Chapter 3 solutions

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

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 $\mathbf{R}$ 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 $(\mathbf{R},+)$ to $(G,\circ)$ (in the case $c = 1$); this structure, being isomorpphic to a group, must itself be a group. For an arbitrary vallue of c, simply rescale (use the function $c \tanh x$).

3.2. (a) $(1\ 2)(1\ 3) = (1\ 2\ 3)$ and $(1\ 3)(1\ 2) = (1\ 3\ 2)$.

(b) The permutations given in (a) actually belong to S_n for any $n \geq 3$.

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 $CA = E$.)

3.4. What does $AA^{-1} \subseteq A$ mean? It means that the set of all elements ab^{-1}, for $a,b \in A$, is a subset of A; in other words, for any $a,b \in A$, we have $ab^{-1} \in A$. But this is precisely the condition of the Second Subgroup Test!

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.

3.6. Closure: If $x,y \in S$ then $(xy)^2 = xyxy = xxyy = 1 \cdot 1 = 1$, where we used the commutativity to show $xyxy = xxyy$. So $xy \in S$.

Associative law: This holds in general for multiplication in a ring.

Identity law: We are given that R has an identity 1 which satisfies $1^2 = 1$, so $1 \in S$.

Inverse law: Every element of S is its own inverse.

Commutative law: We are given that multiplication in R is commutative.

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.)

3.8. The automorphism group of R consists of permutations, that is, it is a subset of the symmetric group. The operation is composition, as in the symmetric group. And, as we showed, it forms a group in its own right. So it is a subgroup of the symmetric group. (There is nothing special here in the fact that R is a ring. The same would hold for the automorphism group of any object whatever.)

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

$$\begin{aligned}(k \circ h) \circ (g \circ h) &= e \circ (g \circ h) = g \circ h, \\ k \circ ((h \circ g) \circ h) &= k \circ (e \circ h) = k \circ h = e,\end{aligned}$$

and these two expressions are equal by the Associative Law.

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

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

3.10. Take G to be any set with more than one element, and define the operation $\circ$ as suggested, that is, $g \circ h = h$ for all $g, h \in G$. Clearly the closure law (G0) holds. For the associative law, we have

$$\begin{aligned}&g \circ (h \circ k) = h \circ k = k, \\ &(g \circ h) \circ k = k.\end{aligned}$$

Take any element $e \in G$; then we have $e \circ g = g$ for all $g \in G$. Now, for any $g \in G$, take $h = e$, and we have $g \circ h = h = e$. So all the conditions hold. But G is not a group; for, if $x \neq y$, then $x \circ y = y \circ y = y$, and so the cancellation law fails.

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

$$\begin{aligned}(gh)^n &= (gh)^{-r} = (hg)^{-r} = ((hg)^r)^{-1} = (h^r g^r)^{-1}\\ &= (g^r)^{-1}(h^r)^{-1} = g^{-r}h^{-r} = g^n h^n.\end{aligned}$$

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

3.12 The surprising conclusion is that the elements a, b, c, d, e all have order 11, and so the order of G is divisible by 11 (by Lagrange's Theorem). The proof is "elementary" (no theory is used), but the manipulations are not easy to find!

From the given equations, we obtain $c = ab$, $d = bab$, $e = ab^2ab$, and so

$$\begin{aligned} a &= babab^2ab && (1)\\ b &= ab^2aba && (2)\end{aligned}$$

Multiply equation (1) on the right by a and use (2) to get

$$a^2 = bab(ab^2aba) = bab^2 \qquad (3)$$

Multiply equation (1) on the left by ab to get

$$aba = (ab^2aba)b^2ab = b^3ab \qquad (4)$$

From (2) and (4),

$$b = ab^2aba = ab^5ab \qquad (5)$$

Cancelling b gives $ab^5a = 1$, so $b^5 = a^{-2}$, or

$$a^2 = b^{-5} \qquad (6)$$

Now (3) gives $b^{-5} = bab^2$, so

$$a = b^{-8} \qquad (7)$$

Combining (6) and (7) gives

$$b^{-5} = a^2 = b^{-16},$$

so $b^{11} = 1$. Since $b \neq 1$, we conclude that b has order 11. Now everything can be expressed in terms of b:

$$a = b^{-8} = b^3,\ c = ab = b^4,\ d = bc = b^5,\ e = cd = b^9.$$

3.13. 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}.

