Math 343 2003 Solutions.

1. (a) 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, it is clear that the powers of (1 3 4 2) (namely (1 3 4 2), (1 4)(2 3), (1 2 4 3) and the identity permutation) are in G, together with the products of these four permutations by (2 3). Thus G has at least 8 elements:

$$1_G, (1\ 3\ 4\ 2), (1\ 4)(2\ 3), (1\ 2\ 4\ 3), (2\ 3), (1\ 3)(2\ 4), (1\ 4), \text{ and } (1\ 2)(3\ 4)$$

[3 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 elements. For convenience denote (1 3 4 2) by π and (2 3) by ρ, so that the 8 elements are $1, \pi, \pi^2, \pi^3$ and $\rho, \pi\rho, \pi^2\rho, \pi^3\rho$. The table then is

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

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 π and π^3 each have order 4, while each other non-identity element of G has order 2.

[3 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. First, we show that the equation does have a solution by setting $x = u^{-1}v$ so that

$$ux = u(u^{-1}v) = (uu^{-1})v = 1v = v$$

using (G2), (G4) and (G3) respectively. Now the solution is unique because if $ux_1 = v$ and $ux_2 = v$ then $ux_1 = ux_2$ so multiplying on the left by u^{-1} gives $u^{-1}(ux_1) = u^{-1}(ux_2)$. now using associativity, $(u^{-1}u)x_1 = (u^{-1}u)x_2$. Then the inverse axiom implies that $1x_1 = 1x_2$, so finally the identity axiom shows that $x_1 = x_2$.

[6 marks]

If $G = D(4)$, the solution to $a^2x = ba$ is

$$\begin{aligned} x &= (a)^{-2}ba = a^2ba = aaba \\ &= a(ab)a = aba^{-1}a = ab = ba^{-1} = ba^3. \end{aligned}$$

[3 marks]

To calculate the square of elements in $D(4)$

$$1^2 = 1, a^2 = a^2, (a^2)^2 = a^4 = 1, (a^3)^2 = a^6 = a^2.$$

Each of the other 4 elements of G has the form ba^i and

$$(ba^i)^2 = ba^iba^i = bba^{-i}a^i = b^2 = 1,$$

and so each has order 2.

[2 marks]

From the list of squares of elements of G, we see that a and a^3 are both solutions of $x^2 = a^2$, so this equation has a solution, but not a unique solution.

[2 marks]

If $x^2 = b$ had a solution, we could find an x whose square is b. However we have seen that the square of $1, a^2, b, ba, ba^2$ and ba^3 are all 1, whereas the square of a and a^3 are both a^2, so the equation has no solution.

[2 marks]

It x were a power of a, then xa would be a power of a, while bx could not be a power of a. On the other hand, if x were of the form ba^i, then bx would be a power of a while xa would be b times a power of a which is again impossible, so the equation has no solutions.

[5 marks]

3. A *subgroup* of a group G is a non-empty subset of G which is itself a group under the same law of composition which holds in the group G. A subgroup H 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.

[4 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]

For $D(6)$, a has order 6, a^2 has order 3, a^3 has order 2, a^4 order 3 and a^5 has order 6. All elements of the form ba^i have order 2, since

$$ba^iba^i = b(a^ib)a^i = ba^{-i}a^i = 1$$

[Alternatively all elements like ba^i correspond to reflections in the dihedral group , so have order 2.] Since $D(6)$ has an element a of order 6, the subgroup generated by a is a cyclic subgroup with 6 elements.

[5 marks]

The elements of $A(4)$ are 1 (order 1), $(1\ 2)(3\ 4), (1\ 3)(2\ 4)(1\ 4)(2\ 3)$ (all of order 2) together with 8 three cycles, obtained by leaving out one of the four symbols, and considering the two possible cycle orientations (all of order 3). Thus each non-identity element of G has order 2 or 3. Thus if H is a cyclic subgroup of G, generated by g, say, then g has order 2 or 3, so $|H| = 2$ or 3. Thus every cyclic subgroup of G has prime order.

[5 marks]

4. Suppose that xH, yH are two left cosets of H in G and suppose that these cosets are unequal. If z were an element in both xH and yH, then $z = xh$ and $z = yh_1$ for some $h, h_1 \in H$. Thus $xh = yh_1$, so $y^{-1}x = h_1h^{-1}$. Then $y^{-1}x$ is an element h_2, say of H since H is a subgroup. It then follows that $xH = yH$ contrary to assumption. We deduce that if xH, yH are unequal they can have no elements in common.

[4 marks]

A subgroup N is a normal subgroup of G if, for all n in N and g in G, gng^{-1} is an element of G.

