NAME : Key

Math 31

Midterm 2
August 27, 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 180 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	24	
2	8	
3	8	
4	8	
5	10	
6	10	
7	8	
8	8	
9	8	
10	8	
11	0	
Total	100	

Section 1: True/False.

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

(a) Let $n \geq 4$. The ideal generated by the element 2 in $(\mathbb{Z}_n, \oplus, \otimes)$ is maximal.

True (False)

If n is odd then $2\mathbb{Z}_n = \mathbb{Z}_n$.

(b) The quaternion group Q_8 has an element of order 8.

True (False)

(c) Let G be a group and let $H \leq G$. If $[G : H] = 2$ then $H \lhd G$.

Proved in class.

(True) False

(d) Let $\varphi : G \to K$ be a group homomorphism. All normal subgroups of G contain $\ker(\varphi)$.

Ex: Trivial map $\varphi(g) = e_K$, $\forall g \in G$,
If G is abelian, all subgps are normal but $\ker(\varphi) = G$.

True (False)

(e) Up to isomorphism there are exactly five finite abelian groups of order 48.

$48 = 2^4 \cdot 3$

5 partitions of 4
1 partition of 1

$5 \cdot 1 = 5$.

(True) False

(f) Every infinite abelian group has at least one element of infinite order.

$(P(\mathbb{Z}), \Delta)$

True (False)

(g) Every infinite cyclic group has at least one element of infinite order.

(the generator, but also everything except the identity).

(True) False

(h) A finite group is abelian if and only if all of its subgroups are normal.

Ex: Q_8.

True (False)

(i) An integral domain is a ring in which all non-units are zero-divisors.

True (False)

(j) S_{10} has an element of order 21.

$(1\,2\,3)(4\,5\,6\,7\,8\,9\,10)$

$\operatorname{lcm}(3,7) = 21.$

(True) False

(k) All prime ideals are maximal.

All maximal ideals are prime.

True (False)

(l) Every polynomial of degree 2 in $\mathbb{C}[X]$ is reducible.

(True) False

(quadratic equation)

Section 2: 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.

2. (8) Let G be a group of order pq, for primes p and q. Show that all proper subgroups of G are cyclic.

(We do not need to assume distinct primes.)

Proof: Let $H \leq G$. By Lagrange's Theorem, $|H|$ divides pq. So must be 1, p, or q.

There is only one group of each prime order (up to isomorphism) and it's cyclic.

There is only one group of order 1, and it's cyclic.

∎

3. (8) Which of the four maps below are group homomorphisms? (Either show briefly that they are, or give an example that shows they aren't.)

(a) $G = (\mathbb{Q}, +)$, $\varphi : G \to G$ given by $\varphi(x) = |x|$

No

$\varphi(-1+1) = |-1+1| = |0| = 0.$

$\varphi(-1) + \varphi(1) = |-1| + |1| = 1 + 1 = 2.$ $\quad 2 \neq 0.$

(b) $G =$ the group of polynomials with integer coefficients under addition of polynomials, $\varphi : G \to G$ given by $\varphi(p(x)) = p'(x)$ (where $p'(x)$ is the usual derivative of a polynomial from calculus)

Yes

$\varphi(p(x)+q(x)) = (p(x)+q(x))' = p'(x) + q'(x)$ (by calculus)

$\varphi(p(x)) + \varphi(q(x)) = p'(x) + q'(x)$

(c) $G = (\mathbb{R}^+, \cdot)$, $H = (\mathbb{R}, +)$, $\varphi : G \to H$ given by $\varphi(x) = \log_3(x)$.

Yes

$\varphi(x \cdot y) = \log_3(x \cdot y) = \log_3(x) + \log_3(y)$

$\varphi(x) + \varphi(y) = \log_3(x) + \log_3(y)$

(d) $G =$ the group of all 2×2 matrices with real entries under addition of matrices, $H = (\mathbb{R}, +)$, $\varphi : G \to H$ given by $\varphi(M) =$ the product of the entries of M.

No

$\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right) = 1$

$1 \neq 0$

$\varphi\left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) = 0 + 0 = 0$

4. (8) Let R be a commutative ring with 1 and let $a \in R$. Prove that $aR = R$ if and only if a is a unit. (Recall that aR is the ideal generated by a.)