3.14. (a) Suppose that $n_1, n_2 \in I$, so that $g^{n_1} = g^{n_2} = 1$. Then $g^{n_1-n_2} = g^{n_1}(g^{n_2})^{-1} = 1$, so $n_1 - n_{\in} I$

Suppose that $n \in I$ and r is any integer. Then $g^{nr} = (g^n)^r = 1$, so $nr \in I$.

Thus I passes the Ideal Test.

Since $\mathbf{Z}$ is a PID, there is an integer m such that $I = (m)$. We may take $m \geq 0$. This means that *either*

- $m = 0$, whence no power of g except g^0 is the identity, and g has infinite order; *or*

- $m > 0$, in which case $g^n = 0$ if and only if n is a multiple of m, that is, g has order m.

(b)

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 $x_1, y_1, x_2, y_2, \ldots, x_m, y_m$ be the elements of G which are not equal to their inverses, with the notation chosen so that $x_i^{-1} = y_i$ for $i = 1, \ldots, m$; and let $z_1, \ldots, z_r$ 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.

3.16. Follow the hint by taking Ω to be the set of displayed p-tuples. The first $p-1$ elements $g_1, \ldots, g_{p-1}$ can be chosen arbitrarily, and g_p is then forced to be the inverse of their product. So $|\Omega| = |G|^{p-1}$, and in particular $|\Omega|$ is a multiple of p.

If $g_1 g_2 \cdots g_p = 1$, then $g_1 = (g_2 \cdots g_p)^{-1}$, and so $g_2 \ \cdots g_p g_1 = 1$. Thus the cyclic permutation π does indeed take any member of Ω to another. Since π^p is the identity, each cycle of π on Ω has length 1 or p. Because of the divisibility by p, the number of fixed points is also a multiple of p.

If $(g_1, \ldots, g_p)$ is fixed by π, then

$$(g_1, g_2, \ldots, g_p) = (g_2, \ldots, g_p, g_1),$$

and so $g_1 = g_2 = \ldots = g_p = g$, say. Since this element belongs to Ω, we have $g^p = 1$. So the number of elements satisfying $g^p = 1$ is a multiple of p. One of these is the identity; the rest all have order p. We conclude that G contains elements of order p, as required.

3.17. (a) Show that G is a subgroup of the general linear group (the group of non-singular matrices) by applying the Subgroup Test.

(b) Define a map θ from G to the multiplicative group of F by

$$\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \theta = a.$$

It is straightforward to verify that θ is a homomorphism. Its kernel is the set of matrices in G with $a = 1$, that is, N (which is thus a normal subgroup of G).

To show that N is isomorphic to the additive group of F, we define another map ϕ from N to the additive group by

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \phi = b,$$

and verifying that this is a homomorphism; it is clearly a bijection.

(c) This is done by restricting the map θ to H and noting that the result is a bijection.

(d) By the First Isomorphism Theorem, G/N is isomorphic to the multiplicative group of F, which is itself isomorphic to H.

3.18. G is a group of order 6 (since there are three choices for b, and two for a, since $a \neq 0$). One can check directly from Cayley tables that the map θ given by

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \theta = (1), \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \theta = (1\,2\,3), \quad \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \theta = (1\,3\,2),$$
$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \theta = (1\,2), \quad \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix} \theta = (2\,3), \quad \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix} \theta = (1\,3),$$

is an isomorphism.

In Section 2.4, you will see that any non-abelian group of order 6 is isomorphic to S_3.

3.19 You have to verify the group axioms. Closure is clear since, if $a_1, a_2 \neq 0$, then $a_1a_2 \neq 0$. The identity is easily checked to be $(1,0)$ while the inverse of (a,b) is $(1/a, -b/a)$. The associative law involves doing some calculation to show that both $((a_1,b_1)\circ(a_2,b_2))\circ(a_3,b_3)$ and $(a_1,b_1)\circ((a_2,b_2)\circ(a_3,b_3))$ are equal to $(a_1a_2a_3, b_1a_2a_3 + b_2a_3 + b_3)$.

