Section 1

Suitable Questions from Jordan and Jordan.

- We will come back to the exercises in Chapter 1 once we have done group actions.
- Chapter 2, Questions 1–2, 4, 6–12 and 14–20 are practise with permutations, and should mainly be revision from Proofs and Problem Solving [L, §20]. It is important that you can do them.

1.1 (Revision of functions) We often take functions for granted, but this is dangerous. Are the following functions?

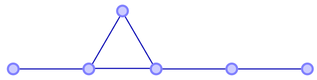
1. $\mathbb{Z} \to \mathbb{Z}$ sending $a \mapsto a + 2$.
2. $\mathbb{Q} \to \mathbb{Q}$ sending $\frac{a}{b} \mapsto \frac{a}{b} + 2$.
3. $\mathbb{Q} \to \mathbb{Z}$ sending $\frac{a}{b} \mapsto a + b$.
4. $\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ sending $(a, b) \mapsto a + 2$.
5. $\mathbb{Q} \times \mathbb{Z} \to \mathbb{Q}$ sending $(\frac{a}{b}, z) \mapsto \frac{a}{bz} + 2$.
6. $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ sending $(\frac{a}{b}, \frac{c}{d}) \mapsto \frac{a}{b} + \frac{c}{d}$.
7. $\mathbb{Q} \times \mathbb{Q} \to \mathbb{Q}$ sending $(\frac{a}{b}, \frac{c}{d}) \mapsto \frac{a+c}{b+d}$.

Solution In each case, denote the rule by f. To be a function, we need f to take an element x of the domain to a *single* element $f(x)$ in the codomain. Formally, this means that we need to show that $x = y$ implies that $f(x) = f(y)$.

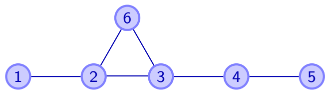
1. Yes. If $a = b$ then $a + 2 = b + 2$ so $f(a) = f(b)$.
2. Yes. If $\frac{a}{b} = \frac{c}{d}$ then $\frac{a}{b} + 2 = \frac{c}{d} + 2$ so $f(\frac{a}{b}) = f(\frac{c}{d})$.
3. No. $\frac{1}{1} = \frac{2}{2}$ but $f(\frac{1}{1}) = 1 + 1 = 2 \neq 4 = 2 + 2 = f(\frac{2}{2})$, so $f(\frac{1}{1}) \neq f(\frac{2}{2})$.
4. Yes. If $(a_1, b_1) = (a_2, b_2)$ then $a_1 = a_2$ and so $a_1 + 2 = a_2 + 2$, hence $f(a_1, b_1) = f(a_2, b_2)$.
5. No. The rule does not assign to $(\frac{1}{1}, 0) \in \mathbb{Q} \times \mathbb{Z}$ an element in $\mathbb{Q}$.
6. Yes. If $(\frac{a_1}{b_1}, \frac{c_1}{d_1}) = (\frac{a_2}{b_2}, \frac{c_2}{d_2})$ then $\frac{a_1}{b_1} = \frac{a_2}{b_2}$ and $\frac{c_1}{d_1} = \frac{c_2}{d_2}$, so $a_1 b_2 = a_2 b_1$ and $c_1 d_2 = c_2 d_1$. Now on one hand
$$f\left(\frac{a_1}{b_1}, \frac{c_1}{d_1}\right) = \frac{a_1}{b_1} + \frac{c_1}{d_1} = \frac{a_1 d_1 + c_1 b_1}{b_1 d_1}$$
whilst on the other
$$f\left(\frac{a_2}{b_2}, \frac{c_2}{d_2}\right) = \frac{a_2}{b_2} + \frac{c_2}{d_2} = \frac{a_2 d_2 + c_2 b_2}{b_2 d_2}.$$
These two expressions are equal, since
$$\begin{aligned}(a_1 d_1 + c_1 b_1) b_2 d_2 &= a_1 b_2 d_1 d_2 + c_1 d_2 b_1 b_2 \\ &= a_2 b_1 d_1 d_2 + c_2 d_1 b_2 b_1 \\ &= (a_2 d_2 + c_2 b_2) b_1 d_1.\end{aligned}$$
7. No. $(\frac{1}{1}, \frac{1}{2}) = (\frac{1}{1}, \frac{2}{4})$, but $f(\frac{1}{1}, \frac{1}{2}) = \frac{2}{3} \neq \frac{3}{5} = f(\frac{1}{1}, \frac{2}{4})$.

1.2 Find a graph whose only symmetry is the identity.

Solution The easiest example is the graph with only one vertex. A more substantial example is the graph



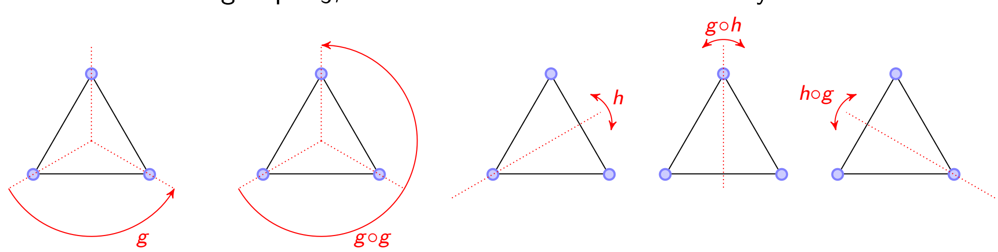
For convenience, number the vertices



and let f be a symmetry. We will argue that f must be the identity. Note first that $f(2) = 2$ or 3 and $f(3) = 3$ or 2 since these are the only vertices with valency three. Either way, this means that f must fix 6 since $f(6)$ must be connected to both $f(2)$ and $f(3)$. The only other valency two vertex is 4 and so it must also be fixed. This forces 5 to be fixed (as it is the only valency one vertex connected to $f(4) = 4$), and hence 1 must be fixed (as it is the only valency one vertex that is left). This in turn forces 2 to be fixed (as it must be connected to $f(1) = 1$) and so $f(3) = 3$. Hence f fixes everything, so it is the identity.

(Note: in lectures, in the definition of a graph we assumed that there is at most one edge joining two given vertices and no edge joins a vertex to itself. If we drop either assumption, producing examples here is much easier.)

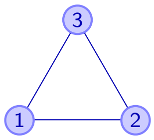
1.3 Consider the group D_3, which has as elements the identity e and



1. Verify, using a similar argument as in lectures (or otherwise), that these are all the symmetries of the 3-gon.
2. Verify that $h \circ g = g \circ g \circ h$ and so the elements of D_3 are $\{e, g, g \circ g, h, g \circ h, g \circ g \circ h\}$. As in lectures, we drop the $\circ$ and write $D_3 = \{e, g, g^2, h, gh, g^2h\}$.
3. (Cayley Table) Calculate all possible multiplications in D_3. In other words complete the table below, where by definition the entry in the (r, c) position (where r is the row, c the column) is the product $r \circ c$

	e	g	g^2	h	gh	g^2h
e	e	g	g^2			
g	g	g^2	e			
g^2	g^2	e	g			
h						
gh						
g^2h						

Solution 1. Label the vertices

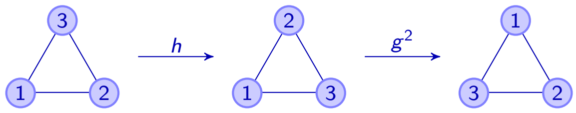


so that $V = \{1, 2, 3\}$. Let $f : V \to V$ be a symmetry. If f fixes 1, then either f fixes both 2 and 3 (so f is the identity), or f swaps 2 and 3 (so f is the element h). Hence we can assume that f does not fix 1. If $f(1) = 2$ then either

$$\begin{cases} f(2) = 3 \\ f(3) = 1 \end{cases} \quad \text{or} \quad \begin{cases} f(2) = 1 \\ f(3) = 3 \end{cases}.$$

The left hand case is g, the right hand case is $g \circ h$. The only other option is $f(1) = 3$, which by similar reasoning must be either g^2 or $h \circ g$.

2. This is direct verification. We know from lectures that $h \circ g$ is reflection in the line through the bottom right vertex. Further

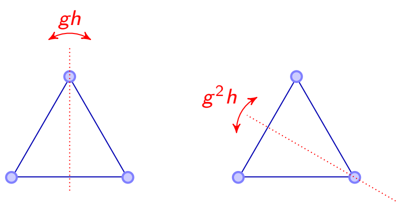


which is also reflection in the line through the bottom right vertex.

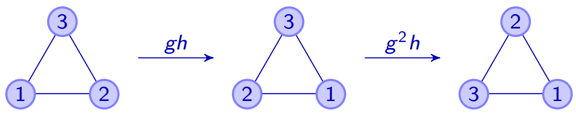
3. This can be done algebraically or pictorially. For example, by part (2)

$$(g^2h)(gh) = g^2(hg)h = g^4h^2 = g$$

since $g^3 = e$ and $h^2 = e$. Alternatively



and so



which is clearly g, hence $(g^2h) \circ (gh) = g$.

Either way, verifying all possibilities gives

	e	g	g^2	h	gh	g^2h
e	e	g	g^2	h	gh	g^2h
g	g	g^2	e	gh	g^2h	h
g^2	g^2	e	g	g^2h	h	gh
h	h	g^2h	gh	e	g^2	g
gh	gh	h	g^2h	g	e	g^2
g^2h	g^2h	gh	h	g^2	g	e

1.4 Show that in D_n, the identity e, the $n-1$ rotations and the n reflections are precisely the elements

$$\{e, g, g^2, \dots, g^{n-1}, h, gh, g^2h, \dots, g^{n-1}h\},$$

where g and h were defined in Lecture 2. Then, by modifying your argument to Problem 1.3, show that these are all the symmetries of the n-gon.

