Group Theory Answers

1. (a) A **semigroup** is a set F together with a binary operation $(x,y) \mapsto xy : F \times F \to F$ such that $(xy)z = x(yz)$ for all x, y, $z \in F$. An **identity** if F is an element e of F such that $xe = ex = x$ for every $x \in F$. If F has an identity e, and $x \in F$, an **inverse** of x is a $y \in F$ such that $xy = yx = e$.

(b)(i) If e, e' are identities in F, then $e = ee' = e'$.

(ii) If y, y' are inverses of $x \in F$, then $y = ye = y(xy') = (yx)y' = ey' = y'$.

(c)(i) There is a $y \in F$ such that $xy = e$, and now there is a $z \in F$ such that $yz = e$; now $ez = (xy)z = x(yz) = xe = x$.

(ii) If $x \in F$ there is a $z \in F$ such that $ez = x$; now $ex = e(ez) = (ee)z = ez = x = xe$. Thus e is an identity in F.

(iii) If $x \in F$ we know that there are y, $z \in F$ such that $xy = yz = e$ and $ez = x$, as in (i) above. But (ii) now tells us that $z = ez = x$, so that $xy = yx = e$ and y is an inverse of x in F.
Thus every element of F has an inverse, and F is a group.

(d)(i) If $x \in F$, there is a $z \in F$ such that $x = zx_0$, so that $xe = (zx_0)e = z(x_0e) = zx_0 = x$.
(ii) Because F is not empty, it does have an element, call this x_0. We know that there is an $e \in F$ such that $x_0e = x_0$, and now (by (i)) $xe = x$ for every $x \in F$. Also, for every $x \in F$, there is a $y \in F$ such that $xy = e$. By (c), F is a group.

(e) Take x, $y \in F$. The map $z \mapsto xz : F \to F$ is injective. As F is finite, it must also be surjective. So there is a $z \in F$ such that $xz = y$. Similarly, because $z' \mapsto z'x : F \to F$ is injective, there is a $z' \in F$ such that $z'x = y$.
By (d), this is enough to show that F is a group.

2. (a) If i, j, $k \in \mathbb{Z}_n$ then

$$i \times_n (j \times_n k) \equiv_n i(j \times_n k) \equiv_n i(jk) = (ij)k \equiv_n (i \times_n j)k \equiv_n (i \times_n j) \times_n k;$$

but both $i \times_n (j \times_n k)$ and $(i \times_n j) \times_n k$ belong to $\{0, \dots, n-1\}$, so if they differ by a multiple of n they must be equal. Thus $(\mathbb{Z}_n, \times_n)$ is a semigroup.
Since $i \times_n 1 = 1 \times_n i = i$ for every $i \in \mathbb{Z}_n$, 1 is an identity of $\mathbb{Z}_n$.

(b)(i) If $i \in \mathbb{Z}_n$ is invertible, with inverse j say, then $ij - 1$ is a multiple of n; now any common factor of i and n is also a factor of ij and $ij - 1$ so must be 1.

(ii) If $i \in \mathbb{Z}_n$ and n have no non-trivial common factor, let r, $s \in \mathbb{Z}$ be such that $ri + sn$ is a factor of both i and n. Then $ri + sn$ must actually be 1, so $ri \equiv_n 1$. Let $j \in \mathbb{Z}_n$ be such that $r \equiv_n j$; then $ij \equiv_n 1$ so j is an inverse of i in $\mathbb{Z}_n$ and i is invertible.

(d) Tabulating,

n	$\mathbb{Z}_n^*$	generators	
2	$\{1\}$	1	
3	$\{1,2\}$	2	
4	$\{1,3\}$	3	
5	$\{1,2,3,4\}$	2, 3	
6	$\{1,5\}$	5	
7	$\{1,2,3,4,5,6\}$	3, 5	
8	$\{1,3,5,7\}$	–	$\mathbb{Z}_8^* \cong K_4$
9	$\{1,2,4,5,7,8\}$	2, 5	
10	$\{1,3,7,9\}$	3, 7	
11	$\{1,2,3,4,5,6,7,8,9,10\}$	2, 6, 7, 8	
12	$\{1,5,7,11\}$	–	$\mathbb{Z}_{12}^* \cong K_4$

3. (a) Let G be a group.

(i) A **subgroup** of G is a set $H \subseteq G$ such that (α) $xy \in H$ for all x, $y \in H$ (β) $e \in H$ (γ) $x^{-1} \in H$ for every $x \in H$.

(ii) For $A \subseteq G$, a **left coset** of A is a set of the form $xA = \{xa : a \in A\}$ where $x \in G$; a **right coset** of A is a set of the form $Ax = \{ax : a \in A\}$ where $x \in G$.

(b) **Lagrange's theorem** If G is a finite group and H is a subgroup of G then $\#(H)$ is a factor of $\#(G)$.
P (i) If $x \in G$ then the function $x \mapsto xh : H \to xH$ is injective (by the cancellation law) and surjective (by the definition of xH), so $\#(xH) = \#(H)$.
(ii) If $y \in G$, then yH is a left coset of H containing $ye = y$.
On the other hand, if we have any left coset V of H containing y, then $V = xH$ for some $x \in H$. Now $yH \subseteq xHH \subseteq xH = V$; but also there is some $h \in H$ such that $y = xh$, so that $x = yh^{-1} \in yH$ and $V = xH \subseteq yHH \subseteq yH$. Accordingly $V = yH$.
What this means is that every member of G belongs to exactly one left coset of H.
(iii) Since all the left cosets of H have the same number $\#(H)$ of elements,

$$\#(G) = (\text{number of left cosets of } H) \times \#(J)$$

is a multiple of $\#(H)$. **Q**

(c) If G is a group and $a \in G$, the **subgroup generated by** a is $< a >= \{a^n : n \in \mathbb{Z}\}$, the smallest subgroup of G containing a.
The subgroup generated by $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ is $\{\begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} : n \in \mathbb{Z}\}$.

(d) Examine $e, a, a^2, a^3, \ldots$. Because G is finite, these cannot all be different. Let $r \in \mathbb{N} \setminus \{0\}$ be the least number such that $a^r = a^k$ for some $0 \le k < r$. Then $a^{r-1} = a^{k-1}$ so $k-1$ must be less than 0 and $k = 0$, that is, $a^r = e$. Now $H = \{e, a, \ldots, a^{r-1}\}$ has just r elements. Also H is a subgroup of G. **P** (α) If $0 \le i, j < r$ then $a^i a^j = a^{i+j} = a^{i+j-r} \in H$, so the product of two elements of H belongs to H. (β) $e = a^0 \in H$. (γ) If $0 \le i < r$ then $(a^i)^{-1} = a^{r-i} = a^{-i} \in H$. Thus the inverse of any element of H belongs to H. **Q**
By Lagrange's theorem, $r = \#(H)$ is a factor of $n = \#(G)$; say $n = rm$. Now $a^n = (a^r)^m = e^m = e$.

4. g^2 is the identity. $h^2(x) = \frac{1}{1-x}$, h^3 is the identity, $g^{-1}hg = h^2$. Consequently

$$\{e, h, h^2, g, gh, gh^2\}$$

is a subgroup of G. (It is closed under multiplication because $hg = gh^2$; being a finite semigroup satisfying the cancellation laws, it must be a group, so is a subgroup of G.) All these six elements are different because $g \notin < h >$.
The subgroup is therefore a non-abelian group with six elements and must be isomorphic to S_3.

(b)(i) If H is a subgroup of $\mathbb{C} \setminus \{0\}$ with n elements, then every element of H is an nth root of 1. But the nth complex roots of 1 in $\mathbb{C}$ are just the powers of $e^{2\pi i/n}$, so form a cyclic group.
Conversely, any finite cyclic group with n elements is isomorphic to the subgroup $< e^{2\pi i/n} >$ of $\mathbb{C} \setminus \{0\}$.

