Algebra HW1

$\frac{34}{35}$

① let R be a ring. Let $a, b \in R$

ⓐ $a \times 0 = a \times (0+0) = a\times 0 + a \times 0 \Rightarrow \underline{a \times 0 = 0}$. □ ✓

5

ⓑ $0 = a + (-a)$
$= 0 \times a = (1+(-1)) \times a = 1 \times a + (-1)\times a = a + (-1)\times a$

$\Rightarrow a + (-a) = a + (-1)\times a \Rightarrow \underline{-a = (-1)\times a}$ □ ✓

ⓒ $0 = a\times b - (a \times b)$
$= 0 \times b = (a-a)\times b = a \times b + (-a)\times b$

$\Rightarrow a \times b - (a\times b) = a \times b + (-a)\times b \Rightarrow \underline{-(a\times b) = (-a)\times b}$ □ ✓

② describe explicitly the smallest subring of $\mathbb{C}$ that contains the real cube root of 2:

4

$\mathbb{Z}[\sqrt[3]{2}] = \{\beta \in \mathbb{C} \mid \beta = a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2$ where $a_i \in \mathbb{Z}\}$ ✓

please justify your answer.

③ ring or not?

ⓐ U is an arbitrary set, and R is the set of subsets of U. Addition and Multiplication of elts of R are defined by the rules $A + B = (A \cup B) - (A \cap B)$ and $A \cdot B = A \cap B$.

(hint: characteristic functions?) let $A, B, C \in R$.

R^+ is abelian group? ① identity: $0 = \emptyset$: $A + \emptyset = A \cup \emptyset - (A \cap \emptyset) = A - \emptyset = A$. ✓ ✓

② inverse: $-A = A$: $A + A = A \cup A - (A \cap A) = A - A = \emptyset$. ✓ ✓

③ associative? char. fcn → membership table: ✓

A	B	C	A+B	(A+B)+C	B+C	A+(B+C)
1	1	1	0	1	0	1
0	1	1	1	0	0	0
1	0	1	1	0	1	0
0	0	1	0	1	1	1
1	1	0	0	0	1	0
0	1	0	1	1	1	1
1	0	0	1	1	0	1
0	0	0	0	0	0	0

OK---
again, please explain.

④ abelian ✓ $A + B = (A \cup B) - (A \cap B) = (B \cup A) - (B \cap A) = B + A$ ✓ ✓

$R, \times$?

⑤ $1 = U$: $U \cdot A = U \cap A = A$. ✓ ✓

⑥ associative: $(AB)C = (A\cap B)\cap C$. $x \in (A \cap B) \cap C \Leftrightarrow x \in A \cap B \wedge x \in C$ ✓
$\Leftrightarrow x \in A \wedge x \in B \wedge x \in C$
$\Leftrightarrow x \in A \wedge x \in B \cap C$
$\Leftrightarrow x \in A \cap (B \cap C)$.

$\Rightarrow (AB)C = (A\cap B)\cap C = A \cap (B \cap C) = A(BC)$. ✓

⑦ Commutative? $AB = A \cap B = B \cap A = BA$. ✓ ✓

distributive?

⑧ ~~distributive~~ $(A+B)C = AC + BC$?
characteristic fcn → membership table:
(next page)

A	B	C	A+B	(A+B)C	AC	BC	AC+BC
1	1	1	0	0	1	1	0
0	1	1	1	1	0	1	1
1	0	1	1	1	1	0	1
0	0	1	0	0	0	0	0
1	1	0	0	0	0	0	0
0	1	0	1	0	0	0	0
1	0	0	1	0	0	0	0
0	0	0	0	0	0	0	0

1–8 $\Rightarrow$ R is a ring.

✓

(6) R is the set of continuous functions $\mathbb{R} \to \mathbb{R}$. Addition + Multiplication: $[f+g](x) = f(x) + g(x)$, $[f \circ g](x) = f(g(x))$

✓ not a ring.

