Wednesday 12/2/15 611 HW7 solutions.

1. Suppose (for a contradiction) there are only finitely many monic irreducible polynomials $p_1, \dots, p_n$.
Consider $f = p_1 p_2 \cdots p_n + 1. \in F[x]$.
Let p be a monic irreducible factor of f.
$p_i \nmid f \ \forall i \implies p \neq p_i \ \forall i$ #. $\square$

2. $x, \ x+1, \ x^2+x+1, \ x^3+x+1, \ x^3+x^2+1, \ x^4+x+1, \ x^4+x^3+1, \ x^4+x^3+x^2+x+1$

3. a. $\deg f = 3$, so f irred $\iff \nexists$ root $\alpha = a/b \in \mathbb{Q}$

$$f = 1 \cdot x^3 + 4 \cdot x + 1 \implies b \mid 1, \ a \mid 1, \ \alpha = \pm 1.$$

Check $x = \pm 1$ is not a root: $f(1) = 6$, $f(-1) = -4$.
So f irred.

b. $(x^2+1)(x^2+9)$ (these factors are irreducible over $\mathbb{Q}$ because degree 2 & no roots in $\mathbb{Q}$)

c. $(x^6 - 1) = (x^3-1)(x^3+1)$
$= (x-1)(x^2+x+1)(x+1)(x^2-x+1)$ irreducibles (as in b.)

d. $f \equiv x^4+x^3+x^2+x+1 \mod 2$, irred (see Q2)
$\implies f$ irred in $\mathbb{Z}[x]$

~~f~~
e $57 = 3 \cdot 19$ prime factorization.
Eisenstein, $p = 3 \implies x^n + 57$ irreducible.

4. a. $x^n + (y^n - 1) \in \mathbb{C}[y][x]$
$(y-1) \mid (y^n - 1)$, $(y-1)^2 \nmid (y^n-1) \implies$ irreducible in $\mathbb{C}(y)[x]$.
primitive $\implies$ irreducible in $\mathbb{C}[y][x]$
$= \mathbb{C}[x,y]$.

b. $y \cdot x^n + z^n \cdot x + y^n z \in (\mathbb{C}[y,z])[x] \subset \underbrace{FF\,\mathbb{C}[y,z]}_{=\mathbb{C}(y,z)}$

$z \mid z^n, \quad z \mid y^n z, \quad z^2 \nmid y^n z \overset{\text{Eisenstein}}{\Rightarrow}$ irred in $\mathbb{C}(y,z)[x]$

$\gcd(y, z^n, y^n z) = 1$ in $\mathbb{C}[y,z]$, i.e. primitive,
$\Rightarrow$ irred in $\mathbb{C}[y,z][x]$
$= \mathbb{C}[x,y,z]$

5. If f is reducible in $\mathbb{Q}[x]$ then f is reducible in $\mathbb{Z}[x]$ by the Gauss Lemma, $f = g \cdot h$, $g, h \in \mathbb{Z}[x]$, $\deg g, \deg h > 0$.

$\deg f = 2n+1$ odd $\Rightarrow \deg g \neq \deg h$, say $\underbrace{\deg g}_{=m} < \deg h$

$$f = a_{2n+1} x^{2n+1} + \dots + a_1 x + a_0 = gh$$

$p \nmid a_{2n+1}$, $p \mid a_{2n}, \dots, a_{n+1}$, $p^2 \mid a_n, \dots, a_0$, $p^3 \nmid a_0$.

Modulo p: $\bar{f} = \bar{a}_{2n+1} x^{2n+1} = \bar{g} \cdot \bar{h}$ (bars denote reduction mod p)

$\Rightarrow \quad g = b_m x^m + \dots + b_0, \quad \bar{g} = \bar{b}_m x^m$

$h = c_l x^l + \dots + c_0, \quad \bar{h} = \bar{c}_l x^l$, $m+l = 2n+1$, $m < l$; $\bar{b}_m \bar{c}_l = \bar{a}_{2n+1} \neq 0$.

i.e. $p \mid b_{m-1}, \dots, b_0$, $p \nmid b_m$
$p \mid c_{l-1}, \dots, c_0$, $p \nmid c_l$.

Coefficient of x^m in f

$$a_m = b_m c_0 + b_{m-1} c_1 + \dots + b_0 c_m$$

$p^2 \mid a_m \quad (m \leq n)$

$p \mid b_{m-1}, \dots, b_0, \quad p \mid c_1, \dots, c_m \quad (m < l)$

$\Rightarrow p^2 \mid b_m c_0 \Rightarrow p^2 \mid c_0.$

Then $a_0 = b_0 c_0$, $p^3 \mid a_0$ # $\square$.

