Takehome solutions:

1. (a) Let $\mathcal{N}$ be the norm defined in part (b), and observe that $\mathcal{N}(\alpha\beta) = \mathcal{N}(\alpha) + \mathcal{N}(\beta)$. As $\mathcal{N}(1) = 0$, any unit α must have $\mathcal{N}(\alpha) = 0$, i.e. have const term $a_0 \neq 0$. Conversely, assuming $\mathcal{N}(\alpha) = 0$, we will construct the inverse $\beta = \sum b_n t^n$ inductively as follows:

   (i) Define $b_0 = 1/a_0$

   (ii) Having defined $b_0, \ldots, b_k$ so that

   $$\alpha \cdot (b_0 + b_1 t + \cdots + b_k t^k) = 1 + c_{k+1} t^{k+1} + \text{higher order terms}$$

   set $b_{k+1} = -c_{k+1}/a_0$, which insures

   $$\alpha \cdot (b_0 + \cdots + b_{k+1} t^{k+1}) = 1 + c'_{k+2} t^{k+2} + \text{higher order terms.}$$

(b) Let $\alpha, \beta \in R$ with β nonzero. Let $k = \mathcal{N}(\beta)$ and let $\gamma = \sum_{n=0}^{k-1} a_n t^n$. Let $u = \sum_{n=0}^{\infty} b_{n-k} t^n$ which we uformally denote $u = t^{-k} \cdot \beta$ even though $t^{-k} \notin R$.

Now u is a unit in R, so can solve

$$t^{-k}(\underbrace{\alpha - \gamma}_{\mathcal{N} \geq k}) = \delta u \quad \text{for } \delta \text{ in } R.$$

Thus $\alpha - \gamma = \delta\beta$ or $\alpha = \delta\beta + \gamma$ with $\gamma = 0$ or $N(\gamma) < N(\beta)$. So N makes R into a Euclidean domain.

(c) First, the element t is irred in R since if $t = \alpha \cdot \beta$ then $N(\alpha) + N(\beta) = 1$ $\Rightarrow$ one of α, β has norm 0 and is hence a unit by part (a). Since R is Euclidean, it is a P.I.D, and so t is also prime. The irreducibility of $x^n - t$ now follows immediately from Eisenstein's crititerion with the prime $p = t$.

2. (a) Set $I = (1+i)$. Given $\bar{r} = a+bi + I$ in $\bar{R} = R/I$, note $\bar{r} = a+bi - b(1+i) + I = \underbrace{a-b}_{\in \mathbb{Z}} + I$. As $2 = (1-i)(1+i)$ is in I, we see $\bar{r} = I$ or $\bar{r} = 1+I$, and so $|\bar{R}| \leq 2$. Now $1+i$ is not a unit ($N(1+i) = 2$) and so $I \neq R$ $\Rightarrow |\bar{R}| = 2$. So $\bar{R}$ is a ring with two elements and hence a field as $\bar{1}$ in $\bar{R}$ is its own mult. inverse.

(b) Consider the map $R \longrightarrow I_n/I_{n+1}$. By distributivity of ring multiplication, $r \longmapsto \pi^n r + (\pi^{n+1})$ this is a homomorphism of additive groups (though not rings).

Since $\pi \longmapsto 0$, we get a map $\phi: (\bar{R} = R/I_1) \longrightarrow I_n/I_{n+1}$

$$r + I_1 \longmapsto \pi^n r + I_{n+1}$$

Clearly, ϕ is onto, so just need to show ϕ is 1-1.

Suppose $\pi^n r + I_{n+1} = 0$, i.e. $\pi^n r \in I_{n+1}$ and so $\pi^n r = s\pi^{n+1}$ for some $s \in R$. As R is an int. domain, get $r = s\pi$ $\Rightarrow r \in I_1$. So ϕ is an isomorphism.