Let $f_{a,b}$ be the permutation of the real numbers which maps x to $ax+b$: that is (writing permutations on the right)

$$x f_{a,b} = ax + b.$$

Now we have

$$x f_{a_1,b_1} f_{a_2,b_2} = (a_1x + b_1) f_{a_2,b_2} = a_2a_1x + a_2b_1 + b_2;$$

that is,

$$f_{a_1,b_1} f_{a_2,b_2} = f_{a_1a_2, b_1a_2+b_2}.$$

Now the permutations of this shape form a subgroup of the symmetric group. (Applying the First Subgroup Test, we have already shown that this set is closed under composition; so it is enough to verify that the inverse of $f_{a,b}$ is $f_{1/1a,-b/a}$, which is again in the set.)

Clearly this group is isomorphic to the ‘group’ G in the first part of the question. So G really is a group!

The saving is that we do not have to verify the associative law (since the composition of permutations is necessarily associative).

3.20. (a) We have

$$(xy)\iota_g = g^{-1}(xy)g = g^{-1}xg\cdot g^{-1}yg = x\iota_g\cdot y\iota_g,$$

so ι_g is a homomorphism. It is a bijection because it has an inverse function $\iota_{g^{-1}}$ (see (b) below).

(b) We have

$$(x\iota_g)\iota_h = h^{-1}g^{-1}xgh = (gh)^{-1}x(gh) = x\iota_{gh},$$

so the set $\{\iota_g : g\in G\}$ is closed under composition. We also see that $\iota_{g^{-1}}$ is the inverse of ι_g (since ι_1 is the identity map), so this set is also closed under inversion, and is a subgroup of the group $\mathrm{Aut}(G)$.

(c) The displayed equation in (b) shows that the map $g\to\iota_g$ is a homomorphism. Clearly it is onto. Its kernel is

$$\{g\in G:\iota_g=1\} = \{g\in G:(\forall x\in G)g^{-1}xg=x\} = Z(G),$$

since $g^{-1}xg=x$ if and only if $xg=gx$. The result follows from the First Isomorphism Theorem.

(d) Let α be any automorphism of G. We claim that $\alpha^{-1}\iota_g\alpha=\iota_{g\alpha}$, where the product on the left of the equation is calculated in the group $\mathrm{Aut}(G)$. This will show that any conjugate of an inner automorphism is an inner automorphism, and hence that the group of inner automorphisms is a normal subgroup of $\mathrm{Aut}(G)$.

We prove the claim by calculating the effect of the composite automorphism on an arbitrary element $x\in G$:

$$\begin{aligned} x\alpha^{-1}\iota_g\alpha &= (g^{-1}x\alpha^{-1}g)\alpha \\ &= g^{-1}\alpha x\alpha^{-1}\alpha g\alpha \\ &= (g\alpha) =^{-1} xg\alpha \\ &= x\iota_{g\alpha}. \end{aligned}$$

3.21 There is

- one subgroup of order 6 (viz. S_3), which is normal;
- one subgroup of order 3 (viz. $\{(1),(1\ 2\ 3),(1\ 3\ 2)\}$), which is normal;
- three subgroups of order 2 (viz. $\{(1),(1\ 2)\}$, $\{(1),(1\ 3)\}$, and $\{(1),(2\ 3)\}$), which are all conjugate, and hence not normal;

- one subgroup of order 1 (viz. $\{(1)\}$), which is normal.

3.22. The *exponential function* $\exp(x) = e^x$ is a bijection between all the reals and the positive reals (its inverse is the *logarithm function* $\log(x)$). It is a homomorphism, since $\exp(x+y) = \exp(x)\cdot\exp(y)$. So it is an isomorphism.

