16.24 Only do a,b,c

a. for any $a + bi, c + di, e + fi \in \mathbb{Z}[i]$, we have

$$(a + bi) + (c + di) = (a + c) + (b + d)i = (b + di) + (a + bi) \in \mathbb{Z}[i]$$

as well as

$$(a + bi)(c + di) = ac - bd + (ad + bc)i = (c + di)(a + bi) \in \mathbb{Z}[i]$$

Finally

$$(a{+}bi{+}c{+}di)(e{+}fi) = (a{+}bi)e{+}(c{+}di)e{+}(a{+}bi)fi{+}(c{+}di)fi = (a{+}bi)(e{+}fi){+}(c{+}di)(e{+}fi)$$

And

$$1(a + bi) = (a + bi)1 = a + bi$$

Which means $\mathbb{Z}[i]$ satisfies all the properties to be a commutative ring with unity 1.

b. For $r = a + bi, s = c + di \in \mathbb{Z}[i]$ we have

$$N(rs) = N(ac{-}bd{+}(ad{+}bc)) = (ac{-}bd)^2{+}(ad{+}bc)^2 = (ac)^2{-}2abcd{+}(bd)^2{+}(ad)^2{+}2abcd{+}(bc)^2$$

$$(ac)^2 + (bd)^2 + (ad)^2 + (bc)^2 = a^2(c^2 + d^2) + b^2(c^2 + d^2) = (a^2 + b^2)(c^2 + d^2)N(r)N(s)$$

c. In order for a to be a unit, there must be some $a^{-1} \in \mathbb{Z}[i]$ such that

$$aa^{-1} = 1$$

Applying the norm to both sides we have

$$N(aa^{-1}) = N(a)N(a^{-1}) = N(1) = 1$$

However since the terms in a and a^{-1} are integers, the norms must be integers. Therefore in order for the product of their norms to be 1, both norms must be 1. Therefore $N(a) = 1$. Looking at the other direction, we can ceck every element with norm 1: $1, -1, i, -i$. Each of these terms have the respective inverse $1, -1, -i, i$. And so every element with norm one is a unit.

17.1

a. This is not a subring since it is not closed under multiplication:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \notin S$$

b. This is a subring since it is closed under multiplication and addition, and every element has an addative inverse:

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}\begin{pmatrix} d & 0 \\ e & f \end{pmatrix} = \begin{pmatrix} ad & 0 \\ be+cf & cf \end{pmatrix} \in S$$

$$\begin{pmatrix} a & 0 \\ b & c \end{pmatrix}+\begin{pmatrix} d & 0 \\ e & f \end{pmatrix} = \begin{pmatrix} a+d & 0 \\ b+e & c+f \end{pmatrix} \in S$$

c. As established last quarter, S is a group under multiplication and a group under division, and therefore is closed under multiplication, and so satisfies the requirements to be a subring.

d. We have $S = M_2(\mathbb{R})$, which has been established to be a ring. Therefore S is a subring.

17.20 If $aR = R$ then since $1 \in R$ there must be $1 \in aR$ which means there must be some a^{-1} such that $aa^{-1} = 1$ which means a is a unit. For implication in the other direction, we have for any $x \in R$, assuming a is a unit with multiplicative inverse a^{-1}, we have $a^{-1}x \in R$ and $a(a^{-1}x) = x \in aR$. Therefore every element of R is an element of aR and so $R \subseteq aR$, and since R is closed under multiplication, for any $x \in R$, $ax \in R$, so $aR \subseteq R$ and so it follows

$$R = aR$$

A

a. We have

$$a^2 = a \Rightarrow a^2 - a = 0 \Rightarrow a(a-1) = 0$$

Since R is an integral domain, $a(a-1) = 0$ if and only if either a or $a-1$ is zero, and since the additive inverse is unique, that means a is either 1 or 0.

b. The idempotents are 1, 5, and 6.

c. For any $(a, b) \in \mathbb{Z} \times \mathbb{Z}$ we have

$$(a, b)(a, b) = (a, b) \Rightarrow (a^2 - a, b^2 - b) = (0, 0) \Rightarrow a^2 - a = 0, b^2 - b = 0$$

And since $\mathbb{Z}$ is an integral domain, from question Aa it means $a, b \in \{0, 1\}$ and so the idempotents are $(0, 0), (1, 1), (1, 0), (0, 1)$

B We can deduce the set of idempotents in S is a subset of the idempotents in R since $s \in S \Rightarrow s \in R$ and the conditions in either set is the same: $s^2 = s$.
As shown in problem Aa, the only idempotents in R are 1_R and 0_R

Subrings of an integral domain is an integral domain as well so S also has the property that the idempotents in S are 1_S and 0_R. Therefore we have.

$$\{0_S, 1_S\} \subseteq \{0_R, 1_R\}$$

From basic group theory we know the identity of a subgroup is equal to the identity of the containing group. Therefore $0_S = 0_R$ since 0 is the identity of the groups R, S over addittion. So we have $1_S \neq 0_S \Rightarrow 1_S \neq 0_R$. The only other element in $\{0_R, 0_S\}$ that 1_S can be is 1_R

C $U(R) = \{(1,1), (-1,1), (1,-1), (-1,-1)\}$ since the only units in $\mathbb{Z}$ is 1 and -1.

D True:
Consider the subring

$$S = 5\mathbb{Z}_{25} = \{0, 5, 10, 15, 20\}$$

This is a subring since we have $x|5 \Leftrightarrow x \in S$ and for any $a, b \in S$, $ab|5$ so $ab \in S$. We also have $a + b|5$ so $a + b \in S$. Thererfore S is closed under addition and multiplication and is finite, so it is a subring. S is isomorphic to $\mathbb{Z}_5$, let $\varphi : S \to \mathbb{Z}_5$ with $\varphi(5x) = x$. We have

$$\varphi(5x)\varphi(5y) = xy = \varphi(5xy)$$

and

$$\varphi(5x) + \varphi(5y) = x + y = \varphi(5(x + y))$$

So φ is a homomorphism. We have $\varphi(0) = 0, \varphi(5) = 1, \varphi(10) = 2, \varphi(15) = 3, \varphi(20) = 4$, and so φ is a bijections so an isomorphism.

E The four ideals are R, $R_r = \{(0, x) : x \in \mathbb{R}\}, R_l = \{(x, 0) : x \in \mathbb{R}\}, \{(0, 0)\}$. Since the idempotents of R are $(0, 0), (1, 0), (0, 1), (1, 1)$ and we know that the multiplicative identity of a subring must be one of these terms. If the identity is $(0, 0)$ we get the subring $\{(0, 0)\}$ since every term in R multiplies with $(0, 0)$ to $(0, 0)$. If the identity is $(1, 1)$, then for any $(x, y) \in R$ $(1, 1)(x, y) = (x, y)(1, 1) = (x, y)$, and so the subring would have to be R to satisfy the ideal property. If the identity is $(1, 0)$ then for any $(x, y) \in R$ we have $(1, 0)(x, y) = (x, y)(1, 0) = (x, 0)$ therefore the group would be R_l, and by symmetry for the identity being $(0, 1)$, the group would be R_r.