Solutions to odd-numbered exercises
Peter J. Cameron, *Introduction to Algebra*, Chapter 3

3.1 (a) Yes; (b) No; (c) No; (d) No; (e) Yes; (f) Yes; (g) Yes; (h) No; (i) Yes.

Comments: (a) is the additive group of the Boolean ring; (e) is a subgroup of the multiplicative group of $\mathbb{R}$; and (f) is a subgroup of the multiplicative group of $\mathbb{C}$ (apply the subgroup test).

(b) This example satisfies the closure and associative laws. Is there a set E such that $A \cup E = A$ for every subset A of X? Yes; in fact the only such subset is the empty set (for $\emptyset \cup E = \emptyset$ implies that $E = \emptyset$). But now, as long as X is not itself empty, we see that the inverse law holds: there is no set A such that $X \cup A = \emptyset$, since $X \cup A$ is at least as big as X. So this example is not a group as long as $X \neq \emptyset$. [If it happens that $X = \emptyset$, then $\mathscr{P}(X)$ has just one element, namely $\emptyset$, and we have the trivial group with one element.]

(c) The associative law fails. For example, if $A = B = C = \{1\}$, then

$$\begin{aligned} A \setminus (B \setminus C) &= \{1\} \setminus \emptyset = \{1\}, \\ (A \setminus B) \setminus C &= \emptyset \setminus \{1\} = \emptyset. \end{aligned}$$

(d) The inverse law fails: the identity element is 1, and 0 has no inverse.

The proof of (g) by direct calculation is quite difficult. A trick makes it easier. Use the hyperbolic tangent function $\tanh(x) = (\mathrm{e}^x - \mathrm{e}^{-x})/(\mathrm{e}^x + \mathrm{e}^{-x})$. This function is strictly increasing and maps $\mathbb{R}$ onto the interval $(-1, 1)$; and it satisfies the equation

$$\tanh(x+y) = \frac{\tanh x + \tanh y}{1 + \tanh x \tanh y}.$$

So it is an isomorphism from the additive group $(\mathbb{R}, +)$ to $(G, \circ)$ (in the case $c = 1$); this structure, being isomorphic to a group, must itself be a group. For an arbitrary value of c, simply rescale (use the function $c \tanh x$).

3.3. Call the matrices I, A, B, C, D, E. Construct a Cayley table. (This involves a fair amount of work.) From the Cayley table we read off the closure law, the identity law (I is the identity), and the inverse law. The associative law holds because matrix multiplication is associative. So the matrices do form a group.

It is not abelian: again, two non-commuting matrices can be found from the Cayley table. (For example, $AC = D$ but $CA = E$.)

3.5. $U(R)$ is infinite. For $(1+\sqrt{2})(-1+\sqrt{2}) = 1$, so $1+\sqrt{2}$ is a unit. Then all its powers are units, and clearly they are all distinct.

3.7. (a) If $gh = hg$ then $ghgh = gghh$, and conversely (cancelling g from the left and h from the right).

(b) Since $g^{-1}h^{-1} = (hg)^{-1}$, the result is clear.

(c) Suppose that $(gh)^n = g^n h^n$ holds for $n = m, m+1, m+2$. The equatins for $n = m, m+1$ give

$$g^{n+1}h^{n+1} = (gh)^n gh = g^n h^n gh.$$

Cancelling g^n from the left and h from the right, we see that $gh^n = h^n g$, that is, g commutes with h^n. Simimlarly, the equations for $m = n+1, n+2$ show that g commutes witth h^{n+1}. So g commutes with $h^{n+1}h^{-n} = h$, as required. (The last step can be done by direct calculation, or by showing that the set of elements which commute with g (the so-called *centraliser* of g) is a subgroup.)

3.9. We are given (G0) and (G1) and half of each of the conditions (G2) and (G3), and have to prove the other half. That is, we must show that $g \circ e = g$ (in (b)) and $g \circ h = e$ (in (c)).