3.23. We apply the subgroup test. If $n_1h_1, n_2h_2 \in NH$, then $(n_1h_1)(n_2h_2)^{-1} = n_1h_1h_2^{-1}n_2^{-1}$. Now N is a normal subgroup, so $h_1h_2^{-1}N = Nh_1h_2^{-1}$. The left-hand side contains $h_1h_2^{-1}n_2^{-1}$, so the right-hand side does also; that is, $h_1h_2^{-1}n_2^{-1} = n_3n_1h_2^{-1}$, for some $n_3 \in N$. Thus we have

$$(n_1h_1)(n_2h_2)^{-1} = n_1n_3h_11h_2^{-1} \in NH$$

as required; so NH is a subgroup.

(a) True. If N and H are normal subgroups, then for any $nh \in NH$ and $g \in G$, we have

$$g^{-1}(hn)g = (g^{-1}ng)(g^{-1}hg) \in NH.$$

(b) False: take, for example, $G = S_3$, and let N and H be subgroups of orders 3 and 2 respectively. Then $NH = G$, but H is not normal.

3.24. (a)

$$\theta(k_1+k_2) = e^{2\pi i(k_1+k_2)/n} = e^{2\pi ik_1/n}\cdot e^{2\pi ik_2/n} = \theta(k_1)\theta(k_2).$$

Its image is G_2, since every nth root of unity has this form. Its kernel is $\{k \in G_1 : e^{2\pi ik/n} = 1\}$, which is the set of all multiples of n.

(b) A coset of $\mathrm{Ker}(\theta)$ is obtained by adding a fixed integer k to every multiple of n, so is a congruence class as claimed. So $G_1/\mathrm{Ker}(\theta)$ is the set of congruence classes modulo n, which comprise the 'integers mod n'.

3.25. Let the sizes of the conjugacy classes be $n_1, \ldots, n_r$, with $n_1 = 1$ (correspoding to the identity). Each n_i divides the order of G, say $n_i = |G|/a_i$. Since $\sum n_i = |G|$, we have

$$\sum \frac{1}{a_i} = 1.$$

The group order is the largest of the numbers a_i.

(a) The only solution of this equation with $r = 2$ is $1/2 + 1/2 = 1$. So a group with 2 conjugacy classes has order 2.

(b) S_3 has three conjugacy classes: the identity, the three transpositions, and the two 3-cycles.

(c) The class equation with $r = 3$ has just three solutions, viz.

$$1 = 1/3+1/3+1/3 = 1/2+1/4+1/4 = 1/2+1/3+1/6.$$

So a group with three classes has order at most 6. If its order is 6, then it is non-abelian and so is isomorphic to S_6. (In fact, the solution $1 = 1/3+1/3+1/3$ coresponds to the cyclic group of order 3, while the solution $1 = 1/2+1/4+1/4$ doesn't correspond to any group, since there is no group of order 4.

(d) We show that the equation $\sum_{i=1}^{r} 1/a_i = 1$ has only a finite number of solutions in positive integers. Then there is a bound on the order of a group with r conjugacy classes, namely, the largest a_i occurring in any solution.

In fact we prove the more general result that, for any x and r, the equation $\sum_{i=1}^{r} 1/a_i = x$ has only finitely many solutions. The proof is by induction on r: there is at most one solution when $r = 1$, so the induction starts.

Suppose that the result is true with $r-1$ replacing r. Now in the given equation, it is not possible that all the numbers a_i are greatr than r/x, or else the sum of their reciprocals would be smaller than r. So one of them, say a_r, is at most r/x, in which case it takes only finitely many values. For each value m of a_r, we have the equation $\sum_{i=1}^{r-1} 1/a_i = x - 1/m$, which by induction has only finitely many solutions. So there are only finitely many solutions altogether.

3.26 Check the ring axioms. Closure requires that the pointwise sum and the composition of endomorphisms are endomorphisms. The zero element is the enromorphism which maps everything to the zero element of A. As an example, the right distributive law is proved as follows:

$$\begin{aligned} a((\theta+\phi)\psi) = (a(\theta+\pi))\psi &= (a\theta + a\phi)\psi = (a\theta)\psi + (a\phi)\psi, \\ a(\theta\psi + \phi\psi) = a(\theta\psi) + a(\phi\psi) &= (a\theta)\psi + (a\phi)\psi. \end{aligned}$$

Note thet the endomorphism ring has an identity (the map which takes every element of A to itself) but is not in general commutative.

