Math 343 2004 Solutions

1. A group is a set G with a law of composition satisfying the following axioms:

(G1) for any $x, y \in G$, xy is in G,

(G2) for any x, y, z in G, $x(yz) = (xy)z$,

(G3) there is an element 1 in G such that for all $g \in G$, $g1 = g = 1g$,

(G4) given an element $g \in G$, there is an element g^{-1} of G with $gg^{-1} = 1 = g^{-1}g$.

[4 marks]

Writing the given permutations in cycle notation, we have an element $\pi = (1\ 2\ 3\ 4)(5\ 8\ 7\ 6)$ in G. It is clear that the powers of π (namely $(1\ 3)(2\ 4)(5\ 7)(6\ 8), (1\ 4\ 3\ 2)(5\ 6\ 7\ 8)$ and the identity permutation) are also in G, together with the products of these four permutations by $\rho = (1\ 5\ 3\ 7)(2\ 6\ 4\ 8)$. Thus G has at least 8 elements:

$$1_G, (1\ 2\ 3\ 4)(5\ 8\ 7\ 6), (1\ 3)(2\ 4)(5\ 7)(6\ 8), (1\ 4\ 3\ 2)(5\ 6\ 7\ 8),$$
$$(1\ 5\ 3\ 7)(2\ 6\ 4\ 8), (1\ 6\ 3\ 8)(2\ 7\ 4\ 5), (1\ 7\ 3\ 5)(2\ 8\ 4\ 6), (1\ 8\ 3\ 6)(2\ 5\ 4\ 7).$$

[4 marks]

In order to show that G consists of precisely these 8 elements, we must show that these elements do indeed form a group, since we have already seen that the group generated by the permutations contains at least these 8 elements. To establish that the elements do indeed form a group, we need to do something equivalent to calculating the multiplication table for the eight elements. In our earlier notation, these elements are $1, \pi, \pi^2, \pi^3$ and $\rho, \rho\pi, \rho\pi^2, \rho\pi^3$. The table then is

	1	π	π^2	π^3	ρ	$\rho\pi$	$\rho\pi^2$	$\rho\pi^3$
1	1	π	π^2	π^3	ρ	$\rho\pi$	$\rho\pi^2$	$\rho\pi^3$
π	π	π^2	π^3	1	$\rho\pi^3$	ρ	$\rho\pi$	$\rho\pi^2$
π^2	π^2	π^3	1	π	$\rho\pi^2$	$\rho\pi^3$	ρ	$\rho\pi$
π^3	π^3	1	π	π^2	$\rho\pi$	$\rho\pi^2$	$\rho\pi^3$	ρ
ρ	ρ	$\rho\pi$	$\rho\pi^2$	$\rho\pi^3$	π^2	π^3	1	π
$\rho\pi$	$\rho\pi$	$\rho\pi^2$	$\rho\pi^3$	ρ	π	π^2	π^3	1
$\rho\pi^2$	$\rho\pi^2$	$\rho\pi^3$	ρ	$\rho\pi$	1	π	π^2	π^3
$\rho\pi^3$	$\rho\pi^3$	ρ	$\rho\pi$	$\rho\pi^3$	π^3	1	π	π^2

The table shows closure, identity and inverses. Since permutations are maps and are therefore associative under composition, we have shown that the 8 elements form a group and so this is the group generated by π and ρ. [Of course any alternative way to enumerate the group elements or express the table will attract full marks.] [8 marks]

As for the orders of the elements of G, we can use the table (say) to see that the only element of order 2 is π^2. All other non-identity elements of G have square equal to π^2 and so have order 4.

[2 marks]

Finally, we need to find a non-trivial element of G for which the corresponding row of the table is equal to the column for that element. A visual inspection shows that we can take z to be π^2.

[2 marks]

2 (1). Let x, y be the elements of X. The possible maps from X to X are then

$$f_1(x) = x \quad f_1(y) = y \quad ; \quad f_2(x) = x \quad f_2(y) = x;$$
$$f_3(x) = y \quad f_3(y) = y \quad ; \quad f_4(x) = y \quad f_4(y) = x.$$

We see that two of these maps are bijections (f_1 and f_4), but the other two are not bijections. Since the condition for a map to have an inverse is that it is bijective, some members of the set of maps from X to X do not have inverses and so this set cannot be a group. [6 marks]

(2) A subgroup H of a group G is said to be *cyclic* if there is an element h in H such that each element of H is a power of our fixed h.

