Math 343 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 inverse of X is X itself and the inverse of Y is the matrix

$$\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}.$$

[2 marks]

Since $X = X^{-1}$, $X^2 = I$. Also, we note that $Y^2 = -I, Y^3 = Y^{-1}$, so Y has order 4.

[2 marks]

Thus it is clear that $\langle X \rangle$ contains $I, Y, Y^2, Y^3, X, XY, XY^2, XY^3$. To show that these eight matrices form a group, we compute their multiplication table:

	I	Y	Y^2	Y^3	X	XY	XY^2	XY^3
I	I	Y	Y^2	Y^3	X	XY	XY^2	XY^3
Y	Y	Y^2	Y^3	I	XY^3	X	XY	XY^2
Y^2	Y^2	Y^3	I	Y	XY^2	XY^3	X	XY
Y^3	Y^3	I	Y	Y^2	XY	XY^2	XY^3	X
X	X	XY	XY^2	XY^3	I	Y	Y^2	Y^3
XY	XY	XY^2	XY^3	X	Y^3	I	Y	Y^2
XY^2	XY^2	XY^3	X	XY	Y^2	Y^3	I	Y
XY^3	XY^3	X	XY	XY^2	Y	Y^2	Y^3	I

[6 marks]

This group is non-abelian since XY and YX are unequal. [1 mark]

Let

$$Z = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

be the required matrix. Then the condition that $XZ = ZX$ yields the matrix equation

$$\begin{pmatrix} c & d \\ a & b \end{pmatrix} = \begin{pmatrix} b & a \\ d & c \end{pmatrix}$$

so that $a = d$ and $b = c$. Then the condition that $YZ = ZY$ gives that

$$\begin{pmatrix} ai & -bi \\ bi & -ai \end{pmatrix} = \begin{pmatrix} ai & bi \\ -bi & -ai \end{pmatrix}.$$

Thus $b = 0$, so Z has the form

$$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}.$$

If $Z^2 = I$, then $a = \pm 1$, so the only non-identity matrix of this from is $-I$ which is equal to Y^2. [3 marks]

It then follows from our table that Z commutes with every element of G. [2 marks]

2. 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. [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 $H \cap K = \{1\}$. [2 marks]

Now, we are given that $yx = x^{-1}y$ (the anchor step), so suppose that $yx^k = x^{-k}y$ then

$$yx^{k+1} = yx^k x = x^{-k}yx = x^{-(k+1)}y,$$

as required [2 marks]

To find the order of each of the 12 elements of G we note that x has order 6, so x^2 has order 3, x^3 has order 2, x^4 has order 3 and x^5 has order 6. Also $yx^iyx^i = y(yx^{-i})x^i = y^2 = 1$, so each other element of G has order 2. [4 marks]

Since G has 12 elements, the possible orders of subgroups of G are $1, 2, 3, 4, 6$ or 12. Thus G has no element of order 4 but could possibly have a subgroup of order 4 since 4 divides 12. If G has a non-cyclic subgroup with 4 elements, each non-identity element has order 2, and this group is abelian. The element x^3 has order 2 and commutes with y (since $yx^3 = x^{-3}y = x^3y$), so the required subgroup is $\{1, x^3, y, yx^3\}$. [5 marks]

Finally, we see that the only number in the list of divisors of 12 which could correspond to a non-abelian subgroup of G is 6, so the only possible proper non-abelian subgroup of G could have order 6, since the other divisors are prime or 4 and groups of order 4 are abelian. [2 marks]

3. Suppose that xH, yH are two left cosets of H in G and suppose that these cosets are unequal. If z is 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 $x = yh_2$, so that $xH = yh_2H$. Since h_2 is an element of H, and H is a subgroup, $h_2H = H$, so $xH = yH$ contrary to assumption. We deduce that if xH, yH are unequal they can have no elements in common. [4 marks].

