MATH343 January 2007

Solutions

1. A *group* is a set G together with an operation $\circ$ satisfying the following axioms:

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

(G2) for any x, y, z in G, $(x \circ y) \circ z = x \circ (y \circ z)$,

(G3) there is an element e in G such that for any element g in G, $e \circ g = g \circ e = g$,

(G4) for any element g in G there is an element g^* in G with $g \circ g^* = g^* \circ g = e$.
[4 marks]

Writing the given permutation in cycle notation, it is clear that $\pi = (1324)$ and so $\pi^{-1} = (1423)$. The condition $\pi\rho = \rho\pi^{-1}$ can now be checked for each element of $\{1, 2, 3, 4\}$, so given that $\rho(1) = 1$:

$$\rho(4) = \rho(\pi^{-1}(1)) = \pi(\rho(1)) = \pi(1) = 3.$$

Similarly,

$$\rho(2) = \rho(\pi^{-1}(4)) = \pi(\rho(4)) = \pi(3) = 2$$

and

$$\rho(3) = \rho(\pi^{-1}(2)) = \pi(\rho(2)) = \pi(2) = 4.$$

It follows that

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix} = (34).$$

[5 marks]

Now let $G = \langle \pi, \rho \rangle$. Then the four powers of π are clearly in G together with their products with ρ. Thus G has at least 8 elements: identity e, $\pi = (1324)$, $\pi^2 = (12)(34)$, $\pi^3 = (1423)$, $\rho = (34)$, $\rho\pi = (14)(23)$, $\rho\pi^2 = (12)$ and $\rho\pi^3 = (13)(24)$. [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 π and ρ contains at least these 8 permutations. To establish this, we need to do something equivalent to calculating the multiplication table for the elements. To calculate the multiplication table we can use the equations $\pi^4 = e$, $\rho^2 = e$ and $\pi\rho = \rho\pi^{-1} = \rho\pi^3$. The table is

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

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.]

[6 marks]

Finally, we need to find a non-identity element of G for which the corresponding row of the table is equal to the corresponding column of the table. 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

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

using (G2), (G4) and (G3) respectively. Now the solution is unique because if x_1 and x_2 would be two solutions of the equation, then $ux_1 = ux_2 = v$. Multiplying the equation $ux_1 = ux_2$ by u^{-1} on the left gives $u^{-1}(ux_1) = u^{-1}(ux_2)$. Now using (G2), $(u^{-1}u)x_1 = (u^{-1}u)x_2$. Then using (G4), $ex_1 = ex_2$. Finally, using (G3), $x_1 = x_2$. [4 marks]

Now let G be a cyclic group of order 30 generated by an element g. The elements of G are $e, g, g^2, \ldots, g^{29}$. The equation $x^5 = e$ has 5 solutions in G, they are elements of the form g^k with k divisible by $\frac{|G|}{5} = 6$, i.e. $e, g^6, g^{12}, g^{18}, g^{24}$. The equation $x^{15} = e$ has 15 solutions in G, they are elements of the form g^k with k divisible by $\frac{|G|}{15} = 2$, i.e. g^k with even k. The equation $x^6 = e$ has 6 solutions in G, they are elements of the form g^k with k divisible by $\frac{|G|}{6} = 5$, i.e. $e, g^5, g^{10}, g^{15}, g^{20}, g^{25}$. The equations $x^{15} = e$ and $x^6 = e$ have three common solutions, they are elements of the form g^k with k divisible by $2 \times 5 = 10$, i.e. e, g^{10}, g^{20}. [4 marks]

Now let G be the dihedral group $D(10)$. We use the notation explained before question 1. The solution to $ba^8x = a^2$ is $x = (ba^8)^{-1}a^2 = a^{-8}b^{-1}a^2$. The elements a and b are of orders 10 and 2 respectively, hence $a^{-8} = a^2$ and $b^{-1} = b$, so $x = a^2ba^2$. Using $ab = ba^{-1}$ we obtain

$$x = a^2ba^2 = a(ab)a^2 = a(ba^{-1})a^2 = aba = (ab)a = (ba^{-1})a = b.$$

[3 marks]

Next consider the equation $ax = xa^{-1}$. Using $ab = ba^{-1}$ we see that the element b is a solution of this equation. There are no solutions of this equation among the powers of a because they commute with a: For $x = a^k$, $ax = a^{k+1}$, $xa^{-1} = a^{k-1}$. So we consider $x = ba$, then $ax = a(ba) = (ab)a = (ba^{-1})a = b$ and $xa^{-1} = baa^{-1} = b$, so ba is another solution. [In fact the elements ba^k for $k = 2, \ldots, 9$ are the others.] [3 marks]