(ii) The only finite subgroups of $\mathbb{R} \setminus \{0\}$ are $\{1\} \cong \mathbb{Z}_1$ and $\{1, -1\} \cong \mathbb{Z}_2$.

5. (a) A **normal subgroup** of G is a subgroup H of G such that $gH = Hg$ for every $g \in G$.

(b) If H is a normal subgroup of G, let G/H be the set of (left or right) cosets of H in G. Then $AB \in G/H$ for all A, $B \in G/H$. **P** We can express A as aH and B as bH. Now

$$AB = (aH)(bH) = a(Hb)H = a(bH)H = abHH = abH \in G/H. \text{ } \mathbf{Q}$$

So we have a binary operation $(A,B) \mapsto AB : G/H \times G/H \to G/H$. If A, B, $C \subseteq G$, then $(AB)C = A(BC)$; in particular, $(AB)C = A(BC)$ for all A, B, $C \in G/H$, so G/H is a semigroup. $H = eH$ belongs to G/H, and $eH \cdot aH = (ea)H = aH = (ae)H = aH \cdot eH$ for every $a \in G$, so eH is an identity in the semigroup G/H. If $a \in G$ then $a^{-1}H \in G/H$ and

$$a^{-1}H \cdot aH = aa^{-1}H = eH = a^{-1}aH = a^{-1}H \cdot aH,$$

so $a^{-1}H$ is an inverse of aH in G/H; thus every element of G/H has an inverse and G/H is a group.

If H is not normal then $aHbH$ need not belong to G/H for all a, $b \in G$ so we can't use this as a definition of multiplication in G/H.

(c)(i) Try $H = \{\mathbf{A} : \mathbf{A} \in G, \det \mathbf{A} = 1\}$. Because $\det : G \to (\mathbb{R} \setminus \{0\}, \times)$ is a homomorphism, its kernel H is a normal subgroup of G.

(ii) G/H is isomorphic to the image $\{\det \mathbf{A} : \mathbf{A} \in G\} = \mathbb{R} \setminus \{0\}$.

(iii) Try $K = \{\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} : \alpha \in \mathbb{R}\}$. Then K is a subgroup of G because it is the image of the homomorphism $\alpha \mapsto \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} : (\mathbb{R}, +) \to G$. It is not normal because, e.g.,

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \notin K$$

even though $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in K$.

6. (a)

	e	a	b	c	p	q	r	s	w	x	y	z
e	e	a	b	c	p	q	r	s	w	x	y	z
a	a	e	c	b	q	p	s	r	x	w	z	y
b	b	c	e	a	r	s	p	q	y	z	w	x
c	c	b	a	e	s	r	q	p	z	y	x	w
p	p	s	q	r	w	z	x	y	e	c	a	b
q	q	r	p	s	x	y	w	z	a	b	e	c
r	r	q	s	p	y	x	z	w	b	a	c	e
s	s	p	r	q	z	w	y	x	c	e	b	a
w	w	y	z	x	e	b	c	a	p	r	s	q
x	x	z	y	w	a	c	b	e	q	s	r	p
y	y	w	x	z	b	e	e	c	r	p	q	s
z	z	x	w	y	c	a	a	b	s	q	p	r

(b) $H = \{e, a, b, c\}$ is the normal subgroup with 4 elements; its cosets are $A = \{p, q, r, s\}$ and $B = \{w, x, y, z\}$; the group table is

	H	A	B
H	H	A	B
A	A	B	H
B	B	H	A

(c) There are four subgroups with three elements ($\{e, p, w\}$, $\{e, q, y\}$, $\{e, r, z\}$, $\{e, s, x\}$); none are normal.

(d) There is no subgroup with six elements.

7. (a) If G and H are groups, a homomorphism from G to H is a function $\phi : G \to H$ such that $\phi(ab) = \phi(a)\phi(b)$ for all a, $b \in G$. ϕ is an isomorphism if it is a bijective homomorphism. The kernel of ϕ is $\{a : a \in G,\ \phi(a) = e_H\}$.

(b)(i) Let $\phi : G \to H$ be a homomorphism and K its kernel. Then $e_G \in K$ because $\phi(e_G) = e_H$. If a, $b \in K$, then

$$\phi(ab) = \phi(a)\phi(b) = e_H e_H = e_H,$$

so $ab \in K$. If $a \in K$, then

$$\phi(a^{-1}) = \phi(a)^{-1} = e_H^{-1} = e_H,$$

so $a^{-1} \in K$. Thus K is a subgroup of G. If $a \in G$ and $k \in K$ then

$$\phi(aka^{-1}) = \phi(a)\phi(k)\phi(a^{-1}) = \phi(a) \cdot e_H \cdot \phi(a)^{-1} = \phi(a)\phi(a)^{-1} = e_H,$$

so $aka^{-1} \in K$; as a and k are arbitrary, $K \lhd G$.

(ii) Let $\phi : G \to H$ be a homomorphism and K its set of values. Then $e_H \in K$ because $e_H = \phi(e_G)$. If x, $y \in K$ there are a, $b \in G$ such that $\phi(a) = x$ and $\phi(b) = y$; now

$$xy = \phi(a)\phi(b) = \phi(ab) \in K.$$

If $x \in K$ there is an $a \in G$ such that $\phi(a) = x$, and now

$$x^{-1} = \phi(a)^{-1} = \phi(a^{-1}) \in K.$$

Thus K is a subgroup of G.

(c) **First Isomorphism Theorem** Let G and H be groups, and $\phi : G \to H$ a homomorphism. Write K for the kernel of ϕ and $\phi[G]$ for the set of values of ϕ, so that K is a normal subgroup of G and $\phi[G]$ is a subgroup of H. Then the quotient group G/K is isomorphic to $\phi[G]$.

proof (i) For x, $y \in G$, $\phi(x) = \phi(y)$ iff $xK = yK$. **P** (α) If $xK = yK$, then $y \in xK$ so there is a $k \in K$ such that $y = xk$ and

$$\phi(y) = \phi(xk) = \phi(x)\phi(k) = \phi(x)e_H = \phi(x).$$

(β) If $\phi(x) = \phi(y)$, set $k = x^{-1}y$; then

$$\phi(k) = \phi(x)^{-1}\phi(y) = e_H,$$

and $k \in K$. But $y = xk$, so $y \in xK$; as certainly $y \in yK$, xK and yK have a common element and must be identical. **Q**

(ii) We can therefore define $\psi : G/K \to \phi[G]$ by saying that $\psi(A) = \phi(x)$ whenever $x \in G$ and $A = xK$. If A, $B \in G/H$, express them as $A = xK$ and $B = yK$ where x, $y \in G$; then $AB = xyK$, so

$$\psi(AB) = \phi(xy) = \phi(x)\phi(y) = \psi(A)\psi(B).$$

Thus $\psi : G/H \to \phi[G]$ is a homomorphism. It is injective because if A, $B \in G/H$ and $\psi(A) = \psi(B)$, we can express A as xK and B ans yK, and $\phi(x) = \psi(A) = \psi(B) = \phi(y)$, so $A = xK = yK = B$. It is surjective because if $h \in \phi[H]$ there is some $x \in G$ such that $h = \phi(x) = \psi(xK)$. Thus ψ is a bijective homomorphism and is an isomorphism.

(d)(i) $e = ee \in HK$. If x, $y \in HK$ we can express them as $x = h_1k_1$, $y = h_2k_2$ where h_1, $h_2 \in H$ and k_1, $k_2 \in K$; now

$$xy = h_1k_1h_2k_2 \in h_1k_1Hk_2 = h_1Hk_1k_2 \in HHKK = HK.$$

If $x \in HK$ we can express it as $x = hk$, where $h \in H$ and $k \in K$; now

$$x^{-1} = k^{-1}h^{-1} \in k^{-1}H = Hk^{-1} \subseteq HK.$$

Thus HK is a subgroup of G.

(ii) $e \in H$ and $e \in K$ so $e \in H \cap K$. If x, $y \in H \cap K$ then $xy \in H$ and $xy \in K$ so $xy \in H \cap K$. If $x \in H \cap K$ then $x^{-1} \in H$ and $x^{-1} \in K$ so $x^{-1} \in H \cap K$. Thus $H \cap K$ is a subgroup of K.

