Summer Programme 2021

Solutions to exercises from M.A. Armstrong's *Groups and Symmetry*

Satvik Saha
19MS154

Indian Institute of Science Education and Research, Kolkata,
Mohanpur, West Bengal, 741246, India.

Chapter 1

Symmetries of the Tetrahedron

Exercise 1.1 Glue two copies of a regular tetrahedron together so that they have a triangular face in common, and work out all the rotational symmetries of this new solid.

Solution. The resultant bi-pyramid has five vertices; label the ones furthest apart as 1 and 2, and then label the remaining ones on the equator as 3, 4, 5. The rotational symmetries are those which permute these five vertices such that 1 and 2 never leave the long axis, and the cyclicity of the vertices 1, 2, 3, 4 is preserved. Thus, we have 3 rotations about the long axis (by 0, $2\pi/3$, and $4\pi/3$) which cycle the vertices 3, 4, 5, then three rotations, each about an axis through one of the vertices 3, 4, 5 and the midpoint of the opposite edge (by 0, π) which swap the positions of 1 and 2 and reverse the cyclicity of 3, 4, 5. This gives a total of $2 \times 3 = 6$ symmetries.

Exercise 1.2 Find all rotational symmetries of a cube.

Solution. First consider the four rotations (by 0, $\pi/2$, π, $3\pi/2$) about an axis which passes through the centres of opposite faces; there are three such axes giving $3 \times 3 = 9$ such rotational symmetries (excluding the identity symmetry, which we will add on at the end). Next, consider the two rotations (by 0, π) about an axis passing through the centres of opposite edges; there are six such axes, giving $1 \times 6 = 6$ such rotational symmetries. Next, consider the three rotations (by 0, $2\pi/3$, $4\pi/3$) about an axis passing through opposite vertices; there are four such axes, giving $2 \times 4 = 8$ such rotational symmetries. Adding these up, we have $9 + 6 + 8 = 23$ rotational symmetries. The identity symmetry brings the total to 24 rotational symmetries of the cube.

Exercise 1.3 Adopt the notation of Figure 1.4. Show that the axis of the composite rotation srs passes through the vertex 4, and that the axis of $rsrr$ is determined by the midpoints of edges 12 and 34.

Solution. Let the original state of the tetrahedron be represented by the tuple $(1, 2, 3, 4)$, indicating the labels on the four vertices. Applying s permutes this to $(4, 3, 2, 1)$, and applying r permutes (the original) to $(1, 4, 2, 3)$. Thus, the action srs is the permutation $(1, 2, 3, 4) \to (4, 3, 2, 1) \to (4, 1, 3, 2) \to (2, 3, 1, 4)$. Note that the vertex labelled 4 is a fixed point, hence the axis of this composite rotation must have passed through this vertex.

Similarly, the action $rsrr$ maps $(1, 2, 3, 4) \to (1, 4, 2, 3) \to (1, 3, 4, 2) \to (2, 4, 3, 1) \to (2, 1, 4, 3)$. There are no fixed points, hence this is not a rotation through a vertex. Instead, the first pair and last pair of vertices have swapped, which indicates a rotation about an axis through the centres of the edges 12 and 34.

Exercise 1.4 Having completed the previous exercise, express each of the twelve rotational symmetries of the tetrahedron in terms of r and s.

Solution. The twelve rotational symmetries of the tetrahedron are e (the identity), r, r^2, s, rs, r^2s, srs, $rsrs$, r^2srs, sr^2s, rsr^2s, r^2sr^2s. See Exercise 1.7 for their actions on the $(1, 2, 3, 4)$ state.

Exercise 1.5 Again with the notation of Figure 1.4, check that $r^{-1} = rr$, $s^{-1} = s$, $(rs)^{-1} = srr$ and $(sr)^{-1} = rrs$.

Solution. Note that r^3 maps $(1, 2, 3, 4) \to (1, 4, 2, 3) \to (1, 3, 4, 2) \to (1, 2, 3, 4)$, so $r^3 = e$. Thus, $(rr)r = e = r(rr)$, so $r^{-1} = rr$.

Next, note that ss maps $(1, 2, 3, 4) \to (4, 3, 2, 1) \to (1, 2, 3, 4)$, so $ss = e$. Thus, $(s)s = e = e(s)$, so $s^{-1} = s$.

