Amherst College
Department of Mathematics and Statistics

MATH 350 | FINAL EXAM | FALL 2019

NAME: Solutions

Read This First!

- Keep cell phones off and out of sight.
- Do not talk during the exam.
- You are allowed one page of notes, front and back. No other books, notes, calculators, cell phones, communication devices of any sort, webpages, or other aids are permitted.
- Please read each question carefully. Show **ALL** work clearly in the space provided. There is an extra page at the back for additional scratchwork.
- In order to receive full credit on a problem, solution methods must be complete, logical and understandable.

Grading - For Instructor Use Only

Question:	1	2	3	4	5	6	7	8	9	Total
Points:	6	12	9	12	10	8	12	6	10	85
Score:										

This page intentionally left blank. You may use it for scratchwork or to continue answers to any question (note clearly on the original page if you do so).

1. [6 points] Let R be a ring, and I an ideal in R. Prove that the quotient ring R/I is commutative if and only if $xy - yx \in I$ for all $x, y \in R$.

~~Suppose R/I is~~

Given $x, y \in R$, observe that

$I+x$ & $I+y$ commute in R/I

iff $(I+x)(I+y) = (I+y)(I+x)$

iff $I + xy = I + yx$ (defn of mult. in R/I)

iff $xy - yx \in I$ (coset criterion).

Hence R/I is commutative

$\Leftrightarrow \forall x, y \in R$, $I+x$ & $I+y$ commute

$\Leftrightarrow \forall x, y \in R$, $xy - yx \in I$,

as desired.

This page intentionally left blank. You may use it for scratchwork or to continue answers to any question (note clearly on the original page if you do so).

2. (a) [4 points] List all the elements of the symmetric group S_3, using notation of your choice.

(based on "suggested problem" 1.2.5 from PSet 1)

$1_{[3]}$, $(1,2)$, $(1,3)$, $(2,3)$,

$(1,2,3)$, $(1,3\,2)$.

(b) [4 points] Which elements from part (a) are in the alternating group A_3?

even perms: $1_{[3]}$, $(1,2,3)$, $(1,3\,2)$.

(c) [4 points] Let $f = (1\ 2\ 3)$. Determine the centralizer $C_{S_3}(f)$ of f in S_3.

(Recall that the centralizer of f is the set of all elements of the group that commute with f.)

$(1,2,3)\cdot 1_{[3]} = (1,2,3)$ & $1_{[3]}(1,2,3) = (1,2,3)$ $\Rightarrow$ $1_{[3]} \in C(f)$

$(1,2,3)(1,2) = (1,3)$ & $(1,2)(1,2,3) = (2,3)$ $\Rightarrow$ $(1,2) \notin C(f)$

$(1,2,3)(1,3) = (2,3)$ & $(1,3)(1,2,3) = (1,2)$ $\Rightarrow$ $(1,3) \notin C(f)$

$(1,2,3)(2,3) = (1,2)$ & $(2,3)(1,2,3) = (1,3)$ $\Rightarrow$ $(2,3) \notin C(f)$

$(1,2,3)$ ~~(1,2,3)~~ commutes w/ itself $\Rightarrow$ $(1,2,3) \in C(f)$

$(1,2,3)(1,3,2) = 1_{[3]}$ & $(1,3,2)(1,2,3) = 1_{[3]}$ $\Rightarrow$ $(1,3,2) \in C(f)$

So $C_{S_3}(f) = \{1_{[3]}, (1,2,3), (1,3,2)\}$ (aka. $\langle f \rangle$, aka A_3).

alternate quick argument: note $\langle f \rangle \subseteq C(f)$ & $|C(f)|$ is 1, 2, 3, or 6 (Lagrange). So $|\langle f \rangle| = 3$ & $C(f) \neq S_3$ (since $(1,2) \notin C(f)$) implies $C(f) = \langle f \rangle$

This page intentionally left blank. You may use it for scratchwork or to continue answers to any question (note clearly on the original page if you do so).

3. Let $\phi : R \to S$ be a ring homomorphism.

(a) [4 points] Define the *kernel* of ϕ, denoted $\ker\phi$, and prove that it is an ideal.