If $x \in K$ and $y \in H \cap K$ then $xyx^{-1} \in H$ (because $H \lhd G$ and $x \in G$ and $y \in H$), while $xyx^{-1} \in K$ because K is a subgroup and both x and y belong to K. So $xyx^{-1} \in H \cap K$. As x and y are arbitrary, $H \cap K \lhd K$.

(iii) (Because H is a normal subgroup of G it is also a normal subgroup of HK.) Define $\phi : K \to HK/H$ by setting $\phi(a) = aH$ for $a \in K$. Since $aH \cdot bH = abH$ for all a, $b \in HK$, ϕ is a homomorphism. For $k \in K$,

$$\phi(k) = e_{HK/H} \iff kH = H \iff k \in H \iff k \in H \cap K,$$

so the kernel of ϕ is $H \cap K$. (This gives an alternative proof that $H \cap K \lhd K$.) Also $\phi[K] = HK/H$. **P** If $A \in HK/H$, it is of the form aH for some $a \in HK$. Now a is expressible as hk where $h \in H$ and $k \in K$, so that

$$aH = Ha = Hhk = Hk = kH = \phi(k) \in \phi[K].$$

As A is arbitrary, ϕ is surjective. **Q**

By the First Isomorphism Theorem

$$K/H = \phi[K] \cong K/\ker\phi = K/H \cap K,$$

as required.

8. (a) $e \in H$ and $e \in K$ so $e \in H \cap K$. If $x, y \in H \cap K$ then $xy \in H$ and $xy \in K$ so $xy \in H \cap K$. If $x \in H \cap K$ then $x^{-1} \in H$ and $x^{-1} \in K$ so $x^{-1} \in H \cap K$. Thus $H \cap K$ is a subgroup of G.

(b) $e = ee \in KH$. If $a, b \in KH$ then

$$ab \in (KH)(KH) = K(HK)H = KKHH = KH.$$

If $a \in KH$, express it as kh where $k \in K$, $h \in H$; then

$$a^{-1} = h^{-1}k^{-1} \in HK \subseteq KH.$$

So KH is a subgroup of G. Now if $a \in KH$, $a^{-1} \in KH$; express a^{-1} as kh where $k \in K$ and $h \in H$; then $a = h^{-1}k^{-1} \in HK$. This shows that $KH \subseteq HK$ so $KH = HK$.

(c) If $h_1, h_2 \in H$, then

$$h_1K = h_2K \iff h_2 \in h_1K \iff h_1^{-1}h_2 \in h_1^{-1}h_1K = K,$$

while similarly $h_1(H \cap K) = h_2(H \cap K)$ iff $h_1^{-1}h_2 \in H \cap K$. But of course $h_1^{-1}h_2 \in H$, so $h_1^{-1}h_2 \in H \cap K$ iff $h_1^{-1}h_2 \in K$, and $h_1(H \cap K) = h_2(H \cap K)$ iff $h_1K = h_2K$.

What this means is that we have a bijection between the set $P = \{hK : h \in H\}$ and the set $Q = \{h(H \cap K) : h \in H\}$, matching hK with $h(H \cap K)$ for every $h \in H$.

Now consider HK. This is just the union of the cosets hK with $h \in H$. Since these all have exactly $\#(K)$ members, $\#(HK) = \#(P)\#(K)$. On the other hand, we know from Lagrange's theorem that $\#(H) = \#(Q)\#(H \cap K)$. Since $\#(P) = \#(Q)$,

$$\#(HK)\#(H \cap K) = \#(P)\#(K)\#(H \cap K) = \#(Q)\#(K)\#(H \cap K) = \#(H)\#(K).$$

(d) We know that A_4 has subgroups $H = \{e, (\overleftarrow{123}), (\overleftarrow{132})\}$ and $K = \{e, (\overleftarrow{12})\}$. By (c), HK has 6 members; but we also know that A_4 has no subgroup of size 6.

9. (a) 1 element with 4 orbits, 11 elements with 2 orbits.

(b) 1 identity with 4 orbits, 6 transpositions with 3 orbits (because $6 = {}^2C_4$), 11 elements with 2 orbits (3 double transpositions, 8 3-cycles), 6 4-cycles with 1 orbit (because there are 3! ways of writing a 4-cycle starting with 1).

(c)(i) If $\rho = (\overleftarrow{1...})(\overleftarrow{2**\!*})(\overleftarrow{3!!!})\dots$, then $(\overleftarrow{123})\rho = (\overleftarrow{1...2***3!'!})\dots$ has $m-2$ orbits.

(ii) If $\rho = (\overleftarrow{1...2**\!*})(\overleftarrow{3!!!})\dots$, then $(\overleftarrow{123})\rho = (\overleftarrow{1...3!!!})(\overleftarrow{2**\!*})\dots$ has m orbits.

(iii) If $\rho = (\overleftarrow{1...2***3!!!})\dots$, then $(\overleftarrow{123})\rho = (\overleftarrow{1...3!!!2**\!*})\dots$ has m orbits; but if $\rho = (\overleftarrow{1...3!!!2**\!*})\dots$, then $(\overleftarrow{123})\rho = (\overleftarrow{1...})(\overleftarrow{2**\!*})(\overleftarrow{3!!!})\dots$ has $m+2$ orbits. So no, we cannot determine how many orbits $(\overleftarrow{123})\rho$ has. (Or just say: take $n = 3$, $m = 1$, $\rho = (\overleftarrow{123})$ or $(\overleftarrow{132})$.)

10. (a) $<\rho> = \{e, (\overleftarrow{12})(\overleftarrow{3456}), (\overleftarrow{35})(\overleftarrow{46}), (\overleftarrow{12})(\overleftarrow{3654})\}$; the order of ρ is 4.

(b) $3 \times 4 = 12$.

(c) $3 \times 5 = 15$ for $(\overleftarrow{123})(\overleftarrow{45678})$ and its conjugates. This is the best we can do because anything with a 6-, 7- or 8-cycle will have order 6, 7 or 8 respectively; something with two 4-cycles will have order 4; something with a 4-cycle and a 3-cycle will have order 12; and if we have only 2- and 3-cycles we can't get an order above 6.

11. Imagine that the tray, underneath the moving pieces, is coloured black and white in a chessboard pattern; for definiteness, let us take the diagonal squares to be black, so that in the original position the '16' tile is on a black square. Each move is a transposition of two tiles, one of them the '16' tile; so after an even number of moves we shall have an even permutation and the '16' tile will be on a black square, while after an odd number of moves we shall have an odd permutation and the '16' tile will be on a white square. This means that only half the 16! permutations will be achievable.

(It is in fact the case that exactly half the 16! permutations are achievable. But the proof of this is more difficult.)

12. (a) Since $\rho\sigma\rho^{-1} = (\overleftarrow{\rho(1)\,\rho(2)\,\rho(3)})$, the conjugates of σ in S_4 are just the 3-cycles, and there are 8 of them ($4 \times 3 \times 2$, divide by 3 because you can start anywhere).

(b) $(\overleftarrow{123})$ (of course), $(\overleftarrow{134})$, $(\overleftarrow{142})$, $(\overleftarrow{234})$.

(Working this out without the help of general theory is a bit of a slog. There is a general theorem that, for any finite group G and any $x \in G$,

$$\#(G) = (\text{no. of conjugates of } x) \times (\text{no. of elements commuting with } x).$$

Now there are at least 3 elements of A_4 commuting with $(\overleftarrow{123})$, viz., e, $(\overleftarrow{123})$ and $(\overleftarrow{123})^2 = (\overleftarrow{132})$, so there can't be more than 4 conjugates.)

(c) All the 3-cycles, and there are $5 \times 4 \times 3 \div 3 = 20$ of them.