Next, note that $(rs)(srr) = r(ss)(rr) = r(e)(rr) = rrr = e$, and $(srr)(rs) = s(rrr)s = s(e)s = ss = e$, so $(rs)^{-1} = srr$.

Finally, note that $(sr)(rrs) = (srr)(rs) = e$ and $(rrs)(sr) = (rr)(ss)r = rrr = e$, so $(sr)^{-1} = rrs$.

Exercise 1.6 Show that a regular tetrahedron has a total of twenty-four symmetries if reflections and products of reflections are allowed. Identify a symmetry which is not a rotation and not a reflection. Check that this symmetry is a product of three reflections.

Solution. Note that a reflection about the plane passing through an edge and the centroid swaps the remaining two vertices. Thus, by representing the vertex configuration of the tetrahedron as a tuple $(1, 2, 3, 4)$, this can be mapped to any of the $4! = 24$ permutations by employing suitable reflections (for example, see bubble sort).

Consider the action which takes the tetrahedron $(1, 2, 3, 4)$ to the state $(4, 1, 2, 3)$. This is not a rotation about a vertex, nor a reflection about a plane through an edge because there are no fixed points. This is not a rotation about an axis through the centres of opposite sides either, since those must swap the labels on two pairs of adjacent vertices. However, this can be reached via the reflections $(1, 2, 3, 4) \to (4, 2, 3, 1) \to (4, 1, 3, 2) \to (4, 1, 2, 3)$; these were reflections about planes passing through the edges 23, 13, 12.

Exercise 1.7 Let q denote reflection of a regular tetrahedron in the plane determined by its centroid and one of its edges. Show that the rotational symmetries, together with those of the form uq, where u is a rotation, give all twenty-four symmetries of the tetrahedron.

Solution. We let q mean the reflection in the plane through the centroid and the side 12; note that this maps $(1, 2, 3, 4) \to (1, 2, 4, 3)$. Below, we list all 24 permutations of the tuple $(1, 2, 3, 4)$, which represent all 24 symmetries of the tetrahedron.

Symmetry	State	Symmetry	State
e	1, 2, 3, 4	q	1, 2, 4, 3
r	1, 4, 2, 3	rq	1, 3, 2, 4
r^2	1, 3, 4, 2	r^2q	1, 4, 3, 2
s	4, 3, 2, 1	sq	3, 4, 2, 1
rs	4, 1, 3, 2	rsq	3, 1, 4, 2
r^2s	4, 2, 1, 3	r^2sq	3, 2, 1, 4
srs	2, 3, 1, 4	$srsq$	2, 4, 1, 3
$rsrs$	2, 4, 3, 1	$rsrsq$	2, 3, 4, 1
r^2srs	2, 1, 4, 3	r^2srsq	2, 1, 3, 4
sr^2s	3, 1, 2, 4	sr^2sq	4, 1, 2, 3
rsr^2s	3, 4, 1, 2	rsr^2sq	4, 3, 1, 2
r^2sr^2s	3, 2, 4, 1	r^2sr^2sq	4, 2, 3, 1

Exercise 1.8 Find all plane symmetries (rotations and reflections) of a regular pentagon and of a regular hexagon.

Solution. Any symmetry of a regular n-gon is one which preserves adjacent vertices, i.e. two labelled vertices must remain adjacent before and after the symmetry action. Thus, we have n rotations (by $2k\pi/n$), along with n rotations followed by a reflection (these are mirror images of the previous n symmetries). Thus, a regular n-gon has $2n$ plane symmetries; ten for a pentagon and twelve for a hexagon.

Exercise 1.9 Show that the hexagonal plate of Figure 1.2 has twenty-four symmetries in all. Identify those symmetries which commute with all the others.

Solution. By representing the vertices of the hexagon as the tuple $(1, 2, 3, 4, 5, 6)$, we see symmetries of the plate are precisely those actions which permute these elements, preserving the adjacency but allowing a reversal in order. There are six tuples of the form $(1+n, 2+n, \ldots, 6+n)$ and six more of the form $(6 + n, 5 + n, \ldots, 1 + n)$. Because we are dealing with a hexagonal plate, there is another symmetry which is a reflection passing through a plane parallel to the hexagonal face. This does not change the labels on the vertices on the hexagonal face in any way, but exchanges the top and bottom faces. Thus, this symmetry commutes with all other symmetries, and the combination of any one of the twelve previously shown symmetries with this reflection symmetry produces a new symmetry, bringing our total to twenty-four.