To show that the given set H is a subgroup, name its elements as I, A, B (in the given order) and compute the table

	I	A	B
I	I	A	B
A	A	B	I
B	B	I	A

It is clear from this that H is closed, has an identity (I) and the inverse of A is B. Since matrix multiplication is associative, H is a subgroup. [3 marks]

Now to compute the left cosets of H in G, $IH = H = \{1, A, B\}$, and $-IH = \{-I, -A, -B\}$. Then

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} H = \{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}\}.$$

Finally, we note that

$$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} H = \{\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\}.$$

These 12 elements exhaust the complete list of elements of the group, so we have found 4 distinct cosets [4 marks].

To find the right cosets, use the same coset representatives. It is clear that $IH = HI$ and that $(-I)H = H(-I)$, so we only need to compute

$$H\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}\},$$

and

$$H\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \{\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}\}.$$

Thus, we see that left cosets are right cosets so H is a normal subgroup [2 marks]

The square of every element of G is in the subgroup H, so the square of every coset is the identity coset, so G/H is not cyclic. [4 marks]

The given set is not closed under multiplication, (the square of neither non-identity element is in the set) so K cannot be a normal subgroup. [3 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]

Then K=ker ϑ is a subgroup, because $1_G \in K$. If x, y are elements of K, then $\vartheta(x) = \vartheta(y) = 1_H$, so $\vartheta(x \circ y) = \vartheta(x) * \vartheta(y) = 1_H * 1_H = 1_H$, so $x \circ y \in K$. Finally since $\vartheta(g^{-1}) = \vartheta(g)^{-1}$, $\vartheta(g^{-1}) = {1_H}^{-1} = 1_H$ and $g^{-1} \in K$. It only remains to show that K is a normal subgroup. If $g \in G$ and $k \in K$ then

$$\vartheta(g \circ k \circ g^{-1}) = \vartheta(g) * 1_H * \vartheta(g)^{-1} = 1_H$$

so $g \circ k \circ g^{-1} \in K$. [4 marks]

The homomorphism theorem says

(a) im ϑ is a subgroup of H;

(b) ker ϑ is a normal subgroup of G;

(c) the quotient group $G/\ker\vartheta$ is isomorphic to im ϑ. [3 marks]

$$\vartheta(\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & a & b \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}) + \vartheta(\begin{pmatrix} 1 & d & e & f \\ 0 & 1 & d & e \\ 0 & 0 & 1 & d \\ 0 & 0 & 0 & 1 \end{pmatrix}) = a + d,$$

since $a + d$ is the (1,2) entry of the product matrix, ϑ is a homomorphism.

[2 marks]

However

$$\phi(\begin{pmatrix} 1 & a & b & c \\ 0 & 1 & a & b \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}) + \phi(\begin{pmatrix} 1 & d & e & f \\ 0 & 1 & d & e \\ 0 & 0 & 1 & d \\ 0 & 0 & 0 & 1 \end{pmatrix}) = b + e,$$

whereas the (1,3) entry of the product matrix is $b + e + ad$. Since these are unequal in general, ϕ is not a homomorphism. [2 marks]

Now $\ker \vartheta$ consists of those matrices with $a = 0$, and

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

so $\ker \vartheta$ is clearly abelian. Thus $G/\ker \vartheta$ is isomorphic to a subgroup of the integers so is cyclic and so G has an abelian normal subgroup with quotient group infinite cyclic, using the homomorphism theorem. [4 marks]

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

It follows that the product of two even permutations is even, that the identity is in $A(n)$ and that the inverse of a permutation π has the same sign as π, so $A(n)$ 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. [3 marks]

The set of odd permutations is not a subgroup because it isn't closed (the product of two odds is even). [1 mark].

