Homework 1 Key

12.2.1)

(a) Since $1 = 3$, we have $x^3 + x^2 + x + 1 = x^3 + 3x^2 + 3x + 1 = (x+1)^3$, and $x + 1$ is irreducible in $\mathbb{F}_2[x]$.

(b) Since $-3 = 2$, we have $x^2 - 3x - 3 = x^2 - 3x + 2 = (x+3)(x-1) = (x-2)(x-1)$, and $x - 2, x - 1$ are irreducible in $\mathbb{F}_5[x]$.

(c) Notice that $x^2 + 1$ is a polynomial of degree 2, so if it is reducible in $\mathbb{F}_7[x]$, it must be of the form $(x-a)(x-b)$ for $a, b \in \mathbb{F}_7$. In particular, $x^2 + 1$ must have a root in $\mathbb{F}_7$. However, testing each possibility,

- $0^2 + 1 = 1 \neq 0$
- $1^2 + 1 = 2 \neq 0$
- $2^2 + 1 = 5 \neq 0$
- $3^2 + 1 = 10 = 3 \neq 0$
- $4^2 + 1 = 17 = 3 \neq 0$
- $5^2 + 1 = 26 = 5 \neq 0$
- $6^2 + 1 = 37 = 2 \neq 0$

Since none of these are 0, $x^2 + 1$ is irreducible in $\mathbb{F}_7[x]$.

12.2.4) Let $f_1, \dots, f_k$ be monic irreducible polynomials in $F[x]$ for a field F. We can assume that $k \geq 2$, because in any field F, x and $x+1$ are distinct monic irreducible polynomials. Consider the monic polynomial

$$f := f_1 \cdots f_k + 1.$$

Notice that f has degree $\deg f_1 + \deg f_2 + \cdots + \deg f_k$, which is strictly greater than $\deg f_i$ for any i (this is true since constant polynomials over a field are either 0 or are units, so are not irreducible). Thus f is distinct from each f_i. Assume that $f_i \mid f$ for some i. Then $f = f_i g$ for some $g \in F[x]$, so

$$f_i \left(g - f_1 \cdots f_{i-1} f_{i+1} \cdots f_k\right) = 1.$$

Thus f_i is a unit, a contradiction, so $f_i \nmid f$ for each i. Since $F[x]$ is a UFD, f must have some irreducible factor f_{k+1} that is distinct from f_i for $1 \leq i \leq k$, and by multiplying by a unit we can assume f_{k+1} is monic. We conclude that there are infinitely many monic irreducible polynomials in $F[x]$.

12.2.6) (a) Every element in $\mathbb{Z}[\omega]$ is of the form $a+b\omega$ because of the relation $\omega^2=-\omega-1$. Let $\sigma:\mathbb{Z}[\omega]\setminus\{0\}\to\mathbb{Z}_{\geq 0}$ be given by $\sigma(z)=|z|^2$, which is nonnegative. Then for any nonzero $z=a+b\omega=\left(a-\frac{b}{2}\right)+\frac{\sqrt{3}}{2}bi$, we have

$$\sigma(z)=a^2-ab+\frac{b^2}{4}+\frac{3b^2}{4}=a^2-ab+b^2.$$

Now let $\alpha,\beta\in\mathbb{Z}[\omega]$ with $\beta\neq 0$, so $\alpha=\alpha_1+\alpha_2\omega$ and $\beta=\beta_1+\beta_2\omega$ for integers α_i,β_i. Working in $\mathbb{Q}[\omega]$, we have

$$\begin{aligned}\frac{\alpha}{\beta}&=\frac{\alpha_1+\alpha_2\omega}{\beta_1+\beta_2\omega}\\&=\frac{\alpha_1+\alpha_2\omega}{\beta_1+\beta_2\omega}\cdot\frac{\beta_1+\beta_2\omega^2}{\beta_1+\beta_2\omega^2}\\&=\frac{\alpha_1\beta_1+\alpha_2\beta_1\omega+\alpha_1\beta_2\omega^2+\alpha_2\beta_2\omega^3}{\beta_1^2+\beta_1\beta_2\omega+\beta_1\beta_2\omega^2+\beta_2^2\omega^3}\\&=\frac{(\alpha_1\beta_1-\alpha_1\beta_2+\alpha_2\beta_2)+(\alpha_2\beta_1-\alpha_1\beta_2)\omega}{\beta_1^2-\beta_1\beta_2+\beta_2^2}\\&=s_1+s_2\omega\end{aligned}$$

for rational numbers s_1,s_2. Pick integers x,y closest to s_1,s_2 respectively so $|x-s_1|\leq\frac{1}{2}$ and $|y-s_2|\leq\frac{1}{2}$. Let $q=x+y\omega$. Let $r=\alpha-\beta q$, showing that there $q,r\in\mathbb{Z}[\omega]$ with $\alpha=\beta q+r$. For $r\neq 0$, we have

$$\begin{aligned}\sigma(r)&=|r|^2\\&=|\beta|^2\cdot\left|\frac{\alpha}{\beta}-q\right|^2\\&=|(s_1+s_2\omega-(x+y\omega)|^2\cdot\sigma(\beta)\\&=|(s_1-x)+(s_2-y)\omega|^2\cdot\sigma(\beta)\\&=\left((s_1-x)^2-(s_1-x)(s_2-y)+(s_2-y)^2\right)\cdot\sigma(\beta)\\&\leq\left((s_1-x)^2+|(s_1-x)|\cdot|(s_2-y)|+(s_2-y)^2\right)\cdot\sigma(\beta)\\&\leq\frac{3}{4}\sigma(\beta)\\&<\sigma(\beta).\end{aligned}$$

We conclude that $\mathbb{Z}[\omega]$ is a Euclidean domain.