Finally the equation $ux^5 = v$ is equivalent to the equation $x^5 = u^{-1}v$. To solve $x^5 = u^{-1}v$, work out g^5 for all g in G: $(a^k)^5 = a^5$ for odd k, $(a^k)^5 = e$ for even k, $(ba^k)^5 = ba^k$ for all integer k. We see that the element e has 5 fifth roots e, a^2, a^4, a^6, a^8 in G, the element a^5 has 5 fifth roots a, a^3, a^5, a^7, a^9 in G, the element ba^k with integer k has a unique fifth root ba^k in G, while the elements a^k for $k = 1, 2, 3, 4, 6, 7, 8, 9$ do not have fifth roots in G at all. So the given equation has no solutions in G if $v = ua^k$ with $k = 1, 2, 3, 4, 6, 7, 8, 9$, has five solutions in G if $v = u$ or $v = ua^5$, and has a unique solution otherwise. [It is sufficient to provide one example of u and v such that the solution of the equation $ux^5 = v$ is not unique to get the full marks.] [6 marks]

3. A *subgroup* of a group G is a non-empty subset H of G which is itself a group under the same operation as that of G. [Alternatively if H is a subset such that $e_G \in H$ and H is closed under products and inverses.] [2 marks]

Lagrange's theorem states that if H is a subgroup of a finite group G then $|H|$ divides $|G|$ and the number $|G : H|$ of distinct cosets of H in G is equal $|G|/|H|$. [2 marks]

A subgroup H of a group G is said to be *cyclic* generated by g if g is an element of H and every element of H is a power of g. [1 marks]

Let G be a group with p elements. Let x be any non-identity element of G. Using Lagrange's theorem, the order of the cyclic subgroup $\langle x \rangle$ of G is a divisor of $|G| = p$. This implies $|\langle x \rangle| = 1$ or $|\langle x \rangle| = p$, since the number p is prime. But $|\langle x \rangle| \neq 1$ by choice of x, hence $|\langle x \rangle| = p = |G|$, so $G = \langle x \rangle$ and so G is cyclic.

[4 marks]

Let H be a subgroup of G with p elements and K be a subgroup of G with q elements, where p and q are distinct prime numbers. Since $H \cap K$ is a subgroup of H and H has p elements, the number of elements in $H \cap K$ divides p. Since $H \cap K$ is a subgroup of K and K has q elements, the number of elements in $H \cap K$ divides q. Since p and q are distinct prime numbers, the only possibility is for $H \cap K$ to contain just one element, so $H \cap K = \{e\}$.

[2 marks]

The alternating group $A(4)$ contains, by definition, only even permutations on 4 symbols. There are 12 such permutations: the identity, which is of order 1, eight 3-cycles (123), (132), (124), (142), (134), (143), (234), (243), which are of order 3, and three products of a pair of disjoint 2-cycles (12)(34), (13)(24), (14)(23), all of order 2. [4 marks]

Our calculations show that each non-identity element of $A(4)$ has order 2 or 3. Thus if H is a cyclic subgroup of $A(4)$ generated by an element g, say, then g has order 1, 2, or 3, so H consists of 1, 2, or 3 elements. Thus every cyclic subgroup of $A(4)$ has order 1 or a prime order. [2 marks]

Let H and K be cyclic subgroups of $A(4)$. Let $p = |H|$ and $q = |K|$. We know that $p, q \in \{1, 2, 3\}$. Since $H \cap K$ is a subgroup of both H and K, the order $|H \cap K|$ is by Lagrange's theorem a common divisor of p and q. The integers p and q are 1 or prime. If $p \neq q$, then the only (positive) common divisor of p and q is 1, so $H \cap K = \{e\}$. If $p = q$, then there are two common divisors of p and q, they are 1 and p. Thus $|H \cap K|$ is either 1, in which case $H \cap K = \{e\}$, or p, in which case $H \cap K = H = K$. [1 marks]

Let H be a subgroup of $S(4)$ with $A(4) \subset H$. Using Lagrange's theorem, the order of the subgroup H divides $|S(4)| = 24$. On the other hand, $|H| \geq |A(4)| = 12$ since $A(4) \subset H$. There are only two divisors of 24 larger than 12, they are 12 and 24 and correspond to $H = A(4)$ and $H = S(4)$.

