Solutions

Take-home midterm – Math 412

Due in class: Thursday, Oct. 24, 2019, at the beginning of class

Instructions:

- You may use your notes and the textbook.
- You can*not* talk about the exam with other people. This should be your own work entirely. (Though you can talk to me.)
- As with the assignments, please write up your solutions nicely.
- This exam has 5 questions on 3 pages.

Reminder about definitions: Unlike the textbook:

- we define a ring to have an identity element;
- we define a subring to have the same identity as the bigger ring;
- we define ring homomorphisms to bring the identity to the identity.

---

(1) Consider the ring $R = \mathbf{Z}/12\mathbf{Z}$.

(a) For each unit $u \in R$, write down u and u^{-1}.

(b) For each zerodivisor $a \in R$, write down a nonzero $b \in R$ such that $ab = 0$.

(c) Find all nilpotents in R.

(d) Find all idempotents in R.

(2) Let F be a field and let $f(x) = a_n x^n + \cdots + a_0 \in F[x]$. The (*formal*) *derivative* of $f(x)$ is $f'(x) \in F[x]$ given by the formula you learn in calculus, namely

$$f'(x) := na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

It satisfies the Leibniz rule for products (just like you learn in calculus):

$$(fg)' = fg' + f'g.$$

(You don't need to prove this, just take it as given.)

(a) Suppose that $a \in F$ is a root of $f(x)$ and write $f(x) = (x-a)q(x)$. Show that $q(a) = f'(a)$ and conclude that when $f(x)$ is divided by $(x-a)^2$ the remainder is $f'(a)(x-a)$. (Hint: what happens when you try to divide $q(x)$ by $(x-a)$?)

(b) Suppose that $r \in F$. Show that the remainder when $f(x)$ is divided by $(x-r)^2$ is $f'(r)(x-r) + f(r)$.

(3) For each field F and polynomial $f(x) \in F[x]$ below, determine if $f(x)$ is irreducible.

(a) $f(x) = x^5 + x - 1$, $F = \mathbf{Z}/3\mathbf{Z}$.

(b) $f(x) = x^{25} + 25x + 5$, $F = \mathbf{Q}$.

(c) $f(x) = x^3 - x^2 + x - 2$, $F = \mathbf{Q}$.

(d) $f(x) = x^3 - x^2 - x - 2$, $F = \mathbf{Q}$.

(e) $f(x) = x^5 + x^2 + 1$, $F = \mathbf{Z}/2\mathbf{Z}$.

(4) The Subset-that-is-a-ring Test. Let R be a ring with respect to the binary operations $+$ and $\cdot$, and with additive identity $0 \in R$ and multiplicative identity $1 \in R$. Suppose S is a subset of R such that

(1) for all $a, b \in S$, $a - b \in S$,

(2) for all $a, b \in S$, $a \cdot b \in S$,

(3) there is an element $1_S \in S$ such that for all $a \in S$, $1_S \cdot a = a = a \cdot 1_S$.

Note that 1_S need not equal 1.

(a) Show that S is a ring. (Remark: if $1_S = 1$, then the above conditions were what we called the "Subring Test" and they show that S is a subring of R; if $1_S \neq 1$, then S is not a subring of R, but you are showing that S is still a ring.)

(b) Let $R = \mathbf{Z}/10\mathbf{Z}$ and let $S = \{0, 2, 4, 6, 8\} \subseteq R$. Show that S satisfies (1), (2), and (3) and hence is a ring.

(c) Let R be a ring and $S \subseteq R$ be a subset satisfying (1), (2), and (3). Suppose also that $1_S \neq 1$. Show that, as an element of R, 1_S is a zerodivisor, i.e. there is a non-zero element $a \in R$ such that $1_S \cdot a = 0$.

(5) Let R be a ring and let $\mathcal{F}$ denote the ring of functions $f : \mathbf{Z}_{\geq 1} \to R$ as defined in class. Note that you can think of such a function as a *sequence* of elements in R, namely the sequence $f(1), f(2), \ldots$ (usually, you'd use the notation $a_1, a_2, \ldots$ for a sequence); you don't have to think about it that way, but you can.

(a) Let $\mathcal{C}$ denote the subset of elements in $\mathcal{F}$ that are "eventually constant", i.e. $\mathcal{C}$ consists of the functions $f : \mathbf{Z}_{\geq 1} \to R$ such that there is an $N_f > 0$ with $f(n) = f(m)$ for all $m, n > N_f$. Show that $\mathcal{C}$ is a subring of $\mathcal{F}$. (Note that the number N_f can depend on f.)

