Math 343 2002 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]

The reason why X is not a group is that not every element of X has a multiplicative inverse, because we did not insist that every element has non-zero determinant, (the condition for a matrix to have an inverse).

[2 marks]

To show that G is a group, first note that

$$\begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & ay + bz \\ 0 & cz \end{pmatrix}.$$

If the product of these two matrices is I then $ax = 1$ (so $x = a^{-1}$, and a must be non-zero), also $cz = 1$ (so $z = c^{-1}$, and c must be non-zero). Finally, $ay + bz = 0$, so that $y = -bz/c$. Now closure follows from the above product rule, we are allowed to assume associativity, the identity is I and we have just checked that the inverse of an element of G is another element of G.

[4 marks]

If A were an element of order 2, then

$$A^2 = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}^2 = \begin{pmatrix} a^2 & ab + bc \\ 0 & c^2 \end{pmatrix} = I.$$

It would then follow that $a^2 = c^2 = 1$, so that a and c are each ± 1. If a and c are equal, b must be zero and the only element of order 2 arising in this way is $-I$. If however $a = -c$ then each such matrix has order 2 irrespective of the value of b. [4 marks]

An example of an element of infinite order in G is the matrix $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, since C^n is the matrix $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ So, to write C in the form AB where A, B each have order 2, use the product rule to consider the product of two matrices

$$A = \begin{pmatrix} 1 & b \\ 0 & -1 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & d \\ 0 & -1 \end{pmatrix},$$

then C will equal AB provided that $d - b = 1$ or $d = 1 + b$. [4 marks]

Finally, to find two elements to establish that G is non-abelian, we can use our basic multiplication formula, and a little experimentation produces many examples such as $c = 2$, $z = 3$ and each of a, b, x, y are equal to 1. Thus G is non-abelian. [2 marks]

2. A subgroup of a group G is a non-empty subset H of G which is itself a group under the same law of composition as that of G. [Alternatively if H is a subset such that $1_G \in H$ and H is closed under products and inverses.] [2 marks]

Lagrange's Theorem states that if $|G|$ is a group of finite order and H is a subgroup of G, then the number of distinct right (or left) cosets of H in G is $|G|/|H|$. In particular then $|H|$ divides $|G|$. [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. [3 marks]

The subsets $H \cap K$ contains 1_G since 1_G is in both H and K. Also products and inverses of elements in $H \cap K$ are in each of H and K (since both are subgroups). Finally, $H \cap K$ is a subset of H so is a subgroup of H and $H \cap K$ is a subset of H so is also a subgroup of K . [3 marks]

If H has p elements and K has q elements, then since $H \cap K$ is a subgroup of H, the number of elements in $H \cap K$ divides p and since $H \cap K$ is a subgroup of K this number of elements divides q. Since p and q are distinct prime numbers, the only possibility is for $H \cap K$ to contain just one element, so $H \cap K = \{1\}$. [3 marks]

When $|H| = p = |K|$, the number of elements in $H \cap K$ divides p so is 1 or p. If this number were p, then $H \cap K = H$ and $H \cap K = K$ so $H = K$ and H, K are not distinct. [3 marks]

Finally, if G is the dihedral group of order 10, and H is a strict subgroup of G, the number of elements in H is 1,2 or 5. It follows from the above :

if either H or K is $\{1\}$, then so is $H \cap K$,

if neither is trivial then each has prime order and so the intersection is trivial unless $H = K$. [4 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 $xH = yH$. [5 marks]

Now let G be the dihedral group $D(6)$ and H be the set with three elements 1, x^2 and x^4. The best way to check that H is a subgroup is to produce the 3×3 multiplication table:

	1	x^2	x^4
1	1	x^2	x^4
x^2	x^2	x^4	1
x^4	x^4	1	x^2

[2 marks]

Since $|H| = 3$, there are four distinct left cosets. However

$$H, \quad xH = \{1, x^2, x^4\}, \quad yH = \{y, yx^2, yx^4\} \text{ and } yxH = \{yx, yx^3, yx^5\},$$

so this is the complete list of left cosets The first two are clearly right cosets. Since $yx^2 = x^4y$ we see that $yH = \{y, yx^2, yx^4\} = Hy$. Also we have that $Hyx = \{yx, yx^2, yx^5\} = yxH$. Since every left coset is a right coset, H is a normal subgroup of G. [5 marks]

The quotient group G/H has the four elements H, xH, yH and yxH. However $xHxH = x^2H = H$ and $yHyH = y^2H = H$, so two of these four elements have order 2, so G/H cannot be cyclic. [3 marks]

For the final part, take A to be the subset $\{1, x^2, x^4, y, yx^2, yx^4\}$. Since

$$y^{-1}x^2y = y^{-1}xxy = y^{-1}xyy^{-1}xy = x^{-1}x^{-1} = x^{-2}$$

and also x^2 has order 3 while y has order 2, A is (isomorphic to) the dihedral group with six elements, and A has index 2 and so is normal. Now let B

be the subgroup $\{1, x^3\}$. Since x^3 is a central element, B is normal. Then $A \cap B = \{1\}$ (since x^3 is not in A), but every element of G may be written as a product of an element of A with an element of B. We show this for the six elements of G outside A:

$$x = x^4x^3; \quad x^3 = x^3; \quad x^5 = x^2x^3; yx = (yx^4)x^3; \quad yx^3 = (y)x^3; \quad yx^5 = (yx^2)x^3.$$

[5 marks].

