NAME : Key

Math 31

Midterm 2
August 7, 2017

Prof. Pantone

INSTRUCTIONS: This is a closed book exam and no notes are allowed. You are not to provide or receive help from any outside source during the exam except that you may ask the instructor for clarification of a problem. You have 120 minutes and you should attempt all problems.

- Print your name in the space provided.
- Calculators or other computing devices are not allowed.
- Except when indicated, you must show all work and give justification for your answer. **A correct answer with incorrect work will be considered wrong.**

All work on this exam should be completed in accordance with the Dartmouth Academic Honor Principle.

TIPS:

- You don't have numerically expand all answers.
- Use scratch paper to figure out your answers and proofs before writing them on your exam.
- Work cleanly and neatly; this makes it easier to give partial credit.

Problem	Points	Score
1	20	
2	20	
3	12	
4	12	
5	12	
6	12	
7	12	
Total	100	

Section 1: True/False.

1. (20) Choose the correct answer. *No justification is required for your answers. No partial credit will be awarded.*

(a) The group $A_3 \times \mathbb{Z}_4$ has an element of order 8.

$|A_3 \times \mathbb{Z}_4| = 3 \cdot 4 = 12$

8 does not divide 12.

True [✓ False]

(b) All right cosets of a subgroup H in a group G have the same size.

[✓ True] False

(c) Every permutation can be written as the product of transpositions.

[✓ True] False

(d) If k evenly divides $|G|$, then there exists a subgroup H of G such that $|H| = k$.

(converse of Lagrange's Theorem)

True [✓ False]

(e) If G is an infinite group, then G has subgroups of all positive integer orders.

Ex: $(\mathbb{Z}, +)$

True [✓ False]

(f) Let G be a group. Then $|G|$ is prime if and only if G is cyclic.

$\mathbb{Z}_{10}$ is cyclic

True [✓ False]

(g) If G is abelian, then $G/Z(G)$ is cyclic.

If G is abelian, then $Z(G)=G$, and $G/Z(G)$ is a group of order 1.

[✓ True] False

(h) If $G/Z(G)$ is cyclic, then G is abelian.

Proved on HW

[✓ True] False

(i) $\mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_{20}$

$\gcd(4,5)=1$

[✓ True] False

(j) If $\pi \in S_n$, then $o(\pi)$ divides n.

Ex: $(1\ 2\ 3) \in S_4$ has order 3.

True [✓ False]

Section 2: Short Response.

2. (20) *Justify all answers unless otherwise stated.*

(a) What are the distinct right cosets of $\{1, -1\}$ in $(\mathbb{R} \setminus \{0\}, \cdot)$? Give a group that is isomorphic to $(\mathbb{R} \setminus \{0\})/\{1, -1\}$. (You do not need to justify the isomorphism.)

Compressing by $\{-1, 1\}$ "forgets" the sign of the real #. a and b are in the same coset if $ab^{-1} = 1$ or $= -1$

↑ same # $a=b$ ↑ $a=-b$.

So the right cosets are (set $H = \{-1, 1\}$):

$$(\mathbb{R}\setminus\{0\}, \cdot)/H = \{Ha : a \in \mathbb{R}^+\}$$

$$(\mathbb{R}\setminus\{0\}, \cdot)/H \cong (\mathbb{R}^+, \cdot)$$

(b) Give a cyclic subgroup of order four and a non-cyclic subgroup of order four of S_4.

$\langle (1\,2\,3\,4) \rangle$ is cyclic

(generated by an element of order 4)

$\langle (12), (34) \rangle = \{1, (12), (34), (12)(34)\}$

is not cyclic, has order 4

(isomorphic to K_4)

(c) What is the largest order of an element in S_7? In ~~S_10~~? S_{10}

S_7 options

7-cycle → order 7

6,1 → 6

5,2 → 10

5,1,1 → 5

4,3 → $\boxed{12}$

4,2,1 → 4

4,1,1,1 → 4

3s+2s+1s → ≤ 6

S_{10} options

10 → 10

9,1 → 9

8,2 → 8

7,3 → 21

7,2,1 → 14

7,1s → 7

6,(4s/3s/2s/1,s) → ≤ 12

5,5 → 5

5,4,1 → 20

5,3,2 → $\boxed{30}$

4s/3s/2s/1,s → ≤ 12

(d) Write the permutation below in: one-line notation, disjoint cycle notation, and as a product of transpositions. What is its order?