(b) For a function $f \in \mathcal{C}$, define $f(\infty)$ to be the constant value that f eventually equals (i.e. $f(n) = f(\infty)$ for all $n > N_f$). Define a function $\varphi : \mathcal{C} \to R$ by

$$\varphi(f) := f(\infty).$$

Show that φ is a ring homomophism.

Solutions:

(1) All the calculations will be easier if the numbers are smaller, so let's use $\mathbb{Z}/12\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5, 6\}$

(a) $[a] \in \mathbb{Z}/n\mathbb{Z}$ is a unit iff $(a, n) = 1$

$[a] \in \mathbb{Z}/12\mathbb{Z}$ ... iff $2 \nmid a$ & $3 \nmid a$

so units are $\boxed{\pm 1, \pm 5}$ $\quad 5 \cdot 5 = 25 = 2 \cdot 12 + 1$ so $5^{-1} = 5$

so $(-5)^{-1} = -5$

so for all $u \in (\mathbb{Z}/12\mathbb{Z})^\times$, $\boxed{u^{-1} = u}$

(b) The zero divisors in $\mathbb{Z}/n\mathbb{Z}$ are the non-zero non-units

Here's a table of zero divisors a with a $b \neq 0$ s.t. $ab = 0$

a	b
± 2	6
± 3	4
± 4	3
6	2

(c) $[a]$ is nilpotent in $\mathbb{Z}/12\mathbb{Z}$ iff $\exists m \in \mathbb{Z}_{\geq 1}$ s.t. $12 \mid a^m$

Since $12 = 2^2 \cdot 3$, $12 \mid a^m$ implies $2, 3 \mid a$. Thus $a = 2 \cdot 3 \cdot k$ $k \in \mathbb{Z}$

so $\boxed{a = 0 \text{ or } 6}$. $(6^1 = 0 \quad 6^2 = 36 \equiv 0 \pmod{12})$

(d) $[a]$ is idempotent in $\mathbb{Z}/n\mathbb{Z}$ iff $a^2 \equiv a \pmod{n}$

iff $n \mid a(a-1)$

Get $\boxed{0, 1, 4, 9}$

(2)(a) $f(x) = (x-a)\,q_f(x)$

$f'(x) = (x-a)\,q_f'(x) + 1 \cdot q_f(x)$

so $f'(a) = \cancel{(a-a)\,q_f'(a)} + q_f(a)$

$= q_f(a)$ ✓

By the Remainder Theorem

$q_f(x) = (x-a)\,p(x) + q_f(a)$ for some $p(x) \in F[x]$

So $f(x) = (x-a)^2 p(x) + (x-a)\,q_f(a)$

$= (x-a)^2 p(x) + (x-a)\,f'(a)$

Since $\deg((x-a)\,f'(a)) = 1 < 2 = \deg((x-a)^2)$, $(x-a)\,f'(a)$ is the remainder when $f(x)$ is divided by $(x-a)^2$

(b) Let $g(x) = f(x) - f(r)$. Then r is a root of $g(x)$, so by part (a), $g(x) = (x-r)^2 p(x) + (x-r)\,g'(r)$ for some $p(x) \in F[x]$

Note $g'(x) = f'(x)$ so $f(x) - f(r) = (x-r)^2 p(x) + (x-r)\,f'(r)$

i.e. $f(x) = (x-r)^2 p(x) + (x-r)\,f'(r) + f(r)$ with $\deg((x-r)\,f'(r) + f(r)) < 2$ as desired $\mathbb{Q}.\mathbb{E}.\mathbb{D}$

(3)(a) $f(-1) = -1-1-1 = 0$ so f has a root, so it is **reducible**

(b) $f(x)$ satisfies the Eisenstein Criterion for $p=5$ so f is **irred**

(c) $f(x)$ mod 3 is $\bar{f}(x) = x^3 - x^2 + x + 1$

$\bar{f}(0) = 1 \neq 0$

$\bar{f}(1) = 2 \neq 0$

$\bar{f}(-1) = -2 \neq 0$

So $\bar{f}(x)$ has no roots. Since $\deg(\bar{f}) = 3$, this implies $\bar{f}(x)$ is irred (over $\mathbb{Z}/3\mathbb{Z}$). By the mod 3 irred. test, **$f(x)$ is irred over $\mathbb{Q}$.**

(d) By the Rational Root Test, the only possible roots of $f(x)$ are $\pm 1, \pm 2$.

