Wednesday 11/4/15 MATH 611 HW5 solutions.

1. a) $\varphi: \mathbb{Q}[x] \longrightarrow \mathbb{Q}$
$\varphi(f(x)) = f(3)$

$\ker\varphi = (x-3)$

FIT $\Rightarrow$ $\mathbb{Q}[x]/(x-3) \xrightarrow[\sim]{\bar{\varphi}} \mathbb{Q}$.

b) $\mathbb{R}[x]/(x^2-4x-5) = \mathbb{R}[x]/((x-5)(x+1))$

$\underset{\text{C.R.T.}}{\cong} \mathbb{R}[x]/(x-5) \times \mathbb{R}[x]/(x+1) \cong \mathbb{R}\times\mathbb{R}$

$(x-5)$ & $(x+1)$ are coprime.

using FIT applied to evaluation at 5 & -1 respectively (cf. part (a)).

c) $\mathbb{R}[x]/(x^2+4)$

$\varphi: \mathbb{R}[x] \longrightarrow \mathbb{C}$
$\varphi(f(x)) = f(2i)$

$\ker\varphi = \mathbb{R}[x] \cap (x-2i)$
$= (x^2+4)$

$$\begin{array}{ccc} & & \mathbb{R}[x] \\ & & \cap \\ (x-2i) & \subset & \mathbb{C}[x] \end{array}$$

if $f\in\mathbb{R}[x]$, & $f(2i)=0$, then also $f(-2i)=\overline{f(2i)}=0$.
So f is divisible by $(x-2i)$ & $(x+2i)$ in $\mathbb{C}[x]$,
& $(x-2i)$ & $(x+2i)$ are coprime, so f is divisible by
$(x^2+4)=(x-2i)(x+2i)$ in $\mathbb{C}[x]$. Now since $f, (x^2+4)\in\mathbb{R}[x]$,
it follows that f is divisible by (x^2+4) in $\mathbb{R}[x]$.

FIT $\Rightarrow$ $\mathbb{R}[x]/_{(x^2+4)} \xrightarrow[\sim]{\overline{\varphi}} \varphi(\mathbb{R}[x]) = \mathbb{C}$.

2. a) $\varphi: \mathbb{Z} \to R$

$$\varphi(m) = \begin{cases} 0 & m = 0 \\ \overbrace{1+1+\dots+1}^{m} & m > 0 \\ -(\underbrace{1+1+\dots+1}_{|m| = -m}) & m < 0. \end{cases}$$

Write $\ker \varphi = (n)$, $n \geq 0$.

b) FIT $\Rightarrow$ $\mathbb{Z}/_{n\mathbb{Z}} \underset{\overline{\varphi}}{\hookrightarrow} R$

R integral domain $\Rightarrow$ $\mathbb{Z}/_{n\mathbb{Z}}$ integral domain $\Rightarrow$ $n = 0$ or p, prime.

3. $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \underset{\text{subring}}{\subset} \mathbb{C}$

$\mathbb{Z}[i]/_{(3+4i)} \cong ?$

$\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}[i]/_{(3+4i)}$ $\qquad \varphi(n) = n + (3+4i)$

φ surjective: Required to prove: given $x+iy \in \mathbb{Z}[i]$, $\exists\, n \in \mathbb{Z}$ s.t.

$x+iy - n \in (3+4i)$

i.e. $x+iy = n + (a+bi)(3+4i)$, some $n \in \mathbb{Z}$, $a, b \in \mathbb{Z}$.

$= (n + 3a - 4b) + i(4a+3b)$

$\exists$ solution to $y = 4a+3b$ (because $\gcd(4,3) = 1$)

Then can choose n so that $x = n + 3a - 4b$. ✓

$\ker \varphi \overset{?}{=}$ eg $\quad n \in \ker \varphi \Leftrightarrow n = (a+bi)\cdot(3+4i)$, some $a, b \in \mathbb{Z}$

$= (3a-4b) + i(4a+3b)$

i.e., $4a+3b=0 \Rightarrow a=3k,\ b=-4k$, some $k\in\mathbb{Z}$

& $n = 3a-4b = 9k+16k = 25k$.

$\therefore \ker\varphi = (25) \subset \mathbb{Z}$.

FIT $\Rightarrow \mathbb{Z}/25\mathbb{Z} \xrightarrow[\sim]{\bar{\varphi}} \mathbb{Z}[i]/(3+4i)$

4 a. $F: R \to R$, $F(a) = a^p$

$F(1)=1$ ✓

$F(ab) = F(a)F(b)$ ✓ (R commutative!)

$F(a+b) \stackrel{?}{=} F(a)+F(b)$

$$(a+b)^p \underset{\text{B.T.}}{=} \sum_{i=0}^{p} \binom{p}{i} a^i \cdot b^{p-i}$$

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!} \Rightarrow p \mid \binom{p}{i} \text{ for } 0<i<p$$

$$\Rightarrow (a+b)^p = \binom{p}{0}\cdot a^p + \binom{p}{p} b^p = a^p + b^p$$

because "$p=0$" in R"

[more carefully, $\varphi(p)=0$ where $\varphi:\mathbb{Z}\to R$ is the ring hom of $\mathbb{Z}$.