$\ker\varphi = \{a \in R : \varphi(a) = 0_S\}$.

nonempty: $\varphi(0_R) = 0_S$ (property of ring hom)
so $0_R \in \ker\varphi$.

closure under $-$:
Suppose $a, b \in \ker\varphi$.
Then $\varphi(a-b) = \varphi(a) - \varphi(b)$ (property of ring hom)
$= 0_S - 0_S$ ($a, b \in \ker\varphi$)
$= 0_S$
so $a-b \in \ker\varphi$.

sticky property:
if $a \in \ker\varphi$ & $r \in R$, then
$\varphi(ar) = \varphi(a)\varphi(r)$ (defn of ring hom.)
$= 0_S \cdot \varphi(r)$
$= 0_S$
& $\varphi(ra) = \varphi(r)\varphi(a)$
$= \varphi(r) \cdot 0_S$
$= 0_S$
Hence $ar \in \ker\varphi$ & $ra \in \ker\varphi$. ie $\ker\varphi$ is sticky.

As proved in class, these three properties imply that $\ker\varphi$ is an ideal.

(continued on reverse)

(b) [5 points] Assume that R is a commutative ring with unity, and S is an integeral domain. Prove that either $\ker \phi = R$ or $\ker \phi$ is a *prime* ideal.

(Recall: An integral domain is a commutative ring with unity with at least two elements and no zero divisors. A prime ideal is a ideal $I \neq R$ such that for all $a, b \in R$, if $ab \in I$ then either $a \in I$ or $b \in I$, or both.)

↯ Suppose that $\ker\varphi \neq R$ and $\ker\varphi$ is not prime.

Then $\exists\, a, b \in R$ s.t. $ab \in \ker\varphi$ but $a \notin \ker\varphi$ & $b \notin \ker\varphi$.

Then $\varphi(ab) = 0_S$ (defn of $\ker\varphi$)

$\Rightarrow \varphi(a)\varphi(b) = 0_S$. ($\varphi$ is a hom.).

Now $\varphi(a)$ & $\varphi(b)$ are nonzero since $a, b \notin \ker\varphi$.

Thus $\varphi(a)$ ~~is a~~ & $\varphi(b)$ are zero-divisors.

But S is an integral domain, so it has no zero-divisors; this is a contradiction. ↯

Hence either $\ker\varphi = R$ or $\ker\varphi$ is prime.

4. Suppose that G is a finite group, and $g \in G$ is an element of order 9.

(a) [4 points] Prove that $|G|$ is divisible by 9.

$|\langle g \rangle| = o(g) = 9$, & $\langle g \rangle \leq G$.

So by Lagrange's thm, $9 \mid |G|$.

(b) [5 points] Prove that for all integers n, $g^n = e_G$ if and only if $9 \mid n$.

Suggestion: For the "only if" direction, use the division algorithm for $\mathbb{Z}$.

"$\Rightarrow$" Suppose that $g^n = e_G$. By divn. algo for $\mathbb{Z}$, $\exists\, q, r \in \mathbb{Z}$ w/ $0 \leq r < 9$ & $n = 9q + r$.

Thus $e_G = g^n = (g^9)^q \cdot g^r = e_G^q \cdot g^r = g^r$.

Now since $g^r = e_G$ & $r < o(g)$, r can't be positive ($o(g)$ is the minimum positive integer m s.t. $g^m = e_G$).

Hence $r = 0$ & $n = 9q$, hence $9 \mid n$.

"$\Leftarrow$" Suppose $9 \mid n$. Then $n = 9q$ for some $q \in \mathbb{Z}$.

Then $g^n = (g^9)^q = e_G^q = e_G$.

(continued on reverse)

(c) [3 points] Determine $o(g^2)$ and $o(g^3)$.

$(g^2)^m = e_G \iff 9 \mid 2m$

$\iff 9 \mid m$ (since $\gcd(2,9)=1$)

so the smallest such m is 9.

$o(g^2) = 9$

$(g^3)^m = e_G \iff 9 \mid 3m$

$\iff 3 \mid m$

so similarly

$o(g^3) = 3$.