[2 marks]

4. Suppose first that $aH = bH$. Then, since $e \in H$, $a = ae \in aH = bH$. Since $a \in bH$, there is an element $h \in H$ such that $a = bh$. Then $a^{-1}b = h^{-1} \in H$. Conversely, if $a^{-1}b$ is in H and ah_1 with $h_1 \in H$ is in aH, then $ah_1 = b(b^{-1}ah_1) = b((a^{-1}b)^{-1}h_1) = bh_2$ with $h_2 = (a^{-1}b)^{-1}h_1 \in H$, so each element ah_1 of aH is in bH, so $aH \subset bH$. On the other hand, if bh_1 with $h_1 \in H$ is in bH, then $bh_1 = a(a^{-1}bh_1) = a((a^{-1}b)h_1) = ah_2$ with $h_2 = (a^{-1}b)h_1 \in H$, so each element bh_1 of bH is in aH, so $bH \subset aH$. We deduce that $aH = bH$.

[5 marks]

A subgroup N is a normal subgroup of G if $gN = Ng$ for all g in G. [Any other correct definition of a normal subgroup will attract full marks, for example: A subgroup N is a normal subgroup of G if gng^{-1} is an element of N for any n in N and g in G.]

[1 marks]

Now let G be the dihedral group $D(10)$. The set $H = \{e, a^2, a^4, a^6, a^8\}$ is a subgroup of G because it is the subgroup generated by a^2. [Alternatively, one could construct the multiplication table for H.] [1 marks]

The distinct left cosets of H in G are:

$$H = eH = \{e, a^2, a^4, a^6, a^8\}, \quad aH = \{a, a^3, a^5, a^7, a^9\},$$
$$bH = \{b, ba^2, ba^4, ba^6, ba^8\}, \quad baH = \{ba, ba^3, ba^5, ba^7, ba^9\}.$$

[4 marks]

The right cosets of H in G are:

$$He = H = eH, \quad Ha = aH, \quad Hb, \quad Hba.$$

Since $ab = ba^9$, an easy check shows that

$$Hb = bH \quad \text{and} \quad Hba = baH.$$

[2 marks]

Every left coset of H in G is a right coset of H in G, so H is a normal subgroup of G. [1 marks]

The elements of G/H are the four cosets $\{H, aH, bH, abH\}$. Now

$$H^2 = HH = H, \quad (aH)^2 = aHaH = a^2H = H,$$
$$(bH)^2 = bHbH = b^2H = H, \quad (baH)^2 = baHbaH = (ba)^2H = eH = H.$$

Since every non-identity element of G/H has order 2, the group G/H is not cyclic. [3 marks]

Finally, as all non-identity elements of the group G/H are of order 2, we have $(gH)^2 = H$ for any element g of G, hence $g^2H = (gH)^2 = H$, so g^2 is an element of H. [3 marks]

5. Let f be a map between the groups $(G, \circ)$ and $(H, *)$. Then f is a *homomorphism* if for all a, b in G, $f(a \circ b) = f(a) * f(b)$. [1 marks]

The *kernel* of f is $\ker(f) = \{g \in G \mid f(g) = e_H\}$ [1 marks]

and the *image* of f is

$$\text{im}(f) = \{h \in H \mid h = f(g) \text{ for some } g \in G\}.$$

[1 marks]

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

- $\text{im}f$ is a subgroup of H,
- $\ker f$ is a normal subgroup of G,
- $G/\ker f \cong \text{im}f$. [3 marks]

Let G be the set of invertible 2×2 matrices of the form

$$A = \begin{pmatrix} a & b \\ b & a \end{pmatrix},$$

where a and b are real numbers. Before checking for the homomorphism property, it might be convenient to obtain the formula for the product of two elements in G:

$$\text{For} \quad A = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \quad \text{and} \quad B = \begin{pmatrix} r & s \\ s & r \end{pmatrix}:$$

$$AB = \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} r & s \\ s & r \end{pmatrix} = \begin{pmatrix} ar+bs & as+br \\ as+br & ar+bs \end{pmatrix}.$$

(1) Let H be the group of all real numbers under addition and f be given by $f(A) = a$. To check if f is a homomorphism, we need to see if $f(AB) = f(A) + f(B)$ since the operation in H is addition. From our formula for AB, we see that $f(AB) = ar + bs$. However $f(A) = a$ and $f(B) = r$, so $f(A) + f(B) = a + r$, i.e. $f(AB) \neq f(A) + f(B)$ in general (for example if $a = r = 2$ and $b = s = 1$). Thus f is **not a homomorphism.** [4 marks]

