**Problem 6.**

(1) Let \( I \) and \( J \) be ideals of a commutative ring \( R \) with \( I + J = R \). Prove that \( IJ = I \cap J \).

(2) Let \( I, J, \) and \( K \) be ideals of a principal ideal domain. Prove that \( I \cap (J + K) = I \cap J + I \cap K \).

**Solution**

For (1) pick \( a \in I \) and \( b \in J \) so that \( a + b = 1 \). To see that \( I \cap J \subseteq IJ \) let \( d \) be any element of \( I \cap J \). Then \( d = d \cdot 1 = d(a + b) = da + db = ad + db \) where the last equality holds by commutativity. Since \( a \in I \) and \( d \in J \) we see that \( ad \in IJ \), while since \( d \in I \) and \( b \in J \) we see that \( db \in IJ \). So \( d = ad + db \in IJ \). Thus, \( I \cap J \subseteq IJ \). But \( IJ \subseteq I \) since \( I \) is closed with respect to the multiplication on the right by any element of \( R \) (much less those in \( J \)). Likewise \( IJ \subseteq J \). So \( IJ \subseteq I \cap J \), giving the opposite inclusion.

For Part (2), it pays to think about this equality in lattices more generally. Lattices are just partially ordered sets in which any elements \( x \) and \( y \) have both a least upper bound (denoted by \( x \lor y \)) and greatest lower bound (denoted by \( x \land y \)). Rendered in this notation the equality we are interested in becomes

\[
x \land (y \lor z) = (x \land y) \lor (x \land z).
\]

Consider the case of a linearly ordered set, like the real numbers. Here \( x \land y = \min(x, y) \) and \( x \lor y = \max(x, y) \). The equality above holds in linearly ordered sets for the following reason. The elements \( y \) and \( z \) are comparable, and in view of the symmetry of the roles of \( y \) and \( z \) in the equality, it does no harm to suppose that \( y \leq z \). Then \( y \lor z = z \) and the equality becomes obvious. Turning a lattice upside down interchanges the notion of least upper bound with the notion of greatest lower bound. Since the upside down version of a linearly ordered set is also linearly ordered we see that a linearly ordered set also makes the following equality true.

\[
x \lor (y \land z) = (x \lor y) \land (x \lor z).
\]

While it might not be so clear, this holds more generally: a lattice that satisfies one distributive law must also satisfy the other.

Returning to our ideals in the principal ideal domain, pick elements \( a, b, \) and \( c \) so that \( I = (a), J = (b), \) and \( K = (c) \). Since our domain is a unique factorization domain, we pick primes \( p_0, p_1, \ldots, p_{n-1} \) so that each of \( a, b, \) and \( c \) can be written, to within unit multipliers as a product of these primes. This means we can pick natural numbers \( k_0\ell_0, m_0, k_1, \ell_1, m_1, \ldots, k_{n-1}, \ell_{n-1}, m_{n-1} \) and units \( u, v \) and \( w \) so that

\[
a = up_0^{k_0}p_1^{k_1} \cdots p_{n-1}^{k_{n-1}}
\]

\[
b = vp_0^{\ell_0}p_1^{\ell_1} \cdots p_{n-1}^{\ell_{n-1}}
\]

\[
c = wp_0^{m_0}p_1^{m_1} \cdots p_{n-1}^{m_{n-1}}
\]

Now \( J + K = (d) \) where \( d \) is any greatest common divisor of \( b \) and \( c \). This means we can take

\[
d = p_0^{\min(\ell_0,m_0)}p_1^{\min(\ell_1,m_1)} \cdots p_{n-1}^{\min(\ell_{n-1},m_{n-1})}
\]
So we are done. But we saw at the start that this distributive law holds in linearly ordered sets, like the natural numbers.

Likewise (multiple of a notation, we see

So the whole right side becomes (q) + (r) = (s) where s is any greatest common divisor of q and r. We put

Our problem will be finished if we can show that e and s are associates. This amounts to showing for each i < n that

This equality concerns natural numbers, which are linearly ordered. So rendering this equation in lattice notation, we see

But we saw at the start that this distributive law holds in linearly ordered sets, like the natural numbers. So we are done.

**Problem 7.**

Let R be a commutative ring and I be a proper prime ideal of R such that R/I satisfies the descending chain condition on ideals. Prove that R/I is a field.

**Solution**

Let S = R/I. Then S is a nontrivial integral domain with the descending chain condition. Our problem is to show that it is a field. So let a ∈ S be any nonzero element. Consider the elements a, a^2, a^3, . . . . If we look at the ideals generated by these elements we see the descending chain (a) ⊇ (a^2) ⊇ (a^3) ⊇ . . . and conclude that it must be finite. So pick n large enough so that (a^n) = (a^{n+1}). This entails that a^n = a^{n+1}b for some b. But since a ≠ 0 and S is an integral domain, then a^n ≠ 0 and we can cancel it, leaving 1 = ab. This means that a is invertible, and so S is a field.