3.27. Construct a Cayley table.

3.28. The (i,j) entry of $P(\pi_1)P(\pi_2)$ counts the number of times that there is an index k such that the (i,k) entry of $P(\pi_1)$ and the (k,j) entry of $P(\pi_2)$ are both equal to 1. This requires that $i\pi_1 = k$ and $k\pi_2 = j$. So there is at most one k, and there is such a k if and only if $i\pi_1\pi_= j$. So $P(\pi_1)P(\pi_2) = P(\pi_1\pi_2)$ as required.

For any field F, the map $P : \pi \mapsto P(\pi)$ from an arbitrary subgroup H of the symmetric group S_n to the group of non-singular $n \times n$ matrices over F is one-to-one, and is a homomorphism (by what has just been proved). So $\mathrm{Im}(P)$ is a group of matrices isomorphic to H.

[*Remark:* By Cayley's Theorem it follows that every finite group is isomorphic to a matrix group. Not every infinite group is isomorphic to a matrix group, however.]

3.29. The Cayley table has g_i in row r and column s if and only if $g_r g_s = g_i$. How many times does g_i occur in row r? The answer is the number of values of s such that $g_r g_s = g_i$. But there is exactly one, since necessarily $g_s = g_r^{-1} g_i$ is the unique solution. Similarly g_i occurs just once in column s.

G is abelian if and only if $g_r g_s = g_s g_r$ for all r, s, that is, the element in row r and column s is equal to the element in row s and column r (which is to say that the Cayley table is symmetric).

3.30. Verification of the axioms is straightforward: closure is obvious, a simple calculation proves associativity, the identity is $(1,1)$ (where, note, the first 1 is the identity of G and the second is the identity of H), and the inverse of (g,h) is (g^{-1}, h^{-1}).

The formula for its order is given by Proposition 1.1.

The last part is another simple calculation similar to the proof of associativity.

3.31. (a) Every element (g,h) of $C_2 \times C_2$ satisfies $(g,h)^2 = (g^2,h_2) = (1,1)$.

(b) If $C_2 = \langle a \rangle$, $C_3 = \langle b \rangle$, and $C_6 = \langle c \rangle$, then the map $c^n \mapsto (a^n,b^n)$ is the required isomorphism. (The key point is that, if $(a^n,b^n) = 1$, then $a^n = b^n = 1$, so both 2 and 3 divide n, so 6 divides n, so $c^n = 1$.)

(c) C_8 is the one containing elements of order 8. $C_2 \times C_2 \times C_2$ is the one with no element of order greater than 2.

$C_2 \times C_4$ occurs in two guises: in terms of the discussion, the cases $ab = ba$, $b^2 = 1$ and $ab = ba$, $b^2 = a^2$ both give rise to this group. (Suppose that $a^4 = 1$, $b^2 = 1$, and $ab = ba$. If we had instead chosen $b' = ab$ as an element outside $\langle a \rangle$, then $(b')^2 = a^2$ and $ab' = b'a$.)

3.32. (a) These permutations form the dihedral group, the group of symmetries of a square (acting as a permutation group on the vertices of the square.)

(b) Construct a Cayley table to verify the closure and inverse laws. Associativity and the identity law are clear.

The non-isomorphism is shown by counting elements of order 2: the dihedral group in (a) has five, the quaternion group in (b) has only one.

3.33. (a) If $Z_p = \langle a \rangle$ and $Z_q = \langle b \rangle$, then the element (a,b) of $Z_p \times Z_q$ has order pq.

(b) In $Z_p \times Z_p$, every element has order dividing p.

3.34. There are several ways to solve this question. We note first that A_4 contains the identity, three elements of order 2, and eight elements of order 3 (and none of order 6). So a supposed subgroup H of order 6 could not contain an element of order 6 either, that is, it could not be cyclic. So it must be isomorphic to S_3, with all three elements of order 2 and just two of the eight elements of order 3. But the identity and the three elements of order 2 form the Klein group V. So, if such a subgroup H could exist, it would contain V. But then Lagrange's Theorem is contradicted, since 4 doesn't divide 6.

