4. Permutations - worked solutions

Alastair Farrugia MAT 1101

1. (a) **What is the length of $(abcd)$? Its order? Its parity?**

   $(abcd)$ has length 4 [because there are 4 elements in the cycle], and order 4 [because $(abcd)^4 = \mathrm{ID}$].
   $(abcd) = (ab)(ac)(ad)$, so it is odd [it has sign -1].

   (b) **What is the length of (efg)? Its order? Its parity?**

   (efg) has length 3 [because there are 3 elements in the cycle] and order 3 [because $(efg)^3 = \mathrm{ID}$].
   $(efg) = (ef)(eg)$, so it is even [it has sign $+1$].

   (c) **What is the order of $\sigma := (abcd)(efg)$? Write σ as a product of 5, 7 or 9 transpositions. Is it possible to write it as a product of 483 transpositions? 484?**

   The order of σ is the lcm of the orders of $(abcd)$ and (efg); $\mathrm{lcm}(4, 3) = 12$.
   $\sigma = (ab)(ac)(ad)(ef)(eg) = (ab)(ac)(ad)(ef)(eg)(ab)(ab) = (ab)(ac)(ad)(ef)(eg)(ab)(ab)(ab)(ab)$.
   [Note that $\mathrm{sgn}(\sigma) = \mathrm{sgn}((abcd))\mathrm{sgn}((efg)) = -1 \times +1$. It is best to consider the sign of $(abcd)$, (efg) and σ; it could be confusing to talk instead about odd and even parity, because we are used to 'odd times even' being even, which is not the case with permutations.]
   We can write σ as 483 transpositions, because 5 and 483 have the same parity [and $5 < 483$; for example, 1 is also an odd number, but σ cannot be written as a single transposition].
   It cannot be written as 484 transpositions, because 5 and 484 have different parity.

   (d) **Write σ^{-1} as a product of transpositions.**

   $\sigma^{-1} = (eg)(ef)(ad)(ac)(ab)$. [We basically use the result that $[xy]^{-1} = y^{-1}x^{-1}$; here $[xy]$ is "x times y", not a transposition. Note that σ and σ^{-1} can both be written as 5 transpositions.]

2. **Write the following permutations as a product of disjoint cycles, and as a product of transpositions:**

   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \mathrm{X} \\ 7 & \mathrm{X} & 3 & 2 & 8 & 9 & 6 & 5 & 1 & 4 \end{pmatrix} \begin{array}{l} = (1769)(2X4)(58) \\ = (17)(16)(19)(2X)(24)(58). \end{array}$

   (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & \mathrm{X} \\ 9 & 3 & 7 & 1 & 6 & 5 & 2 & \mathrm{X} & 4 & 8 \end{pmatrix} \begin{array}{l} = (194)(237)(56)(8X) \\ = (19)(14)(23)(27)(56)(8X). \end{array}$

   (c) $(abc)(cad) = (ab)(cd)$.

   (d) $(213)(3421)(153) = (214)(35) = (21)(24)(35)$.

3. **We know that every permutation can be written as a product of transpositions; that is, the 2-cycles generate S_n. The aim of this exercise is to show that the 3-cycles generate A_n. Show that**

   (a) **the product of any number of 3-cycles is even;**

   A 3-cycle can be written as a product of two transpositions, e.g. $(xyz) = (xy)(xz)$. So the product of k 3-cycles can be written as a product of $2k$ transpositions.

   (b) **every even permutation in S_n ($n \geq 3$) can be written as a product of 3-cycles.**

   Consider $\sigma = \sigma_1\sigma_2 \cdots \sigma_{2r}$, where each σ_i is a transposition. If $r = 0$ (i.e. σ is the identity), then $\sigma = (123)(123)(123)$.
   If $r = 1$, [i.e. we have two transpositions] we consider different cases depending on whether the transpositions have 0, 1 or 2 elements in common:

$$\begin{aligned} (ab)(cd) &= (abc)(cad) \\ (ab)(ac) &= (abc) \\ (ab)(ab) &= (abc)(abc)(abc) \end{aligned}$$

   If $r > 1$, then we have r pairs of transpositions — $\sigma_1\sigma_2, \sigma_3\sigma_4, \ldots,$ $\sigma_{2r-1}\sigma_{2r}$ — and we know how to write each pair in terms of 3-cycles, so we are done.

