Math 343 2001 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]

Before computing the inverse of A, we note that

$$\begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ d & 1 & 0 \\ e & f & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ d+a & 1 & 0 \\ dc+b+e & c+f & 1 \end{pmatrix}.$$

If the product of these two matrices is to be I, it follows that: $a + d = 0$ so $d = -a$, $c + f = 0$, so $f = -c$ and $dc + b + e = 0$ so that $e = -b + ac$.

[3 marks]

To show that G is a group, closure follows by the above multiplication rule. We are given associativity. The identity is I, and we have just found the inverse to be of the required form.

[3 marks]

If A were an element of order 2 then, since $A^2 = I$,

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b & c & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ 2a & 1 & 0 \\ 2b+a^2 & 2c & 1 \end{pmatrix}.$$

It would follow that $a = c = 0$ and so b would also be zero, so G has no elements of order 2.

[3 marks]

To find the order of Z, first note that

$$Z^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2 & 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 4 & 0 & 1 \end{pmatrix}$$

and so (by induction)

$$Z^n = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 2n & 0 & 1 \end{pmatrix}.$$

It follows that Z has infinite order.

[3 marks]

For a general element A in G, we see that

$$AZ = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b+2 & c & 1 \end{pmatrix},$$

whereas

$$ZA = \begin{pmatrix} 1 & 0 & 0 \\ a & 1 & 0 \\ b+2 & c & 1 \end{pmatrix}$$

so $AZ = ZA$.

[2 marks]

Finally, to find two elements of G which do not commute, we take our basic multiplication formula, and note that the entry in the third row of column 1 for AB would be $dc+b+e$, and the the corresponding entry in BA would be $af+e+b$. Clearly these are not equal in general, and a specific example of non-commuting elements may be found when $a = f = d = 1$ and $c = 0$.

[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 $bax = a^2$ is

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

[3 marks]

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

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

using the basic relations the other four elements all gave order 2. (A sample justification is

$$(ba)^2 = baba = bba^{-1}a = b^2.1 = 1).$$

[4 marks]

If $bax^2 = a$ had a solution, we could find an x such that $x^2 = ba^3$ (using the above), but we have just seen that no element of G squares to give ba^3.

[2 marks]

Finally to solve $ux^3 = v$, work out the cubes of elements of G to get $1, a^3, a^2, a$ and b, ba, ba^2, ba^3 (elements in"standard order") We see that every element has a unique cube root, so the given equation has a unique solution.

[5 marks]

3. Suppose first that $xH = yH$. Then, since $1 \in H$, $x.1 = x \in yH$. 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 $xH = yH$.

[5 marks]

Now let G be the dihedral group $D(6)$, and H be the subgroup with two elements 1 and x^3. Since $|H| = 2$, there are six distinct left cosets and since

$$\begin{aligned} H, \quad xH &= \{x, x^3\}, \quad x^2H = \{x^2, x^5\}, \\ yH = \{y, yx^3\}, \quad yxH &= \{yx, yx^4\}, \quad yx^2 = \{yx^2, yx^5\} \end{aligned}$$

this is the complete list of (left) cosets. The first three are clearly right cosets, and since x^3 commutes with y, $yH = Hy$, $Hyx = \{yx, yx^4\} = yxH$

and $Hyx^2 = yx^2H$. Since every left coset is a right coset, H is a normal subgroup of G.

[5 marks]

The quotient group G/H has order 6 and $yHxH = yxH = \{yx, yx^4\}$, whereas $xHyH = xyH = yx^{-1}H = \{yx^5, yx^2\}$ so G/H is non-abelian and so non-cyclic.

[4 marks]

For the final part, take (for example) $K = \{1, y\}$, so that $xK = \{x, xy\} = \{x, yx^5\}$, but $Kx = \{x, yx\}$, so left and right cosets are different, and K is not normal.

[6 marks]

4. 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]

To check if θ is a homomorphism, note that G is a group under matrix multiplication, and consider

$$a_1 b_1 = \theta(\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix})\ \ \theta(\begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix})$$

whereas

$$AB = \begin{pmatrix} a_1b_1 & a_1b_2 + a_2b_3 \\ 0 & a_3b_3 \end{pmatrix}.$$

Thus $\theta(AB) = a_1b_1$ so θ is a homomorphism from G to the (multiplicative) group of non-zero real numbers. The image of θ is clearly the whole set (θ is surjective) and the kernel, N, of θ are those matrices in G with $a_1 = 1$.

[4 marks]

As for ϕ

$$a_2b_2 = \phi(\begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix}) \;\; \phi(\begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix})$$

and $\phi(AB) = a_1b_2 + a_2b_3$, so ϕ is not a homomorphism.

[2 marks]

It follows by the homomorphism theorem that G/N is isomorphic to im ϑ and so is abelian.

[2 marks]

To find the subgroup K of N, we define a map λ on N by:

$$\lambda(\begin{pmatrix} 1 & a_2 \\ 0 & a_3 \end{pmatrix}) = a_3.$$

This is easily checked to be a homomorpism with kernel K consisting of those elements of N with $a_3 = 1$, and image the non-zero real numbers. It then follows that K is abelian, as is K/N.

[4 marks]

5. 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 an element x of order d, consider the powers

$$H = \{1, x, x^2, \ldots, x^{d-1}\}.$$

This is a subgroup of G: it contains 1_G (which is its own inverse). The inverse of x^i (for $1 \le i \le d-1$) is x^{d-i}, an element of H. For products $x^ix^j = x^{i+j}$ an element of H unless $i + j > d - 1$ in which case $i + j = d + k$ with $0 \le k \le d - 1$ when $x^{d+k} = x^dx^k = 1.x^k \in H$.