Alternatively, argue that the hypothetical H must contain an element of order 2 and an element of order 3, but any such elements *generate* the whole of A_4 (that is, every element of A_4 can be written as a product of them), so no proper subgroup could contain them.

3.35. If a is the rotation through 90°, and b any reflection, then $z = a^2$. We have $b^{-1}ab = a^{-1}$. This shows that no reflection lies in the centre (it doesn't commute with a), and a and a^{-1} don't lie in the centre (they don't commute with reflections). On the other hand, checking shows that z lies in the centre, which thus consists of z and the identity.

Now $Z(G)$ is a normal subgroup of G, so $G/Z(G)$ is defined, and is a group of order 4. It is the Klein group: for we have $(Z(G)a)^2 = Z(G)a^2 = Z(G)z = Z(G)$ and $(Z(G)b)^2 = Z(G)b^2 = Z(G)$ for any reflection b.

3.36. θ is a homomorphism more-or-less by definition: if g induces g^* and h induces h^*, then gh induces g^*h^*.

Direct calculation shows that any permutation of $\{A,B,C\}$ is induced by some element of S_4, so the image of θ is S_3, with order 6.

If $g \in \mathrm{Ker}(\theta)$, then g fixes all three of A,B,C. Suppose that $g \neq 1$: say g maps 1 to 2. Since g fixes the partition A, it must map 2 back to 1, and either fix or interchange 3 and 4. But if it fixed 3, then it would map the set $\{1,3\}$ to the set $\{2,3\}$, and so would not fix B. In this way we find that the kernel of θ consists of the identity and the three elements with two 2-cycles. So it has order 4, and the equation is true.

3.37. Consider the element $m^{-1}n^{-1}mn$, where $m \in M$ and $n \in N$. On one hand, it is the product of two elements of M, namely m^{-1} and $n^{-1}mn$ (the latter is a conjugate of m, so lies in M since M is a normal subgroup), so is in M. On the other, it is the product of two elements of N, namely $m^{-1}n^{-1}m$ (a conjugate of n^{-1}) and n, so lies in N. So this element is in $M \cap N$. By assumption, $m^{-1}n^{-1}mn = 1$, so $nm = mn$.

The assumption $NM = G$ means that every element can be written in this form. Suppose that an element has more than one such expression, say $g = n_1m_1 = n_2m_2$. Then $n_2^{-1}n_1 = m_2m_1^{-1} \in N \cap M$, so $n_2^{-1}n_1 = m_2m_1^{-1} = 1$, or $n_1 = n_2$, $m_1 = m_2$.

Define a map $\theta : N \times M$ to G by the rule that $(n,m)\theta = nm$. According to the fact just proved, this is a bijection. Also, it is a homomorphism, since

$$(n_1,m_1)\theta(n_2,m_2)\theta = n_1m_1n_2m_2 = n_1n_2m_1m_2 = (n_1n_2,m_1m_2)\theta$$

(the second equality holding because n_2 and m_1 commute). So θ is an isomorphism, as required.

3.38. Check that, if g is a rotation through an angle θ about an axis A, then $h^{-1}gh$ is a rotation through an angle θ about the axis Ah. So each type of axis and angle of rotation determines a conjugacy class. So the classes, and corresponding permutations, are:

- Identity (one element), identity permutation.
- Rotations through 90° about face axis (6 elements), 4-cycles.
- Rotations through 180° about face axis (3 elements), products of two 2-cycles.
- Rotations through 180° about edge axis (6 elements), transpositions.
- Rotations through 120° about vertex axis (long diagonal) (8 elements), 3-cycles.

3.39. You are not actually asked to do anything in this question. The point is that there is an equivalence relation on the set of 30 edges, two edges being equivalent if they are parallel or perpendicular, and this relation has five equivalence classes with six edges in each class; any rotation of the figure permutes the five classes.

For the final deduction, we are in the position of knowing that the group G of permutations of the five frames induced by rotations of the figure is isomorphic to the rotation group and has order 60. So G has index 2 in S_5 and is normal, hence is A_5.