Problem 1:

Let p be a prime number, and G be an abelian group of order p^2.

Then G is isomorphic to a group of the form $\bigoplus_{i=1}^{n} \mathbb{Z}/p_i^{\alpha_i}$, for some p_i, α_i.

For that representation to make sense, $p_i = p$ or $p_i = p^2$ for all i, because G is a group of order p^2; if $p_i \not| p$ for any i, then the order of G would not be divisible by p. So $p_i \mid p$ for all i. Also, $p_i \leq p^2$ for all i, else the group has order bigger than p^2.

The only two ways to make that work are if $p_1 = p^2$ or if $p_1 = p_2 = p$, and this is clear.

So $\mathbb{Z}/p^2$ and $\mathbb{Z}/p \oplus \mathbb{Z}/p$ are the only two abelian groups of order p^2.

Note: Didn't we also have a homework problem that said that any group of order p^2 was abelian? You can throw out "abelian" in the problem and it works the same as long as you've given that problem previously, can't you?

Problem 2:

Note: For the sake of transparency, I am obliged to state that I found a chunk of this proof in Dummit and Foote.

Let R be a finite, nontrivial ring (the one ring is not a field nor an integral domain, so we can get away with this).

If R is an integral domain, then R is commutative. Also, R has no zero divisors. Thus, $R \setminus \{0_R\}$ is closed under multiplication.

Before continuing, we show that for all $a, b, c \in R$, $ab = ac$ implies that $a = 0$ or $b = c$;

If $ab = ac$, then $ab - ac = 0$, so $a(b - c) = 0$. This means that $a = 0$ or $b - c = 0$, so we have our result.

Now, $R \setminus \{0_R\}$ is a group with respect to multiplication:

First, note that multiplication is associative.

Next, note that $1_R \neq 0_R$, so $R \setminus \{0_R\}$ contains an identity element.

Last, each element has an inverse: let $a \in R \setminus \{0_R\}$. The map $\phi : R \setminus \{0\} \to R \setminus \{0\}$ given by $x \mapsto ax$ is injective, by the above cancellation law. Because $R \setminus \{0\}$ is finite, this means that ϕ is a bijection. In particular, $\phi(x) = 1$ for some $x \in R \setminus \{0\}$. In other words, $ax = 1$ for some $x \in R \setminus \{0\}$. Hence, a has a multiplicative inverse.

If R is a field, then R is commutative. Also, R is a division ring. So, $R \setminus \{0_R\} = R^*$ is a group (with the operation multiplication). That means that R has no zero divisors (otherwise, $R \setminus \{0_R\}$ wouldn't be closed under multiplication). So R is a commutative ring with no zero divisors, R is an integral domain.

Problem 3:

Let R be a ring and $S = M_n(R)$.

Part a:

Let $\phi : \mathcal{I} \to \mathcal{J}$ be given by $I \mapsto J = \{(a_{ij}) : a_{ij} \in I\}$. Then ϕ is a bijection:

First, ϕ is well defined: if I is an ideal, then $\phi(I) = \{(a_{ij}) : a_{ij} \in I\}$. Now, $\phi(I)$ is an ideal of S; if $M \in S$ and $N \in \phi(I)$, then each entry of MN (or NM) is a linear combination of elements of the form ma_{ij} with $m \in R$ and $a_{ij} \in I$. This means that each entry of MN (or NM) is in I, so that MN (and NM) is in $\phi(I)$. Also, if $M, N \in \phi(I)$, then each entry of $M + N$ is a sum of two elements in I, so that each entry of $M + N$ is an element of I, so that $M + N \in \phi(I)$.

Second, ϕ is injective: let I_1, I_2 be R-ideals, and $J = \phi(I_1) = \phi(I_2)$. For each $i \in I_1$, the matrix $\left[\begin{smallmatrix} i & 0 \\ 0 & 0 \end{smallmatrix}\right] \in J$. This implies that for each $i \in I_1$, $i \in I_2$. Similarly, for each $i \in I_2$ we have that $i \in \mathbb{I}_1$. So $I_1 = I_2$.

Last, ϕ is surjective: let J be an S-ideal.

Part b:

If R is a division ring then (0) and R are the only R-ideals; we discussed this in class. (Make sure we did).

So by the bijection above, there can only be two distinct S-ideals. We know that (0) and S are distinct S-ideals. This satisfies the problem.