- R^+ forms abelian group. (prop. of continuous fcns) ✓
- multiplication is not commutative: let $f(x) = x^2$, $g(x) = 2x$. $f(g(x)) = 4x^2$, $g(f(x)) = 2x^2$.
- multiplication is associative: $[[\overset{\in R}{f} \circ \overset{\in R}{g}] \circ \overset{\in R}{h}](x) = (f \circ g)(h(x)) = f(g(h(x)))$
  $= f(g \circ h(x)) = f \circ (g \circ h)(x)$.
- mult identity: $f(x) = x$. let $g \in R$. $f \circ g(x) = f(g(x)) = g(x)$,
  $g \circ f(x) = g(f(x)) = g(x)$.
- distributive? yes on the left at least... let $f, g, h \in R$

$$((f+g) \circ h)(x) \overset{\text{let } \theta(x) = f(x)+g(x)}{=} f(h(x)) + g(h(x)) = f \circ h(x) + g \circ h(x) = (fh + gh)(x).$$

5

(4) for which $n \in \mathbb{N}$ does $x^2 + x + 1 \mid x^4 + 3x^3 + x^2 + 7x + 5$ in $[\mathbb{Z}/(n)][x]$?

$$\begin{array}{r} x^2+2x-2 \\ x^2+x+1 \overline{)\, x^4+3x^3+x^2+7x+5} \\ -x^4-x^3-x^2+0+0 \\ \hline 2x^3+0+7x+5 \\ -2x^3-2x^2-2x+0 \\ \hline -2x^2+5x+5 \\ +2x^2+2x+2 \\ \hline 7x+7 \end{array}$$

$7x + 7 = 0 \Rightarrow n \in \{7, 1\}$ ✓

$(n \mid 7)$

5

(*) (5) find generators for the kernels of...

I struggled to formalize these coherently, see last page for my attempt

(a) $\mathbb{R}[x,y] \to \mathbb{R}$ st. $f(x,y) \rightsquigarrow f(0,0)$: $\ker = (x, y)$ ✓

(b) $\mathbb{R}[x] \to \mathbb{C}$ st. $f(x) \rightsquigarrow f(2+i)$: $f(2+i) = 0 \Rightarrow (z-(2+i))(z-2+i) = z^2 - 4z + 5 \Rightarrow$ $(-2-i)(-2+i) = 4+1$
$\Rightarrow \ker = (z^2 - 4z + 5)$. ✓

(c) $\mathbb{Z}[x] \to \mathbb{R}$ st. $f(x) \rightsquigarrow f(1+\sqrt{2})$: $f(1+\sqrt{2}) = 0 \Rightarrow (x-1-\sqrt{2})(x-1+\sqrt{2}) = x^2 - 2x - 1$
$\Rightarrow \ker = (x^2 - 2x - 1)$. ✓

(d) $\mathbb{Z}[x] \to \mathbb{C}$ st. $x \rightsquigarrow \sqrt{2} + \sqrt{3}$: $\rightsquigarrow (x - (\sqrt{2}+\sqrt{3}))(x + \sqrt{2} + \sqrt{3}) = x^2 - 5 - 2\sqrt{2}\sqrt{3} \rightsquigarrow (x^2 - 5 - 2\sqrt{2}\sqrt{3})(x^2 - 5 + 2\sqrt{2}\sqrt{3})$
$\rightsquigarrow x^4 - 10x^2 + 1 \Rightarrow \ker = (x^4 - 10x^2 + 1)$. ✓

(e) $\mathbb{C}[x,y,z] \to \mathbb{C}[t]$ st. $x \rightsquigarrow t$, $y \rightsquigarrow t^2$, $z \rightsquigarrow t^3$. $(x^2 - y), (y^3 - z^2), (x^3 - z) \in \ker$...
$\hookrightarrow (x^2 - y, x^3 - z) \rightsquigarrow (y - x^2, z - x^3)$ (for convenience) ✓

5

⑥ an elt. $a \in R$ is a unit if $\exists b \in R$ s.t. $ab = 1$. Let $R = \mathbb{Z}[i]$ be the ring of Gaussian integers. Show that the units of R are $1, -1, i, -i$.

ignore

Claim: $a \in R_0$ is a unit iff $(a) = R_0$. (Let R_0 be a ring).

