Math 103A, Modern Algebra I, Final

Friday, December 13th, 2019, 8–11am, APM B402A

• Your Name: SOLUTIONS

• ID Number:

• Section:

B01 (5:00 PM)   B02 (6:00 PM)

<table>
<thead>
<tr>
<th>Problem #</th>
<th>Points (out of 10)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td></td>
</tr>
</tbody>
</table>

Total (out of 90):
Problem 1. Let \((G, \cdot)\) be a cyclic group of size 10. Choose a generator \(a \in G\).

(a) Find the order of each of its elements:

\[ e \quad a \quad a^2 \quad a^3 \quad a^4 \quad a^5 \quad a^6 \quad a^7 \quad a^8 \quad a^9 \]

Circle those \(x\) above for which \(G = \langle x \rangle\) holds.

(b) List the elements of the two non-trivial subgroups \(\langle a^2 \rangle\) and \(\langle a^5 \rangle\).

(c) Find all the elements of the cosets \(a \cdot \langle a^2 \rangle\) and \(a \cdot \langle a^5 \rangle\).

\(a\) use that \(a^n\) has order \(\frac{10}{\text{GCD}(10, n)}\). 
- see table next page.
  
  Shows \(a^n\) generates \(G\) for \(n = 1, 3, 7, 9\).

(b) \(\langle a^2 \rangle = \{e, a^2, a^4, a^6, a^8\}\)
\(\langle a^5 \rangle = \{e, a^5\}\).

(c) \(a \cdot \langle a^2 \rangle = \{a, a^3, a^5, a^7, a^9\}\).
\(a \cdot \langle a^5 \rangle = \{a, a^6\}\).
**Table (Problem 1):**

<table>
<thead>
<tr>
<th>n</th>
<th>( \text{ord}(a^n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>10</td>
</tr>
<tr>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>6</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>5</td>
</tr>
<tr>
<td>9</td>
<td>10</td>
</tr>
</tbody>
</table>
Problem 2. Recall that $(\mathbb{Z}_{11}^\times, \cdot)$ denotes the multiplicative group of all the invertible residue classes modulo 11.

(a) Find $|\mathbb{Z}_{11}^\times|$ and check that the residue class $[2]$ generates $\mathbb{Z}_{11}^\times$.

(b) Give the order of each of the elements:

\[
\begin{array}{cccccccccc}
\end{array}
\]

Circle those $[x]$ above where $\mathbb{Z}_{11}^\times = \langle [x] \rangle$ holds.


(a) $|\mathbb{Z}_{11}^\times| = \varphi(11) = 10$, and $[2]$ generates $\mathbb{Z}_{11}^\times$:

\[
\begin{align*}
2^1 & \equiv 2, \quad 2^2 \equiv 4, \quad 2^3 \equiv 8, \quad 2^4 \equiv 5, \quad 2^5 \equiv 10, \\
2^6 & \equiv 9, \quad 2^7 \equiv 7, \quad 2^8 \equiv 3, \quad 2^9 \equiv 6, \quad 2^{10} \equiv 1.
\end{align*}
\]

(all modulo 11).

(b) Use the formula $\ker[2]^n = \frac{10}{\gcd(10, n)}$. See table next page.

Shows $[a]$ generates $\mathbb{Z}_{11}^\times$ for $a = 2, 6, 7, 8$.

(c) $[2] \cdot \langle [4] \rangle = [2] \cdot \{ [1], [4], [5], [9], [3] \}$

and $[3] \cdot \langle [4] \rangle = \{ [3], [1], [4], [5], [9] \}$


**Table (Problem 2):**

<table>
<thead>
<tr>
<th>a</th>
<th>( \text{ord}[a] )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>6</td>
<td>10</td>
</tr>
<tr>
<td>7</td>
<td>10</td>
</tr>
<tr>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>9</td>
<td>5</td>
</tr>
<tr>
<td>10</td>
<td>2</td>
</tr>
</tbody>
</table>

**Ex** \( \text{ord}[3] = \text{ord}[2]^8 = \frac{10}{\text{gcd}(10,8)} = \frac{10}{2} = 5 \)
Problem 3. Recall that \((Z_{15}, +)\) denotes the additive group of all residue classes modulo 15.