(d) This time all 20 of them are conjugate to σ in A_5. To see this, take any 3-cycle σ'. Then there is a $\rho \in S_5$ such that $\rho\sigma\rho^{-1} = \sigma'$. If $\rho \in A_5$, then certainly σ' is conjugate to σ in A_5. Otherwise, because σ' is a 3-cycle, and we have 5 elements to play with, there is a transposition τ which is disjoint from σ', so that $\tau\sigma' = \sigma'\tau$ and $\tau\sigma'\tau^{-1} = \sigma'$. But this means that

$$\sigma' = \tau\rho\sigma\rho^{-1}\tau^{-1} = (\tau\rho)\sigma(\tau\rho)^{-1}$$

is conjugate to σ in A_5, because $\tau\rho$ is a product of odd permutations and belongs to A_5.

13. (a) By the definition of G/K, $xK \cdot yK = (xy)K$ for all x, $y \in G$, and therefore for all x, $y \in H$; so the map $x \mapsto xK : H \to G/K$ is a homomorphism. Its kernel is $\{x : x \in H, xK = K\} = H \cap K = \{e\}$, so it is injective.

(b) $\#(S_4/K) = \frac{24}{4} = 6$.

Let H be $\{\rho : \rho \in S_4, \rho(4) = 4\}$; then H is a subgroup of S_4 and can be identified with S_3 (if $\rho \in H$, then its restriction to $\{1, 2, 3\}$ belongs to S_3).

Now $H \cap K = \{e\}$, so the map $x \mapsto xK : H \to S_4/K$ is an injective homomorphism. Because $\#(H) = 6 = \#(S_4/K)$, it must also be surjective, and is an isomorphism.

14. (a)(i) If $a = xyx^{-1}y^{-1} \in A$ then $a^{-1} = yxy^{-1}x^{-1} \in A$.

(ii) If $a = xyx^{-1}y^{-1} \in A$ and $z \in G$, then

$$\begin{aligned} zaz^{-1} &= zxyx^{-1}y^{-1}z^{-1} = zxz^{-1}zyz^{-1}zx^{-1}z^{-1}zy^{-1}z^{-1} \\ &= (zxz^{-1})(zyz^{-1})(zxz^{-1})^{-1}(zyz^{-1})^{-1} \in A. \end{aligned}$$

(iii) $e = eee^{-1}e^{-1} \in A \subseteq H$.

If $x, y \in H$ there are strings in A with products x and y; putting these together we get a string in A with product xy, so $xy \in H$.

If $a_1 \dots a_n \in H$ then (using (i)) $a_n^{-1} \dots a_1^{-1} \in H$; thus H is closed under inverses.

If $a_1 \dots a_n \in H$ and $x \in G$ then (using (ii))

$$xa_1 \dots a_n x^{-1} = xa_1x^{-1}xa_2x^{-1} \dots xa_nx^{-1} \in H.$$

(b) If $x, y \in G$ then

$$(yx)^{-1}(xy) = x^{-1}y^{-1}xy = x^{-1}y^{-1}(x^{-1})^{-1}(y^{-1})^{-1} \in A \subseteq H$$

so

$$xH \cdot yH = xyH = yxH = yH \cdot xH.$$

(c) If $\phi : G \to K$ is a homomorphism and $x, y \in G$, then

$$\phi(xyx^{-1}y^{-1}) = \phi(x)\phi(y)\phi(x)^{-1}\phi(y)^{-1} = \phi(x)\phi(x)^{-1}\phi(y)\phi(y)^{-1} = e_K,$$

so $xyx^{-1}y^{-1}$ belongs to the kernel of ϕ; as x and y are arbitrary, $A \subseteq \ker(\phi)$; as $\ker(\phi)$ is a subgroup, $H \subseteq \ker(\phi)$.

(d)(i) $A = H = \{0\}$, because Z_6 is abelian.

(ii) H must be either $\{e\}$ or A_3 or S_3; since S_3 is not abelian, $A \neq \{e\}$; since every member of A is even, $H = A_3$.

(iii) H must be either $\{e\}$ or the 4-element group K or A_4. Since $A_4/K \cong \mathbb{Z}_3$ is abelian, K includes H; since A_4 is not abelian, $H \neq \{e\}$; so $H = K$.

(e)(i) Since $H \neq \{e\}$, A must contain at least one 3-cycle; since the two 3-cycles are inverses of each other, it contains both; so $A = A_3$.

(ii) We know that A contains at least one member of $K \setminus \{e\}$. But since these all look exactly the same it had better contain all the others. (This is a touch unrigorous, failing a proper definition of 'look exactly the same'. Alternatively: all the members of $K \setminus \{e\}$ are conjugate in A_4, e.g., $(\overleftarrow{123})(\overleftarrow{12})(\overleftarrow{34})(\overleftarrow{321}) = (\overleftarrow{23})(\overleftarrow{14})$, so if A contains one of them it must contain the others.) So $A = K$.

15. (a) If H is a subgroup of $< \rho >$ it is certainly a subgroup of D_n. If $h \in H$ and $a \in D_n$, express h as ρ^i and a as either ρ^j or $\sigma\rho^j$. Then aha^{-1} is either

$$\rho^j \rho^i \rho^{-j} = \rho^i \in H$$

or

$$\sigma\rho^j\rho^i\rho^{-j}\sigma^{-1} = \sigma\rho^i\sigma^{-1} = (\sigma\rho\sigma^{-1})^i = (\rho^{-1})^i = (\rho^i)^{-1} \in H.$$

So we always have $aha^{-1} \in H$; as a, h are arbitrary, $H \lhd D_n$.

(b) $\rho\sigma\rho^{-1} = \sigma\rho^{-1}\rho^{-1} = \sigma\rho^{-2}$.

(c) If $\sigma \in H \lhd D_n$, then H must contain $\sigma\rho^{-2}$ so contains ρ^{-2} and ρ^2 and all its powers. But as n is odd, $\rho = \rho^{n+1}$ is a power of ρ^2 and belongs to H. So H contains both ρ and σ and must be the whole of D_n.

(d) Because n is even, $H^* = \{\sigma^i\rho^{2j} : i, j \in \mathbb{Z}\}$. Now $e = \sigma^0\rho^0 \in H^*$,

$$\begin{aligned}
\rho^{2i} \cdot \rho^{2j} &= \rho^{2(i+j)} \\
\sigma\rho^{2i} \cdot \rho^{2j} &= \sigma\rho^{2(i+j)} \\
\rho^{2i} \cdot \sigma\rho^{2j} &= \sigma(\sigma\rho^{2i}\sigma^{-1})\rho^{2j} = \sigma\rho^{-2i}\rho^{2j} = \sigma\rho^{2(j-i)} \\
\sigma\rho^{2i} \cdot \sigma\rho^{2j} &= \sigma^2\rho^{2(j-i)} = \rho^{2(j-i)}
\end{aligned}$$

belong to H^* for all $i, j \in \mathbb{Z}$, so H^* is closed under multiplication. Finally

$$(\rho^{2i})^{-1} = \rho^{-2i}, \quad (\sigma\rho^{2i})^{-1} = \rho^{-2i}\sigma$$

belong to H^* (the latter because it is the product of two members of H^*) for every $i \in \mathbb{Z}$, so H^* is closed under inversion.

Thus H^* is a subgroup of D_n. It is normal because it has just $n = \frac{1}{2}\#(D_n)$ members.

(e) Let H be a normal subgroup of D_n which is not a subgroup of $< \rho >$. Then H contains $\sigma_1 = \sigma\rho^i$ for some i. But now H contains $\rho\sigma_1\rho^{-1} = \sigma_1\rho^{-2}$; so H contains ρ^2 and ρ, and must be the whole of D_n.

(f) Let H be a normal subgroup of D_n which is not a subgroup of $< \rho >$. Then H contains $\sigma_1 = \sigma\rho^i$ for some i, and (as above) ρ^2 and all its powers belong to H. So either H contains ρ, and is equal to D_n, or it contains $\sigma\rho^{2i}$ for every i, and includes H^*. In the latter case, because $\#(H^*) = \frac{1}{2}\#(D_n)$, H is either H^* or D_n.