($\Rightarrow$) $R_0 = (1) \Rightarrow$ if $a \in R_0$ is unit, then $\exists b \in R_0$ st $ab = 1 \Rightarrow 1 \in (a) \Rightarrow (a) = R$.

($\Leftarrow$) $(a) = R_0 \Rightarrow \exists r_1, \dots, r_k \in R_0$ st $r_1 a + \dots + r_k a = 1 \Rightarrow a\underbrace{(r_1 + \dots + r_k)}_{\in R_0} = 1 \Rightarrow a$ is a unit. $\square$

back to problem at hand: let $R = \mathbb{Z}[i]$. let $x \in R$ be a unit.
will show: $x \in \{1, -1, i, -i\}$ let $S = \{x \in R \mid \exists y \in R \text{ st } xy = 1\}$

$x \in S \Rightarrow \exists y \in R$ st $x^{-1} = y \Rightarrow (\overset{\text{also}}{y^{-1} = x} \Rightarrow y \in S) \Rightarrow S^{\times}$ is an abelian group.
$\Rightarrow S$ is a field.

ⓐ let $z = a + bi \in S \Rightarrow z^{-1} \in S \subset R \Rightarrow \exists a', b' \in \mathbb{Z}$ st $z^{-1} = a' + b'i$

$$z^{-1} = \frac{1}{z} = \frac{1}{a+bi} \frac{(a-bi)}{(a-bi)} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i = a' + b'i \Rightarrow a' = \frac{a}{a^2+b^2} \in \mathbb{Z} \text{ and } b' = \frac{-b}{a^2+b^2} \in \mathbb{Z}$$

$\Rightarrow a^2 + b^2 = 1$. $\underset{\in \mathbb{Z}}{a^2} \geq 0$ and $\underset{\in \mathbb{Z}}{b^2} \geq 0 \Rightarrow (a,b) \in \{(1,0), (0,1), (-1,0), (0,-1)\}$.

$\Rightarrow z \in \{1, -1, i, -i\} \Rightarrow \{1, -1, i, -i\} \supseteq S$. ✓

5

ⓑ $\{1, -1, i, -i\} \subseteq S$: $1 \cdot 1 = 1 \Rightarrow 1$ is unit. $(-1)(-1) = 1 \Rightarrow -1$ is unit. $i(-i) = 1$, $(-i)i = 1 \Rightarrow i, -i$ are units.

$\therefore$ ⓐ, ⓑ $\Rightarrow S = \{1, -1, i, -i\}$ ✓

⑦ let R be a ring of prime characteristic p. (a ring R has characteristic n if the kernel of the unique homomorphism $\mathbb{Z} \to R$ is $n\mathbb{Z}$) Prove that the map $R \to R$ defined by $x \mapsto x^p$ is a ring homomorphism

let R be ring of prime char. p. let $\varphi: R \to R$ be the Frobenius map.
let $\phi_p: \mathbb{Z} \to R$ st. $\ker \phi_p = p\mathbb{Z}$. let $a, b \in R$

$$\phi_p(p) = \phi_p(0) = \phi_p(\underbrace{1 + \dots + 1}_{p \text{ times}}) = \underbrace{1 + \dots + 1}_{p \text{ times}} \overset{\in R}{=} 0.$$

5

ⓐ $\varphi(a+b) = (a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$.. (note: $\binom{p}{k} = \frac{p!}{k!(p-k)!}$ where $p \geq k$.
$\Rightarrow$ for $k \notin \{0, p\}$, $p \mid \binom{p}{k}$) ✓

$= a^p + 0 \cdot c_1 a^{p-1} b + \dots + b^p = a^p + b^p$

$= \varphi(a) + \varphi(b)$. ✓

ⓑ $\varphi(ab) = (ab)^p = a^p b^p$ (R is commutative ring)
$= \varphi(a)\varphi(b)$. ✓

ⓒ $\varphi(1) = 1^p = 1$.

