Saturday 11/7/15 611 HW6 solutions.

1. $0 \neq a \in R$ is irreducible if a is not a unit & $\nexists$ $a = bc$ w/ b, c not units.

a. i. By the fundamental theorem of algebra, the irreducible elements in $\mathbb{C}[x]$ are the polynomials of degree 1 $c \cdot (x-\alpha)$, $0 \neq c \in \mathbb{C}$, $\alpha \in \mathbb{C}$.

ii. The irreducible elements in $\mathbb{R}[x]$ are

- $c \cdot (x-\alpha)$ $0 \neq c \in \mathbb{R}$, $\alpha \in \mathbb{R}$ (polynomials of degree 1)
- $c \cdot (x-\beta)(x-\overline{\beta})$ $0 \neq c \in \mathbb{R}$, $\beta \in \mathbb{C} \setminus \mathbb{R}$

(equivalently, polynomials ax^2+bx+c of degree 2 s.t. $b^2-4ac < 0$).

Proof: Let $0 \neq f \in \mathbb{R}[x]$, not a unit (i.e., $\deg(f) > 0$)

FTA: $\exists$ $\alpha \in \mathbb{C}$ s.t. $f(\alpha) = 0$.

If $\alpha \in \mathbb{R}$, $(x-\alpha) \mid f(x)$ in $\mathbb{R}[x]$

So f irred $\iff$ $f(x) = c \cdot (x-\alpha)$, $0 \neq c \in \mathbb{R}$

If $\alpha \in \mathbb{C} \setminus \mathbb{R}$, $(x-\alpha) \mid f(x)$ in $\mathbb{C}[x]$

& $f(\bar{\alpha}) = \overline{f(\alpha)} = 0$ $\Rightarrow$ $(x-\bar{\alpha}) \mid f(x)$ in $\mathbb{C}[x]$.

$\alpha \neq \bar{\alpha}$ $\Rightarrow$ $\underbrace{(x-\alpha)(x-\bar{\alpha})}_{\in \mathbb{R}[x]} \mid f(x)$ in $\mathbb{C}[x]$

$\Rightarrow$ $(x-\alpha)(x-\bar{\alpha}) \mid f(x)$ in $\mathbb{R}[x]$,

So f irred $\iff$ $f(x) = c \cdot (x-\alpha)(x-\bar{\alpha})$, $0 \neq c \in \mathbb{R}$. □

2. a. $\mathbb{Z}$ is PID $\Rightarrow$ $\mathbb{Z}$ Noetherian.

F field $\Rightarrow$ ideals are $\langle 0 \rangle = (0)$ & $F = (1)$

$\Rightarrow$ F Noetherian.

b. R Noetherian $\Rightarrow$ $R[x]$ Noetherian. (Hilbert basis theorem)

$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n]$.

Now a + HBT + induction $\Rightarrow$ $\mathbb{Z}[x_1, \dots, x_n]$, $F[x_1, \dots, x_n]$ Noeth.

c. $q: R \longrightarrow R/I$ quotient hom. $q(a) = a+I$.

$\leadsto K \subset R/I$ ideal $\Rightarrow K = J/I = q(J)$, $J \subset R$ ideal, $I \subset J$.

R Noeth $\Rightarrow J = (a_1, \dots, a_n)$, $a_1, \dots, a_n \in R$

$\Rightarrow K = q(J) = (q(a_1), \dots, q(a_n))$

$\therefore R/I$ Noeth.

d. $\varphi: R \to S$ ring hom.

$\varphi(R) \underset{\text{FIT}}{\simeq} R/\ker\varphi$. $\therefore R$ Noeth $\overset{c}{\Rightarrow} R/\ker\varphi$ Noeth

$\Rightarrow \varphi(R)$ Noeth.

e. We have surj. hom $\varphi: A[x_1, \dots, x_n] \longrightarrow R$

$\varphi(f(x_1, \dots, x_n)) = f(\alpha_1, \dots, \alpha_n)$

$\therefore$ By b+d, $R = \varphi(A[x_1, \dots, x_n])$ is Noeth.

3. a. $\left(\sum a_{ij} x^i y^j\right) \cdot \left(\sum b_{ij} x^i y^j\right) = \sum_{i,j} \left(\sum_{\substack{k+l=i \\ m+n=j}} a_{km} b_{ln} \right) x^i y^j$

$= \sum_{i,j} c_{ij} x^i y^j$

In particular $c_{0j} = \sum_{m+n=j} a_{0m} b_{0n}$.

