III.13.28. The map \( \phi_g \) is a homomorphism if and only if \( g = e \). Note that one should prove that \( \phi_e \) is a homomorphism.

III.13.34. A nontrivial homomorphism is for example \( \phi(n) := n \mod 4 \).

III.14.4. The answer is 3.

III.14.6. The answer is \( \frac{12 \cdot 18}{6} = 36 \).

III.14.8. The answer is 1.

III.14.12. The order of the element is 2.


III.15.4. The answer is \( \mathbb{Z}_8 \).

III.15.8. The answer is \( \mathbb{Z} \times \mathbb{Z} \).

III.15.10. The answer is \( \mathbb{Z} \times \mathbb{Z}_4 \times \mathbb{Z}_8 \).

III.15.12. The answer is \( \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_3 \).

IV.18.11. The set is commutative ring with identity (unity), but not a field.

IV.18.12. The set is a field (and thus it is commutative ring with identity).

IV.18.22. It is not a ring homomorphism since \( \det(A + B) \neq \det A + \det B \) in general.

IV.18.55. We have that \( a^2 = a \) and \( -a = (-a)(-a) = a^2 \). Therefore \( a = -a \) for every \( a \in R \), or \( 2a = 0 \). But then from \( a^2 + b^2 = a + b = (a + b)(a + b) = a^2 + ab + ba + b^2 \) we find that \( ab = -ba = ba \).

IV.19.4. There is only one solution: \( x = 2 \) (case-by-case proof).

IV.19.26. (a) Suppose that \( ax = 0 \) for some \( a, x \in R \). Assume that \( a \neq 0 \) (possible because \( R \) has at least two elements, and therefore at least one non-zero). Must show that \( x = 0 \). Let \( b \) be the unique element in \( R \) for which \( a = aba \). Then \( a(b + x)a = aba + axa = a + 0 = a \), and by the uniqueness of \( b \) we have \( b + x = b \). Thus \( x = 0 \).
(b) We showed this in class: If \( a = aba \), then \( a = ababa \) and by the uniqueness of \( b \) we have \( b = bab \).

(c) Since the ring has at least two elements we may choose a nonzero element \( a \) in \( R \). Let \( b \) be the unique element for which \( a = aba \). Then we will show that the element \( e := ab \) is left and right identity (unity) of \( R \).

- \( e \) is a left unity: Let \( r \in R \). Then \( abr = ababr \) and thus \( ab(r - abr) = 0 \). But by (a), \( R \) is an integral domain and because \( ab \neq 0 \) we have \( r - abr = 0 \). Therefore \( r = er \).

- \( e \) is a right unity: Let \( r \in R \). Then \( rab = rabab \) and thus \( (r - rab)ab = 0 \). Again, since \( R \) is an integral domain we conclude \( r - rab = 0 \). Therefore \( r = re \).

(d) If \( a \in R \) and \( a \neq 0 \), as we proved in (c) we have that \( ab \) equals the identity of \( R \) where \( b \) is the unique element in \( R \) for which \( a = aba \). Therefore \( a \) has (right) inverse.

IV.20.8. The answer is \( \varphi(p^2) = p^2 - p \).

IV.21.1. In this problem we have to describe the field \( F \) of quotients of the domain \( D \). Note that by definition, \( F \) is the set of equivalence classes \([([n_1 + m_1 i, n_2 + m_2 i])\) of \( D \times D^* \) with equivalence relation

\[
(n_1 + m_1 i, n_2 + m_2 i) \sim (k_1 + l_1 i, k_2 + l_2 i)
\]

if and only if

\[
(n_1 + m_1 i)(k_2 + l_2 i) = (n_2 + m_2 i)(k_1 + l_1 i).
\]

We will show that \( F \) is isomorphic to the following field:

\[
\mathbb{Q}[i] := \{a + bi \mid a, b \in \mathbb{Q}\}.
\]

The isomorphism \( \varphi : F \to \mathbb{Q}[i] \) is given by the formula

\[
\varphi([([n_1 + m_1 i, n_2 + m_2 i])] := \frac{n_1 + m_1 i}{n_2 + m_2 i}
\]

or in short \( \varphi([z, w]) := \frac{z}{w} \) for \((z, w) \in D \times D^* \). In what follows we show that \( \varphi \) is an isomorphism.

- The map \( \varphi \) is well-defined because of (??).
- The map \( \varphi \) is a homomorphism of rings because:

\[
\varphi([([z_1, w_1]) + ([z_2, w_2])]) = \varphi(([z_1, w_2] + [z_1, w_1], [z_2, w_2])) = \frac{z_1 w_2 + w_1 z_2}{w_1 w_2} = \frac{z_1}{w_1} + \frac{z_1}{w_1} = \varphi(([z_1, w_1])) + \varphi(([z_2, w_2]))
\]

Similarly \( \varphi(([z_1, w_1]) \cdot ([z_2, w_2])) = \varphi(([z_1, w_1]) \cdot \varphi(([z_2, w_2]))).

- The map \( \varphi \) is onto because for \( \frac{z}{w} \in \mathbb{Q}[i] \) we have \( \varphi(([z, w])) = \frac{z}{w} \).
- The map \( \varphi \) is one-to-one because if \( \varphi(([z, w])) = 0 \) then \( z = 0 \), i.e. \([z, w] = [(0, 1)]\).