1. a) $\mathbb{Z}[i]$ is an integral domain
   - commutative ring with identity 1 for multiplication
   - as it is a subring of $\mathbb{C}$ containing 1 (Gallian, p. 249)
   - Since $\mathbb{C}$ is a field, it has no 0-divisors (Gallian, p. 251)
   - which implies $\mathbb{Z}[i]$ has no 0-divisors

   $\mathbb{Z}/12\mathbb{Z}$ is not an integral domain

   2. $(\mod 12)$ is a zero divisor as $2 \cdot 6 = 0 \mod 12$

   $M_2(\mathbb{Z}_2)$ is not an integral domain (it's not commutative) (either)

   $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$

   $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$

   $\mathbb{Z} \oplus \mathbb{Z}$ is not an integral domain

   $(1,0)(0,1) = (0,0)$

   $\mathbb{Z}/11\mathbb{Z}$ is an integral domain

   - commutative ring with identity $1 \mod 11$, for multiplication
   - no zero divisors by Euclid's Lemma

   $\mathbb{Q}$ is a field $\Rightarrow \mathbb{Q}$ is an integral domain (Gallian, p. 251)

   $f(x) = \frac{p(x)}{q(x)}$, $p, q \in \mathbb{Z}$, $q \neq 0$

   $\mathbb{C}[\mathbb{R}]$ is not an integral domain

   If $f(x) = 0$, $x \in (a, b)$, $f$ is a zero divisor

   For $f \in \mathbb{C}[\mathbb{R}]$ s.t. $f(x) = 0$ for all $x \notin (a, b)$, $f \equiv 0$

   Then $\mathbb{C}[\mathbb{R}]$ is not an integral domain

   So $fg = 0$ function.

b) $\mathbb{Z}[i]$ is not a field, $\frac{1}{2} \notin \mathbb{Z}[i]$ $\mathbb{Z}/12\mathbb{Z}$ is not a field, as not an integral domain

   $M_2(\mathbb{Z}_2)$ is not a field, as not an integral domain

   $\mathbb{Z} \oplus \mathbb{Z}$ is not an integral domain

   $\mathbb{Z}/11\mathbb{Z}$ is a field, as it is a finite integral domain (Gallian, p. 251)

   $\mathbb{C}[\mathbb{R}]$ is not a field, as not an integral domain

   The rationals are a field as stated in a).
Define \( g \) to be non-0 at \( x_0 \) but 0 everywhere else. Then \( fg = 0 \).

\[ \mathbb{Z}/12\mathbb{Z} \] has no zero divisors
\[ \mathbb{Z}/12\mathbb{Z} \] has 0-divisors: \( 2, 3, 4, 6, 8, 9, 10 \) (mod 12)
\[ \mathbb{Z}/2\mathbb{Z} \] has 0-divisors
\( (0, 0), (1, 0), (0, 1) \)
\( (1, 0), (0, 1), (1, 1) \)
\[ \mathbb{Z} \times \mathbb{Z} \] has 0-divisors (infinitely many)
\( (n, 0), (0, n) \), \( n \in \mathbb{Z} \)

\[ \mathbb{Z}/11\mathbb{Z} \] has no zero divisors

\( \mathbb{C}(\mathbb{R}) \) zero divisors: non-0 functions \( f(x) \) s.t. \( \exists x_0 + \mathbb{R} \) with \( f(x_0) = 0 \)

b) \( U(\mathbb{Z}[i]) = \{ 1, -1, i, -i \} \) Lectures #4, p. 6
\( U(\mathbb{Z}/12\mathbb{Z}) = \{ 1, 5, 7, 11 \) (mod 12) \}
\( U(\mathbb{Z}/2\mathbb{Z}) = \{ (a, b) \mid a, b, c, d \in \mathbb{Z}/2\mathbb{Z}, \ ad-bc \neq 0 \) (mod 2) \}
\( = \{ (1, 0), (0, 1), (1, 1), (0, 1), (1, 0), (1, 1) \} \)
\( U(\mathbb{Z} \times \mathbb{Z}) = \{ (1, 1) \} \)
\( U(\mathbb{Z}/11\mathbb{Z}) = (\mathbb{Z}/11\mathbb{Z})^* = \{ x(\text{mod} 11) \mid x \neq 0 \) (mod 11) \}
\( U(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q} - \{ 0 \} \)
\( U(\mathbb{C}(\mathbb{R})) = \{ f : \mathbb{R} \to \mathbb{R} \mid f \) continuous, \( f(x) + 0 \) for \( x \in \mathbb{R} \} \)

