• Exercises 4.1 4(f), 10, 12, 13(a), 15(a)(e).

4(f) Find all ring homomorphisms in \( \mathbb{Q} \).

We always have the zero ideal \((0)\). Suppose \( I \) is a non-zero ideal.

Then it contains a non-zero element, i.e. a unit since \( \mathbb{Q} \) is a
field. But once an ideal contains a unit it contains everything. 
So the only ideals are \((0)\) and \( \mathbb{Q} \).

10 Prove that if \( f(x) \in F[x] \) is not irreducible, then \( F[x]/(f(x)) \)
contains zero-divisors.

Proof. If \( f(x) \) is reducible, then \( f(x) = g(x)h(x) \) with
\( \deg g(x), h(x) < \deg f(x) \). But that means that \( g(x) + (f(x)) \) and
\( h(x) + (f(x)) \) are non-zero elements of \( F[x]/(f(x)) \). Their product is
\( g(x)h(x) + (f(x)) = f(x) + (f(x)) = 0 + (f(x)) = 0 \). Hence we've found
two non-zero elements whose product is zero.

12 Show that the equation \( y^2 = 4 \) has at least four solutions in the
ring \( \mathbb{Z}_5[x]/(x^2 + 1) \).

Solution. Suppose \( y = ax + b + (x^2 + 1) \) is a solution of the
equation. Then, \( y^2 = a^2x^2 + 2abx + b^2 + (x^2 + 1) = 4 + (x^2 + 1) \).
Rewriting \( x^2 = -1 \) to get back to our standard names of the
elements, we get that \( 2abx + b^2 - a^2 + (x^2 + 1) = 4 + (x^2 + 1) \).
Hence \( ab \equiv 0 \) (mod 5) and \( b^2 - a^2 \equiv 4 \) (mod 5). So either
\( a = 0 \) and \( b = \pm 2 \) or \( b = 0 \) and \( a = \pm 1 \). We've found four
solutions: \( \pm 2x + (x^2 + 1) \) and \( \pm 1 + (x^2 + 1) \).
This means that \( \mathbb{Z}_5[x]/(x^2 + 1) \) cannot possibly be a field, since
over a field a quadratic like \( y^2 - 4 \) has at most two solutions.
In other words, \( x^2 + 1 \) is not irreducible in \( \mathbb{Z}_5[x] \): it factors as
\( (x + 2)(x - 2) \).

13(a) Prove the equation \( x^2 - 5y^2 = 2 \) has no solution for \( x, y \in \mathbb{Z} \).

Proof. Suppose \( x^2 - 5y^2 = 2 \) is a solution. Apply the homomor-
phism \( \phi : \mathbb{Z} \rightarrow \mathbb{Z}_5 \). We get that \( \phi(x)^2 = 2 \) in \( \mathbb{Z}_5 \). But \( 2 \) is not
a square in \( \mathbb{Z}_5 \) (\( 0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 4, 4^2 = 1 \) so nothing
squares to \( 2 \)). So this is a contradiction.

15(a) Find all ring homomorphisms \( \phi : \mathbb{Z}_2 \rightarrow \mathbb{Z} \).

Solution. A ring homomorphism has to send \( 0 \) to 0 and \( 1 \) to 1.
So there is at most one possibility. But this is NOT a homo-

morphism since \( \phi(1 + 1) \neq \phi(1) + \phi(1) \).

15(e) Find all ring homomorphisms \( \phi : \mathbb{Q} \rightarrow \mathbb{Q} \).

Solution. Suppose \( \phi \) is a ring homomorphism from \( \mathbb{Q} \) to \( \mathbb{Q} \).
Then, \( \phi(0) = 0, \phi(1) = 1 \). But then \( \phi(2) = \phi(1 + 1) = \phi(1) + \phi(1) = 1 + 1 = 2 \). Continuing in this way you get that \( \phi(n) = n \)
for all \( n \in \mathbb{N} \). Then \( \phi(-n) = -\phi(n) \) so you get that \( \phi(n) = n \)
for all \( n \in \mathbb{Z} \). Finally if \( u \) is a unit, \( \phi(u^{-1}) = \phi(u)^{-1} \). So for
\( m \in \mathbb{Z} \text{ and } n \in \mathbb{N}, \text{ we get that} \)
\[
\phi\left(\frac{m}{n}\right) = \phi(mn^{-1}) = \phi(m)\phi(n^{-1}) = \phi(m)\phi(n)^{-1} = mn^{-1} = \frac{m}{n}.
\]

Hence the only such homomorphism is the identity map.