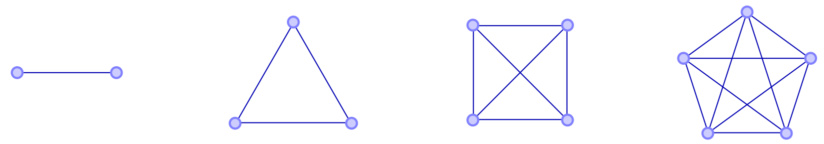
Solution The first part is direct verification, as in lectures, and is tedious to write down.

For the second part of the question, if $f(1) = 1$, then argue that f is e or h. If $f(1) = 2$ then argue that f is g or $h \circ g$. If $f(1) = 3$ then argue that f is g^2 or $h \circ g^2$. Continuing in this way shows that there are precisely $2n$ elements.

(The point of the last part of the question is that the above argument is quite messy. After we know a little theory, an easier solution is given in the Workshops.)

1.5 In lectures we showed that we can view the symmetric group S_n as symmetries of the graph with n vertices and no edges. For every $n \geq 2$, produce a *different* graph which also has symmetry group S_n. This is part of the general phenomenon that many different graphs can have the same symmetry group.

Solution There are many different solutions. For example, let G_n be the graph with n vertices, in which every vertex is connected to all other vertices, i.e.

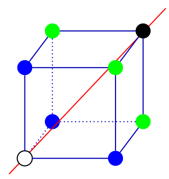


$n = 2$ $\qquad$ $n = 3$ $\qquad$ $n = 4$ $\qquad$ $n = 5$

Then $f(1)$ can be any member of $\{1, \dots, n\}$, $f(2)$ can be any member of $\{1, \dots, n\} \backslash \{f(1)\}$, $f(3)$ can be any member of $\{1, \dots, n\} \backslash \{f(1), f(2)\}$ etc. Thus every symmetry of G_n gives a member of S_n, and all members of S_n arise in this way.

1.6 We would like an example of a rotational symmetry of the cube which, if repeated three times, gives the identity. The identity itself has this property. Are there any others?

Solution Rotation about the line through the black and white vertices



is such an example. It rotates the three green vertices and the three blue vertices, and so after three applications it gives the identity.

1.7 How many elements does $\mathrm{GL}(2, \mathbb{Z}_2)$ have? How about $\mathrm{GL}(n, \mathbb{Z}_p)$ with p a prime?

Solution $\mathrm{GL}(2,\mathbb{Z}_2)$ has six elements. This follows from the more general formula

$$|\mathrm{GL}(n,\mathbb{Z}_p)| = (p^n-1)(p^n-p)(p^n-p^2)\dots(p^n-p^{n-1})$$

To see this, an element of $\mathrm{GL}(n,\mathbb{Z}_p)$ is given by specifying a non-zero vector v_1 in $\mathbb{Z}_p^n$ to go in the first column (of which there are p^n-1 possibilities), then a vector outwith the span of v_1 to go in the second column (of which there are p^n-p possibilities), then a choice of p^n-p^2 elements to go in the third column, etc. Substituting $p=n=2$ we see that

$$|\mathrm{GL}(2,\mathbb{Z}_2)| = 3\times 2 = 6.$$

1.8 Are the following operations? For the ones that are operations, do they make the set into a group?

1. $\mathbb{Z}$ with $a*b := a+2$.
2. $\mathbb{Z}$ with $a*b := a+b$.
3. $\mathbb{Q}$, with $\frac{a}{b}*\frac{c}{d} := \frac{a}{b}+\frac{c}{d}$.
4. $\mathbb{Q}$, with $\frac{a}{b}*\frac{c}{d} := \frac{a+c}{b+d}$.

Solution

1. Yes, this is an operation, by Problem 1.1(d). It does not make $\mathbb{Z}$ into a group, since if $e\in\mathbb{Z}$ was the identity, then $e*z=z=z*e$ for all $z\in\mathbb{Z}$. But we have $e*z=e+2$ and $z*e=z+2$, hence we require that $e=z$ for all $z\in\mathbb{Z}$, which is a contradiction since the identity e must be unique. (Note that there are many other possible arguments for this question)
2. Yes, this is just the group $\mathbb{Z}$ under addition.
3. Yes, this is just the field $\mathbb{Q}$ under addition.
4. No, this is not an operation by Problem 1.1(g).

1.9 Are the following groups?

1. The set $G=\{a+bi\,|\,a,b\in\mathbb{Z}\}$ with group operation given by addition of complex numbers.
2. The set $G=\{a+bi\,|\,a,b\in\mathbb{Z}\text{ and } a,b \text{ not both zero}\}$ with group operation given by multiplication of complex numbers.
3. The set $G=\{a+bi\,|\,a,b\in\mathbb{Q}\text{ and } a,b \text{ not both zero}\}$ with group operation given by multiplication of complex numbers.
4. The set $K=\{e,x,y,z\}$ with the abelian multiplication defined by

$$x^2=y^2=z^2=e,\ xy=z,\ yz=x,\ zx=y$$

and $eg=g$ for all $g\in K$. (Note: you need to check for the existence of inverses and for whether the multiplication is associative: try and organize your reasoning for the latter, exploiting symmetry rather than checking all 64 possibilities.)

Solution

1. Yes. Addition is closed, zero is the identity and the inverse of $a+ib$ is $-a-ib$.
2. No — most elements don't have inverses.
3. Yes. Just check the axioms. You need the co-efficients in $\mathbb{Q}$ to construct the inverse.
4. Yes. It is not empty, and clearly e acts as an identity. Each of x, y, z is its own inverse so no problem there, so inverses exist. For associativity, we must check that $(ab)c = a(bc)$ for all $a, b, c \in K$. If any of a, b, c is the identity that is trivial, as indeed it is if they are all equal. If two are the same we have two cases: $x(xy) = (xx)y$ which reduces to $xz = ey = y$ which is fine and $x(yx) = (xy)x$ which similarly reduces to $xz = zx$. Finally if all three are different we have $x(yz) = (xy)z$ which reduces to $x^2 = z^2$ or $e = e$. Now the obvious symmetry of the definitions means that these cases imply those where any permutation is applied to the x, y, z, hence we have covered all cases.

   Alternatively, for the last part note that we can regard x, y, z as the three non-zero vectors in $\mathbb{Z}_2^2$, and we know that $\mathbb{Z}_2^2$ is a vector space.

1.10 Fix $n \in \mathbb{N}$ and consider multiplication mod n. Let G be the subset of $\{1, 2, \ldots, n-1\}$ consisting of all those elements that have a multiplicative inverse (under multiplication mod n). Show that G is a group under multiplication. Describe this group when $n = 12$.

Solution Clearly if a and b both have a multiplicative inverse, then ab has a multiplicative inverse (namely $a^{-1}b^{-1}$) and so the operation is closed. It is associative since multiplying numbers is always associative. Further $1 \in G$ (since $1 \times 1 = 1$ and so 1 has a multiplicative inverse), hence G has an identity. Also, if $k \in G$ then k has a multiplicative inverse k^{-1} and so k^{-1} has multiplicative inverse k, hence $k^{-1} \in G$. Thus we have inverses and so G is a group. When $n = 12$, $G = \{1, 5, 7, 11\}$.

Section 2

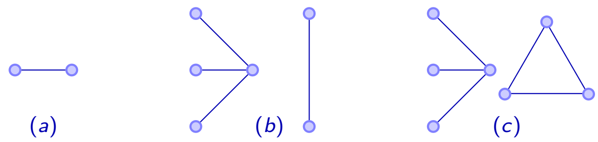
Suitable Questions from Jordan and Jordan.

- Chapter 4, Questions 1–11 (all questions).
- Chapter 5, Questions 1–13 (all questions).
- Chapter 6, Questions 1–21 (all questions).

Products

2.1 Give examples of graphs which have symmetry groups $\mathbb{Z}_2$, $S_3 \times \mathbb{Z}_2$ and $S_3 \times D_3$ respectively.

Solution Consider, for example



That (a) has symmetry group $\mathbb{Z}_2$ is clear. That (b) has symmetry group $S_3 \times \mathbb{Z}_2$ and (c) has symmetry group $S_3 \times D_3$ follows from the general theory in Workshop 1. (It can also be argued directly).

Subgroups

2.2 Suppose that G is a *finite* group and let H be a non-empty subset of G. Show that H is a subgroup of G if and only if $h, k \in H$ implies that $hk \in H$.

Solution ($\Rightarrow$) is trivial.
($\Leftarrow$) We just need to verify that H is closed under inverses. so let $h \in H$. Since G is finite, $h^{|G|} = e$ (this is a consequence of Lagrange, see [JJ, §10, Thm. 7]), hence $h^{|G|-1} = h^{-1}$. Since $h^{|G|-1} \in H$ (we are assuming that H is closed under products), $h^{-1} \in H$.

2.3 For each of the following, is H a subgroup of G?

1. $G = \mathbb{Z}$ (under addition) and H is all the elements that are multiples of both 3 and 5.
2. $G = \mathbb{Z}$ (under addition) and H is all the elements that are multiples of 3 or multiples of 5.
3. Consider a non-zero vector v in $\mathbb{R}^n$. Take $G = \mathrm{GL}(n, \mathbb{R})$ and
$$H = \{g \in G \,|\, gv = \lambda v \text{ for some } \lambda \in k\}.$$

Solution

1. Yes, since H consists of all multiples of 15, which is certainly a subgroup.
2. No, since 3 and 5 are in G but $3 + 5 = 8$ is not.
3. Yes. The identity has the required property. If $h \in H$ then $hv = \lambda v$ for some λ and $\lambda \neq 0$ since h is invertible. Then $h^{-1}v = (1/\lambda)v$ and so $h^{-1} \in H$. Finally, if $h, h' \in H$ then there exists λ, λ' such that $hv = \lambda v$ and $h'v = \lambda' v$. Then $hh'v = \lambda\lambda' v$ and so $hh' \in H$.

