Math 31 – Take-home Midterm Solutions

Due July 26, 2013

Name: ____________________

Instructions: You may use your textbook (Saracino), the reserve text (Gallian), your notes from class (including the online lecture notes), and your old homework assignments. All other written materials are forbidden, as are any other electronic materials. You may not discuss the exam with anyone, and I will not give any assistance in solving the problems. You may ask me to clarify questions if necessary. Please hand this sheet in with your solutions. The exam is due on **Friday, July 26 at the beginning of class**.

Honor statement:

I have neither given nor received any help on this exam, and I have not discussed the exam with anyone. I attest that all of the answers are my own work.

____

Signature

Question	Points	Score
1	10	
2	8	
3	12	
4	7	
5	7	
6	14	
7	22	
Total	80	

1. Consider the cyclic group $\mathbb{Z}_{20}$.

(a) [7 points] Any element $x \in \mathbb{Z}_{20}$ can be written in the form

$$x = a +_{20} b$$

for some $a \in \langle 4 \rangle$ and some $b \in \langle 5 \rangle$. Explain why this is so.

Solution. It will suffice to see that there are $a \in \langle 4 \rangle$ and $b \in \langle 5 \rangle$ such that $1 = a +_{20} b$. Since $\gcd(4, 5) = 1$, Bézout's lemma implies that there exist $x, y \in \mathbb{Z}$ such that

$$4x + 5y = 1.$$

Define $a, b \in \mathbb{Z}_{20}$ by

$$a = [4x]_{20}, b = [5y]_{20}.$$

Then $a \in \langle 4 \rangle$, $b \in \langle 5 \rangle$, and $a +_{20} b = 1$. Now if $z \in \mathbb{Z}_{20}$ is any element, we have

$$za +_{20} zb = z,$$

and $za \in \langle 4 \rangle$ and $zb \in \langle 5 \rangle$.

(b) [3 points] The elements a and b from part (a) are actually unique. Why?

Solution. Suppose that $x \in \mathbb{Z}_{20}$, and we can write $x = a +_{20} b$ and $x = a' +_{20} b'$ for some $a, a' \in \langle 4 \rangle$ and $b, b' \in \langle 5 \rangle$. Then

$$(a +_{20} b) - (a' +_{20} b') = 0,$$

or

$$(a - a') = (b' - b)$$

in $\mathbb{Z}_{20}$. However, $a - a'$ is a multiple of 4, while $b' - b$ is a multiple of 5. Therefore, both $a - a'$ and $b' - b$ are divisible by both 4 and 5, hence by 20. That is, $a \equiv a' \bmod 20$ and $b \equiv b' \bmod 20$, so each element of $\mathbb{Z}_{20}$ can be written uniquely in the form described in part (a).

Here is an alternative argument. Note that there are at most 20 possible elements of the form $a +_{20} b$, since there are 5 choices for a and 4 choices for b. But we saw in part (a) that there are exactly 20 such combinations of a and b, so they must all be distinct. Therefore, each element of $\mathbb{Z}_{20}$ can be expressed in exactly one way as $a +_{20} b$ with $a \in \langle 4 \rangle$ and $b \in \langle 5 \rangle$.

2. [8 points] Define $\mathrm{O}_n(\mathbb{R}) \subseteq \mathrm{GL_n}(\mathbb{R})$ by

$$\mathrm{O}_n(\mathbb{R}) = \left\{A \in \mathrm{GL_n}(\mathbb{R}) : A^{-1} = A^T\right\},$$

where A^T denotes the transpose of A. (You might remember from linear algebra that the elements of $\mathrm{O}_n(\mathbb{R})$ are called *orthogonal matrices.*) Verify that $\mathrm{O}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL_n}(\mathbb{R})$. [**Hint:** Recall that if A and B are $n \times n$ matrices, then $(AB)^T = B^T A^T$ and $(A^T)^{-1} = (A^{-1})^T$.]

Proof. We will first show that $\mathrm{O}_n(\mathbb{R})$ is closed. Let $A, B \in \mathrm{O}_n(\mathbb{R})$. Then

$$(AB)^{-1} = B^{-1}A^{-1} = B^T A^T = (AB)^T,$$

so AB is also an orthogonal matrix. Clearly the identity matrix belongs to $\mathrm{O}_n(\mathbb{R})$, since

$$I = I^{-1} = I^T.$$

Finally, suppose that $A \in \mathrm{O}_n(\mathbb{R})$. Then

$$(A^{-1})^{-1} = A = (A^T)^T = (A^{-1})^T,$$

so $A^{-1} \in \mathrm{O}_n(\mathbb{R})$ as well. Therefore, $\mathrm{O}_n(\mathbb{R})$ is a subgroup of $\mathrm{GL_n}(\mathbb{R})$. □

3. Recall that S_n denotes the symmetric group on n letters.

(a) [8 points] Given a fixed permutation $\sigma \in S_n$, we can define a relation $\sim$ on the set $\{1, 2, \ldots, n\}$ as follows: $i \sim j$ whenever there is an integer k such that

$$\sigma^k(i) = j.$$

Note that

$$\sigma^k = \underbrace{\sigma \circ \cdots \circ \sigma}_{k \text{ times}}.$$

Prove that $\sim$ defines an equivalence relation on $\{1, 2, \ldots, n\}$.

