |(1\ 3)| = |(1\ 4)| = |(2\ 3)| = |(2\ 4)| = |(3\ 4)| = |(1\ 2)(3\ 4)| = |(1\ 3)(2\ 4)| = |(1\ 4)(2\ 3)| = 2$, $|(1\ 2\ 3)| = |(1\ 3\ 2)| = |(1\ 2\ 4)| = |(1\ 4\ 2)| = |(1\ 3\ 4)| = |(1\ 4\ 3)| = |(2\ 3\ 4)| = |(2\ 4\ 3)| = 3$, $|(1\ 2\ 3\ 4)| = |(1\ 2\ 4\ 3)| = |(1\ 3\ 2\ 4)| = |(1\ 3\ 4\ 2)| = |(1\ 4\ 3\ 2)| = |(1\ 4\ 2\ 3)| = 4$.

5. This permutation is order 30.

6. See exercise 4.(b).

7. See exercise 4.(b).

8. Consider the function $f : \Omega \to S_\Omega$ defined by $f(n) = (1\ n)$, where we define $(1\ 1)$ to be the identity 1. The function f is clearly injective, so $|S_\Omega| \geq |\Omega|$. Since $|\Omega| = \aleph_0$, we have the claim.

9. (a) σ^i is also a 12-cycle when $(i, 12) = 1$.

9. (b) σ^i is also an 8-cycle when $(i, 8) = 1$.

9. (c) σ^i is also a 14-cycle when $(i, 14) = 1$.

10. Let $\sigma = (a_1\ a_2\ ...\ a_m)$. By definition, $\sigma(a_k) = a_{k+1}$, where subscripts are understood to be replaced by their least positive residues mod m from here on. Suppose $\sigma^j(a_k) = a_{k+j}$ for all $j < i$. Then $\sigma^i(a_k) = \sigma(\sigma^{i-1}(a_k)) = \sigma(a_{k+i-1}) = a_{k+i}$. By induction on i, $\sigma^i(a_k) = a_{k+i}$ holds for all i. Note that $a_k = a_{k+i}$ for all k iff $k = k + i \pmod m$. The smallest such i greater than 0 is m, from which we deduce that $|\sigma| = m$.

11. Let $\sigma = (1\ 2\ ...\ m)$. Suppose that $(m, i) = 1$. Then for any integer j, $m|ij$ iff $m|j$. It follows that the $\sigma^{ik}(n) \neq \sigma^{i\ell}(n)$ for any $0 \leq k, \ell < m$ unless $k = \ell$. Otherwise, we would have $m|(k - \ell)$, which is absurd since $|k - \ell| < m$. So, the first m powers of σ^i are distinct and can be used to express the m-cycle $(1\ \sigma^i(1)\ \sigma^{2i}(1)\ ...\ \sigma^{(m-1)i}(1))$, which is exactly σ^i.

Now suppose that σ^i is an m-cycle. Then $|\sigma^i| = |\sigma| = m$, so for any integer j, $m|ij$ iff $m|j$. It follows that $(m, i) = 1$, since otherwise, there would exist j not divisible by m such that $m|ij$.

12. (a) $\tau = \sigma^5$, where $\sigma = (1\ 3\ 5\ 7\ 9\ 2\ 4\ 6\ 8\ 10)$.

12. (b) There is no such σ. First, observe that such a σ must be a 5-cycle, since no power of an n-cycle ρ can fix any element that ρ does not fix unless it is the identity. For if $\rho^k(m) = m + k \pmod n = m$ but $\rho^k(\ell) = \ell + k \pmod n \neq \ell$, the first equation would imply that $n|k$, but the second would imply $n \nmid k$. From the fact that τ is not a 5-cycle, we have the restriction $(5, k) > 1$, and since σ must be a 5-cycle, we need only consider $k < 5$. There is clearly no $k < 5$ satisfying $(5, k) > 1$. So no such σ exists.

13. Consider an element σ of S_n whose cycle decomposition is a product of commuting 2-cycles. Then σ^2 can be written as the product of the squares of 2-cycles. However, since 2-cycles are of order 2, their squares are identity permutations. It follows that σ^2 is the identity and $|\sigma| = 2$.

Now suppose that $|\sigma| = 2$. Then for any element j not fixed by σ, $\sigma^2(j) = j$. For any two elements j, k not fixed by σ, we find that $j = \sigma(k)$ iff $k = \sigma(j)$. Otherwise, we would have $\sigma^2(j) \neq j$ or $\sigma^2(k) \neq k$, which would mean that $|\sigma| \neq 2$. Thus, the set of 2-cycles $\{(j\ \sigma(j)) \mid \sigma(j) \neq j\}$ has elements that are pairwise disjoint. Clearly, the product of all elements in this set acts identically to σ, so σ is a product of disjoint 2-cycles.

14. Let p be a prime, and $\sigma \in S_n$ be such that σ is a product of commuting p-cycles. Then σ^p is a product of p^{th} powers of p-cycles. But the p^{th} power of a

p-cycle is the identity and no lower power of a p-cycle yields the identity. Hence, σ^p is the identity and $|\sigma| = p$.

Now suppose that $|\sigma| = p$. Then for all j not fixed by σ, $\sigma^p(j) = j$. Furthermore, there is no $k < p$ such that $\sigma^k(j) = j$. Assuming otherwise, and letting k be the smallest positive integer such that $\sigma^k(j) = j$, we would arrive at the conclusion that $k|p$. But p is prime so this is impossible. Therefore, for any j such that $\sigma(j) \neq j$, we can construct the p-cycle $(j\ \sigma(j)\ \sigma^2(j)\ ...\ \sigma^{p-1}(j))$, which describes how σ acts on j. Note that if two elements j, k exist such that $\sigma^\alpha(j) = \sigma^\beta(k)$, then j, k belong to the same cycle. Assuming without loss of generality that $\alpha > \beta$, this is because $\sigma^\alpha(j) = \sigma^\beta(k)$ implies that $\sigma^{\alpha-\beta}(j) = k$. Writing j's p-cycle so that it starts at $\sigma^{\alpha-\beta}(j) = k$, we see that their p-cycles are identical. Therefore, the elements of $\{(j\ \sigma(j)\ \sigma^2(j)\ ...\ \sigma^{p-1}(j) \mid \sigma(j) \neq j\}$ are pairwise disjoint. The product of all elements in this set acts identically to σ, so σ is the product of disjoint p-cycles.

If p is not prime, this is not necessarily true. $\tau = (1\ 2)(3\ 4\ 5)$ is of order 6, yet it is not a product of disjoint 6-cycles.

15. Let $\sigma \in S_n$ and let $\sigma_1, ..., \sigma_m$ be the component cycles of its cycle decomposition so that $\sigma = \sigma_1\sigma_2...\sigma_m$. We know from exercise 10 that if σ_i is an ℓ_i-cycle, then $|\sigma_i| = \ell_i$. It follows that each of the ℓ_i must divide $|\sigma|$. By definition, $|\sigma|$ must be the smallest positive integer such that this is true. Since the lcm of $\ell_1, ...\ell_m$ is by definition the smallest positive integer such that it is divisible by all the ℓ_i, it is equal to $|\sigma|$.

16. There are $n(n-1)...(n-m+1)$ ways to select an ordering of m elements to write as an m-cycle. However, any given m-cycle may be written using m different orderings (related by cyclic permutation) of the m elements it permutes. Thus, the total number of m-cycles in S_n is $n(n-1)...(n-m+1)/m$

17. There are $n(n-1)(n-2)(n-3)$ ways to select an ordering of 4 elements to write as two 2-cycles. However, each of the 2-cycles may be written 2 different ways, and the cycles are disjoint so they may be written in either order. Each product of 2-cycles may thus be written 8 different ways. The number of elements of S_n that are products of two disjoint 2-cycles is therefore $n(n-1)(n-2)(n-3)/8$.

18. S_5 contains cycles of length $1, 2, ..., 5$ along with their products. The only new n added by these products is 6, which comes from the product of a 2-cycle and 3-cycle.

19. Similarly to the previous exercise, $1, 2, ..., 7$ are possible since S_7 contains cycles of all those lengths. In addition, $|(1\ 2)(3\ 4\ 5\ 6\ 7)| = 10$ and $|(1\ 2\ 3)(4\ 5\ 6\ 7)| = 12$, so n can take on the values $1, 2, 3, 4, 5, 6, 7, 10, 12$.

20. Let $r = (1\ 2)$, and $s = (1\ 3)$. Then $T = \{r, s\}$ is a set of generators of S_3. To see this, observe that $rs = (1\ 3\ 2)$, $sr = (1\ 2\ 3)$, $r^2 = 1$, and $rsr = (2\ 3)$. They satisfy the relations $r^2 = s^2 = 1$, and $rs = (sr)^2$. These relations allow us to easily reduce any element of S_3 to a product of at most three r's and s's, allowing us to determine exactly when two elements of S_3 are equal.

1.4 Matrix Groups

1. There cannot be more than two zero entries in an element of $GL_2(\mathbb{F}_2)$, for such matrices are not invertible. Therefore, there are only two "free" entries for an element of $GL_2(\mathbb{F}_2)$. Furthermore, there must be at least one zero entry in an element of $GL_2(\mathbb{F}_2)$, because otherwise the matrix is not invertible. All four possible matrices with exactly one zero entry, and only two matrices with two zero entries are invertible. So, $|GL_2(\mathbb{F}_2)| = 6$.