(a) Give all integers \(x\) in the range \(0 \leq x < 15\) such that \(Z_{15} = \langle [x] \rangle\).

(b) Write down all elements of the two non-trivial subgroups of \(Z_{15}\).

(c) Explain why the quotient group \(Z_{15}/\langle [5] \rangle\) is isomorphic to \(Z_5\).

(a) Know \([x]\) generates \(Z_{15}\) iff \(\text{GCD}(x, 15) = 1\).

In the interval \(0 \leq x < 15\) we have \(x = 1, 2, 4, 7, 8, 11, 13, 14\).

(b) Since 15 has 4 divisors \(\{1, 3, 5, 15\}\) we only have two non-trivial subgroups:

\[
\langle [3] \rangle = \{ [0], [3], [6], [9], [12] \} \quad \text{and}
\]

\[
\langle [5] \rangle = \{ [0], [5], [10] \}.
\]

(c) \(|Z_{15}/\langle [5] \rangle| = \frac{15}{3} = 5\) prime.

Every group of order \(p =\) prime is cyclic, and therefore isomorphic to \(Z_p\).

— or more concretely: \([1] + \langle [5] \rangle\) is a generator for \(Z_{15}/\langle [5] \rangle\).

a "quotient of cyclic group is cyclic".

\[ Z_{15}/\langle [5] \rangle \cong Z_5. \]
Problem 4. Consider the additive group \((\mathbb{Z}, +)\) of all integers. Recall that \(N\mathbb{Z}\) denotes the subgroup of \(\mathbb{Z}\) consisting of all integer multiples of \(N\).

(a) Find the positive integer \(M\) such that \(65\mathbb{Z} \cap 91\mathbb{Z} = M\mathbb{Z}\).

(b) Find the positive integer \(N\) such that \(65\mathbb{Z} + 91\mathbb{Z} = N\mathbb{Z}\), and express \(N\) as a linear combination \(65x + 91y\) for suitable integers \(x, y \in \mathbb{Z}\).

(c) Let \(f : 65\mathbb{Z} \rightarrow \mathbb{Z}/91\mathbb{Z}\) be the homomorphism sending an \(a \in 65\mathbb{Z}\) to its residue class \([a]\) modulo 91. Calculate the following two quantities:

(i) The cardinality of \(\text{im}(f)\).

(ii) The index of \(\ker(f)\) in \(65\mathbb{Z}\).

\[(a)\ 65\mathbb{Z} \cap 91\mathbb{Z} = \text{LCM}(65, 91)\mathbb{Z} = 455\mathbb{Z},\]

\[(b)\ 65\mathbb{Z} + 91\mathbb{Z} = \text{GCD}(65, 91)\mathbb{Z} = 13\mathbb{Z},\]

\[-\text{Euclid:}\]

\[\begin{align*}
  91 & = 1 \cdot 65 + 26 \\
  65 & = 2 \cdot 26 + 13 \\
  26 & = 2 \cdot 13
\end{align*}\]

\[-\text{given: LCM} = 5 \cdot 7 \cdot 13 = 455\]

\[-\text{check:}\]

\[65 = 5 \cdot 13 \\
91 = 7 \cdot 13\]

\[-\text{prime factors}\]

\[N = 13 = 65 - 2(91 - 65) = 3 \cdot 65 + (-2) \cdot 91\]

so many take:\n
\[x = 3, \ y = -2\]

\[-\text{other solutions too!}\]

\[(c)\ \text{im}(f) = (65\mathbb{Z} + 91\mathbb{Z})/91\mathbb{Z}\
\[= 13\mathbb{Z}/91\mathbb{Z} = \mathbb{Z}/13\mathbb{Z}.\]

\[\ker(f) = 65\mathbb{Z} \cap 91\mathbb{Z} = 455\mathbb{Z}, \text{ has index}\]

\[\left[ 65\mathbb{Z} : \ker(f) \right] = 5 \quad \text{im}(f) = 7.\]

First isomorphism Thm.
Problem 5. Let \( \alpha \in S_9 \) be the permutation \( \alpha = (1234)(25)(617)(389) \).