2.4 Let $H_1, \dots, H_k$ be subgroups of G. Prove that their intersection $\bigcap_{j=1,\dots,k} H_j$ is a subgroup of G.

Solution Denote the intersection by H. The identity is in H_j for all j and hence in H. If $g \in H$ then $g \in H_j$ for all j. Hence $g^{-1} \in H_j$ for all j and so $g^{-1} \in H$. Finally, let $x, y \in H$. Then x, y are in all the H_j, hence xy is in all the H_j, so $xy \in H$. Hence H is a subgroup.

Cyclic and abelian groups

2.5 Show that if G is cyclic, then G is abelian. Give an example of an abelian group that is not cyclic.

Solution If $G = \langle g \rangle$ then every element of G can be written as g^k for some $k \in \mathbb{Z}$. We know that $g^k g^l = g^{k+l} = g^l g^k$ for all $l, k \in \mathbb{Z}$. Hence G is abelian. For the last part, an example would be $\mathbb{Z}_2 \times \mathbb{Z}_2$, which has no element of order 4.

2.6 Let G be cyclic and suppose $G = \langle g \rangle$. Show that if $H \leq G$ and $g \in H$ then $H = G$.

Solution Since H is closed under multiplication, if $g \in H$ then $\langle g \rangle \leq H$. Thus we have a chain of inclusions $G = \langle g \rangle \leq H \leq G$ and hence equality holds throughout.

2.7 Find a non-trivial symmetry f of the square (that is, an element of D_4 that is not the identity) that commutes with all the other elements. Which of the groups D_n have such an element?

Solution The half-turn g^2 is the only such symmetry. The groups D_n have such a symmetry if and only if n is even.

2.8 Show that if $g^2 = e$ for all $g \in G$, then G is abelian.

Solution For all g, h we have $gh \in G$ and so $e = (gh)^2 = ghgh$. Multiplying on the left by g and on the right by h, we get $g^2hgh^2 = gh$. Now $g^2 = e = h^2$ implies that $hg = gh$.

2.9 Consider the symmetry groups of the graphs in Workshop 1. Which of them are abelian?

Solution In short, any graph whose symmetries involve permutations of three or more things can't be abelian since S_3 isn't. So (a),(b),(d),(f) have nonabelian symmetry groups. On the other hand, (c) and (e) both only have four elements, hence are abelian (hint: either its cyclic, or you can use Problem 2.8).

2.10 Let G be the group of 2×2 invertible matrices with entries in $\mathbb{R}$. Let H be the subset consisting of those matrices which are upper-triangular and of determinant 1. Show that H is a subgroup of G. Show that if we replace $\mathbb{R}$ by $\mathbb{Z}_3$, then H is cyclic and hence abelian. Show also that if we replace $\mathbb{R}$ by $\mathbb{Z}_5$ then H is not abelian.

Solution The product of upper-triangular matrices, the inverse of an upper-triangular matrix, and the identity are all upper-triangular. Thus (since $\det(AB) = \det A \det B$) the product of elements in H belongs to H, and (since $\det A^{-1} = (\det A)^{-1}$), the inverse of an element in H is in H. Hence H is a subgroup.

For $\mathbb{Z}_3$ one easily checks that either both diagonal elements are 1 or both are 2. The top-right element can be 0,1 or 2. So we have a six-element group. A bit of trial and error shows that $t = 6$ is the smallest such that $A^t = \mathbb{I}$, where

$$A = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}.$$

Hence G is cyclic, with $G = \langle A \rangle$. We know (by Problem 2.5) that this implies that G is abelian. For the last part, note

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

but

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

2.11 Show that $\mathbb{Z}_7^*$ (the multiplicative group of nonzero integers mod 7) is a cyclic group.

Solution By experimenting, one finds that the group is $\langle 3 \rangle$ or $\langle 5 \rangle$ as both 3 and 5 have order six.

Order

2.12 Let $x = (g, h) \in G \times H$. Express the order of x in $G \times H$ in terms of the order of g in G and the order of h in H. (A proof is required!)

Solution First, note that

$$(g, h)^k = 1_{G \times H} \iff (g^k, h^k) = (1_G, 1_H) \iff g^k = 1_G \text{ and } h^k = 1_H.$$

Hence the order of $x = (g, h)$ is the *smallest* k such that $g^k = 1_G$ and $h^k = 1_H$. By definition of order of g and h, this is equal to the lowest common multiple of $o(g)$ and $o(h)$.

2.13 In the dihedral group D_6 what are the orders of the various symmetries? (Think carefully and if necessary cut a regular hexagon out of paper and experiment.)

Solution In brief: the identity has order 1, and all the six reflections have order 2. There are two rotations by one sixth of a turn (g and g^{-1}) which have order 6, two by one third (g^2 and g^{-2}) that have order 3, and one by half a turn ($g^3 = g^{-3}$) which has order 2.

2.14 What is the order of the various elements of the symmetric group S_3?

Solution In the order

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$

we have the identity which has order 1, the next three just swap two elements and so have order 2, and the last two have order 3 (they cycle round the three elements).

2.15 Consider $\mathbb{Z}_n$ under addition. Find the orders of all the elements in the cases $n = 3, 4, 5, 6$. What is your guess for the possible orders of elements in $\mathbb{Z}_n$?

Solution The orders of the elements $0, \dots, n-1$ are as follows:

- $n = 3$ orders: 1,3,3
- $n = 4$ orders: 1,4,2,4
- $n = 5$ orders: 1,5,5,5,5
- $n = 6$ orders: 1,6,3,2,3,6

The guess is that one has elements of every order that divides n.

2.16 Suppose $o(g) = k$. If $n \in \mathbb{N}$, show that $g^n = e$ if and only if n is a multiple of k.

Solution ($\Rightarrow$) Suppose $n = kl$. Then $g^n = (g^k)^l = e^l = e$.
($\Leftarrow$) Suppose that $o(g) = k$ and $g^n = e$. Write $n = lk + r$ for some $l \in \mathbb{Z}_{\geq 0}$ and some $0 \leq r < k$. Then $g^{lk+r} = e$. But $g^{lk} = e$ and so it follows that $g^r = e$. Since $r < k$ and k is the smallest non-negative power of g which is the identity, we must have $r = 0$.

2.17 Suppose $o(g) = k$. What can you say about the order of g^2?

Solution In brief, it is $k/2$ if k is even and k if k is odd.

2.18 Is $o(g) = o(g^{-1})$ always? Give a proof or a counterexample.

Solution Yes. Proof: $\left(g^{-1}\right)^k g^k = e$ and so $\left(g^{-1}\right)^k = \left(g^k\right)^{-1}$. Thus $g^k = e$ if and only if $\left(g^{-1}\right)^k = e$ and so g and g^{-1} have the same order.

Sections 3 and 4

Suitable Questions from Jordan and Jordan.

- Chapter 10, Questions 1, 4–8, and 10–14.
- Chapter 9, Questions 1–4 and 9–10.

Cosets and Lagrange

3.1 Consider the group D_3. Find the left and right cosets of H in D_3 where:

1. $H = \langle g \rangle = \{e, g, g^2\}$.
2. $H = \langle h \rangle = \{e, h\}$

where g and h were defined in Problem 1.3.

Solution 1. The subgroup H itself is one left coset (by general theory). Since all cosets are the same size, everything else (i.e. the three reflections) must constitute another. The same argument applies to right cosets. (Note that in this example, and indeed any other where $|G| = 2|H|$, the left and right cosets of H are identical.)

2. The subgroup H is a left coset and a right coset. The other two cosets, each of size two, consist of one reflection and one rotation. You should discover that the left and right cosets are different.

3.2 Show that if G is abelian and $H \leq G$, then the left cosets of H in G are the same as the right cosets. Find the cosets in the case where $G = \mathbb{Z}_9$ and $H = \{0, 3, 6\}$.

Solution Let $g \in G$, then since G is abelian

$$gH = \{gh \mid h \in H\} = \{hg \mid h \in H\} = Hg$$

and so left cosets are the same as right cosets. In the given example, we are computing the cosets $g * H$ where $*$ is given by addition. The cosets are

$$\{0, 3, 6\}, \quad \{1, 4, 7\}, \quad \{2, 5, 8\},$$

where the first corresponds to $e * H = 3 * H = 6 * H$, the second corresponds to $1 * H = 4 * H = 7 * H$ and the third to $2 * H = 5 * H = 8 * H$. To see this, for example note that

$$e * H = \{e * h \mid h \in H\} = \{0 + h \mid h \in H\} = \{0, 3, 6\}$$

and

$$3 * H = \{3 * h \mid h \in H\} = \{3 + h \mid h \in H\} = \{0, 3, 6\}.$$

since addition is mod 9. The others are checked similarly.

3.3 Find all the subgroups of D_3.

Solution There is of course $\{e\}$ and D_3 itself. By Lagrange, the only other possibilities are subgroups of order 2 and 3. Since 2 and 3 are prime, necessarily these must be cyclic. Hence the possible subgroups are

$$\langle g \rangle, \langle g^2 \rangle, \langle h \rangle, \langle gh \rangle, \langle g^2 h \rangle$$

The first two are equal (of order 3), and the last three are distinct (of order 2). Hence there are precisely 6 subgroups.