(c) The nested ideals $R \supseteq I_1 \supseteq I_2 \supseteq \cdots \supseteq I_n$ give rise give to subgroups $S_0 \supseteq S_1 \supseteq S_2 \supseteq \cdots \supseteq S_n$ of $\bar{R}_n = R/(\pi^n)$ via $S_k = \phi(I_k)$. (Here $\bar{R}_n$ is an <u>abelian</u> group under $+$). Now $S_0 = \bar{R}_n$ and $S_n = \{1\}$.

As $\bar{\phi}: I_k/I_{k+1} \longrightarrow S_k/S_{k+1}$ is an isomorphism,

have $|S_k/S_{k+1}| = |R/(\pi)|$ by part (b). Hence

$$|R/(\pi^n)| = |R/(\pi)|^n.$$

(d) No. Note that $4 = (1+i)^3 \cdot (-1-i)$ is in (π^3) and hence any elt of $\mathbb{Z}/(\pi^3)$ has (additive) order at most 4. Since $\mathbb{Z}/8\mathbb{Z}$ has an elt of order 8, these are distinct groups under $+$.

3. $D_1, D_2 \in F$ (a field of char $\neq 2$), neither of which is a square in F. Prove $K = F(\sqrt{D_1}, \sqrt{D_2})$ has $[K:F] = 4$ is $D_1 D_2$ is not a square in F and $= 2$ otherwise.

Pf. Let $L = F(\sqrt{D_1}) \subseteq K$. As D_1 is not a square in F, the polynomial $f(x) = x^2 - D_1$ is inducible in $F[x]$. Hence $[L:F] = 2$ and an F-basis for L is $\{1, \sqrt{D_1}\}$

(a) $\sqrt{D_2} \in L$. Then $\sqrt{D_2} = a \cdot 1 + b\sqrt{D_1}$ for $a, b \in F$. Squaring gives $D_2 = 2ab\sqrt{D_1} + a^2 b^2 D_1$. As char $F \neq 2$ and $D_2 \in F$, must have one of $a, b = 0$ so that $2ab\sqrt{D_1} = 0$. As $\sqrt{D_2} \notin F$, must have $a = 0$, so that $\sqrt{D_2}/\sqrt{D_1} = b \in F$ Then $\sqrt{D_1} \cdot \sqrt{D_2} = bD_1$ so $D_1 D_2$ has a square root in F, as claimed.

(b) $\sqrt{D_2} \notin L$. In this case $x^2 - D_2$ is irred in $L[x]$, so $[K = L(\sqrt{D_2}) : L] = 2$. Thus

$$[K:F] = [K:L][L:F] = 4 \text{ as needed.}$$

4. $F = \mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ where $\alpha_i^2 \in \mathbb{Q}$ for all n. Prove $\sqrt[3]{2} \notin F$.

Pf: Set $F_k = \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$. Since α_{k+1} satisfies $X^2 - \underbrace{\alpha_{k+1}^2}_{\in \mathbb{Q}}$ in $F_k[x]$, have $[F_{k+1} : F_k] = 1$ or 2.

Hence $[F : \mathbb{Q}] = \prod [F_{k+1} : F_k] = 2^l$ for some $l \in \mathbb{Z}_{\geq 0}$.

But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ by class, so $\mathbb{Q}(\sqrt[3]{2})$ can't be contained in F.

5. K/F of degree n, $\alpha \in K$. Fix $\alpha_1, \ldots, \alpha_n$ a K basis for F. From class, know we have an injective ring homomorphism

$$\Phi : K \longrightarrow M_n(F) \quad \text{sending } \alpha \text{ to } A = \begin{pmatrix} \text{matrix of the} \\ \text{linear trans} \\ K \to K \\ \beta \mapsto \alpha\beta \end{pmatrix}$$

Let $p(x) =$ char poly of A. By Cayley-Hamilton, $p(A) = 0$; as $p(x) \in F[x]$ and $\Phi(f \in F) = f \cdot Id$

we have $\Phi(p(\alpha)) = p(\Phi(\alpha)) = p(A) = 0$

As Φ is 1-1, can conclude $p(\alpha) = 0$.

The poly you get for $1 + \sqrt[3]{2} + \sqrt[3]{4}$ is $x^3 - 3x^2 - 3x - 1$