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:

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...(Definition) Now, $r^m = 1$ for some $m \in \mathbb{N}$;

Assume not. Then $r^m \neq 1$ for any $m \in \mathbb{N}$. So $r^m \neq r^k$ for any $k, m \in \mathbb{N}$ with $k \neq m$ (else, (apply definition)).

If R is a field, then...

Problem 3:

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

Part a:

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

First, ϕ is well defined:

Second, ϕ is injective:

Last, ϕ is surjective

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 $I_j \cap \sum_{i \neq j} I_i = (0)$ for all j. Then...

Now, let ther 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 $e_i e_j = 0$ for every $i \neq j$. Then...