It is possible to solve this problem directly without Lagrange, but such a solution is quite messy. This is another example of theory helping calculations.

3.4 Find all the subgroups of $\mathbb{Z}_5$ and $\mathbb{Z}_6$.

Solution By Lagrange, the only possible subgroups of $\mathbb{Z}_5$ have order 1 or 5, hence are either $\{0\}$ or $\mathbb{Z}_5$. $\mathbb{Z}_6$ also has subgroups $\{0\}$ and $\mathbb{Z}_6$, but in addition might also have subgroups of order 2 and 3. Again (as in Problem 3.3), since these are prime we can restrict our hunt to cyclic subgroups. The non-trivial cyclic subgroups are

$$\langle 1 \rangle, \langle 2 \rangle, \langle 3 \rangle, \langle 4 \rangle, \langle 5 \rangle$$

It is easy to show that $\langle 1 \rangle = \mathbb{Z}_6$, $\langle 2 \rangle = \langle 4 \rangle = \{0, 2, 4\}$ and $\langle 3 \rangle = \{0, 3\}$. Hence there is one subgroup of order 6, one of order 3, one of order 2 and one of order 1.

3.5 What are all the subgroups of D_4?

Solution Apart from $\{e\}$ and D_4, the only other possible orders of subgroups are 2 or 4. We consider first all possible cyclic subgroups. Certainly

$$\langle g \rangle = \{e, g, g^2, g^3\} = \langle g^3 \rangle$$

has order 4. Also, $\langle g^2 \rangle = \{e, g^2\}$ has order two. Finally, every reflection (there are four) generates a cyclic subgroup of order 2.

Now the only possibility left is a non-cyclic subgroup of order 4. Necessarily this will have two generators, both of order 2, which must commute. Argue that the only possibilities are the subgroups $\langle g^2, h \rangle$ and $\langle g^2, gh \rangle$.

Homomorphisms

4.1 Show that exp is a group homomorphism between $\mathbb{R}$ (under addition) and $\mathbb{R}^* := \mathbb{R} - \{0\}$ (under multiplication). What is its kernel and what is its image? Now answer the same question for $\exp : \mathbb{C} \to \mathbb{C}^*$.

Solution exp is certainly a map $\mathbb{R} \to \mathbb{R}^*$ (remembering that $\exp x$ is never zero). That it is a homomorphism is simply the formula $\exp(a + b) = \exp a \exp b$. The kernel is $\{0\}$ and the image is the multiplicative group of positive reals.

For $\exp : \mathbb{C} \to \mathbb{C}^*$ the image is all of $\mathbb{C}^*$ and the kernel is $\{2k\pi i \mid k \in \mathbb{Z}\}$.

4.2 Let p, q be different primes. Show that the only homomorphism $\phi : C_p \to C_q$ is the trivial one (i.e. $\phi(g) = e$ for all g). (Hint: consider kernels and images.)

Solution Since p is a prime, the only subgroups of C_p are $\{e\}$ and C_p. Hence the kernel, being a subgroup, must be either C_p or $\{e\}$. The former case implies that ϕ is the trivial homomorphism. If the latter, ϕ is injective (by Workshop 3, Q2(a)) and so $\operatorname{Im}\phi$ must be a subgroup of C_q isomorphic to C_p (again, by by Workshop 3, Q2(b)). This is impossible since the only subgroups of C_q are itself and $\{e\}$, so C_q cannot have a subgroup of order p.

4.3 Consider the function $\det : \mathrm{GL}(n, k) \to k^*$. Show that it is a group homomorphism. Identify its kernel and image.

Solution It is a homomorphism because $\det(AB) = \det A \det B$. Its kernel is the subgroup consisting of matrices of determinant one, i.e. $\mathrm{SL}(n, k)$. The image is all of k^*.

Isomorphisms and Products

4.4 Consider the group $\mathbb{C}$ under addition. Show that complex conjugation $\phi : z \to \bar{z}$ is an isomorphism $\mathbb{C} \to \mathbb{C}$.

Solution The group operation $*$ is addition of complex numbers. Now ϕ is clearly a bijective map and further

$$\phi(z * w) = \phi(z + w) = \overline{z + w} = \bar{z} + \bar{w} = \phi(z) + \phi(w) = \phi(z) * \phi(w)$$

for all $z, w \in \mathbb{C}$. Hence ϕ is an isomorphism of groups.

4.5 Let $a, b \in \mathbb{N}$. True or false: $a!b!$ always divides $(a + b)!$

Solution Yes. One way to see this is that $H := S_a \times S_b$ is a subgroup of $G := S_{a+b}$. Note that $|H| = |S_a| \times |S_b| = a!b!$ and $|G| = (a + b)!$. By Lagrange, $|H|$ divides $|G|$.

A more direct (non group–theoretic) way of seeing this is that the binomial coefficient $\binom{a+b}{a} = \frac{(a+b)!}{a!b!}$, and we know that binomial coefficients are always integers.

4.6 Prove that every group G of order 4 is isomorphic to C_4 or $C_2 \times C_2$. (Hint: If G has an element of order 4 then we know the group is isomorphic to C_4. So the only possibility is that every non-identity element has order 2. Call them x, y, z. What are xy and yx equal to?)

Solution Following the hint, if G has an element of order 4 then G is isomorphic to C_4. Otherwise, we must have $G = \{e, x, y, z\}$ with x, y, z having order 2, so $x^2 = y^2 = z^2 = e$. Now we must have $xy = z$ since any other possibility for xy contravenes cancelling laws. Similarly $yx = z$. Then either argue directly (by writing down a map between $C_2 \times C_2$ and G and showing it is a group isomorphism) that G is isomorphic to $C_2 \times C_2$.

Alternatively, use the theorem in lectures [JJ, p145] with the subgroups $\langle x \rangle = \{e, x\}$ and $\langle y \rangle = \{e, y\}$ of G.

4.7 Describe a subgroup of S_7 isomorphic to $S_3 \times S_4$.

Solution All permutations that permute $\{1, 2, 3\}$ amongst themselves, and permute $\{4, 5, 6, 7\}$ amongst themselves.

4.8 Consider the argument in lectures showing that $D_6 \cong D_3 \times \mathbb{Z}_2$. Does a similar argument apply to D_n, with n *even*, $n \geq 6$? What about D_4?

Solution Since n is even, write $n = 2m$ with $m \geq 3$. If m is odd, an identical argument to lectures (involving choosing a regular n-gon inside the $2n$-gon) shows that $D_n \cong D_m \times \mathbb{Z}_2$. The problem when m is even is that when we consider the half–turn g^m, it now intersects the subgroup $H = \{e, g^2, g^4 \dots, g^{n-2}, h, g^2h, g^4h, \dots, g^{n-2}h\}$ and so we cannot apply the same argument.

For D_4, although the half-turn commutes with everything and generates a subgroup isomorphic to $\mathbb{Z}_2$, there is no 4-element subgroup that intersects it trivially.

4.9 If $G \cong H \times \mathbb{Z}_2$, show that G contains an element a of order 2 with the property that $ag = ga$ for all $g \in G$. Deduce (briefly!) that the dihedral group D_{2n+1} (where $n \geq 1$) is not isomorphic to a product $H \times C_2$.

Solution The element $(e, 1)$ is such an element (where $\mathbb{Z}_2 = \{0, 1\}$) of $H \times \mathbb{Z}_2$. Pulling this element across the isomorphism gives us such an element for G. In the group D_n with n odd, the only elements of order 2 are the reflections, which do not commute with everything.

(Note that the half-turn is a central order-2 element in D_{2n} and so the restriction to odd dihedral groups is necessary for the argument in this exercise.)

4.10 Show that no two of the three abelian groups of size 8

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_8$$

are isomorphic.

Solution The last group has an element (in fact several) of order 8. The second has an element of order 4 but none of order 8. The first has all its non-identity elements of order 2.

Section 5

Suitable Questions from Jordan and Jordan.

- Chapter 1, Questions 4–10 are good practice for orbits and stabilizers.
- Chapter 7, Questions 1–9 and 13–16 are more practice for orbits and stabilizers.
- Chapter 9, Questions 6–8 for group actions $\leftrightarrow$ homomorphisms.
- Chapter 11, Questions 1–10 mainly involve the orbit–stabilizer theorem.
- Chapter 12, Questions 1–14 are great practice for Pólya counting.

Group actions and Cayley's theorem

5.1 Let a group G act on X. Show that if $y = g \cdot x$ then $x = g^{-1} \cdot y$. (Note: you must argue from the axioms for a group action.)

Solution Let $y = g \cdot x$. Then

$$g^{-1} \cdot y = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x.$$

5.2 Identify the subgroup of S_4 that arises in Cayley's theorem applied to $C_2 \times C_2$. Do the same for C_4.

Solution Consider $G = C_2 \times C_2 = \{e := (1,1), (g,1), (1,h), (g,h)\}$. Note $G = \langle (g,1), (1,h) \rangle$. Now relabel $X = G$ by $e \leftrightarrow 1$, $(g,1) \leftrightarrow 2$, $(1,h) \leftrightarrow 3$ and $(g,h) \leftrightarrow 4$. Then multiplication by $(g,1)$ sends $1 \mapsto 2$, $2 \mapsto 1$, $3 \mapsto 4$ and $4 \mapsto 3$, hence it corresponds to

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}.$$

Similarly multiplication by $(1,h)$ sends 1 to 3, 3 to 1, 2 to 4 and 4 to 2, hence it corresponds to

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

Thus

$$G = \langle (g,1), (h,1) \rangle \cong \langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \rangle \leq S_4.$$

In a similar way

$$C_4 = \langle g \rangle \cong \langle \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \rangle \leq S_4.$$

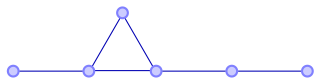
Faithful and transitive actions

5.3 Show that the symmetry group of any graph always acts faithfully on the set of vertices. Find a graph (with at least two edges) whose symmetry group acts transitively on the set of vertices. Find one whose symmetry group does not act transitively.