(a) Express \( \alpha \) in array form. That is, fill in the blank boxes below.

\[
\alpha = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
\square & \square & \square & \square & \square & \square & \square & \square & \square
\end{pmatrix}
\]

(b) Is \( \alpha \) a cycle? If not, find its decomposition into disjoint cycles.

(c) Compute \( \text{ord}(\alpha) \) and \( \text{sign}(\alpha) \). Does \( \alpha \) belong to \( A_9 \)?

\( \alpha = \begin{pmatrix}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
7 & 5 & 8 & 1 & 3 & 2 & 6 & 9 & 4
\end{pmatrix} \)


**Example.** \( 9 \mapsto 3 \mapsto 1 \mapsto 3 \mapsto 1 \mapsto 4 \) by the cycles in \( \alpha \).

(b) \( \alpha \) takes \( 1 \mapsto 7 \mapsto 6 \mapsto 2 \mapsto 5 \mapsto 3 \mapsto 8 \mapsto 9 \) → so yes, \( \alpha \) is a \( 9 \)-cycle:

\[\alpha = (176253894)\]

(c) \( \text{ord}(\alpha) = \text{length}(\alpha) = 9 \)

\[\text{sign}(\alpha) = (-1)^{9-1} = +1\] → in other words \( \alpha \) is an even permutation.

So yes, \( \alpha \in A_9 \).
Problem 6. For each of the five statements below indicate whether it is true or false. Justify your answers.

- **F** (a) The group of rotational symmetries of a tetrahedron is isomorphic to $S_4$.
- **T** (b) The group of rotational symmetries of a cube is isomorphic to $S_4$.
- **T** (c) The direct product $G \times G$ is not cyclic for any non-trivial group $G$.
- **T** (d) All subgroups of an abelian group are normal.
- **F** (e) If $G$ is any group, and $H \subset G$ is a normal subgroup, the following holds:

$$G \text{ cyclic } \iff \text{ } H \text{ and } G/H \text{ are cyclic.}$$

(c) **FALSE.** The group is isomorphic to $A_4$ which has 12 elements. ($153!! = 3! = 6$)

(b) **TRUE.** The group permutes the $4$ diagonals of the cube, giving an injective hom. $G \to S_4$.

One can easily rule down $24$ rotational symmetries.

$\Rightarrow \ G \cong S_4$.

(c) Suppose $G \times G$ is generated by $(a,b)$. Then, if $|G| < \infty$:

**TRUE.**

$$\text{ord}(a,b) = \text{LCM}(\text{ord}a, \text{ord}b) : \text{divides } |G|.$$ 

$$|G|^2 \quad \uparrow \quad \uparrow \quad \text{both divide } |G| = \text{common multiple by LAGRANGE.}$$

$\Rightarrow \ |G| = 1$, i.e. $G$ must be **trivial**.

- If $|G| = \infty$ and $G \times G$ is cyclic, $G$ must be cyclic (view $G$ as a subgroup $\{(a,a) : a \in G \} \subset G \times G$)

---

**CONT.**
Therefore, \( G \cong \mathbb{Z} \) and \( G \times G \cong \mathbb{Z} \).

Must show \( \mathbb{Z} \times \mathbb{Z} \) is not isomorphic to \( \mathbb{Z} \).

Why not? All quotient of \( \mathbb{Z} \) are cyclic, but

\[ \mathbb{Z} \times \mathbb{Z} \text{ admits } V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2 \text{ as a quotient: } \frac{\mathbb{Z} \times \mathbb{Z}}{\mathbb{Z} \times \mathbb{Z}} \text{ (non-cyclic)}. \]

(d) TRUE. If \( G \) abelian and \( H \leq G \), then \( H \) must be normal.

\[ g \in G \land h \in H \implies ghg^{-1} \in H. \]

But \( ghg^{-1} = hgg^{-1} = h \leq H \checkmark \]

\( g,h \) commute \( (G \) abelian) \n
(e) FALSE. The direction \( \implies \) is true, but

\[ \impliedby \text{ is false. Therefore the statement } \impliedby \text{ is altogether false.} \]

**Details:**

\( \implies \) is true. Indeed we know subgroups of cyclic groups are cyclic, and if \( G = \langle a \rangle \) then \( G/H \) is generated by the set \( a * H \).

