Amherst College
Department of Mathematics and Statistics

MATH 350 MIDTERM 2 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	Total
Points:	12	18	18	12	60
Score:					

1. [12 points] Let G be a group, and N a normal subgroup such that $[G : N] = m$. Prove that for all $g \in G$, $g^m \in N$.

(Suggested problem 10.3.9 from PSet 8; also see class notes from 10/29)

G/N is a group of order $[G:N]=m$.

By (a corollary of) Lagrange's theorem,

$\forall Ng \in G/N, \quad (Ng)^{|G/N|} = e_{G/N}$,

ie. $\quad Ng^m = Ne$, for all $g \in G$.

By the coset criterion, $\forall g \in G$ $g^m \cdot e^{-1} \in N$, ie. $g^m \in N$,

as desired.

2. [18 points] Let R denote the ring of all 2×2 matrices with real entries. Let S denote the following subset of R.

$$S = \left\{ \begin{pmatrix} a & -5b \\ b & a \end{pmatrix} : a, b \in \mathbb{Z} \right\}$$

(a) Prove that S is a subring of R.

<u>nonempty:</u> $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in S$.

<u>closure under −</u>

$\forall \begin{pmatrix} a & -5b \\ b & a \end{pmatrix}, \begin{pmatrix} c & -5d \\ d & c \end{pmatrix} \in S,$

$$\begin{pmatrix} a & -5b \\ b & a \end{pmatrix} - \begin{pmatrix} c & -5d \\ d & c \end{pmatrix} = \begin{pmatrix} (a-c) & -5(b-d) \\ (b-d) & (a-c) \end{pmatrix} \in S.$$

<u>closure under mult.:</u>

for the same two elements:

$$\begin{pmatrix} a & -5b \\ b & a \end{pmatrix}\begin{pmatrix} c & -5d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-5bd & -5da-5bc \\ bc+ad & -5bd+ac \end{pmatrix}$$

$$= \begin{pmatrix} ac-5bd & -5(bc+ad) \\ bc+ad & ac-5bd \end{pmatrix} \in S.$$

By the subring criterion, S is a subring of R.

(b) What element is the additive identity 0_S? Does S has a multiplicative identity 1_S?

$$0_S = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$1_S = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (S <u>does</u> have a mult. id.).

(continued on reverse)

3. [18 points] Let G be a finite group, and suppose that we have an action of G on a set Ω.

(a) Suppose $\alpha \in \Omega$. Define the *stabilizer* $\mathrm{Stab}_G(\alpha)$ of α, and prove that it is a subgroup of G.

$$\mathrm{Stab}_G(\alpha) = \{ g \in G : \quad g \cdot \alpha = \alpha \}.$$

nonempty:

$e \in \mathrm{Stab}_G \alpha$ since $e \cdot \alpha = \alpha$ (one of the axioms of a group action).

closed under mult.

if $g, h \in \mathrm{Stab}_G \alpha$ then $g \cdot \alpha = h \cdot \alpha = \alpha$.

So
$$\begin{aligned} (gh) \cdot \alpha &= g \cdot (h \cdot \alpha) \\ &= g \cdot \alpha \\ &= \alpha, \end{aligned}$$

hence $gh \in \mathrm{Stab}_G(\alpha)$.

closed under inverse

if $g \cdot \alpha = \alpha$

then $g^{-1} \cdot (g \cdot \alpha) = g^{-1} \cdot \alpha$,

so $(g^{-1} g) \cdot \alpha = g^{-1} \alpha$

$\Rightarrow \quad e \cdot \alpha = g^{-1} \cdot \alpha$

$\Rightarrow \quad \alpha = g^{-1} \cdot \alpha$,

ie. $g^{-1} \in \mathrm{Stab}_G(\alpha)$.

(continued on reverse)

So $\mathrm{Stab}_G(\alpha) \leq G$.

(b) Suppose that $|G| = 27$ and $|\Omega| = 10$. Prove that there exists at least one element $\alpha \in \Omega$ such that $\mathrm{Stab}_G(\alpha) = G$.
Hint: use the fundamental counting principle.

