16.24. **SOLUTION:** We already proved in class that \( \mathbb{Z}[i] \) is a commutative ring with unity. It is the smallest subring of \( \mathbb{C} \) containing \( \mathbb{Z} \) and \( i \). If \( r = a + bi \) is in \( \mathbb{Z}[i] \), then \( a \) and \( b \) are in \( \mathbb{Z} \). It follows that \( N(r) = a^2 + b^2 \) is a nonnegative integer.

Suppose that \( r = a + bi \) and \( s = c + di \) are elements of \( \mathbb{Z}[i] \). Then \( N(r) = a^2 + b^2 \) and \( N(s) = c^2 + d^2 \). Note that \( rs = (ac - bd) + (ad + bc)i \) and therefore

\[
N(rs) = (ac - bd)^2 + (ad + bc)^2 = (a^2c^2 - 2acbd + b^2d^2) + (a^2d^2 + 2adbc + b^2c^2)
\]

\[
= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 = (a^2 + b^2)(c^2 + d^2) = N(r)N(s)
\]
as stated in the problem.

Suppose that \( r \) is a unit in \( \mathbb{Z}[i] \). Then there exists an element \( s \in \mathbb{Z}[i] \) such that \( rs = 1 = 1 + 0i \). We have \( N(1) = 1 \). Hence \( N(rs) = 1 \). Therefore, \( N(r)N(s) = 1 \). Since both factors are nonnegative integers and their product is 1, it is clear that each factor must be 1. Thus, if \( r \) is a unit in \( \mathbb{Z}[i] \), then \( N(r) = 1 \).

For the converse, note that if \( r = a + bi \in \mathbb{Z}[i] \), then \( N(r) = a^2 + b^2 = (a + bi)(a - bi) \). Let \( s = a - bi \). Then \( s \in \mathbb{Z}[i] \) too. We have \( N(r) = rs \). If \( N(r) = 1 \), then \( rs = 1 \). It follows that \( r \) is a unit in \( \mathbb{Z}[i] \).

We have proved that \( r \) is a unit in \( \mathbb{Z}[i] \) if and only if \( N(r) = 1 \). The equation \( a^2 + b^2 = 1 \), where \( a, b \in \mathbb{Z} \), obviously has only four solutions, namely

\[
(a, b) = (1, 0), (-1, 0), (0, 1), \text{ or } (0, -1)
\]

It follows that there are four units in \( \mathbb{Z}[i] \), namely, 1, \(-1\), \(i\), and \(-i\). Thus, \( U(\mathbb{Z}[i]) \) has order 4. It is clearly the cyclic group generated by \( i \).

---

**Problem 16.26** Give an example of a finite noncommutative ring.

**SOLUTION:** Let \( F = \mathbb{Z}_2 = \{0,1\} \). Let \( R = M_2(F) \). Since \( F \) has two elements, it is clear that \( R \) has \( 2^4 = 16 \) elements. As discussed in class, \( R \) is a ring. One verifies that \( R \) is noncommutative by just considering the elements

\[
A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.
\]
One finds that

\[ AB = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad BA = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} . \]

We have \( A, B \in R \) and \( AB \neq BA \). Thus, \( R \) is a noncommutative ring with just a finite number of elements.

**Problem 17.1 SOLUTIONS:** For part (a), the subset \( S \) fails to be closed under multiplication. In fact, \( A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \) is in \( S \), but \( AA = A^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \) is not in \( S \).

For part (c), the set \( S \) is not closed under addition. It is not a subgroup of \( M_2(\mathbb{R}) \) under addition. Let \( A = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \) and let \( B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \). Then \( A \) and \( B \) have nonzero determinant and hence are in the given subset, but \( A + B = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \) has determinant equal to 0 and is not in the given subset.

For parts (b) and (d), one sees easily that they are both subgroups of \( M_2(\mathbb{R}) \) under addition. Concerning multiplication, we note that

\[ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \begin{pmatrix} e & 0 \\ g & f \end{pmatrix} = \begin{pmatrix} ae & 0 \\ ce + df & df \end{pmatrix} \]

and

\[ \begin{pmatrix} a & b \\ b & a \end{pmatrix} \begin{pmatrix} c & d \\ d & c \end{pmatrix} = \begin{pmatrix} ac + bd & ad + bc \\ bc + ad & bd + ac \end{pmatrix} = \begin{pmatrix} ad + bc & ac + bd \end{pmatrix} \]

These calculations show that both of the sets specified in parts (b) and (d) are closed under multiplication.

It follows that the subsets of \( M_2(\mathbb{R}) \) in parts (b) and (d) are subrings.

**Problem 17.20** Suppose \( R \) is a commutative ring with unity 1 and that \( a \in R \). Prove that \( aR = R \) if and only if \( a \) is a unit in \( R \).

