Also, $1 \in U(R)$ is the identity w.r.t. $\cdot$.

Finally, for $x \in U(R), \exists\ y \in U(R)$ s.t. $xy = 1$, i.e., $y = x^{-1}$, so that $x^{-1} \in U(R)$.

Hence $(U(R), \cdot)$ is a group.

Let $\phi : R \to R'$ be a ring homomorphism.

Consider $\psi : U(R) \to U(R') : \psi(x) = \phi(x)$.

Then ψ is well-defined since ϕ is well-defined.

Also $\psi(x_1x_2) = \phi(x_1x_2) = \phi(x_1)\phi(x_2) = \psi(x_1)\psi(x_2)$.

Hence ψ is a group homomorphism.

E11) i) $\overline{2}$ in $\mathbb{Z}_8$, and $\overline{1}$ in $\mathbb{Z}_7$ (both $\overline{2}$ and $\overline{6}$ are units in $\mathbb{Z}_7$).

ii) $x^2 + 8x + 15 = (x+3)(x+5)$, $x^2 + 12x + 35 = (x+5)(x+7)$.
Thus, their g.c.d is $x + 5$.

iii) $x^3 - 2x^2 + 6x - 5 = (x-1)(x^2 - x + 5)$,

$$5x^3 + x^2 - 3x - \frac{3}{5} = (5x+1)\left(x^2 - \frac{3}{5}\right),$$

$x^2 - 2x + 1 = (x-1)^2$.

Thus, their g.c.d is 1.

E12) Firstly, I is an ideal of $C[0, 1]$ (because $f, g \in I \Rightarrow f - g \in I$, and for $h \in C[0, 1], f \in I, hf \in I$.)

Secondly, since any non-zero constant function over $[0, 1]$ is in $C[0, 1] \setminus I$, I is a proper ideal.

Finally, let $fg \in I$. Then $f(0)g(0) = 0$ in $\mathbb{R}$. Since $\mathbb{R}$ is a domain, we must have $f(0) = 0$ or $g(0) = 0$, i.e., $f \in I$ or $g \in I$.

Thus, I is a prime ideal of $C[0, 1]$.

E13) Let us first assume that P is a prime ideal of R. Since R has identity, so has R/P. Now, let $a + P$ and $b + P$ be in R/P such that $(a + P)(b + P) = P$, the zero element of R/P.

Then $ab + P = P$, i.e., $ab \in P$.

As P is a prime ideal of R, either $a \in P$ or $b \in P$, i.e., either $a + P = P$ or $b + P = P$.

Thus, R/P has no zero divisors. Hence, R/P is an integral domain.

Conversely, assume that R/P is an integral domain. Let $a, b \in R$ such that $ab \in P$. Then $ab + P = P$ in R/P, i.e., $(a + P)(b + P) = P$ in R/P.

As R/P is an integral domain, either $a + P = P$ or $b + P = P$, i.e., either $a \in P$ or $b \in P$.

This shows that P is a prime ideal of R.

E14) i) From E35 of Unit 8, you know that $f^{-1}(J)$ is an ideal of R. Since f is surjective and $J \neq S$, $f^{-1}(J) \neq R$.

Now, let $a, b \in R$ such that $ab \in f^{-1}(J)$.

$\Rightarrow f(ab) \in J$
$\Rightarrow f(a)f(b) \in J$
$\Rightarrow f(a) \in J$ or $f(b) \in J$, since J is a prime ideal.
$\Rightarrow a \in f^{-1}(J)$ or $b \in f^{-1}(J)$.
Thus, $f^{-1}(J)$ is a prime ideal in R.