2. The elements are

$$a_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \; a_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \; a_3 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

$$a_4 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \; a_5 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; a_6 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$$

The orders of these elements are $|a_1| = 1$, $|a_2| = |a_4| = |a_5| = 2$, $|a_3| = |a_6| = 3$.

3. We have $a_5 a_3 = a_4$ but $a_3 a_5 = a_2$. So $GL_2(\mathbb{F}_2)$ is non-abelian.

4. Consider the set $\mathbb{Z}/n\mathbb{Z}$ for n not a prime. Then there exist positive integers a, b such that $n = ab$ and $a, b > 1$. Suppose there exists a multiplicative inverse $\overline{c}$ of $\overline{a}$. Then it must be true that $ac = qn + 1$ for some $q \in \mathbb{Z}$. However, $n = ab$ so $ac = qn + 1 = qab + 1$ from which it follows that $a(c - qb) = 1$. This is impossible because $a > 1$! So $\overline{a}$ has no inverse in $\mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z} - \{0\}, \cdot)$ is not a group. We must conclude that $\mathbb{Z}/n\mathbb{Z}$ is not a field for n not prime.

5. Suppose that F is a field of finite order m. Then an $n \times n$ matrix taking its entries from F has m possible choices for each of its n^2 entries. So, there are exactly m^{n^2} different $n \times n$ matrices taking elements from F, and at least one of these is not invertible (the matrix of all zeros, for example). It follows that $|GL_n(F)| < m^{n^2}$ and $GL_n(F)$ is therefore a finite group.

Now let $GL_n(F)$ be a finite group, and assume that F has infinitely many elements. Then there can only be finitely many invertible $n \times n$ matrices taking elements from F. Because F is a field, every element $x \in F$ has a multiplicative inverse $x^{-1} \in F$. But from every element $x \in F$, we can construct the matrix xI_n, where I_n is the identity matrix. This matrix clearly has an inverse $x^{-1}I_n$ and so is an element of $GL_n(F)$. Since there are infinitely many such matrices, $GL_n(F)$ must be an infinite group. This is a contradiction, so F must have a finite number of elements.

6. Let $|F| = q$. Then each entry of an $n \times n$ matrix can take any of q possible values. There are n^2 entries in an $n \times n$ matrix, so there are q^{n^2} different $n \times n$ matrices taking entries from F. However the zero matrix with all entries the additive identity of F is not invertible. There are thus strictly less than q^{n^2} invertible $n \times n$ matrices taking entries from F and therefore, $|GL_n(F)| < q^{n^2}$.

7. As described in exercise 6, there are p^4 different 2×2 matrices taking entries from $\mathbb{F}_p$. Remembering that a 2×2 matrix is not invertible iff one of its rows is a multiple of the other, we simply have to count the number of such matrices. First, consider matrices of the form

$$\begin{pmatrix} a & b \\ ca & cb \end{pmatrix}$$

Counting only those matrices such that a and b are not both zero, we find that there are $p(p^2-1)$ such matrices, since we are excluding one of the p^2 sets of values that a and b can take, and c can also take on p different values. Now, counting matrices of the form

$$\begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix}$$

it is easy to see that there are p^2 such matrices. Thus, there are $p(p^2-1) + p^2 = p^3 + p^2 - p$ non-invertible 2×2 matrices. It follows that $|GL_n(\mathbb{F}_p)| = p^4 - p^3 - p^2 + p$.

8. Let A be the $n \times n$ antidiagonal matrix with all non-zero entries equal to 1, and let B be the matrix constructed by changing the $(n-1, 1)$ entry of A to 1. It's easy to see that for any matrix M, AM simply reverses the order of the rows of M, while MA reverses the order of the columns of M. Then the $(AB)_{2,1} = 1$ but $(BA)_{2,1} = 0$, so $AB \neq BA$. A is an element of $GL_n(F)$, since $A^2 = I$, and B is also an element of $GL_n(F)$, since the matrix C constructed by changing the $(2, n)$ entry of A to -1 satisfies $BC = CB = I$. We can construct such matrices for all fields F because F by definition must have an additive identity 0 and a multiplicative identity 1. F must also contain the additive inverse -1 because it is an abelian group under $+$. Therefore, for any $n \geq 2$ and any F, $GL_n(F)$ is non-abelian.

9. Define matrices A, B, C as follows

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix},\ B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix},\ C = \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix}$$

Then the following holds

$$\begin{aligned}
A(BC) &= \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} \begin{pmatrix} b_1c_1 + b_2c_3 & b_1c_2 + b_2c_4 \\ b_3c_1 + b_4c_3 & b_3c_2 + b_4c_4 \end{pmatrix} \\
&= \begin{pmatrix} a_1(b_1c_1 + b_2c_3) + a_2(b_3c_1 + b_4c_3) & a_1(b_1c_2 + b_2c_4) + a_2(b_3c_2 + b_4c_4) \\ a_3(b_1c_1 + b_2c_3) + a_4(b_3c_1 + b_4c_3) & a_3(b_1c_2 + b_2c_4) + a_4(b_3c_2 + b_4c_4) \end{pmatrix} \\
&= \begin{pmatrix} (a_1b_1 + a_2b_3)c_1 + (a_1b_2 + a_2b_4)c_3 & (a_1b_1 + a_2b_3)c_2 + (a_1b_2 + a_2b_4)c_4 \\ (a_3b_1 + a_4b_3)c_1 + (a_3b_2 + a_4b_4)c_3 & (a_3b_1 + a_4b_3)c_2 + (a_3b_2 + a_4b_4)C_4 \end{pmatrix} \\
&= \begin{pmatrix} a_1b_1 + a_2b_3 & a_1b_2 + a_2b_4 \\ a_3b_1 + a_4b_3 & a_3b_2 + a_4b_4 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & c_4 \end{pmatrix} \\
&= (AB)C
\end{aligned}$$

So matrix multiplication of 2×2 matrices with entries in $\mathbb{R}$ is associative.

10. (a) The product is

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}$$

Since $a_1, a_2 \neq 0$ and $c_1, c_2 \neq 0$ for any elements of G, $a_1a_2 \neq 0$ and $c_1c_2 \neq 0$. Therefore, the product of any two elements of G is also an element of G.

10. (b) The matrix inverse must satisfy

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} d & e \\ f & g \end{pmatrix} = \begin{pmatrix} ad + bf & ae + bg \\ cf & cg \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Immediately, we find that $f = 0$, $g = c^{-1}$, and $d = a^{-1}$. Since $ae = -bg = -bc^{-1}$, we have $e = -b(ac)^{-1}$ and the inverse is

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -b(ac)^{-1} \\ 0 & c^{-1} \end{pmatrix}$$

The inverse is clearly an element of G, since if $a, c \neq 0$, then $a^{-1}, c^{-1} \neq 0$.

10. (c) The identity is clearly an element of G, and from exercise 9, the binary operation of G is associative. Every element of G is obviously also an element of $GL_2(\mathbb{R})$, since G contains only invertible 2×2 real matrices. These properties along with those shown in exercises $10.(a)$ and $10.(b)$ allow us to conclude that G is a subgroup of $GL_2(\mathbb{R})$.

10. (d) Let us call this set H. Clearly, the identity I is in H. Furthermore, H is closed under matrix multiplication since

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \begin{pmatrix} c & d \\ 0 & c \end{pmatrix} = \begin{pmatrix} ac & ad+bc \\ 0 & ac \end{pmatrix}$$

Every element of H is also an element of G, so from exercise $10.(b)$, the inverse takes the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} a^{-1} & -ba^{-2} \\ 0 & a^{-1} \end{pmatrix}$$

So H is closed under inverses. Again, matrix multiplication for 2×2 real matrices is associative from exercise 9, and all elements of H are clearly elements of $GL_2(\mathbb{R})$. Thus, H is also a subgroup of $GL_2(\mathbb{R})$.

11. (a) The product is

$$XY = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & d & e \\ 0 & 1 & f \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & d+a & e+af+b \\ 0 & 1 & f+c \\ 0 & 0 & 1 \end{pmatrix}$$

So H is closed under matrix multiplication. Let X and Y now be the matrices

$$X = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 4 \\ 0 & 0 & 1 \end{pmatrix}, \; Y = \begin{pmatrix} 1 & 4 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

Then we have

$$XY = \begin{pmatrix} 1 & 6 & 10 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 6 & 22 \\ 0 & 1 & 6 \\ 0 & 0 & 1 \end{pmatrix} = YX$$

So H must be non-abelian.

11. (b) The inverse must satisfy

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} d & e & f \\ g & h & i \\ j & k & l \end{pmatrix} = \begin{pmatrix} d+ag+bj & e+ah+bk & f+ai+bl \\ g+cj & h+ck & i+cl \\ j & k & l \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We see immediately that $j = k = 0$ and $l = 1$, allowing us to simplify the form of the product to

$$\begin{pmatrix} d+ag & e+ah & f+ai+b \\ g & h & i+c \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

giving the results $g = 0$, $h = 1$, and $i = -c$. It follows that $d = 1$, $e = -a$, and $f = ac - b$. The inverse is therefore

$$\begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a & ac-b \\ 0 & 1 & -c \\ 0 & 0 & 1 \end{pmatrix}$$

The inverse is clearly an element of $H(F)$, so $H(F)$ is closed under inverses.

