3. Proof  Consider \((a+b)^2\). Since \((a+b)^2 = a^2 + ab + ba + b^2\), and \(a^2 = a\), so \(ab + ba = 0\). Now let \(b = a\), we have \(a + a = 0\). So \(ab = -ba = (-b)a = ba\), then \(R\) is commutative.

6. Proof  Let \(R = \{0, a_1, L, a_n\}\), then \(\forall a_i (i = 1, L, n)\), \(a_i a_i, L, a_i a_n\) are relatively unequal, otherwise \(a_i a_k = a_i a_l\) for some \(k, l\), so \(a_i (a_k - a_l) = 0\), it is contradict. So \(\forall a_i\), \(a_i = a_i a_j\), for some \(j\). Therefore \(a_i x = a_i\) and \(x a_i = a_i\) have solutions in \((R, \cdot)\). By proposition 1.4, \((R, \cdot)\) is a group, so \((R, +, \cdot)\) is a division ring.

8. Proof  First to prove \(R\) is a ring.

   Obviously, \((R, +)\) is an abelian group. Because matrix satisfies associative on multiplication, we only need to prove that \(\forall a, b \in R, ab \in R\). Let \(a = \begin{pmatrix} z & w \\ -w & z \end{pmatrix}, b = \begin{pmatrix} x & y \\ -y & x \end{pmatrix}\), then

   \[
   ab = \begin{pmatrix} zx - \overline{w y} & \overline{z y + w x} \\ -\overline{z y + w x} & zx - w y \end{pmatrix} \in R, \text{ so } R \text{ is a ring.}
   \]

   Now to prove \(R \cong K\).

   By the hint, to prove it is a ring isomorphism. It is easy.

14. Proof  We have a fact: if \(p\) is prime, \(p | C_p^k\) for \(1 \leq k \leq p - 1\).

   For \(\forall r_1, r_2 \in R\), \(\phi(r_1 + r_2) = (r_1 + r_2)^p = r_1^p + r_2^p + \sum_{k=1}^{p-1} C_p^k r_1^k r_2^{p-k}\). By the fact, we have \(C_p^k r_1^k r_2^{p-k} = 0\) for \(1 \leq k \leq p - 1\). So

   \[
   \phi(r_1 + r_2) = r_1^p + r_2^p = \phi(r_1) + \phi(r_2) \].
\[ \phi(r_1r_2) = (r_1r_2)^p = r_1^pr_2^p = \phi(r_1)\phi(r_2). \]

P133---P135

5. Proof Obviously, \( I \subset [R:I] \). \( \forall r_1, r_2 \in [R:I], r, x, y \in R \), we have \( x(r_1 - r_2) = xr_1 - xr_2 \in I \), and \( r(xr_1y) = (rx)r_1y \in I \), so \( r_1 - r_2, xr_1y \in [R:I] \).

10. Proof \( \forall I < Z \), then \( (I,+)<(Z,+), \) since \( (Z,+) \) is cyclic, so \( (I,+)=nZ, \) for some \( n \). So \( Z \) is a principal ideal ring.

(b) let \( R \) be principal ideal ring and \( G \) be a ring, \( \phi : R \to G \) is a ring homomorphism. Then \( \phi(R) \) is a subring of \( G \). Let \( I < \phi(R) \), then \( \phi^{-1}(I) < R \), since \( R \) is principal ideal ring, so \( \phi^{-1}(I) \) is a principal ideal, that is \( \phi^{-1}(I) = (a) \), for some \( a \in R \). So \( I = (\phi(a)) \) is a principal ideal, then \( \phi(R) \) is principal ideal ring.

(c) According to (a), (b).

15. Proof Let \( S = R - \{ r \in R \mid r = 0 \text{ or } r \text{ is divisor} \}, \) \( \Omega = \{ I < R \mid I \cap S = \Phi \} \). By Zorn’s Lemma, \( \Omega \) contains a maximal ideal \( P \). Now to prove \( P \) is prime ideal. It is clear that \( P \subset \{ r \in R \mid r = 0 \text{ or } r \text{ is divisor} \} \).

For \( \forall x, y \in R, xy \in P \),

If \( x = 0 \) or \( y = 0 \), then \( x \in P \) or \( y \in P \);

If \( x \neq 0 \) and \( y \neq 0 \), suppose \( x \notin P \) and \( y \notin P \). Since \( xy \in P \), so there exists \( 0 \neq r \in R \) such that \( (xy)r = 0 \).

(i) if \( yr = 0 \), then \( y \in \{ r \in R \mid r = 0 \text{ or } r \text{ is divisor} \} \), so \( \langle P, y \rangle < R \), and \( \langle P, y \rangle \mid \Omega = \Phi \), it is contradict to the maximal of \( P \).

(ii) if \( yr \neq 0 \), then \( x \in \{ r \in R \mid r = 0 \text{ or } r \text{ is divisor} \} \), so \( \langle P, x \rangle < R \),
and \( \langle P, x \rangle \not| \Omega = \Phi \), it is contradict to the maximal of \( P \).

So \( P \) is prime ideal.

21. Proof (i) if \( m \) is prime, then prime and maximal ideals are both \( \{0\} \).

(ii) if \( m \) is not prime, let \( m = p_1^{n_1} \cdots p_r^{n_r} \), since \( Z_m \) is a principal ideal ring and \( Z_m \cong \mathbb{Z}/m\mathbb{Z} \), so all the ideals of \( Z_m \) can be viewed as \( n\mathbb{Z}/m\mathbb{Z} \) for some \( n \in \mathbb{Z} \). By the Theorem 2.16, \( P \) is prime ideal of \( Z_m \) if and only if \( Z_m/P \) is an integral domain. Since \( Z_m/P = Z/n\mathbb{Z} \cong \mathbb{Z} \), for some \( n \in \mathbb{Z} \), so \( n \) is prime (because \( Z \) is an integral domain if and only if \( n \) is prime) and \( n|m \). So \( P = Z_{p_i} \) for some \( p_i \). According to Theorem 2.20, similarly, maximal ideals are the same to the prime ideals.

23. Proof (a) Since \( e \) is a central idempotent in \( R \), so \( \forall a \in R \),
\[
e^2 = e, \quad ea = ae.
\]
\[
(1_r - e) a = 1_r a - ae = a 1_r - ae = a (1_r - e), \quad \text{and} \quad (1_r - e)^2 = 1_r - e.
\]

(b) \( \forall r_1, r_2, r \in R \), we have
\[
er_1 - er_2 = e(r_1 - r_2) \in eR \quad \text{and} \quad r_1 (er_2) = e(r_1 r_2) \in R,
\]
so \( eR < R \). Similarly \( (1_r - e) R < R \).

Obviously, \( R = eR + (1_r - e) R \). \( \forall a \in eR \) \( (1_r - e) R \),
\[
a = e r_1 = (1_r - e) r_2 \quad \text{for some} \quad r_1, r_2 \in R. \quad \text{So} \quad r_2 = e(r_1 + r_2) \in eR.
\]
So \( a = (1_r - e) e (r_1 + r_2) = (e - e^2)(r_1 + r_2) = 0 \), \( eR \) \( (1_r - e) R = \{0\} \).

By Theorem 2.24, \( R \cong eR \times (1_r - e) R \).