[Alternatively, we could use induction on r, the base case $r = 0$ being ready. So suppose $\sigma_1 \cdots \sigma_{2r}$ can be written as $\tau_1 \cdots \tau_t$, where each τ_i is a 3-cycle. We showed above that $\sigma_{2r+1}\sigma_{2r+2}$ can be written as one, two or three 3-cycles, $\tau_{t+1} \cdots \tau_{t+u}$, where $u \leq 3$. So $\sigma_1 \cdots \sigma_{2(r+1))} = \tau_1 \cdots \tau_{t+u}$.]

4. **Show that A_n is normal in S_n.**
[You can use any result from the lectures or worksheets.]
Proof 1. $|A_n| = \frac{1}{2}n! = \frac{1}{2}|S_n|$, that is A_n has index 2 in S_n. This means that every left coset of A_n is a right coset of A_n [Wksh 2, question 4 – it has two left cosets (A_n and $S_n \setminus A_n$) and two right cosets (A_n and $S_n \setminus A_n$)] which means that A_n is normal in S_n.

Proof 2: We will show that, for all $\sigma \in S_n$ and $\theta \in A_n$, $\sigma\theta\sigma^{-1}$ is in A_n. [A_n is defined to be the set of even permutations in S_n, therefore:] The sign of θ is +1. Let $\text{sgn}(\sigma)$ be $s \in \{+1, -1\}$. Then $\text{sgn}(\sigma\theta\sigma^{-1}) = \text{sgn}(\sigma)\text{sgn}(\theta)\text{sgn}(\sigma^{-1}) = s^2 = +1$. So $\sigma\theta\sigma^{-1}$ is even.

Proof 3: We will show that, for all $\sigma \in S_n$ and $\theta \in A_n$, $\sigma\theta\sigma^{-1}$ is in A_n. Since A_n is the set of even permutations in S_n, θ can be written as a product of $2k$ transpositions, for some $k \in \mathbf{N}$. If σ is a product of r transpositions, then σ^{-1} can also be written as a product of r transpositions, and so $\sigma\theta\sigma^{-1}$ is a product of $2r + 2k$ transpositions, so it is even.

5. (a) **Show that S_3 is not commutative.**
(12)(123) = (13) but (123)(12) = (23).
(b) **Show that S_n is not commutative for $n \geq 3$.**
[Same proof — (12), (13) and (123) represent elements not just of S_3 but of any S_n, $n \geq 3$.]
(12)(123) = (13) but (123)(12) = (23).

6. **By Cayley's Theorem, every group can be written as a group of permutations. The proof is sketched in the handout on permutations. Write out the proof in full.**

Cayley's Theorem. Every group G is isomorphic to a group of permutations. Specifically, $G \cong H$ for some $H \leq S_G$.
[The idea is that, if we look at the Cayley Table of G, each column is a permutation of G; and if I use first the column for g, and then the column for h, that is the same as using the column for gh.
It might be helpful to first look at the examples in the next two exercises, and then come back to the formal proof.]

Proof. The permutation defined by the column for g is

$$\begin{aligned} \tau_g : \ & G \longrightarrow G \\ \tau_g : \ & x \longrightarrow xg \qquad \forall x \in G. \end{aligned}$$

Our isomorphism will therefore be

$$\begin{aligned} \phi : \ & G \longrightarrow S_G \\ \phi : \ & g \longrightarrow \tau_g \qquad \forall g \in G \end{aligned}$$

and H will be $\phi(G) = \{\tau_g : g \in G\}$.
[Any function ϕ maps G *onto* $\phi(G)$, by definition, and we simply took H to be $\phi(G)$, so we do not need to prove that ϕ is onto. In fact, some people define an isomorphism $\psi : P \to Q$ to be just a 1-1 homomorphism, where it is understood that P is isomorphic not to Q, but to $\psi(P)$.]

We need to show that:

1. $\phi(g)$ is in S_G.
S_G is the set of bijections from G to G. So we want to show that τ_g is a 1-1 mapping from G onto G. By closure, for any $h \in G$, gh is in G, so τ_g does map G to G. Let us show it is 1-1:
if $\tau_g(x) = \tau_g(y)$ then $xg = yg \Rightarrow xgg^{-1} = ygg^{-1} \Rightarrow x = y$.
To show that it is onto, consider an arbitrary $z \in G$;
zg^{-1} exists and is in G (by Inverse and Closure properties),
and $\tau_g(zg^{-1}) = zg^{-1}g = z$.