So $R \subset S$ is closed under multiplication.

Also $(R,+) \subset (S,+)$ is a subgroup & $1 \in R$

So R is a subring.

b. $I_n := (x, xy, xy^2, \dots, xy^n) \subset R$.

Claim: $I_n \subsetneq I_{n+1} \quad \forall n \geq 0$. ($\Rightarrow$ R not Noeth.)

Proof: Required to prove $xy^{n+1} \notin I_n$

i.e. $\nexists\ r_0, \dots, r_n \in R$ s.t. $xy^{n+1} = r_0 x + r_1 xy + \dots + r_n xy^n$

Writing $r_k = \sum a_{ijk} x^i y^j$,

Coefficient of monomial xy^{n+1} in $r_0 x + \dots + r_n xy^n$
equals $a_{0,n,0} + a_{0,n-1,1} + \dots + a_{0,1,n} = 0$. $\square$.

4. a. $\mathbb{Z} \supsetneq (2) \supsetneq (2^2) \supsetneq \dots$

b. $R[x] \supsetneq (x) \supsetneq (x^2) \supsetneq \dots$

c. If $R > I_1 \supsetneq I_2 \supsetneq \dots$

then $|I_n| \leq |R| - (n-1) < 0$ for $n \gg 0$ $\#$.

d. If $I \subset R$ is an ideal then I is a subspace of
the F-vector space R
($(I, +) \subset (R, +)$ is a subgroup, & $\lambda \cdot v \in I$ for $\lambda \in F$
& $v \in I$ (because more generally $r \cdot v \in I$ for $r \in R$ & $v \in I$)).
$\therefore$ If $R > I_1 \supsetneq I_2 \supsetneq \dots$
then $\dim_F I_n \leq \dim_F R - (n-1) < 0$ for $n \gg 0$ $\#$.

$e \leq c$

$f \leq d$ (because $F[x]/(f)$ has basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$, where $\alpha = x + (f)$, & $n = \deg(f)$, in particular $\dim_F \left(F[x]/(f)\right) = n < \infty$)

5. a.

$$R[x] \xrightarrow{\varphi} F$$

$$\varphi(f(x)) = f(1/a)$$

$$\varphi(R[x]) = S := \{ b/a^n \mid b \in R, n \in \mathbb{Z}_{\geq 0} \} \subset F.$$

(claim: $\ker \varphi = (ax-1)$ $\left(\underset{\text{FIT}}{\Rightarrow} R_a := R[x]/(ax-1) \xrightarrow[\bar{\varphi}]{\sim} S \right)$

Proof: Let $f \in \ker \varphi$, i.e. $f(1/a) = 0$.

We certainly have $(x - 1/a) \mid f$ in $F[x]$.

Required to prove $(ax-1) \mid f$ in $R[x]$.

Proof by induction on $\deg(f)$

$f = a_n x^n + \dots + a_1 x + a_0$.

$f(1/a) = 0 \quad a_n a^{-n} + \dots + a_1 a^{-1} + a_0 = 0.$

Clear denominators $a_n + a_{n-1} a + \dots + a_0 a^n = 0.$

$\Rightarrow a \mid a_n$, $a_n = q \cdot a$.

$g := f - q x^{n-1}(ax-1)$, $\deg(g) < \deg(f)$, $g \in \ker \varphi$.

Base case: $n = 0$. $f(1/a) = 0 \Rightarrow f = 0$ ✓. □.

b. $\ker \varphi = R \cap (ax-1)$ by definition of φ.

