Problem 1 (Problem 9.2.3). We know that $F[x]$ is a PID since $F$ is a field (corollary 4 in section 9.2). By proposition 7 in section 8.2, every nonzero prime ideal in $F[x]$ is a maximal ideal; so in our particular case, the ideal $(f(x))$ (when nonzero), is prime if and only if it is maximal, and this latter condition holds if and only if the quotient $F[x]/(f(x))$ is a field.

Notice that the zero polynomial $f(x) = 0$ is not irreducible (since by definition an irreducible element is nonzero), and indeed the quotient $F[x]/0 \simeq F[x]$ is not a field, so we can assume that the ideal $(f(x))$ is nonzero, and it remains to show that $(f(x))$ is a prime ideal if and only if $f(x)$ is irreducible.

On the other hand, by proposition 11 in section 8.3, in a PID $R$ (such as $F[x]$) an element $r \in R$ is irreducible if and only if it is a prime element, which by definition means exactly that the ideal $(r)$ it generates is a prime ideal. This concludes the proof.

Problem 2 (Q1). Consider the $R$-module $K := R \oplus R$. That is, we take two copies of the $R$-module $R$ as in example 1 at page 338, and then we consider the $R$-module given by the direct sum

$$K = R \oplus R = \{(r_1, r_2) | r_1, r_2 \in R\}.$$ 

Addition is component-wise, so that $K$ certainly is an abelian group as $R$ is. The action of $R$ on $K$ is given as follows: for each $r \in R$, $(r_1, r_2) \in K$ we set

$$r.(r_1, r_2) = (r \cdot r_1, r \cdot r_2)$$

where in each coordinate we use the multiplication operation of $R$. The axioms a, b, c, d of part 2 of the definition of $R$-module at page 337 are then easy to check, and follow by the properties of addition and multiplication on the ring $R$ (associativity of multiplication gives axiom 2b, for instance).

Consider now an $R$-module $M$. For every two elements $m_1, m_2 \in M$ we aim to define a homomorphism $f_{m_1, m_2} : K \longrightarrow M$ which sends $(1, 0) \mapsto m_1$ and $(0, 1) \mapsto m_2$. For such an $f_{m_1, m_2}$ to be an $R$-module homomorphism, we need it to be a homomorphism of abelian groups such that moreover

$$r.(f_{m_1, m_2}(s_1, s_2)) = f_{m_1, m_2}(r.(s_1, s_2)) \quad \forall r \in R, (s_1, s_2) \in K.$$ 

Notice that this forces our definition of $f_{m_1, m_2}$ on the entire $K$, as we need to have

$$f_{m_1, m_2}((r_1, r_2)) = f_{m_1, m_2}(r_1 \cdot (1, 0) + r_2 \cdot (0, 1)) = r_1 \cdot m_1 + r_2 \cdot m_2;$$

it remains to check that this a well-defined homomorphism.
Now, the fact that any such $f_{m_1,m_2}$ is a homomorphism of abelian groups is easy to see because addition is componentwise. Explicitly, given $(r_1, r_2), (s_1, s_2) \in K$ we have

$$f_{m_1,m_2}((r_1, r_2) + (s_1, s_2)) = f_{m_1,m_2}((r_1 + s_1, r_2 + s_2)) = (r_1 + s_1) \cdot m_1 + (r_2 + s_2) \cdot m_2 = $$

$$r_1 \cdot m_1 + s_1 \cdot m_1 + r_2 \cdot m_2 + s_2 \cdot m_2 = f_{m_1,m_2}(r_1, r_2) + f_{m_1,m_2}(s_1, s_2).$$

Similarly, we can check that for each $r \in R$ and each $(r_1, r_2) \in K$ we have

$$f_{m_1,m_2}(r \cdot (r_1, r_2)) = f_{m_1,m_2}((r \cdot r_1, r \cdot r_2)) = (r \cdot r_1) \cdot m_1 + (r \cdot r_2) \cdot m_2 =$$

$$= (r \cdot r_1) \cdot m_1 + (r \cdot r_2) \cdot m_2 = r \cdot (r_1 \cdot m_1 + r_2 \cdot m_2) = r \cdot f_{m_1,m_2}((r_1, r_2)),$$

proving that $f_{m_1,m_2}$ is a homomorphism of $R$-modules.