4. Let $\vartheta : (G, \circ) \to (H, *)$ be a group homomorphism. Then for all x, y in G, $\vartheta(x \circ y) = \vartheta(x) * \vartheta(y)$. [1 mark]

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

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

We have

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

[1 mark]

and

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

[1 mark]

The homomorphism theorem states that if f is a homomorphism between groups G and H then

(a) im f is a subgoup of H,

(b) ker f is a normal subgoup of G, and

(c) $G/\ker f$ is isomorphic to im f. [3 marks]

(a) Now $\theta_1(XY) = (ac - bd)(ab + bc)$ but this is not equal to $a+b+c+d$ (as an example, if $b = 0$ but $a = c = d = 1$ we see that $0 \neq 1$). Thus θ_1 is not a homomorphism. [2 marks]

(b) In this case

$$\theta_2(XY) = (ac - bd)^2 + (ad + bc)^2.$$

This simpifies to $a^2c^2 - 4abcd + b^2d^2 + a^2d^2 + 4abcd + b^2c^2$, which is equal to $(a^2 + b^2)(c^2 + d^2)$, so θ_2 is a homomorphism. Its kernel is the set of elements of G with $a^2 + b^2 = 1$ and its image is the set of positive real numbers.

[5 marks]

(c) Finally

$$\theta_3(XY) = (ac - bd) + i(ad + bc) = (a + ib)(c + id)$$

so θ_3 is a homomorphism. Its kernel is 1 and image is the whole of the set of non-zero complex numbers. [5 marks]

5. The sign of the identity permutation is even. The sign of an l-cycle is odd if the length of l is an even integer and its sign is even if the length of l is an odd integer. The sign of a composite of two permutations is the product of the signs. [2 marks]

In disjoint cycle notation, the given permutations are $(1\ 8)(2\ 7)(3\ 6)(4\ 5)$ and $(1\ 2\ 4\ 8\ 7\ 5)(3\ 6)$. The first of these is a product of four odd cycles, so will be even. The second is a product of a cycle of length 6 (odd permutation) with a cycle of length 2 (odd permutation) so is also an even permutation. [2 marks]

Since the product of two even permutations is even, the identity is even and the inverse of a permutation π has the same sign as π, $A(n)$ is a subgroup. It is normal since if π is even and α is any permutation then the sign of $\alpha^{-1}\pi\alpha$ is 1, so $A(n)$ is normal. [4 marks]

If π is any permutation, then

$$\text{sign}(\pi^2) = \text{sign}(\pi\pi) = (\text{sign}(\pi))^2 = 1.$$

[2 marks]

An example of an even permutation of order 2 is $(1\ 2)(3\ 4)$. [2 marks]

Now let π be a permutation of odd order. If π were odd and π had odd order k, then

$$1 = \text{sign}(1) = \text{sign}(g^k) = \text{sign}(g)^k = (-1)^k = -1.$$

This contradiction shows that π must be an even permutation. [5 marks]

If we could write any cycle as a product of 3-cycles, the cycle would be even (since a 3-cycle is even). Since there are odd cycles, this is impossible. [3 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 $gx^{-1} = x^{-1}g$ so $x^{-1} \in C_G(g)$. Thus $C_G(g)$ is a subgroup of G. [3 marks]

Now supose that $x^{-1}gx = y^{-1}gy$. After rearranging this expression, we see that $(xy^{-1})^{-1}g(xy^{-1}) = g$ so that $xy^{-1} \in C_G(g)$ and so the right cosets $C_G(g)x$ and $C_G(g)y$ are equal. Now let $C_G(g)x_1, \ldots, C_G(g)x_r$ be the complete list of distinct right cosets of $C_G(g)$ in G. This means that each element of G is in one of this list of cosets, and there are no repetitions in this list. This has the consequence that $x_i{x_j}^{-1}$ is not an element of $C_G(g)$ unless $i = j$ and so the conjugates $x_1^{-1}gx_1, \ldots, x_r^{-1}gx_r$ are all distinct. If x is any element of G, then x is in $C_G(g)x_i$ for some i, so $x = cx_i$ with $c \in C_G(g)$. Then

$$x^{-1}gx = (cx_i)^{-1}gcx_i = x_i^{-1}(c^{-1}gc)x_i = x_i^{-1}gx_i$$

so each conjugate of g is equal to one of the r conjugates $x_i^{-1}gx_i$. This shows that g has precisely r conjugates where $r = |G : C_G(g)|$. [4 marks]

