MAT301 Fall 2018

Term Test 1 Solutions

1. [7] Let G be a group. Let $g \in G$ be an element of order 10.

(a) [3] List the elements of $\langle g \rangle$. No explanation is necessary. (Every element of $\langle g \rangle$ must appear exactly once on your list.)

(b) [4] Find the order of every element of $\langle g \rangle$.

Solution:

(a) $e, g, g^2, \ldots, g^9$ (Here e is the identity element of the group.)

(b) Using the formula $|g^k| = \dfrac{|g|}{\gcd(|g|, k)}$ we get g, g^3, g^7 and g^9 have order 10, while g^2, g^4, g^6 and g^8 have order 5 and g^5 has order 2. The identity e has order 1.

2. [5] Let G be a group and H be a subgroup of G. Define a relation $\sim$ on G as follows: for any $g, g' \in G$, set $g' \sim g$ if and only if $g' = hgh^{-1}$ for some $h \in H$. Show that $\sim$ is an equivalence relation on G.

Solution:

(a) Reflexivity: Let $g \in G$. Let e be the identity element of G. We have $g = ege^{-1}$. Since H is a subgroup, it contains e. Thus $g \sim g$.

(b) Symmetry: Let $g, g' \in G$ and $g' \sim g$. Then by the definition of the relation there exists $h \in H$ such that $g' = hgh^{-1}$. We then have $g = h^{-1}g'h = h^{-1}g'(h^{-1})^{-1}$. Note that $h^{-1} \in H$, as H is a subgroup and $h \in H$. Thus $g \sim g'$.

(c) Transitivity: Let $g, g', g'' \in G$. Suppose $g'' \sim g'$ and $g' \sim g$. Then there are $h', h \in H$ such that $g'' = h'g'h'^{-1}$ and$g' = hgh^{-1}$. Substituting the latter in the former we get

$$g'' = h'hgh^{-1}h'^{-1} = (h'h)g(h'h)^{-1}.$$

This together with the fact that $h'h \in H$ (as $h, h' \in H$ and H is a subgroup) implies that $g'' \sim g$.

3. [5] Suppose G is a finite group of even order. Show that G has an element of order 2.

Solution: Let A be the set consisting of the elements of G that are their own inverses, i.e. $A = \{g \in G : g = g^{-1}\}$. Let $B = G - A$. Thus B consists of the elements of G that are not their own inverses. The elements of B can be partitioned into pairs of inverse elements, i.e. pairs of the form $\{g, g^{-1}\}$. Thus the number of elements of B is even. Since $|G|$ is even, it follows that the number of elements of A is even. Since $g^{-1} = g$ is equivalent to $g^2 = e$, we can write A as the union of the two disjoint sets

$$\{e\} \quad \text{and} \quad \{g \in G : |g| = 2\}.$$

It follows that $\{g \in G : |g| = 2\}$ has an odd number of elements. It particular, it is nonempty.

4. [5] Let G be a finite group. Let H be a nonempty subset of G that is closed under the operation (i.e. if $g, h \in H$, then $gh \in H$). Show that H is a subgroup of G.

Solution: We shall show that H contains the identity element and that it is closed under taking inverses.

- Claim: H contains the identity element.

  Proof: Since H is nonempty, there exists an element $h \in H$. Then there exists a positive integer n such that $h^n = e$ (as every element of a finite group has finite order). Since $h \in H$ and H is closed under the operation, it follows that $h^n \in H$. Thus $e \in H$.

- Claim: H is closed under taking inverses.

  Proof: Let $h \in H$. If $h = e$ then $h^{-1} = h \in H$. Otherwise, again as above, being an element of a finite group, h has finite order. Thus there exists a positive integer $n > 1$ such that $h^n = e$. Then $h^{-1} = h^{n-1}$. Since $n - 1 \geq 1$, $h \in H$, and H is closed under the operation, we have $h^{n-1} \in H$.

5. [10] Let U be the subset of $GL_2(\mathbb{R})$ consisting of upper triangular matrices of determinant 1. In other words, let

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} : a, b, c \in \mathbb{R} \text{ and } ac = 1 \right\}.$$

(a) [5] Show that U is a subgroup of $GL_2(\mathbb{R})$. (Recall that $GL_2(\mathbb{R})$ is the group of invertible 2×2 matrices with real entries under matrix multiplication.)

(b) [5] Find the centre of the group U. (Recall that for any group G, the centre of G is by definition the subset $Z(G) := \{h \in G : gh = hg \text{ for every } g \in G\}$.)

Solution:

(a) The identity matrix is certainly in U. Let $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \in U$. Then, since $\det(A) = ac = 1$, we have

$$A^{-1} = \begin{pmatrix} c & -b \\ 0 & a \end{pmatrix},$$

which belongs to U. Thus U is closed under taking inverses. Now suppose moreover that $B = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in U$. Then

$$AB = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} = \begin{pmatrix} ax & * \\ 0 & cz \end{pmatrix},$$

which is upper triangular and moreover its determinant (= product of diagonal entries) is $\det(A)\det(B) = 1$. Thus $AB \in U$, so that U is closed under the operation.

(b) Let I be the 2×2 identity matrix. We claim that $Z(U) = \{I, -I\}$. First note that $-I$ (and I) both belong to U. Being scalar matrices, I and $-I$ commute with every 2×2 matrix, in particular, with every element of U. Thus $\{I, -I\} \subset Z(U)$. (Continued on the next page.)