Proof. Let $i \in \{1, 2, \ldots, n\}$. Then $i \sim i$, since $i = \sigma^0(i) = \iota(i)$. (If you want to deal only with positive integers, you could recall that $|S_n| = n!$, so $\sigma^{n!} = \iota$, and $i = \sigma^{n!}(i)$ for all i.) Therefore, $\sim$ is reflexive.

If $i, j \in \{1, 2, \ldots, n\}$ with $i \sim j$, then there is a $k \in \mathbb{Z}$ such that $j = \sigma^k(i)$. But then

$$\sigma^{-k}(j) = \sigma^{-k}\sigma^k(i) = \iota(i) = i,$$

so $j \sim i$, and the relation is symmetric. (Again, you could show alternatively that $\sigma^{n!-k}(j) = i$.)

Finally, suppose that $i, j, l \in \{1, 2, \ldots, n\}$ with $i \sim j$ and $j \sim l$. Then $j = \sigma^{k_1}(i)$ and $l = \sigma^{k_2}(j)$ for some $k_1, k_2 \in \mathbb{Z}$. But then

$$l = \sigma^{k_2}(j) = \sigma^{k_2}(\sigma^{k_1}(i)) = \sigma^{k_2}\sigma^{k_1}(i) = \sigma^{k_1+k_2}(i),$$

so $l \sim i$. Therefore, $\sim$ is transitive, and it is an equivalence relation. □

(b) [4 points] Consider the permutation $\sigma \in S_8$ defined by

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 1 & 3 & 7 & 2 & 8 & 4 & 6 \end{pmatrix}$$

If we use this particular σ to define the equivalence relation from part (a) on the set $\{1, 2, 3, \ldots, 8\}$, what are the equivalence classes?

Solution. The equivalence classes will all have the form

$$[i] = \{i, \sigma(i), \sigma^2(i), \ldots\}.$$

Therefore, we have

$$\begin{aligned} [1] = [2] = [5] &= \{1, 5, 2\} \\ [3] &= \{3\} \\ [4] = [7] &= \{4, 7\} \\ [6] = [8] &= \{6, 8\} \end{aligned}$$

4. [7 points] Suppose that G is a finite group of order n, and $m \in \mathbb{Z}$ is relatively prime to n. If $g \in G$ and $g^m = e$, prove that $g = e$.

Proof. Let $n = |G|$. We know from Lagrange's theorem that $o(g)$ must divide n. However, since $g^m = e$, we must also have $o(g) \mid m$. But then $o(g)$ must divide $\gcd(n, m)$, which is 1. The only possibility is that $o(g) = 1$, which forces $g = e$. □

5. [7 points] Let G be a group of order 49. Show that G must have a subgroup of order 7.

Proof. Choose an element $a \in G$ with $a \neq e$. Since $o(a)$ must divide $|G|$ by Lagrange's theorem, we must have either $o(a) = 7$ or $o(a) = 49$. In the first case we are done, since the subgroup $\langle a \rangle$ has order 7. In the second case (i.e., where G is cyclic), note that a^7 has order 7, so the subgroup $\langle a^7 \rangle$ has order 7. □

6. Let G be a group with respect to a binary operation $*$. Define another binary operation ☺ on G by

$$a \mathbin{\text{☺}} b = b * a.$$

Use G^{op} to denote the set G endowed with the binary operation ☺.

(a) [7 points] Prove that G^{op} is a group with respect to the operation ☺. (This group is called the *opposite group*.)

Proof. The operation $\smiley$ certainly gives a well-defined binary operation on G. We need to check that $\smiley$ associative, and we need to verify the existence of an identity and inverses.

Suppose that $a, b, c \in G$. Then

$$a \smiley (b \smiley c) = a \smiley (c * b) = (c * b) * a,$$

while

$$(a \smiley b) \smiley c = (b * a) \smiley c = c * (b * a).$$

SInce $*$ is associative, these are the same. Therefore, $\smiley$ is associative as well.