Solution The identity is the only symmetry which fixes every vertex, hence the action is faithful.

As explained in lectures, the action of the symmetry group D_n on the n-gon is an example of a transitive action. There are many other examples.

For the last part, again there are many answers. For example, any graph (with more than one vertex) whose only symmetry is the identity clearly cannot act transitively on the set of vertices. One such example, from Problem 1.2, is



5.4 Consider a regular 9-gon with symmetry group D_9. There are three separate equilateral triangles that can be constructed using the nine vertices, and D_9 acts on the set X of the three triangles. Identify the subgroup that acts trivially.

Solution The subgroup that acts trivially is the cyclic subgroup of size 3 generated by a (1/3)-turn g^3. That is, the subgroup is the set $\{e, g^3, g^6\}$.

Orbits and stabilizers

5.5 Let G act on X and let $x \in X$. Prove that the stabilizer of x is a subgroup of G.

Solution First, $\mathrm{Stab}(x) \neq \emptyset$ since $e \cdot x = x$ for all $x \in X$ implies that $e \in \mathrm{Stab}(x)$. Now, let $g, h \in \mathrm{Stab}(x)$. Then $g \cdot x = x$ and $h \cdot x = x$ for all $x \in X$. Hence

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

for all $x \in X$ and so $gh \in \mathrm{Stab}(x)$. Finally, let $g \in \mathrm{Stab}(x)$ then

$$x = e \cdot x = (g^{-1}g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$$

for all $x \in X$ and so $g^{-1} \in \mathrm{Stab}(x)$.

5.6 Consider the group $G = S_n$ acting on $X = \{1, 2, \dots, n\}$. Let $x = n$. How many elements does the stabilizer $\mathrm{Stab}_G(x)$ have? To what group is this stabilizer isomorphic?

Solution The stabilizer is all the permutations of the remaining elements $\{1, \dots, n-1\}$, so it has $(n-1)!$ elements. It is isomorphic to S_{n-1}.

5.7 Fix a line L through opposite vertices of a cube. Consider the subgroup H of the symmetries of the cube generated by g, where g is a rotation by 1/3 of a turn about L (this is the element in Problem 1.6). Then H acts on the set of vertices of the cube. Describe the orbits.

Solution Each of the two vertices on the line L is an orbit with one element. The remaining 6 vertices divide into two orbits, each containing three vertices. These orbits are the three green vertices in the solution of Problem 1.6, and the three blue vertices in the solution of Problem 1.6.

5.8 Consider the rotational symmetry group G of the cube acting on the set of vertices of the cube. Describe the stablizer of a particular chosen vertex. How many elements does it have? Now do the same for the action of G on the set of faces and the set of edges.

Solution The stabilizer of a vertex is the 3-element group containing the rotational symmetries about the line through the vertex and its opposite vertex. For faces it is the 4-element group containing the rotational symmetries about the line through the centre of the face and its opposite face. For edges it is analogous — the 2-element group containing the half-turn about the line through the centre of the edge and its opposite.

5.9 For each graph in Workshop 1, let G denote the symmetry group of the graph. Then G acts on the set of vertices. In each case, find how the set of vertices is partitioned into orbits.

Solution Since symmetries preserve the valency of a vertex, all members of an orbit must have the same valency (but not all vertices with the same valency belong to the same orbit!). This, together with the fact that we already know all the symmetries, determines the answers.

In part (b), the middle vertices are always fixed by any symmetry and so form two orbits, each of one element. A symmetry is specified by a permutation of the three left danglers and a permutation of the two right danglers. Thus the two right danglers form an orbit (of two elements), and the three left danglers form an orbit.

In brief, the numbers in each orbit are as follows:

(a):(6,2), (b):(3,2,1,1), (c):(2,2), (d):(4), (e):(2,2,2,1), (f):(6,3,1).

5.10 Consider the group $G = \mathrm{GL}(2, \mathbb{Z}_2)$. Then G acts on the vector space $\mathbb{Z}_2^2$ in the usual way by multiplication. Let X be the set of 1-dimensional subspaces of $\mathbb{Z}_2^2$. Then G acts on X. Show that $|G| = 6$, $|X| = 3$, and that every permutation of the elements of X is realized by an element of G. (Hence this is another realization of S_3 acting by permutation on $\{1, 2, 3\}$.)

Solution We already know from Problem 1.7 that G has six elements. Explicitly, they are

$$\begin{pmatrix}1 & 0\\0 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\0 & 1\end{pmatrix}, \begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}0 & 1\\1 & 1\end{pmatrix}, \begin{pmatrix}1 & 1\\1 & 0\end{pmatrix}, \begin{pmatrix}1 & 0\\1 & 1\end{pmatrix}.$$

The three non-zero vectors (each determining a unique 1-dim subspace) are

$$\begin{pmatrix}1\\0\end{pmatrix}, \quad \begin{pmatrix}0\\1\end{pmatrix}, \quad \begin{pmatrix}1\\1\end{pmatrix}.$$

A bit of calculation shows that multiplication on the left gives every possible permutation of the vectors. Better though is to argue that no two distinct matrices can give the same permutation since a linear map is determined by its action on a pair of basis vectors. There are only six permutations so we must get all of them.

Orbit–stabilizer theorem

5.11 Check the orbit-stabilizer theorem for the case of the group S_n acting on a set of n objects by permuting them.

Solution Choose one of the objects in the set. Its orbit is the whole set and so has size n. The stabilizer is all permutations of the other $n-1$ objects which has size $(n-1)!$. It is indeed true that $|S_n| = n! = n(n-1)!$

5.12 The rotational symmetry group G of a dodecahedron acts transitively on the set V of its 20 vertices. Pick $v \in V$. How many elements are in the stabilizer of v? (you may have to make the model of the dodecahedron and play with it) Deduce the order of G. Using a similar method, deduce the order of the group of rotational symmetries of the octahedron.

Solution Three. Thus by the orbit-stabilizer theorem, $3 \times 20 = 60$ is the order of the group. For the octahedron, the stabilizer consists of the rotations about the vertex, and thus has order 4. There are 6 vertices on which the rotational symmetry group clearly acts transitively. Hence by orbit–stabilizer there are $4 \times 6 = 24$ rotational symmetries of the octahedron.

5.13 By Problem 5.12 you should know that there are 24 elements in the group of rotational symmetries of the octahedron. What are they? (you just have to describe 24 distinct symmetries, then automatically you have them all.)

Solution These are quite hard to TeX, but much easier to describe if you have an octahedron.

Pólya counting

5.14 Dice have the numbers $1, 2, 3, 4, 5, 6$ on the faces of a cube in such a way that opposite faces add up to 7. How many different dice are there? (Two dice are the same if they differ by a rotational symmetry of the cube. There are 24 such symmetries.) You can solve this by "pure thought" only because the numbers involved are small; try to find a group-theoretic answer.

Solution Let X denote the set of all numberings of the six faces satisfying the sum condition. Then $|X| = 48$ (there are six choices where to put 1 on the dice, then four choices for 2, and two choices for 3. Everything is now fixed and $6 \times 4 \times 2 = 48$).

Now $|G| = 24$ (where G is the rotational symmetries) and it is clear that every rotation of the dice gives a different numbering, hence the number of essentially different dice is $48/24 = 2$.

It is more clear if we use "Pólya counting". The identity fixes all numberings and the other 23 symmetries fix none. Hence the number of dice (=number of orbits) is

$$\tfrac{1}{24}(48 + (0 \times 23)) = 2.$$

A "pure thought" approach is to find the vertex surrounded by the faces numbered 1,2,3. These either go clockwise or anticlockwise round the vertex, but then everything else is fixed. Hence there are only two possibilities.

5.15 How many ways are there of colouring the vertices of a 6-gon with two colours, where two colourings are regarded as the same if they differ by an element of D_6? (Be careful to think about the different sorts of rotation and reflection. It is more complicated than the 5-gon example in lectures.)

Solution In brief, the fixed point analysis is

Type of element	Number	Fixed points
e	1	$2^6 = 64$
reflection in vertex	3	$2^4 = 16$
reflection in edge	3	$2^3 = 8$
$\pm(1/6)$-turn rotation	2	2
$\pm(1/3)$-turn rotation	2	$2^2 = 4$
$(1/2)$-turn rotation	1	$2^3 = 8$

Hence, by Pólya counting, the number of orbits is

$$\tfrac{1}{12}(64 + (3 \times 16) + (3 \times 8) + (2 \times 2) + (2 \times 4) + 8) = 13.$$

Challenge Question

5.16 (Sylow's 1st Theorem) Let G be a finite group and let p be a prime factor of $|G|$, and suppose that $k \in \mathbb{N}$ is largest such that p^k divides $|G|$. Then G contains a subgroup H such that $|H| = p^k$. Prove this in stages:

1. Let $\mathcal{S} := \{U \subseteq G : |U| = p^k\}$, i.e. the set of all subsets of G with p^k elements. Show that G acts on $\mathcal{S}$ via the rule $g \cdot U := gU$.
2. Argue that p does not divide $|\mathcal{S}|$.
3. By 1, $\mathcal{S}$ is partitioned into orbits. Using 2, deduce that there exists an orbit $\mathcal{A}$ such that p does not divide $|\mathcal{A}|$.
4. Pick an element $V \in \mathcal{A}$, and consider $H := \mathrm{Stab}_G(V)$. Why is H a subgroup?
5. Argue that p^k divides $|H|$ by using the orbit-stabilizer theorem.
6. Argue directly that $|H| \leq p^k$.
7. By combining your answer to 4, 5 and 6, prove the 1st Sylow Theorem.