11. (c) Let $A, B, C \in H(F)$ be written as follows

$$A = \begin{pmatrix} 1 & a_1 & a_2 \\ 0 & 1 & a_3 \\ 0 & 0 & 1 \end{pmatrix},\ B = \begin{pmatrix} 1 & b_1 & b_2 \\ 0 & 1 & b_3 \\ 0 & 0 & 1 \end{pmatrix},\ C = \begin{pmatrix} 1 & c_1 & c_2 \\ 0 & 1 & c_3 \\ 0 & 0 & 1 \end{pmatrix}$$

Then the following is true

$$\begin{aligned} A(BC) &= \begin{pmatrix} 1 & a_1 & a_2 \\ 0 & 1 & a_3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_1+c_1 & b_2+c_2+b_1c_3 \\ 0 & 1 & b_3+c_3 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a_1+b_1+c_1 & a_2+b_2+c_2+b_1c_3+a_1(b_3+c_3) \\ 0 & 1 & a_3+b_3+c_3 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a_1+b_1+c_1 & a_2+b_2+c_2+a_1b_3+(a_1+b_1)c_3 \\ 0 & 1 & a_3+b_3+c_3 \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & a_1+b_1 & a_2+b_2+a_1b_3 \\ 0 & 1 & a_3+b_3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & c_1 & c_2 \\ 0 & 1 & c_3 \\ 0 & 0 & 1 \end{pmatrix} \\ &= (AB)C \end{aligned}$$

So the group operation of $H(F)$ is associative. Note that there are only three "free" entries for an element of $H(F)$, each of which can take any one of $|F|$ values. This implies that $|H(F)| = |F|^3$.

11. (d) Label the elements of $H(\mathbb{Z}/2\mathbb{Z})$ as follows

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \Lambda_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \Lambda_2 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \Lambda_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\Lambda_4 = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},\ \Lambda_5 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix},\ \Lambda_6 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},\ \Lambda_7 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Their orders are $|I| = 1$, $|\Lambda_1| = |\Lambda_2| = |\Lambda_3| = |\Lambda_4| = |\Lambda_6| = 2$, $|\Lambda_5| = |\Lambda_7| = 4$.

11. (e) Let A be any non-identity element of $H(\mathbb{R})$ and suppose $|A| = n$, for $n \in \mathbb{Z}^+$. Then $A^n = I$, which implies that $A^{n-1} = A^{-1}$. As we saw in exercise 11.(b),

$$\begin{pmatrix} 1 & A_{1,2} & A_{1,3} \\ 0 & 1 & A_{2,3} \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -A_{1,2} & A_{1,2}A_{2,3} - A_{1,3} \\ 0 & 1 & -A_{2,3} \\ 0 & 0 & 1 \end{pmatrix}$$

Now we prove that A^m takes the form

$$A^m = \begin{pmatrix} 1 & mA_{1,2} & mA_{1,3} + \frac{m(m-1)}{2}A_{1,2}A_{2,3} \\ 0 & 1 & mA_{2,3} \\ 0 & 0 & 1 \end{pmatrix}$$

The equation holds for $m = 2$, since a simple application of the result of exercise 11.(a) yields

$$A^2 = \begin{pmatrix} 1 & 2A_{1,2} & 2A_{1,3} + A_{1,2}A_{2,3} \\ 0 & 1 & 2A_{2,3} \\ 0 & 0 & 1 \end{pmatrix}$$

Now, suppose it holds for all $k < m$, and consider A^m. We have

$$\begin{aligned} A^m &= A^{m-1}A \\ &= \begin{pmatrix} 1 & (m-1)A_{1,2} & (m-1)A_{1,3} + \frac{(m-1)(m-2)}{2}A_{1,2}A_{2,3} \\ 0 & 1 & (m-1)A_{2,3} \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & A_{1,2} & A_{1,3} \\ 0 & 1 & A_{2,3} \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & (m-1)A_{1,2} + A_{1,2} & (m-1)A_{1,3} + \frac{(m-1)(m-2)}{2}A_{1,2}A_{2,3} + A_{1,3} + (m-1)A_{1,2}A_{2,3} \\ 0 & 1 & (m-1)A_{2,3} + A_{2,3} \\ 0 & 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & mA_{1,2} & mA_{1,3} + \frac{m(m-1)}{2}A_{1,2}A_{2,3} \\ 0 & 1 & mA_{2,3} \\ 0 & 0 & 1 \end{pmatrix} \end{aligned}$$

and by induction on m, the equation holds for all $m \in \mathbb{Z}^+$. Observing that A^{n-1} cannot possibly be equal to A^{-1} unless $A_{1,2} = A_{1,3} = A_{2,3} = 0$, we find that we have arrived at a contradiction. It must be that every non-identity element of $H(\mathbb{R})$ has infinite order.

1.5 The Quaternion Group

1. The orders are $|1| = 1$, $|-1| = 2$, $|i| = |j| = |k| = |-i| = |-j| = |-k| = 4$.

2. For S_3, using the labels given on page 31 of the text, we have

$$\begin{pmatrix} \sigma_1 & \sigma_2 & \sigma_3 & \sigma_4 & \sigma_5 & \sigma_6 \\ \sigma_2 & \sigma_1 & \sigma_5 & \sigma_6 & \sigma_3 & \sigma_4 \\ \sigma_3 & \sigma_6 & \sigma_1 & \sigma_5 & \sigma_4 & \sigma_2 \\ \sigma_4 & \sigma_5 & \sigma_6 & \sigma_1 & \sigma_2 & \sigma_3 \\ \sigma_5 & \sigma_4 & \sigma_2 & \sigma_3 & \sigma_6 & \sigma_1 \\ \sigma_6 & \sigma_3 & \sigma_4 & \sigma_2 & \sigma_1 & \sigma_5 \end{pmatrix}$$

For D_8, we have

$$\begin{pmatrix} 1 & r & r^2 & r^3 & s & sr & sr^2 & sr^3 \\ r & r^2 & r^3 & 1 & sr^3 & s & sr & sr^2 \\ r^2 & r^3 & 1 & r & sr^2 & sr^3 & s & sr \\ r^3 & 1 & r & r^2 & sr & sr^2 & sr^3 & s \\ s & sr & sr^2 & sr^3 & 1 & r & r^2 & r^3 \\ sr & sr^2 & sr^3 & s & r^3 & 1 & r & r^2 \\ sr^2 & sr^3 & s & sr & r^2 & r^3 & 1 & r \\ sr^3 & s & sr & sr^2 & r & r^2 & r^3 & 1 \end{pmatrix}$$

Finally, for Q_8, we have

$$\begin{pmatrix} 1 & -1 & i & -i & j & -j & k & -k \\ -1 & 1 & -i & i & -j & j & -k & k \\ i & -i & -1 & 1 & k & -k & -j & j \\ -i & i & 1 & -1 & -k & k & j & -j \\ j & -j & -k & k & -1 & 1 & i & -i \\ -j & j & k & -k & 1 & -1 & -i & i \\ k & -k & j & -j & -i & i & -1 & 1 \\ -k & k & -j & j & i & -i & 1 & -1 \end{pmatrix}$$

3. It is easy to see that i, j generate Q_8. They satisfy the relations $i^2 = j^2$, $i^4 = 1$, and $ij = -ji$.

1.6 Homomorphisms and Isomorphisms

1. (a) This equation holds for $n = 2$ by definition of a group homomorphism. Suppose now that it holds for all $k < n$. Then for $\varphi(x^n)$ we have $\varphi(x^n) = \varphi(x^{n-1}x) = \varphi(x^{n-1})\varphi(x) = \varphi(x)^{n-1}\varphi(x) = \varphi(x)^n$. By induction on n, we find that the claim is true.

1. (b) First, we handle $\varphi(x^0) = \varphi(1)$. Let $e \in H$ be the identity of H. Then we have $e\varphi(1) = \varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$. Multiplying by $\varphi(1)^{-1}$, we obtain $e = \varphi(1)$ or $\varphi(x)^0 = \varphi(x^0)$. Now, we consider φ applied to powers of x^{-1}. Since φ is a homomorphism, we have $\varphi(1) = \varphi(x^{-1}x) = \varphi(x^{-1})\varphi(x)$. This implies that $\varphi(x^{-1}) = \varphi(x)^{-1}$. Applying the proof of part (a) to x^{-1}, we find that $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$.

2. From the results of exercise 1, we have $\varphi(x^n) = \varphi(x)^n$ for all $n \in \mathbb{Z}$. So, assuming $|x|$ is finite, $\varphi(1) = \varphi(x^{|x|}) = \varphi(x)^{|x|}$, meaning $|\varphi(x)| \leq |x|$. Similarly, assuming $|\varphi(x)|$ is finite, we have $\varphi(x^{|\varphi(x)|}) = \varphi(x)^{|\varphi(x)|} = \varphi(1)$. Since φ is an isomorphism, this implies that $x^{|\varphi(x)|} = 1$, so $|\varphi(x)| \geq |x|$. It follows that $|x|$ is finite iff $|\varphi(x)|$ is finite, and that $|\varphi(x)| = |x|$. Because φ is a bijection, the two groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. This is not necessarily true if φ is merely a homomorphism, since a homomorphism is not necessarily injective.

