Math 343 2005 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 permutation in cycle notation, it is clear that $\theta = (1\ 2\ 3\ 4)$ and so $\theta^{-1} = (1\ 4\ 3\ 2)$. The condition that $\theta\phi = \phi\theta^{-1}$ can now be checked at each integer in $\{1, 2, 3, 4\}$, so given that $\phi(1) = 1$:

$$\theta\phi(1) = \phi\theta^{-1}(1)$$

or $\phi(4) = \theta\phi(1) = 2$. Similarly, $\theta\phi(2) = \phi(1) = 1$, so $\phi(2) = 4$. Finally $\theta\phi(3) = \phi(2) = 4$ so $\phi(3) = 3$. It follows that $\phi = (2\ 4)$.

[5 marks]

Now let $G = \langle \theta, \phi \rangle$. Then the four powers of θ are clearly in G together with their products with ϕ. Thus G has at least 8 elements:

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

(or $1, \theta, \theta^2, \theta^3, \phi, \phi\theta, \phi\theta^2, \phi\theta^3$ in our previous notation).

[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 this, we need to do something equivalent to calculating the multiplication table for the elements. The table is

	1	θ	θ^2	θ^3	ϕ	$\phi\theta$	$\phi\theta^2$	$\phi\theta^3$
1	1	θ	θ^2	θ^3	ϕ	$\phi\theta$	$\phi\theta^2$	$\phi\theta^3$
θ	θ	θ^2	θ^3	1	$\phi\theta^3$	ϕ	$\phi\theta$	$\phi\theta^2$
θ^2	θ^2	θ^3	1	θ	$\phi\theta^2$	$\phi\theta^3$	ϕ	$\phi\theta$
θ^3	θ^3	1	θ	θ^2	$\phi\theta$	$\phi\theta^2$	$\phi\theta^3$	ϕ
ϕ	ϕ	$\phi\theta$	$\phi\theta^2$	$\phi\theta^3$	1	θ	θ^2	θ^3
$\phi\theta$	$\phi\theta$	$\phi\theta^2$	$\phi\theta^3$	ϕ	θ^3	1	θ	θ^2
$\phi\theta^2$	$\phi\theta^2$	$\phi\theta^3$	ϕ	$\phi\theta$	θ^2	θ^3	1	θ
$\phi\theta^3$	$\phi\theta^3$	ϕ	$\phi\theta$	$\phi\theta^2$	θ	θ^2	θ^3	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 θ and ϕ. [Of course any alternative way to enumerate the group elements or express the table will attract full marks.]

[6 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 θ^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 $x_1 = x_2$.

[4 marks]

Now

$$(uv)(v^{-1}u^{-1}) = u(v(v^{-1}u^{-1})) = u((vv^{-1})u^{-1}) = u1_Gu^{-1} = uu^{-1} = 1_G,$$

so since inverses are unique, the inverse of uv is $v^{-1}u^{-1}$ as required.

[2 marks]

If $G = D(6)$, the solution to $ax = ba^2$ is obtained by premultiplying by a^{-1} to obtain $x = a^{-1}ba^2$. It only remains to put this in our standard form using the relation that $b^{-1}ab = a^{-1}$ or $ba = a^{-1}b$ to obtain the unique solution that $x = baa^2 = ba^3$.

[2 marks]

Similarly, if $a^{-1}ya = b$, postmultiply by a^{-1} to give $a^{-1}y = ba^{-1}$. Now premultiply by a to obtain $y = aba^{-1}$. Then using the fact that $ab = ba^{-1}$, we see that the equation has the unique solution $y = ba^{-1}a^{-1} = ba^{-2} = ba^4$.

[3 marks]

Next consider the equation $xax^{-1} = a^5 = a^{-1}$. We are given that b provides one solution to this equation. Clearly, all powers of a commute with a, so also consider

$$(ba)a(ba)^{-1} = baaa^{-1}b^{-1} = bab^{-1} = a^{-1},$$

so ba is another solution. (In fact ba^2, ba^3 ba^4 and ba^5 are the others).