[3 marks]

The elements in $A(4)$ are 1 (of order 1) $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$ (all of order 2) and eight elements of order 3 :

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

so that $|A(4)| = 12$.

[3 marks]

We see that $A(4)$ has no element of order 6 even though 6 divides 12.

[3 marks]

Next we note that $A(4)$ has a subgroup with 4 elements consisting of $\{1, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ (justify this in some way e.g. produce the table) . This subgroup is not cyclic because every non-trivial element has order 2.

[5 marks]

Finally an example of a non-cyclic group with each subgroup cyclic is $S(3)$. This group is non-abelian since $(1\ 2)(2\ 3) \neq (2\ 3)(1\ 2)$, and so non-cyclic. Any proper subgroup of $S(3)$ has prime order so is cyclic by Lagrange.

[4 marks]

6. A set X is a G-set if there is an action $\circ : G \times X \to X$ such that:

$1_G \circ x = x$ for all $x \in X$, and

$gh \circ x = g \circ (h \circ x)$ for all $g, h \in G$ and all $x \in X$.

[2 marks]

The stabilizer G_x of $x \in X$ is

$$G_x = \{g \in G : g \circ x = x\}.$$

[1 mark]

The orbit O_x is

$$O_x = \{y : y = g \circ x \text{ for some } g \in G\}.$$

[1 mark]

The orbit-stabilizer theorem says

G_x is a subgroup of G.

If G is finite, then $|O_x| = |G : G_x|$.

[2 marks]

Now consider the set of subgroups of G. If H is in this set, $1_g \circ H = 1_g H 1_G{}^{-1} = H$ and if x, y are in G, then $xyH(xy)^{-1} = xyHy^{-1}x^{-1} = x(y \circ H)x^{-1} = x \circ (y \circ H)$ as required.

[2 marks]

The orbit of H is the set of subgroups of the form xHx^{-1} as x varies over G and the stabilizer of H is the set of those g for which $gHg^{-1} = H$.

[2 marks]

(a) H is a subgroup of index 2 in G so is normal and $G = N_G(H)$.

[2 marks]

(b) When $H = \langle y \rangle$, we see that H is contained in the abelian subgroup $K = \langle y, x^2 \rangle$ of order 4, so $N_G(H) \subseteq K$. However, H is not normal in G since $xHx^{-1} = \{1, yx\}$, so K is the required normalizer [5 marks]

(c) For $G = S(3)$, G has six elements so $|N_G(H)|$ divides 6 (by Lagange) and is divisible by 2 so is 2 or 6. But H is not normal, so we conclude that $H = N_G(H)$.

[3 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 $\times$ 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 $56{=}8 \times 7$ 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. These distinct subgroups would all intersect in the identity element, giving in total 48 elements of order 7, 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 $G = 30$ the number of Sylow 5-subgroups is 1 or 6. If this number is 1, there is an element of order 5 which generates a normal subgroup N and G/N has order 6. Then G/N would have a Sylow 3-subgroup H/N and H would be a subgroup of G with 15 elements. If the number of Sylow 5-subgroups is 6, there are 25 elements of order 5, so there is only room for one Sylow 3-subgroup K, say. Since $K$is unique it is normal and G/K has order 10. Thus G/K would have a Sylow 5-subgroup L/K giving a subgroup L of order 15. In either case, G has a subgroup of order 15, which is cyclic by part (a). Thus G has an element of order 15.

[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 of order 4 generated by x (so $x^4 = 1$). Then $\langle x^2 \rangle$ is a subgroup of G which is normal since G is abelian. It follows (since 2 is prime) that a composition series for G is

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

[2 marks]

(b) Now let G be a non-cyclic of order 4 and let y be a non-identity element of G (so that $y^2 = 1$). Apply the same argument as in (1) with $\langle y \rangle$ replacing $\langle x^2 \rangle$, to obtain the composition series

$$G \geq \langle y \rangle \geq \{1\}.$$

($\langle y \rangle$ is normal since it has index 2).

[2 marks]

(c) Next, let G be cyclic of order 15 (so it is generated by x with $x^{15} = 1$). Consider the subgroup $\langle x^3 \rangle$ of order 5. It is normal because G is abelian. The series

$$G \geq \langle x^3 \rangle \geq \{1\}$$

cannot be refined because 3 and 5 are primes, so it is a composition series.

[3 marks]

(d) Now let G be the alternating group $A(4)$. The four elements

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

form a subgroup V which is normal since the three non-idenitity elements form a conjugacy class. So we have a series for G

$$A(4) \geq V \geq \{1\}$$

since $A(4)/V$ has order 3 this bit cannot be refined, so we are left with the problem of whether V has a better composition series. This is solved in (b), so a composition series for G is (all indices prime)

$$G \geq A(4) \geq V \geq \{1, (1\ 2)(3\ 4)\} \geq \{1\}.$$

[4 marks])

(e) We finally turn to the dihedral group $D(10)$. The subgroup $\langle x \rangle$ is cyclic of order 10 and is normal because it is of index 2. Also $\langle x^2 \rangle$ is a subgroup of this and is normal because $\langle x \rangle$ is abelian, so a composition series is

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

This cannot be refined because the factors are of prime order.

[3 marks]