**SOLUTION:** First of all, assume that \( aR = R \). In particular, \( 1 \in R = aR \) and hence there exists an element \( b \in R \) such that \( 1 = ab \). Since \( R \) is commutative, we also have \( ba = 1 \). Hence \( a \) is a unit of \( R \).
Now assume that $a$ is a unit in $R$. Hence there exists an element $b \in R$ such that $ab = 1$. Suppose that $r \in R$ Then

$$r = 1r = (ab)r = a(br) \in aR$$

because $br \in R$. Thus, $R \subseteq aR$. It is obvious that $aR \subseteq R$. Therefore, we have shown that $aR = R$ whenever $a$ is a unit of $R$.

**Problem A, part (a)** Suppose that $R$ is an integral domain. Find all the idempotents in $R$.

**SOLUTION:** Let $0 = 0_R$ and $1 = 1_R$. First of all, note that $0 \cdot 0 = 0$ and $1 \cdot 1 = 1$. Hence the elements 0 and 1 are idempotents. Also $1 \neq 0$ because $R$ is an integral domain. Suppose that $e \in R$ is an idempotent. Then

$$e \cdot e = e = e \cdot 1$$

We already know that 0 is an idempotent in $R$. Suppose that $e \neq 0$. Then, by the cancellation law discussed in class (which is valid for any integral domain $R$), the equation $e \cdot e = e \cdot 1$ implies that $e = 1$. Therefore, there are only two idempotents in $R$, namely the elements 0 and 1.

**Problem A, part (b)** Suppose that $R$ is $\mathbb{Z}_{10}$. Find the idempotents in $R$.

**SOLUTION:** We just have to check each of the 10 elements in $R$. We find that

$$0 \cdot 0 = 0, \ 1 \cdot 1 = 1, \ 2 \cdot 2 = 4, \ 3 \cdot 3 = 9, \ 4 \cdot 4 = 6, \ 5 \cdot 5 = 5, \ 6 \cdot 6 = 6, \ 7 \cdot 7 = 9, \ 8 \cdot 8 = 6, \ 9 \cdot 9 = 1.$$  

Therefore, the idempotents in $R$ are 0, 1, 5, and 6.

**Problem A, part (c)** Suppose that $R = \mathbb{Z} \oplus \mathbb{Z}$. Find the idempotents in $R$.

**SOLUTION:** We make the following general observation. Suppose that $R_1$ and $R_2$ are rings. Let $R = R_1 \oplus R_2$. Every element $r \in R$ is of the form $r = (r_1, r_2)$ where $r_1 \in R_1$ and $r_2 \in R_2$. Note that $rr = (r_1r_1, r_2r_2)$. We have

$$rr = r \iff (r_1r_1, r_2r_2) = (r_1, r_2) \iff r_1r_1 = r_1 \ and \ r_2r_2 = r_2.$$
It follows that $r$ is an idempotent in the ring $R$ if and only if $r_1$ is an idempotent in $R_1$ and $r_2$ is an idempotent in $R_2$.

We can apply the above observation to the ring $R = \mathbb{Z} \oplus \mathbb{Z}$. Since $\mathbb{Z}$ is an integral domain, the idempotents in $\mathbb{Z}$ are 0 and 1. It then follows that the idempotents in $R$ are the four elements

$$(0, 0), \quad (1, 0), \quad (0, 1), \quad (1, 1).$$

**Problem B:** Suppose that $R$ is an integral domain. Let $1_R$ be the unity element of $R$. Suppose that $!$ is a subring of $R$, that $S$ is a ring with unity $1_S$, and that $1_S \neq 0_S$. Prove that $1_S = 1_R$. Furthermore, prove that $S$ is an integral domain.

**SOLUTION** Since $1_S$ is the unity in $S$, we have $1_S1_S = 1_S$. Also, $S$ is a subset of $R$ and hence $1_S$ is an element of $R$. Since $1_S1_S = 1_S$, it follows that $1_S$ is an idempotent in the ring $R$. Now $S$ is a subgroup of $R$ under the operation + and hence $0_S = 0_R$. Since $1_S \neq 0_S$, it follows that $1_S \neq 0_R$.

Since $R$ is an integral domain, we can use part (a) of problem A. The only idempotents in $R$ are $0_R$ and $1_R$. Now $1_S$ is an idempotent in $R$ and $1_S \neq 0_S$. Therefore, we must have $1_S = 1_R$.

We can see that $S$ is an integral domain as follows. Since $S$ is a subring of $R$ and $R$ is a commutative ring, it follows that $S$ is a commutative ring. Also, $S$ has a unity $1_S$ and $1_S \neq 0_S$. Furthermore, if $a, b \in S$ and $a \neq 0, b \neq 0$, then we can conclude that $ab \neq 0$ because $a$ and $b$ are also nonzero elements of $R$ and $R$ is an integral domain. Therefore, $S$ is indeed an integral domain.