And when we write $n\cdot a$ for $n\in\mathbb{Z}$ & $a\in R$,

we mean $\varphi(n)\cdot a = \begin{cases} \underbrace{a+a+\cdots+a}_{n} & n>0 \\ 0 & n=0 \\ -\underbrace{(a+\cdots+a)}_{|n|=-n} & n<0. \end{cases}$]

b. $R = (\mathbb{Z}/p\mathbb{Z})[x]$

$f\in R$, $f = \sum a_i x^i$

$F: R\to R$, $F(f) = F(\sum a_i x^i) = \sum F(a_i x^i) = \sum a_i^p (x^i)^p \rightarrow$

$= \sum_i a_i x^{pi}$ using $a_i^p = a_i$ for $a_i \in \mathbb{Z}/p\mathbb{Z}$.

i.e $F(f(x)) = f(x^p)$.

5. a. $f(x,y) = y^2 - x^3 \in \ker \varphi$.

Claim: $\ker\varphi = (f)$.

Proof: given $g \in \ker\varphi$, write $g = q \cdot f + r$

where $q, r \in \mathbb{C}[x,y] = (\mathbb{C}[x])[y]$ & $r = 0$ OR $\deg_y r < \underset{\deg_y f}{\underset{\parallel}{2}}$

Then $r = a_0(x) + a_1(x) \cdot y$, & required to prove $r = 0$.

$(\Rightarrow g \in (f))$

$r = g - q \cdot f \in \ker\varphi$ because $g, f \in \ker\varphi$.

$\varphi(r) = r(t^2, t^3) = a_0(t^2) + a_1(t^2) \cdot t^3 = 0$

$\Rightarrow a_0(x) = a_1(x) = 0 \Rightarrow r = 0$

because $a_0(t^2)$ involves only ~~odd~~ even powers of t

$a_1(t^2) \cdot t^3$ " " odd " " " $\square$

$$\varphi(g(x,y)) = g(t^2, t^3)$$

$$\underset{\sum a_{ij} x^i y^j}{\parallel} \qquad \underset{\sum a_{ij} t^{2i+3j}}{\parallel}$$

$a_{ij} \in \mathbb{C}$

Any $n \in \mathbb{Z}_{\geq 0}$ can be written in the form $2i+3j$ for $i, j \in \mathbb{Z}_{\geq 0}$ except $n = 1$.

$\Rightarrow \varphi(\mathbb{C}[x,y]) = \{ h(t) = a_0 + a_1 t + \dots + a_n t^n \in \mathbb{C}[t] \mid a_1 = 0 \} \underset{\text{subring}}{\subset} \mathbb{C}[t]$

b. $\varphi : \mathbb{C}[x,y] \to \mathbb{C}[t]$

$\varphi(g(x,y)) = g(t^2-1,\ t(t^2-1))$

$y^2 \mapsto t^2(t^2-1)^2 \leftarrow (x+1)x^2$

$\therefore f = y^2 - x^2(x+1) \in \ker\varphi$.

Claim: $\ker\varphi = (f)$.

Proof: Similar to (a), given $g \in \ker\varphi$,

write $g = qf + r$, $r = 0$ or $\deg_y r < \deg_y f = 2$.

$r = a_0(x) + a_1(x)\cdot y$

$r \in \ker\varphi$

$$0 = r(t^2-1,\ t\cdot(t^2-1)) = \underbrace{a_0(t^2-1)}_{\text{even powers of } t} + \underbrace{a_1(t^2-1)\cdot t(t^2-1)}_{\text{odd powers of } t}$$

$\Rightarrow a_0(t^2-1) = a_1(t^2-1) = 0$

$\Rightarrow a_0(x) = a_1(x) = 0. \Rightarrow r = 0.$ $\square$.

$\varphi(g(x,y)) = \sum a_{ij}(t^2-1)^{i+j}\cdot t^j$

$\quad\ \ = \sum a_{ij}x^iy^j$

Claim: $\varphi(\mathbb{C}[x,y]) = \{h \in \mathbb{C}[t] \mid h(1) = h(-1)\}$

Proof: $\subseteq$ ✓ $\varphi(g) = a_{00} + (t^2-1)\cdot q$, some $q \in \mathbb{C}[t]$.

$\supseteq$ Conversely given $h \in$ RHS,

write $h = \alpha + (t^2-1)\cdot q$, $\alpha \in \mathbb{C}$ $(\alpha = h(1) = h(-1))$

$q \in \mathbb{C}[t]$

Observe $t^{2k}\cdot(t^2-1) = \varphi((x+1)^k\cdot x)$

$t^{2k+1}\cdot(t^2-1) = \varphi((x+1)^k\cdot y)$ $\square$.

6. a. $a, b \in N$.