Solution

1. For $U \in \mathcal{S}$ and $g \in G$, gU is a subset of G with $|gU| = |U|$, thus $gU \in \mathcal{S}$. It is easy to check the axioms to see that G acts on the set $\mathcal{S}$.
2. Write $|G| = p^k m$, where $\gcd(p, m) = 1$. Consider the set $\mathcal{S}$ of all subsets of U of G with $|U| = p^k$. The number of such subsets is
$$|\mathcal{S}| = \binom{p^k m}{p^k} = \frac{p^k m}{p^k} \times \frac{p^k m - 1}{p^k - 1} \times \ldots \times \frac{p^k m - p^k + 1}{1}.$$
If in each term $\frac{p^k m - j}{p^k - j}$ we cancel all common divisors of the numerator and denominator, p does not remain a divisor of the numerator. To see this (it is clear for $j = 0$), let $j > 0$ then we may certainly write j as $j = p^l s$, where $l, s \in \mathbb{N} \cup \{0\}$ and $\gcd(p, s) = 1$. Then $l < k$, so
$$\frac{p^k m - j}{p^k - j} = \frac{p^{k-l} m - s}{p^{k-l} - s}.$$
Certainly p does not divide $p^{k-l} m - s$, and hence since p is prime, it follows that p does not divide the product of the numerators. Therefore $p \nmid |\mathcal{S}|$.
3. Under the action in (1), $\mathcal{S}$ is partitioned into orbits. Hence if p divides the size of every orbit, p divides $|\mathcal{S}|$. Thus it follows (since $p \nmid |\mathcal{S}|$) that there exists an orbit $\mathcal{A}$ such that $p \nmid |\mathcal{A}|$.
4. Pick an element V of $\mathcal{S}$ which belongs to the orbit $\mathcal{A}$, and set $H := \mathrm{Stab}_G(V)$. Stabilizers are always subgroups, hence $H \leq G$.
5. By orbit–stabilizer,
$$|\mathcal{A}| = \frac{|G|}{|H|}.$$
Thus $p^k m = |G| = \frac{|G|}{|H|} |H| = |\mathcal{A}| \, |H|$. But $p \nmid |\mathcal{A}|$, so necessarily p^k divides $|H|$.
6. Since $|V| = p^k$, let $V = \{x_1, x_2, \ldots, x_{p^k}\}$ denote the elements of V. Then for any $h \in H = \mathrm{Stab}_G(V)$, $hV = V$, that is
$$\{hx_1, hx_2, \ldots, hx_{p^k}\} = \{x_1, x_2, \ldots, x_{p^k}\}.$$
Hence $hx_1 = x_i$ for some i with $1 \leq i \leq p^k$, and so $h = x_i x_1^{-1}$. This shows that
$$H \subseteq \{e, x_2 x_1^{-1}, x_3 x_1^{-1}, \ldots, x_{p^k} x_1^{-1}\},$$
hence $|H| \leq p^k$, as required.
7. By 5, p^k divides $|H|$ and so $|H| \geq p^k$. By 6, $|H| \leq p^k$. Hence $|H| = p^k$, and by 4 H is a subgroup. This proves the theorem.

Sections 6 and 7

Suitable Questions from Jordan and Jordan.

- Chapter 13, Q1–21 are good practice for conjugates, centralizers and centres.
- Chapter 14, Q1–17 for Cauchy's Theorem, product groups and applications.
- Chapter 15, Q1–18 for kernels and normal subgroups.

Symmetric and Alternating Groups

6.1 Prove that if σ_1 and σ_2 are disjoint cycles, then $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Solution This is clear by direct calculation. Let $X = \{1, \dots, n\}$ and consider the elements of S_n as bijections $X \to X$. Convince yourself that $\sigma_1 \circ \sigma_2$ has the same effect as $\sigma_2 \circ \sigma_1$ on every object in X, hence as maps $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

6.2 Show that the number of elements of S_n of cycle type $1^{m_1}, 2^{m_2}, \dots, n^{m_n}$ is

$$\frac{n!}{m_1! \dots m_n! 1^{m_1} 2^{m_2} \dots n^{m_n}}.$$

Solution A permutation of the given cycle type is produced by filling $\{1, 2, \dots, n\}$ into the blanks in the following pattern:

$$\underbrace{(\bullet)\dots(\bullet)}_{m_1}\underbrace{(\bullet\bullet)\dots(\bullet\bullet)}_{m_2}\underbrace{(\bullet\bullet\bullet)\dots(\bullet\bullet\bullet)}_{m_3}\dots$$

There are $n!$ ways of doing this, but we must account for the fact that some of these ways give the same element of S_n.

- Since $(a)(b) = (b)(a)$, the one-cycles can be permuted and this gives the same element. Similarly for the 2-cycles, etc. There are $m_1!$ permutations of the 1-cycles, $m_2!$ permutations of the 2-cycles, etc, so we must divide by $m_1! \dots m_n!$
- Each 2-cycle has two different ways of being written (since $(ab) = (ba)$). Similarly each 3-cycle has three different ways of being written (since $(abc) = (bca) = (cab)$), etc, and so we must also divide by $1^{m_1} 2^{m_2} \dots n^{m_n}$.

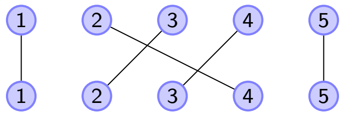
6.3 Let $\sigma \in S_n$ have cycle type $l_1, \dots, l_k$. What is the order of σ? What are the possible orders of elements in S_7?

Solution The order is the least common multiple of the l_j. The possible orders are $1, 2, 3, 4, 5, 6, 7, 10, 12$.

6.4 Let $\sigma \in S_n$ and let $H := \langle\sigma\rangle$ act on $\{1, 2, \dots, n\}$ in the obvious way. Convince yourself that the cycle type of σ is the list of the sizes of all the orbits of this action.

Solution Write σ into disjoint cycles. The point is that if $(x_1 x_2 \dots x_k)$ is one of these, then $\{x_1, x_2, \dots, x_k\}$ is an orbit.

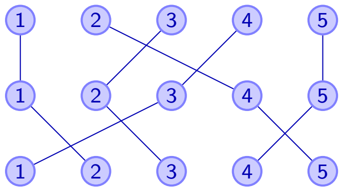
6.5 Let $\sigma \in S_n$. Another notation for writing σ is the following: write the numbers $1, \ldots, n$ in two rows, one above the other. Then for every number i in the top row, draw a line between i (in the top row) and $\sigma(i)$ on the bottom row, for example



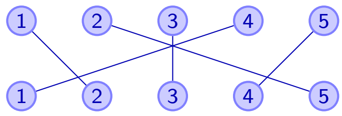
represents $1 \mapsto 1$, $2 \mapsto 4$, $3 \mapsto 2$, $4 \mapsto 3$ and $5 \mapsto 5$. From this picture, can you tell whether a permutation is odd or even? Also, how do you compose permutations using this picture?

Solution Let c denote the number of points where lines cross. Then the permutation is even if c is even, and odd when c is odd.

To compose, just write one on top of the other and follow the lines through



$=$



6.6 Prove that A_4 is not isomorphic to D_6.

Solution There are many ways of seeing this. For example, A_4 has no element of order 6 (whereas D_6 does, namely rotation anticlockwise by $2\pi/6$), hence A_4 and D_6 cannot be isomorphic. Alternatively, A_4 and D_6 have different class equation, so therefore they cannot be isomorphic. One other way would be to observe that A_4 has trivial centre, whereas the half-turn g^3 belongs to the centre of D_6

Conjugate elements, centres and centralizers

6.7 Let $g \in G$. Show that $\langle g \rangle \leq C(g)$.

Solution $g^k g = g^{k+1} = g g^k$ and so every power of g commutes with g.

6.8 Let $g \in G$. Prove directly (i.e. without using general properties of group actions) that $C(g) \leq G$.

Solution By Problem 6.7, $g \in C(g)$ and so $C(g) \neq \emptyset$. It is also easy to show directly that $C(g)$ is closed under multiplication and inverses.

6.9 Let $A = \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \in G = \mathrm{GL}(2, \mathbb{Z}_3)$. Show that $|C(A)| = 4$. What is $|G|$? How many conjugates does A have in G?

Solution Let $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Then one easily calculates that $MA = AM$ iff $c = 0$ and $d = a + b$. One finds that $\mathbb{I}, A, 2\mathbb{I}, 2A$ are the only such matrices. From the general formula in the solution to Problem 1.7, $|G| = 48$. So by orbit–stabilizer A has $\frac{48}{4} = 12$ conjugates in G.

6.10 Let $\phi : G \to \mathrm{GL}(n, k)$ be a group homomorphism. Show that the function $f : G \to k$ defined by $f(g) = \mathrm{Trace}\,\phi(g)$ is constant on every conjugacy class of G.

Solution This follows from the fact that

$$\mathrm{Trace}\,\phi(hgh^{-1}) = \mathrm{Trace}(\phi(h)\phi(g)\phi(h^{-1})) = \mathrm{Trace}(\phi(h^{-1})\phi(h)\phi(g)) = \mathrm{Trace}(\phi(g))$$

since $\mathrm{Trace}(ABC) = \mathrm{Trace}(CAB)$.

