Exercise 15.23. *Show that the homomorphism preserve idempotent.*

Proof. $\phi(a) = \phi(a^2) = \phi(a)^2$. □

Exercise 15.36. *The sum of the squares of three consecutive integers can not be a square.*

Proof. This proof comes from math stackexchange.

For any integer x, we found $(x-1)^2 + x^2 + (x+1)^2 = 3x^2 + 2$, if such square exists, then it must not a multiple of 3, and the remainder should be 2, therefore, the number we want has form $3n + r$ where n is integer and $0 < r < 3$ (Note that $0 \neq r$ since the number we want is not a multiple of 3). Then $(3n+r)^2 = 9n^2 + 6nr + r^2$, and $1^2 = 1$, $2^2 = 1$. Therefore no r such that $r^2 = 2$, so $3x^2 + 2$ can not be a square. □

Exercise 15.46. *Prove that any automorphism of a field F is the identity from the prime subfield to itself.*

Proof. We know prime subfield is a subfield that does not contain any proper non-trivial subfield, therefore it is the minimal subfield that contains 1. It is finite if $\operatorname{char} R \neq 0$ and it is Q if $\operatorname{char} R = 0$.

Let ϕ a automorphism of F, then $\phi(1) = 1$, any element in such prime subfield has form $n \cdot (b \cdot 1)^{-1}$ where n and b are integers. Note that $\phi(n \cdot (b \cdot 1)^{-1})$ is determined by $\phi(1)$, and $\phi(1) = 1$, so ϕ is the identity. □

Exercise 15.49. *Let R and S be commutative rings with unity, ϕ a homomorphism from R onto S and* $\operatorname{char} R \neq 0$. *Prove that* $\operatorname{char} S$ *divides* $\operatorname{char} R$.

Proof. Since ϕ is onto and R has unity, we know $\phi(1) = 1$. Let $\operatorname{char} R = n$, then $\phi(n \cdot 1) = n \cdot \phi(1) = 0$, therefore the order of unity of S under additive divides n. □

Exercise 15.52. *Show that a homomorphism from a field onto a non-zero ring must be an isomorphism.*

Proof. We need to show that such homomorphism ϕ is one-to-one. Since F a field, we know $\operatorname{Ker} \phi$ is either a zero ideal or F itself. We may suppose $\operatorname{Ker} \phi = F$, since another case is trivial. Then $\phi(F) = \{0\}$, however, ϕ is onto and the codomain is not a zero-ring, so $\phi(F)$ cannot be $\{0\}$. □

Exercise 15.53. *Suppose that R and S are commutative ring with unities. Let ϕ a homomorphism from R to S and let A be an ideal of S:*

- *If A is prime, show that $\phi^{-1}(A)$ is also prime.*
- *If A is maximal, show that $\phi^{-1}(A)$ is also maximal.*

Proof. If A is prime, for any element $ab \in \phi^{-1}(A)$, we have $\phi(ab) \in A$, therefore $\phi(a)$ or $\phi(b)$ in A, which implies a or $b \in \phi^{-1}(A)$.

If A is maximal, for any ideal I that properly contains $\phi(A)^{-1}$ in R, then $\phi(I)$ properly contains A and $\phi(I) = S$, therefore $I = \phi(S)^{-1} = R$. □

Exercise 15.54. *Show that the homomorphic image of a principal ideal ring is also a principal ideal ring.*

Proof. Let ϕ a homomorphism from a principal ideal ring R onto some ring S, then S is commutative and has a unity. For any ideal I of S, $\phi^{-1}(I)$ is a principal ideal, say, $\langle r \rangle = rR$, then $I = \phi(rR) = \phi(r)\phi(R) = \phi(r)S$, therefore I is a principal ideal ring which generated by $\phi(r)$. □

Exercise 15.57. *Show that Z_{mn} is ring-isomorphic to $Z_m \oplus Z_n$ when m is coprime to n.*

Proof. By Group Theory, we know Z_{mn} is group-isomoprhic to $Z_m \oplus Z_n$, then there is an isomorphism ϕ that maps $\phi(1)$ to any generator of $Z_m \oplus Z_n$, we choose $\phi(1) = (1, 1)$. Then, for any $a\ b \in Z_{mn}$

$$
\begin{aligned}
&\phi(a\ b) \\
=&\phi((a \cdot 1)b) \\
=&\phi(a \cdot (1b)) \\
=&a \cdot \phi(b) \\
=&a \cdot (\phi(1)\phi(b)) \\
=&(a \cdot \phi(1))\phi(b) \\
=&\phi(a \cdot 1)\phi(b) \\
=&\phi(a)\phi(b)
\end{aligned}
$$

□

Exercise 15.58. *Let m and n are distinct positive integer, Show that $mZ \approx nZ$ implies False.*

Proof. Note that a ring isomorphism $\phi : mZ \to nZ$ is also a (additive) group isomorphism, therefore $\phi(m) = n$ or $-n$. Consider $\phi(m^2)$, we know $n^2 = \phi(m^2) = \phi(m \cdot m)$ since we are in Z, then $m \cdot \phi(m) = m \cdot (\pm n) = \pm mn$, we get $\pm m = n$ by cancellation (since Z is an integral domain). We know both m and n are positive, so $-m = n$ is impossible, therefore $m = n$, but we also know m and n are distinct. □

Exercise 15.59. *Let D an integral domain and let F be the field of quotient of D. For any field E that contains D, show that F is ring-isomorphic to some subfield of E.*

Proof. Consider the mapping $\phi(a/b) = ab^{-1}$, but we have to show that it **is** a mapping. For any a/b and c/d in F such that $a/b = c/d$, that is, $ad = bc$. Then $\phi(a/b) = ab^{-1} = ab^{-1}dd^{-1} = bcb^{-1}d^{-1} = cd^{-1} = \phi(c/d)$ (recall that E is commutative).

We claim ϕ is a homomorphism from F to E, for any a/b $c/d \in F$ (We denote $+_F$ as the addition of F and $+$ as the addition of E):

- $$\begin{aligned} &\phi(a/b +_F c/d) \\ =&\phi((ad + bc)/bd) \\ =&(ad + bc)(bd)^{-1} \\ =&add^{-1}b^{-1} + bcd^{-1}b^{-1} \\ =&ab^{-1} + cd^{-1} \\ =&\phi(a/b) + \phi(c/d) \end{aligned}$$

- $$\begin{aligned} &\phi(a/b \cdot c/d) \\ =&\phi(ac/bd) \\ =&ac(bd)^{-1} \\ =&ab^{-1}cd^{-1} \\ =&\phi(a/b)\phi(c/d) \end{aligned}$$

Further more, we hope that ϕ is also one-to-one, suppose $\phi(a/b) = \phi(c/d)$, we know $ab^{-1} = cd^{-1}$ and then $ad = bc$, which implies $a/b = c/d$.

Therefore, $F \approx \phi(F)$ where $\phi(F)$ is a subfield of E (it is a field since F is a field). □