(g) $D_{n/2}$.

(h) $\rho^i\rho(\rho^i)^{-1} = \rho$, $(\sigma\rho^i)\rho(\sigma\rho^i)^{-1} = \rho^{-1}$, so just two elements of D_n are conjugate to ρ in D_n.
$\rho\sigma\rho^{-1} = \sigma\rho^{-2}$, so $\rho^i\sigma(\rho^i)^{-1} = \sigma\rho^{-2i}$ for every $i \in \mathbb{N}$ (induce on i) and

$$(\sigma\rho^i)\sigma(\sigma\rho^i)^{-1} = \sigma(\rho^i\sigma\rho^{-i}\sigma^{-1} = \sigma\sigma\rho^{-2i}\sigma = \sigma\rho^{2i}$$

for every $i \in \mathbb{N}$. Thus the elements of D_n conjugate to σ are of the form $\sigma(\rho^2)^i$ for some $i \in \mathbb{Z}$; if n is even there are $n/2$ of them; if n is odd there are n of them.

(This corresponds to the fact that if n is odd, all axes of reflection are of the same type, while if n is even, they are of two types. σ, as defined here, is a reflection in an axis through the midpoint of an edge, and such reflections are conjugates of σ. If n is even, then half the reflections are about axes through vertices, and these aren't conjugate to σ.)

16. (a)(i) $(\overleftarrow{123})(\overleftarrow{456})$
(ii) $(\overleftarrow{25})(\overleftarrow{36})$
(iii) $(\overleftarrow{26})(\overleftarrow{35})$.

(Of course these depend on the labelling of the vertices and on which rotations/reflections you pick. But any representation must give double-3-cycles and double-transpositions as above.)

(b) Because every simple exchange of vertices in the tetrahedron gives an even permutation of the edges, so does every rotation/reflection of the tetrahedron. So the action of the isometry group of the tetrahedron corresponds to a homomorphism from S_4 to A_6. Also any isometry which keeps all the edges in place must be the identity, so this homomorphism is injective and its image is a subgroup H of A_6 isomorphic to S_4. Since any edge can be moved to any other by an isometry, H is transitive.

(c) I expect there are lots; but an easy one is just

$$K = \{\rho : \rho \in A_6,\ \{\rho(5), \rho(6)\} = \{5, 6\}\}.$$

(The point is that every member of K permutes the numbers 1,2,3,4, and that for any permutation of 1,2,3,4 there is exactly one member of K acting in that way, because if the permutation is even we need to set $\rho(5) = 5$ and $\rho(6) = 6$ to keep it even, and if it is odd we need to set $\rho(5) = 6$ and $\rho(6) = 5$.)

17. (a) Consider the action of rotations of the cube on the four long diagonals. This corresponds to a homomorphism from the rotation group to S_4. If we look at a 180° rotation about an axis through the midpoints of two opposite edges, this exchanges two of the diagonals and leaves the other two unmoved; so every transposition is in the image H of the rotation group, and H must be S_4. Since the number of rotations is $6 \cdot 4 = 8 \cdot 3 = 24 = \#(S_4)$, the homomorphism must be injective as well as surjective and is an isomorphism.

[Alternative argument: A 90° rotation about an axis through the midpoints of opposite faces corresponds to a 4-cycle in S_4, and a 120° rotation about a long diagonal corresponds to a 3-cycle. So H has subgroups of orders 3 and 4 and has at least 12 members. But the only subgroup of S_4 with 12 members is A_4, which does not contain any 4-cycle, so H must be the whole of S_4.]

(b)(i) $e \in K_4$ corresponds to the identity rotation. A double-transposition in K_4 corresponds to a rotation through 180° about an axis through the midpoints of two opposite faces. The elements of K_4 correspond to rotations which do not move the three axes of the cube which pass through the midpoints of two opposite faces.

(ii) A 3-cycle corresponds to a rotation through 120° about a long diagonal; other members of K_4 as above.

(c)(i) We have already seen double-transpositions in (b-i); there are 3 of them, corresponding to the 3 pairs of opposite faces. As for simple transpositions, these are got by rotating 180° about an axis through the midpoints of opposite edges; there are 6 of them, corresponding to the 6 pairs of opposite edges.

(ii) As noted in (b-ii), 3-cycles are rotations about long diagonals; there are 8 of them, 2 for each diagonal axis.

(iii) 4-cycles are 90° rotations about axes through the midpoints of opposite faces; there are 6 of them, 2 for each axis.

18. (a) We can inscribe 5 cubes in the surface of a regular dodecahedron; each cube has each of its 12 edges lying in a different face of the dodecahedron, being one of the 5 diagonals of that face. Two cubes meet at each vertex of the dodecahedron. Each isometry of the dodecahedron shuffles the five cubes; thus we have an action of the isometry group G of the dodecahedron on the set of cubes, which can be interpreted as a homomorphism $\phi : G \to S_5$.

$\#(G) = 60$. **P** The dodecahedron has 12 faces, and each face can be oriented in 5 directions, so $\#(G) = 5 \cdot 12 = 60$. **Q**

$\phi[G]$ contains a 5-cycle. **P** Let $a \in G$ be a rotation through an angle of 72° about an axis through the centres of two opposite faces. Looking at the 5 diagonals of that face, each belonging to a different cube, we see that $\phi(a)$ is a 5-cycle. **Q**

$\phi[G]$ contains a 3-cycle. **P** Let $b \in G$ be a rotation through an angle of 120° about an axis through two opposite vertices v, v'. Then $b^3 = e$ so $\phi(b)$ is either the identity or has order 3. But if we look at any of the cubes not using the vertices V and V', we see that they are moved. So $\phi(b)$ is not the identity; as the only permutations in S_5 of order 3 are 3-cycles, $\phi(b)$ is a 3-cycle. **Q**

$\phi[G]$ contains a double-transposition. **P** Let $c \in G$ be a rotation through 180° about an axis through the midpoints of two opposite edges E and E'. Then $c^2 = e$ so $\phi(c)$ is either the identity, a transposition or a double-transposition. But the four cubes which use the vertices at the ends of E and E' are exchanged in pairs, so $\phi(c)$ moves 4 points and must be a double-transposition. **Q**

Now consider $H = A_5 \cap \phi[G]$. This is a subgroup of A_5 and contains elements of orders 2, 3 and 5. So $\#(H)$ is a multiple of $2 \cdot 3 \cdot 5 = 30$. But A_5 is simple, so has no subgroup of order 30 (which would have to be normal). This means that $\#(H) = 60$. This tells us that $\phi[G] \supseteq A_5$. But as $\#(G) = \#(A_5) = 60$, $\phi[G] = A_5$ and ϕ is injective, therefore an isomorphism, and $G \cong A_5$.

(b) Consider the isometry t which takes each vertex to its opposite vertex. Then t^2 is the identity ι. Also $tf = ft$ for every isometry f, because if v is any vertex then v, $t(v)$ are opposite so $f(v)$, $f(t(v))$ are opposite, that is, $(t \circ f)(v) = (f \circ t)(v)$. But this means that $\{\iota, t\}$ is a normal subgroup of the isometry group. As S_5 has no normal subgroup of order 2, it cannot be isomorphic to the isometry group.

(c)(i) A rotation of order 3 is a rotation through 120° about a long diagonal. There are 20 of these (two for each of 10 diagonals).

(ii) A rotation of order 5 is a rotation through 72° about an axis through the midpoints of opposite faces. There are 24 of these (four for each of 6 axes).

(iii) A rotation of order 2 is a rotation through 180° about an axis through the midpoints of opposite edges. There are 15 of these (since the dodecahedron has 30 edges in 15 pairs).

19. I will call the three points of the glued-together faces the *equatorial points* of X and the other two points the *poles*.

(a) There are 6 rotations (2 places for a pole, then three for one of the equatorial points); 12 isometries (if the poles and an equatorial point are fixed, you can exchange the other two equatorial points). $H \lhd G$ because $\#(H) = \frac{1}{2}\#(G)$.