**Problem C:** Let $R = \mathbb{Z} \oplus \mathbb{Z}$. Determine $U(R)$.

**SOLUTION:** We will use what we proved in the solution of problem 16.11 in problem set 1. If $R_1$ and $R_2$ are rings with unity, we proved that an element $(a_1, a_2)$ is a unit in $R_1 \oplus R_2$ if and only if $a_1$ is a unit in $R_1$ and $a_2$ is a unit in $R_2$. We can apply that to this question. The units in the ring $\mathbb{Z}$ are 1 and -1. Therefore, it follows that the units in the ring $R$ are

$$(1, 1), \quad (1, -1), \quad (-1, 1), \quad (-1, -1).$$

**Problem D:** TRUE OR FALSE: The ring $R = \mathbb{Z}_{25}$ contains a subring which is isomorphic to $\mathbb{Z}_5$. Explain your answer carefully.
SOLUTION: The statement is false. It is true that the additive group $\mathbb{Z}_{25}$ contains a subgroup of order 5. This is true because the group $\mathbb{Z}_{25}$ is a cyclic group of order 25 and 5 divides 25. In fact, that subgroup is unique and consists of the elements $S = \{0, 5, 10, 15, 20\}$. Furthermore, it is clear that $S$ is closed under multiplication and so $S$ is a subring of $R$. In fact, one checks easily that $ab = 0$ for all $a, b \in S$.

Suppose that $T$ is a ring which is isomorphic to $S$ and let $\phi : S \to T$ be an isomorphism. Then $T$ must also have five elements. Since $ab = 0_S$ for all elements $a, b \in S$, it follows that $\phi(a)\phi(b) = \phi(ab) = \phi(0_S) = 0_T$. Since $\phi$ is surjective, it follows that $t_1t_2 = 0_T$ for all $t_1, t_2 \in T$.

In the ring $\mathbb{Z}_5$, one has $1 \cdot 1 = 1 \neq 0$. Hence the ring $\mathbb{Z}_5$ cannot be isomorphic to $S$. Since $S$ is the only subring of $R$ with five elements, we have proved that the statement in the problem is indeed false.

Problem E: Determine all the ideals in the ring $R = \mathbb{R} \oplus \mathbb{R}$.

SOLUTION: Let $I$ be an ideal in the ring $R$. One possible ideal is the trivial ideal $I = \{(0, 0)\}$. Assume now that $I$ is a nontrivial ideal. Thus, it contains an element $(a, b)$, where $a \neq 0$ or $b \neq 0$.

Assume that $I$ contains an element $r = (a, b)$ where $a \neq 0$ and $b \neq 0$. This means that both $a$ and $b$ are units in the ring $\mathbb{R}$. It follows that $r$ is a unit in $R$. (Here we are using the result we proved in our solution to problem 16.11 which was mentioned in our solution to problem C above.) Since $I$ is an ideal of $R$ and $r \in I$, it follows that $rR \subseteq I$. We now use the result from problem 17.20. Since $r$ is a unit in $R$, it follows that $rR = R$. Therefore, $R \subseteq I$. Obviously, $I \subseteq R$. Therefore, we have proved that $I = R$.

Assume for the rest of this proof that $I$ contains no elements which satisfy the assumption in the previous paragraph. Thus, if $(a, b) \in I$, then either $a = 0$ or $b = 0$. Two such ideals are the principal ideals generated by $(1, 0)$ or by $(0, 1)$. Those ideals are the following

$$J = R(0, 1) = \{(0, b) \mid b \in \mathbb{R}\} \quad \text{and} \quad K = R(1, 0) = \{(a, 0) \mid a \in \mathbb{R}\}$$

As proved in class, principal ideals are ideals and so both $J$ and $K$ are ideals of the ring $R$. Our assumptions about $I$ is that $I \subseteq J \cup K$.

Assume that $I$ is not the trivial ideal. Then either $I$ contains a nonzero element of $J$ or a nonzero element of $K$. Suppose first that $I$ contains a nonzero element $(0, b)$ of $J$. Thus $b \neq 0$. This means that $b$ is a unit in $\mathbb{R}$ because $\mathbb{R}$ is a field. It follows that $I$ contains $(0, b^{-1})(0, b) = (0, 1)$. It then follows that $I$ contains the principal ideal $J$. Thus,
$J \subseteq I \subseteq J \cup K$. By a similar argument, if we assume that $I$ contains a nonzero element of $K$, then we must have $K \subseteq I \subseteq J \cup K$. It follows that either $J \subseteq I$ or that $K \subseteq I$.

Assume now that $I$ contains a nonzero element of $J$ and also a nonzero element of $K$. The remarks in the previous paragraph then show that both $J$ and $K$ are contained in $I$. Hence $J \cup K \subseteq I$. We also have $I \subseteq J \cup K$. Hence $I = J \cup K$. However, this leads to a contradiction because $J \cup K$ is not an ideal of $R$. To verify this, just note that both $(0, 1)$ and $(1, 0)$ are in $J \cup K$, but their sum is $(1, 1)$ which is not in $J \cup K$.

If $J \subseteq I$, then we must have $J = I$. For otherwise, $I$ would contain an element in $J \cup K$ which is not in $J$. It would then follow that $I$ contains a nonzero element of $K$ too. This is impossible. If $K \subseteq I$, then we must have $K = I$ for a similar reason. It follows that either $I = J$ or $I = K$.

To summarize, we have proved that the ring $R$ has exactly four ideals, namely the trivial ideal \{(0, 0)\}, the ring $R$ itself, and the ideals $J$ and $K$. 