Proof:

($\Rightarrow$)

Assume $aR = R$. Since $1 \in R$, $\exists\, r \in R$ such that $ar = 1$. As R is commutative, $ra = 1$ as well. Thus a is a unit.

($\Leftarrow$)

Assume a is a unit. Then $\exists\, b \in R$ such that $ab = 1$. Since $ab \in aR$, we have $1 \in aR$. An ideal contains 1_R iff it equals R (from class), so $aR = R$. ∎

5. (10) Let $\varphi : G \to K$ be an onto homomorphism. Let $J \lhd K$. Prove that there exists a normal subgroup H of G such that $G/H \cong K/J$.

Proof: φ gives us a mechanism to get from elements of G to elements of K, which we need to get started.

We will define $\psi: G \to K/J$, show it's an onto hom, then conclude by 1st Iso Thm that $G/\ker(\psi) \cong K/J$.

We need to map *from* elements of G *to* cosets of the form Jk. The only bridge we have between G and K is φ. So, define $\psi: G \to K/J$ by

$$\psi(g) = J\cdot\varphi(g)$$

Now, $\psi(g_1g_2) = J\varphi(g_1g_2) = J(\varphi(g_1)\varphi(g_2))$

and $\psi(g_1)\psi(g_2) = (J\varphi(g_1))(J\varphi(g_2)) = J(\varphi(g_1)\varphi(g_2))$

Thus, ψ is a homomorphism.

Why is ψ onto? Let Jk be an arbitrary element of K/J. As φ is onto, $\exists g \in G$ such that $\varphi(g) = k$. Thus, $\psi(g) = J\varphi(g) = Jk$. As Jk was arbitrary, ψ is onto.

Thus, by the 1st Iso Thm, $G/\ker(\psi) \cong K/J$, and so $\ker(\psi)$ is the desired subgroup. ∎

For funsies: what is $\ker(\psi)$?

$\ker(\psi) = \{g \in G : \psi(g) = e_{K/J}\}$
$= \{g \in G : J\varphi(g) = J\}$
$= \{g \in G : \varphi(g) \in J\} = \varphi^{-1}(J)$.

6. (10) (Be sure to justify your answers.)

(a) Is $\mathbb{Q}[X]/(X^2-1)$ an integral domain?

From Chapter 17, $\mathbb{Q}[X]/(X^2-1)$ is an integral domain iff $I=(X^2-1)$ is a prime ideal, so this is what we'll check.

Note that X^2-1 factors as $(X+1)(X-1)$ in $\mathbb{Q}[X]$. (Why? 1 is a root, so $X-1$ divides it. -1 is a root, so $X+1$ divides it.)

Also, $X+1 \notin I$ and $X-1 \notin I$, since everything in (X^2-1) has degree at least 2 (since $\mathbb{Q}$ is an integral domain).

Since $X+1 \notin I$, $X-1 \notin I$, but their product is, we have (X^2-1) not prime, so $\mathbb{Q}[X]/(X^2-1)$ not an integral domain.

(b) Is $\mathbb{Q}[X]/(X^2+1)$ a field?

From Chapter 17, $\mathbb{Q}[X]/(X^2+1)$ is a field iff $I=(X^2+1)$ is a maximal ideal. From Chapter 19 or 20, (X^2+1) is maximal in $\mathbb{Q}[X]$ iff it is irreducible in $\mathbb{Q}[X]$. For all $q \in \mathbb{Q}$, $q^2+1>0$, so X^2+1 has no roots in $\mathbb{Q}$. By a theorem that works for degree 2 or 3 polynomials, it is thus irreducible in $\mathbb{Q}[X]$. Thus, as outlined above, $\mathbb{Q}[X]/(X^2+1)$ is a field.

7. (8) Find the right cosets of the subgroup $H = \{(0,0),(2,0),(0,2),(2,2)\}$ in $\mathbb{Z}_4 \times \mathbb{Z}_4$ (under addition).

$|\mathbb{Z}_4 \times \mathbb{Z}_4| = 16$, $|H| = 4$, so we expect 4 right cosets.

One is the identity

(1) $H = H + (0,0) = \{(0,0),(2,0),(0,2),(2,2)\}$.

To find a new one, pick any of the 16 elements not already spoken for.

