Problem 1.

Proof. (a) Recall that \( \overline{a} \in \mathbb{Z}/n\mathbb{Z} \) if and only if \( n|a \) in \( \mathbb{Z} \). Thus \( \overline{ab} \) is nilpotent in \( \mathbb{Z}/n\mathbb{Z} \) if there exists \( m \in \mathbb{Z}^+ \) such that \( n|(ab)^m \). Since \( n = a^kb \), any \( m \geq k \) has this property, hence \( \overline{ab} \) is indeed nilpotent in \( \mathbb{Z}/n\mathbb{Z} \).

(b) From the fundamental theorem of arithmetic, we can write (uniquely) \( n = p_1^{a_1} \cdots p_k^{a_k} \) where \( p_k \) are distinct prime numbers. Let \( m = \max(a_1, \ldots, a_k) \). It is clear that \( n = p_1^{a_1} \cdots p_k^{a_k} \) divides \( (p_1 \cdots p_k)^m \), which in turn divides \( a^m \) if every \( p_i \) divides \( a \). As seen above \( n|a^m \) means precisely that \( \overline{a} \) is nilpotent. Conversely, assume \( n|a^m \). Assume \( p \) is a prime dividing \( n \). Then \( p|a^m \). By looking at the prime factorization of \( a \), we see that \( p \) has to divide \( a \).

Nilpotents of \( \mathbb{Z}/72\mathbb{Z} \) are \( \{0, 6, 12, 18, 30, 36, 42, 48, 54, 60, 66\} \).

(c) Assume that \( R \) contains a nonzero nilpotent element, call it \( f : X \rightarrow F \). By definition for some integer \( m > 0 \), \( f^m \) is the zero function on \( X \), i.e. \( f(x)^m = 0 \) for all \( x \in X \). Since \( F \) is a field, \( f(x)^m = 0 \) implies \( f(x) = 0 \) for all \( x \in X \), i.e. that \( f \) is, in fact, the zero function, contrary to our assumption.

\[ \square \]

Problem 2.

Proof. (a) Since \( x \) is nilpotent, by definition there is an integer \( m > 0 \) such that \( x^m = 0 \). Then \( x \cdot x^{m-1} = 0 \) so \( x \) is a zero-divisor (or zero).

(b) If \( x^m = 0 \), then \( (rx)^m = r^m x^m = r^m \cdot 0 = 0 \). Note that we used commutativity for the equality \( (rx)^m = r^m x^m \).

(c) If \( x^m = 0 \), then \( 1 = 1 + x^m = (1 + x)(1 - x + x^2 - x^3 + \cdots + x^{m-1}) \). The second parenthesis is an element of \( R \), and the inverse of \( 1 + x \), hence \( 1 + x \) is a unit.

(d) Let \( x \) be a nilpotent and \( u \) a unit with inverse \( u^{-1} \). We want to show that \( x + u \) is a unit. Indeed \( x + u = u(1 + u^{-1}x) \). By (b), \( u^{-1}x \) is nilpotent, and by (c), \( 1 + u^{-1}x \) is a unit. Thus \( x + u = u \cdot (1 + u^{-1}x) \) is the product of two units, hence a unit itself.

\[ \square \]

Problem 3.

Proof. \( \mathcal{O}_f \) contains the identity \( 1 = 1 + 0 \cdot f \omega \). Closure under addition is straightforward: \( (a + bf \omega) + (c + df \omega) = (a + c) + (b + d)f \omega \in \mathcal{O}_f \). Closure under multiplication is easy to verify as well: \( (a + bf \omega)(c + df \omega) = (ac + bdf^2D) + (ad + bc)f \omega \in \mathcal{O}_f \).

We show that \( 0, \omega, \ldots, (f - 1)\omega \) is a complete set of coset representatives for \( \mathcal{O}_f \) in \( \mathcal{O} \). Two such elements \( i\omega \neq j\omega \) represent distinct cosets because the difference is \( (i - j)\omega \), which is not of the form \( a + bf \omega \) because \( f \) does not divide \( i - j \) which is a nonzero integer satisfying \( -f < i - j < f \).

It is a complete set of representatives because given any \( \alpha = a + b\omega \in \mathcal{O} \), if we write \( b = qf + r \) with \( 0 \leq r < q \) (the usual division with remainder in \( \mathbb{Z} \)), then \( (a + b\omega) - r \cdot \omega = a + qf \omega \in \mathcal{O}_f \), so \( \alpha \) and \( r\omega \) represent the same coset.
Conversely, assume $A$ is a subring of $\mathcal{O}$ containing the identity and having finite index.