For a counterexample to the problem without the added stipulation of primeness, take R to be the ring of integers and let I = (6). Then R/I = Z_6 which is a finite ring (and hence has the descending chain condition) which is not even an integral domain (much less a field).

**Problem 8.**

Let R be a commutative ring and I be an ideal which is contained in a prime ideal P. Prove that the collection of prime ideals contained in P and containing I has a minimal member.
Solution
Let us try using the upside down version of Zorn’s Lemma. So let \( \mathcal{F} = \{ J \mid I \subseteq J \subseteq P \text{ and } J \text{ is a prime ideal} \} \).

Notice that \( P \in \mathcal{F} \). Let \( \mathcal{C} \) be a chain in \( \mathcal{F} \). We need to argue that \( \mathcal{C} \) has a lower bound in \( \mathcal{F} \). First let’s take care of the case when \( \mathcal{C} \) is empty. In this case \( P \) will be a lower bound. Now suppose \( \mathcal{C} \) is not empty. We argue that \( \bigcap \mathcal{C} \) is the desired lower bound. The definition of intersection gives us \( I \subseteq \bigcap \mathcal{C} \subseteq J \subseteq P \) for all \( J \in \mathcal{C} \). So the only thing that remains is to show that \( \bigcap \mathcal{C} \in \mathcal{F} \)—that is that \( \bigcap \mathcal{C} \) is a prime ideal containing \( I \) and contained in \( P \). Everything is clear except that \( \bigcap \mathcal{C} \) is prime. (Recall that the intersection of any nonempty collection of ideals is always an ideal.) To see the primeness, let \( ab \in \bigcap \mathcal{C} \).

For contradiction, suppose that \( a \in \bigcap \mathcal{C} \) and \( b \in \bigcap \mathcal{C} \). Since \( \bigcap \mathcal{C} \) is a chain, we can suppose without loss of generality, that \( J_a \subseteq J_b \). Therefore we also get that \( b \notin J_a \). On the other hand, \( ab \in J_a \) since it belongs to every member of \( \mathcal{C} \). This means we have contradicted the primeness of \( J_a \). So we conclude that the hypotheses for the minimal-element version of Zorn’s Lemma hold. Thus \( \mathcal{F} \) must have a minimal element, as desired.

Problem 9.
Let \( X \) be a finite set and let \( \mathbb{R} \) be the ring of functions from \( X \) into the field \( \mathbb{R} \) of real numbers. Prove that an ideal \( M \) of \( \mathbb{R} \) is maximal if and only if there is an element \( a \in X \) such that
\[
M = \{ f \mid f \in \mathbb{R} \text{ and } f(a) = 0 \}.
\]

Solution
First, suppose that \( a \in X \) and that \( M = \{ f \mid f \in \mathbb{R} \text{ and } f(a) = 0 \} \). Upon immediate reflection, we see that \( M \) is an proper ideal of \( \mathbb{R} \). Let \( J \) be an ideal of \( \mathbb{R} \) so that \( M \subseteq J \) with \( M \neq J \). Pick \( g \in J \) so that \( g \notin M \). Let \( X = \{x_0, \ldots, x_{n-1}\} \) and suppose \( a = x_0 \). Observe that \( g(x_0) \neq 0 \). For each \( i < n \) with \( 0 < i \) we define
\[
f_i(x_j) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}
\]
So \( f_1, f_2, \ldots, f_{n-1} \in M \subseteq J \). We also define
\[
h(x) = \begin{cases} 0 & \text{if } x \neq x_0 \\ \frac{1}{g(x_0)} & \text{otherwise.} \end{cases}
\]
Now notice that
\[
h(x)g(x) + f_1(x) + f_2(x) + \cdots + f_{n-1}(x) \in J.
\]
But this function is constantly 1. This means that \( J = \mathbb{R} \) and so \( M \) is a maximal proper ideal.

For the converse, suppose that \( I \) is an ideal of \( \mathbb{R} \) but that for each \( i < n \) there is \( f_i(x) \in M \) with \( f_i(x_i) \neq 0 \). Define \( g_i(x) \) via
\[
g_i(x_j) = \begin{cases} \frac{1}{f_i(x_i)} & \text{if } i = j \\ 0 & \text{otherwise.} \end{cases}
\]
So \( g_i(x)f_i(x) \in I \) for all \( i < n \). But then
\[
g_0(x)f_0(x) + \cdots + g_{n-1}(x)f_{n-1}(x) \in I.
\]
But this function is constantly 1. So the ideal \( I \) is not proper. This means that for an ideal \( M \) which is maximal among proper ideals there must be \( a \in \{x_0, x_1, \ldots, x_{n-1}\} \) so that \( f(a) = 0 \) for all \( f(x) \in M \).
Hence $M \subseteq \{ f(x) \mid f(a) = 0 \text{ and } f(x) \in R \}$. As this last set was already shown to be a maximal ideal, it must be that $M = \{ f(x) \mid f(a) = 0 \text{ and } f(x) \in R \}$.