Exercise 1.10 Make models of the octahedron, dodecahedron, and icosahedron. Try to spot as many symmetries of these solids as you can.

Chapter 2

Axioms

Exercise 2.1 Compare the symmetry of a snow crystal with that of the hexagonal plate in Figure 1.2.

Exercise 2.2 Show that the set of positive real numbers form a group under multiplication.

Solution. First note that multiplication of real numbers is associative, which means that $(xy)z = x(yz)$ for all $x, y, z \in \mathbb{R}^+$. Next, $1x = x = x1$ for all $x \in \mathbb{R}^+$, so $1 \in \mathbb{R}^+$ serves as our identity element. Finally, every positive real number x has a multiplicative inverse $1/x \in \mathbb{R}^+$, which satisfies $x(1/x) = 1 = (1/x)x$.

Exercise 2.3 Which of the following collections of 2×2 matrices with real entries form groups under matrix multiplication?

(i) Those of the form $\begin{bmatrix} a & b \\ b & c \end{bmatrix}$ for which $ac \neq b^2$.

(ii) Those of the form $\begin{bmatrix} a & b \\ c & a \end{bmatrix}$ for which $a^2 \neq bc$.

(iii) Those of the form $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$ for which $ac \neq 0$.

(iv) Those which have non-zero determinant and whose entries are integers.

Solution.

(i) Matrices of this form are not closed under multiplication. Consider

$$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 1 & 1 \end{bmatrix}.$$

(ii) Matrices of this form are not closed under multiplication. Consider

$$\begin{bmatrix} 1 & 1 \\ 2 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 3 & 1 \end{bmatrix} = \begin{bmatrix} 4 & 2 \\ 5 & 3 \end{bmatrix}.$$

(iii) First, note that multiplication of such matrices is closed,

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

Next, the identity matrix $\mathbb{I}_2$ satisfies the role of the multiplicative identity, with $\mathbb{I}_2 M = \mathbb{I}_2 = M\mathbb{I}_2$ for all such matrices M. Finally, we have

$$\begin{bmatrix} 1/a & -b/ac \\ 0 & 1/c \end{bmatrix} \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \begin{bmatrix} 1/a & -b/ac \\ 0 & 1/c \end{bmatrix},$$

so all such matrices have a multiplicative inverse. This means that this collection of matrices forms a group under matrix multiplication.

(iv) Note that all the collection of all matrices must have $\mathbb{I}_2$ as the identity element. However, not all matrices have a multiplicative inverse in this collection. For example,

$$\begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix} \begin{bmatrix} 1/2 & 0 \\ 0 & 1/2 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Exercise 2.4 Let f be a similarity of the plane. Show that f is a bijection and that the inverse function f^{-1} is also a similarity. Verify that the collection of all similarities of the plane forms a group under composition of functions.

Solution. Any similarity $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ of the plane can be written in the form

$$f(\boldsymbol{x}) = \lambda A\boldsymbol{x} + \boldsymbol{x}_0,$$

where $A \in O_2(\mathbb{R})$ is an orthogonal matrix, $\boldsymbol{x}_0 \in \mathbb{R}^2$ is a translation vector and $\lambda \in \mathbb{R} \setminus \{0\}$ is a scaling factor. The fact that all such λA are invertible guarantees that f is a bijection. This immediately gives

$$f^{-1}(\boldsymbol{x}) = \frac{1}{\lambda}A^{-1}\boldsymbol{x} - \frac{1}{\lambda}A^{-1}\boldsymbol{x}_0,$$

which is also a similarity of the plane.