Note first that $A$ contains 1 some number of the form $b\omega$. Otherwise, the elements $\mathbb{Z}\omega$ yield infinitely many distinct cosets. Let $f'$ be the smallest, strictly positive, such number $b$. We claim that $f' = f$, i.e. $A = \mathcal{O}_{f'}$. Indeed, since $1, f'\omega \in A$, we have $\mathcal{O}_{f'} \subset A$. Moreover since $\mathcal{O}_{f'}$ has index $f'$ in $\mathcal{O}$, it follows that $[\mathcal{O} : A] \leq [\mathcal{O} : \mathcal{O}_{f'}]$, i.e. $f \leq f'$. On the other side, the elements $0, \omega, \ldots, (f' - 1)\omega$ yield distinct cosets, hence $f \geq f'$. Thus $f = f'$, as wanted. 

\textbf{Problem 4.}

\textit{Proof.} (a) Since $\phi$ is a nonzero homomorphism, $\phi(1_R) \neq 0_S$. Now, from $\phi(1_R) = \phi(1_R \cdot 1_R) = \phi(1_R) \cdot \phi(1_R)$, it follows that $\phi(1_R) \cdot (1 - \phi(1_R)) = 0$. Thus either $\phi(1_R) = 1_S$ or $\phi(1_R)$ is a zero-divisor. The only zero-divisor in an integral domain is zero. If $\phi$ is nonzero, by the above $\phi(1_R)$ is either $1_S$ or a non-zero divisor. Since the second case can’t happen, $\phi(1_R) = 1_S$, as wanted.

(b) Assume $\phi(1_R) = 1_S$ and let $u$ be a unit of $R$. Then $1_S = \phi(u \cdot u^{-1}) = \phi(u)\phi(u^{-1})$, hence $\phi(u)$ is invertible with inverse $\phi(u^{-1})$.

\textbf{Problem 5.}

\textit{Proof.} (a) Since $I$ and $J$ are subrings of $R$, they both contain 0, hence so does $I \cap J$. If $a, b \in I \cap J$, then $a + b, ab \in I$ and $a + b, ab \in J$, hence $a + b, ab \in I \cap J$. Thus $I \cap J$ is a subring of $R$. If $a \in I \cap J$ and $r \in R$, then $ra \in I$ and $ra \in J$ since $I$ and $J$ are ideals. Thus $ra \in I \cap J$. Similarly $ar \in I \cap J$. We have verified all the conditions in the definition of an ideal for $I \cap J$.

(b) Let now $(I_j)_{j \in J}$ be an arbitrary nonempty collection of ideals (indexed by $J$). Let $A = \cap_j I_j$. We want to show $A$ is an ideal. Each $I_j$ is a subring of $R$, hence contains 0. Thus so does $A$. If $a, b \in A$, then $a, b \in I_j$ for every $j \in J$. Since $I_j$ is closed under addition and multiplication, $a + b$ and $ab$ belong to $I_j$ for every $j$. Thus $a + b$ and $ab$ belong to $\cap_j I_j = A$. This shows that $A$ is a subring of $R$. Finally, let $a \in A$ and $r \in R$. Since $a \in I_j$ for every $I_j$ and $I_j$ is an ideal, we have that $ra$ and $ar$ are in $I_j$ for every $j$. Thus $ar$ and $ra$ belong to the intersection of all $I_j$’s, which is $A$. Thus $A$ satisfies all the conditions in the definition of an ideal.

\textbf{Problem 6.}

\textit{Proof.} (a) Let $I = \{x \in R \mid ax = 0\}$. Since $a \cdot 0 = 0$, we have $0 \in I$. If $x, y \in I$, then $a(x + y) = ax + ay = 0 + 0 = 0$, hence $x + y \in I$. Moreover, $a(xy) = (ax)y = 0 \cdot y = 0$, hence $xy \in I$. Thus $I$ is a subring of $R$. Let now $r \in R$ and $x \in I$. Then $a(xr) = (ax)r = 0 \cdot r = 0$, thus $rx \in I$. We have verified, for $I$, all the conditions of a right ideal. The proof for left ideals is almost identical.

(b) Let $I = \{x \in R \mid xa = 0 \text{ for all } a \in L\}$. Given $a \in L$, let $I_a = \{x \in R \mid xa = 0\}$. Then $I_a$ is the left annihilator of $a$ from part (a) and $I = \cap_{a \in L} I_a$. We have verified in Problem 18 that $\cap I_a$ is a left ideal. It remains to check that it is also a right ideal, i.e. that $x \in I$ and $r \in R$ imply $xr \in I$. 

\textbf{Problem 7.}
Indeed, $x \in I$ means, by definition, that $xa = 0$ for all $a \in L$. Since $L$ is a left ideal $rL \subset L$, i.e. $x(ra) = (xr)a = 0$ for all $a \in L$. This, by definition of $I$, implies $xr \in I$, hence $I$ is also a right ideal.

Remark: Note that we did not apply Problem 18 directly. It is not, in general, true that $I_a$ are both left and right ideals. Instead we have applied part of the proof in Problem 18 to conclude that $I = \bigcap_{a \in L} I_a$ is a left ideal and then proved that it is also a right ideal.