ii) Since f is onto, you know that $f(I)$ is an ideal of S. Since $I \neq R, 1 \notin I$. Also $f^{-1}f(I) = I$, since $N \subseteq I$. So $f(1) \notin f(I)$. Thus, $f(I) \neq S$.
Next, let $x, y \in S$ such that $xy \in f(I)$.
Since $S = \text{Im } f$, $\exists\ a, b \in R$ such that $x = f(a)$ and $y = f(b)$.
Then $f(ab) = xy \in f(I)$, i.e., $ab \in f^{-1}(f(I)) = I$.
$\therefore a \in I$ or $b \in I$, i.e., $x \in f(I)$ or $y \in f(I)$.
Thus, $f(I)$ is a prime ideal of S.

iii) **ϕ is $1-1$:** $\phi(I) = \phi(J) \Rightarrow f(I) = f(J)$
$\Rightarrow f^{-1}(f(I)) = f^{-1}(f(J))$, since $N \subseteq I$, $N \subseteq J$.
$\Rightarrow I = J$.
ϕ is onto: Let J be a prime ideal of S. Then $f^{-1}(J)$ is a prime ideal of R and $\phi(f^{-1}(J)) = f(f^{-1}(J)) = J$. Thus, $J \in \text{Im } \phi$.

E15) i) Firstly, $< p_1p_2 > \subseteq < p_1 > \cap < p_2 >$, clearly.
Next, if $\alpha \in < p_1 > \cap < p_2 >$, then $\alpha = p_1x = p_2y$ for some $x, y \in \mathbb{Z}$. So $p_1 | p_2y$. Therefore, $p_1 | y$. Let $y = p_1z$. Then $\alpha = p_1p_2z \in < p_1p_2 >$. So $< p_1 > \cap < p_2 > \subseteq < p_1p_2 >$.
$\therefore < p_1 > \cap < p_2 > = < p_1p_2 >$.
Since p_1p_2 is not a prime, $< p_1 > \cap < p_2 >$ is not a prime ideal.

ii) Let $x \in I_1 \setminus I_2$ and $y \in I_2 \setminus I_1$. Then $xy \in I_1$ and $xy \in I_2$, since I_1 and I_2 are ideals. $\therefore xy \in I_1 \cap I_2$.
But $x \notin I_1 \cap I_2$ and $y \notin I_1 \cap I_2$.
Thus, $I_1 \cap I_2$ is not prime.

E16) Suppose $p\mathbb{Z} \subseteq m\mathbb{Z}$, $m \in \mathbb{Z}$. Then $p = mn$ for some $n \in \mathbb{Z}$.
So $m = \pm 1$ or $m = \pm p$, since p is a prime number.
Thus, $m\mathbb{Z} = \mathbb{Z}$ or $m\mathbb{Z} = p\mathbb{Z}$.
Thus, $p\mathbb{Z}$ is a maximal ideal of $\mathbb{Z}$.

Now, you know that $\{0\} \subsetneq 2\mathbb{Z} \subsetneq \mathbb{Z}$. Thus, $\{0\}$ is not a maximal ideal of $\mathbb{Z}$.

E17) Consider $< 4 >$ in $\mathbb{Z}$.
Since 4 is not a prime, $< 4 >$ is not a prime ideal. Hence it cannot be a maximal ideal either.

E18) $d : \mathbb{C} \setminus \{0\} \to \mathbb{N} \cup \{0\} : d(x) = 1$.

For any $a, b \in \mathbb{C} \setminus \{0\}$,
$d(ab) = 1 = d(a)$.
$\therefore d(a) = d(ab)\ \forall\ a, b \in \mathbb{C} \setminus \{0\}$.
Also, for any $a, b \in \mathbb{C}, b \neq 0$,
$a = (ab^{-1})b + 0$.
So, d trivially satisfies the second condition for a function to be a Euclidean valuation.
Thus, $\mathbb{C}$ is a Euclidean domain.

E19) You know that
$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)\ \forall\ f(x), g(x) \in \mathbb{R}[x] \setminus \{0\}$.
You also know that given $f(x), g(x) \in \mathbb{R}[x], g(x) \neq 0, \exists!\ q(x)$ and $r(x)$ s.t. $f(x) = q(x)g(x) + r(x)$, with $\deg r(x) < \deg g(x)$.
Hence d is a Euclidean valuation on $\mathbb{R}[x]$, and $\mathbb{R}[x]$ is a Euclidean domain.