✓

$\therefore \varphi$ is ring homomorphism.

(*) (5) (a) $\varphi: \mathbb{R}[x,y] \longrightarrow \mathbb{R}: f(x,y) \rightsquigarrow f(0,0)$ claim: $\ker\varphi = (x,y)$

$\mathbb{R}[x,y] \to \mathbb{R}[x][y] \longrightarrow \mathbb{R}[x] \to \mathbb{R}$

$f(x,y) \longrightarrow f_y(x)(y) \longrightarrow f_x(x)(0) \longmapsto f_x(0)$

let $g \in \ker\varphi \Rightarrow \overset{\in \ker}{g_y(x)(y)} = y\,\overset{\in \ker}{g_x(x)(y)} + r(x)(y) \Rightarrow r(x)(y) = 0$ (y) is principle $(\mathbb{R}[x][y])$ deg 0.

$\Rightarrow \overset{\in \ker}{g_x(x)} = \underset{\ker}{x}\,\overset{\deg 1}{g_x(x)} + \overset{\in \ker}{r(x)} \Rightarrow r(x) = 0$ (x) is principle (in $\mathbb{R}[x]$)

$\Rightarrow g(x,y) = x\,p(x,y) + y\,q(x,y)$ for some $p, q \in \mathbb{R}[x,y]$

$\therefore \ker\varphi = (x,y)$ □

(b) $\varphi: \mathbb{R}[x] \longrightarrow \mathbb{C}: f(x) \rightsquigarrow f(2+i)$ claim: $\ker\varphi = ((z-(2+i))(z-(2-i)))$ $= z^2-4z+5$

let $p(x) \in \ker\varphi \Rightarrow \overset{\in \ker\varphi}{p(x)} = \overset{\in \ker\varphi}{(z^2-4z+5)}q(x) + \overset{\in \ker\varphi}{r(x)}$

$\Rightarrow r(x) = x+\alpha$ or $r(x) = 0$ (monic)

suppose $r(x) = x+\alpha$ for some $\alpha \in \mathbb{R}$

but $\Rightarrow 0 = 2+i+\alpha \Rightarrow \alpha = -(2+i) \Rightarrow \alpha \notin \mathbb{R}$ # contradiction

$\Rightarrow (z^2-4z+5)$ is smallest and $\mathbb{R}[x]$ is field

$\therefore \ker\varphi = (z^2-4z+5)$ □

(c) $\varphi: \mathbb{Z}[x] \to \mathbb{R}: f(x) \longmapsto f(1+\sqrt{2})$. Claim $\ker\varphi = (x^2-2x-1)$

note: $x^2-2x-1 = (x-(1+\sqrt{2}))(x-(1-\sqrt{2}))$

Consider $\mathbb{Z}[x] \to \mathbb{Q}[x] \to \mathbb{R}$, let $p(x) \in \mathbb{Z}[x] \mapsto p'(x) \in \mathbb{Q}[x]$

$f(x) \to f(x) \longrightarrow f(1+\sqrt{2})$

$\Rightarrow p'(x) = (x^2-2x-1)q(x) + r(x) \Rightarrow r(x) \in \ker$. suppose $r(x) = x+\alpha$ w/ $\alpha \in \mathbb{Q}$

$\Rightarrow 0 = 1+\sqrt{2}+\alpha \Rightarrow \alpha = -(1+\sqrt{2}) \Rightarrow \alpha \notin \mathbb{Q} \Rightarrow r(x) = 0$. #

$\Rightarrow r(x) = 0 \Rightarrow (x^2-2x-1)$ is smallest in $\mathbb{Q}$ so ideal is principle.

(coefficients are integers! so we're done) more importantly, leading is 1.