- Exercises 4.2 3(a)(b)(c), 6(a)

3(a) \( \mathbb{R}[x]/(x^2 + 6) \cong \mathbb{C} \).

Proof. Let \( \phi: \mathbb{R}[x] \to \mathbb{C} \) be the homomorphism \( f(x) \mapsto f(\sqrt{6}i) \).
This is onto: to see that \( a + ib \) is in the image, apply \( \phi \) to the polynomial \( a + xb/\sqrt{6} \). Its kernel is the ideal \( (m(x)) \) where \( m(x) \) is the minimal polynomial of \( \sqrt{6}i \) over \( \mathbb{R} \), that is, \( m(x) = x^2 + 6 \).
Now we get by the isomorphism theorem that \( \mathbb{R}[x]/(x^2 + 6) \cong \mathbb{C} \).

Done.

3(b) \( \mathbb{Z}_{18}/(6) \cong \mathbb{Z}_6 \).

Proof. Define a map \( \mathbb{Z}_{18} \) to \( \mathbb{Z}_6 \) by sending \( n \mod 18 \) to \( n \mod 6 \).
This is WELL-DEFINED (it is important to note this) because if \( n \mod 18 = n' \mod 18 \) then \( 18|(n - n') \) so \( 6|(n - n') \) too so \( n \mod 6 = n' \mod 6 \). Given that, it is easy to see that it really is a ring homomorphism.

It is onto. Its kernel is \( \{0, 6, 12\} = (6) \). Hence the isomorphism theorem gives us that \( \mathbb{Z}_{18}/(6) \cong \mathbb{Z}_6 \).

3(c) \( \mathbb{Q}[x]/(x^2 + 1) \cong \mathbb{Q}[\sqrt{3}i] \).

Proof. The roots of \( x^2 + x + 1 \) are \(-1/2 \pm \sqrt{3}/2 \). Obviously, \( \mathbb{Q}[\sqrt{3}i] = \mathbb{Q}[\sqrt{3}/2 + i] \). Now consider the homomorphism \( \mathbb{Q}[x] \to \mathbb{C}, f(x) \mapsto f(-1/2 + i\sqrt{3}/2) \). The minimal polynomial of \(-1/2 + \sqrt{3}/2 \) over \( \mathbb{Q} \) is \( x^2 + x + 1 \). So the kernel is \( \{x^2 + x + 1\} \). The image is \( \mathbb{Q}[\sqrt{3}i] \). So we’re done by the isomorphism theorem.

6(a) Let \( f(x) = x^2 + x - 1 \). Find the multiplicative inverse of the element \( x^3 + x + 2 \) in \( \mathbb{Q}[x]/(f(x)) \).

Solution. Let me first simplify \( x^3 + x + 2 \) using that \( x^2 = 1 - x \).
It equals \( x - x^2 + 2 = 3x + 1 \). Now, \( x^3 + x + 1) = (3x + 1)(x + 2/3) - 11/9 \). Hence, \( 11/9 = (3x + 1)(x/3 + 2/9) - (x^2 + x - 1) \). Reduce everything modulo \( f(x) \) to get that \( 11/9 = (3x + 1)(x/3 + 2/9) \). Multiply through by 9/11 to get finally that \( 1 = (3x + 1)(3x/11 + 2/11) \). Hence the inverse of \( x^3 + x + 2 \) is \( 3x/11 + 2/11 \).

- Finally one true or false question: IS \( \mathbb{Z}_2[x]/(x^2) \cong \mathbb{Z}_4 \)? NO! In \( \mathbb{Z}_4 \), \( 1 + 1 = 2 \) is non-zero. In \( \mathbb{Z}_2[x]/(x^2) \), \( 1 + 1 = 0 \). So there is no way they could be isomorphic: an isomorphism sends \( 1 \) to \( 1 \) and so sends \( 1 + 1 \) to \( 1 + 1 \).