3. Suppose G is abelian. Since φ is a bijection, for every element $h \in H$, there exists $g \in G$ such that $h = \varphi(g)$. Then consider any two elements $h_1, h_2 \in H$ and let $g_1, g_2 \in G$ be such that $h_1 = \varphi(g_1)$ and $h_2 = \varphi(g_2)$. We have $h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2) = \varphi(g_2g_1) = \varphi(g_2)\varphi(g_1) = h_2h_1$. So H is abelian. If φ is assumed to only be a homomorphism, then we require that φ also be a surjection for this proof to work.

Now suppose that H is abelian. Then for any $g_1, g_2 \in G$, we have $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \varphi(g_2)\varphi(g_1) = \varphi(g_2g_1)$. Since φ is an isomorphism, this implies that $g_1g_2 = g_2g_1$, so G is abelian.

4. $\mathbb{R} - \{0\}$ cannot be isomorphic to $\mathbb{C} - \{0\}$ because the former has no elements of order 3, while the latter has two elements of order 3.

5. Suppose there exists an isomorphism $\varphi : \mathbb{Q} \to \mathbb{R}$. Then there must be $q_1, q_2 \in \mathbb{Q}$ such that $\varphi(q_1) = \sqrt{2}$ and $\varphi(q_2) = 2$. Let n_1, n_2, k_1, k_2 be integers such that $(n_i, k_i) = 1$ and $q_i = \frac{k_i}{n_i}$. Then $k_1\varphi(1) = \varphi(k_1) = \varphi(q_1n_1) = n_1\varphi(q_1) = n_1\sqrt{2}$ and

$k_2\varphi(1) = \varphi(k_2) = \varphi(q_2n_2) = n_2\varphi(q_2) = 2n_2$. It follows that $\sqrt{2} = \frac{k_2n_1}{k_1n_2}$, which is absurd! Thus, $\mathbb{Q}$ cannot be isomorphic to $\mathbb{R}$.

6. Suppose there exists an isomorphism $\varphi : \mathbb{Z} \to \mathbb{Q}$. Then there must be $z \in \mathbb{Z}$ such that $\varphi(z) = \frac{1}{2}\varphi(1)$. But $\varphi(z) = z\varphi(1)$, which implies that $z = \frac{1}{2}$. This is absurd, so $\mathbb{Z}$ cannot be isomorphic to $\mathbb{Q}$.

7. Q_8 has one element of order 2, while D_8 has five such elements. Thus, they cannot be isomorphic.

8. If $n \neq m$, then $|S_n| = n! \neq m! = |S_m|$. Then there cannot exist a bijection $\varphi : S_m \to S_n$, so S_m and S_n cannot be isomorphic.

9. S_4 has 9 elements of order 2, whereas D_{24} has 13 such elements. Therefore, they cannot be isomorphic.

10. (a) Let $\sigma : \Delta \to \Delta$ be a permutation. We must show that $\varphi(\sigma)$ is a bijection from Ω to itself. It is obvious from the fact that $\theta : \Delta \to \Omega$ and $\sigma : \Delta \to \Delta$ that $\theta \circ \sigma \circ \theta^{-1}$ is a map from Ω to itself. Let a, b be any two elements of Ω. If $a \neq b$, then $\theta^{-1}(a) \neq \theta^{-1}(b)$ because θ^{-1} is a bijection. For the same reason, $\sigma(\theta^{-1}(a)) \neq \sigma(\theta^{-1}(b))$ and $\theta(\sigma(\theta^{-1}(a))) \neq \theta(\sigma(\theta^{-1}(b)))$. Therefore, $\theta \circ \sigma \circ \theta^{-1}$ is a bijection from Ω to itself (i.e., it is a permutation of Ω).

10. (b) Define $\varphi^{-1} : S_\Omega \to S_\Delta$ by $\varphi^{-1}(\tau) = \theta^{-1} \circ \tau \circ \theta$ for all $\tau \in S_\Omega$. Then for any $\sigma \in S_\Delta$, we have $\varphi^{-1}(\varphi(\sigma)) = \theta^{-1} \circ \varphi(\sigma) \circ \theta = \theta^{-1} \circ \theta \circ \sigma \circ \theta^{-1} \circ \theta = \sigma$. Similarly, for any $\tau \in S_\Omega$, we have $\varphi(\varphi^{-1}(\tau)) = \theta \circ \varphi^{-1}(\tau) \circ \theta^{-1} = \theta \circ \theta^{-1} \circ \tau \circ \theta \circ \theta^{-1} = \tau$. φ^{-1} is clearly the inverse of φ, so φ must be a bijection from $S_\Delta \to S_\Omega$.

10. (c) Simply observe that $\varphi(\sigma \circ \tau) = \theta \circ \sigma \circ \tau \circ \theta^{-1} = \theta \circ \sigma \circ \theta^{-1} \circ \theta \circ \tau \circ \theta^{-1} = \varphi(\sigma) \circ \varphi(\tau)$. Thus, φ is a homomorphism.

11. Define $\varphi : A \times B \to B \times A$ by $\varphi((a, b)) = (b, a)$ for all $(a, b) \in A \times B$. We will prove that φ is an isomorphism. First, we prove that φ is a surjection. For any element $(b, a) \in B \times A$, we have $b \in B$ and $a \in A$, so (a, b) is necessarily an element of $A \times B$. Since $\varphi((a, b)) = (b, a)$, for every element (b, a) of $B \times A$, there exists an element (a, b) of $A \times B$ such that $\varphi((a, b)) = (b, a)$. Next, we prove that φ is also an injection. Let $(a_1, b_1), (a_2, b_2) \in A \times B$ be such that $(a_1, b_1) \neq (a_2, b_2)$. Then necessarily, $a_1 \neq a_2$ or $b_1 \neq b_2$, and it follows that $(b_1, a_1) \neq (b_2, a_2)$. All that remains is to prove that φ is a homomorphism. Since $\varphi((a_1, b_1)(a_2, b_2)) = \varphi((a_1a_2, b_1b_2)) = (b_1b_2, a_1a_2) = (b_1, a_1)(b_2, a_2) = \varphi((a_1, b_1))\varphi((a_2, b_2))$, φ must be a homomorphism. Thus, $A \times B \cong B \times A$.

12. Define $\varphi : G \times C \to A \times H$ by $\varphi(((a,b),c)) = (a,(b,c))$ for all $((a,b),c) \in G \times C$. The proof that φ is an isomorphism is almost identical to the one presented in exercise 11. Since φ is an isomorphism, it follows that $G \times C \cong A \times H$.

13. Let 1_G be the identity of G and 1_H be the identity of H. From exercise 1, we know that $\varphi(1_G) = 1_H$, so $\varphi(G)$ contains the identity element. Since $\varphi(G) \subseteq H$, the group operation of H must be associative on $\varphi(G)$ as well. By the definition of a homomorphism, for any two elements $\varphi(g_1), \varphi(g_2) \in \varphi(G)$, their product $\varphi(g_1)\varphi(g_2) = \varphi(g_1 g_2)$ is also an element of $\varphi(G)$. Finally, for any $\varphi(g) \in \varphi(G)$, its inverse $\varphi(g)^{-1} = \varphi(g^{-1})$ is an element of $\varphi(G)$. Thus, $\varphi(G)$ is a subgroup of H.

Now suppose that φ is injective. By definition, for every $h \in \varphi(G)$, there exists $g \in G$ such that $\varphi(g) = h$. Then the map $\psi : G \to \varphi(G)$ defined as $\psi(g) = \varphi(g)$ for all $g \in G$ is an injection, a surjection, and a homomorphism. It follows that $G \cong \varphi(G)$.

14. Let 1_G be the identity of G and $K_\varphi = \{g \in G \mid \varphi(g) = 1_H\}$. As shown in exercise 1, 1_G is always an element of K_φ, so the kernel contains the identity element. Because the group operation of G is associative and K_φ is a subset of G, it must also be associative on K_φ. Consider the product $g_1 g_2$ of any two elements $g_1, g_2 \in K_\varphi$. We have $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = 1_H 1_H = 1_H$, so K_φ is closed under the group operation. Finally, for any $g \in K_\varphi$, we have $1_H = \varphi(1_G) = \varphi(g^{-1}g) = \varphi(g^{-1})\varphi(g) = \varphi(g^{-1})$, so $g^{-1} \in K_\varphi$. Therefore, K_φ is a subgroup of G.

Now we prove that φ is injective iff K_φ is the identity subgroup of G. If φ is injective, then $g_1 \neq g_2$ implies that $\varphi(g_1) \neq \varphi(g_2)$. Thus, for any element $g \in G$ such that $g \neq 1_G$, we have $\varphi(g) \neq 1_H$. Then K_φ must be the identity subgroup of G. If K_φ is the identity subgroup, then for any $g \in G$ such that $g \neq 1_G$, $\varphi(g) \neq 1_H$. Suppose that there exists $g_1, g_2 \in G$ such that $g_1 \neq g_2$ but $\varphi(g_1) = \varphi(g_2)$. Then $\varphi(g_1)\varphi(g_2)^{-1} = 1_H$. But $\varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1 g_2^{-1})$. Since $g_1 \neq g_2$, $g_1 g_2^{-1} \neq 1_G$, so this implies that there is another element $g_1 g_2^{-1} \neq 1_G$ in K_φ. We have a contradiction, so there are no such $g_1, g_2 \in G$ and φ is injective.

15. For any $(x_1, y_1), (x_2, y_2) \in \mathbb{R}^2$, we have $\pi((x_1, y_1) + (x_2, y_2)) = \pi((x_1 + x_2, y_1 + y_2)) = x_1 + x_2 = \pi((x_1, y_1)) + \pi((x_2, y_2))$ so π is a homomorphism. The kernel of π is clearly $\{(x, y) \in \mathbb{R}^2 \mid x = 0\}$.