5. Let $R = \mathbb{Z} \times \mathbb{Z}$, and let $I = \{(2m, 3n) : m, n \in \mathbb{Z}\}$.

("suggested problem" 18.1.24 from PSet 11)

(a) [4 points] Prove that I is an ideal in R.

nonempty: $(0,0) \in I$ (use $m=0, n=0$).

closed under $-$: For any two elements $(2m,3n)$ & $(2m',3n') \in I$,

$(2m,3n) - (2m',3n')$

$= (2(m-m'), 3(n-n'))$

$= (2m'', 3n'')$ where $m''=m-m'$ & $n''=n-n'$

$\in I$.

stickiness: For any $(2m,3n) \in I$ & $(a,b) \in R$,

$(a,b)(2m,3n) = (2m,3n)(a,b) = (2am, 3bn)$

$= (2m', 3n')$ where $m'=am$ & $n'=bn$,

$\in I$,

so I is sticky.

Hence I is an ideal.

(continued on reverse)

(b) [2 points] Is I a principal ideal? Briefly justify your answer.

Yes

$$I = \{ (2,3)\cdot(m,n) : m,n \in \mathbb{Z} \}$$
$$= \{ (2,3)\cdot r : r \in \mathbb{Z}\times\mathbb{Z} \}$$
$$= \langle (2,3) \rangle.$$

(c) [2 points] Is I a prime ideal? Briefly justify your answer.

No

$(1,3)$ & $(2,1) \notin I$,

but $(1,3)\cdot(2,1) = (2,3) \in I$.

(d) [2 points] Is I a maximal ideal? Briefly justify your answer.

No

because if it were max'l it would also be prime.

(proved in class: in a CR w/1, max'l $\Rightarrow$ prime).

6. Let G be a group, H a subgroup of G, and g an element of G. Define

(based on prob. 2.6.27, from PSet 4)

$$K = gHg^{-1} = \{ghg^{-1} : h \in H\}.$$

(a) [4 points] Prove that $K \leq G$ (K is a subgroup of G).

nonempty: $e_G \in H$ (H is a subgroup)

so $g e_G g^{-1} = gg^{-1} = e_G \in K$.

closure under mult.

For any two elements gh_1g^{-1} & $gh_2g^{-1} \in K$ (where $h_1, h_2 \in H$),

$$(gh_1g^{-1}) \cdot (gh_2g^{-1}) = gh_1(g^{-1}g)h_2g^{-1}$$
$$= g(h_1h_2)g^{-1}$$

& $h_1h_2 \in H$ since H is a subgroup (hence closed under mult.)

so this product is in $gHg^{-1} = K$.

closure under inverse For any $ghg^{-1} \in K$,

$$(ghg^{-1})^{-1} = (g^{-1})^{-1}h^{-1}g^{-1}$$
$$= gh^{-1}g^{-1}$$

& $h^{-1} \in H$ (H is closed under inverse)

so $(ghg^{-1})^{-1} \in K$.

Hence K is a subgroup of G.

(continued on reverse)

(b) [4 points] Prove that $K \cong H$.

Define

$$\varphi : H \longrightarrow K$$

by

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

This is a group homomorphism since

$$\begin{aligned}\varphi(h_1h_2) &= gh_1h_2g^{-1} \\ &= gh_1g^{-1}gh_2g^{-1} \\ &= \varphi(h_1)\varphi(h_2).\end{aligned}$$

φ is surjective since $\forall k \in K$, $k = ghg^{-1}$ for some $h \in H$, so $k = \varphi(h)$.

φ is injective since $\forall h_1, h_2 \in H$,

$$\begin{aligned}&\varphi(h_1) = \varphi(h_2) \\ \Rightarrow\ & gh_1g^{-1} = gh_2g^{-1} \\ \Rightarrow\ & g^{-1}(gh_1g^{-1})g = g^{-1}(gh_2g^{-1})g \\ \Rightarrow\ & e_Gh_1e_G = e_Gh_2e_G \\ \Rightarrow\ & h_1 = h_2.\end{aligned}$$

So φ is a bijective group homomorphism, i.e. a group isomorphism. Hence $H \cong K$.