(2) $H + (1,0) = \{(0,0)+(1,0),\ (2,0)+(1,0),\ (0,2)+(1,0),\ (2,2)+(1,0)\}$

$= \{(1,0),(3,0),(1,2),(3,2)\}$.

Repeat.

(3) $H + (0,1) = \{(0,1),(2,1),(0,3),(2,3)\}$

Repeat.

(4) $H + (1,1) = \{(1,1),(3,1),(1,3),(3,3)\}$.

Done!

8. (8) Show that the group $(\mathbb{Q}^+, \cdot)$ is not cyclic.

Proof: Assume toward a contradiction that $(\mathbb{Q}^+, \cdot) = \langle x \rangle$ for some $x \in \mathbb{Q}^+$. Since $e_{(\mathbb{Q}^+, \cdot)} = 1$, we can't have $x = 1$.

If $x > 1$, then the elements of $(\mathbb{Q}^+, \cdot)$ listed from smallest to largest are

$$\left\{ \ldots, \frac{1}{x^3}, \frac{1}{x^2}, \frac{1}{x}, 1, x, x^2, x^3, \ldots \right\}$$

If $x < 1$, then the elements of $(\mathbb{Q}^+, \cdot)$ listed from smallest to largest are

$$\left\{ \ldots, x^3, x^2, x, 1, \frac{1}{x}, \frac{1}{x^2}, \frac{1}{x^3}, \ldots \right\}$$

In the first case, $\frac{1+x}{2}$ is an element of $\mathbb{Q}^+$ such that $1 < \frac{1+x}{2} < x$, and so it's not in our list.

In the second case, $\frac{1+x}{2}$ is still a missing element, but this time $x < \frac{1+x}{2} < 1$.

Either way, we're missing $\frac{1+x}{2}$, a contradiction. So, $(\mathbb{Q}^+, \cdot)$ is not cyclic. ∎

(Really, we can assume without loss of generality that $x > 1$ because if x is a generator, so is $x^{-1} = \frac{1}{x}$.)

9. (8) Find, up to isomorphism, all finite abelian groups of order 600.

$600 = 2 \cdot 300 = 2^2 \cdot 150 = 2^3 \cdot 75$
$= 2^3 \cdot 3 \cdot 5^2$.

(Abelian) Groups of order 8: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$

order 3: $\mathbb{Z}_3$

order 25: $\mathbb{Z}_{25}$, $\mathbb{Z}_5 \times \mathbb{Z}_5$

} by Fundamental Theorem.

# of partitions of 3 = 3
1 = 1
2 = 2,

So $3 \cdot 1 \cdot 2 = 6$ groups.

(1) $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
(2) $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
(3) $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
(4) $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$
(5) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}$
(6) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$.

10. (8) Let $\varphi : R \to S$ be a ring homomorphism. Show that if J is a prime ideal in S then $\varphi^{-1}(J)$ is a prime ideal in R. (You may assume that $\varphi^{-1}(J)$ is an ideal in R.)

Proof:

Assume J is a prime ideal in S. So, if $s_1 s_2 \in J$ then either $s_1 \in J$ or $s_2 \in J$ (or both).

Let $I = \varphi^{-1}(J)$. We are given that I is an ideal of R.

To show that I is a prime ideal of R, we need to show that whenever $r_1 r_2 \in R$ we must have $r_1 \in R$ or $r_2 \in R$ (or both).

So, to that end, assume $r_1 r_2 \in I$. Clearly we have to use φ at some point... now is that time.

$\varphi(r_1 r_2) = \varphi(r_1)\varphi(r_2)$.

Since $I = \varphi^{-1}(J)$ (by definition) $\varphi(r_1 r_2) \in J$.

Thus $\varphi(r_1) \cdot \varphi(r_2) \in J$.

Thus $\varphi(r_1) \in J$ or $\varphi(r_2) \in J$ (or both) b/c J is prime.

Thus $r_1 \in \varphi^{-1}(J)$ or $r_2 \in \varphi^{-1}(J)$ (or both)

$\varphi^{-1}(J) = I$

Hence I is prime. ∎

11. (0) **Bonus:** *(3 points)* Tell me a little bit about how you prepared for this class (what were your study techniques, did you cram or spread out the work, etc.) What worked for you and what didn't? This will help me give advice to future classes.