Introduction to Analysis – MA 542 – Fall 2019 – R. Pollack
HW #6 Solutions

Section 29:
2) Let $\alpha = \sqrt{2}+\sqrt{3}$. Then $\alpha^2 = 2+3+2\sqrt{6}$ and so $\alpha^2 - 5 = 2\sqrt{6}$. Squaring again then gives $(\alpha^2-5)^2 = 24$ and thus α satisfies the polynomial $(x^2-5)^2 - 24 = x^4 - 10x^2 + 1$.

4) Let $\alpha = \sqrt{1+\sqrt[3]{2}}$. Then $\alpha^2 = 1+\sqrt[3]{2}$ and $\alpha^2 - 1 = \sqrt[3]{2}$. Cubing now gives $(\alpha^2-1)^3 = 2$ and thus α satisfies the polynomial $(x^2-1)^3 - 2 = x^6 - 3x^4 + 3x^2 - 3$.

6) Let $\alpha = \sqrt{3-\sqrt{6}}$. Then $\alpha^2 = 3-\sqrt{6}$ and $\alpha^2 - 3 = -\sqrt{6}$. Squaring again gives $(\alpha^2-3)^2 = 6$ and thus α satisfies the polynomial $(x^2-3)^2 - 6 = x^4 - 6x^2 + 3$. Note that this polynomial is irreducible by the Eisenstein criteria with $p = 3$. Thus, $\text{irr}(\alpha, \mathbb{Q}) = x^4 - 6x^2 + 3$ and $\deg(\alpha, \mathbb{Q}) = 4$.

12) $\sqrt{\pi}$ is algebraic over $\mathbb{R}$ as it satisfies $x^2 - \pi \in \mathbb{R}[x]$. Since $\sqrt{\pi} \notin \mathbb{R}$, it must be that $\deg(\sqrt{\pi}, \mathbb{R}) = 2$.

16) π^2 is algebraic over $\mathbb{Q}(\pi^3)$ as it satisfies $x^3 - \pi^6 \in \mathbb{Q}(\pi^3)[x]$. This polynomial is irreducible over $\mathbb{Q}(\pi^3)$ as it has no roots in this field (and is a cubic polynomial) and thus is the minimal polynomial. In particular, $\deg(\pi^2, \mathbb{Q}(\pi^3)) = 3$.

18) $x^2 + 1$ is irreducible over $\mathbb{Z}_3$ as it has no roots in this field (and is a quadratic polynomial).

$+$	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
1	1	2	0	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$	α	2α
2	2	0	1	$2+\alpha$	$2+2\alpha$	α	2α	$1+\alpha$	$1+2\alpha$
α	α	$1+\alpha$	$2+\alpha$	2α	0	$1+2\alpha$	1	$2+2\alpha$	2
2α	2α	$1+2\alpha$	$2+2\alpha$	0	α	1α	$1+\alpha$	2	$2+\alpha$
$1+\alpha$	$1+\alpha$	$2+\alpha$	α	$1+2\alpha$	1	$2+2\alpha$	2	2α	0
$1+2\alpha$	$1+2\alpha$	$2+2\alpha$	2α	1	$1+\alpha$	2	$2+\alpha$	0	α
$2+\alpha$	$2+\alpha$	α	$1+\alpha$	$2+2\alpha$	2	2α	0	$1+2\alpha$	1
$2+2\alpha$	$2+2\alpha$	2α	$1+2\alpha$	2	$2+\alpha$	0	α	1	$1+\alpha$

$\cdot$	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	α	2α	$1+\alpha$	$1+2\alpha$	$2+\alpha$	$2+2\alpha$
2	0	2	1	2α	α	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	$1+\alpha$
α	0	α	2α	2	1	$2+\alpha$	$1+\alpha$	$2+2\alpha$	$1+2\alpha$
2α	0	2α	α	1	2	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	$2+\alpha$
$1+\alpha$	0	$1+\alpha$	$2+2\alpha$	$2+\alpha$	$1+2\alpha$	2α	2	1	α
$1+2\alpha$	0	$1+2\alpha$	$2+\alpha$	$1+\alpha$	$2+2\alpha$	2	α	2α	1
$2+\alpha$	0	$2+\alpha$	$1+2\alpha$	$2+2\alpha$	$1+\alpha$	1	2α	α	2
$2+2\alpha$	0	$2+2\alpha$	$1+\alpha$	$1+2\alpha$	$2+\alpha$	α	1	2	2α

23)

a. True

b. True. $\mathbb{C} = \mathbb{R}(i)$.

c. True. α satisfies $x - \alpha \in F[x]$.

d. True.

e. False. There is no injective ring homomorphism from $\mathbb{Z}_2$ to $\mathbb{Q}$ since 1 has no place to map (as $1+1=0$ in $\mathbb{Z}_2$).

f. True. The minimum polynomial of α divides $f(x)$.

g. False. Consider $\alpha = \sqrt{2}$. Then α satisfies $x - \sqrt{2} \in \mathbb{R}[x]$, but $\deg(\sqrt{2}, \mathbb{Q}) = 2$.

h. True.

i. False. Take $F = \mathbb{Q}$ and consider $x^2 + 1$. This polynomial has no roots in $\mathbb{R}$.

j. True.