[1 mark]

Now let G be the dihedral group $D(3)$, and H be the subgroup with two elements 1 and b. Since $|H| = 2$, there are three distinct left cosets and since

$$H, \quad aH = \{a, ab = ba^2\}, \quad a^2H = \{a^2, a^2b = ba\},$$

this is the complete list of (left) cosets. The right cosets are

$$H, \quad Ha = \{a, ba\}, \quad Ha^2 = \{a^2, ba^2\}.$$

Note that aH is not equal to Ha.

[5 marks]

Now let K be the subgroup with the three elements $\{1, a, a^2\}$. Since H has index 2 in G, H is a normal subgroup of G and so is a normal subgroup. The quotient group G/K has order 2 and so is cyclic. [4 marks]

First of all N is a subgroup because 0 (the identity element) is a multiple of n, if r and s are multiples of n, say $r = kn$ and $s = ln$ then $r+s = kn+ln = (k+l)n$ and finally $-r = -(kn) = (-k)n$. Every subgroup of $\mathbf{Z}$ is normal because $\mathbf{Z}$ is abelian.

[3 marks]

When $n = 10$, two integers r, s are in the same coset of $\mathbf{Z}$ precisely when $r - s$ is a multiple of 10, so that $r - s$ ends in a zero and r, s have the same last digit. Thus the 10 cosets of N are ten sets of integers. Each set being those ending in the same digit (the congruence classes modulo 10).

[3 marks]

5. Let $\theta : (G, \circ) \to (H, *)$ be a group homomorphism. Then 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]

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]

Before checking for the homomorphism property, it might be convenient to obtain the formula for the product of two element A, B in G:

$$\begin{pmatrix} a_1 & a_2 & a_3 \\ 0 & a_1 & a_2 \\ 0 & 0 & a_1 \end{pmatrix} \begin{pmatrix} b_1 & b_2 & b_3 \\ 0 & b_1 & b_2 \\ 0 & 0 & b_1 \end{pmatrix} = \begin{pmatrix} a_1b_1 & a_2b_1 + b_2a_1 & a_1b_3 + a_2b_2 + a_3b_1 \\ 0 & a_1b_1 & a_2b_1 + b_2a_1 \\ 0 & 0 & a_1b_1 \end{pmatrix}$$

(a) To check if θ_1 is a homomorphism, we need to see if $\theta_1(A)\theta_1(B) = \theta_1(AB)$. From our formula for AB, we see that this is so (θ_1 is a homomorphism). Its image is the whole group (every real number can occur on the diagonal of an element of G) and its kernel K is the subgroup of G consisting of those matrices in G with 1 down the main diagonal (so $a_1 = 1$).

[4 marks]

(b) A similar argument for θ_2 (remembering that the target group is a group under addition), shows that we need to check if $a_1b_2 + a_2b_1$ is equal to $a_1 + b_1$. This is not the case (take $b_2 = 0 = a_2$), so θ_2 is not a homomorphism.

[2 marks]

(c) the required check for this case is that $a_1b_3 + a_2b_2 + a_3b_1 = a_1 + b_1$, so this also fails to be a homomorphism (take $b_3 = b_2 = 0 = a_3$).

[2 marks]

For the final part, the map of case (a) is a homomorpism, and its image is abelian. Thus, by the homomorphism theorem, G/K is isomorphic to an abelian group. Since K is a normal subgroup of G, it only remains to see if the subgroup K is abelian. Our general formula for AB would then give

$$\begin{pmatrix} 1 & a_2 + b_2 & a_3 + a_2b_2 + b_3 \\ 0 & 1 & a_2 + b_2 \\ 0 & 0 & 1 \end{pmatrix}$$

Since this is symmetric in the a's and b's, K is an abelian group as required.

[4 marks]

6. The conjugacy class of g is the set of distinct elements of G of the form $x^{-1}gx$ as x varies over G. The centralizer of g is the set of elements of G which commute with g so

$$C_G(g) = \{x \in G : xg = gx\} = \{x \in G : g = x^{-1}gx\}$$

[2 marks]

To show that $C_G(g)$ is a subgroup, it is clear that the identity element commutes with g, if $x, y \in C_G(g)$ then $xg = gx$ and $yg = gy$, so

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

so $xy \in C_G(g)$. Also if $x \in C_G(g)$, then $xg = gx$ so $g = x^{-1}Gx$ and so $gx^{-1} = x^{-1}g$, so x^{-1} is also in $C_G(g)$. Thus $C_G(g)$ is a subgroup of G.

[3 marks]

The required result is that the number of distinct elements in the conjugacy class of G is equal to $|G|/|C_G(g)|$. [2 marks]

For the group $D(4)$ we first observe that $a^2b = ba^{-2}$. Since a has order 4, $a^2 = a^{-2}$, so b is in $C_G(a^2)$. Since a is also in this group, every element of G is in $C_G(a^2)$, so $G = C_G(a^2)$, This means that a^2 has only one conjugate.