[3 marks]

To show that $xax^{-1} = a^3$ has no solution, square both sides to obtain

$$(a^3)^2 = a^6 = 1 = (xax^{-1})^2 = xax^{-1}xax^{-1} = xa^2x^{-1}$$

If this were the case, we would deduce (after premultiplying by x^{-1} and postmultiplying by x) that $a^2 = 1$, so this is impossible. Taking x to be any of the six powers of a gives $xax^{-1} = a$ and if $x = ba^i$, then

$$xax^{-1} = ba^ia(ba^i)^{-1} = ba^{i+1}a^{-i}b^{-1} = bab^{-1} = a^{-1},$$

so the equation $xax^{-1} = a^2$ has no solutions. (Alternatively, one could cube the equation $xax^{-1} = a^2$ to obtain a contradiction.)

[6 marks]

3. An *element* g of a group G has order k if k is the smallest positive integer such that $g^k = 1_G$.

[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 now g is an element of G of order k, we consider the k distinct powers of g $H = \{1, g, g^2, \ldots, g^{k-1}\}$. It can be checked that H is a subgroup:

the set contains $1_G(= x^0)$, and is closed under products since $g^i g^j = g^{i+j}$. After reducing $i + j$ modulo k, this is another element of H. Similarly H is closed under inverses (the inverse of 1 is 1 and for $i \neq 0$ the inverse of g^i is g^{k-i}).

It follows by Lagrange that k divides $|G|$. In particular, if G has an element of order 2, then 2 divides $|G|$, so G has even order.

[4 marks]

The subgroup H is cyclic generated by g if g is an element of H and every element of H is a power of g. Now suppose that g has order k and m is a divisor of k so that $k = mn$ for some integer n. Then g^n certainly satisfies $(g^n)^m = g^{mn} = g^k = 1_G$. If g^n has order r, say for $r < m$, then $1_G = (g^n)^r = g^{nr}$. This would contradict the definition of k since $nr < mn = k$, so g^n has order m as required.

[6 marks]

Now let n be an even integer and G be $D(n)$. In G , every element of the form ba^i has order 2 (since $ba^iba^i = b^{-1}a^iba^i = a^{-i}a^i = 1_G$), so in the search for elements of order 4, we only need consider powers of a, these generate a subgroup with n elements, so the condition that one of these has order 4 is that 4 divides n (by Lagrange). Conversely, if 4 divides n, then by the previous argument H, the subgroup generated by a will have an element of order 4. Thus the required condition is that 4 divides n.

[6 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 $D(4)$, and H be the subgroup with two elements 1 and b. Since $|H| = 2$, there are four distinct left cosets and since

$$H, \quad aH = \{a, ab = ba^3\}, \quad a^2H = \{a^2, a^2b = ba^2\}, \quad a^3H = \{a^3, a^3b = ba\}$$

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

$$H, \quad Ha = \{a, ba\}, \quad Ha^2 = \{a^2, ba^2\}, \quad Ha^3 = \{a^3, ba^3\}.$$

Note that aH is not equal to Ha. We see that $\{1, a, a^2, a^3\}$ are representatives for the distinct left cosets, and that these elements form a subgroup of G (generated by a).

[6 marks]

Now let K be the subgroup with the two elements $\{1, a^2\}$. Clearly, for all g in G, $g1g^{-1} = 1$, so consider conjugates of a^2. Since a^2 commutes with both a and b, it commutes with all elements of G and so $g^{-1}a^2g = a^2$ for all g. Thus H is a normal subgroup of G. The quotient group G/K has order 4 and is not cyclic, since every coset gK has order 2. [4 marks]

If now L were a subgroup with 4 elements and two left cosets, L and a^2L, first consider the possibility that some power a^i is in L. If this power is 1 or 3, then $a^2 = a^{i^2}$ would also be in L since L is a subgroup. If this power were 0 or 2, then clearly a^2 would again be an element of L. It follows in either case that L and a^2L would not be distinct cosets (having the element a^2 in common). We conclude that L would consist of 1 together with 3 elements of the form ba^i. Since the product of any two distinct elements ba^i with ba^j is a power of a, we return to the impossible situation that a power of a is in L.