We prove the second of these things first. Given $g \in G$, let $h \in G$ be as in (c). Also by (c), there exists $k \in G$ with $k \circ h = e$. Now we have

$$(k \circ h) \circ (g \circ h) = e \circ (g \circ h) = g \circ h,$$
$$k \circ ((h \circ g) \circ h) = k \circ (e \circ h) = k \circ h = e,$$

and these two expressions are equal by the Associative Law.

Now, if h is as in (c), we have

$$g \circ e = g \circ (h \circ g) = (g \circ h) \circ g = e \circ g = g.$$

3.11. Recall that, if $n > 0$, then g^n is defined by induction: $g^1 = g$ and $g^{n+1} + g^n \cdot g$. Also, $g^0 = 1$ and $g^{-m} = (g^m)^{-1}$ for $m > 0$. Alternatively, if $n > 0$, then g^n is the product of n factors equal to g, and if $n < 0$, it is the product of $-n$ factors equal to g^{-1}. The last form is the most convenient. (Here we implicitly used that $(g^n)^{-1} = (g^{-1})^n$. This holds because $g^n \cdot (g^{-1})^n$ is the product of n factors g followed by n factors g^{-1}; everything cancels, leaving the identity.)

To prove that $g^{m+n} = g^m \cdot g^n$, there are nine different cases to consider, according to whether m and n are positive, zero or negative. If one or other of them is zero, the result is easy: for example,

$$g^{m+0} = g^m = g^m \cdot 1 = g^m \cdot g^0.$$

This leaves four cases. If $m, n > 0$, then $g^m \cdot g^n$ is the product of m factors g followed by the product of n factors g, which is the product of $m+n$ factors g, that is, g^{m+n}. Suppose that m is positive and n negative, say $m = -r$. Then $g^m \cdot g^n$ is the product of m factors g followed by r factors g^{-1}. If $m \geq r$, then r of the gs cancel all the g^{-1}s, leaving $g^{m-r} = g^{m+n}$. If $m < r$, then m of the g^{-1}s cancel all the gs, leaving $(g^{-1})^{r-m} = g^{-(r-m)} = g^{m+n}$. The argument is similar in the other two cases.

The proof of $(g^m)^n = g^{mn}$ also divides into a number of cases. When m or n is zero, both sides are the identity. When m and n are positive, then $(g^m)^n$ is the product of n terms, each the product of m factors g, giving the result g^{mn}. The case $m < 0$ and $n > 0$ is similar with factors g^{-1} instead. If $m > 0$ and $n < 0$, say $n = -r$, then $(g^m)^n = (g^m)^{-r}$ is the product of r factors equal to $(g^m)^{-1} = (g^{-1})^m$, so is the product of mr factors g^{-1}; thus it is equal to $g^{-mr} = g^{mn}$. The last case is left to the reader.

Finally, suppose that $gh = hg$ and consider $(gh)^n$. If $n > 0$, this is the product of n factors gh, which can be rearranged with all the gs at the beginning to give $g^n \cdot h^n$ as required. If $n < 0$, say $n = -r$, we have

$$(gh)^n = (gh)^{-r} = (hg)^{-r} = ((hg)^r)^{-1} = (h^r g^r)^{-1}$$
$$= (g^r)^{-1}(h^r)^{-1} = g^{-r}h^{-r} = g^n h^n.$$

(We use the fact that $(xy)^{-1} = y^{-1}x^{-1}$ here.) Finally, if $n = 0$, then both sides are the identity.

sol3.13. We claim that, for any $g \in G$, the set gHg^{-1} is a subgroup of G. [Apply the Subgroup Test: take two elements of gHg^{-1}, say gxg^{-1} and gyg^{-1}, where $x,y \in H$. Then

$$(gxg^{-1})(gyg^{-1})^{-1}) = gxg^{-1} \cdot gy^{-1}g^{-1} = g(xy^{-1})g^{-1} \in gHg^{-1},$$

since $xy^{-1} \in H$.]

Now the left coset gH of H is equal to $(gHg^{-1})g$, which is a right coset of the subgroup gHg^{-1}.

3.15. (a) Lagrange's Theorem: if G contains an element of order 2, then 2 divides the order of G.