A similarity of the plane must send lines to lines, in such a way that all lengths scale in the same proportion. This means that

$$f(\boldsymbol{x} + \mu(\boldsymbol{y} - \boldsymbol{x})) = f(\boldsymbol{x}) + \mu(f(\boldsymbol{y}) - f(\boldsymbol{x}))$$

for all scalars μ. Set $f(\mathbf{0}) = \boldsymbol{x}_0$, and set $g = f - \boldsymbol{x}_0$. Then we have $g(\mathbf{0}) = \mathbf{0}$ and

$$g(\boldsymbol{x} + \mu(\boldsymbol{y} - \boldsymbol{x})) = g(\boldsymbol{x}) + \mu(g(\boldsymbol{y}) - g(\boldsymbol{x})).$$

Setting $\boldsymbol{x} = \mathbf{0}$, next $\mu = 1/2$ gives

$$g(\mu\boldsymbol{y}) = \mu g(\boldsymbol{y}), \qquad g(\boldsymbol{x} + \boldsymbol{y}) = g(\boldsymbol{x} + \boldsymbol{y}).$$

Thus, g is a linear transformation, and is thus of the form

$$g(\boldsymbol{x}) = B\boldsymbol{x}$$

for some 2×2 matrix B. Note that if B were not of full rank, then its null space must contain some non-zero vector $\boldsymbol{v}$ such that $B\boldsymbol{v} = \mathbf{0}$. This cannot be allowed for a similarity of the plane, since such a transformation would map the entire line along $\boldsymbol{v}$ onto the single point at the origin. Thus, B must be invertible making g a linear bijection, and this is sufficient to show that $f(\boldsymbol{x}) = B\boldsymbol{x} + \boldsymbol{x}_0$ is a bijection.

To show that $B = \lambda A$ for some $A \in O_2(\mathbb{R})$, note that we require f and g to scale all line segments equally. Thus, $\|g(\boldsymbol{x})\| = \|g(\boldsymbol{y})\|$ whenever $\|\boldsymbol{x}\| = \|\boldsymbol{y}\|$. Set $\lambda = \|g(\hat{\boldsymbol{v}})\|$ for all unit vectors $\hat{\boldsymbol{v}}$, and noting that $\lambda \neq 0$, set $A = B/\lambda$. Thus, $\|g(\boldsymbol{v})\| = \|g(v\hat{\boldsymbol{v}})\| = v\,\|g(\hat{\boldsymbol{v}})\| = \|\boldsymbol{v}\|\,\lambda$ for all vectors $\boldsymbol{v}$. Hence, $\|A\boldsymbol{v}\| = \|\boldsymbol{v}\|$ for all vectors $\boldsymbol{v}$, so the transformation represented by A is an isometry. This can be shown to force $A \in O_2(\mathbb{R})$.

Exercise 2.5 A function from the plane to itself which preserves the distance between any two points is called an *isometry*. Prove that an isometry must be a bijection and check that the collection of all isometries of the plane forms a group under composition of functions.

Solution. Again, an isometry $f\colon \mathbb{R}^2 \to \mathbb{R}^2$ of the plane must be of the form

$$f(\boldsymbol{x}) = A\boldsymbol{x} + \boldsymbol{x}_0,$$

where $A \in O_2(\mathbb{R})$ is an orthogonal matrix and $\boldsymbol{x}_0 \in \mathbb{R}^2$ is a translation vector. The invertibility of A guarantees that f is a bijection.

Exercise 2.6 Show that the collection of all rotations of the plane about a fixed point P forms a group under composition of functions. Is the same true of the set of all reflections in lines which pass through P? What happens if we take all the rotations and all the reflections?

Exercise 2.7 Let x and y be elements of a group G. Prove that G contains w, z which satisfy $wx = y$ and $xz = y$, and show that these elements are unique.

Solution. Note that x has an inverse $x^{-1} \in G$. Set $w = yx^{-1}$ and $z = x^{-1}y$, whence

$$wx = (yx^{-1})x = y(x^{-1}x) = ye = y, \qquad xz = x(x^{-1}y) = (xx^{-1})y = ey = y.$$

Next, suppose that $w_1x = w_2x = y$. Right multiplying by x^{-1} gives $w_1 = w_2 = yx^{-1}$. Similarly, if $xz_1 = xz_2 = y$, left multiplying my x^{-1} gives $z_1 = z_2 = x^{-1}y$.

Exercise 2.8 If x and y are elements of a group, prove that $(xy)^{-1} = y^{-1}x^{-1}$.

Solution. Using the associativity of multiplication,

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x = xex^{-1} = xx^{-1} = e,$$

$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e.$$

Chapter 3

Numbers

Exercise 3.1 Show that each of the following collections of numbers forms a group under addition.

(i) The even integers.

(ii) All real numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Z}$.

(iii) All real numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$.

(iv) All complex numbers of the form $a + bi$ where $a, b \in \mathbb{Z}$.