7. Let F be a field, and let $F[X]$ denote the polynomial ring over F.

(a) [4 points] Prove that $F[X]$ is an integral domain. You may assume F[X] is commutative. w/unity.

Recall that $\forall p(x) \neq 0_F$, $\deg(p(x)) \geq 0$,
(by convention, $\deg(0_F) = -\infty$)
& $\forall p(x), q(x) \in F[X]$,
$$\deg[p(x)q(x)] = \deg(p(x)) + \deg(q(x)).$$
(where $-\infty + n$ is $-\infty$, by convention).

So if $p(x), q(x) \neq 0_F$,

then $\deg(p(x)q(x)) = \deg(p(x)) + \deg(q(x)) \geq 0$,

& in particular $\deg(p(x)), \deg(q(x)) \neq -\infty$,

i.e. $p(x) \cdot q(x) \neq 0_F$.

So F[x] has no zero-divisors.

So F[X] is a comm. ring w/ unity & has no zero-divisors, so it is an integral domain.

(continued on reverse)

(b) [4 points] Let $I = \langle X^2+1 \rangle$ denote the principal ideal generated by X^2+1 in $F[X]$. Prove that every element in the quotient ring $F[X]/I$ is equal to $I + (a + bX)$ for some choice of elements $a, b \in F$.

Let $I + p(X) \in F[X]/I$.

By the division algo for $F[X]$,

$\exists\, q(X), r(X) \in F[X]$ w/ $\deg(r(X)) < \deg(X^2+1) = 2$

& $p(X) = q(X)\cdot(X^2+1) + r(X)$.

Since $\deg r(X) \leq 1$, $r(X) = aX + b$ for some $a, b \in F$.

Now, $p(X) - (aX+b) = q(X)\cdot(X^2+1) \in \langle X^2+1 \rangle$,

so by the coset criterion,

$$I + p(X) = I + (aX+b),$$

as desired

(c) [4 points] Let I be as in part (b). Prove that if $a, b \in K$ satisfy $a^2 + b^2 \neq 0$, then the element $I + a + bX \in F[X]/I$ is a unit in $F[X]/I$.
Hint: mimic the way that inverses are computed in $\mathbb{C}$ or $\mathbb{Q}[\sqrt{-1}]$.

Observe that

$$(I + a + bX)\cdot(I + a - bX)$$

$$= I + (a^2 + abX - abX - b^2X^2)$$

$$= I + (a^2 - b^2X^2)$$

$$= I + (a^2 + b^2) \quad \text{by the coset criterion}$$

$\left((a^2+b^2) - (a^2 - b^2X^2) = b^2 + b^2X^2 = (1+X^2)\cdot b^2 \in \langle 1+X^2 \rangle \right).$

& since $a^2+b^2 \neq 0_F$, & since F is a field, $\exists\ (a^2+b^2)^{-1} \in F$.

Hence $(I + a + bX)\cdot[I + (a^2+b^2)^{-1}(a - bX)] = I + 1$,

& so $I + a + bX$ is a unit in $F[X]/I$.

8. [6 points] Let R be an integral domain. Prove that if $p \in R$ is a prime element, then p is also an irreducible element.

(Recall: An element $p \in R$ is *prime* if it is nonzero, it is not a unit, and for all $a, b \in R$ such that $p \mid ab$, either $p \mid a$ or $p \mid b$. An element $p \in R$ is *irreducible* if it is nonzero, it is not a unit, and for all $a, b \in R$ such that $p = ab$, either a is a unit or b is a unit.)

Suppose p is a prime element, and

$$p = ab \quad \text{for some } a, b \in R.$$

Then $p \mid ab$ $(ab = p \cdot 1_R)$, so either $p \mid a$ or $p \mid b$.

Suppose first that $p \mid a$.

Then $\exists\, c \in R$ s.t. $a = pc$. So

$$p = ab = pcb$$

$$\Rightarrow p(1 - cb) = 0_R.$$

Since $p \neq 0_R$, it is not a zero-divisor since R is an integral domain.