[5 marks]

5. 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]

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]

Now let G be the dihedral group $D(n)$ with $n = 2k$. Since $a^ia^j = a^{i+j} = a^ja^i$, each power of a commutes with each other power of a. Also, as given, $b^{-1}a^kb = a^{-k}$. Since $a^{2k} = 1$, $b^{-1}a^kb = a^k$, so $a^kb = ba^k$. Since a and b commute with a^k, every element of G commutes with a^k, and so $C_G(a^k) = G$ and, by our basic result, a^k only has one conjugate. In any group, 1_G only has one conjugate. All other powers of a have n elements in their centralizer (all powers of a), but b does not centralize any such power, and so a^i (for $0 < i < k$) has precisely 2 conjugates. Thus the $2k$ powers of a fall into $2 + (n-2)/2 = (n+2)/2$ conjugacy classes.

[6 marks]

Now turn to elements of the form ba^i and consider first the conjugates of b. Clearly b and a^k centralize b, so defining K to be the subgroup $\{1, b, a^k, ba^k\}$ it is clear that $K \subseteq C_G(b)$. This subgroup K has k distinct left cosets. Representatives for these are $\{1, a, a^2, \ldots a^{k-1}\}$. This is because every element of G is clearly a product of an element of K with a^i for some $0 \leq i \leq k-1$ and furthermore, any two cosets a^iK and a^jK are distinct (inspect powers of a in each). Thus b has k conjugates these being the elements

$$a^{-i}ba^i = i^{-i}a^{-i}b = a^{-2i}b = ba^{2i} \text{ for } 0 \leq i \leq k-1.$$

[6 marks]

A similar argument show that ba also has k conjugates these being ba^{2i+1} for $0 \leq i \leq k-1$. Thus elements of the form ba^i fall into 2 conjugacy classes both with k elements so G has $(n+2)/2 + 2 = (n+6)/2$ conjugacy classes in total.

[4 marks]

6. 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]

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 elements A, B in G:

$$\begin{pmatrix} a & b & c & d \\ 0 & a & b & c \\ 0 & 0 & a & b \\ 0 & 0 & 0 & a \end{pmatrix} \begin{pmatrix} r & s & t & u \\ 0 & r & s & t \\ 0 & 0 & r & s \\ 0 & 0 & 0 & r \end{pmatrix}$$

$$= \begin{pmatrix} ar & as+rb & at+bs+cr & au+bt+cs+dr \\ 0 & ar & as+rb & at+bs+cr \\ 0 & 0 & ar & as+rb \\ 0 & 0 & 0 & ar \end{pmatrix}.$$

(a) To check if θ_1 is a homomorphism (since addition is the operation in H), we need to see if $\theta_1(A)+\theta_1(B) = \theta_1(AB)$. From our formula for AB, we see that $\theta_1(AB)$ would be $as+br$. However $\theta_1(A) = b$ and $\theta_1(B) = s$, so θ_1 is not a homomorphism in general (for example if $b = s = 1$ and $a = r = 2$).

[4 marks]

(b) A similar argument for θ_2 (remembering that the target group is a group under multiplication) shows that we need to check if ar is equal to ar. This is clearly the case, so θ_2 is a homomorphism.

[2 marks]

Now compute ker θ_2. This is the set of matrices in G with $a = 1$ also im θ_2 is the whole of H.

