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)

Problem #	Points (out of 10)
1	
2	
3	
4	
5	
6	
7	
8	
9	

Total (out of 90):

Problem 1. Let $(G, *)$ be a cyclic group of size 10. Choose a generator $a \in G$.

(a) Find the <u>order</u> 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 $a * \langle a^2 \rangle$ and $a * \langle a^5 \rangle$.

(a) Use that a^n has order $\dfrac{10}{GCD(10,n)}$.

– see table next page.

Shows a^n <u>generates</u> G for $n = 1, 3, 7, 9$. ← those <u>coprime</u> to 10.

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

$\langle a^5 \rangle = \{e, a^5\}$.

(c) $a * \langle a^2 \rangle = \{a, a^3, a^5, a^7, a^9\}$.

$a * \langle a^5 \rangle = \{a, a^6\}$.

TABLE (PROBLEM 1):

n	$\operatorname{ord}(a^n)$
0	1
1	10
2	5
3	10
4	5
5	2
6	5
7	10
8	5
9	10

Problem 2. Recall that $(\mathbb{Z}_{11}^{\times}, \bullet)$ 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:

[1] [2] [3] [4] [5] [6] [7] [8] [9] [10]

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

(c) List all the elements of the cosets $[2] \bullet \langle [4] \rangle$ and $[3] \bullet \langle [4] \rangle$.

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

$2^1 \equiv 2 \quad 2^2 \equiv 4 \quad 2^3 \equiv 8 \quad 2^4 \equiv 5 \quad 2^5 \equiv 10$

$2^6 \equiv 9 \quad 2^7 \equiv 7 \quad 2^8 \equiv 3 \quad 2^9 \equiv 6 \quad 2^{10} \equiv 1.$

(all modulo 11). – shows $\mathrm{ord}([2]) = 10$.

(b) Use the formula $\mathrm{ord}[2]^n = \dfrac{10}{\mathrm{GCD}(10,n)}$.
– see table next page.
Shows $[a]$ generates $\mathbb{Z}_{11}^{\times}$ for $a = 2, 6, 7, 8$.

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

and $\qquad = \{[2], [8], [10], [7], [6]\}.$

$[3] \bullet \langle [4] \rangle = \{[3], [1], [4], [5], [9]\}$
$= \langle [4] \rangle$ since $[3] \in \langle [4] \rangle$.

TABLE (PROBLEM 2):

a	$\text{ord}[a]$
1	1
2	10
3	5
4	5
5	5
6	10
7	10
8	10
9	5
10	2

EX $\text{ord}[3] = \text{ord}[2]^8 = \dfrac{10}{GCD(10,8)} = \dfrac{10}{2} = 5$

Problem 3. Recall that $(\mathbb{Z}_{15}, +)$ denotes the additive group of all residue classes modulo 15.

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

(b) Write down all elements of the two non-trivial subgroups of $\mathbb{Z}_{15}$.

(c) Explain why the quotient group $\mathbb{Z}_{15}/\langle [5] \rangle$ is isomorphic to $\mathbb{Z}_5$.

(a) Know $[x]$ generates $\mathbb{Z}_{15}$ iff $GCD(x, 15) = 1$.
In the interval $0 \leq x < 15$ we have $\underline{x = 1, 2, 4, 7, 8, 11, 13, 14}$.

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

$\langle [3] \rangle = \{[0], [3], [6], [9], [12]\}$ and
$\langle [5] \rangle = \{[0], [5], [10]\}$.

(c) $|\mathbb{Z}_{15}/\langle [5] \rangle| = \frac{15}{3} = 5$ prime.
Every group of order $p =$ prime is cyclic, and therefore isomorphic to $\mathbb{Z}_p$.

— or more concretely: $[1] + \langle [5] \rangle$ is a generator for $\mathbb{Z}_{15}/\langle [5] \rangle$.

a "<u>quotient</u> of <u>cyclic</u> <u>group</u> is <u>cyclic</u>".

$\mathbb{Z}_{15}/\langle [5] \rangle \cong \mathbb{Z}_5$.

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 $f : 65\mathbb{Z} \longrightarrow \mathbb{Z}_{91}$ 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 $\mathrm{im}(f)$.

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

see part (b).