16. For any $(a_1, b_1), (a_2, b_2) \in G$, we have $\pi_1((a_1, b_1)(a_2, b_2)) = \pi_1((a_1 a_2, b_1 b_2)) = a_1 a_2 = \pi_1((a_1, b_1))\pi_1((a_2, b_2))$ and $\pi_2((a_1, b_1)(a_2, b_2)) = \pi_2((a_1 a_2, b_1 b_2)) = b_1 b_2 = \pi_2((a_1, b_1))\pi_2((a_2, b_2))$, so π_1, π_2 are homomorphisms. The kernel of π_1 is $\{(a, b) \in G \mid a = 1_A\}$, while the kernel of π_2 is $\{(a, b) \in G \mid b = 1_B\}$.

17. Define the map $\varphi : G \to G$ by $\varphi(g) = g^{-1}$ for all $g \in G$. If φ is a homomorphism, then for any $g_1, g_2 \in G$, we have $g_2^{-1}g_1^{-1} = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = g_1^{-1}g_2^{-1}$. Left-multiplying by g_1g_2 and right-multiplying by g_2g_1, we have $g_2g_1 = g_1g_2$. So, G is abelian.

If G is abelian, then for any $g_1, g_2 \in G$, we have $g_1g_2 = g_2g_1$. Then $\varphi(g_1g_2) = \varphi(g_2g_1) = g_1^{-1}g_2^{-1} = \varphi(g_1)\varphi(g_2)$, so φ is a homomorphism.

18. Define the map $\varphi : G \to G$ by $\varphi(g) = g^2$ for all $g \in G$. If φ is a homomorphism, then for any $g_1, g_2 \in G$, we have $(g_1g_2)^2 = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = g_1^2g_2^2$. Left-multiplying by g_1^{-1} and right-multiplying by g_2^{-1}, we find that $g_2g_1 = g_1g_2$. So, G is abelian.

If G is abelian, then for any $g_1, g_2 \in G$, we have $g_1g_2 = g_2g_1$. Then $\varphi(g_1g_2) = g_1g_2g_1g_2 = g_1^2g_2^2 = \varphi(g_1)\varphi(g_2)$ so φ is a homomorphism.

19. Define the map $\varphi : G \to G$ by $\varphi(z) = z^k$ (for fixed $k \in \mathbb{Z}^+$) for all $z \in G$. Let z_1, z_2 be any two elements of G. Noting that $\mathbb{C} - \{0\}$ is an abelian group under multiplication, we have $\varphi(z_1z_2) = (z_1z_2)^k = z_1^kz_2^k = \varphi(z_1)\varphi(z_2)$, so φ is a homomorphism. Let z be any element of G, and let $n \in \mathbb{Z}^+$ be such that $z^n = 1$. The element $z^{1/k}$ is also an element of G, since $(z^{1/k})^{nk} = z^n = 1$ and $nk \in \mathbb{Z}^+$. In addition, $\varphi(z^{1/k}) = z$, so φ is surjective. Note that φ is not injective, since its kernel contains other elements besides the identity.

20. Define the map $\mathrm{id} : G \to G$ by $\mathrm{id}(g) = g$ for all $g \in G$. Clearly, id is an automorphism. In addition, for any $\sigma \in \mathrm{Aut}(G)$, we have $\sigma(\mathrm{id}(g)) = \sigma(g)$ and $\mathrm{id}(\sigma(g)) = \sigma(g)$ for all $g \in G$, making id the identity element of $\mathrm{Aut}(G)$. Now, we show that function composition is associative. For any $\sigma, \tau, \theta \in \mathrm{Aut}(G)$, we have $\sigma \circ (\tau \circ \theta)(g) = \sigma(\tau \circ \theta(g)) = \sigma(\tau(\theta(g))) = \sigma \circ \tau(\theta(g)) = (\sigma \circ \tau) \circ \theta(g)$ for all $g \in G$. Next, consider any two elements $\sigma_1, \sigma_2 \in \mathrm{Aut}(G)$. Since σ_1, σ_2 are bijections, they have two-sided inverses $\sigma_1^{-1}, \sigma_2^{-1}$. Then the product $\sigma_1 \circ \sigma_2$ also has a two-sided inverse $\sigma_2^{-1} \circ \sigma_1^{-1}$, so the product is a bijection. It is also a homomorphism because $\sigma_1 \circ \sigma_2(g_1g_2) = \sigma_1(\sigma_2(g_1g_2)) = \sigma_1(\sigma_2(g_1)\sigma_2(g_2)) = \sigma_1(\sigma_2(g_1))\sigma_1(\sigma_2(g_2)) = (\sigma_1 \circ \sigma_2(g_1))(\sigma_1 \circ \sigma_2(g_2))$. So $\mathrm{Aut}(G)$ is closed under function composition. Finally, for any $\sigma \in$ G, σ^{-1} is clearly an automorphism as well. It has a two-sided inverse σ, making it a bijection, and for any two elements $\sigma(g_1), \sigma(g_2) \in G$, we have $\sigma^{-1}(\sigma(g_1)\sigma(g_2)) = \sigma^{-1}(\sigma(g_1g_2)) = g_1g_2 = \sigma^{-1}(\sigma(g_1))\sigma^{-1}(\sigma(g_2))$, making σ^{-1} a homomorphism. We may conclude that $\mathrm{Aut}(G)$ is a group under function composition.

21. Fix $k \in \mathbb{Q} - \{0\}$, and define the map $\varphi : \mathbb{Q} \to \mathbb{Q}$ by $\varphi(q) = kq$ for all $q \in \mathbb{Q}$. Then for any two elements $q, r \in \mathbb{Q}$, we have $\varphi(q+r) = k(q+r) = kq + kr = \varphi(q) + \varphi(r)$ so φ is a homomorphism. Defining $\varphi^{-1} : \mathbb{Q} \to \mathbb{Q}$ by $\varphi^{-1}(q) = \frac{q}{k}$ for all $q \in \mathbb{Q}$, it is clear that φ^{-1} is the two-sided inverse of φ: $\varphi(\varphi^{-1}(q)) = \varphi(\frac{q}{k}) = q$ and $\varphi^{-1}(\varphi(q)) = \varphi^{-1}(kq) = q$ for all $q \in \mathbb{Q}$. Thus, φ is both a bijection and a homomorphism, making it an automorphism of $\mathbb{Q}$.

22. Let A be an abelian group, and fix $k \in \mathbb{Z}$. Define $\varphi : A \to A$ by $\varphi(a) = a^k$ for all $a \in A$. Then for any two elements $a, b \in A$, we have $\varphi(ab) = (ab)^k = a^k b^k = \varphi(a)\varphi(b)$, so φ is a homomorphism. Suppose in addition that $k = -1$. Then note that $\varphi(\varphi(a)) = \varphi(a^{-1}) = (a^{-1})^{-1} = a$, so φ has a two-sided inverse and is a bijection. Therefore, in this case, φ is an isomorphism.

23. Let G, σ be as defined in the problem statement. Consider the map $\varphi : G \to G$ defined by $\varphi(g) = g^{-1}\sigma(g)$ for all $g \in G$. Since G is a finite group, φ is a bijection iff it is an injection. Suppose that there exist $g, h \in G$ such that $g \neq h$ but $\varphi(g) = \varphi(h)$. Then we have $g^{-1}\sigma(g) = h^{-1}\sigma(h)$ or $hg^{-1} = \sigma(hg^{-1})$. Then we must have $hg^{-1} = 1$, which implies $h = g$. This is a contradiction, so φ is injective (and therefore bijective). Then for every $g \in G$, there exists $h \in G$ such that $g = h^{-1}\sigma(h)$. Applying σ to any element g, we have $\sigma(g) = \sigma(h^{-1}\sigma(h)) = \sigma(h)^{-1}h = g^{-1}$. Then for the product of any two elements $g, h \in G$, we have $h^{-1}g^{-1} = (gh)^{-1} = \sigma(gh) = \sigma(g)\sigma(h) = g^{-1}h^{-1}$ from which it follows that $gh = hg$. Thus, G is abelian.

24. If x and y generate G, then xy and y also generate G, since we can obtain x from xy and y via $xy \cdot y = x$. Then letting $|xy| = n$, we have the relations $(xy)^n = 1$, $y^2 = 1$ and $(xy)y = y(xy)^{-1}$. So, there is a unique homomorphism $\varphi : G \to D_{2n}$ satisfying $\varphi(xy) = r$ and $\varphi(y) = s$. Since r, s generate D_{2n}, φ is surjective. Furthermore, $|D_{2n}| = |G|$. To see this, note that the relation $(xy)y = y(xy)^{-1}$ allows us to write any product of xy and y (and therefore every element of G) in the form $y^k(xy)^\ell$ for some $k, \ell \in \mathbb{R}$. Since there are n distinct powers of (xy) and 2 distinct powers of y, we have $|G| = 2n = |D_{2n}|$. Thus φ is also injective, which makes it an isomorphism. So, we may conclude that $G \cong D_{2n}$.