Thus $1 - cb = 0_R$, i.e. $1 = cb$.

Therefore b is a unit $(b^{-1} = c)$.

Similarly (exchanging a&b in the paragraph above), if $p \mid b$ then a is a unit.

Hence either a is a unit or b is a unit.

Combined w/ the fact that p is nonzero & nonunit (part of the defn of "prime element"), p is an irreducible element, as desired.

This page intentionally left blank. You may use it for scratchwork or to continue answers to any question (note clearly on the original page if you do so).

9. Suppose that G is a group, and H is a subgroup of $Z(G)$.

   (a) [4 points] Prove that H is a normal subgroup of G.

$H \subseteq Z(G) \subseteq G$, so $H \subseteq G$.

$H \leq Z(G) \Rightarrow H$ closed under mult. & inverse & nonempty

$\Rightarrow H$ is a subgroup of G as well.

Now, $\forall h \in H$, $\forall g \in G$ h & g commute since

$h \in Z(G)$, so

$ghg^{-1} = hgg^{-1}$

$= h e_G$

$= h \in H$.

So $ghg^{-1} \in H$. This shows $H \trianglelefteq G$,

as desired.

(continued on reverse)

(b) [6 points] Suppose that the quotient group G/H is cyclic, with generator Hg. Prove that G is abelian.
Hint: First show every element $x \in G$ is equal to hg^n for some $h \in H$ and integer n.

For any $x \in G$,

$Hx \in \langle Hg \rangle$ (since Hg generates G/H)

$\Rightarrow \exists n \in \mathbb{Z}$ st. $Hx = (Hg)^n = Hg^n$

$\Rightarrow xg^{-n} \in H$ (coset criterion)

$\Rightarrow \exists h \in H$ st. $xg^{-n} = h \Rightarrow$ ~~$\exists h$~~ $x = hg^n$.

Now, $\forall x, y \in G$, the above shows that $\exists\, h, k \in H$ & $m, n \in \mathbb{Z}$ st. $x = hg^m$ & $y = kg^n$.

Then
$xy = hg^m kg^n$
$= hk\, g^m g^n$ ← (since $k \in Z(G) \Rightarrow k$ & g^m commute)
$= kh\, g^{m+n}$ ← (since h & k commute)
$= kh\, g^n g^m$ (exponent laws)
$= kg^n hg^m$ (h & g^n commute)
$= yx$.

So any two elements of G commute, ie. G is abelian.

(c) (**Bonus**; up to 2 points of extra credit. I don't recommend spending time on this unless you've completed the rest of the exam!)

Prove that if G is a group of order p^3, for p a prime number, then $g^p \in Z(G)$ for all $g \in G$.

Abbreviate $Z(G)$ by Z below.

~~***~~ First observe that $g^p \in Z \iff Zg^p = Ze$ in G/Z (coset criterion)

$\iff (Zg)^p = Ze.$

So we will analyze orders of elements in G/Z ($Z \trianglelefteq G$ by part (a)).

~~Case~~ By Lagrange, $|Z| = 1, p, p^2$, or p^3.

~~Case 1: Z~~ As proved in class, $p \mid |Z|$ when $|G|$ is a power of a prime p. so $|Z| \neq 1$.

case 1: $|Z| = p$. Then $|G/Z| = p^2$. Since $Z \neq G$, G isn't abelian. By (the contrapositive of) part (b), G/Z is not cyclic, so no element has order p^2. So all elements have order 1 or p, hence $(Zg)^p = Ze$ $\forall g \in G$, as desired.

case 2: $|Z| = p^2$.
We proved in class that this is impossible (since $\forall g \notin Z$, $Z < C_G(g) < G$).
But even if it were, it would imply $|G/Z| = p$, so by a corollary of Lagrange $(Zg)^p = Ze$ $\forall g \in G$.

case 3: $|Z| = p^3$.
Then G is abelian, so all elements are in Z.

In all cases, we see that $o(Zg) = 1$ or p $\forall Zg \in G/Z$, which gives the result.

This page intentionally left blank. You may use it for scratchwork or to continue answers to any question (note clearly on the original page if you do so).