6.11 Consider D_6, the symmetries of a regular hexagon. Let $H \leq G$ be the subgroup consisting of the identity and the five nontrivial rotations. Let g denote a rotation by $1/6$ of a turn. Show that $H \leq C(g)$. Find an element in D_6 that does not commute with g and hence use Lagrange's theorem to deduce that $C(g) = H$. From this, deduce that g is conjugate to only one other element of D_6, and find that element.

Solution $H = \langle g \rangle$ and so $H \leq C(g)$ by Problem 6.7. Now the reflection h does not commute with g, hence $C(g) \neq G$. By Lagrange's theorem, since $|D_6| = 12$ and $|H| = 6$ the only subgroups of D_6 containing H are D_6 and H itself. Since $C(g) \neq G$, this forces $C(g) = H$.

We know (by orbit–stabilizer) that g has precisely $\frac{|D_6|}{|C(g)|} = \frac{12}{6} = 2$ conjugates. One is g itself. Now note (e.g. by calculation) that $hgh^{-1} = g^{-1}$, and so g^{-1} is another. Since there are only two, these are them all.

6.12 Let k be a field, $n \in \mathbb{N}$. Show that the centre of $\mathrm{GL}(n, k)$ is $\{\lambda\mathbb{I} \mid \lambda \in k^*\}$. (It is clear that the centre contains at least these matrices. The content in the question is that it does not contain other things.)

Solution Suppose $A \in C(\mathrm{GL}(n,k))$. Let E_{ij} be the elementary matrix with 1 in position (i,j) and 0's elsewhere. Note that $\mathbb{I} + E_{ij} \in \mathrm{GL}(n,k)$ for all i,j. Thus

$$A(\mathbb{I} + E_{ij}) = (\mathbb{I} + E_{ij})A$$

and so

$$AE_{ij} = E_{ij}A$$

for all i,j. But now

$$E_{ij}A = \begin{pmatrix} 0 & 0 & \dots & 0 \\ & \vdots & & \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ & \vdots & & \\ 0 & 0 & \dots & 0 \end{pmatrix}$$

where all entries are zero, except the row shown, which lives in the ith row. Similarly

$$AE_{ij} = \begin{pmatrix} 0 & & a_{1i} & & 0 \\ 0 & \dots & a_{2i} & \dots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & & a_{ni} & & 0 \end{pmatrix}$$

where all entries are zero, except the column shown, which lives in the jth column. This shows that $a_{ii} = a_{jj}$ and all off-diagonal entries are zero. Hence $A \in \{\lambda\mathbb{I} \mid \lambda \in k^*\}$.

6.13 What is the centre of the dihedral group D_n? (Hint: consider n odd and even separately.)

Solution A bit of messing around rapidly convinces one that the only possible non-trivial symmetry that commutes with all the others is a half-turn, which is in D_n iff n is even. Hence $C(D_n) = \{e, g^{\frac{n}{2}}\}$ when n is even, and $C(D_n) = \{e\}$ when n is odd.

Conjugacy classes

6.14 Find the conjugacy classes in D_4. (If necessary, cut out a square from paper, label the corners and play with it.)

Solution Note that $D_4 = \{g^a h^b \mid 0 \le a \le 3, 0 \le b \le 1\}$. Now the relation $hg = g^{-1}h$ implies, by induction on t, that

$$g^t = h^{-1}g^{-t}h \tag{3}$$

for all $0 \le t \le 3$. Also, $ghg^{-1} = hg^{-2} = hg^2$, which implies that

$$g^t hg^{-t} = \begin{cases} h & \text{if } t = 0, 2 \\ hg^2 & \text{if } t = 1, 3 \end{cases}. \tag{4}$$

Now to calculate the conjugacy class containing g^t, we calculate the set $\{x^{-1}g^t x \mid x \in D_4\}$. Since $x = g^a h^b$ for some a, b, we have

$$(g^a h^b)^{-1} g^t (g^a h^b) = h^{-b}g^{-a}g^t g^a h^b = h^{-b}g^t h^b \overset{(3)}{=} \begin{cases} g^t & \text{if } b = 0 \\ g^{-t} & \text{if } b = 1 \end{cases},$$

which shows that $\{e\}$, $\{g, g^3\}$ and $\{g^2\}$ are all conjugacy classes.

Now to calculate the conjugacy class containing h, note that

$$(g^a h^b)h(g^a h^b)^{-1} = g^a h^b h h^{-b} g^{-a} = g^a hg^{-a} \overset{(4)}{=} \begin{cases} h & \text{if } a = 0, 2 \\ hg^2 & \text{if } a = 1, 3 \end{cases},$$

and so since $hg^2 = g^2 h$ (g^2 is central since it is a one-element conjugacy class) it follows that the conjugacy class containing h is $\{h, g^2 h\}$.

Lastly, since

$$h(gh)h^{-1} = hg = g^{-1}h = g^3 h,$$

the conjugacy class containing gh also contains $g^3 h$. But these are the only two elements in D_4 that we have not yet put into conjugacy classes. Since conjugacy classes partition D_4, it follows that $\{gh, g^3 h\}$ is the last conjugacy class.

6.15 Let $G = H \times K$. Show that (h, k) is conjugate to (h', k') in G if and only if h and h' are conjugate in H, and k and k' are conjugate in K. This shows that every conjugacy class in G is of the form $C \times D$ where C is a conjugacy class in H, and D is a conjugacy class in K. Hence write down the class equation for $C_2 \times S_3$.

Solution (h, k) is conjugate to (h', k') in G if and only if there exists $(p, q) \in G$ such that $(h', k') = (p, q)(h, k)(p, q)^{-1}$, which holds if and only if

$$h' = php^{-1} \quad \text{and} \quad k' = qkq^{-1}.$$

In turn, this holds if and only if h and h' are conjugate in H, and k and k' are conjugate in K. So clearly a conjugacy class in $G \times H$ is of the said form. Now the class equation for S_3 is $6 = 1 + 2 + 3$ and that for C_2 is $2 = 1 + 1$. It follows that the class equation for the product is

$$12 = 1 + 1 + 2 + 2 + 3 + 3.$$

6.16 Write down the class equation for D_4. (You should have done most of the work in Problem 6.14.)

Solution By Problem 6.14 there are two conjugacy classes of size 1 and three of size 2, hence the class equation is $8 = 1 + 1 + 2 + 2 + 2$.

6.17 Let p be a prime. You know that every group of order p is cyclic, and thus abelian (by Problem 2.5). You also know (from lectures) that every group of order p^2 is abelian. Is the same true for p^3, i.e. is every group of order p^3 abelian?

Solution No. Symmetries of the square D_4 has order $2^3 = 8$ but is not abelian.

6.18 Consider the cycles $c = (125)$ and $d = (234)$ in S_5. Find $g \in S_5$ such that $d = gcg^{-1}$. How many such g are there?

Solution We choose g so that it maps $1 \mapsto 2, 2 \mapsto 3, 5 \mapsto 4$. It does not matter what else it does. So (in a mixed notation) we have

$$(234) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} (125) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 2 & 5 & 4 \end{pmatrix}.$$

There are 6 such elements — there are 3 ways to map $\{1, 2, 5\}$ to $\{2, 3, 4\}$ that preserve the cyclic order, and for each of those two choices about where the other two elements are sent.

6.19 S_4 has five conjugacy classes. Find them, and the number of elements in each, and hence write down the class equation for S_4.

Solution We know that two elements in S_n are conjugate if and only if they have the same cycle type (up to ordering). The possible cycle types in S_4 are 1^4, $1^2.2$, 2.2, 3.1 and 4. It follows that there are precisely five conjugacy classes. Now by Problem 6.2 the number of elements of a fixed cycle type $1^{m_1}2^{m_2} \dots n^{m_n}$ is $\frac{n!}{m_1! \dots m_n! 1^{m_1} 2^{m_2} \dots n^{m_n}}$. and hence this equals the number of elements in the corresponding conjugacy class. Thus the conj class 1^4 has one element, the conj class $1^2.2$ has 6 elements, the conj class 2.2 has 3 elements, the conj class 3.1 has 8 elements and the conj class 4 has 6 elements.

6.20 Show that $(12)(34)$ together with its conjugates and the identity form a subgroup of S_4 isomorphic to $C_2 \times C_2$.

Solution Each of the three elements with this cycle-type is its own inverse. By experiment, multiplying any two gives the third. Thus they form a subgroup of order 4. There is no element of order 4, so it must be isomorphic to $C_2 \times C_2$.

Alternatively, choose two of the three and observe that they are both of order 2 and commute (and the product is the other element of the same cycle type). Hence we can use [JJ, 14.3] to show that they generate a subgroup isomorphic to $C_2 \times C_2$.

Normal subgroups

6.21 Let $N \leq G$. Prove that the following are equivalent:

1. N is normal in G.
2. $gNg^{-1} = N$ for all $g \in G$.
3. $gN = Ng$ for all $g \in G$.

Solution (1)⇒(3) Let $g \in G$. Then for all $n \in N$, since $gng^{-1} \in N$, by multiplying on the right by g we see that $gn \in Ng$. This shows that $gN \subseteq Ng$. On the other hand, since $g^{-1} \in G$ and $(g^{-1})^{-1} = g$, $g^{-1}ng \in N$. Multiplying on the left by g, we see that $ng \in gN$, which implies that $Ng \subseteq gN$. Hence $Ng = gN$.
(3)⇒(2) Let $g \in G$. Let $n \in N$, then $gn \in gN = Ng$ implies that there exists $n' \in N$ such that $gn = n'g$ and hence $gng^{-1} = n' \in N$. This shows that $gNg^{-1} \subseteq N$. The other inequality is similar.
(2)⇒(1) If $n \in N$ and $g \in G$ then $gng^{-1} \in gNg^{-1} = N$.