Exercise 3.2 Write $\mathbb{Q}(\sqrt{2})$ for the set described in Exercise 3.1 (iii). Given a non-zero element $a + b\sqrt{2}$, express $1/(a + b\sqrt{2})$ in the form $c + d\sqrt{2}$ where $c, d \in \mathbb{Q}$. Prove that multiplication makes $\mathbb{Q}(\sqrt{2}) - \{0\}$ into a group.

Solution. For all non-zero elements $a + b\sqrt{2}$, write

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} + \frac{-b}{a^2 - 2b^2}\sqrt{2}.$$

Note that $a^2 \neq 2b^2$ for any $a, b \in \mathbb{Q}$ other than $a = b = 0$, because of the irrationality of $\sqrt{2}$.

Note that multiplication of real numbers is associative, and that $1 = 1 + 0\sqrt{2}$ serves as an identity element since $1(a+b\sqrt{2}) = a+b\sqrt{2} = (a+b\sqrt{2})1$. Furthermore, every non-zero element $a+b\sqrt{2}$ has a multiplicative inverse as indicated above. This proves that $\mathbb{Q}(\sqrt{2})-\{0\}$ is a group under multiplication.

Exercise 3.3 Let n be a positive integer and let G consist of all those complex numbers z which satisfy $z^n = 1$. Show that G forms a group under multiplication of complex numbers.

Solution. Note that multiplication of complex numbers is associative, and that 1 serves as an identity element. Multiplication is closed since if $x^n = y^n = 1$, $(xy)^n = 1$. Given a complex number $z \in G$, we have its multiplicative inverse z^{n-1} since $zz^{n-1} = 1 = z^{n-1}z$. Thus, G is a group under multiplication of complex numbers.

Exercise 3.4 Vary n in the previous exercise and check that the union of all these groups

$$\bigcup_{n=1}^{\infty} \{z \in \mathbb{C} : z^n = 1\}$$

is also a group under multiplication of complex numbers.

Solution. Let G be the set described above. Note that multiplication of complex numbers is associative, and that 1 serves as the identity element. Furthermore, if $z \in G$, then $z^n = 1$ for some $n \in \mathbb{N}$, which means that z^{n-1} is its multiplicative inverse. Thus, G is a group under multiplication of complex numbers.

Exercise 3.5 Let n be a positive integer. Prove that

$$(x._n y)._n z = x._n (y._n z)$$

for all $x, y, z \in \mathbb{Z}$.

Solution. Using Euclid's Division Lemma, find integers $0 \leq a, b, c \leq n-1$ such that

$$x = pn + a, \qquad y = qn + b, \qquad z = rn + c$$

for integers p, q, r. This gives

$$xy = (pn + a)(qn + b) = pqn + pbn + qan + ab = (pq + pb + qa)n + ab,$$

so $x._n y = xy \pmod n = ab$. Similarly, $y._n z = xy \pmod n = bc$. Thus,

$$(x._n y)._n z = ab._n z = ab(rn + c) \pmod n = (abr)n + abc \pmod n = abc,$$

and

$$x._n (y._n z) = x._n bc = (pn + a)bc \pmod n = (pbc)n + abc \pmod n = abc.$$

Exercise 3.6 Verify that each of the sets

$$\{1, 3, 7, 9, 11, 13, 17, 19\}$$
$$\{1, 3, 7, 9\}$$
$$\{1, 9, 13, 17\}$$

forms a group under multiplication modulo 20.

Solution. Verifying that a set forms a group comes down to furnishing a complete multiplication table, and ensuring that every row and column contains every element exactly once.

(i)

$\cdot_{20}$	1	3	7	9	11	13	17	19
1	1	3	7	9	11	13	17	19
3	3	9	1	7	13	19	11	17
7	7	1	9	3	17	11	19	13
9	9	7	3	1	19	17	13	11
11	11	13	17	19	1	3	7	9
13	13	19	11	17	3	9	1	7
17	17	11	19	13	7	1	9	3
19	19	17	13	11	9	7	3	1

(ii) Note that $3^{-1} = 7$, $7^{-1} = 3$, $9^{-1} = 9$.

(iii) Note that $9^{-1} = 9$, $13^{-1} = 17$, $17^{-1} = 13$.