(a) $65\mathbb{Z} \cap 91\mathbb{Z} = \mathrm{LCM}(65, 91)\mathbb{Z} = 455\mathbb{Z}$, $\boxed{M = 455}$

(b) $65\mathbb{Z} + 91\mathbb{Z} = \mathrm{GCD}(65, 91)\mathbb{Z} = 13\mathbb{Z}$, $\boxed{N = 13}$

- Euclid:

$$\begin{cases} 91 = 1 \cdot 65 + 26 \\ 65 = 2 \cdot 26 + 13 \\ 26 = 2 \cdot 13 \end{cases}$$

- gives: $\mathrm{LCM} = 5 \cdot 7 \cdot 13 = 455$

- check: $65 = 5 \cdot 13$, $91 = 7 \cdot 13$ (prime factors)

Back-substitution:

$N = 13 = 65 - 2(91 - 65) = 3 \cdot 65 + (-2) \cdot 91$ so may take:

$\boxed{x = 3, \ y = -2}$

(other solutions too!)

(c) $\mathrm{im}(f) = (65\mathbb{Z} + 91\mathbb{Z})/91\mathbb{Z}$

$= 13\mathbb{Z}/91\mathbb{Z}$

$\simeq \mathbb{Z}/7\mathbb{Z}$.

$\ker(f) = 65\mathbb{Z} \cap 91\mathbb{Z} = 455\mathbb{Z}$ has index

$[65\mathbb{Z} : \ker(f)] = |\mathrm{im}(f)| = \boxed{7}$.

First isomorphism Thm.

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

(a) Express α 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 α a cycle? If not, find its decomposition into disjoint cycles.

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

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

(ex. $9 \mapsto 3 \mapsto 3 \mapsto 3 \mapsto 4$ by the cycles in α)

(b) α takes $1 \mapsto 7 \mapsto 6 \mapsto 2 \mapsto 5 \mapsto 3 \mapsto 8 \mapsto 9 \mapsto 4 \mapsto 1$.

— so yes α is a 9-cycle:

$\alpha = (176253894)$.

(c) $\operatorname{ord}(\alpha) = \operatorname{length}(\alpha) = \boxed{9}$

$\operatorname{sign}(\alpha) = (-1)^{9-1} = \boxed{+1}$ — in other words α 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_3.

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.

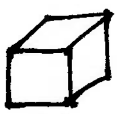
T (d) All subgroups of an abelian group are normal.

F (e) If G is any group, and $H \subset G$ is a normal subgroup, the following holds:

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

(a) FALSE. The group is isomorphic to A_4 which has 12 elements. ($|S_3| = 3! = 6$)

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



One can easily write down 24 rotational symmetries.

so $G \xrightarrow{\sim} S_4$.

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

$$\underset{\substack{\| \\ |G|^2}}{\operatorname{ord}(a,b)} = \operatorname{LCM}(\operatorname{ord} a, \operatorname{ord} b) : \underline{\text{divides}}\ |G|.$$

both divide $|G|$ (= common multiple) by LAGRANGE.

$\Rightarrow |G| = 1$, i.e. G must be $\underline{\text{trivial}}$.

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

CONT. $\longrightarrow$

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 quotients of $\mathbb{Z}$ are cyclic, but $\mathbb{Z} \times \mathbb{Z}$ admits $\underset{\text{(non-cyclic)}}{V_4 = \mathbb{Z}_2 \times \mathbb{Z}_2}$ as a quotient: $\dfrac{\mathbb{Z} \times \mathbb{Z}}{2\mathbb{Z} \times 2\mathbb{Z}}$.

(d) TRUE. If G abelian and $H \leqslant G$, then H must be normal: Have to check

$$g \in G \wedge h \in H \Longrightarrow g h g^{-1} \in H.$$

But $g h g^{-1} = h g g^{-1} = h \in H$ ✓

g, h commute (G abelian)

(e) FALSE. The direction $\Longrightarrow$ is true, but $\Longleftarrow$ is false. Therefore the statement $\Longleftrightarrow$ is altogether false.

+ Details:

$\Longrightarrow$ is true. Indeed we know subgroups of cyclic groups are cyclic, and if $G = \langle a \rangle$ then G/H is generated by the coset $a * H$.

$\Longleftarrow$ is false, however: $G = \mathbb{Z}_2 \times \mathbb{Z}_2$

Here $H = \{(a,a) : a \in \mathbb{Z}_2\} \leqslant G$.