If π is a product of r distinct cycles of lengths $l_1, \dots l_r$ then π has order the l.c.m. of $l_1, \dots l_r$. [1 mark]

Now suppose that π has odd order k. Then if π were odd, π^k would have sign $(-1)^k = -1$, so would also be odd. But $\pi^k = 1$ is even, so this contradiction shows that π is even. [3 marks]

To determine orders of elements, we only need consider possible cycle types:

$n=4$		$n=5$		$n=6$	
cycle type	*order*	*cycle type*	*order*	*cycle type*	*order*
(2)	2	(2)	2	(2)	2
(3)	3	(3)	3	(3)	4
(4)	4	(4)	4	(4)	4
(2)(2)	2	(2)(2)	2	(2)(2)	2
		(5)	5	(5)	5
		(2)(3)	6	(2)(3)	6
				(6)	6
				(2)(2)(2)	2
				(2)(4)	4
				(3)(3)	3

[4 marks]

We now see that 5 is the smallest integer such that $S(n)$ has an element of order 6, since $S(2)$ and $S(3)$ do not have elements of order 6. [2 marks]

Finally, the smallest n with $S(n)$ having an element of order 10 is 7 (an example being (1 2 3 4 5)(6 7)), but this element is odd so we need the mimimum of an extra transposition to have an even element of order 10 ((1 2 3 4 5)(6 7)(8 9)), so the required number is 9. [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 $x \in X$

$gh \circ x = g \circ (h \circ x)$ 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]

To show conjugacy satisfies the two G-set axioms:

$1 \circ x = 1x1^{-1}$, and

$(gh) \circ x = ghx(gh)^{-1} = ghxh^{-1}g^{-1} = g \circ (hxh^{-1}) = g \circ (h \circ x)$.

The orbit of x is the conjugacy class of x and the stabilizer of x is its centralizer

$$C_G(x) = \{h \in G : hg = gh\}.$$

[4 marks]

The elements of $A(4)$ are the identity element together with the 8 3-cycles

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

and the 3 products of disjoint 2-cycles

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

[1 mark]

The identity element is always a conjugacy class on its own. [1 mark]

The elements $\{1, (1\ 2\ 3), (1\ 3\ 2)\}$ are in the centralizer of (1 2 3), so it has at most 4 conjugates. However

$$\begin{aligned}(1\ 2)(3\ 4)(1\ 2\ 3)(1\ 2)(3\ 4) &= (2\ 1\ 4) = (1\ 4\ 2), \\ (1\ 3)((2\ 4)(1\ 2\ 3)(1\ 3)(2\ 4) &= (3\ 4\ 1) = (1\ 3\ 4), \text{ and} \\ (1\ 4)((2\ 3)(1\ 2\ 3)(1\ 4)(2\ 3) &= (4\ 3\ 2) = (2\ 4\ 3)\end{aligned}$$

so (1 2 3) has precisely 4 conjugates [3 marks]

In a similar way, we see that (1 3 2) has as its 4 conjugates (1 3 2), (1 2 4), (1 4 3) and (2 3 4). [2 marks]

We now have counted 9 elements of G, so only 3 remain. These form a single conjugacy class since

$$\begin{aligned}(1\ 2\ 3)(1\ 2)(3\ 4)(1\ 3\ 2) &= (2\ 3)(1\ 4); \\ (1\ 2\ 4)(1\ 2)(3\ 4)(1\ 4\ 2) &= (2\ 4)(3\ 1); \text{ and} \\ (1\ 3\ 4)(1\ 2)(3\ 4)(1\ 4\ 3) &= (1\ 3)(2\ 4).\end{aligned}$$

Thus G has 4 conjugacy classes. [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=3×5 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. [5 marks]

Now suppose that G is a group with 12=4×3 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]

Finally, there are 5 possible groups to choose from, but an obvious choice is an abelian group (such as C_8) together with $D(4)$ and Q, the quaternion group of order 8. Since the latter 2 are non-abelian, neither can be isomorphic to the abelian one. Also Q only has one element of order 2 whereas $D(4)$ has 5 elements of order 2, so these are not isomorphic. [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]

(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

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

[3 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).

[3 marks]

(c) Next, let G be cyclic of order 10 (so it is generated by x with $x^{10} = 1$). Consider the subgroup $\langle x^2 \rangle$ of order 5. It is normal because G is abelian. The series

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

cannot be refined because 2 and 5 are primes, so is a composition series.

[3 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-idenitity 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

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

[5 marks])

(e) We finally turn to the dihedral group $D(6)$. The subgroup $\langle x \rangle$ is cyclic of order 6 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 beacuse the factors are of prime order.

[3 marks]