We claim that the identity element of G^{op} is still e: for any $a \in G^{\text{op}}$, we have

$$e \smiley a = a * e = a$$

and

$$a \smiley e = e * a = a.$$

Finally, the inverses are the same as well: if $a \in G^{\text{op}}$, then

$$a^{-1} \smiley a = a * a^{-1} = e$$

and

$$a \smiley a^{-1} = a^{-1} * a = e.$$

Therefore, G^{op} is a group. □

(b) [7 points] Define $\varphi : G \to G^{\text{op}}$ by $\varphi(a) = a^{-1}$ for all $a \in G$. Show that φ is one-to-one and onto, and that

$$\varphi(a * b) = \varphi(a) \smiley \varphi(b)$$

for all $a, b \in G$.

Proof. The fact that φ is one-to-one follows from uniqueness of inverses: $\varphi(a) = \varphi(b)$ implies that $a^{-1} = b^{-1}$, which means that $a = b$. Similarly, φ is onto because every element has an inverse: given $b \in G^{\text{op}}$, we have

$$\varphi(b^{-1}) = (b^{-1})^{-1} = b.$$

Finally, if $a, b \in G$, then

$$\varphi(a * b) = (a * b)^{-1} = b^{-1} * a^{-1} = a^{-1} \smiley b^{-1} = \varphi(a) \smiley \varphi(b).$$

(Note that this shows that φ is a homomorphism, and that $G \cong G^{\text{op}}$.) □

7. Let G be a group. For each $a \in G$, define

$$C(a) = \{x \in G : ax = xa\} = \left\{x \in G : x^{-1}ax = a\right\}.$$

Thus $C(a)$ can be thought of as the set of all elements of G which commute with a, and it is called the *centralizer* of a in G.

(a) [4 points] If G is abelian, prove that $C(a) = G$ for all $a \in G$.

Proof. Suppose that G is abelian, and let $g \in G$. Then $ga = ag$ for all $a \in G$, so clearly $g \in C(a)$. Thus $C(a) = G$ for all $a \in G$. □

(b) [6 points] Prove that for any $a \in G$, $C(a)$ is a subgroup of G.

Proof. First we note that $e \in C(a)$, since $ea = ae = a$. Next, if $x, y \in C(a)$, then

$$(xy)a = x(ya) = x(ay) = (xa)y = (ax)y = a(xy),$$

so $xy \in C(a)$ as well. Therefore, $C(a)$ is closed. Finally, if $x \in C(a)$, then $ax = xa$ implies that $x^{-1}ax = a$, so

$$x^{-1}a = ax^{-1},$$

and $x^{-1} \in C(a)$. Therefore, $C(a)$ is a subgroup of G. □

(c) [6 points] For $a \in G$, define

$$\mathrm{cl}(a) = \left\{g^{-1}ag : g \in G\right\}.$$

Recall that $G/C(a)$ denotes the set of all (right) cosets of $C(a)$ in G. Define a function $f : \mathrm{cl}(a) \to G/C(a)$ by

$$f(g^{-1}ag) = C(a)g.$$

Prove that f is one-to-one and onto.

Proof. To show that f is one-to-one, suppose that $f(g^{-1}ag) = f(h^{-1}ah)$ for some $g, h \in G$. Then $C(a)g = C(a)h$, so $gh^{-1} \in C(a)$. Therefore,

$$a = (gh^{-1})^{-1}a(gh^{-1}) = hg^{-1}agh^{-1}.$$

But then

$$h^{-1}ah = g^{-1}ag,$$

so f is one-to-one. It is certainly onto, since if $C(a)g \in G/C(a)$, then $f(g^{-1}ag) = C(a)g$. □

[**Note:** Part (c) is a special case of a major theorem, called the *Orbit-Stabilizer Theorem.* This result is important in the theory of group actions, and we are dealing with the case of a group acting on itself by conjugation.]

(d) [6 points] If $a, b \in G$ and $b = g^{-1}ag$ for some $g \in G$, prove that $C(b) = g^{-1}C(a)g$.

Proof. First let $x \in C(a)$; then we need to show that $g^{-1}xg \in C(b)$. Well, we know that $a = gbg^{-1}$, so

$$\begin{aligned}(g^{-1}xg)^{-1}b(g^{-1}xg) &= g^{-1}x^{-1}gbg^{-1}xg \\ &= g^{-1}x^{-1}axg \\ &= g^{-1}ag \\ &= b,\end{aligned}$$

since $x \in C(a)$. Therefore, $g^{-1}C(a)g \subset C(b)$. Now suppose that $y \in C(b)$. Then $y^{-1}by = b$, so

$$y^{-1}(g^{-1}ag)y = g^{-1}ag.$$

Multiplying on left and right g and g^{-1}, respectively, we have

$$gy^{-1}(g^{-1}ag)yg^{-1} = a,$$

or

$$(gyg^{-1})^{-1}a(gyg^{-1}) = a.$$

That is, $x = gyg^{-1} \in C(a)$, and $y = g^{-1}xg$, so $y \in g^{-1}C(a)g$. It follows that $C(b) = g^{-1}C(a)g$. □