c) \{ zero-divisors in \( \mathbb{R} \} \cup \{ 0 \} \cup U(\mathbb{R}) = \mathbb{R} \\
except for \# e, iv
3) See Lectures 5, p.12

4) Since this integral domain \( D \) is finite, it must be a field (by Thm. 13.2 of Gallian). \( \Rightarrow \) characteristic of \( D \) is 0 or a prime. (by Thm. 13.4 of Gallian).

Under addition, \( D \) must be an abelian group under + of order 6. Therefore \( D \) must be cyclic. Why? (if there were no element of additive order 6, all non-0 elements of \( D \) would have additive order 2 or 3. Let \( a \neq 0 \) in \( D \).

\[ D/\langle a \rangle \text{ has order } \frac{6}{\text{order}(a)} \Rightarrow \text{you get elements of both orders say } a^k. \text{ Then order } \langle a^6 \rangle = 6. \]

Call the generator \( a \). Then \( D = \{ 0, a, 2a, \ldots, 5a \} \).

This means \( \phi: D \to \mathbb{Z}/6\mathbb{Z} \) is a group isomorphism, for \( D \) under + \( \mathbb{Z}/6\mathbb{Z} \) under +.

\[ \begin{align*}
\phi(0) &= 0 \\
\phi(a) &= 1 \pmod{6} \\
\phi(5a) &= 5 \pmod{6}
\end{align*} \]

But \( (a)^1 + (5a)^1 = 0 \in D \Rightarrow \text{characteristic of } D = 6 \).

This contradicts Thm. 13.4. So \( D \) can't be an integral domain.

\[ \text{and 6 is the smallest } n \text{ such that } n \cdot a = 0. \]

5) a)

If \( a \) and \( b \) are in \( F^* \), then \( ab \) can't be 0 as \( F \) has no zero divisors so \( ab \) is in \( F^* \). Also 1 is not equal to 0 so it must be in \( F^* \). This means \( F^* \) is closed under multiplication and has an identity for multiplication.

If \( a \) is not 0, then \( a^{-1} \) is not 0, as \( aa^{-1} = 1 \). Thus every element of \( F^* \) has an inverse.

So \( F^* \) is a group under multiplication, as we know multiplication is associative in a field.

b) Since \( F^* \) is a group of order \( n-1 \), we know \( x^* F^* = x^{n-1} = 1 \) by Cor 4, p.143 of Gallian.

This happens because \( \text{order}(x) = \frac{1}{\text{order}(F^*)} \) by Lagrange's Thm, p.141 of Gallian.

\( \text{cyclic as generated by } x \), \( x^n \equiv 1 \pmod{2} \).
a) \( \mathbb{Z}_5 [i] \) has 0-divisors

\[(2+i)(2-i) = 4 + 1 = 0 \text{ in } \mathbb{Z}_5 [i] \]

b) \( \mathbb{Z}_7 [i] \) is certainly a commutative ring with identity (1) for multiplication. By Thm 13.2 in Gallian, we just need to show \( \mathbb{Z}_7 [i] \) has no zero divisors—which says it's an integral domain and thus a field.