(2) Let H be the group of non-zero real numbers under multiplication and h be given by $h(A) = a^2 - b^2$. To check if h is a homomorphism, we need to see if $h(AB) = h(A)h(B)$ since the operation in H is multiplication. From our formula for AB, we see that

$$h(AB) = (ar+bs)^2 - (as+br)^2 = (a^2r^2 + b^2s^2 + 2abrs) - (a^2s^2 + b^2r^2 + 2abrs),$$

hence

$$h(AB) = a^2r^2 + b^2s^2 - a^2s^2 - b^2r^2.$$

On the other hand, $h(A) = a^2 - b^2$ and $h(B) = r^2 - s^2$, so

$$h(A)h(B) = (a^2 - b^2)(r^2 - s^2) = a^2r^2 - a^2s^2 - b^2r^2 + b^2s^2 = h(A)h(B).$$

[Alternatively, notice that $h(A) = \det(A)$ and use $\det(AB) = \det(A)\det(B)$.]
Thus h is **a homomorphism.** [5 marks]

The kernel $\ker(h)$ of h is

$$\left\{ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \in G \mid a^2 - b^2 = 1 \right\}.$$

The image $\mathrm{im}(h)$ is the whole of H. [3 marks]

It follows by the homomorphism theorem that G has a normal subgroup $N = \ker(h)$ with G/N isomorphic to $\ker(h) = H$. The group G/N is abelian since the group H is abelian. [2 marks]

6. If a permutation 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 lengths of disjoint cycles of π. [1 marks]

In disjoint cycle notation, the given permutations are written as

$$\pi = (12)(34)(56)(78)(9\ 10) \quad \text{and} \quad \rho = (1\ 10)(24689753).$$

The permutation π is a product of five odd cycles, hence $\mathrm{sign}(\pi) = (-1)^5 = -1$, so π is odd, and π has order 2. The permutation ρ is a product of two odd cycles, hence $\mathrm{sign}(\rho) = (-1)^2 = 1$, so ρ is even, and ρ has order 8. [4 marks]

The identity permutation is even (as a product of disjoint 1-cycles). If permutations π and ρ are even, then their product $\pi\rho$ is even. If a permutation π is even, then π^{-1} is also even, since π^{-1} has the same set of lengths of disjoint cycles. Thus the alternating group $A(n)$ is a subgroup of $S(n)$. It is a subgroup of index 2, hence normal. [4 marks]

The identity permutation is not odd. The set of odd permutations is also not closed because the product of two odd permutations is even. [1 marks]

Now suppose that a permutation π has odd order k. If π were odd, $\mathrm{sign}(\pi^k) = (\mathrm{sign}(\pi))^k = (-1)^k$ would be -1. But $\pi^k = e$, hence $\mathrm{sign}(\pi^k) = \mathrm{sign}(e) = 1$, so this contradiction shows that π is even. [4 marks]

An example of an even permutation of order 2 is $(12)(34)$. An example of an even permutation of order 3 is (123). [2 marks]

If π is any element of $S(n)$, then $\mathrm{sign}(\pi^2) = (\mathrm{sign}(\pi))^2 = 1$, so π^2 is even.

[2 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

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

(b) the number of these is congruent to 1 mod p.

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

(d) 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 be equal to P. [2 marks]

(1) Suppose that G is a group with $35 = 5 \times 7$ elements. The number of Sylow 5-subgroups is 1 mod 5 and divides 35, so is one. The number of Sylow 7-subgroups is 1 mod 7 and divides 35, so is also one. Thus G has a unique Sylow 5-subgroup, say P, and a unique Sylow 7-subgroup, say Q, and the subgroups P and Q are both normal in G. The subgroup P contains all 4 non-identity elements of G of order 5. The subgroup Q contains all 6 non-identity elements of G of order 7. The only other divisor of 35 is 35. It follows by Lagrange that there must be an element of G of order 35, so G is cyclic. [4 marks]