(b) As suggested, let $x_1, y_1, x_2, y_2, \dots, x_m, y_m$ be the elements of G which are not equal to their inverses, with the notation chosen so that $x_i^{-1} = y_i$ for $i = 1, \dots, m$; and let $z_1, \dots, z_r$ be the elements equal to their inverses. Then $|G| = 2m + r$. If $|G|$ is even, then r is even. But the identity is equal to its inverse, so $r \geq 1$. Hence $r \geq 2$, and there is at least one non-identity element z_i, say z. Then $z = z^{-1}$, so $z^2 = 1$; since $z \neq 1$, z has order 2.

3.17 We know that an element $x \in \mathbb{Z}_m$ is a unit if and only if $\gcd(x,m) = 1$ (by Proposition 2.15). The number of units in $\mathbb{Z}_m$ is thus equal to $\phi(m)$; in other words, $\phi(m)$ is the order of the group $U(\mathbb{Z}_m)$ of units of $\mathbb{Z}_m$.

By Theorem 3.6(c), $x^{\phi(m)} = 1$ in $\mathbb{Z}_m$, in other words, $x^{\phi(m)} \equiv_m 1$.

Suppose that $m = p$ is a prime number. Then all the non-zero elements $1, \dots, p-1$ of $\mathbb{Z}_p$ are units, since the only possible common divisor with p would be p itself, and none of these are divisible by p. So $\phi(p) = p - 1$, and $x^{p-1} \equiv_p 1$ if $x \not\equiv_p 0$. Multiplying both sides by x we see that $x^p \equiv_p x$ if $x \not\equiv_p 0$. But this congruence holds also if $x \equiv_p 0$; so it holds for all elements of $\mathbb{Z}_p$, in other words, all integers x satisfy $x^p \equiv_p x$.

3.19 We show first that the group G is isomorphic to the group G_1 consisting of all transformations of F of the form $\theta_{a,b} : x \mapsto ax + b$, where $a, b \in F$ and $a \neq 0$. Clearly for every matrix there is such a transformation, so the map is a bijection. We check the homomorphism property:

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c & d \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} ac & ad+b \\ 0 & 1 \end{pmatrix},$$

while

$$\theta_{a,b}\theta_{c,d} : x \mapsto (cx + d) \mapsto a(cx + d) + b = acx + (ad + b),$$

in other words,

$$\theta_{a,b}\theta_{c,d} = \theta_{ac,ad+b}.$$

Now suppose that $F = \mathbb{Z}_3$. Then G_1 is a group with $2 \times 3 = 6$ elements (since there are 2 choices for a and 3 for b), each element of which is a permutation of F. Since the symmetric group on F has only six elements, we must have $G_1 = S_3$, and so G is isomorphic to S_3.

3.21 The fact that $G/Z(G)$ is cyclic, generated by $Z(G)g$, means that $G/Z(G)$ (the set of cosets of $Z(G)$ in G) consists of all the powers $(Z(G)g)^i = Z(G)g^i$. So every coset has this form. Now every element $h \in G$ lies in a unique coset of $Z(G)$, of the form $Z(G)g^i$ for some i; thus $h = zg^i$ for some $z \in Z(G)$.

Take two elements h_1 and h_2 of G; say $h_1 = z_1g^i$ and $h_2 = z_2g^j$ for some $z_1, z_2 \in Z(G)$ and $i, j \in \mathbb{Z}$. Then

$$h_1h_2 = z_1g^i \cdot z_2g^j = z_1z_2g^{i+j} = z_2z_1g^{i+j} = z_2g^j \cdot z_1g^i = h_2h_1,$$

where for the second inequality we use the fact that z_2 commutes with g^i; for the third, the fact that z_1 and z_2 commute; and for the fourth, the fact that z_1 commutes with g^i. Thus h_1 and h_2 commute. Since they were arbitrary elements of G, we see that G is abelian, and indeed $G = Z(G)$.