By FCP, $\forall x \in \Omega$ we have

$$|\mathcal{O}_\Omega(x)| = [G : \mathrm{Stab}_G(x)]$$
$$= |G| \,/\, |\mathrm{Stab}_G(x)|$$

hence $|\mathcal{O}_\Omega(x)|$ divides $|G|$. ie it must equal 1, 3, 9, or 27.

$\lightning$ Suppose that $\forall x \in \Omega$, $\mathrm{Stab}_G(x) \neq G$.

Then $\forall x \in \Omega$, $[G : \mathrm{Stab}_G(x)] \neq \frac{|G|}{|G|} = 1$,

so $|\mathcal{O}_\Omega(x)| = 3, 9,$ or 27.

In particular, $|\mathcal{O}_\Omega(x)|$ is a multiple of 3.

Since the orbits partition Ω, we can write $|\Omega|$ as a sum of mults. of 3,

so $3 \mid |\Omega|$, ie. $3 \mid 10$. $\lightning$

So $\exists x \in \Omega$ st. $\mathrm{Stab}_G(x) = G$.

4. [12 points] Let R be a commutative ring with unity. Suppose that $a \in R$ satisfies $a^2 = a$ and $a \neq 0_R, 1_R$.

(a) Prove that a is a zero-divisor.

$a^2 = a \Rightarrow a^2 - a = 0_R$ ~~$\Rightarrow a(1_R - a)$~~

$\Rightarrow a(a-1_R) = 0_R$.

Since $a \neq 1_R$, $a - 1_R \neq 0_R$. So both a & $a-1_R$ are nonzero, but their product is 0_R. So both are zero-divisors.

Alternative Solution

Suppose a is not a zero-divisor. Then the cancellation law applies: $\cancel{a} \cdot a = \cancel{a} \cdot 1$ implies $a = 1$, a contradiction.

(b) Define $\langle a \rangle = \{ar : r \in R\}$ and $\langle 1_R - a \rangle = \{(1_R - a)r : r \in R\}$ as usual. Prove that the map $\phi : R \to \langle a \rangle$ given by

$$\phi(r) = ar$$

is a ring homomorphism.

$\forall r, s \in R$, $\varphi(r+s) = a(r+s)$

$= ar + as$

$= \varphi(r) + \varphi(s)$.

and $\varphi(rs) = ars$

$= a^2 rs$ (since $a^2 = a$)

$= a(ar)s$

$= a(ra)s$ (since R is comm.)

$= (ar)(as)$

$= \varphi(r)\varphi(s)$

so φ is a ring homomorphism.

(we used R commutative because we need a to commute w/ all $r \in R$).

(continued on reverse)

(c) Prove that $R/\langle 1_R - a\rangle$ and $\langle a\rangle$ are isomorphic rings.
Suggestion: first prove that $\ker\phi = \langle 1_R - a\rangle$.

By the fund. thm. of ring homomorphisms,

$R/\ker\varphi \cong \operatorname{im}\varphi$. ($\varphi$ = the hom. from part (b)).

Note that $\operatorname{im}\varphi = \{\varphi(r) : r\in R\}$
$= \{ar : r\in R\}$
$= \langle a\rangle$.

So the result will follow from showing that $\ker\varphi = \langle 1_R - a\rangle$.

Claim 1: $\ker\varphi \subseteq \langle 1_R - a\rangle$.

Pf: If $r\in\ker\varphi$, then

$$ar = 0_R$$
$$\Rightarrow (1_R - a)r = r - ar$$
$$\Rightarrow (1_R - a)r = r$$

so $r\in\langle 1_R - a\rangle$ (it is $(1_R - a)$ times itself).

Claim 2: $\langle 1_R - a\rangle \subseteq \ker\varphi$.

Pf: $\forall\ (1_R - a)r \in \langle 1_R - a\rangle$, we have

$$\varphi((1_R - a)r) = a(1_R - a)r$$
$$= (a\cdot 1_R - a^2)\, r$$
$$= (a - a)r$$
$$= 0_R\cdot r$$
$$= 0_R$$

so $(1_R - a)r \in \ker\varphi$.

Hence indeed $\ker\varphi = \langle 1_R - a\rangle$ & thus $R/\langle 1_R - a\rangle \cong \langle a\rangle$.