[2 marks]

It follows by the homomorphism theorem that G has a normal subgroup ($N =$ ker θ_2) with G/N isomorphic to H. Thus G/N is abelian. Finally N is abelian because our general formula would give AB as

$$\begin{pmatrix} 1 & s+b & t+bs+c & u+bt+cs+d \\ 0 & 1 & s+b & t+bs+c \\ 0 & 0 & 1 & s+b \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

and BA as

$$\begin{pmatrix} 1 & b+s & c+sb+t & u+bt+cs+d \\ 0 & 1 & b+s & c+sb+t \\ 0 & 0 & 1 & s+b \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Since AB and BA are symmetric in their entries, N is abelian as required.
[6 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 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. If x is an element of order 3, then $\langle x \rangle$ has three elements and so is equal to P. Thus P contains all (both!) non-identity elements of G of order 3. Similarly Q contains 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 $12 = 4 \times 3$ elements. The number of Sylow 2-subgroups is either 1 or 3. The number of Sylow 3-subgroups is either 1 or 4. If the Sylow 3-subgroup is not normal, there are 4 Sylow 3-subgroups. In this case, these distinct subgroups would pairwise intersect in the identity element (if $S_1 \neq S_2$ then $S_1 \cap S_2$ would be a strict subgroup of a group with 3 elements, so would be $\{1_G\}$). This would give, in total, 8 elements of order 3, and so only leave 3 non-identity elements of G to be distributed in the Sylow 2-subgroups. Since a Sylow 2-subgroup has 3 non-identity elements, it follows that there could only be one Sylow 2-subgroup. We deduce that G either has a normal Sylow 3-subgroup or has a normal Sylow 2-subgroup. [4 marks]

Finally, if G is the alternating group on 4 symbols, G has 12 elements. These are the identity element (order 1) three elements of order 2 ((1 2)(3 4), (1 3)(2 4) and (1 4)(2 3) and eight three cycles each of order 3:

$$(1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (1\ 4\ 3).$$

Then G has Sylow 2 subgroups (with 4 elements) and Sylow 3 subgroups (with three elements). There are 8 elements of order 3 in $A(4)$, and since a Sylow 3-subgroup has three elements, these 8 elements must be distributed over 4 subgroups. The number of Sylow 2-subgroups is 1 or 3. Since there are only 3 elements of order 2 in G (and no elements of order 4), there can only be one Sylow 2-subgroup. Thus G has four Sylow 3-subgroups and 1 Sylow 2-subgroup.

[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 (unordered) set of 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 6 generated by x (so $x^6 = 1$). Then $\langle x^2 \rangle$ is a subgroup of G with 3 elments which is normal since G is abelian. It follows (since 3 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 $D(2p)$ with generators a of order $2p$ and b of order 2. Then $K = \langle a \rangle$ has $2p$ elements and is a normal subgroup of G since its index is 2. Next G (or K) has a Sylow p-subgroup with p elements and the number of these is congruent to 1 mod p and divides $4p$ (so is $1, 2, 4, p, 2p$ or $4p$). Thus this number is 1 and there is a unique Sylow p subgroup P. This subgroup P must be contained in K because K also has a Sylow p subgroup and P is unique. The required series is then

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

This is indeed a composition series for G, since we have seen that P is a normal subgroup of G, K has index 2 in G and P has index 2 in K also all the indices are prime .

[6 marks]

(c) Next, let G be a group with 21 elements. The number of Sylow 7-subgroups in G is 1 mod 7 and divides 21, so is one. Thus this subgroup S, say, is a normal subgroup of G. Because 7 is prime, S has no non-trivial proper subgroups 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.

[4 marks]

(d) Now let G be the symmetric group $S(3)$. The alternating group of even permutations has 3 elements and so has index 2 and is a normal subgroup of G (an alternative construction for this subgroup N of index 2 would be as the group generated by $(1\ 2\ 3)$). Thus a composition series is

$$G \geq N \leq \{1_G\}$$

since both the indices in this series are prime.

[3 marks]