$H \cong \mathbb{Z}_2$ 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

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

(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 $(12345) \circ H = H \circ (12345)$?

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

(b) There's no such f. For suppose $f : A_5 \to \{\pm 1\}$ is a homomorphism. Then $\forall$ 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 $[A_5 : H] = \frac{60}{3} = \boxed{20}$.

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

"socks & shoes"

— which shows H is closed under inversion:

$$([a_1,b_1]\cdots[a_N,b_N])^{-1} = [b_N,a_N]\cdots[b_1,a_1] \in H.$$

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

Clearly H closed under $*$:

$[a_1,b_1]\cdots[a_N,b_N] * [c_1,d_1]\cdots[c_M,d_M]$ is a product of finitely many commutators.

$\Rightarrow$ H is a subgroup.

[1] I.e., all expressions $[a_1, b_1] * \cdots * [a_N, b_N]$ for varying N and $a_i, b_i \in G$. This includes e.

CONT. $\longrightarrow$

(b) $g[a,b]g^{-1} = gaba^{-1}b^{-1}g$. On the other hand:

$$[gag^{-1}, gbg^{-1}] = gag^{-1}gbg^{-1}(gag^{-1})^{-1}(gbg^{-1})^{-1}$$

$$= ga\underbrace{g^{-1}g}_{e}b\underbrace{g^{-1}g}_{e}a^{-1}\underbrace{g^{-1}g}_{e}b^{-1}g^{-1} = gaba^{-1}b^{-1}g^{-1} \checkmark$$

– Follows that H is <u>normal</u> in G:

$$g[a_1,b_1]\cdots[a_N,b_N]g^{-1} = [ga_1g^{-1}, gb_1g^{-1}]\cdots[ga_Ng^{-1}, gb_Ng^{-1}] \in H$$

(c) Since $H \triangleleft G$, G/H has a <u>group</u> structure.

G/H is <u>abelian</u> $\iff aH \bullet bH = bH \bullet aH$ (for all $a,b \in G$)

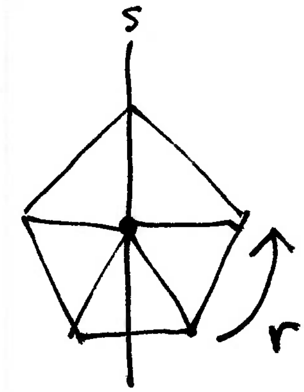
$\iff abH = baH, \ \forall a,b \in G.$

$\iff (ab)^{-1}ba \in H$, —"—

$\iff b^{-1}a^{-1}ba \in H$, —"—

$\iff \underbrace{[b^{-1}, a^{-1}] \in H, \text{ —"—}}$

– 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:

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

(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.

cf. the "commutation relation"

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

(b) $(rs)^2 = (rs)(rs) = (sr^{-1})(rs) = s^2 = e$,
and $rs \neq e$ (otherwise $r = s$, but they have diff. orders.
rotation reflection

This shows:

$\boxed{\mathrm{ord}(rs) = 2}$ i.e., rs is a reflection (can also be seen by computing $\det(rs) = -1$)

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

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

This amounts to (by cancellation law): $r^{-i} = r^i$, i.e. $r^{2i} = e$

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

Since 5 is odd, $5 \mid i$. Therefore $i = 0$ since $0 \leq i < 5$.
Conclude $r^i = e$.

CONT. $\longrightarrow$

• <u>reflections</u>: Suppose $sr^i s = ssr^i$ $(0 \le i < 5)$

$$\begin{array}{ccc} sr^i s & = & ssr^i \\ \| & & \| \\ ssr^{-i} & & r^i \\ \| & & \\ r^{-i} & & \end{array}$$

using $s^2 = e$

As above, $i = 0$.

Conclude $sr^i = s$.

✓

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

the point is the converse. Namely:

• <u>rule out</u> that any <u>reflection</u> sr^i <u>commutes</u> with r.

Suppose:

$$\begin{array}{ccc} sr^i r & = & rsr^i \\ \| & & \| \\ sr^{i+1} & & sr^{i-1} \end{array}$$

Cancellation law implies $r = r^{-1}$, i.e. $r^2 = e$.

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