$d : \mathbb{Z}[x] \setminus \{0\} \to \mathbb{N} \cup \{0\} : d(f(x)) = \deg f(x)$ is not a Euclidean valuation, since the division algorithm is not true within $\mathbb{Z}[x]$. For example, given $3x$ and $2x$ in $\mathbb{Z}[x]$, there are no $q(x)$ and $r(x)$ such that $3x = 2xq(x) + r(x)$. (Why?)

E20) Apply Theorem 2 to the Euclidean domain $\mathbb{R}[x]$.

E21) Let $R = \mathbb{Z}$. Then $S = \{n \in \mathbb{Z}^* \mid |n| > 1\} \cup \{0\}$.
Now, $2 \in S, 3 \in S$ but $2 - 3 \notin S$ since $|2 - 3| = 1$.
Thus, S is not even a subring of R, and hence S is not an ideal.

E22) For example, $\mathbb{Z}[x]$ is a subring of $\mathbb{Q}[x]$, which is a PID. But $\mathbb{Z}[x]$ is not a PID.

E23) $\mathbb{Z}$ is a PID. $\mathbb{Z}/6\mathbb{Z}$ is not even a domain. Thus, it is not a PID.
However, every ideal in the quotient ring will be a principal ideal.

E24) $\exists\ x, y \in R$ such that $ax + by = 1$.
Then $c = 1.\ c = (ax + by)c = acx + bcy$.
Since $a \mid ac$ and $a \mid bc$, $a \mid (acx + bcy) = c$.

E25) (i) is not, since it is $(x-1)^2$.
(ii) is not, because of Theorem 4′.
(iii) is, because of Theorem 4′.
(iv) is not, because of Theorem 5.

E26) Let $p = ab$. Then $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.
Suppose $p \mid a$. Let $a = pc$. Then
$p = ab = pcb \Rightarrow p(1 - cb) = 0 \Rightarrow 1 - cb = 0$, since R is a domain and $p \neq 0$. Thus, $bc = 1$, i.e., b is a unit.
Similarly, you can show that if $p \mid b$, then a is a unit.

So, $p = ab \Rightarrow a$ is a unit or b is a unit, i.e., p is irreducible.

E27) (i), (iii) since 5 and $x^2 + x + 1$ are irreducible in $\mathbb{Z}$ and $\mathbb{R}[x]$, respectively.
(ii) is not, since $x^2 - 1 = (x-1)(x+1)$ in $\mathbb{Q}[x]$.
(iv) is not, since $\mathbb{Z}[x]/< x > \simeq \mathbb{Z}$, which is not a field.

E28) i) 1, ii) 7, iii) 5.

E29) Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ and let the content of $f(x)$ be d. Let $a_i = db_i \ \forall\ i = 0, 1, \ldots, n$. Then the g.c.d of $b_0, b_1, \ldots, b_n$ is 1. Thus, $g(x) = b_0 + b_1x + \cdots + b_nx^n$ is primitive. Also,
$f(x) = db_0 + db_1x + \cdots + db_nx^n = d(b_0 + b_1x + \cdots + b_nx^n) = dg(x)$.

E30) Let $f(x) = \alpha f_1(x), g(x) = \beta g_1(x)$, where α and β are the contents of $f(x)$ and $g(x)$, respectively, and $f_1(x), g_1(x)$ are primitive. Then, by Gauss's Lemma, $f_1(x)g_1(x)$ is primitive, and $f(x)g(x) = \alpha\beta f_1(x)g_1(x)$. Therefore, $\alpha\beta$ is the content of $f(g)g(x)$.