$f(2) = 8 - 4 - 2 - 2 = 0$ so **$f(x)$ is red. over $\mathbb{Q}$**

(e) $f(0) \neq 0 \neq f(1)$, so $f(x)$ has no degree 1 factors

Claim: $f(x)$ has no irred deg 4 factors

proof: If it did, then $f(x) = g(x)h(x)$, $\deg(g) = 4$, $\deg(h) = 1$

↯ contradiction ✓

Claim: $f(x)$ has no irred deg 2 factors

proof: x^2+x+1 is the only irred deg 2 poly over $\mathbb{Z}/2\mathbb{Z}$

Long division $x^2+x+1 \overline{)x^5+x^2+1}$ with quotient x^3+x^2

$-x^5+x^4+x^3$

$x^4+x^3+x^2+1$

$-x^4+x^3+x^2$

1

so remainder is 1 so $x^2+x+1 \nmid f(x)$ ✓

Claim: $f(x)$ has no deg 3 irred factors

proof: If it did, Then $f(x)=g(x)h(x)$ where

$\deg(g)=3$ & h is deg 2 irred

$\Leftarrow$ or h is prod of deg 1

both contradictions ✓

So $f(x)$ has no lower degree irred factors

so $\boxed{f(x) \text{ is irred!}}$

(4) (a) R is a ring with $0, 1 \in R$, $+, \cdot : R \times R \to R$ satisfying conditions (i) – (vii) in the definition of a ring.

By (1), $1_S - 1_S = 0 \in S$

then $\forall s \in S$, $0 - s = -s \in S$

By (1), $\forall a, b \in S$, $a-(-b) = a+b \in S$

so The restriction $+_S$ to S of $+$ is a binary operation

By (2), ------ $\cdot_S$ --- . . -- -- - - --

Since $0 \in S$ & $S \subseteq R$ (so that $\forall a,b,c \in S$, $a,b,c \in R$) properties (i)–(iv), (vi)(vii) of being a ring hold for $S, 0, +_S, \cdot_S$

By (3), property (v) holds. So S is a ring. QED

(b) $S = \{[n] : n \text{ is even}\} = \{[2n] : n \in \mathbb{Z}\}$

(1) $[2n] - [2m] = [2(n-m)] \in S$

(2) $[2n] \cdot [2m] = [2 \cdot (2nm)] \in S$

(3) $6 \cdot 2 = 2$, $6 \cdot 4 = 4$, $6 \cdot 6 = 6$, $6 \cdot 8 = 8$, so $1_S = 6$ QED

(c) If $1_S \neq 1$, then $a = 1 - 1_S \neq 0$

$1_S \cdot a = 1_S \cdot 1 - 1_S \cdot 1_S = 1_S - 1_S = 0$ QED

(5)(a) Subring Criterion: $1_{\mathcal{I}} \in \mathcal{I}$ is the function $1_{\mathcal{I}}(n) = 1 \ \forall n$

(1) Let $N_1 = 1$, then $\forall m, n > N_1$, $1_{\mathcal{I}}(n) = 1 = 1_{\mathcal{I}}(n)$, so $1_{\mathcal{I}} \in \mathcal{E}$

(2) For $m, n > \max(N_f, N_g)$

$(f-g)(m) = f(m) - g(m) = f(n) - g(n) = (f-g)n$ so $f-g \in \mathcal{E}$

(3) For $m, n > \max(N_f, N_g)$

$(fg)(m) = f(m)g(m) = f(n)g(n) = (fg)(n)$ so $fg \in \mathcal{E}$

QED

(b) (1) $1_{\mathcal{I}}(n) = 1 \ \forall n$, so $1_{\mathcal{I}}(\infty) = 1$

so $\varphi(1_{\mathcal{I}}) = 1$ ✓

(2) For $m, n > \max(N_f, N_g)$, $f(m) = f(n) = f(\infty)$

$g(m) = g(n) = g(\infty)$

so $(f+g)(m) = f(m) + g(m) = f(n) + g(n) = (f+g)(n)$

so $(f+g)(\infty) = f(m) + g(m) = f(\infty) + g(\infty)$

i.e. $\varphi(f+g) = (f+g)(\infty) = f(\infty) + g(\infty) = \varphi(f) + \varphi(g)$

(3) For $m, n > \max(N_f, N_g)$, $(fg)(m) = (fg)(n)$ by (3) above

so $(fg)(\infty) = (fg)(m)$

so $\varphi(fg) = (fg)(m) = f(m)g(m) = f(\infty)g(\infty) = \varphi(f)\varphi(g)$

QED