25. (a) Let $v = (|v|\cos(\phi), |v|\sin(\phi))$ be any element of $\mathbb{R}^2$. We have

$$\begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} |v|\cos(\phi) \\ |v|\sin(\phi) \end{pmatrix} = \begin{pmatrix} |v|\cos(\phi)\cos(\theta) - |v|\sin(\phi)\sin(\theta) \\ |v|\cos(\phi)\sin(\theta) + |v|\sin(\phi)\cos(\theta) \end{pmatrix}$$
$$= \begin{pmatrix} |v|\cos(\phi+\theta) \\ |v|\sin(\phi+\theta) \end{pmatrix}$$

So the given matrix clearly rotates every element of $\mathbb{R}^2$ by θ radians.

25. (b) We first prove that $\varphi(r)^m$ takes the form $\begin{pmatrix}\cos(m\theta) & -\sin(m\theta)\\ \sin(m\theta) & \cos(m\theta)\end{pmatrix}$. The equation holds trivially for $m = 1$, and it is clear that the equation holds also for $m = 2$:

$$\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix} = \begin{pmatrix}\cos^2(\theta)-\sin^2(\theta) & -2\sin(\theta)\cos(\theta)\\ 2\sin(\theta)\cos(\theta) & \cos^2(\theta)-\sin^2(\theta)\end{pmatrix}$$
$$= \begin{pmatrix}\cos(2\theta) & -\sin(2\theta)\\ \sin(2\theta) & \cos(2\theta)\end{pmatrix}$$

Suppose it holds for $k < m$. Then for $\varphi(r)^m$, we have

$$\begin{aligned}\varphi(r)^m &= \varphi(r)^{m-1}\varphi(r)\\ &= \begin{pmatrix}\cos((m-1)\theta) & -\sin((m-1)\theta)\\ \sin((m-1)\theta) & \cos((m-1)\theta)\end{pmatrix}\begin{pmatrix}\cos(\theta) & -\sin(\theta)\\ \sin(\theta) & \cos(\theta)\end{pmatrix}\\ &= \begin{pmatrix}\cos((m-1)\theta)\cos(\theta)-\sin((m-1)\theta)\sin(\theta) & -\cos((m-1)\theta)\sin(\theta)-\sin((m-1)\theta)\cos(\theta)\\ \sin((m-1)\theta)\cos(\theta)+\cos((m-1)\theta)\sin(\theta) & \cos((m-1)\theta)\cos(\theta)-\sin((m-1)\theta)\sin(\theta)\end{pmatrix}\\ &= \begin{pmatrix}\cos((m-1)\theta+\theta) & -\sin((m-1)\theta+\theta)\\ \sin((m-1)\theta+\theta) & \cos((m-1)\theta+\theta)\end{pmatrix}\\ &= \begin{pmatrix}\cos(m\theta) & -\sin(m\theta)\\ \sin(m\theta) & \cos(m\theta)\end{pmatrix}\end{aligned}$$

and by induction on m, we have the claim. In the case of $\varphi(r)^n$, we have:

$$\varphi(r)^n = \begin{pmatrix}\cos(n\theta) & -\sin(n\theta)\\ \sin(n\theta) & \cos(n\theta)\end{pmatrix} = \begin{pmatrix}\cos(2\pi) & -\sin(2\pi)\\ \sin(2\pi) & \cos(2\pi)\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

or $\varphi(r)^n = I$. In addition, for $\varphi(s)$, we find

$$\varphi(s)^2 = \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$$

or $\varphi(s)^2 = 1$. Finally, we have the relation

$$\begin{aligned}
\varphi(r)\varphi(s) &= \begin{pmatrix} \cos(\theta) & -\sin(\theta) \\ \sin(\theta) & \cos(\theta) \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} -\sin(\theta) & \cos(\theta) \\ \cos(\theta) & \sin(\theta) \end{pmatrix} \\
&= \begin{pmatrix} \sin(n\theta - \theta) & \cos(n\theta - \theta) \\ \cos(n\theta - \theta) & -\sin(n\theta - \theta) \end{pmatrix} \\
&= \begin{pmatrix} \sin((n-1)\theta) & \cos((n-1)\theta) \\ \cos((n-1)\theta) & -\sin((n-1)\theta) \end{pmatrix} \\
&= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \cos((n-1)\theta) & -\sin((n-1)\theta) \\ \sin((n-1)\theta) & \cos((n-1)\theta) \end{pmatrix} \\
&= \varphi(s)\varphi(r)^{-1}
\end{aligned}$$

Therefore, φ extends to a homomorphism of D_{2n} into $GL_2(\mathbb{R})$.

25. (c) Suppose there exist two elements $s^i r^j, s^k r^\ell \in D_{2n}$ such that $s^i r^j \neq s^k r^\ell$ but $\varphi(s^i r^j) = \varphi(s^k r^\ell)$. Then we would have $\varphi(s)^i \varphi(r)^j \varphi(r)^{-\ell} \varphi(s)^{-k} = I$ so that $(\varphi(s)^i \varphi(r)^j)^{-1} = \varphi(r)^{-j} \varphi(s)^{-i} = \varphi(r)^{-\ell} \varphi(s)^{-k}$. It follows that $\varphi(r)^{\ell - j} = \varphi(s)^{i-k}$ which implies that $n | \ell - j$ and $2 | i - k$. Therefore, $r^{\ell - j} = 1$ and $s^{i-k} = 1$, from which we can conclude that $r^j = r^\ell$ and $s^i = s^k$ so that $s^i r^j = s^k r^\ell$. This is a contradiction, so φ is injective.

26. We have the relations

$$\begin{aligned}
\varphi(i)^2 &= \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \\
&= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \\
\varphi(j)^2 &= \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}
\end{aligned}$$

$$\begin{aligned}
\varphi(i)\varphi(j) &= \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \\
&= \begin{pmatrix} 0 & -\sqrt{-1} \\ -\sqrt{-1} & 0 \end{pmatrix} \\
&= -\begin{pmatrix} 0 & \sqrt{-1} \\ \sqrt{-1} & 0 \end{pmatrix} \\
&= -\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix} \\
&= -\varphi(j)\varphi(i)
\end{aligned}$$

Or $\varphi(i)^2 = \varphi(j)^2 = -I$ and $\varphi(i)\varphi(j) = -\varphi(j)\varphi(i)$. Thus, φ extends to a homomorphism from Q_8 into $GL_2(\mathbb{C})$. If we write the relation $ij = -ji$ in the form $ji = i^3 j$, it is easy to see that all elements of Q_8 may be written in the form $i^k j^\ell$. A similar argument to the one presented in exercise 25.(c) can be used to show that φ is injective.

1.7 Group Actions

1. Because $F^\times$ is an abelian group, for all $g_1, g_2, a \in F^\times$, we have $g_1 \cdot (g_2 \cdot a) = g_1 \cdot (g_2 a) = g_1(g_2 a) = (g_1 g_2)a = (g_1 g_2) \cdot a$. In the case that $a = 0$, we have $g_1 \cdot (g_2 \cdot 0) = g_1 \cdot 0 = 0 = (g_1 g_2) \cdot 0$. Finally, because 1 is the identity of the group $F^\times$, every $a \in F^\times$ satisfies $1 \cdot a = a$. When $a = 0$, we have $1 \cdot 0 = 0$. So, $F^\times$ indeed acts on F by $g \cdot a = ga$.

2. $\mathbb{Z}$ is a group under addition, meaning that $+$ is associative on $\mathbb{Z}$. Therefore, for any two elements $a, b, c \in \mathbb{Z}$, we have $a \cdot (b \cdot c) = a + (b + c) = (a + b) + c = (ab) \cdot c$. In addition, for any $a \in \mathbb{Z}$, we have $0 \cdot a = 0 + a = a$. So, the additive group $\mathbb{Z}$ acts on itself by $z \cdot a = z + a$ for all $z, a \in \mathbb{Z}$.

3. For any two elements $s, t \in \mathbb{R}$ and any element $(x, y) \in \mathbb{R}^2$, we have $s \cdot (t \cdot (x, y)) = s \cdot (x + ty, y) = (x + ty + sy, y) = (x + (t + s)y, y) = (t + s) \cdot (x, y) = (ts) \cdot (x, y)$. In addition, for any $(x, y) \in \mathbb{R}^2$, we have $0 \cdot (x, y) = (x + 0y, y) = (x, y)$. So, the additive group $\mathbb{R}$ acts on $\mathbb{R}^2$ by $r \cdot (x, y) = (x + ry, y)$.

4. (a) The group operation of G is necessarily associative on the kernel of the action. The identity element 1_G is clearly in the kernel, since a group action is required to satisfy $1_G \cdot a = a$ for all $a \in A$. Then note that for any two elements g, h of the kernel, their product satisfies $(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a$ for all $a \in A$, so the kernel is closed under the group operation. Finally, for any element g of the kernel, we find that $g^{-1} \cdot a = g^{-1} \cdot (g \cdot a) = (g^{-1} g) \cdot a = 1_G \cdot a = a$ for all $a \in A$. So, we find that the kernel of the action is a subgroup of G.

4. (b) Now we fix some $a \in A$ and consider the group operation on the set $S = \{g \in G \mid ga = a\}$. As above, the group operation of G is necessarily associative on S. Furthermore, the identity element 1_G of G satisfies $1_G \cdot b = b$ for all $b \in S$, so it is certainly an element of S. For any two elements $g, h \in S$, we have $(gh) \cdot a = g \cdot (h \cdot a) = g \cdot a = a$, so S is closed under the group operation. Finally, for any element $g \in S$, we have $g^{-1} \cdot a = g^{-1} \cdot (g \cdot a) = (g^{-1} g) \cdot a = 1_G \cdot a = a$, so S is closed under inverses. So, we conclude that S is a subgroup of G.