\( \impliedby \) is false, however: \( G = \mathbb{Z}_2 \times \mathbb{Z}_2 \)

Here

\[ H = \{ (a,0) : a \in \mathbb{Z}_2 \} \leq G. \]

\( H \cong \mathbb{Z}_2 \) and \( G/H \cong \mathbb{Z}_2 \) are both cyclic, but the (Klein 4-group) \( G \) is not.
Problem 7. Consider the alternating group $A_5$.

(a) Compute its cardinality $|A_5|$ and its index in $S_5$.

(b) Prove or disprove the existence of a non-trivial homomorphism 

$$f : A_5 \to \{\pm 1\}.$$ 

(c) Let $H \subset A_5$ be the subgroup generated by the 3-cycle (135).

(i) Find the index $[A_5 : H]$.

(ii) List all elements of the coset $(12345) \circ H$. (Express all permutations as a composition of disjoint cycles.) Is $(12345) \circ H = H \circ (12345)$?

(c) $|A_5| = \frac{5!}{2} = \frac{120}{2} = 60$, $[S_5 : A_5] = \frac{120}{60} = 2$.

(b) There is no such $f$. For suppose $f : A_5 \to \{\pm 1\}$ is a homomorphism. Then for any 3-cycle $(abc)$:

$$f((abc)) = f((acb)^2) = f((acb))^2 = (\pm 1)^2 = +1.$$ 

Therefore, $\ker(f)$ contains all $(abc)$, which generate $A_5$. Thus $\ker(f) = A_5$, meaning $f$ must be trivial.

(c) $H = \langle (135) \rangle = \{ e, (135), (153) \}$.

(i) Index $[A_5 : H] = \frac{60}{3} = 20$.

(ii) $(12345) \circ H = \{ (12345), (12345)(135), (12345)(153) \}$

$$= \{ (12345), (14523), (23)(45) \}.$$

Not equal to $H \circ (12345)$: This right coset contains $(135)(12345) = (12534)$ which is not in the left coset $(12345) \circ H$. (So $H$ isn't normal.)
Problem 8. Let \((G, *)\) be a group. The **commutator** of \(a, b \in G\) is the element
\[
[a, b] = a * b * a^{-1} * b^{-1}.
\]
Let \(H \subset G\) be the subset consisting of all finite products\(^1\) of commutators.

(a) Show that \([a, b]^{-1} = [b, a]\). Deduce that \(H\) is a subgroup of \(G\).

(b) Verify the formula below for all \(g, a, b \in G\):
\[
g * [a, b] * g^{-1} = [g * a * g^{-1}, g * b * g^{-1}].
\]
Deduce that \(H\) is a normal subgroup of \(G\).

(c) Prove that the quotient group \(G/H\) is abelian.

\[
(a)\; [a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = (b^{-1})^{-1} (a^{-1})^{-1} b^{-1} a^{-1} = bab^{-1} a^{-1} = [b, a],
\]

which shows \(H\) is closed under inversion:
\[
([a_1, b_1] \ldots [a_N, b_N])^{-1} = [b_N, a_N] \ldots [b_1, a_1] \leq H.
\]

Also, \(e \in H\) by convention (allow the empty product \(N = 0\)).