(b) Every element in $\mathbb{Z}[\sqrt{-2}]$ is of the form $a+b\sqrt{-2}$ for integers a,b. Let $\sigma:\mathbb{Z}[\sqrt{-2}]\setminus\{0\}\to\mathbb{Z}_{\geq 0}$ be given by $\sigma(z)=|z|^2$, which is nonnegative. Then for any nonzero $z=a+b\sqrt{-2}$ we have

$$\sigma(z)=a^2+2b^2.$$

Now let $\alpha, \beta \in \mathbb{Z}[\sqrt{-2}]$ with $\beta \neq 0$, so $\alpha = \alpha_1 + \alpha_2\omega$ and $\beta = \beta_1 + \beta_2\omega$ for integers α_i, β_i. Working in $\mathbb{Q}[\sqrt{-2}]$, just as above we can write

$$\frac{\alpha}{\beta} = s_1 + s_2\sqrt{-2}$$

for rational numbers s_1, s_2. Pick integers x, y closest to s_1, s_2 respectively so $|x - s_1| \leq \frac{1}{2}$ and $|y - s_2| \leq \frac{1}{2}$. Let $q = x + y\sqrt{-2}$. Let $r = \alpha - \beta q$, showing that there $q, r \in \mathbb{Z}[\sqrt{-2}]$ with $\alpha = \beta q + r$. For $r \neq 0$, we have

$$\begin{aligned}
\sigma(r) &= |r|^2 \\
&= |\beta|^2 \cdot \left|\frac{\alpha}{\beta} - q\right|^2 \\
&= \left|(s_1 + s_2\sqrt{-2} - \left(x + y\sqrt{-2}\right)\right|^2 \cdot \sigma(\beta) \\
&= \left|(s_1 - x) + (s_2 - y)\sqrt{-2}\right|^2 \cdot \sigma(\beta) \\
&= \left((s_1 - x)^2 + 2(s_2 - y)^2\right) \cdot \sigma(\beta) \\
&\leq \frac{3}{4}\sigma(\beta) \\
&< \sigma(\beta).
\end{aligned}$$

We conclude that $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain.

12.2.9) Let J be an ideal of $F[x, x^{-1}]$. Then $J \cap F[x]$ is an ideal in $F[x]$. Since $F[x]$ is a PID, there is some $p \in F[x]$ such that $(p) = J \cap F[x]$ in $F[x]$. I claim that $(p) = J$ in $F[x, x^{-1}]$:

- Since $p \in J$, we have $(p) \subseteq J$.
- We now show that $J \subseteq (p)$: Let $f \in J$, and choose $n \in \mathbb{N}$ large enough so that $x^n f \in F[x]$. Since J is an ideal, $x^n f \in J \cap F[x] = (p)$ as an ideal in $F[x]$. Thus there is some $g \in F[x]$ such that $x^n f = gp$, so $f = (x^{-n}g)p$, implying that $f \in (p)$ as an ideal in $F[x, x^{-1}]$. Thus $J \subseteq (p)$.

We conclude that $J = (p)$, so $F[x, x^{-1}]$ is a PID.

12.2.10) It suffices to show that $\mathbb{R}[[t]]$ is a PID. Let J be an ideal of $\mathbb{R}[[t]]$. If $J = 0$, then clearly J is principal, so assume $J \neq 0$. Let $p \in J$ be a formal power series with smallest degree n as low as possible, meaning that $p = \sum_{i=n}^{\infty} p_i t^i$, with $p_n \neq 0$, and if $q = \sum_{i=n'}^{\infty} q_i t^i$ with $q_{n'} \neq 0$, then $n' \geq n$. We have

$$p = t^n(a_n + a_{n+1}t + \cdots)$$

so $\frac{p}{t^n}$ is a unit since $\mathbb{R}$ is a field and the units in $\mathbb{R}[[t]]$ are precisely the power series with nonzero constant terms. I claim that $(p) = J$:

- Clearly $(p) \subseteq J$ since $p \in J$.
- Let $f \in J$. Then $f = t^n g$ for some $g \in \mathbb{R}[[t]]$ by the minimality of n, so

  $$f = t^n g = t^n \left(\frac{p}{t^n}\right)\left(\frac{p}{t^n}\right)^{-1} g = p \cdot \left(\left(\frac{p}{t^n}\right)^{-1} g\right),$$

  which is well-defined since $\frac{p}{t^n}$ is a unit. Thus $f \in (p)$, so $J \subseteq (p)$.

We conclude that $J = (p)$, so $\mathbb{R}[[t]]$ is a PID, and thus is a UFD.