For the group $D(4) = \langle a, b : a^4 = 1 = b^2, b^{-1}ab = a^{-1}\rangle$, the identity element commutes with every element of G, so $C_G(1) = G$, and the only conjugate of 1 is 1 itself. Since $b^{-1}ab = a^{-1}$, it follows that

$$b^{-1}a^2b = b^{-1}aab = b^{-1}abb^{-1}ab = a^{-2}.$$

Since $a^4 = 1$, $a^2 = a^{-2}$, so a^2 is centralized by a and by b. It follows that $G = C_G(a^2)$ and the only conjugate of a^2 is itself. Clearly a is conjugate to a^{-1}, and since $C_G(a)$ includes the four powers of a, there are no more conjugates of a. We have determined all the conjugacy classes inside $\langle a\rangle$ Next note that $1, b, a^2$ and therefore ba^2 all lie in $C_G(b)$ so b has at most 2 conjugates. However $a^{-1}ba = a^{-1}a^{-1}b = a^2b = ba^2$, so b has precisely two conjugates. Finally since the conjugate of ba by a is ba^3, and $1, ba, a^2, ba^3$ all commute with ba, this element also has two conjugates The complete list of conjugates in $D(4)$ is therefore

$$\{1\}, \quad \{a^2\}, \quad \{a, a^3\}, \quad \{b, ba^2\}, \quad \{ba, ba^3\}.$$

[5 marks]

For the group $D(5) = \langle a, b : a^5 1 = b^2, b^{-1}ab = a^{-1}\rangle$, the identity element is again in a conjugacy class on its own. Clearly a is conjugate to a^{-1} and a has the powers of a in its centralizer, so a has precisely two conjugates. Similarly, a^2 is conjugate to $a^{-2} = a^3$, and commutes with all powers of a, so a^2 has precisely two conjugates. We turn to the five elements containing b. Since no power of a commutes with b, it is clear that $C_G(b)$ consists of $\{1, b\}$, so b has five conjugates. The complete list of conjugates in $D(5)$ is therefore

$$\{1\}, \quad \{a, a^4\}, \quad \{a^2, a^3\}, \quad \{b, ba, ba^2, ba^3, ba^4\}.$$

[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]

Suppose that G is a group of order $35 = 5 \times 7$ the number of Sylow 5-subgroups is $1, 6, 11, 16, , \ldots$ and divides 35, so is 1. The number of Sylow 7 subgroups is $1, 8, 15, 22, \ldots$ and divides 35 so is also 1. Thus G has a unique Sylow 5-subgroup, P, say, and a unique Sylow 7-subgroup Q, say. These are each normal with P containing all 4 non-identity elements of G of order 5 and Q containing all 6 non-identity elements of G of order 7. It follows by Lagrange that there must be elements of G of order 35 (the only other divisor of 35), so G is cyclic. [5 marks]

This argument does not show that a group with 14 elements is cyclic, because a group with 14 elements is allowed to have 7 Sylow 2-subgoups.

[2 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. These distinct subgroups would all intersect in the identity element, giving in total 8 elements of order 3, and only leaving 3 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]

To show that $b^{-1}ab = a^{-i}$ by induction, first note that the case $i = 1$ is given for all dihedral groups. Then

$$b^{-1}a^{i+1}b = b^{-1}a^{i}ab = b^{-1}a^{i}bb^{-1}ab = a^{-i}a = a^{-(i+1)}$$

as required. [1 mark]

When $G = D(p)$ with $2p$ elements, the primes dividing $|G|$ are 2 and p. By standard Sylow theory G has one Sylow p-subgroup and the number of Sylow 2-subgroups (each with 2 elements) is 1 or p. However, each element of the form ba^i has order 2 since

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

This means that there are exactly p subgroups with 2 elements, so G has p Sylow 2-subgroups. [4 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]

(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 which is normal since G is abelian. It follows (since 2 and 3 are primes) 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 a group with 21 elements. By Sylow theory, the number of Sylow 7-subgroups is 1 mod 7 and divides 21, so is 1 and G so has a unique Sylow 7-subgroup P which is therefore normal. Then the series $G \geq P \geq \{1\}$ is a series of normal subgroups of G which cannot be refined because 3 and 7 are primes, so is a composition series. [5 marks]

(d) Now let G be the symmetric group $S(4)$. The four elements

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

form a subgroup V which is normal since the three non-identity elements form a conjugacy class. Also the alternating group $A(4)$ has index 2 so is normal. So we have a series for G

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

since $S(4)/A(4)$ has order 2 and $A(4)/V$ has order 3 these bits 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 is

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

[6 marks]

An example of a group with two composition series is provided by almost all of the above examples. For the group in (1), $1 \leq \langle x^2 \rangle \leq G$ and also $1 \leq \langle x^3 \rangle \leq G$ are normal series (G is abelian) with prime indices, so they form two different composition series. (Any other example will suffice.)
[2 marks]