Problem 4:

Let R be a ring, and I_1, I_2, $\ldots$ I_n be R-ideals.

Let $R = I_1 + I_2 \ldots + I_n$, with $I_j \cap \sum\limits_{i \neq j} I_i = (0)$ for all j.

First, we know that $1 \in I_1 + I_2 \ldots + I_n$. So, there are $e_1, e_2 \ldots e_n$ such that $1 = e_1 + e_2 \ldots + e_n$. Pick any such set of e_is.

Next, we show that $I_i = Re_i$:

First, let $r \in I_i$. Then $r = r1 = re_1 + re_2 \ldots re_i + \ldots + re_n$. But each re_k with $k \neq i$ is 0, because each is in I_i and I_k (we know this because we know that $I_i \cap \sum_{i \neq j} I_j = (0)$). So $r = re_i$, so $r \in Re_i$. So $I_i \subset Re_i$.

Next, let $r \in Re_i$. Then $r = r'e_i$ for some $r' \in R$. So $r \in I_i$. So $Re_i \subset I_i$.

So $Re_i = I_i$.

Next, $e_ie_j = 0$ if $i \neq j$; $e_ie_j \in I_i \cap I_j$, so $e_ie_j = 0$ (we know this because we know that $I_i \cap \sum_{i \neq j} I_j = (0)$).

Also, $e_i^2 = e_i$ for all i; $e_i = e_i1 = e_ie_1 + e_ie_2 \ldots e_ie_i + \ldots + e_ie_n = 0 + 0 + 0 \ldots + e_i^2 + \ldots + 0 = e_i^2$.

Last, $e_i \in Z(R)$ for all i; let $r \in R$. Then:

$$r1 = 1r$$
$$re_1 + re_2 + \ldots re_n = e_1r + e_2r + \ldots e_nr$$

This means that $re_i = e_ir$ for all i: if not, then there is an i such that there is a nonzero r' such that $re_i = e_ir + r'$. Moreover, because $Re_i = I_i$, this means that $r' \in I_i$. So, we have that

$$re_1 + re_2 + \ldots re_n - re_i = e_1r + e_2r + \ldots e_nr - re_i$$
$$re_1 + re_2 + \ldots re_{i-1} + re_{i+1} \ldots + re_n = -r' + e_1r + e_2r + \ldots e_{i-1}r + e_{i+1}r \ldots + e_nr$$
$$r' = e_1r + re_1 + e_2r + re_2 \ldots + e_{i-1}r + re_{i-1} + e_{i+1}r + re_{i+1} + \ldots e_nr + re_n$$
$$r' \in I_i \cap \sum_{i \neq j} I_j \text{ If I hadn't formatted it like that, the text would}$$

But this means that $r' = 0$. This is a contradiction.

Now, let there be $e_1, e_2 \ldots e_n$ such that $1 = e_1 + e_2 \ldots + e_n$ with $I_i = Re_i$, $e_i \in Z(R)$, $e_i^2 = e_i$, and $e_ie_j = 0$ for every $i \neq j$.

First, note that $Re_i = I_i$ for each i. Let $r \in R$. Because $1 = e_1 + e_2 \ldots + e_n$, we can take $r = re_1 + re_2 \ldots + re_n$ by multiplying on the left by r. But because $re_i \in I_i$ for each i, this means that $r \in I_1 + I_2 \ldots I_n$. Thus, we have $r \in I_1 + I_2 \ldots I_n$ for each $r \in R$: we have that $R = I_1 + I_2 \ldots + I_n$.

Next, let $r \in I_i \cup I_j$ for any $i \neq j$. Then $r = r'e_i = r''e_j$ for some $r', r'' \in R$. Also, $r'e_ie_i = r''e_je_i$, so $r = r'e_i = r''0 = 0$. That is, $r = 0$ for all $R \in I_i \cup I_j$ if $i \neq j$. So, $I_i \cup I_j = (0)$ for all $i \neq j$, so we have that $I_j \cup \sum_{i \neq j} I_i = (0)$ as well.

Thus, we have that $R = I_1 + I_2 \ldots + I_n$ with $I_j \cup \sum_{i \neq j} I_i = (0)$ if and only if there are $e_1, e_2 \ldots e_n$ such that $1 = e_1 + e_2 \ldots + e_n$ with $I_i = Re_i$, $e_i \in Z(R)$, $e_i^2 = e_i$, and $e_i e_j = 0$ for every $i \neq j$.