6. a. $\mathbb{Q}[x] / \ker\varphi \xrightarrow[\text{FIT}]{\sim} \varphi(\mathbb{Q}[x]) \subset \mathbb{C}$

$\mathbb{C}$ integral domain $\Rightarrow$ $\varphi(\mathbb{Q}[x])$ integral domain
$\Rightarrow$ $\ker\varphi \subset \mathbb{Q}[x]$ prime ideal

i.e. $\ker\varphi = \{0\}$ or (m),
m irreducible in $\mathbb{Q}[x]$
(& WMA m monic).

b. $\mathbb{Q}[x] / \ker\varphi \xrightarrow{\sim} \mathbb{Q}[\alpha] := \varphi(\mathbb{Q}[x])$.

So $\mathbb{Q}[\alpha]$ field $\Leftrightarrow$ $\ker\varphi \subset \mathbb{Q}[x]$ maximal
$\Leftrightarrow$ $\ker\varphi \neq \{0\}$ $\square$.

7. $R/(p) = \mathbb{Z}[i]/(p) \cong \mathbb{Z}[x]/(p, x^2+1) \cong \mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$

$p = 2$: $x^2+1 = (x+1)^2$. $x+1 \mapsto y$

$\mathbb{Z}/2\mathbb{Z}[x]/((x+1)^2) \cong \mathbb{Z}/2\mathbb{Z}[y]/(y^2)$

$p \equiv 1 \bmod 4$. $\quad (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$

$\Rightarrow \quad \exists \; \alpha \in (\mathbb{Z}/p\mathbb{Z})^\times$ of order 4

$\Rightarrow \quad \alpha^2 = -1$

$\Rightarrow \quad x^2+1 = (x+\alpha)(x-\alpha) \qquad (\text{\& } \alpha \neq -\alpha \; : \; p \neq 2)$

$\Rightarrow \quad \mathbb{Z}/p\mathbb{Z}[x]/(x^2+1) \xrightarrow{\sim} (\mathbb{Z}/p\mathbb{Z})^2$

using CRT and FIT.

$p \equiv 3 \bmod 4$. Similarly $\not\exists \; \alpha \in \mathbb{Z}/p\mathbb{Z}$ s.t. $\alpha^2 = -1$

$\Rightarrow \underset{x^2+1}{\overset{\parallel}{f}}$ irred $\quad (\deg f = 2 \,!)$

$\Rightarrow (x^2+1) \subset \mathbb{Z}/p\mathbb{Z}[x]$ maximal,

so $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$ is a field

In general $\mathbb{Z}/p\mathbb{Z}[x]/(x^2+1)$ has order p^2 by the division algorithm.

(each element is represented uniquely by $a+bx$, some $a, b \in \mathbb{Z}/p\mathbb{Z}$).

8. Basis $1, x, x^2, \ldots, x^{n-1}$

matrix $A = \begin{pmatrix} 0 & & & 0 \\ 1 & 0 & & \\ & 1 & \ddots & \\ 0 & & 1 & 0 \end{pmatrix}$

9. a. False. e.g. $\{2\} \subset \mathbb{Z}$ linearly independent,

but only bases of $\mathbb{Z}$ are $\{1\}$ & $\{-1\}$.

b. False. e.g. $\{2,3\} \subset \mathbb{Z}$ spans $\mathbb{Z}$ but does not contain a basis.

c. i. False. e.g. $\varphi: \mathbb{Z} \to \mathbb{Z}$ $\varphi(x) = 2x$.
injective, not surjective.

ii. True: Proof. Since φ is surjective there exist $v_1, \dots, v_n \in M$ s.t. $\varphi(v_i) = e_i$ (standard basis vector in $M = R^n$)
Let B be the matrix with columns v_i,
then $AB = I_n$.
$\Rightarrow$ $\det A \cdot \det B = 1$
$\Rightarrow$ $\det A$ a unit
$\Rightarrow$ A invertible (& $A^{-1} = B$). $\square$

10. a. By the division algorithm, any element of $R[x]/(f)$ has a unique representative in $R[x]$ of degree $< n$,
$r = a_{n-1}x^{n-1} + \dots + a_1 x + a_0$, $a_i \in R$.

Equivalently (the images of) $1, x, \dots, x^{n-1}$ in $R[x]/(f)$ form a R-module basis.

b. $\mathbb{Z}[x]/(2x-1) \xrightarrow{\sim} \left\{ \frac{a}{2^n} \;\middle|\; a \in \mathbb{Z}, n \in \mathbb{Z}, n \geq 0 \right\} \subset \mathbb{Q}$
$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad =: A$

induced by $\varphi: \mathbb{Z}[x] \to \mathbb{Q}$ (FIT)
$\varphi(f(x)) = f(1/2)$

Any two elements in A satisfy a nontrivial relation:
$$(2^n \cdot b)\frac{a}{2^n} - (2^m \cdot a)\frac{b}{2^m} = 0.$$

Also A is not spanned by one element:

$$\left\{ c \cdot \frac{a}{2^n} \;\middle|\; c \in \mathbb{Z} \right\} \subsetneq A$$

So A is not a free $\mathbb{Z}$-module

11.
$$\begin{array}{ccc} R^n & \xrightarrow{\varphi} & R^m \\ i \cap & & \cap\, i \\ F^n & \xrightarrow[\varphi_F]{} & F^m \end{array}$$
commutative diagram.