[2 marks]

Lagrange's Theorem states that if H is a subgroup of a finite group G then $|H|$ divides $|G|$ and $|G|/|H|$ is equal to the number of distinct cosets of H in G.

[2 marks]

If G has order p, let x be any non-trivial element of G, then $|\langle x\rangle|$ has order dividing p. Since this order is not 1 by choice, it must be p, so $G = \langle x\rangle$ and so G is cyclic.

[4 marks]

Now, for the group $D(4)$, the subgroup $\{1, a, a^2, a^3\}$ consisting of the powers of a is a cyclic subgroup with 4 elements. A non-cyclic subgroup is slightly harder to find, but we can check (by giving its multiplication table) that the set $\{1, a^2, b, ba^2\}$ is a subgroup:

	1	a^2	b	ba^2
1	1	a^2	b	ba^2
a^2	a^2	1	ba^2	b
b	b	ba^2	1	a^2
ba^2	ba^2	b	a^2	1

This subgroup is not cyclic because every non-identity element has order 2.

[6 marks]

3. Suppose first that $xH = yH$. Then, since $1 \in H$, $x1_G = x \in yH$. Thus $x = yh$ for some $h \in H$. Then $y^{-1}x = h \in H$. Conversely, if $y^{-1}x = h \in H$ and $xh_1 \in xH$ then, since $x = yh$, $xh_1 = yhh_1 = yh_2$ with $h_2 \in H$ so $xH \subseteq yH$. On the other hand, if $yh_1 \in yH$, then since $y = xh^{-1}$ we see that $yh_1 = xh^{-1}h_1 = xh_3$ for some h_3 in H. We deduce that $yH \subseteq xH$ and conclude that $xH = yH$. [6 marks]

The set H is a subgroup of G because it is the subgroup generated by a^2, of order 4. [Alternatively, one could construst the table for H.]

[1 marks]

The distinct left cosets of H in G are:

$$H = 1H \;=\; \{1, a^2, a^4, a^6\}$$

$$\begin{aligned} aH &= \{a, a^3, a^5, a^7\} \\ bH &= \{b, ba^2, ba^4, ba^6\} \\ baH &= \{ba, ba^3, ba^5, ba^7\}. \end{aligned}$$

[4 marks]

The right cosets H and Ha are clearly equal to H and aH respectively. Also, since $ab = ba^7$, an easy check shows that $bH = Hb$ and $baH = Hba$, so every left coset is a right coset and H is a normal subgroup of G.

[3 marks]

The elements of G/H are the four cosets H, aH, bH, baH. Now

$$H^2 = HH = H; \qquad (aH)^2 = aHaH = a^2H = H;$$
$$(bH)^2 = bHbH = b^2H = H; \qquad (baH)^2 = baHbaH = (ba)^2H = H.$$

Since every element of G/H has order 2, G/H is not cyclic.

[3 marks]

Finally if g is any element of G, gH must be one of our four distinct cosets, so $(gH)^2 = H$. This means that $g^2H = H$, so that g^2 is an element of H.

[3 marks].

4. For any element g in G, the conjugacy class of g is the set of distinct conjugates (elements of the form $x^{-1}gx$) . The centralizer of g is the set of elements in G which commute with our given g: $C_G(g) = \{x \in G : xg = gx\}$.

[2 marks]

To show that $C_G(g)$ is a subgroup of G, first note that 1_G is in $C_G(g)$ because 1_G commutes with every element of G. If $x, y \in C_G(g)$, then $xg = gx$ and $yg = gy$. Then

$$(xy)g = x(yg) = x(gy) = (xg)y = (gx)y = g(xy)$$

so $xy \in C_G(g)$. Finally for $x \in C_G(g)$, $xg = gx$ so $g = x^{-1}gx$ and $gx^{-1} = x^{-1}g$, so $x^{-1} \in C_G(g)$. Thus $C_G(g)$ is a subgroup of G.