6.22 Prove that if $\phi : G \to H$ is a group homomorphism, then $\operatorname{Ker}\phi$ is a normal subgroup of G.

Solution First, we show that $\operatorname{Ker}\phi$ is a subgroup. It is nonempty since $e \in \operatorname{Ker}\phi$ (since $\phi(e) = e$). If $k_1, k_2 \in \operatorname{Ker}\phi$ then $\phi(k_1k_2) = \phi(k_1)\phi(k_2) = ee = e$ and so $k_1k_2 \in \operatorname{Ker}\phi$. Lastly, if $k \in \operatorname{Ker}\phi$ then $\phi(k^{-1}) = \phi(k)^{-1} = e^{-1} = e$ so $k^{-1} \in \operatorname{Ker}\phi$.

To see that K is normal, let $k \in \operatorname{Ker}\phi$ and $g \in G$. Then

$$\phi(gkg^{-1}) = \phi(g)\phi(k)\phi(g^{-1}) = \phi(g)e\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e) = e$$

and so $gkg^{-1} \in \operatorname{Ker}\phi$.

6.23 Find all the normal subgroups of D_4. (There are six in total!) One of them, which we will call N, has order 2. To what familiar group is the quotient D_4/N isomorphic?

Solution By Problem 3.5 we know all subgroups. By Problem 6.14 we know the conjugacy classes. Since a subgroup is normal if and only if it is the union of conjugacy classes, we go through the subgroups one by one to check if they are normal. Clearly $\{e\}$ and D_4 are normal, as is $H := \{e, g, g^2, g^3\}$ (since $\frac{|G|}{|H|} = 2$).

The group $N = \{e, g^2\}$ is normal (since it is the union of two one-element conjugacy classes). A check shows that the only other two normal subgroups consist of the identity, the half-turn and two reflections of the same type. Both of these have order 4, hence there is only one normal subgroup of order 2, namely $N = \{e, g^2\}$.

The quotient has order 4, so must be isomorphic to either $C_2 \times C_2$ or C_4 (by Problem 4.6), according to whether there are elements of order 4. The only candidate for an element of order 4 is rN where r is one of the order 4 rotations in D_4. But in the quotient $rNrN = r^2N = N$ and so rN has order 2. We deduce that the quotient D_4/N is isomorphic to $C_2 \times C_2$.

6.24 Show that the intersection of two normal subgroups is a normal subgroup.

Solution The intersections of subgroups is a subgroup from earlier work. Now let $N_1, N_2 \trianglelefteq G$, let $g \in G$, and let $n \in N_1 \cap N_2$. Then $gng^{-1} \in N_1$ since N_1 is normal and $gng^{-1} \in N_2$ since N_2 is normal. Hence $gng^{-1} \in N_1 \cap N_2$.

6.25 Show that $V_4 = \{e, (12)(34), (13)(24), (14)(23)\}$ is a normal subgroup of S_4.

Solution It is a subgroup (we have seen this in Problem 6.20) and a union of conjugacy classes ($\{e\}$ and the elements of cycle-type 2,2). Hence it is normal by [JJ, 15.5].

6.26 Show that $\{e\}$, V_4 (in the previous exercise), A_4 and S_4 are the only normal subgroups of S_4. (Hint: a subgroup is normal iff it is a union of conjugacy classes. Use the class equation and Lagrange's Theorem.)

Solution The class equation is $24 = 1 + 6 + 8 + 6 + 3$. The identity must be in a subgroup. Thus we need a sum of the numbers on the right-hand side, including the 1, that divides 24. The only possibilities are $1 + 3 = 4$ and $1 + 3 + 8 = 12$. the "3" corresponds to the set $\{(12)(34), (13)(24), (14)(23)\}$, hence the first is V_4. Now all elements in the "3" are even, and further the "8" corresponds to the set of 3-cycles (all of which are even), hence the $1 + 3 + 8 = 12$ subgroup is A_4.

6.27 (harder) The aim of this exercise is to show that A_5 has no normal subgroups other than $\{e\}$ and A_5 itself. (Groups with this property are called *simple*. They are fundamental building blocks because if $N \trianglelefteq G$ is a normal subgroup one can regard G as being in some sense built from the smaller groups N and G/N).

1. Show that A_5 consists of: the identity; 15 elements of cycle-type 2,2; 20 3-cycles; 24 5-cycles.
2. We know that all 5-cycles are conjugate in S_5, however this may not be true in A_5 because the element that does the conjugation in S_5 might be odd (and so doesn't belong to A_5). Now, we know (by orbit-stabilizer) that the number of elements in the conjugacy class of $g \in A_5$ is equal to $\frac{|A_5|}{|C_{A_5}(g)|}$. Show that the centralizer of a 5-cycle in A_5 is the cyclic group that it generates and hence conclude that the 5-cycles constitute 2 size-12 conjugacy classes.
3. Deduce similarly that (in A_5) the elements of cycle-type 2,2 form a conjugacy class of size 15 and the 3-cycles form a conjugacy class of size 20.
4. Use the characterization of a normal subgroup as a subgroup that is a union of conjugacy classes, and Lagrange's theorem, to show that A_5 is simple.

Solution 1. Just count the number in each conjugacy class in S_5 (which is determined by cycle type), and keep only the even elements.
2. By experiment, the only things that commute with a 5-cycle are its powers. So the centralizer has size 5 and so each one has 12 conjugates in A_5. Hence the 5-cycles form 2 classes of size 12.
3. For a 3-cycle g, the centralizer is $\{e, g, g^2\}$ (one can't include a transposition of the two elements the cycle fixes because that would be odd). So the conjugacy class has size $60/3 = 20$ in A_5. The centralizer of an element of type 2,2 is the three elements of the same type that leave the same element fixed together with the identity. So the conjugacy class has size $60/4 = 15$.
4. The class equation is $60 = 1 + 15 + 20 + 12 + 12$. The identity must be in a subgroup. Thus we need a sum of the numbers on the right-hand side, including the 1, that divides 60. The only such combinations are 1 and 60, hence there are no normal subgroups except $\{e\}$ and A_5.

Quotient groups

6.28 Show that D_n has a normal subgroup isomorphic to C_n, with $D_n/C_n \cong C_2$.

Solution Consider the cyclic subgroup of order n consisting of all the rotations, namely $\langle g \rangle = \{e, g, \dots, g^{n-1}\}$. All cyclic subgroups of order n are isomorphic, so $\langle g \rangle \cong C_n$. It is normal since $\frac{|G|}{|\langle g \rangle|} = 2$ (and so we can use [JJ, Thm8, p156]).

Since $G/\langle g \rangle$ has order 2, necessarily it must be isomorphic to C_2 (since all groups of order two are).

6.29 Prove that the map $\bar{\phi} : G \to G/N$ given by $\bar{\phi}(g) = gN$ is a group homomorphism.

Solution The map $\bar{\phi} : G \to G/N$ is given by $\bar{\phi}(g) = gN$. There is no issue of this being well-defined. To see that it is a homomorphism we calculate:

$$\bar{\phi}(gg') = (gg')N = gN * g'N = \bar{\phi}(g) * \bar{\phi}(g')$$

where for clarity we have written $*$ for the group operation in the quotient.

6.30 Show that every homomorphism $\phi : \mathbb{Z} \to G$ (regarding $\mathbb{Z}$ as a group under addition) is of the form $\phi : k \mapsto g^k$ for some $g \in G$. (Hint: consider $\phi(1)$.) Describe the kernel and image of such a ϕ.

Solution Consider a homomorphism $\phi : \mathbb{Z} \to G$. Let $\phi(1) = g$. Then $\phi(-1) = g^{-1}$ and $\phi(2) = \phi(1+1) = \phi(1)\phi(1)$, etc. So in general $\phi(k) = g^k$. We see that the image of ϕ is the subgroup generated by g and the kernel is $\{jn \,|\, j \in \mathbb{Z}\}$ where $n = o(g)$.

6.31 How can one understand the addition of angles in terms of a quotient group?

Solution It is addition in the quotient group of $\mathbb{R}$ by the normal (automatically since $\mathbb{R}$ is abelian) subgroup $\{2k\pi \,|\, k \in \mathbb{Z}\}$.

6.32 Determine whether the following claims are TRUE or FALSE. If they are true give a proof, whereas if they are false give a counterexample.

1. Every group of order six is abelian.
2. Every group of order fourteen is abelian.
3. If G is non-abelian, then $\{g \in G \mid gh = hg \text{ for all } h \in G\} = \{e\}$.
4. Every normal subgroup of a group G is the kernel of some group homomorphism.
5. Let $n \geq 2$, then the group $\mathrm{GL}(n, \mathbb{R})$ has no normal subgroups other than $\{e\}$ and $\mathrm{GL}(n, \mathbb{R})$.

Solution

1. FALSE. D_3 has order six, and is non-abelian.
2. FALSE. D_7 has order fourteen, and is non-abelian.
3. FALSE. Denote $C(G) := \{g \in G \mid gh = hg \text{ for all } h \in G\}$. Now D_4 is non-abelian, with $C(D_4) = \{e, g^2\}$, where g^2 is the half-turn (see Problem 6.13).
4. TRUE. If N is a normal subgroup of G, just consider the natural homomorphism $G \to G/N$. It has kernel N.
5. FALSE. Consider the determinant function $\det : \mathrm{GL}(n, \mathbb{R}) \to \mathbb{R}^*$, then this is a group homomorphism. The kernel is $\mathrm{SL}(n, \mathbb{R})$, hence there is a (proper, non-trivial) normal subgroup of $\mathrm{GL}(n, \mathbb{R})$.