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 5 & 2 & 8 & 7 & 6 & 10 & 4 & 9 & 3 \end{pmatrix}$$

one line: 1,5,2,8,7,6,10,4,9,3

This is in my lecture notes, but maybe I didn't define it in class.

disjoint cycles: (1)(2 5 7 10 3)(4 8)(6)(9)

not necessary

prod of trans: [illegible]

(2 5)(5 7)(7 10)(10 3)(4 8)

order: lcm(1,2,5) = 10

Section 3: Free Response.

You must show all work to receive credit. If you need more space you may use the back of the page. You must clearly indicate on the front of the page that there is more work on the back of the page. Please work neatly.

3. (12) Let G be a group of size at least two. Prove that if G has no proper non-trivial subgroups, then $|G|$ is prime.

Proof: Let $|G| \geq 2$.

Let x be a non-identity element of G.
(exists because $|G| > 1$)

We must have $o(x) = |G|$, because otherwise $\langle x \rangle$ is a proper non-trivial subgroup of G.

We also must have $o(x)$ prime: if not prime, then $o(x)$ is divisible by a number $k \neq 1, o(x)$. Now $\langle x^{o(x)/k} \rangle$ would be a proper non-trivial subgroup of G.

If $|x| = \infty$, then $\langle x^2 \rangle$ is a proper non-trivial subgroup.

Hence $o(x)$ is prime. But $o(x) = |G|$!
So $|G|$ is prime. ∎

4. (12) Suppose that G is a group, that $N \lhd G$, and that G/N abelian. Prove that for all $a, b \in G$, $aba^{-1}b^{-1} \in N$.

Proof:

Suppose G is a group, $N \lhd G$, and G/N abelian.

Let $a, b \in G$ be arbitrary.

Since G/N is abelian:

$$(Na)(Nb) = (Nb)(Na).$$

This implies:

$$(Nab) = (Nba).$$

Recall that for two cosets Nx and Ny, $Nx = Ny$ iff $xy^{-1} \in N$.

Applying this fact tells us that

$$\begin{array}{c} (ab)(ba)^{-1} \in N \\ \parallel \\ aba^{-1}b^{-1} \in N. \end{array}$$

■

5. (12) Prove that $(\mathbb{Z}, +)$ has infinitely many subgroups that are isomorphic to it.

Claim: For all positive integers k,

$\mathbb{Z} \cong k\mathbb{Z}$ (operation is always addition in this answer)

Proof: Define $\varphi : \mathbb{Z} \to k\mathbb{Z}$ by $\varphi(n) = kn$.

Hom? $\varphi(m+n) = k(m+n) = km + kn$

$\varphi(m) + \varphi(n) = km + kn$. ✓ yes

Injective? Suppose $\varphi(n_1) = \varphi(n_2)$. Then $kn_1 = kn_2$ which implies $n_1 = n_2$. ✓ yes

Surjective? Let $x \in k\mathbb{Z}$. Then x has the form $k \cdot m$ for some integer m. This implies that $\varphi(m) = k \cdot m = x$. ✓ yes

Hence, φ is a bijective homomorphism, aka and isomorphism. □

There are an infinite # of groups of the form $k\mathbb{Z}$, and we proved in class that they are all subgroups of $\mathbb{Z}$.

6. (12) Let $\varphi : G \to H$ be an onto homomorphism. Show that if G is cyclic, so is H.

Proof:

Let $\varphi : G \to H$ be a surjective homomorphism.
Assume G is cyclic, i.e., $\exists x \in G$ such that $G = \langle x \rangle$.

Claim: $H = \langle \varphi(x) \rangle$.

Proof of Claim:

We will show that every element in H has the form $\varphi(x)^k$ for some k.

Let $h \in H$. Since φ is surjective, there exists $g \in G$ such that $\varphi(g) = h$.
As $G = \langle x \rangle$, $g = x^\ell$ for some ℓ. Therefore

$$h = \varphi(g) = \underbrace{\varphi(x^\ell) = (\varphi(x))^\ell}_{\text{property of homomorphisms}}$$

Since h was arbitrary, this shows that every element of H is a power of $\varphi(x)$. Therefore $H = \langle \varphi(x) \rangle$. ∎

7. (12) Prove that for any group G, it is not possible that $[G : Z(G)]$ is prime. (*Hint:* Consider $G/Z(G)$.)

Proof:

Let G be a group. Assume toward a contradiction that $[G : Z(G)]$ is prime.

$G/Z(G)$ is a group because $Z(G) \lhd G$ for all groups G.

Moreover $|G/Z(G)| = [G : Z(G)]$ (def. of index) so $|G/Z(G)|$ is prime.

All groups of prime order are cyclic.

If $G/Z(G)$ is cyclic then G is abelian (homework).

Yet, if G is abelian, then $Z(G) = G$!

This implies $[G : Z(G)] = 1$, which is not prime. This is a contradiction. ■