3.23 The group S_3 has order 6. By Lagrange's Theorem, any subgroup has order 1, 2, 3 or 6. The only subgroup of order 1 is $\{1\}$, and the only subgroup of order 6 is S_3. So we have to look for subgroups of orders 2 and 3. Note that, as well as the identity, S_3 contains two elements of order 3 (viz. $(1,2,3)$ and $(1,3,2)$), which are inverses of each other, and three elements of order 2 (viz. $(1,2)$, $(1,3)$ and $(2,3)$).

Again by Lagrange, if H is a subgroup of order 3, then every element of H must have order 1 or 3. There are only three such elements altogether, namely 1, $(1,2,3)$ and $(1,3,2)$; so these form the only possible such subgroup. But this set is indeed a subgroup. So there is one subgroup of order 3.

If K is a subgroup of order 2, then any element of K has order 1 or 2; K must contain the identity, so must consist of the identity and a single element of order 2. Thus there are three possibilities for K, and it is routine to check that each of them is a subgroup.

So there are altogether six subgroups of S_3.

3.25 Note that, since N is a normal subgroup of G, for any elements $n \in N$ and $g \in G$, there exists $n' \in N$ such that $gn = n'g$. (This is because gn lies in the left coset gN, which equals the right coset Ng.)

We apply the first subgroup test.

- Take two elements of NH, say n_1h_1 and n_2h_2, where $n_1, n_2 \in N$ and $h_1, h_2 \in H$. Their product is

  $$(n_1h_1) \cdot (n_2h_2) = n_1(h_1n_2)h_2 = n_1(n'h_1)h_2 = (n_1n')(h_1h_2) \in NH,$$

  where n' is some element of N.

- Take an element $nh \in NH$. Its inverse is

  $$(nh)^{-1} = h^{-1}n^{-1} = n'h^{-1} \in NH,$$

  for some $n' \in N$.

So NH is a subgroup of G.

(a) True. If also H is a normal subgroup of G, take any $nh \in NH$ and $g \in G$; we have

$$g(nh) = (gn)h = (n'g)h = n'(gh) = n'(h'g) = (n'h')g,$$

so left and right cosets of NH are equal.

(b) False. Let $G = S_3$, $N = A_3 = \{1,(1,2,3),(1,3,2)\}$ and $H = \{1,(1,2)\}$. (See Exercise 3.23.) Then $NH = G$, so NH is certainly a normal subgroup of G; but H is not a normal subgroup.

3.27 (a) Suppose that G is a group of finite order n which has just two conjugacy classes. One of these classes consists of the identity; so the other has size $n-1$. Now the size of a conjugacy class is the index of the centraliser of one of its elements, and so divides $|G|$ (see Theorem 3.21); so $n-1$ divides n. It follows that $n-1$ divides $n-(n-1) = 1$; so $n-1 = 1$, and $n = 2$, $G \cong C_2$.

The hint suggests using the class equation, which would say

$$\frac{1}{n} + \frac{1}{k} = 1,$$

where k is the order of the centraliser of a non-identity element. This equation has only the solution $n = n_1 = 2$. [Why?]

(b) Show directly that the conjugacy classes in S_3 are $\{1\}$, $\{(1,2,3),(1,3,2)\}$, and $\{(1,2),(1,3),(2,3)\}$. (Elements in different sets in this list have different orders and so cannot be conjugate; your job is to show that elements in the same set are conjugate.) The class equation in this case becomes

$$\frac{1}{6} + \frac{1}{3} + \frac{1}{2} = 1.$$

(c) Suppose that G has three conjugacy classes, and has order n; let k and l be the orders of the centralisers of elements in the other two classes. Then

$$\frac{1}{n} + \frac{1}{k} + \frac{1}{l} = 1.$$

If three "unit fractions" sum to 1, then the largest of them is at least $1/3$; so, without loss of generality, $l = 2$ or $l = 3$. If $l = 3$, then the only possibility is $1/3+1/3+1/3 = 1$, so $|G| = 3$ (and the cyclic group of order 3 does indeed have three conjugacy classes). If $l = 2$, then $1/n + 1/k = 1/2$, so $k \leq 4$. We have two possible solutions; $(n,k,l) = (4,4,2)$ and $(n,k,l) = (6,3,2)$. So indeed $|G| \leq 6$. But indeed the solution $(4,4,2)$ is impossible, since a group of order 4 is abelian and so has four conjugacy classes. So there are just two finite groups with three conjugacy classes.