2. ϕ is 1-1.
We want to show that $g \neq h \Rightarrow \phi(g) \neq \phi(h)$, that is, $\tau_g \neq \tau_h$.
[τ_g and τ_h are themselves functions; if they disagree on even *one* element they must be different functions.]
Now $\tau_g(e) = eg = g$, while $\tau_h(e) = eh = h$.
So if $g \neq h$ then $\tau_g \neq \tau_h$.

3. ϕ is a homomorphism.
We need to show that, for any $g, h \in G$, $\phi(g)\phi(h) = \phi(gh)$; that is, $\tau_g\tau_h = \tau_{gh}$.
[Note that $\tau_g\tau_h$ and τ_{gh} are functions. To show that they are the *same* function, we have to show that they agree on *each* $x \in G$. Remember that $\tau_g\tau_h$ is the function obtained by doing τ_g first, and then τ_h.]
Now $(\tau_g\tau_h)(x) = \tau_h(\tau_g(x)) = \tau_h(xg) = (xg)h = x(gh)$; while $\tau_{gh}(x) = x(gh)$. Since this holds for arbitrary x, $\tau_g\tau_h = \tau_{gh}$. $\square$

We know from Worksheet 2 that there are two groups of order 4. The next two exercises ask you to apply Cayley's Thm to these gps. In each case, you can use permutations of just four symbols. I took a page to explain in detail where the answer comes from, but the answer itself is just one line.

7. **Find permutations e, a, b, c so that $\{e, a, b, c\}$ is the cyclic group C_4.**

The Cayley table of C_4 is:

	e	r	r^2	r^3
e	e	r	r^2	r^3
r	r	r^2	r^3	e
r^2	r^2	r^3	e	r
r^3	r^3	e	r	r^2

or

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The first column (after the |) gives the permutation:

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

The second column gives us:

$$a = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 1 & 2 & 3 & 0 \end{pmatrix} = (0123).$$

The third column gives us:

$$b = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \end{pmatrix} = (02)(13).$$

The fourth column gives us:

$$c = \begin{pmatrix} 0 & 1 & 2 & 3 \\ 3 & 0 & 1 & 2 \end{pmatrix} = (0321).$$

One can check that, say, $ab = c$, $bb = e$ and so on; that is, $(0123)(02)(13) = (0321)$, $(02)(13)(02)(13) = \textsc{id}$. The full table produced by these permutations is (isomorphic to) C_4:

$+$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

.

The short answer is therefore:

$e = \textsc{id}, a = (0123), b = (02)(13), c = (0321)$.

8. **Find permutations e, a, b, c such that e is the identity, $a^2 = b^2 = e$, and $ab = ba = c$. (The set $\{e, a, b, c\}$ is sometimes called the Klein-4 group.)**

   We can use the information to work out the other products — $ac = aab = eb = b$, $bc = bba = ea = a$, $ca = baa = be = b$, $cb = abb = ae = a$, $c^2 = (ab)(ba) = a(bb)a = aea = aa = e$.
   The Cayley table is therefore given by:

$+$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

   We use the column for a to define the permutation a, and similarly for b, c, e. Note that a is both a permutation, and also one of the elements of the permutation, which can be a bit confusing.

   The column for e gives the permutation:
   $$e = \begin{pmatrix} \mathrm{e} & \mathrm{a} & \mathrm{b} & \mathrm{c} \\ \mathrm{e} & \mathrm{a} & \mathrm{b} & \mathrm{c} \end{pmatrix} = \textsc{id}.$$
   The second column gives us:
   $$a = \begin{pmatrix} \mathrm{e} & \mathrm{a} & \mathrm{b} & \mathrm{c} \\ \mathrm{a} & \mathrm{e} & \mathrm{c} & \mathrm{b} \end{pmatrix} = (ea)(bc).$$
   The third column gives us:
   $$b = \begin{pmatrix} \mathrm{e} & \mathrm{a} & \mathrm{b} & \mathrm{c} \\ \mathrm{b} & \mathrm{c} & \mathrm{e} & \mathrm{a} \end{pmatrix} = (eb)(ac).$$
   The fourth column gives us:
   $$c = \begin{pmatrix} \mathrm{e} & \mathrm{a} & \mathrm{b} & \mathrm{c} \\ \mathrm{c} & \mathrm{b} & \mathrm{a} & \mathrm{e} \end{pmatrix} = (ec)(ab).$$

   The short answer is therefore:
   $e = \textsc{id}, a = (ea)(bc), b = (eb)(ac), c = (ec)(ab)$.