[3 marks]

Now consider what happens if two conjugates of g are equal: if $xgx^{-1} = ygy^{-1}$, then $xg = ygy^{-1}x$ and $y^{-1}xg = gy^{-1}x$. Thus, $y^{-1}x$ is in $C_G(x)$, and so is equal to some element h in $C_G(g)$. Then since $y^{-1}x = h$, we see that

$x = hy$. Conversely, each element of the form hy ($h \in C_G(g)$) will produce the same conjugate as does y

$$(hy)^{-1}ghy = y^{-1}h^{-1}ghy = y^{-1}gy \text{ (since } h \in C_G(g)).$$

It now follows that when we form the $|G|$ conjugates $x^{-1}gx$ as x varies over G, each value is repeated $|C_G(g)|$ times, so the number of distinct values is $|G|/|C_G(g)$.

[5 marks]

We now turn to the group $D(n)$ for n odd. Each power of a centralises each other power. This follows from the index laws because

$$a^i a^j = a^{i+j} = a^{j+i} = a^j a^i.$$

[1 mark]

It now follows that the centralizer of a^i has at least n elements. However b does not centralize a^i, since we are told that $b^{-1}a^ib = a^{-i}$. If a^i were equal to a^{-i} (non-zero i), then a^{2i} would equal 1. This is impossible because a has order n and n is odd. It follows that each $a^i (i \neq 0)$ has precisely two conjugates.

[3 marks]

As for b, we know that no power of a centralizes b, and the only other elements in G are of the form ba^i. If ba^i centralized b, we would have $b(ba^i) = (ba^i)b$. Since b has order 2, this would give that $a^i = a^{-i}$ and, as we have seen, this can only happen when $i = 0$. Thus only 1_G and b centralize b so b has n conjugates.

[4 marks]

Thus we have: the identity element in a class on its own; the remaining $n-1$ powers of a in $(n-1)/2$ classes with two elements each; and all elements of the form ba^i in one conjugacy class. This makes $1 + (n-1)/2 + 1 = (n-1+4)/2 = (n+3)/2$ conjugacy classes.

[2 marks]

5. Let θ be a map from $(G, \circ)$ to $(H, *)$. Then θ is a group homomorphism if for all x, y in G, $\theta(x \circ y) = \theta(x) * \theta(y)$. [1 mark]

It follows that $\theta(1_G) * \theta(g) = \theta(g)$ for all $g \in G$, so $\theta(1_G)$ is the identity element of H (by uniqueness) as required.

Also $\theta(g) * \theta(h) = \theta(1_G) = 1_H$, so $\theta(h)$ is the inverse of $\theta(g)$. [2 marks]

We have

$$\ker\,\theta = \{g \in G : \theta(g) = 1_H\}$$

[1 mark]

and

$$\text{im}\,\theta = \{h \in H : h = \theta(x) \text{ for some } x \in G\}.$$

[1 mark]

To show that $K = \ker\,\theta$ is a subgroup of G, note the 1_G is in H since we have just shown that $\theta(1_G) = 1_H$. Now if $x, y \in K$ then $\theta(x) = 1_H = \theta(y)$. Since θ is a homomorphism,

$$\theta(xy) = \theta(x)\theta(y) = 1_H 1_H = 1_H$$

so $xy \in K$. Finally if $x \in K$, $\theta(x) = 1_H$, and

$$\theta(x^{-1}) = (\theta(x))^{-1} = (1_H)^{-1} = 1_H.$$

Thus H is a subgroup of G. Finally K is a normal subgroup, because if x is in K and g is in G, then

$$\theta(g^{-1}xg) = \theta(g^{-1})\theta(x)\theta(g) = (\theta(g))^{-1}1_H\theta(g) = 1_H$$

[4 marks]

The homomorphism theorem states that if θ is a homomorphism from G to H then

- im θ is a subgroup of H;
- ker θ is a normal subgroup of G and
- $G/\ker\,\theta \cong \text{im}\,\theta$.