E31) $f(x) = x^n - p = a_0 + a_1x + \cdots + a_nx^n$,
where $a_0 = -p, a_1 = 0 = \cdots = a_{n-1}, a_n = 1$.
Thus, $p \mid a_i \ \forall\ i = 0, 1, \ldots, n-1$, $p^2 \nmid a_0$, $p \nmid a_n$.
So, by Eisenstein's criterion, $f(x)$ is irreducible over $\mathbb{Q}$.

E32) All of them are irreducible – (i) and (ii), because of Eisenstein's criterion, taking $p = 3$; and (iii), because any linear polynomial is irreducible.

E33) Since $a \neq 0, \pm 1, \exists$ a prime q such that $q \mid a$. Also $q^2 \nmid a$, since a is square-free. Then, using q as the prime, we can apply Eisenstein's criterion, to conclude that $x^p + a$ is irreducible in $\mathbb{Z}[x]$. Thus, $(x^p + a)$ is a prime element of $\mathbb{Z}[x]$. Hence, $< x^p + a >$ is a prime ideal of $\mathbb{Z}[x]$. Hence the result.

E34) Since $(\mathbb{Z}_p^*, \cdot)$ is a group of order $(p-1)$, $(\bar{a})^{p-1} = \bar{1} \ \forall\ \bar{a} \in \mathbb{Z}_p^*$. Hence $\overline{a^p} = \bar{a} \ \forall\ \bar{a} \in \mathbb{Z}_p$. Now consider $x^p + \bar{a} \in \mathbb{Z}_p[x]$.
$\overline{p-a}$ is a zero of this polynomial, since
$(\overline{p-a})^p + \bar{a} = \overline{p-a} + \bar{a} = \bar{p} = \bar{0}$ in $\mathbb{Z}_p$.
Thus, $x^p + \bar{a}$ is reducible over $\mathbb{Z}_p$.

E35) You can see that the result is true for $n = 1$.
Assume that it holds for some $m \geq 1$, i.e., whenever $p \mid a_1a_2 \ldots a_m$, then $p \mid a_i$ for some $i = 1, 2, \ldots, m$.
Now let $p \mid a_1a_2 \ldots a_{m+1}$. Then $p \mid (a_1a_2 \ldots a_m)a_{m+1}$.

Since p is a prime element, we find that $p \mid a_1 a_2 \ldots a_m$ or $p \mid a_{m+1}$.

If $p \mid a_1 a_2 \ldots a_m$, then $p \mid a_i$ for some $i = 1, \ldots, m$ by our assumption.

If $p \nmid a_1 \ldots a_m$, then $p \mid a_{m+1}$.

Thus, in either case, $p \mid a_i$ for some $i = 1, \ldots, m+1$.

So, our result is true for $n = m+1$.
Hence, it is true $\forall\, n \in \mathbb{N}$.

E36) $3x^5 - 2x^2 + 4x - 6$ is irreducible in $\mathbb{Q}[x]$, using Eisenstein's criterion with $p = 2$. Since $\mathbb{Q}[x]$ is a PID, every irreducible element is prime.
Hence the given polynomial is prime in $\mathbb{Q}[x]$.
In $\mathbb{Z}_2[x]$ the given polynomial is x^5, since $\overline{2} = \overline{0}$ and $\overline{3} = \overline{1}$.
Since x is prime in $\mathbb{Z}_2[x]$, x^5 is its prime factorisation.

E37) Let $f(x)$ be a non-zero non-unit in $F[x]$. We will prove that $f(x)$ can be written as a product of irreducible elements, by induction on $\deg f(x)$.
If $\deg f(x) = 1$, then $f(x)$ is linear, and hence irreducible.
Now suppose that the result is true for polynomials of degree $< n$.
Take $f(x)$ of degree n. If $f(x)$ is irreducible, there is nothing to prove.
Otherwise, there is a prime element $f_1(x)$ such that $f_1(x) \mid f(x)$. Let $f(x) = f_1(x)g_1(x)$. Note that $\deg f_1(x) > 0$.
Hence, $\deg g_1(x) < \deg f(x)$. If $g_1(x)$ is prime, we are through.
Otherwise we can find a prime element $f_2(x)$ such that $g_1(x) = f_2(x)g_2(x)$. Then $\deg g_2(x) < \deg g_1(x)$. This process must stop after a finite number of steps, since each time we get polynomials of lower degree. Thus, we shall finally get
$f(x) = f_1(x)f_2(x)\ldots f_m(x)$, where each $f(x)$ is prime in $F[x]$.
Now, to show that the factorisation is unique, you should follow the lines of the proof of Theorem 14.