[3 marks]

In this same group, now consider $C_G(b)$: we have just seen that a^2 commutes with b, as does b. There are therefore at least 4 elements of G which commute with b: $1, b, a^2, ba^2$. Since the centralizer is a subgroup and a does not commute with b, $|C_G(b)| = 4$ and b has two conjugates. Clearly b is a conjugate of b, so let's work out $a^{-1}ba$:

$$a^{-1}ba = a^3ba = a^2aba = a^2ba^{-1}a = a^2b.$$

Since a^2 commutes with b, the two conjugates of b are b and ba^2.

[3 marks]

To show that $(x^{-1}gx)^k = x^{-1}g^kx$, first note that the anchor step is trivial. Then

$$(x^{-1}gx)^{k+1} = (x^{-1}gx)^k(x^{-1}gx) = x^{-1}g^kx(x^{-1}gx) = x^{-1}g^{k+1}x$$

as required. [2 marks]

Now suppose that g has order k. Then $g^k = 1$, so $(x^{-1}gx)^k = x^{-1}g^kx = x^{-1}1x = 1$. It follows that the order of $x^{-1}gx$ divides k. Conversely, if $x^{-1}gx$ has order l, then $1 = (x^{-1}gx)^l = x^{-1}g^lx$, so $g^l = 1$, and so k divides l. It follows that $k = l$. [3 marks]

If there is only element, z, say in G with order 2, then any conjugate $x^{-1}zx$ must equal z, so $zx = xz$ for all x in G. [2 marks]

7. Let p be a prime and G be a finite group of order p^kn 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 15=3×5 the number of Sylow 3-subgroups is $1, 4, 7, 10, , \ldots$ and divides 15, so is 1. The number of Sylow 5 subgroups is $1, 6, 11, 16, \ldots$ and divides 15 so is also 1. Thus G has a unique Sylow 3-subgroup, P, say, and a unique Sylow 5-subgroup Q, say. These are each normal with P containing all 2 non-identity elements of G of order 3 and Q containing all 4 non-identity elements of G of order 5. It follows by Lagrange that there must be elements of G of order 15 (the only other divisor of 15), so G is cyclic. [4 marks]

Now suppose that G is a group with 80=5×16 elements. The number of Sylow 2-subgroups is either 1 or 5. The number of Sylow 5-subgroups is either 1 or 16. If the Sylow 5-subgroup is not normal, there are 16 Sylow 5-subgroups. In this case, these distinct subgroups would pairwise intersect in the identity element, giving in total 64 elements of order 5, and only leaving 15 non-identity elements of G to be distributed in the Sylow 2-subgroups. Since a Sylow 2-subgroup has 15 non-identity elements, it follows that there could only be one Sylow 2-subgroup. We deduce that G either has a normal Sylow 5-subgroup or has a normal Sylow 2-subgroup. [4 marks]

Finally, if G is the symmetric group on 4 symbols, G has 24 elements, so has Sylow 2 subgroups and Sylow 3 subgroups. The number of Sylow 3-subgroups is 1 or 4. There are 8 elements of order 3 in $S(4)$, and since a Sylow 3-subgroup has three elements, these 8 elements must be distributed over 4 subgroups. The number of Sylow 2-subgroup is 1 or 3. Suppose there was a unique Sylow 2-subgroup, N say. If g were an element of order 2 in G, then $\langle g \rangle$ would be a subgroup of N, so g would be in N. However G has 6 transpositions together with 3 elements of cycle type 2^2, so this is impossible and G has four Sylow 3-subgroups and 3 Sylow 2-subgroups.

[6 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 of order 10 generated by x (so $x^{10} = 1$). Then $\langle x^2 \rangle$ is a subgroup of G with 5 elments which is normal since G is abelian. It follows (since 5 is prime) that a composition series for G is

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

[2 marks]

(b) Now let G be the dihedral group $D(4)$ with generators a of order 4 and b of order 2. Then $K = \langle a \rangle$ has four elements and is a normal subgroup of G since its index is 2. Next $\langle a^2 \rangle$ has 2 elements and is a normal subgroup of K because it has index 2 (or because K is abelian). Then

$$G \geq K \geq \langle a^2 \rangle \geq \{1\}$$

is a composition series for G, since each term is normal in the next and all the indices are prime (=2).

[3 marks]

(c) Next, let G be a group with 39 elements. The number of Sylow 13-subgroups in G is 1 mod 13 and divides 39, so is one. Thus this subgroup S, say, is a normal subgroup of G. Because 13 is prime, S has no non-trivial proper subgroup and since S has index 3 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 symmetric group $S(3)$. The element $g = (1\ 2\ 3)$ has three powers: $g, g^2 = (1\ 3\ 2)$ and $g^3 = 1$ so these three powers form the subgroup $\langle g \rangle$. This subgroup is normal since it has index 2. Thus we have a series for G

$$S(3) \geq \langle g \rangle \geq \{1\}.$$

This is a composition series since the indices are 2 and 3 which are prime.

[4 marks]