[3 marks]

For two elements of G, we can evaluate their product (since in each map the operation in group G is matrix multiplication):

$$\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix} = \begin{pmatrix} a_1a_2 & a_1b_2 + b_1c_2 \\ 0 & c_1c_2 \end{pmatrix}.$$

Now consider the map θ_1. Since

$$\theta_1(\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}) = b_1 \text{ and } \theta_1(\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}) = b_2.$$

It is clear that $b_1 + b_2$ is not equal to $a_1 b_2 + b_1 c_2$ in general (for example if $a_1 = 1$, $c_2 = -1$ and $b_2 \neq 0$). Thus θ_1 is not an homomorphism. [3 marks]

However,

$$\theta_2(\begin{pmatrix} a_1 & b_1 \\ 0 & c_1 \end{pmatrix}) = a_1 \text{ and } \theta_1(\begin{pmatrix} a_2 & b_2 \\ 0 & c_2 \end{pmatrix}) = a_2,$$

whereas

$$\theta_2(\begin{pmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{pmatrix}) = a_1 a_2.$$

Since the group operation in H is multiplication of non-zero numbers, θ_2 is a group homomorphism. Its kernel is the set of matrices of the form $\begin{pmatrix} 1 & b \\ 0 & c \end{pmatrix}$ and its image is the complete set of non-zero real numbers. [5 marks]

6. If a permutation π is an n-cycle, then π is even when n is an odd integer and π is odd when n is an even integer. For a general permutation, we use the fact that the sign of a product of permutations is multiplicative.

[2 marks]

When π is written as a product of disjoint cycles, the order of π is the least common multiple of the disjoint cycle lengths of π. [1 mark]

Now consider

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & & 9 & 10 \\ 10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 & \end{pmatrix} = (1\ 10)(2\ 9)(3\ 8)(4\ 7)(5\ 6).$$

Thus the sign of π is $(-1)^5 = -1$ and π has order 2. As for

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix} = (1\ 2\ 4\ 8\ 7\ 5\ )(3\ 6),$$

we see that ρ has sign $-1 \times -1 = 1$ and order 6. [4 marks]

The identity permutation is even (a product of disjoint 1-cycles). If π and ρ are even, so is $\pi\rho$. If π is even, since $\pi\pi^{-1} = 1_{S(n)}$, it follows that π^{-1} is also even. Thus $A(n)$ is a subgroup of $S(n)$. It is a normal subgroup because it has index 2. [4 marks]

The alternating group $A(4)$ has, by definition, only even elements. There are 12 such elements: the identity element (which is of order 1), eight 3-cycles $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 3\ 4), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)$ (these are all of order 3). The remaining three elements are $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$ all of order 2. [3 marks]

In any symmetric group, orders of elements are determined by cycle types, so possible orders in $S(4)$ are 1, 2, 3, 4 or 2 (corresponding to cycles of length up to 4 and products of two disjoint cycles). In $S(5)$ we have cycles of orders 1, 2, 3, 4 or 5, disjoint cycles may be of the form (1 2)(3 4) (order 2) or (1 2)(3 4 5) (order 6). Thus the required integer n is 5. [2 marks]

The situation is slightly different for alternating groups. The permutation (1 2)(3 4 5) is odd, so the required m is greater then 5. However, $S(6)$ has two types of elements of order 6: 6-cycles and type (1 2)(3 4 5) again. Both these are odd permutations and so are not in $A(6)$. Turning to $S(7)$, we can form an extra type of permutation of order 6 such as (1 2)(3 4)(5 6 7). This permutation is even, so the required m is 7. [4 marks]

7. Let p be a prime and G be a finite group of order $p^k n$ where p does not divide n. Then:

(1) G has Sylow p-subgroups (subgroups of order p^k),

(2) the number of these is congruent to 1 mod p,

(3) if P is a Sylow p-subgroup and Q is any p-subgroup, there is an element g of G such that $gQg^{-1} \subseteq P$,

(4) any two Sylow p-subgroups are conjugate, the number of these divides $|G|$. [4 marks]

If there is precisely one Sylow p-subgroup P, then every conjugate of P must be equal to P, so P is a normal subgroup. If P is normal, then every conjugate of P is equal to P, so each Sylow p-subgroup must equal P. [2 marks]