($(ax-1) = \ker \left(R[x] \to R[x]/(ax-1) \right)$ & $R \subset R[x]$)

To compute $R \wedge (ax-1)$:-

$R \ni b = (ax-1)\cdot(a_n x^n + \cdots + a_1 x + a_0)$ $\quad a_0, \ldots, a_n \in R$

$\iff a \cdot a_n = 0$

$a \cdot a_{n-1} - a_n = 0$

$\vdots$

$a \cdot a_0 - a_1 = 0$

$-a_0 = b.$

$\iff a^{n+1} \cdot b = 0 \qquad (\text{if } a_i = a^i \cdot (-b))$

$\therefore \ker \varphi = \{ b \in R \mid a^n \cdot b = 0 \text{ , some } n \in \mathbb{N}^! s. \}$

e.g. $R = \mathbb{C}[s,t]/(st)$ $\quad a = s \in R.$

$$R_a = \left(\mathbb{C}[s,t]/(st)\right)[x] \Big/ (ax-1)$$

$$= \mathbb{C}[s,t,x]/(st, sx-1)$$

Note, by b, $s \cdot t = 0 \in R \Rightarrow t = 0 \in R_a.$

(Explicitly $t = -t \cdot (sx-1) + x \cdot (st) = 0 \in R_a$)

i.e. $t \in (sx-1, st)$

$$\therefore \mathbb{C}[s,t,x]/(st, sx-1) = \mathbb{C}[s,t,x]/(t) \Big/ (st, sx-1)/(t)$$

$$= \mathbb{C}[s,x]/(sx-1) = \mathbb{C}[x]_x \overset{a.}{=} \left\{ \frac{a(x)}{x^n} \;\middle|\; a(x) \in \mathbb{C}[x], n \geq 0 \right\}$$

field of rational functions in x $\longrightarrow \mathbb{C}(x) = ff(\mathbb{C}[x])$

6. $R = \mathbb{Z}[\sqrt{-2}] = \{a+b\sqrt{-2} \mid a,b \in \mathbb{Z}\} \subset \mathbb{C}$.

Define $\sigma : R \to \mathbb{Z}_{\geq 0}$

$\sigma(\alpha) = |\alpha|^2$

i.e. $\sigma(a+b\sqrt{-2}) = a^2+2b^2$

Claim: R is an ED w/ size function σ ($\Rightarrow R$ UFD)

Proof: Given $\alpha, \beta \in R$, $\beta \neq 0$,

required to prove $\exists\ q, r \in R$ s.t.

$\alpha = q\beta + r$ & $\sigma(r) < \sigma(\beta)$.

$\alpha/\beta \in \mathbb{C}$. $\exists\ q \in R$ s.t. $\left|\alpha/\beta - q\right|^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 \sqrt{2}^2$

(because WMA $\alpha/\beta - q = x + y\sqrt{-2}$, $|x|, |y| \leq 1/2$) $= 3/4 < 1$

Then $\alpha = q\beta + r$,

$$|r|^2 = |q|^2 \cdot \left|\alpha/\beta - q\right|^2 < |q|^2. \quad \square$$

7. R is a subring $\iff \left(\frac{(1+\sqrt{d})}{2}\right)^2 \in R$

$$\| $$

$$\frac{1+d}{4} + \frac{\sqrt{d}}{2}$$

$\iff 1+d \equiv 2 \bmod 4$

$\iff d \equiv 1 \bmod 4$.

8. Arguing as in Q6, given $\alpha, \beta \in R$, $\beta \neq 0$

$\exists\ q \in R$ s.t. $\alpha/\beta - q = x + y\cdot(w)$, $|x|, |y| \leq 1/2$

$$\Rightarrow \left|\alpha/\beta - q\right|^2 = (x - \tfrac{1}{2}y)^2 + \left(\tfrac{\sqrt{3}}{2}y\right)^2 = x^2 - xy + y^2 \leq 3\cdot\left(\tfrac{1}{2}\right)^2 < 1$$

Then $\alpha = q\beta + r$, $|r|^2 < |q|^2$.

So R ED, $\Rightarrow$ UFD. $\square$

1. $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0$.

$\alpha \in F$, $\alpha = a/b$, $f(\alpha) = 0$. Here $a, b \in R$, & WMA $\gcd(a,b) = 1$.

Clearing denominators $a^n + a_{n-1}a^{n-1}b + \dots + a_1 a b^{n-1} + a_0 b^n = 0$

$\Rightarrow b \mid a^n$.

BUT $\gcd(a,b) = 1$, so have b is a unit, $\alpha \in R$.

10. $\tau = \frac{1+\sqrt{5}}{2} \in F = \mathrm{Frac}\, R \subset \mathbb{R}$, $\tau \notin R$.

$\tau^2 = \tau + 1$ i.e. τ satisfies monic polynomial

$f(x) = x^2 - x - 1 \in \mathbb{Z}[x] \subset R[x]$.