$a^n = 0$, $b^m = 0$.

$$\Rightarrow (a+b)^{n+m} \underset{\text{B.T.}}{=} \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i} = 0$$

i.e. $a, b \in N \Rightarrow a+b \in N$.

$0 \in N$ ✓, $a \in N, b \in R \Rightarrow ba \in N$ ✓ (R commutative!)

$\Rightarrow N$ ideal.

[Remark: Recall, say $I \subset R$ is an ideal of a ring R if

1. $(I,+) \subset (R,+)$ is a subgroup
2. $a \in I, b \in R \Rightarrow ba \in I$.

Notice that it suffices for 1. to check $0 \in I$ & I is closed under addition, because additive inverses exist in I by 2: $-a = (-1) \cdot a \in I$.]

b. Write $\bar{a} = a + N \in R/N$

Suppose $\bar{a}^n = 0$. i.e. $a^n \in N$.

Then $(a^n)^m = 0$, some m.

i.e. $a^{nm} = 0$, $a \in N$, $\bar{a} = 0$. $\square$

7. a) $\{\text{Ideals of } \mathbb{Z}/n\mathbb{Z}\} \longleftrightarrow \{\text{ideals of } \mathbb{Z} \text{ containing } n\mathbb{Z} = (n)\}$

$= \{(d) \mid \underbrace{d \mid n}\}$ "d divides n"

$I/n\mathbb{Z} \longleftarrow I$

$J \longmapsto q^{-1}J$ $\qquad q : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ quotient hom.

See, under this correspondence

$$\left\{ \text{Maximal ideals of } \mathbb{Z}/n\mathbb{Z} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{Maximal ideals of } \mathbb{Z} \\ \text{containing } (n) \end{array} \right\}$$

$$\shortparallel$$

$$\{ (p) \mid p \text{ prime}, p \mid n \}.$$

$\therefore$ $\mathbb{Z}/n\mathbb{Z}$ local $\Leftrightarrow$ $n = p^\alpha$, p prime, $\alpha \in \mathbb{N}$.

b. Note first: $\forall\, u \in R$ is a unit $\Leftrightarrow$ $(u) = R$.

In particular, if $I \subsetneq R$ ideal, u unit $\Rightarrow$ $u \notin I$.

So, in our case $R^\times = \{ u \in R \mid u \text{ unit} \} \subset R \setminus M$.

Conversely, suppose $a \in R \setminus M$.

If $(a) = R$ then a is a unit

Otherwise, $\exists$ maximal ideal $M' \supset (a)$.

But $a \in M'$, $a \notin M$ $\Big\}$ ※.

$\Rightarrow$ $M' \neq M$

$\therefore$ $R^\times = R \setminus M$.

c.

R ring, $I \subsetneq R$, $R \setminus I \subset R^\times$.

Then, if $J \subsetneq R$, $J \cap R^\times = \emptyset$ $\Rightarrow$ $J \subset I$.

So I is unique maximal ideal of R, R local. $\square$

8. a. Suffices to show that every $f \in \mathbb{C}[[x]] \setminus (x)$ is a unit (by Q7c.)

We have $f = a_0 + a_1 x + a_2 x^2 + \dots$, $a_0 \neq 0$.

Let $g = b_0 + b_1 x + b_2 x^2 + \dots \in \mathbb{C}[[x]]$

then $fg = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \dots$

See we can solve $fg = 1$ for coefficients b_i inductively :-

$$a_0 b_0 = 1 \Rightarrow b_0 = a_0^{-1}$$
$$a_0 b_1 + a_1 b_0 = 0 \Rightarrow b_1 = a_0^{-1}(-a_1 b_0)$$
etc.

Thus f is a unit, as required.

b. Clearly $\mathbb{C}[[x]] \subset \mathbb{C}((x)) \subseteq \mathrm{ff}\, \mathbb{C}[[x]]$

Required to prove $\mathbb{C}((x)) = \mathrm{ff}\, \mathbb{C}[[x]]$

Given $f/g \in \mathrm{ff}\, \mathbb{C}[[x]]$

we may write $g = x^n \cdot u$, u unit, by a. (units are power series w/ nonzero const. term.)

Then $f/g = \frac{f \cdot u^{-1}}{x^n} \in \mathbb{C}((x))$. □.

9. $$\frac{a+b\sqrt{3}}{c+d\sqrt{3}} = \frac{(a+b\sqrt{3})\cdot(c-d\sqrt{3})}{c^2-3d^2} \overset{\dagger}{=} \frac{(ac-3bd)}{c^2-3d^2} + \frac{(bc-ad)}{c^2-3d^2}\sqrt{3}$$

$\Rightarrow F = \mathrm{ff}\, R \subset \mathbb{R}$ spanned as $\mathbb{Q}$ vector space by 1 & $\sqrt{3}$

Also 1 & $\sqrt{3}$ linearly independent over $\mathbb{Q}$ ($\sqrt{3}$ irrational)

$\Rightarrow 1, \sqrt{3}$ basis of F over $\mathbb{Q}$.

† NB. $c^2 - 3d^2 \neq 0$ because $\sqrt{3}$ irrational.