5. The kernel of the permutation representation φ is the set $S = \{g \in G \mid \varphi(g) = \mathrm{id}\}$. That is, if $g \in S$, then for all $a \in A$, $\varphi(g)(a) = \sigma_g(a) = g \cdot a = a$, so g is also in the kernel of the action. Similarly, if g is in the kernel of the action, then $a = g \cdot a = \sigma_g(a) = \varphi(g)(a)$ for all $a \in A$, meaning $\varphi(g) = \mathrm{id}$, so $g \in S$.

6. Let G act faithfully on A. Then for any two elements $g, h \in G$ such that $g \neq h$, there exists some $a \in A$ such that $g \cdot a \neq h \cdot a$. Thus, for any $g \in G$ such that

$g \neq 1_G$, there exists at least one element $a \in A$ such that $g \cdot a \neq 1_G \cdot a = a$. It follows that the kernel of the action contains only 1_G.

If the kernel of the action is the set consisting of only the identity 1_G, then for any $g \in G$ such that $g \neq 1_G$, there exists at least one element $a \in A$ such that $g \cdot a \neq a$. Now, suppose that there exists two elements $g, h \in G$ with $g \neq h$ such that $g \cdot a = h \cdot a$ for all $a \in A$. Then $g^{-1} \cdot (h \cdot a) = g^{-1} \cdot (g \cdot a) = (g^{-1}g) \cdot a = 1_G \cdot a = a$. Since $g^{-1} \cdot (h \cdot a) = (g^{-1}h) \cdot a$, and the kernel of the action contains only the identity, it follows that $g^{-1}h = 1$ or $h = g$. This is a contradiction, so any two distinct elements $g, h \in G$ induce distinct permutations. In other words, G acts faithfully on A.

7. Here we will prove the statement "$F^\times$ acts faithfully on V iff V is not the zero vector space or F has only two elements", where F is any field and V is any vector space over F.

Let V be a vector space over F and consider the action of $F^\times$ on V via scalar multiplication. By the vector space axioms, $1_F \cdot v = v$ for all $v \in V$. If $|F^\times| = 1$, then the action of $F^\times$ on V is trivially faithful, since there is only one element of $F^\times$.

If $|F^\times| > 1$ and V is not the zero vector space, then we can show that $F^\times$ acts faithfully on V. Suppose there is an element $g \in F^\times$ such that $g \neq 1_F$, but $g \cdot v = v$ for all $v \in V$. Then we would have $g \cdot v = 1_F \cdot v$ for all $v \in V$, or $g \cdot v - 1_F \cdot v = (g - 1_F) \cdot v = \mathbf{0}$. Since V is not the zero vector space, this equation holds for some non-zero $v \in V$, which implies that $g = 1_F$...a contradiction! So the kernel of the action is just $\{1_F\}$, implying that $F^\times$ acts faithfully on V.

If $F^\times$ acts faithfully on V and $|F^\times| > 1$, then distinct elements of $F^\times$ induce distinct permutations on V. That is, for any $a, b \in F^\times$ with $a \neq b$, there exists some $v \in V$ such that $a \cdot v \neq b \cdot v$. Clearly, $v \neq \mathbf{0}$ since, $a \cdot \mathbf{0} = \mathbf{0}$ for all $a \in F^\times$. Thus, V cannot be the zero vector space. Proving these statements together is equivalent to proving that $F^\times$ acts faithfully on V iff $|F^\times| = 1$ or V is not the zero vector space, so we have our claim.

8. (a) Consider any two elements $\sigma_1, \sigma_2 \in S_A$ and any $\{a_1, ..., a_k\} \in B$. Then we have $\sigma_1 \cdot (\sigma_2 \cdot \{a_1, ..., a_k\}) = \sigma_1 \cdot \{\sigma_2(a_1), ..., \sigma_2(a_k)\} = \{\sigma_1(\sigma_2(a_1)), ..., \sigma_1(\sigma_2(a_k))\} = \{\sigma_1 \circ \sigma_2(a_1), ..., \sigma_1 \circ \sigma_2(a_k)\} = (\sigma_1 \circ \sigma_2) \cdot \{a_1, .., a_k\}$. In addition, for any $\{a_1, ..., a_k\} \in B$, $\mathrm{id} \cdot \{a_1, ..., a_k\} = \{\mathrm{id}(a_1), ..., \mathrm{id}(a_k)\} = \{a_1, ..., a_k\}$. Thus, this is a group action.

8. (b) Label the 2-element sets of $\{1,2,3,4\}$ as follows: $a = \{1,2\}$, $b = \{1,3\}$, $c = \{1,4\}$, $d = \{2,3\}$, $e = \{2,4\}$, and $f = \{3,4\}$. Then we have:

$$(1\ 2)\cdot a = a \quad (1\ 2)\cdot b = d \quad (1\ 2)\cdot c = e \quad (1\ 2)\cdot d = b \quad (1\ 2)\cdot e = c \quad (1\ 2)\cdot f = f$$

$$(1\ 2\ 3)\cdot a = d \quad (1\ 2\ 3)\cdot b = a \quad (1\ 2\ 3)\cdot c = e \quad (1\ 2\ 3)\cdot d = b$$

$$(1\ 2\ 3)\cdot e = f \quad (1\ 2\ 3)\cdot f = c$$

9. The proof that the action of S_A on B is a group action is identical to the one in exercise 8. Now, label the 16 ordered 2-tuples as follows: $a = (1,2)$, $b = (1,3)$, $c = (1,4)$, $d = (2,3)$, $e = (2,4)$, $f = (3,4)$, $g = (2,1)$, $h = (3,1)$, $i = (4,1)$, $j = (3,2)$, $k = (4,2)$, $l = (4,3)$, $m = (1,1)$, $n = (2,2)$, $o = (3,3)$, $p = (4,4)$. Then we have:

$$(1\ 2)\cdot a = g \quad (1\ 2)\cdot b = d \quad (1\ 2)\cdot c = e \quad (1\ 2)\cdot d = b \quad (1\ 2)\cdot e = c \quad (1\ 2)\cdot f = f$$

$$(1\ 2)\cdot g = a \quad (1\ 2)\cdot h = j \quad (1\ 2)\cdot i = k \quad (1\ 2)\cdot j = h \quad (1\ 2)\cdot k = i \quad (1\ 2)\cdot l = l$$

$$(1\ 2)\cdot m = n \quad (1\ 2)\cdot n = m \quad (1\ 2)\cdot o = o \quad (1\ 2)\cdot p = p$$

$$(1\ 2\ 3)\cdot a = d \quad (1\ 2\ 3)\cdot b = g \quad (1\ 2\ 3)\cdot c = e \quad (1\ 2\ 3)\cdot d = h$$

$$(1\ 2\ 3)\cdot e = f \quad (1\ 2\ 3)\cdot f = c \quad (1\ 2\ 3)\cdot g = j \quad (1\ 2\ 3)\cdot h = a$$

$$(1\ 2\ 3)\cdot i = k \quad (1\ 2\ 3)\cdot j = b \quad (1\ 2\ 3)\cdot k = l \quad (1\ 2\ 3)\cdot l = i$$

$$(1\ 2\ 3)\cdot m = n \quad (1\ 2\ 3)\cdot n = o \quad (1\ 2\ 3)\cdot o = m \quad (1\ 2\ 3)\cdot p = p$$

10. (a) Let B be the set of k-element subsets of $A = \{1,...,n\}$. Assume that S_n does not act faithfully on B. Then $n > 1$ and there exists $\sigma \in S_n$ with $\sigma \neq \text{id}$ such that $\sigma \cdot b = b$ for all $b \in B$. Because $\sigma \neq \text{id}$, there must exist at least one $a \in A$ such that $\sigma(a) \neq a$. If $k < n$, then there exists $b \in B$ such that $\sigma(a) \notin b$ but $a \in b$. Then $\sigma(a) \notin \text{id} \cdot b$, but $\sigma(a) \in \sigma \cdot b$ and therefore, $\sigma \cdot b \neq b$. This is a contradiction, so S_n acts faithfully. If, instead, $k = n$, then $B = \{A\}$. Because every element $\sigma \in S_n$ is a bijection $\sigma : A \to A$, we have $\sigma(A) = A$ for all $\sigma \in S_n$. It follows that in this case, S_n does not act faithfully on B.

10. (b) Let B be the set of ordered k-tuples containing elements of $A = \{1,...,n\}$. Assume that S_n does not act faithfully on B. Then $n > 1$ and there exists $\sigma \in S_n$ with $\sigma \neq \text{id}$ such that $\sigma \cdot b = b$ for all $b \in B$. Since $\sigma \neq \text{id}$, there exists $a \in A$ such that $\sigma(a) \neq a$. Note that for all k, there exists a k-tuple c in B such that every one of its entries is a. Then $\sigma \cdot c \neq c$. This is a contradiction, so S_n acts faithfully for all k.

11. We have $1 \to \text{id}$, $r \to (1\,2\,3\,4)$, $r^2 \to (1\,3)(2\,4)$, $r^3 \to (1\,4\,3\,2)$, $s \to (1\,4)(2\,3)$, $sr \to (1\,3)$, $sr^2 \to (1\,2)(3\,4)$, and $sr^3 = (2\,4)$.