$\therefore$ φ_F injective $\Rightarrow$ $\varphi_F \circ i$ injective
$$\begin{array}{c} \varphi_F \circ i \\ \| \\ i \circ \varphi \end{array}$$
$\Rightarrow$ φ injective.

Conversely, suppose φ injective.
If $\varphi_F(v) = 0$, some $v \in F^n$, let $0 \neq r \in R$ be such that $r \cdot v \in R^n$.
Then $\varphi(r \cdot v) = \varphi_F(r \cdot v) = r \cdot \varphi_F(v) = 0$
φ inj.
$\Rightarrow$ $r \cdot v = 0$ $\Rightarrow$ $v = 0$
So φ_F is injective.

12. $a \Rightarrow b$ Choose $v_1, \dots, v_m \in R^n$ s.t. $\varphi(v_i) = e_i$
& let B be matrix w/ columns v_i
Then $AB = I_m$.

$b \Rightarrow a$ AB surjective $\Rightarrow$ A surjective.

$b \Rightarrow c.$ $1 = \det(AB) \in J$ by multilinearity of the determinant c => b. Write $1 = \sum_I r_I \det(A_I)$, where the sum is over $I \subset \{1,..,n\}$, $|I| = m$,

A_I is the $m\times m$ submatrix of A formed by the columns labelled by I & $r_I \in R$.

Now $A_I \cdot \operatorname{adj} A_I = (\det A_I) \cdot I_m$

Let B_I be the $n \times m$ matrix w/ the rows labelled by I being the rows of $\operatorname{adj} A_I$, & all other rows zero.

Then $A \cdot B_I = A_I \cdot \operatorname{adj} A_I$

So, defining $B = \sum r_I \cdot B_I$, we have $AB = I_m$. $\square$.

13. a.

Given M an R-module,

M is an abelian group under + (a $\mathbb{Z}$-module)

and $\varphi: M \to M$, $\varphi(m) = i \cdot m$

is a homomorphism of abelian groups such that $\varphi(\varphi(m)) = i^2 m$
$= -m$.

Conversely, given A & φ, we can give A the structure of an R-module by defining $(a+bi)\cdot m = a\cdot m + b\cdot\varphi(m)$ for $a,b \in \mathbb{Z}$ & $m \in A$.

b. $\mathbb{Z}/p\mathbb{Z}$ has the structure of an R-module iff $\exists\ \varphi: \mathbb{Z}/p\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ s.t. $\varphi^2 = -\mathrm{id}$.

$\operatorname{Aut}(\mathbb{Z}/p\mathbb{Z}) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$.

$(x \mapsto ax) \leftarrow a$

So such a φ corresponds to $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ s.t. $a^2 = -1$. in $\mathbb{Z}/p\mathbb{Z}$.
Hence φ exists iff $p = 2$ or $p \equiv 1 \bmod 4$

For $(\mathbb{Z}/p\mathbb{Z})^2$, we can take $\varphi = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{Aut}((\mathbb{Z}/p\mathbb{Z})^2)$, $= GL_2(\mathbb{Z}/p\mathbb{Z})$

then $\varphi^2 = -\mathrm{id}$.
So $(\mathbb{Z}/p\mathbb{Z})^2$ can be given the structure of an R-module.

14 a. $R = F[x,y]$
M R-module.
The $M = V$ is an F-vector space $(F \subset R)$
and we can define linear transformations
$S: V \to V$ & $T: V \to V$ by $S(v) = x \cdot v$ & $T(v) = y \cdot v$.

Note $S \circ T(v) = x(y \cdot v) = (xy) \cdot v = (yx) \cdot v = T \circ S(v)$.
i.e. $S \circ T = T \circ S$, S & T commute.

Conversely, given V & two commuting linear transformations $S: V \to V$ & $T: V \to V$, we can give $M = V$ the structure of an R-module by defining $f \cdot m = f(S,T) \cdot m$

i.e. $\left(\sum a_{ij} x^i y^j\right) \cdot m = \sum a_{ij} S^i T^j (m)$.

b. Consider
$M = F[x,y] \big/ (x^2, y^3, xy^2)$, an $F[x,y]$-module
Then M is an F-vector space w/ basis $1, x, y, xy, y^2$
Let A & B be the matrices of the linear transformations $S(v) = x \cdot v$ & $T(v) = y \cdot v$ with respect to this basis.

Then $A = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}$

Now $AB = BA$, & $A^i B^j = 0$

$\iff x^i y^j \in (x^2, y^3, xy^2) \subset F[x,y]$

$\iff i \geq 2, \; j \geq 3, \;$ or $(i \geq 1 \text{ \& } j \geq 2.)$

$\square$.