Suppose that G is a group of order $33 = 3 \times 11$ the number of Sylow 3-subgroups is $1, 4, 7, 10, , \ldots$ and divides 33, so is 1. The number of Sylow 11 subgroups is $1, 12, 23, , \ldots$ and divides 33 so is also 1. Thus G has a unique Sylow 3-subgroup, P, say, and a unique Sylow 11-subgroup Q, say. These are each normal. If x is an element of order 3, then $P = \langle x \rangle$ so P contains both the elements of G of order 3. Similarly if y is an element of order 11, then $Q = \langle y \rangle$ so Q contains all 10 elements of G of order 11. It follows by Lagrange that there must be elements of G of order 33 (the only divisor of 33 apart from 1, 3, 11), so G is cyclic. [4 marks]

Suppose that G is a group with $56 = 7 \times 8$ elements. The number of Sylow 2-subgroups is either 1 or 7. The number of Sylow 7-subgroups is either 1 or 8. If the Sylow 7-subgroup is not normal, there are 8 Sylow 7-subgroups. In this case, the intersection of any two of these distinct subgroups would (by Lagrange's theorem) intersect in the identity element, giving in total 48 elements of order 5, and only leaving 7 non-identity elements of G to be distributed in the Sylow 2-subgroups. Since a Sylow 2-subgroup has 7 non-identity elements, it follows that there could only be one Sylow 2-subgroup. We deduce that G either has a normal Sylow 7-subgroup or has a normal Sylow 2-subgroup. [5 marks]

Finally, if G is the dihedral group $D(6)$, G has 12 elements, so has Sylow 2 subgroups and Sylow 3 subgroups. The number of Sylow 3-subgroups is 1 or 4. The elements of G are powers of a or ba^i (all of order 2), so only a^2 and a^4 have order 3. This means that there is a unique Sylow 3-subgroup.

The number of Sylow 2-subgroup is one or three, each containing 3 non-identity elements. There are 7 elements in G of order 2 (six of the form ba^i and a^3). Thus, there must be more than one Sylow 2-subgroup, so that there are 3 sylow 2-subgoups.

[5 marks]

8. The Jordan-Hölder Theorem says that any two composition series of a group are isomorphic. [1 mark]

A composition series is a finite series of subgroups, each normal in the next

$$G = G_0 \geq G_1 \geq \cdots G_k = \{1\}$$

which can not be refined without repeating terms. [1 mark]

Two composition series are isomorphic if there is a bijection between the quotient groups in the respective series so that corresponding quotient groups are isomorphic. [1 mark]

If H/K has prime order p, a normal subgroup L of H with $K \leq L \leq H$ would give rise to a normal subgroup of H/K. Since H/K has prime order, so L is either H or K.

[3 marks]

(a) Let G be a cyclic group with 8 elements generated by x (so $x^8 = 1$). Then $\langle x^2 \rangle$ is a subgroup of G with 4 elements which is normal since G is abelian. Then $\langle x^4 \rangle$ is a subgroup of $\langle x^2 \rangle$ of index 2 (and so is normal). It follows from our basic lemma that a composition series for G is

$$G \geq \langle x^2 \rangle \geq \langle x^4 \rangle \geq \{1\}.$$

[3 marks]

(b) Now let G be the dihedral group $D(3)$ with generators a of order 3 and b of order 2. Then $K = \langle a \rangle$ has three elements and is a normal subgroup of G since its index is 2. K has prime order, we again use our basic result to obtain a composition series

$$G \geq K \geq \{1\}.$$

[2 marks]

(c) Next, let G be a group with 35 elements. The number of Sylow 5-subgroups in G is 1 mod 5 and divides 35, so is one. Thus this subgroup S, say, is a normal subgroup of G. Because 5 is prime, S has no non-trivial proper subgroup and since S has index 7 in G, no subgroup of G lies between G and S, so the series

$$G \geq S \geq \{1\}$$

is a composition series.

[5 marks]

(d) Now let G be the dihedral group $D(8)$. The element a generates a subgroup with 8 elements which has index and so is normal. We can then use the composition series for part (1) to obtain the composition series

$$D(8) \geq \langle a \rangle \geq \langle a^2 \rangle \geq \langle a^4 \rangle \geq \{1\}.$$

This is a composition series since the indices are all equal to the prime 2, and all steps are normal since all have index 2.

[4 marks]