Exercise 3.7 Which of the following sets form groups under multiplication modulo 14?

$$\{1, 3, 5\} \qquad \{1, 3, 5, 7\}$$
$$\{1, 7, 13\} \qquad \{1, 9, 11, 13\}$$

Solution. Note that associativity of multiplication modulo 14 holds in all cases, and 1 serves as the identity element. The set $\{1, 3, 5\}$ forms a group since $3^{-1} = 5$, $5^{-1} = 3$. Similarly, the set $\{1, 9, 11, 13\}$ forms a group since $9^{-1} = 11$, $11^{-1} = 9$, $13^{-1} = 13$. Neither set containing 7 forms a group, since 7 has no inverse modulo 14; if $7x \pmod{14} = 1$, then $7x = 14n + 1$ for some integer n, which is impossible since $7x$ is a positive multiple of 7 but $14n + 1$ is not.

Exercise 3.8 Show that if a subset of $\{1, 2, \ldots, 21\}$ contains an even number, or contains the number 11, then it cannot form a group under multiplication modulo 22.

Solution. Suppose that $n = 2m \in G \subseteq \{1, 2, \ldots, 21\}$ is even. For G to be a group, it must contain the multiplicative inverse of n, i.e. some element $x \in G$ such that $nx \pmod{22} = 1$. This means that $nx = 22k + 1$ for some integer k, which is impossible since $nx = 2mx$ is even but $22k + 1 = 2(11k) + 1$ is odd.

Similarly, suppose that $11 \in G$. Again, G must contain a multiplicative inverse of 11, i.e. some $x \in G$ such that $11x \pmod{22} = 1$. This means that $11x = 22k + 1$ for some integer k, which is impossible since $11x$ is a multiple of 11 but $22k + 1 = 11(2k) + 1$ is not.

Exercise 3.9 Let p be a prime number and let x be an integer which satisfies $1 \leq x \leq p - 1$. Show that none of x, $2x$, $\ldots$, $(p - 1)x$ is a multiple of p. Deduce the existence of an integer z such that $1 \leq z \leq (p - 1)$ and $xz \pmod{p} = 1$.

Solution. Let $1 \leq x \leq p-1$ and let $1 \leq k \leq p-1$ such that kx is a multiple of p, i.e. $kx = mp$ for some positive integer m. Since $p \mid mp$, we must have $p \mid kx$. However, neither x nor k can contain p as a prime factor, since they are strictly less than p. This means that the prime factorisation of kx contains no factors of p; no factors of p can be introduced by the multiplication of factors from k and x since p is prime. This is a contradiction, which means that none of x, $2x$, $\ldots$, $(p - 1)x$ is a multiple of p.

Consider the elements 1, x, $2x$, $\ldots$, $(p-1)x$. We have p of them, but there are $p-1$ possible remainders modulo p, which means that two of these elements share the same remainder modulo p by the pigeon-hole principle. If we have $mx = nx \pmod{p}$ for $m > n$ and $1 \leq m, n \leq p - 1$, then $(m - n)x = 0 \pmod{p}$. This is not possible since $1 \leq m - n \leq p - 1$ so $(m - n)$ cannot be a multiple of p. The only remaining possibility is that $zx = 1 \pmod{p}$ for some $1 \leq z \leq p - 1$.

Exercise 3.10 Use the results of Exercises 3.5 and 3.9 to verify that multiplication modulo n makes $\{1, 2, \ldots, n - 1\}$ into a group if n is prime. What goes wrong when n is not a prime number?

Solution. The result of Exercise 3.5 guarantees associativity of multiplication modulo n, and it is clear that 1 serves as an identity element. The result of Exercise 3.9 guarantees that every element $x \in \{1, 2, \ldots, n - 1\}$ has a corresponding multiplicative inverse x^{-1}, with $xx^{-1} = 1 \pmod{n}$ when n is prime. Thus, this set forms a group.

When n is not a prime number, certain elements fail to have multiplicative inverses as seen in Exercises 3.7 and 3.8. Specifically, the factors of n not equal to 1 or n do not have multiplicative inverses. This is clear since if $n = mk$ for $m, k \neq 1$, and $mx = 1 \pmod{n}$ for some $1 \leq x \leq n-1$, then $mx = n\ell + 1 = mk\ell + 1$ for some integer ℓ, which is impossible since mx is a multiple of m but $mk\ell + 1 = m(k\ell) + 1$ is not.