$\therefore \ker\varphi = (x^2-2x-1)$ □

(d) $\mathbb{Z}[x] \to \mathbb{C}: x \mapsto \sqrt{2}+\sqrt{3}$ claim: $\ker = (x^4-10x^2+1)$

note: $x^4-10x^2+1 = (x-(\sqrt{2}+\sqrt{3}))(x-(-\sqrt{2}-\sqrt{3}))(x-(-\sqrt{2}+\sqrt{3}))(x-(\sqrt{2}-\sqrt{3}))$

Similar to above: let $p(x) \in \ker$ and consider $\mathbb{Z}[x] \to \mathbb{Q}[x]: f(x) \mapsto f(x)$

$\Rightarrow p(x) \overset{\in \mathbb{Q}[x]}{=} (x^4-10x^2+1)q(x) + r(x) \Rightarrow \deg(r(x)) \in \{0,1,2,3\}$.

(0) ($\deg(r)=0$) $\Rightarrow r(x) \notin \ker$ #

(1) $\deg(r)=1 \Rightarrow r(x) = x-(\sqrt{2}+\sqrt{3}) \Rightarrow r(x) \notin \mathbb{Q}[x]$ #

$\Rightarrow \deg(r(x)) \neq 3$ (b/c we know how x^4-10x^2+1 factors)

(2) $\deg(r)=2 \Rightarrow r(x) = (x-(\sqrt{2}+\sqrt{3}))q(x)$ where $\deg(q(x)) = 1$

but the product of any two first deg. poly factors of x^4-10x^2+1 #

is not in $\mathbb{Q}[x]$. (contains $\sqrt{6}$ term).

$\Rightarrow r(x) = 0$. $\longrightarrow \ker_{\mathbb{Q}} = (x^4-10x^2+1)$

$\therefore \ker = (x^4-10x^2+1)$

(e) $\mathbb{C}[x,y,z] \to \mathbb{C}[t]: x \mapsto t, y \mapsto t^2, z \mapsto t^3$ (stepping along)

Let $p(x,y,z) \in \ker \Rightarrow p(t,t^2,t^3) = 0$. Clearly $y-x^2, z-x^3 \in \ker$.

$p(x,y)(z) = (z-x^3)q(x,y)(z) + r(x,y)(z) \Rightarrow \deg(r(x,y)(z)) < 1 \Rightarrow r(x,y)(z) = 0$.

$\Rightarrow p(x,y)(t) = (t^3-x^3)q(x,y)(t^3) = p(x,y) \in \ker$

$p(x)(y) = (y-x^2)\underset{\text{constant}}{(t^3-x^3)}q(x)(y) + \underset{\in \mathbb{C}[x](y)}{\overset{\in \ker}{r_1(x)(y)}} \Rightarrow \deg(r_1(x)(y)) < 1 \Rightarrow r_1(x)(y) = 0$

$\therefore \ker = (y-x^2, z-x^3)$. (what about y^3-z^2?)

A solution of Problem 3 using the hint (and avoiding dealing with venn diagrams.).

Recall R = Set of subsets of a set U.

Define S = Set of functions from U to $\{0,1\}$.

Then there is a bijection $R \to S$ defined as follows

A subset $A \subset U \longmapsto$ The function 1_A defined by

$$1_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}$$

The inverse is

$$\{x \in U \mid f(x) = 1\} \longleftarrow f$$

Now, let us interpret $+$ and $\times$ defined on R in terms of S.

We get $\quad A \cap B \rightsquigarrow 1_A \cdot 1_B \quad$ (with the usual definition of product function)

$$A \oplus B = A \cup B \setminus A \cap B \rightsquigarrow 1_A + 1_B \pmod 2$$

Indeed, $x \in A \cup B \setminus A \cap B$ iff $x \in$ exactly one of A or B.

But $\cdot, +\ (\text{mod } 2)$ clearly make S a ring.

$\Rightarrow \cap, \oplus$ must make R a ring.

8. Decide whether the following series converge or diverge. Clearly indicate the test(s) you use.

(a) (4 points) $\displaystyle\sum_{n=0}^{\infty} \frac{4^n + 3^n}{5^n}$

(b) (4 points) $\displaystyle\sum_{n=1}^{\infty} \sin(1/n)$