Thus, for each pair of elements $m_1, m_2 \in M$ we defined a homomorphism $f_{m_1,m_2} : K \rightarrow M$ and hence we gave a function

$$M \times M \xrightarrow{f} \text{Hom}_R(K, M)$$

where on the right we denote by $\text{Hom}_R(K, M)$ the set of homomorphism of $R$-modules from $K$ to $M$.

Given now one homomorphism $\phi : K \rightarrow M$ of $R$-modules, we get two elements of $M$ by setting

$$m_1 = \phi((1, 0)) \text{ and } m_2 = \phi((0, 1)),$$

so this gives a map $g$ in the opposite direction:

$$\text{Hom}_R(K, M) \xrightarrow{g} M \times M.$$ 

It is immediate to see by construction that $g$ is the inverse function of $f$, and hence in particular both are bijection of sets, which proves that the two sets have the same cardinality, i.e.

$$|M|^2 = |M \times M| = |\text{Hom}_R(K, M)|.$$

Problem 3 (Q3). For modules $M$ and $N$ we take the following two ideals of $R$:

$$M = (2, 1 + \sqrt{-5}), \quad N = (7)\textsuperscript{1}.$$

By Q2, every ideal $I$ of $R$ is an $R$-submodule of $R$ (and hence an $R$-module) with the action map $R \times I \rightarrow I$ being just multiplication in the ring $R$, so $M$ and $N$ are indeed $R$-modules.

As $N = (7)$ is principal, we have

$$N = (7) = \{7(a + b\sqrt{-5}) | a, b \in \mathbb{Z}\} = \{7a + 7b\sqrt{-5} | a, b \in \mathbb{Z}\}$$

which is isomorphic to $\mathbb{Z}^2$ as an additive group, since addition is ”coefficient-wise”, i.e. $(7a + 7b\sqrt{-5}) + (7a' + 7b'\sqrt{-5}) = 7(a + a') + 7(b + b')\sqrt{-5}$.

Now let’s consider the ideal $M = (2, 1 + \sqrt{-5})$: to show that $M \cong \mathbb{Z}^2$ as an additive group, we claim that

$$M = \{a + b\sqrt{-5} | (a - b) \text{ is even}\}. \quad (1)$$

\textsuperscript{1}It will turn out that taking $N$ to be any principal ideal of $R$ will work, but let’s fix one to make notation easier
Indeed a generic element of $M$ is of the form

$$2 \cdot (a + b\sqrt{-5}) + (1 + \sqrt{-5}) \cdot (c + d\sqrt{-5}) = 2a + 2b\sqrt{-5} + c + d\sqrt{-5} + c\sqrt{-5} - 5d =$$

$$= (2a + c - 5d) + (2b + d + c)\sqrt{-5}$$

and the difference is indeed

$$(2a + c - 5d) - (2b + d + c) = 2a - 2b - 6d$$

which is even.

This proves that $M$ is contained in the set $\{a + b\sqrt{-5} \mid (a - b) \text{ is even}\}$. On the other hand, let $m + n\sqrt{-5} \in \{a + b\sqrt{-5} \mid (a - b) \text{ is even}\}$, so that we have $m - n = 2k$ for some integer $k$; we can write

$$M \ni 2 \cdot k + (1 + \sqrt{-5}) \cdot n = 2k + n + n\sqrt{-5} = m + n\sqrt{-5},$$

which concludes the proof of the claim in formula 1.

It is now immediate to see that $\{a + b\sqrt{-5} \mid (a - b) \text{ is even}\}$ is isomorphic to $\mathbb{Z}^2$ as an additive group, because again addition works "coefficient-wise" as for $N$. More precisely, we can consider the map

$$\phi : M \to \mathbb{Z}^2 \quad a + b\sqrt{-5} \mapsto \left( a, \frac{a - b}{2} \right)$$

and it is easy to see that it is an isomorphism of groups.

It remains to show that $M$ and $N$ are not isomorphic as $R$-modules. Arguing by contradiction, suppose they are so that $\phi : N \to M$ is an isomorphism of $R$-modules.