Clearly \(H\) closed under \(*\):
\[
[a_1, b_1] \ldots [a_N, b_N] * [c_1, d_1] \ldots [c_M, d_M] \text{ is a product of finitely many commutators.}
\]

\[
\text{\footnotesize \[1\text{I.e., all expressions } [a_1, b_1] * \ldots * [a_N, b_N] \text{ for varying } N \text{ and } a_i, b_i \in G. \text{ This includes } e.\]}
\]

\[\text{CONT.} \quad \rightarrow\]
(b) \( g[a,b]g^{-1} = gaba^{-1}b^{-1}g \). On the other hand:

\[
[ga^{-1}, gb^{-1}] = gagg^{-1}gbg^{-1}(ga^{-1})^{-1}(gb^{-1})^{-1} = gagg^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = gaba^{-1}b^{-1}g^{-1}
\]

Follows that \( H \) is normal in \( G \):

\[
g[a_1, b_1] \cdots [a_n, b_n] g^{-1} = [ga_1^{-1}, gb_1^{-1}] \cdots [ga_n^{-1}, gb_n^{-1}] \in H
\]

(c) Since \( H \triangleleft G \), \( G/H \) has a group structure.

\( G/H \) is abelian \( \iff \) \( aH \circ bH = bH \circ aH \)  
\( \iff \) \( abH = baH, \forall a, b \in G \).

\( \iff \) \( (ab^{-1})a^{-1}b = H \),  
\( \iff \) \( b^{-1}a^{-1}ba \in H \),  
\( \iff \) \( [b^{-1}, a^{-1}] \subseteq H \),  
\( \iff \) certainly true: \( H \) contains all commutators (and finite products of such)
Problem 9. Consider the dihedral group $D_5$ of all symmetries of a pentagon centered at the origin. Recall that $D_5$ is generated by elements $r, s$ satisfying:

$$\text{ord}(r) = 5 \quad \text{ord}(s) = 2 \quad rs = sr^{-1}$$

(a) Write down its cardinality $|D_5|$. Is $D_5$ an abelian group?

(b) What is the order of the element $rs$?

(c) Prove the following two statements:

(i) The only two elements of $D_5$ commuting with $s$ are $e$ and $s$.

(ii) The only elements of $D_5$ commuting with $r$ are the powers of $r$.

\[\text{(a) } |D_5| = 10. \text{ D}_5 \text{ is not abelian since } rs = sr \neq sr^{-1} \text{ (otherwise, } r^2 = e, \text{ but ord}(r) = 5)\]

\[\text{(b) } (rs)^2 = (rs)(rs) = (sr^{-1})(rs) = s^2 = e, \text{ and } r = e \text{ (otherwise, } r = s, \text{ but they have diff. orders).}\]

This shows: rotation \reflect\, reflection.

\[\text{\textbf{ord}}(rs) = 2 \quad \text{i.e., } rs \text{ is a reflection (can also be seen by computing det}(rs) = -1)\]

\[\text{(c) } (i) \text{ Clearly both } e \text{ and } s \text{ commute with } s. \text{ The point is to show } \{e, s\} \text{ are the only elements of } D_5 \text{ with this property.}\]

- \underline{rotations:} Suppose $r^i s = sr^i \quad (0 \leq i < 5)$

This amounts to

(by cancellation law): $r^{-i}sr^i = s$, i.e. $r^{-i} = r^i = e$

in other words, $\text{ord}(r) = 5 | 2i$

Since $5$ is odd, $5 | i$. Therefore $i = 0$ since

Conclude $r^i = e$. \underline{cont.}
reflections: Suppose \( sr^i s = ssr^i \) \((0 \leq i < 5)\)

As above, \( i = 0 \)

\( ssr^{-i} \quad \overset{\text{r indic}}{\Rightarrow} \quad r^{-i} \) using \( s^2 = e \)

Conclude \( s r^i = s \).

\( \checkmark \)

(ii) Obviously all powers of \( r \) commute with \( r \), since \( \langle r \rangle \) is abelian \((r^m r^n = r^{m+n} = r^{n+m} = r^n r^m)\).

The point is the converse. Namely:

- rule out that any reflection \( sr^i \) commutes with \( r \).

Suppose: \( sr^i r = r sr^i \)

\( \overset{\text{r indic}}{\Rightarrow} \quad s r^{i+1} \quad \overset{\text{r indic}}{\Rightarrow} \quad s r^{i-1} \)

Cancellation law implies \( r = r^{-1} \), i.e. \( r^2 = e \),

— but \( \text{ord}(r) = 5 \). Contradiction.