Now by 69 see R is NOT UFD.

11. a. Just check $\theta((a+b\sqrt{+2})(c+d\sqrt{+2})) \stackrel{?}{=} \theta(a+b\sqrt{+2})\,\theta(c+d\sqrt{+2})$

$\theta((ac+2bd) + (ad+bc)\sqrt{+2}) = (a-b\sqrt{+2})\cdot(c-d\sqrt{+2})$ ✓

$\therefore \sigma(\alpha\beta) = |\alpha\beta\cdot\theta(\alpha\beta)| = |\alpha\beta\,\theta(\alpha)\,\theta(\beta)|$

$= |\alpha\cdot\theta(\alpha)|\cdot|\beta\cdot\theta(\beta)| = \sigma(\alpha)\,\sigma(\beta)$.

b. $\sigma(\alpha) = 0 \iff a^2 = 2b^2$, $a, b \in \mathbb{Z}$

$\iff a = b = 0$ (because $\sqrt{2}$ is irrational)

c. α unit $\iff \exists\, \beta.\ \alpha\beta = 1 \Rightarrow \sigma(\alpha)\sigma(\beta) = \sigma(1) = 1$

$\Rightarrow \sigma(\alpha) = \sigma(\beta) = 1$.

Conversely, if $\sigma(\alpha) = 1$, $\alpha = a + b\sqrt{+2}$, $\alpha^{-1} = \frac{a - b\sqrt{+2}}{a^2 - 2b^2} = \frac{a - b\sqrt{2}}{\pm 1} \in R$.

$\uparrow$ $\mathbb{R}$

$\square$.

d. $a^2 - 2b^2 = \pm 1$

has a solution $a = b = 1$

$\therefore \alpha = 1+\sqrt{2}$ is a unit in R $(\sigma|\alpha| = 1)$

Now $R^\times \supset \{\alpha^n \mid n \in \mathbb{Z}\}$

$\Rightarrow R^\times$ infinite (since $\alpha > 1$)

e. Show R is an ED for size function σ ($\Rightarrow$ UFD)

Again, given $\alpha, \beta \in R$, $\beta \neq 0$,

have $\alpha/\beta = u + v\sqrt{2}$, $u, v \in \mathbb{Q}$

Then $\exists\ q \in R$ s.t. $\alpha/\beta - q = x + y\sqrt{2}$, $|x|, |y| \leq \frac{1}{2}$, $x, y \in \mathbb{Q}$

$\Rightarrow \sigma(x+y\sqrt{2}) := |x^2 - 2y^2| \leq 2 \cdot \left(\frac{1}{2}\right)^2 = \frac{1}{2} < 1.$

Now $\alpha = q\beta + r$

$\sigma(r) = \sigma(q) \cdot \sigma(\alpha/\beta - q) < \sigma(q)$

↑ NB σ is multiplicative on $\mathbb{Q}(\sqrt{2}) = \mathrm{Frac}\, R$, as in (a).

□.

12. $R = \mathbb{C}[x,y]/(y^2 - x^3) \xrightarrow{\sim} S \subset \mathbb{C}[t]$

$S = \{\sum a_i t^i \mid a_1 = 0\}$

$x \longmapsto t^2$

$y \longmapsto t^3$.

Have equality $y^2 = x^3$, $y \cdot y = x \cdot x \cdot x$ in R.

Suffices to show x & y are irreducible in R. (then R NOT UFD)

Equivalently, t^2 & t^3 are irred. in S.

But a factorization in S will be in particular a factorization in $\mathbb{C}[t]$

$a = bc$

Only possibilities for t^2 & t^3 are

$t^2 = t \cdot t$ & $t^3 = t \cdot t^2$ (assuming factors are not units)
i.e. not constant

But $t \notin S$.

So t^2 & t^3 are irred. in S.

Alternatively, $t \in F := \mathrm{Frac}\, S = \mathrm{Frac}\, \mathbb{C}[t] = \mathbb{C}(t)$,

↑ because $t = t^3/t^2$, $t^2, t^3 \in S$.

But $t \notin S$, & t satisfies monic polynomial

$f(x) = x^2 - t^2 \in S[x]$

$\Rightarrow$ S NOT UFD.

Q9.