(d) This will be a "non-constructive" proof; that is, we will prove that the function exists without actually finding any information about it. As a harder exercise, you are encouraged to find estimates for the value of $f(r)$.

We start with the class equation for a group with r conjugacy classes:

$$\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_r} = 1,$$

where $n_1,\ldots,n_r$ are the orders of centralisers of elements in the conjugacy classes. Note that the group order is the largest of the numbers $n_1,\ldots,n_r$ (since the centraliser of the indentity is the whole group). So the result will follow if we can show that, given

r, this equation has only a finite number of solutions: then we can take $f(r)$ to be the largest number appearing in any such solution.

In order to prove this, we use induction on r, but we have to prove a more general statement:

Lemma *Given any positive integer r and rational number q, there are only finitely many r-tuples $(n_1, n_2, \dots, n_r)$ of natural numbers such that*

$$\frac{1}{n_1} + \frac{1}{n_2} + \cdots + \frac{1}{n_r} = q.$$

For $q = 1$ this gives the desired conclusion.

Proof The proof is by induction on r. For $r = 1$, the equation has one solution if q is the reciprocal of a natural number and none otherwise.

Suppose that the lemma is true for $r-1$. Consider any solution of the equation with the given values of q and r. If n_r is the smallest of the numbers n_i, then $1/n_r$ is the largest fraction, so it is at least as great as the average q/r; so $n_r \le r/q$.

Now for each possible value of n_r in the range $[1, r/q]$, we have the equation

$$\frac{1}{n_1} + \cdots + \frac{1}{n_{r-1}} = q - \frac{1}{n_r},$$

and by the induction hypothesis, each of these equations has only finitely many solutions. So there are only finitely many solutions altogether.

Remark Note how the argument forced us to prove a more general result; even though we are really interested in equations with right-hand side equal to 1, we have to allow other values in order to use induction.

3.29 Construct a Cayley table for the four elements.

3.31 How many times does the element g_i occur in row r of the table? If such an occurrence occurs in column s, then

$$g_r g_s = g_i,$$

so $g_s = g_r^{-1} g_i$. So there is exactly one position in row r where g_i appears. The argument for columns is similar.

3.33 (a) *First proof:* Let $C_2 = \{1, g\}$, where $g^2 = 1$. The Cayley table for $C_2 \times C_2$ is

$\circ$	$(1,1)$	$(1,g)$	$(g,1)$	(g,g)
$(1,1)$	$(1,1)$	$(1,g)$	$(g,1)$	(g,g)
$(1,g)$	$(1,g)$	$(1,1)$	(g,g)	$(g,1)$
$(g,1)$	$(g,1)$	(g,g)	$(1,1)$	$(1,g)$
(g,g)	(g,g)	$(g,1)$	$(1,g)$	$(1,1)$

which is easily matched up with the Cayley table for V_4.

Second proof: $C_2 \times C_2$ is a group of order 4 which is easily seen to have no elements of order 4; so it is not isomorphic to C_4, and must be isomorphic to V_4 (see p.132).

(b) *First proof:* Let C_2 be as in (a), and $C_3 = \{1, h, h^2\}$, with $h^3 = 1$. The order of $(g,h) \in C_2 \times C_3$ must divide 6; it is not 2 (since $(g,h)^2 = (1,h^2)$), and is not 3 (since $(g,h)^3 = (g,1)$); so it has order 6, and generates the cyclic group.

Second proof: By the preceding exercise, $C_2 \times C_3$ is an abelian group of order 6. Now apply the classification on p.133.

See p.134. C_8 is obtained if there is an element of order 8, and $C_2 \times C_2 \times C_2$ if there is no element of order 4. We obtain $C_2 \times C_4$ in the case where $b^2 = 1$ and $ba = ab$, and also in the case where $b^2 = a^2$ and $ba = ab$.