(b) G has 2 elements of order 3, all of which are in H. (If $f \in G$ has order 3, it must leave the poles unexchanged; now it must act as a 3-cycle on the equatorial points.)

(c) An element of order 2 in G must either be a transposition of two points, which could be the poles or a pair of equatorial points (4 possibilities), or a double-transposition involving the poles and a pair of equatorial points (3 possibilities). So G has 7 elements of order 2, of which 3 belong to H.

(d) $C = \{\iota, t\}$, where ι is the identity rotation and t is the reflection in the equator, exchanging the poles.

(e) The normal subgroups of G are
$\{\iota\}$, the identity alone;
$C = \{\iota, t\}$, the isometries which keep all equatorial points fixed;
H, the group of rotations;
the subgroup S, isomorphic to S_3, of the 6 isometries which leave the poles unexchanged;
$S \cap H = \{\iota, g, g^2\}$ where g is a $120°$ rotation about an axis through the poles; the subgroup, isomorphic to $\mathbb{Z}_3$, of rotations which leave the poles unexchanged.

20. (a) Look at the different possibilities.

(i) If $\rho = e$ then $\rho^{-1} = eee^{-1}$ is conjugate to ρ.

(ii) If $\rho = (\overleftarrow{i_1\, i_2\, i_3})$ then $\rho^{-1} = (\overleftarrow{i_3\, i_2\, i_1}) = \sigma\rho\sigma^{-1}$ where $\sigma = (\overleftarrow{i_1\, i_3})(\overleftarrow{i_4\, i_5})$.

(iii) If $\rho = (\overleftarrow{i_1\, i_2})(\overleftarrow{i_3\, i_4})$ then $\rho^{-1} = \rho = e\rho e^{-1}$.

(iv) If $\rho = (\overleftarrow{i_1\, i_2\, i_3\, i_4\, i_5})$ then $\rho^{-1} = (\overleftarrow{i_5\, i_4\, i_3\, i_2\, i_1}) = \sigma\rho\sigma^{-1}$ where $\sigma = (\overleftarrow{i_1\, i_5})(\overleftarrow{i_2\, i_4})$.

(b) If $\rho \in S_n$, then ρ^{-1} has a disjoint-cycle representation with exactly the same shape as that of ρ, so one can be converted into the other by some $\sigma \in S_n$.

(c) In A_3 and A_4, $\rho = (\overleftarrow{123})$ is not conjugate to its inverse $(\overleftarrow{321})$, because if $\sigma(1) = 3$, $\sigma(2) = 2$ and $\sigma(3) = 1$ then $\sigma = (\overleftarrow{13})$ is odd. In A_7 and A_8, $(\overleftarrow{1234567})$ is not conjugate to its inverse.

In A_6, every permutation is conjugate to its inverse (calculations as in A_5, a little more complicated). In A_5, $(\overleftarrow{123})(\overleftarrow{5678})$ is not conjugate to its inverse.

*If ρ_1, $\rho_2 \in S_n$ have disjoint-cycle representations of the same form, they are conjugate in S_n, and conversely. If $\rho_1 = (\overleftarrow{1 \ldots k_1})(\overleftarrow{k_1 + 1 \ldots k_1 + k_2})(\overleftarrow{k_2 + 1 \ldots k_2 + k_3})\ldots$, then it is conjugate in A_n to ρ_2 iff $\rho_2 = (\overleftarrow{\sigma(1) \ldots \sigma(k_1)})(\overleftarrow{\sigma(k_1 + 1) \ldots \sigma(k_1 + k_2)})\ldots$ for an even permutation σ. Now if ρ_1 and ρ_2 are conjgate in S_n, we know that there is a permutation σ which does the trick, but it need not be even.

If there is an *odd* permutation σ_1 such that $\sigma_1\rho_1\sigma_1^{-1} = \rho_1$, then one of σ, σ_1 will be even, and both will transform ρ_1 to ρ_2. So in this case ρ_1 will certainly be conjugate to ρ_2 in A_n. There will be such a σ_1 if *either* ρ_1 has a cycle of even length (we can take σ_1 to be that cycle) or ρ_1 has two cycles of the same odd length (we can take σ_1 to be the product of transpositions which exchanges the two cycles). If ρ_1 has only cycles of different odd lengths (including 1-cycles), then there is no such σ_1, because the only σ such that $\sigma\rho_1\sigma^{-1} = \rho_1$ are products of powers of the cycles belonging to ρ_1.

In this second case, ρ_2 will be conjugate to ρ_1 in A_n iff *any* σ such that

$$\rho_2 = (\overleftarrow{\sigma(1) \ldots \sigma(k_1)})(\overleftarrow{\sigma(k_1 + 1) \ldots \sigma(k_2)})\ldots$$

is even. So to determine whether ρ_1 and ρ_1^{-1} are conjugate in A_n, we simply need to determine the parity of the permutation σ which reverses all the cycles of ρ_1. Now if ρ_1 has cycles of odd lengths $k_1 = 2r_1 + 1, \ldots, k_m + 2r_m + 1$ then we need just $r_1 + r_2 + \ldots + r_m$ transpositions to turn them all round.

Thus A_n will have an element ρ not conjugate to its inverse in A_n iff there are distinct numbers $r_1 < \ldots < r_m$ (allowing $r_1 = 0$) such that $2(r_1 + \ldots + r_m) + m = n$ and $r_1 + \ldots + r_m$ is odd. With $m = 1$, $r_1 = 1$, for instance, we have $n = 3$; with $m = 2$, $r_1 = 0$, $r_2 = 1$ we have $n = 4$; with $m = 1$, $r_2 = 3$ we have $n = 7$; with $m = 2$, $r_1 = 0$, $r_2 = 3$ we have $m = 8$; similarly with $m = 2$, $r_0 = 1$, $r_2 = 2$.

Taking $m = 1$, $r_1 = 2j + 1$ we get $n = 4j + 3$ for any $j \geq 0$. Taking $m = 2$, $r_1 = 0$, $r_2 = 2j + 1$ we get $n = 4j + 4$ for any $j \geq 1$. Taking $m = 3$, $r_1 = 0$, $r_2 = 1$, $r_3 = 2j$ we get $n = 4j + 5$ for any $j \geq 1$. Taking $m = 4$, $r_1 = 0$, $r_2 = 1$, $r_2 = 2$, $r_4 = 2j$ we get $n = 4j + 10$ for any $j \geq 2$. What this means is that the *only* n in which every element of A_n is conjugate in A_n to its inverse are $n = 0$, 1, 2, 5, 6, 10, 14.

21. (a) $C=\{a : ax=xa \text{ for every } x\in G\}$.
$C\lhd G$.

P method 1 $ex=x=xe$ for every x, so $e\in C$. If a, $b\in C$, then $abx=axb=xab$ for every x, so $ab\in C$. If $a\in C$, then $a^{-1}x=a^{-1}xaa^{-1}=a^{-1}axa^{-1}=xa^{-1}$ for every x, so $a^{-1}\in C$. Thus $C\le G$. If $a\in C$ and $y\in G$, then $yay^{-1}=yy^{-1}a=a\in C$; thus $C\lhd G$.

method 2 Setting $a\bullet x=axa^{-1}$ for a, $x\in G$, we have

$$e\bullet x=exe^{-1}=x,\qquad (ab)\bullet x=abx(ab)^{-1}=a(bxb^{-1})a^{-1}=a\bullet(b\bullet x)$$

for all x, a, $b\in G$, so $\bullet$ is an action of G on itself. The kernel of this action is a normal subgroup of G; but this is just

$$\{a : axa^{-1}=x\;\forall\, x\in G\}=\{a : ax=xa\;\forall\, x\in G\}=C.\ \mathbf{Q}$$

(b) Suppose that G/C is cyclic, with generator aC. If $x\in X$, then $xC=(aC)^n=a^nC$ for some $n\in\mathbb{Z}$, so $x=a^nc$ for some $n\in\mathbb{Z}, c\in C$. Now

$$xa=a^nca=a^nac=aa^nc=ax.$$

This is true for every $x\in G$, so $a\in C$ and $aC=C$ is the identity of G/C and G/C has just one element and $C=G$.