12. Let $B = \{(k, k+\frac{n}{2}) \mid 1 \leq k \leq \frac{n}{2}\}$. Define the action of $t \in D_{2n}$ on $b \in B$ by $t \cdot b = \sigma_t \cdot b$, where σ_t is the permutation corresponding to t, and $\sigma_t \cdot b$ is defined as in exercise 8. Then we are required to show that the action of a subset of S_n on B (which is a subset of the set C of ordered 2-tuples of $\{1, .., n\}$) is a group action. From exercise 9, we have that for all $\sigma_t, \sigma_u \in S_n$ and any $c \in C$, we have $\sigma_t \cdot (\sigma_u \cdot c) = (\sigma_t \sigma_u) \cdot c$. If it holds for all $\sigma_t, \sigma_u \in S_n$, then it necessarily holds for all σ_t, σ_u in a subset of S_n and any c in a subset of C. In addition, since $1 \in D_{2n}$ corresponds to $\text{id} \in S_n$, and $1 \cdot b = \text{id} \cdot b = b$ for all $b \in B$, we have that the action of D_{2n} on B is a group action.

An element $t \in D_{2n}$ is in the kernel of the action iff $t \cdot b = b$ for all $b \in B$. In other words, this requires that $(\sigma_t(k), \sigma_t(k+\frac{n}{2})) = (k, k+\frac{n}{2})$ for all $1 \leq k \leq \frac{n}{2}$ or $\sigma_t(k) = k$ and $\sigma_t(k+\frac{n}{2}) = k+\frac{n}{2}$. Since this is true for all $1 \leq k \leq \frac{n}{2}$, we must have $\sigma_t(\ell) = \ell$ for all $1 \leq \ell \leq n$, from which it follows that $t = \text{id}$ is the only such element.

13. The kernel of the left regular action is the set of $g \in G$ such that $g \cdot a = ga = a$ for all $a \in G$. Assuming there exists $g \neq 1$ in G such that $g \cdot a = a$ for all $a \in G$, we have that $g \cdot 1 = 1$, but by the definition of the identity, $g \cdot 1 = g$. We find that $g = 1$, which is a contradiction. The kernel of the left regular action thus only contains the identity 1.

14. For any $g, h \in G$ and any $a \in G$, we have $g \cdot (h \cdot a) = g \cdot (ah) = ahg = (hg) \cdot a$. G is not abelian, so $gh \neq hg$ in general and therefore $g \cdot (h \cdot a) \neq (gh) \cdot a$ in general. This action therefore cannot be a group action of G on itself.

15. For any $g, h \in G$ and any $a \in G$, we have $g \cdot (h \cdot a) = g \cdot ah^{-1} = ah^{-1}g^{-1} = a(gh)^{-1} = (gh) \cdot a$. In addition, by definition, the identity 1 of G satisfies $1 \cdot a = a$ for all $a \in G$. Thus, this is a group action of G on itself.

16. For any $g, h \in G$ and any $a \in G$, we have $g \cdot (h \cdot a) = g \cdot hah^{-1} = ghah^{-1}g^{-1} = gha(gh)^{-1} = (gh) \cdot a$. In addition, by definition of the identity 1 of G, we have $1 \cdot a = 1a1 = 1a = a$ for all $a \in G$. Thus, this is a group action of G on itself.

17. Fix $g \in G$ and define $\varphi_g : G \to G$ by $\varphi_g(x) = gxg^{-1}$ for all $x \in G$. Note that for any $x, y \in G$, we have $\varphi(x)\varphi(y) = gxg^{-1}gyg^{-1} = gxyg^{-1} = \varphi(xy)$, so φ is a homomorphism. Now consider the map $\varphi^{-1} : G \to G$ given by $\varphi^{-1}(x) = g^{-1}xg$ for all $x \in G$. We have $\varphi^{-1}(\varphi(x)) = \varphi^{-1}(gxg^{-1}) = g^{-1}gxg^{-1}g = x$ and

$\varphi(\varphi^{-1}(x)) = \varphi(g^{-1}xg) = gg^{-1}xgg^{-1} = x$. Since φ has a two-sided inverse, it is a bijection. Therefore, φ is an automorphism of G.

If x is of finite order $|x| = n$, then we have $\varphi(x)^n = \varphi(x^n) = \varphi(1) = gg^{-1} = 1$ so $|\varphi(x)| \leq n$. On the other hand, we have $\varphi(1) = 1 = \varphi(x)^{|\varphi(x)|} = \varphi(x^{|\varphi(x)|})$. Since φ is a bijection, this implies that $x^{|\varphi(x)|} = 1$, so $|\varphi(x)| \geq n$. It must be that x and $\varphi(x) = gxg^{-1}$ have the same order. The fact that $|A| = |gAg^{-1}|$ follows from the fact that φ is a bijection.

18. Because H is a group that acts on A, it contains an identity element 1 satisfying $1 \cdot a = a$ for all $a \in A$. Therefore $\sim$ is reflexive. If $a \sim b$, then there exists $h \in H$ such that $a = h \cdot b$. Applying h^{-1}, we have $h^{-1} \cdot a = h^{-1} \cdot (h \cdot b) = (h^{-1}h) \cdot b = 1 \cdot b = b$, so $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, then there exist $h_1, h_2 \in H$ such that $a = h_1 \cdot b$ and $b = h_2 \cdot c$. We may write $a = h_1 \cdot b = h_1 \cdot (h_2 \cdot c) = (h_1h_2) \cdot c$, so $a \sim c$ because $h_1h_2 \in H$. Therefore, $\sim$ is an equivalence relation.

19. Let $\varphi : H \to \mathcal{O}$ be the map defined by $\varphi(h) = hx$ for all $h \in H$. Consider the map $\varphi^{-1} : \mathcal{O} \to H$ defined by $\varphi^{-1}(s) = sx^{-1}$ for all $s \in \mathcal{O}$. It is easy to see by looking at the definition of $\mathcal{O}$ that the image of φ^{-1} is indeed a subset of H. Then we have $\varphi(\varphi^{-1}(s)) = \varphi(sx^{-1}) = sx^{-1}x = s$ for all $s \in \mathcal{O}$ and $\varphi^{-1}(\varphi(h)) = \varphi^{-1}(hx) = hxx^{-1} = h$ for all $h \in H$. Since φ has a two-sided inverse, it is a bijection. We conclude that because G is finite (and hence, so are H and $\mathcal{O}$), x was arbitrary, and φ is a bijection, it must be that every orbit has cardinality $|H|$.

If G is a finite group and H is a subgroup of G, the orbits under the action of H on G partition G. It follows that $|G| = \sum_{i \in I} |\mathcal{O}_i|$ where I is the index set used to index the orbits in the partition. Since $|\mathcal{O}_i| = |H|$ for every orbit $\mathcal{O}_i$, $|G| = |I||H|$. In other words, $|H|$ divides $|G|$.

20. Let G be the group of rigid motions of the tetrahedron. If we label the vertices of the tetrahedron $1, 2, 3, 4$, each rigid motion $g \in G$ gives rise to a permutation σ_g of $\{1, 2, 3, 4\}$ by the way the motion g permutes the corresponding vertices. Then the map from $G \times \{1, 2, 3, 4\} \to \{1, 2, 3, 4\}$ defined by $g \cdot i = \sigma_g(i)$ defines a group action of G on $\{1, 2, 3, 4\}$. Thus, there is a homomorphism φ from G to S_4. It is quite obvious that the only permutation of the vertices that fixes all of them is the identity of G, so φ is injective. Since $\varphi(G)$ is a subgroup of S_4 (cf. Exercise 14 of Section 6), and φ is injective, we have that G is isomorphic to a subgroup of S_4.

21. Let G be the group of rigid motions of the cube. It is easy to see that every element of G maps a pair of opposite vertices to another such pair. Label the pairs of opposite vertices p_1, p_2, p_3, p_4. Each $g \in G$ gives rise to a permutation σ_g of

$\{p_1, p_2, p_3, p_4\}$ by the way g permutes the corresponding pairs of vertices. As in the previous exercise, there is therefore a natural homomorphism $\varphi : G \to S_4$. Now, suppose there is an element $g \in G$ such that g is not the identity motion but g is in the kernel of the action. Such an element must send at least one pair of opposite vertices to each other. Let a, b be any pair of opposite vertices, and let c, d, e be the neighbors of a, with b, e on the same face. Then sending a to b also sends c to d's partner and vice versa. The corresponding permutation of $\{p_1, p_2, p_3, p_4\}$ is not the identity, and it is clear that no such g can exist. Thus, φ is injective and since $|G| = |S_4| = 24$ (cf. Exercise 10 of Section 2), φ is a bijection. We conclude that $G \cong S_4$.

22. Let G be the group of rigid motions of the octahedron. Through a similar argument (just replace "vertices" with "faces") to the one in Exercise 21, we find that there is a natural homomorphism $\varphi : G \to S_4$ and that φ is an injection. Since $|G| = |S_4| = 24$ (cf. Exercise 11 of Section 2), φ is a bijection and $G \cong S_4$.

23. The rotation of π radians about the axis through the center of a pair of opposite faces maps every pair of opposite faces to themselves. Then the kernel is not trivial and therefore, the action of the group on this set is not faithful. The kernel of the action consists of just the three rotations of this type and the identity. All other elements of G send at least one face of the cube to one of its neighbors, and so, cannot be in the kernel.