25) (a) $x^3 + x^2 + 1$ is irreducible over $\mathbb{Z}_2$ as it has no roots and is a cubic polynomial.
(b) We have $x^3 + x^2 + 1 = (x - \alpha)(x - \alpha^2)(x - (1 + \alpha + \alpha^2))$. This question is not very conceptual, but note that $1 + \alpha + \alpha^2 = \alpha^4$ and so the roots of the polynomial are α, α^2 and α^4 and that's no coincidence.

30) By Theorem 29.18, every element of $F(\alpha)$ can be expressed uniquely as $b_0 + b_1\alpha + \cdots + b_{n-1}\alpha^{n-1}$ with each $b_i \in F$. Since F has size q, there are q^n such choices for the coefficients b_i and thus $F(\alpha)$ has size q^n.

31) (a) $x^3 + 2x + 2$ is irreducible in $\mathbb{Z}_3[x]$ as it has no roots and is a cubic.
(b) We know then that $E = \mathbb{Z}_3[x]/\langle x^3 + 2x + 2\rangle$ is a field as $x^3 + 2x + 2$ irreducible implies $\langle x^3 + 2x + 2\rangle$ is maximal. Arguing either using (30) above or the fact that every element of E is uniquely expressible as $a_0 + a_1x + a_2x^3 + \langle x^3 + 2x + 2\rangle$ with $a_i \in \mathbb{Z}_3$ proves that E has size 27.

32) (a) Note that the collection $\{x^2 \mid x \in \mathbb{Z}_p\}$ has size less than p as $x^2 = (-x)^2$ and as long as $x \neq 0$, then $x \neq -x$ when $p > 2$.
(b) There is some element $b \in \mathbb{Z}_p$ such that b is not a square. This implies that $x^2 - b$ is irreducible in $\mathbb{Z}_p$ and we then have that $\mathbb{Z}_p[x]/\langle x^2 - b\rangle$ is a field with p^2 elements as in 31(b) above.

35) $\mathbb{Z}_2[x]/\langle x^3 + x + 1\rangle$ is a field of size 8 as this polynomial is irreducible having no roots in $\mathbb{Z}_2$.

To find a field of size 16, we need an irreducible 4th degree polynomial. Now we can no longer argue just by roots as a 4th degree can be a product of two 2nd degree irreducible polynomials. However, the only irreducible quadratic polynomial in $\mathbb{Z}_2[x]$ is $x^2 + x + 1$ as all of the other have roots. We thus see that $x^4 + x^3 + 1$ is irreducible as it has no roots and is not divisible by $x^2 + x + 1$. Thus $\mathbb{Z}_2[x]/\langle x^4 + x^3 + 1\rangle$ is a field with 16 elements.

Lastly, $x^2 + 2$ over $\mathbb{Z}_5$ as this quadratic polynomial has no roots. Thus $\mathbb{Z}_5[x]/\langle x^2 + 2\rangle$ is a field of 25 elements.

Section 30:
1) {(1,0),(0,1)}, {(1,-1),(1,1)}, {(-1,0),(0,-1)}.

3) This is not a basis as

$$2(-1, 1, 2) + -4(2, -3, 1) + (10, -14, 0) = 0.$$

4) $\{1, \sqrt{2}\}$

6) $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$

15)

a. True.

b. False.

c. True.

d. True.

e. False. For instance, $\mathbb{R}$ is infinite-dimensional over $\mathbb{Q}$.

f. True.

g. False. The zero vector is linearly dependent even with itself as $1 \cdot \mathbf{0} = \mathbf{0}$.

h. True.

i. True.

j. True.

22) (a) This system of equations can be rewritten as:

$$X_1 \begin{pmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{pmatrix} + \cdots + X_n \begin{pmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix} \tag{1}$$

and so there is a solution to this system of equation iff $\begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ is in the span of the vectors $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$.

(b) If $m = n$ and the vectors $\begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ form a basis for $j = 1, ...m$, then there is one and only one way to solve the vector equation (1) and thus the system of equations has a unique solution.

24) (a) For any $v \in V$, write $v = \sum_i c_i \beta_i$. Then $\phi(v) = \sum c_i \phi(\beta_i)$ by linearity and one sees that the values of $\phi(\beta_i)$ determine the value of $\phi(v)$.

(b) By part (a) there is clearly at most one map. One thus needs to check that this map is actually linear, but this is clear.