Suppose
\[(a+bi)(c+di) = 0 \text{ in } \mathbb{Z}_7 [i] \]

Then
\[(a+bi)(a-bi)(c+di)(c-di) = 0 \]
\[(a^2+b^2)(c^2+d^2) = 0 \text{ in } \mathbb{Z}_7 \]

But \( x \neq 0 \text{ (mod 7)} \) \( \Rightarrow \)

\[x^2 \text{ (mod 7)} \notin \{1, 4, 2 \text{ (mod 7)} \} \]

if \( a+bi \neq 0 \), then \( a^2+b^2 \in \{1, 4, 2 \text{ (mod 7)} \} \)

But this means the only way \( a^2+b^2 = 0 \text{ in } \mathbb{Z}_7 \)
is for \( a = b = 0 \text{ in } \mathbb{Z}_7 \).

A more direct proof:

Show \( a+bi \neq 0 \text{ in } \mathbb{Z}_7 [i] \) \( \Rightarrow \) \( \exists \frac{1}{a+bi} \in \mathbb{Z}_7 [i] \).

\[
\frac{1}{a+bi} = \frac{1}{a+bi} \frac{a-bi}{a^2+b^2} = \frac{a}{a^2+b^2} - \frac{b}{a^2+b^2} i
\]

Once more we just need to know \( a^2+b^2 \neq 0 \text{ in } \mathbb{Z}_7 \)
assuming either \( a \) or \( b \) is non-0.

c) (109) We need \( p \text{ s.t. } a, b \text{ not both 0 in } \mathbb{Z}_p \Rightarrow \)

\[a^2+b^2 \neq 0 \text{ in } \mathbb{Z}_p, \text{ Assume } a \neq 0 \]

\[\Rightarrow \exists a^{-1} \in \mathbb{Z}_p \Rightarrow l+\left(\frac{b}{a}\right)^2 \neq 0 \text{ in } \mathbb{Z}_p \]

\[\Rightarrow 1+x^2 \text{ has no root } x \in \mathbb{Z}_p \]

\[\Rightarrow -1 \neq x^2. \forall x \in \mathbb{Z}_p \]

Math 109 shows -1 is a non-square in \( \mathbb{Z}_p \)

\[\Rightarrow p \equiv 3 \text{ (mod 4)} \]
Thm (from Math 104)

If $p$ is an odd prime, $p 
mid a$

$a$ is a square $\pmod{p}$ $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

$a$ is a non-square $\pmod{p}$ $\iff a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Proof

$0 = a^{p-1} - 1 \equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \pmod{p}$

$\Rightarrow$ either $a^{\frac{p-1}{2}} \equiv 1$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

If $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$, then $a$ can't be square $\pmod{p}$.

For $a \equiv c^2 \pmod{p}$, $a^{\frac{p-1}{2}} \equiv (c^{\frac{p-1}{2}})^2 \equiv c^{p-1} \equiv 1 \pmod{p}$

Moreover, all numbers

$\ldots (\frac{p-1}{2}, \frac{p-1}{2}, \frac{p-1}{2}, \ldots)$

give $\frac{p-1}{2}$ congruent squares $\pmod{p}$ as

$1 \leq n \leq \frac{p-1}{2} \Rightarrow 0 < m-n < n < p-1 < p$

$\Rightarrow m^2 - n^2 = (m-n)(m+n) \not\equiv 0 \pmod{p}$

of the $p-1$ elements of $\mathbb{Z}_p^\times$ half are squares and give the roots of $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

The other half are the roots of $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

and must be non-squares. Once we know $\mathbb{Z}_p^\times$ is cyclic generated by $g$, the squares are the even powers of $g \pmod{p}$.

If $a = -1$ we see

$-1$ is a square $\pmod{p} \iff (-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$

$-1$ is a non-square $\pmod{p} \iff (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Since $p$ is odd, and $(-1)^{\frac{p-1}{2}}$ is $\pm 1$, we see

that

$(-1)^{\frac{p-1}{2}}$ must equal 1 or -1, according to whether -1 is a square $\pmod{p}$ or not.

Thus

$-1$ is a square $\pmod{p} \iff p \equiv 1 \pmod{4}$

$-1$ is a non-square $\pmod{p} \iff p \equiv 3 \pmod{4}$.