We have then that $\phi$ is surjective and since $N = (7)$ is principal, every element of $M$ can be written down as

$$m = \phi(n) = \phi(r \cdot 7) = r \cdot \phi(7)$$

for some $r \in R$. This means that $M$ is principal, generated by $\phi(7)$ - but this is a contradiction, since in HW7 Q2c we proved that $M$ (which was denoted $I_2$ there) is not a principal ideal.

**Problem 4** (Q5). a) Since $G$ has finitely many elements, the additive order of 1 must be finite, so call it $m$. Arguing by contradiction, suppose that $m = pq$ is composite (with $1 < p, q < m$), then we have

$$0 = m \cdot 1 = 1 + 1 + \ldots + 1 \quad \text{m times}$$

In any field, distributivity of multiplication with respect to addition holds, which means that since $m = pq$ we can write

$$1 + 1 + \ldots + 1 = \left( \underbrace{1 + 1 + \ldots + 1}_{\text{p times}} \right) \cdot \left( \underbrace{1 + 1 + \ldots + 1}_{\text{q times}} \right)$$

Since a field is an integral domain and the left hand side of the above equation is zero by assumption, either $\underbrace{1 + 1 + \ldots + 1}_{\text{p times}}$ or $\underbrace{1 + 1 + \ldots + 1}_{\text{q times}}$ is zero, and this yields a contradiction since $p, q < m$, which is the order of 1 in $(F, +)$. 

---

---
b) Let $x \neq 0$ be a nonzero element of $F$, so that its additive order $m$ is strictly greater than 1. It suffices to prove that $x + x + \ldots + x = 0$, since then we will have $m|p$ and as $m \neq 1$, this will imply that $m = p$ as needed.

Notice that the distributivity of multiplication with respect to addition implies that

$$x + x + \ldots + x = x \cdot \left(1 + 1 + \ldots + 1\right) = x \cdot 0 = 0,$$

since we proved in part a) that the element 1 has additive order $p$. This shows that any $x \in G$ has order $p$.

In particular, $G$ is a finite group where every element has order $p$. Arguing by contradiction, if there was a prime number $q \neq p$ dividing $|G|$, then Cauchy’s theorem (theorem 11 in section 3.2 of the textbook) implies that $G$ contains an element of order $q$, which is a contradiction.

Therefore, the only prime number dividing the order of $G$ is $p$, and hence $|G| = p^n$ for some $n \in \mathbb{N}$.

c) Consider the ring $\mathbb{Z}/3\mathbb{Z}$ of residue classes modulo 3, where both addition and multiplication is mod 3. Since $1 \cdot 1 = 1$ and $-1 \cdot -1 = 1$, every nonzero element is invertible, and hence this ring is a field. It has 3 elements and it is easy to see that it is the only field with 3 elements (for instance because there is only one group with 3 elements up to isomorphism, and then the axioms of a ring forces multiplication to be exactly the one in $\mathbb{Z}/3\mathbb{Z}$).

We denote this field with 3 elements by $\mathbb{F}_3$. By problem 9.2.3, the quotient $\mathbb{F}_3[x]/(f(x))$ is a field if and only if the polynomial $f(x) \in \mathbb{F}_3[x]$ is irreducible.

Consider then the polynomial

$$f(x) = x^2 + 1 \in \mathbb{F}_3[x];$$

it is a quadratic polynomial, hence if it was reducible in $\mathbb{F}_3[x]$ it would decompose into linear factors - that is to say, its roots would be in the field $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$. On the other hand, it is immediate to see that none of $\{0, 1, -1\} = \mathbb{Z}/3\mathbb{Z}$ is a root of $f$, which proves that $f(x)$ is irreducible.

Therefore, $\mathbb{F}_3[x]/(f(x))$ is a field, so it remains to check that it has exactly 9 elements. By polynomial division, it is clear that every $g(x) \in \mathbb{F}_3[x]$ can be written down as

$$g(x) = q(x) \cdot f(x) + r(x) \quad \text{with} \quad \deg r(x) < \deg f(x) = 2$$

which proves that every coset in $\mathbb{F}_3[x]/(f(x))$ has a representative of degree at most 1. On the other hand, two different polynomials $r_1$ and $r_2$ of degrees at most 1 cannot be in the same coset, as their nonzero difference $r_1 - r_2$ also has degree at most 1, but it would have to be divisible by $f(x)$ which has degree 2.