3.35 (a) As in the first proof in Exercise 3.33(b), let $C_p = \langle g \rangle$ and $C_q = \langle h \rangle$. Then the element (g,h) of $C_p \times C_q$ has order dividing pq, but not p or q; so its order is pq, and the group is cyclic.

(b) In $C_p \times C_p$, every element has order 1 or p; so the group is not cyclic.

3.37 For convenience we represent the elements of G by permutations, as on p.139. Check that $z = (1,3)(2,4)$ commutes with all elements of G. (In fact, we know that every element of G can be written in the form $a^i b^j$, where $a = (1,2,3,4)$ and $b = (1,4)(2,3)$ (see the analysis on p.134); so it is enough to show that z commutes with a and b.) So the subgroup $Z = \{1, z\}$ is contained in $Z(G)$.

If $Z(G)$ were larger than Z, then its order would be 4 or 8, so that $G/Z(G)$ would have order 1 or 2, and would be cyclic; by Exercise 3.21, G would be abelian, which it is not. So $Z(G) = Z$. (You can check this directly by showing that for any element $g \in G$ apart from 1 and z, there is an element $h \in G$ which does not commute with g.)

Now the only elements of order 4 in G are a and a^3, and $a^3 = za$, so $Za = Za^3$, and $(Za)^2 = Z$. Thus the factor group G/Z is a group of order 4 in which no element has order greater than 2, and is necessarily the Klein group. (More simply, invoke Exercise 3.21 again to see that $G/Z(G)$ cannot be cyclic.)

3.39 Take $m \in M$ and $n \in N$. Consider the element $g = m^{-1}n^{-1}mn$, the so-called *commutator* of m and n. Writing it as $m^{-1}(n^{-1}mn)$, we see that it is the inverse of m times a conjugate of m; both of these lie in M, so $g \in M$. Similarly, writing it as $g = (m^{-1}n^{-1}m)n$, we see that $G \in N$. Since $M \cap N = \{1\}$, we see that $g = 1$, so that $mn = nm$.

Since $G = MN$, every element of G can be written in the form $g = mn$ for $m \in M$ and $n \in N$. Suppose we have another representation, $g = m'n'$ with $m' \in M$ and $n' \in N$. Then $mn = m'n'$. Multiplying this equation on the left by $(m')^{-1}$ and on the right by n^{-1}, we obtain $(m')^{-1}m = n'n^{-1}$. The left-hand expression lies in M and the right-hand one in N; so both are the identity, giving $m = m'$ and $n = n'$.

Now define a map θ from G to $M \times N$ by

$$\theta : mn \in G \mapsto (m,n) \in M \times N.$$

By what we just proved, this map is well-defined. Clearly it is one-to-one and onto. Also, if $mn, m'n' \in G$ (with $m, m' \in M$ and $n, n' \in N$), then $(mn)(m'n') = (mm')(nn')$ by what we showed in the first paragraph; so

$$\begin{aligned} ((mn)(m'n'))\theta &= ((mm')(nn'))\theta = (mm', nn'), \\ (mn)\theta \cdot (m'n')\theta &= (m,n)(m',n') = (mm', nn'), \end{aligned}$$

where the last equation is the definition of the group operation in $M \times N$. So θ is an isomorphism.

Let N be the rotation group of the cube and $M = \{\pm I\}$. Since every rotation has determinant 1, we have $M \cap N = \{I\}$. Also, $|G| = 48$, $|N| = 24$ and $|M| = 2$, so $|MN| = |G|$ and $MN = G$. Moreover, both M and N are normal subgroups (N because it has index 2, and M because its elements commute with everything so it is in $Z(G)$). So the conditions of the first part of the exercise are satisfied, and we conclude that $G \cong M \times N$.

3.41 The first part of this exercise is “obvious” from playing with a model. It could of course be proved by coordinate geometry but I do not expect you to do this!

Clearly any rotation maps a frame to a frame, so induces a permutation on the set of five frames. Could a rotation fix every frame? Again, a few moments’ playing with a model shows that only the identity does so. So the map from the rotation group G to the group S_5 of permutations of the frames is a one-to-one homomorphism. Its image is a subgroup of S_5 having order 60, so a normal subgroup, necessarily A_5.