(2) The group G has $56 = 2^3 \times 7$ elements, so has Sylow 2-subgroups (of order 8) and Sylow 7-subgroups (of order 7). The number of Sylow 2-subgroups is odd and divides 56, so is either 1 or 7. The number of Sylow 7-subgroups is 1 mod 7 and divides 56, so is either 1 or 8. Let us assume that there are 8 (not-normal) Sylow 7-subgroups. If P and Q are distinct Sylow 7-subgroups, the number of elements in their intersection is smaller than 7, but this number divides $|P| = |Q| = 7$ by Lagrange's theorem, hence $P \cap Q = \{e\}$ for any two distinct Sylow 7-subgroups of G. Thus the total number of non-identity elements in the union of those 8 Sylow 7-subgroups is $8 \times 6 = 48$. Hence there are no more than $56 - 48 - 1 = 7$ non-identity elements in the union of all Sylow 2-subgroups of G. Since any Sylow 2-subgroup of G has 8 elements (and 7 non-identity elements), it follows that there can be only one Sylow 2-subgroup. We deduce that G has either a normal Sylow 7-subgroup or a normal Sylow 2-subgroup. [5 marks]

(3) Finally suppose that G is the symmetric group $S(4)$ of permutations on 4 symbols. The group G has $24 = 2^3 \times 3$ elements, so has Sylow 2-subgroups

(of order 8) and Sylow 3-subgroups (of order 3). The number of Sylow 3-subgroups is 1 mod 3 and divides 24, so is either 1 or 4. There are 8 elements of order 3 in G (cycles of length 3), and since a Sylow 3-subgroup of G has 3 elements, these 8 elements of order 3 must be distributed over 4 subgroups. The number of Sylow 2-subgroups is odd and divides 24, so is either 1 or 3. Any element of order 2 generates a cyclic subgroup of order 2. Any subgroup of order 2 is contained in a Sylow 2-subgroup. Thus any element of order 2 is contained in a Sylow 2-subgroup. There are 9 elements of order 2 in G (6 transpositions and 3 products of two disjoint transpositions), and since a Sylow 2-subgroup of G has 8 elements, these 9 elements of order 2 must be distributed over 3 subgroups. Thus the group $G = S(4)$ has 4 Sylow 3-subgroups and 3 Sylow 2-subgroups. [5 marks]

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

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

$$G = G_0 > G_1 > \cdots > G_k = \{e\},$$

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

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 marks]

If H/K has prime number of elements p, a normal subgroup L of H with $K < L < H$ would give rise to a normal subgroup of H/K. Since H/K has prime number of elements, L is either H or K. [3 marks]

(1) Let G be a cyclic group with 4 elements generated by an element x (of order 4). Then $\langle x^2 \rangle$ is a subgroup of G. The subgroup $\langle x^2 \rangle$ is normal since G is abelian. It follows (since 2 is prime) that a composition series for G is

$$G > \langle x^2 \rangle > \{e\}.$$

[2 marks]

(2) Now let G be a non-cyclic group with 4 elements and let y be a non-identity element of G (of order 2). Then $\langle y \rangle$ is a subgroup of G. The subgroup $\langle y \rangle$ is normal since G has index 2. It follows (since 2 is prime) that a composition series for G is

$$G > \langle y \rangle > \{e\}.$$

[2 marks]

(3) Next, let G be a group with 21 elements. The number of Sylow 7-subgroups of G is 1 mod 7 and divides 21, so is one. Thus this Sylow 7-subgroup S, say, is a normal subgroup of G. Because 7 is prime, S has no non-trivial proper subgroups. Since S has index 3 in G, no subgroup of G lies between G and S, so the series

$$G > S > \{e\}$$

is a composition series. [4 marks]

(4) Now let G be the symmetric group $S(3)$. The alternating group $A(3)$ of even permutations has 3 elements and so has index 2 in G and is a normal subgroup of G. Because 3 is prime, $A(3)$ has no non-trivial proper subgroups. Since $A(3)$ has index 2 in G, no subgroup of G lies between G and $A(3)$, so the series

$$S(3) > A(3) > \{e\}$$

is a composition series. [3 marks]

(5) We finally turn to the dihedral group $D(6)$. We use the notation explained before question 1. The subgroup $\langle a \rangle$ is cyclic of order 6. This subgroup is normal because it is of index 2. Also $\langle a^2 \rangle$ is a subgroup of $\langle a \rangle$. The subgroup $\langle a^2 \rangle$ is normal in $\langle a \rangle$ because $\langle a \rangle$ is abelian, so

$$G > \langle a \rangle > \langle a^2 \rangle > \{e\}$$

is a composition series. This series can not be refined because the factors are of prime order. [3 marks]