Therefore, a complete set of representatives for $\mathbb{F}_3[x]/(f(x))$ is given by polynomials in $\mathbb{F}_3[x]$ of degrees at most 1. We have exactly 9 of those (since we have 3 possibilities for the linear term and 3 possibilities for the constant term), and hence here’s our field with 9 elements.

d) We know that the group of units in a field $F$ is the set $F^\times = F - \{0\}$ under multiplication.

From part c, we have then that $F^\times$ is an abelian group on $9 - 1 = 8$ elements, and to distinguish
between the three possibilities mentioned we will show that \( \mathbb{F}_3[x]/(f(x)) \) contains an element whose multiplicative order is not 1, 2 or 4: this rules out (A) and (B) and thus show that \( F^\times \cong \mathbb{Z}/8\mathbb{Z} \) as in possibility C.

Consider then \( a = x+1 \), which is obviously not the identity \( 1 \). We have

\[
a^2 = (x+1)^2 = x^2 + 2x + 1 = -1 + 2x + 1 = -x
\]

because in the quotient \( \mathbb{F}_3[x]/(x^2+1) \) the class of \( x^2 \) is \( -1 \); therefore \( a^2 \neq 1 \). We square again to get

\[
a^4 = (-x)^2 = x^2 = -1 \neq 1
\]

which shows that \( a \) does not have order 1, 2 or 4 and thus finishes the proof.

[Alternate proof: the equation \( z^4 = 1 \) can have at most 4 solutions in a domain, because the degree-4 polynomial \( z^4 - 1 \) can have at most 4 roots. But in the groups in (A) and (B), all eight elements satisfy \( g^4 = 1 \). Therefore it must be (C).]

e) We want to repeat the steps used in part c to produce a field with 9 elements. If we run through our argument, we see that it consisted of the following steps:

1) Start with a finite field \( F \) of size 3 - we produce this by hand since this is just \( \mathbb{Z}/3\mathbb{Z} \).
2) Find an irreducible polynomial \( f(x) \in F[x] \) of degree \( n = 2 \), and using problem 9.2.3 conclude that the quotient \( F[x]/(f(x)) \) is a field.
3) Using explicit representatives given by remainders of polynomial division in \( F[x] \), count the elements of \( F[x]/(f(x)) \) to find out that it has exactly \( 3^n \) elements.

We can see that step 1 did not depend on the final size of the field we want to produce, and neither does step 3. Indeed, the possible remainders of polynomial division by a polynomial of degree \( n \) in a field \( F \) are exactly all the polynomials of degree at most \( n-1 \), and in case \( F \) is a finite of size \( p \) we have exactly \( p \) possibilities for each coefficient (from the coefficient of \( x^0 \) to the coefficient of \( x^{n-1} \)), for a total of \( p^n \) elements.

Therefore, we only need to adapt step 2 in our quest for a field with \( 27 = 3^3 = p^n \) elements, i.e. we need to find an irreducible polynomial \( g(x) \in \mathbb{F}_3[x] \) of degree \( n = 3 \).

Notice now that over any field \( F \), a cubic polynomial \( g(x) \) is irreducible if and only if it has no roots over \( F \). Indeed reducibility means that \( g(x) = m(x)n(x) \) so that \( 3 = \deg g = \deg m + \deg n \) with \( \deg m, \deg n < \deg g = 3 \) and thus either \( \deg m \) or \( \deg n \) is 1, which means that \( g(x) \) has a root over \( F \).

It remains to write down a polynomial of degree 3 over \( \mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z} \) with no roots over \( \mathbb{F}_3 \). We take \( g(x) = x^3 - x + 1 \). It is easy to check that any \( n \in \mathbb{Z}/3\mathbb{Z} \) has \( n^3 = n \) and hence the polynomial \( g(x) \) evaluates to \( 1 \) on any \( n \in \mathbb{F}_3 \), in particular, it has no root over \( \mathbb{F}_3 \) and hence is irreducible.

To conclude, the field \( \mathbb{F}_3[x]/(g(x)) \) has order 27.