(c) Suppose that $\#(G)=p^r$ where p is a prime and $r\ge 1$. Consider the orbits in G under the action of G on itself. If $x\in G\setminus C$, there is an $a\in G$ such that $ax\ne xa$, that is, $axa^{-1}\ne x$, and $\mathrm{Orb}(x)\ne\{x\}$, so $\#(\mathrm{Orb}(x))>1$. But $\#(\mathrm{Orb}(x))$ is a factor of $\#(G)=p^r$, so must be a multiple of p. This shows that $\#(G\setminus C)$ is a multiple of p and $\#(C)$ is a multiple of p. In particular, $C\ne\{e\}$.

(d) Because $C\le G$, $\#(C)$ must be a factor of p^2, that is, 1 or p or p^2. By (c), it cannot be 1. By (b), G/C cannot be of order p, so $\#(C)\ne p$. We are left with only one possibility, $\#(C)=p^2$, so that $C=G$ and G is abelian.

(e) D_4 has $8=2^3$ members; if we take the standard generators ρ, σ such that $\rho^4=\sigma^2=e$ and $\sigma\rho\sigma^{-1}=\rho^{-1}$, the centre is $\{e,\rho^2\}$.

22. **(a)** If G is a group, an *automorphism* of G is an isomorphism from G to itself.

If $a\in G$, then the function $x\mapsto\hat a(x)=axa^{-1}: G\to G$ is an automorphism. **P** $\hat a(xy)=axya^{-1}=axa^{-1}aya^{-1}$ for all x, $y\in G$, so $\hat a$ is a homomorphism. If $axa^{-1}=aya^{-1}$ then $x=y$ by the cancellation law, so $\hat a$ is injective. If $y\in G$ then $\hat a(a^{-1}ya)=aa^{-1}yaa^{-1}=y$, so $\hat a$ is surjective, therefore an automorphism. **Q** Automorphisms of this kind are called inner automorphisms.

The identity function from G to itself is an isomorphism, so belongs to $\mathrm{Aut}\,G$. If ϕ, $\psi\in\mathrm{Aut}\,G$, then the composition $\phi\psi$ belongs to $\mathrm{Aut}\,G$, because the composition of two isomorphisms is an isomorphism. If $\phi\in\mathrm{Aut}\,G$, then $\phi^{-1}\in\mathrm{Aut}\,G$, because the inverse of an isomorphism is an isomorphism. So $\mathrm{Aut}\,G$ is a subgroup of the group S_G of bijections from G to itself, and is a group in its own right.

(b)(i) Consider the conjugacy action of G on itself given by the formula $a\bullet x=\hat a(x)=axa^{-1}$. We know that this corresponds to a homomorphism $a\mapsto\hat a: G\to S_G$. The image of this homomorphism is J, which must therefore be a subgroup of S_G; because also $J\subseteq\mathrm{Aut}\,G$, as noted in (a), J is a subgroup of $\mathrm{Aut}\,G$. The kernel of the homomorphism is

$$\{a:\hat a=\iota\}=\{a : axa^{-1}=x\;\forall\, x\in G\}=\{a : ax=xa\;\forall\, x\in G\}=C.$$

So $C\lhd G$ and $G/C\cong J$, by the First Isomorphism Theorem.

(ii) Now suppose that $a\in G$ and $\phi\in\mathrm{Aut}\,G$, and consider $\phi\hat a\phi^{-1}$. Set $b=\phi(a)$. Then for any $x\in G$,

$$\begin{aligned}(\phi\hat a\phi^{-1})(x)&=\phi(\hat a(\phi^{-1}(x)))=\phi(a\phi^{-1}(x)a^{-1})\\&=\phi(a)\phi(\phi^{-1}(x))\phi(a^{-1})=bxb^{-1}=\hat b(x)\in J.\end{aligned}$$

As ϕ and a are arbitrary, $J\lhd\mathrm{Aut}\,G$.

(c)(i) As G is abelian, $C = G$ and $J = \{\iota\}$. Since the multiplication table of G is symmetric in the three elements of order 2 (the product of any two of them is the third), any permutation of these elements corresponds to an automorphism of G, and $\mathrm{Aut}\, G \cong S_3$.

(ii) $C = \{e\}$ so $J \cong G$. There are three elements of G of order 2, and any element of G is a product of these; so an automorphism of G is determined by its values on the transpositions, and there can be at most 3! automorphisms. As $\#(J) = 6$, $J = \mathrm{Aut}\, G$ and $\mathrm{Aut}\, G \cong S_3 = G$.

(iii) $C = G$ so $J = \{\iota\}$. G has two elements of order 6; an element of $\mathrm{Aut}\, G$ must either keep them in their places or exchange them; since both generate G, $\mathrm{Aut}\, G$ has at most two members. Because G is abelian, $x \mapsto x^{-1}$ is an automorphism, and $\mathrm{Aut}\, G \cong \mathbb{Z}_2$.

(iv) $C = G$ so $J = \{\iota\}$. If $\phi : G \to G$ is an automorphism, set $j = \phi(1)$. Then $\phi(2) = j +_5 j = 2 \times_5 j$, $\phi(3) = j +_5 j +_5 j = 3 \times_5 j$ etc., where $+_5$, $\times_5$ are addition and multiplication mod 5. Because 5 is prime, this defines an automorphism of G for any $j \in \mathbb{Z}_5^* = \{1, 2, 3, 4\}$. The group operation of $\mathrm{Aut}\, G$ corresponds to $\times_5$ on $\mathbb{Z}_5^*$; so that $2 \times_5 2 = 4$ and $2 \times_5 2 \times_5 2 = 3$, and $\mathrm{Aut}\, G \cong (\mathbb{Z}_5^*, \times_5) \cong (\mathbb{Z}_4, +_4)$ is cyclic.

(v) If we express $G = D_4$ in terms of generators ρ and σ where $\rho^4 = \sigma^2 = e$ and $\sigma\rho\sigma^{-1} = \rho^{-1}$, then $C = \{e, \rho^2\}$. Since $x^2 \in C$ for every $x \in G$, $J \cong G/C$ has every element of order 1 or 2, and is congruent to K.

Next, $\mathrm{Aut}\, G \cong D_4$. **P** If $\phi \in \mathrm{Aut}\, G$, then $\phi(e) = e$ and $\phi[C] = C$, so $\phi(\rho^2) = \rho^2$. Let $Q = \{\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$ be the other four members of G of order 2. Then $\phi(a) \in Q$ for every $a \in Q$. What this means is that $\mathrm{Aut}\, G$ acts on Q. Because every element of G can be expressed as a product of elements of Q, this action is faithful and $\mathrm{Aut}\, G$ can be identified with a subgroup of the group S_Q of bijections from Q to itself. If we arrange the elements of Q in order around a square, we see that every element of $\mathrm{Aut}\, G$ leaves opposite corners as opposite corners (because it leaves ρ^2 unmoved), so $\mathrm{Aut}\, G$ corresponds to a subgroup of D_4. To see that it corresponds to the whole of D_4, observe that the defining relations remain true of ρ and $\sigma\rho$ (since $(\sigma\rho)^2 = e$ and $(\sigma\rho)\rho(\sigma\rho)^{-1} = \rho^{-1}$), so there is a $\psi_1 \in \mathrm{Aut}\, G$ with $\psi_1(\rho) = \rho$, $\psi_1(\sigma) = \sigma\rho$, corresponding to a 90° rotation of Q; and also that $\hat{\sigma}(\sigma\rho^j) = \sigma\rho^{-j}$, so that $\hat{\sigma}$ corresponds to a reflection in the diagonal $(\sigma, \sigma\rho^2)$. So $\mathrm{Aut}\, G$ corresponds to the whole of D_4. **Q**