E38) $6 = 2.3 = (1+\sqrt{-5})(1-\sqrt{-5})$.
Using the norm function, you should check that each of $2, 3, 1+\sqrt{-5}$ and $1-\sqrt{-5}$ are irreducible in $\mathbb{Z}[\sqrt{-5}]$.

E39) For example, consider
$4 = 2.2 = (1+\sqrt{-3})\,(1-\sqrt{-3})$.
Let us show that each of these factors is irreducible in $\mathbb{Z}[\sqrt{-3}]$, by contradiction.
Suppose $1+\sqrt{-3}$ is reducible.
Then $1+\sqrt{-3} = \alpha\beta$ for some non-units α, β in $\mathbb{Z}[\sqrt{-3}]$.
Taking the norm function, we get
$4 = N(1+\sqrt{-3}) = N(\alpha)N(\beta)$.
So the only possibility is $N(\alpha) = 2,\ N(\beta) = 2$.
Let $\alpha = a + b\sqrt{-3}$, $a, b \in \mathbb{Z}$.
Then $a^2 + 3b^2 = 2$.

If $b \neq 0$, then $a^2 + 3b^2 \geq 2$, and if $b = 0$, then $a^2 = 2$.
Neither case is possible, and we reach a contradiction.
$\therefore 1+\sqrt{-3}$ is irreducible in $\mathbb{Z}[\sqrt{-3}]$.
Similarly, you can check that the other factors of 4 are irreducible in $\mathbb{Z}[\sqrt{-3}]$. Also, none of them are associates of each other, since the only units of $\mathbb{Z}[\sqrt{-3}]$ are 1 and -1.
Hence, $\mathbb{Z}[\sqrt{-3}]$ is not a UFD.

E40) $\mathbb{Z}[x]$, as you have seen in Theorem 17 and Example 8.

E41) i) False. For example, x is irreducible in $\mathbb{Z}[x]$, but $\bar{x}$ is zero in $\mathbb{Z}[x]/< x > \simeq \mathbb{Z}$, and hence not irreducible.

ii) False. For example, $\mathbb{Z}$ is a UFD, but in $\mathbb{Z}/< 6 >$, $\bar{4}$ has two different prime factorisations, viz., $\bar{2}.\bar{2} = \bar{2}.\bar{2}.\bar{2}.\bar{2} = \bar{4}$.
For another example, $\mathbb{Z}[\sqrt{-5}] \simeq \mathbb{Z}[x]/< x^2 + 5 >$ is not a UFD, while $\mathbb{Z}[x]$ is.

iii) False. For example, $\mathbb{Z}[\sqrt{-5}]$ is a subring of $\mathbb{C}$, a UFD. But $\mathbb{Z}[\sqrt{-5}]$ is not a UFD.

iv) True. To see why, let r be a non-zero non-unit in R.
Then r is also a non-unit in $R[x]$.
Hence $r = p_1(x)p_2(x)\ldots p_n(x)$ uniquely, where $p_i(x) \in R[x]$ are irreducibles.
So $0 = \deg r = \sum_{i=1}^{n} \deg p_i(x)$.
Hence, $\deg p_i = 0 \ \forall\ i = 1, \ldots, n$, i.e., $p_i \in R \setminus \{0\} \ \forall\ i = 1, \ldots, n$.
That is, $r = p_1 p_2 \ldots p_n$ uniquely, where $p_i \in R$ are irreducible in R.
Thus, R is a UFD.