Extra space for Question 5. Question 6 is on the next page.

Solution to Question 5(b), continued:

Now we show that $Z(U) \subset \{I, -I\}$. Indeed, let $A \in Z(U)$. Let $A = \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$. Then A commutes with every element of U, in particular with the matrix $B = \begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix}$. We have

$$AB = \begin{pmatrix} 2a & 1/2\,b \\ 0 & 1/2c \end{pmatrix} \quad \text{and} \quad BA = \begin{pmatrix} 2a & 2b \\ 0 & 1/2c \end{pmatrix}.$$

Since $AB = BA$, we get $b = 0$, so that $A = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$. Now consider the matrix $C = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. Note that $C \in U$ and hence we must have $AC = CA$. We have

$$AC = \begin{pmatrix} a & a \\ 0 & c \end{pmatrix} \quad \text{and} \quad CA = \begin{pmatrix} a & c \\ 0 & c \end{pmatrix}.$$

Comparing the (1,2) entries of the two matrices we get $a = c$. Now on recalling $\det(A) = ac = 1$ we get that $a = c = 1$ or $a = c = -1$, i.e. $A = I$ or $A = -I$.

6. [13] A part of the Cayley table of a group G of order 8 is shown below. The elements of G are denoted by s, t, u, v, w, x, y and z. Answer the following questions (with justification).

	s	t	u	v	w	x	y	z
s								
t		w	v					
u		z	w					
v				w				
w		x	y	z				
x								
y	y							
z								

(a) [2] What is the identity element of the group?

(b) [1] Is the group G abelian?

(c) [3] Show that $|t| = |u| = |v| = 4$. (Suggestion: Use $|G| = 8$ to limit the possibilities for the order of the elements of G.)

(d) [2] Show that $w^2 = s$.

(e) [3] Show that $x^2 = y^2 = z^2 = w$.

(f) [2] Can $G = D_4$? (Suggestion: How many elements of order 4 does D_4 have?)

Solution:

(a) The table gives us $ys = y$. Multiplying by y^{-1} on the left we see that s is the identity of the group.

(b) No, as $ut = z$ and $tu = v$.

Extra space for Question 6. Question 7 is on the next page.

Solution to Question 6 continued:

(c) Since $|G| = 8$, by Lagrange's theorem the order of every element of G divides 8. Thus $|t|$ is one of the numbers 1,2,4,8. It is not 1 or 2 since $t^2 = w$ and w is not the identity element. It is not 8 as otherwise $G = \langle t \rangle$ and would be cyclic, and hence abelian (which is not). Thus $|t| = 4$. The same argument applies to u and v.

(d) From the table $w = t^2$. Thus $w^2 = t^4$, which is s by Parts (c) and (a).

(e) From the table $x = wt$ and $w = t^2$. Thus $x = t^3$ and $x^2 = t^6 = t^2 = w$ (where in $t^6 = t^2$ we used the fact that t^4 is the identity, as $|t| = 4$). The arguments for y and z is similar (with every occurrence of t replaced respectively by u and v).

(f) No it cannot. Indeed, D_4 has only 2 elements of order 4 (namely rotations by $\pi/2$ and $3\pi/2$), whereas G has at least 3 (in fact, 6, as x, y, z also have order 4) such elements.

7. [10] Let G be a group with the identity element denoted by e. Let H and K be finite subgroups of G with $|H| = m$ and $|K| = n$. Suppose that $\gcd(m, n) = 1$.

(a) [5] Show that $H \cap K = \{e\}$.

(b) [5] Suppose moreover that $|G| = mn$. Show that for every $g \in G$, there are unique $h \in H$ and $k \in K$ such that $g = hk$.

Solution:

(a) Since the intersection of subgroups is a subgroup, $H \cap K$ is a subgroup of G. Being contained in H and K, the intersection $H \cap K$ is then a subgroup of both H and K. By Lagrange's theorem, $|H \cap K|$ divides both $m = |H|$ and $n = |K|$. Since m and n are relatively prime, we get $|H \cap K| = 1$, i.e. $H \cap K = \{e\}$.

(b) We first prove a

Claim: If $hk = h'k'$ for some $h, h' \in H$ and $k, k' \in K$, then $h = h'$ and $k = k'$.

Proof: Indeed, suppose $hk = h'k'$ for some $h, h' \in H$ and $k, k' \in K$. Then $h'^{-1}h = k'k^{-1}$. Since H is a subgroup and $h, h' \in H$, we have $h'^{-1}h \in H$. Similarly, using the fact that K is a subgroup, we see $k'k^{-1} \in K$. Thus the element $h'^{-1}h = k'k^{-1}$ belongs to $H \cap K$. Combining with Part (a) we get $h'^{-1}h = k'k^{-1} = e$, which gives the desired conclusions.

By the above claim, the subset

$$A := \{hk : h \in H \text{ and } k \in K\}$$

of G has mn elements. Since $|G| = mn$, we must have $A = G$. Thus every element of G can be written in the form hk for some $h \in H$ and $k \in K$. The uniqueness follows from the claim we first proved.

Extra space. What you write here will not be graded unless you write next to the relevant question(s) “Continued on page 11”.

Extra space. What you write here will not be graded unless you write next to the relevant question(s) “Continued on page 12”.

Extra space. What you write here will not be graded unless you write next to the relevant question(s) “Continued on page 13”.

Extra space. What you write here will not be graded unless you write next to the relevant question(s) “Continued on page 14”.

The end. (Total marks=55)