23. **(a)** If $g_1,\, g_2,\, g_3 \in G$ and $h_1,\, h_2,\, h_3 \in H$ then

$$\begin{aligned}(g_1,h_1)*((g_2,h_2)*(g_3,h_3)) &= (g_1,h_1)*(g_2\cdot\phi(h_2)(g_3),h_2h_3)\\ &= (g_1\cdot\phi(h_1)(g_2\cdot\phi(h_2)(g_3)),h_1h_2h_3)\\ &= (g_1\cdot\phi(h_1)(g_2)\cdot\phi(h_1)(\phi(h_2)(g_3))),h_1h_2h_3)\\ &= (g_1\cdot\phi(h_1)(g_2)\cdot\phi(h_1)\circ\phi(h_2))(g_3)),h_1h_2h_3)\\ &= (g_1\cdot\phi(h_1)(g_2)\cdot\phi(h_1h_2)(g_3)),h_1h_2h_3)\\ &= (g_1\cdot\phi(h_1)(g_2),h_1h_2)*(g_3,h_3)\\ &= ((g_1,h_1)*(g_2,h_2))*(g_3,h_3).\end{aligned}$$

Thus $(G\times H,*)$ is a semigroup.

If $(g,h)\in G\times H$, then

$$(g,h)*(e_G,e_H) = (g\cdot\phi(h)(e_G),he_H) = (ge_G,h) = (g,h).$$

Set $g_1=\phi(h^{-1})(g^{-1})$, $h_1=h^{-1}$; then

$$\begin{aligned}(g_1,h_1)*(g,h) &= (\phi(h^{-1})(g^{-1})\cdot\phi(h^{-1})(g),h^{-1}h)\\ &= (\phi(h^{-1})(g^{-1}g),e_H) = (\phi(h^{-1})(e_G),e_H) = (e_G,e_H).\end{aligned}$$

By the result in 1(c), $(G\times H,*)$ is a group.

[Of course it is also easy to check directly that $(e_G,e_H)*(g,h)=(g,h)$ and $(g,h)*(g_1,h_1)=(e_G,e_H)$.]

(b) If $g_1,\, g_2\in G$ then

$$(g_1,e_H)*(g_2,e_H) = (g_1\cdot\phi(e_H)(g_2),e_He_H) = (g_1g_2,e_H).$$

Thus the map $g\mapsto(g,e_H):G\to G\times H$ is a homomorphism. Since it is injective, its image G' is a subgroup of $G\times H$ isomorphic to G.

If we look at the second-coordinate map $(g,h)\mapsto h:G\times H\to H$, we see that this is a homomorphism with kernel G'; so G' is a normal subgroup of $G\times H$.

(c) If $h_1,\, h_2\in H$ then

$$(e_G,h_1)*(e_G,h_2) = (e_G\cdot\phi(h_1)(e_G),h_1h_2) = (e_Ge_G,h_1h_2) = (e_G,h_1h_2).$$

Thus the map $h\mapsto(e_G,h):H\to G\times H$ is a homomorphism. Since it is injective, its image is a subgroup of $G\times H$ isomorphic to H.

(d) For $h\in H$, $g\in G$ set $\phi(h)(g)=hgh^{-1}$. Because $G\lhd Q$, $\phi(h):G\to G$ is a function; because the conjugacy action corresponds to a homomorphism from H to $\operatorname{Aut}Q$, ϕ is a homomorphism from H to $\operatorname{Aut}G$. Let $*$ be the corresponding product on $G\times H$. Define $\psi:G\times H\to Q$ by setting $\psi(g,h)=gh$ for $g\in G$, $h\in H$. If $g_1,\, g_2\in G$ and $h_1,\, h_2\in H$ then

$$\begin{aligned}\psi((g_1,h_1)*(g_2,h_2)) &= \psi(g_1\cdot\phi(h_1)(g_2),h_1h_2) = \psi(g_1h_1g_2h_1^{-1},h_1h_2)\\ &= g_1h_1g_2h_1^{-1}h_1h_2 = g_1h_1g_2h_2 = \psi(g_1,h_1)\psi(g_2,h_2).\end{aligned}$$

Thus ψ is a homomorphism. Because $GH=Q$, ψ is surjective. If $g\in G$, $h\in H$ are such that $\psi(g,h)=e$, then $gh=e$, so $g=h^{-1}\in G\cap H$, $g=e$ and $h=e$; thus the kernel of ψ is $\{(e,e)\}$, the trivial subgroup of $G\times H$, and ψ is injective. So ψ is an isomorphism.

24. **(a)** If $D \in X$, then $D = dH$ for some $d \in G$, so $a{\bullet}D = a(dH) = (ad)H \in X$. Now if a, $b \in G$ and $D \in X$,

$$a{\bullet}(b{\bullet}D) = a(bD) = (ab)D = ab{\bullet}D, \quad e{\bullet}D = eD = D.$$

(b) Let $a \in K$. Since $H = eH \in X$, $aH = H$ so $a \in H$; thus $K \subseteq H$.

If we interpret the action as a homomorphism ϕ from G to the group S_X of bijections from X to itself, $G/K \cong \phi[G]$, which is a subgroup of S_X. Now $\#(X) = \frac{\#(G)}{\#(H)} = m$, by Lagrange's theorem, so $\#(S_X) = m!$ and $\#(G/K) = \#(\phi[G])$ is a factor of $m!$.

(c) Suppose that $K = H$ and that $a \in G$, $h \in H$. Then $haH = h{\bullet}(aH) = aH$, so $ha \in aH$. As h is arbitrary, $Ha \subseteq aH$. Similarly, $Ha^{-1} \subseteq a^{-1}H$ so $aH \subseteq Ha$ and $aH = Ha$. As a is arbitary, $H \triangleleft G$.

(d) If m is a prime and is the smallest prime factor of $\#(G)$, then m is the greatest common divisor of $\#(G)$ and $m!$, so $\#(G/K)$ must be a factor of m, that is, $\frac{\#(G)}{\#(K)}$ is a factor of $\frac{\#(G)}{\#(H)}$. Since $K \subseteq H$, we must have $K = H$ and $H \triangleleft G$.

(e) Suppose that $H \leq A_5$. Setting $m = \frac{60}{\#(H)}$, A_5 has a normal subgroup K such that $K \subseteq H$ and $\frac{60}{\#(K)}$ is a factor of $m!$. But this means that either $K = \{e\}$ and $m \geq 5$ and $\#(H) \leq 12$, or $K = A_5$ and $H = A_5$.

(f) A_5 has a subgroup of order n iff $n = 1$, 2, 3, 4, 6, 10, 12 or 60. **P** By (e) and Lagrange's theorem, these are the only possibilities. For examples of subgroups of these orders:

$\{e\}$ has order 1.

$<(\overleftarrow{12})(\overleftarrow{34})>$ has order 2.

$<(\overleftarrow{123})>$ has order 3.

$\{e, (\overleftarrow{12})(\overleftarrow{34}), (\overleftarrow{13})(\overleftarrow{24}), (\overleftarrow{14})(\overleftarrow{23})\}$ has order 4.

$<(\overleftarrow{12345})>$ has order 5.

Set $\rho = (\overleftarrow{123})$ and $\sigma = (\overleftarrow{12})(\overleftarrow{34})$. Then $\rho^3 = \sigma^2 = e$ and $\sigma\rho\sigma^{-1} = \rho^{-1}$. So $\{e, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$ is a subgroup of A_5 of order 6.

Set $\rho = (\overleftarrow{12345})$ and $\sigma = (\overleftarrow{15})(\overleftarrow{24})$. Then $\rho^5 = \sigma^2 = e$ and $\sigma\rho\sigma^{-1} = \rho^{-1}$. So $\{e, \rho, \rho^2, \rho^3, \rho^4, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3, \sigma\rho^4\}$ is a subgroup of A_5 of order 10.

A_4 is a subgroup of A_5 of order 12.

A_5 is a subgroup of A_5 of order 60.