**Problem 10.**
Let $R$ be a commutative ring and let $n$ be a positive integer. Let $I_0, I_1, \ldots, I_{n-1}$ be ideals of $R$ so that $I_k$ is a prime ideal for every $k < n$ and so that $J \subseteq I_0 \cup \cdots \cup I_{n-1}$. Prove that $J \subseteq I_k$ for some $k < n$.

**Solution**
We proceed by induction on $n$. The base step, when $n = 1$ is evident. For the induction step, we can suppose that $J$ is not included in the union of fewer than all $n$ of the $I_k$’s, for otherwise we can appeal to the induction hypothesis. We must reject this supposition. So for each $i < n$ we pick $a_i \in J \cap I_i$ so that $a_i \notin I_j$ for any $j \neq i$. The element $a_0 + a_1 a_2 \ldots a_{n-1}$ certainly belongs to $J$ since $J$ is an ideal. Therefore pick $k < n$ so that $a_0 + a_1 \ldots a_{n-1} \in I_k$. There are two cases, both of which we can reject. The first case is that $k = 0$. Then we have both $a_0$ and $a_0 + a_1 \ldots a_{n-1}$ in $I_0$. This entails that $a_1 \ldots a_{n-1} \in I_0$. Now $I_0$ is a prime ideal so there must be $j$ with $1 \leq j < n$ and $a_j \in I_0$. But this contradicts the choice of $a_j$. The second case is that $k > 0$. Then both $a_0 + a_1 \ldots a_{n-1}$ and $a_1 \ldots a_{n-1}$ belong the $I_k$, the latter membership follows since $I_k$ is an ideal and $a_1 \ldots a_{n-1}$ is a multiple of $a_k$. In consequence $a_0 \in I_k$, contradicting the choice of $a_0$.

**Problem 11.**
Let $R$ be a nontrivial commutative ring and let $J$ be the intersection of all the maximal proper ideals of $R$. Prove that $1 + a$ is a unit of $R$ for all $a \in J$.

**Solution**
Suppose that $a$ belongs to all the proper maximal ideals. Were $1 + a$ not a unit, then $(1 + a)$ would be a proper ideal. By the Maximal Ideal Theorem there would be a maximal proper ideal $M$ so that $1 + a \in M$. But also $a \in M$ since it is in every maximal proper ideal. This would force $1 \in M$ and we would have the contradiction that $M$ is not a proper ideal.

**Problem 12.**
Let $F$ be a field and let $p(x) \in F[x]$ be a polynomial of degree $n$. Prove that $p(x)$ has at most $n$ distinct roots in $F$. 

4
**Solution**

Suppose \( r \) is a root of \( p(x) \). We know that \((x - r)\) is a factor of \( p(x) \). So pick \( q(x) \in \mathbb{F}[x] \) such that \( p(x) = (x - r)q(x) \). Now let \( s \) be a root of \( p(x) \) distinct from \( r \). Now both \( x - r \) and \( x - s \) are prime and \( x - s \mid (x - r)q(x) \). We see \( x - s \) cannot divide \( x - r \) since \( r \neq s \). So \( x - s \) divides \( q(x) \). So we can pick \( t(x) \in \mathbb{F}[x] \) with \( p(x) = (x - r)(x - s)t(x) \). Continuing in this way, we see that if \( r_0, r_1, \ldots, r_{m-1} \) are distinct roots of \( p(x) \) then there is a polynomial \( u(x) \in \mathbb{F}[x] \) such that \( p(x) = (x - r_0)(x - r_1)\cdots(x - r_{m-1})u(x) \). So \( m \) can be no bigger than the degree of \( p(x) \).

**Problem 13.**

Let \( \mathbb{F} \) be a field and let \( \mathbb{F}^* \) be its (multiplicative) group of nonzero elements. Let \( G \) be any finite subgroup of \( \mathbb{F}^* \). Prove that \( G \) must be cyclic.

**Solution**

Our group \( G \) is a finite Abelian group, so it factors into a direct product of cyclic groups of prime power order. In the case that each of these direct factors is associated with a different prime, we see that \( G \) is cyclic (by taking the product of the generators of each factor. So let us suppose this is not the case. Then there is a prime \( p \) and two subgroups \( H \) and \( K \) of \( \mathbb{F}^* \) such that \(|H| = p^n, |K| = p^m\), where \( n \) and \( m \) are positive integers, and \( H \cap K \) is trivial. We invoke Cauchy to have \( n = m = 1 \). This means that there are at least \( 2p - 1 \) elements of order \( p \) in \( \mathbb{F}^* \). These elements would all have to be roots of \( x^p - 1 \). On the other hand, this polynomial can have at most \( p \) roots in \( \mathbb{F} \).

**Problem 14.**

Suppose that \( \mathbb{D} \) is a commutative ring such that \( \mathbb{D}[x] \) is a principal ideal domain. Prove that \( \mathbb{D} \) is a field.

**Solution**

The polynomial \( x \in \mathbb{D}[x] \) is irreducible and hence prime. This means that the ideal \((x)\) generated by \( x \) is a prime ideal. In a principal ideal domain, every prime ideal in maximal. Hence \( \mathbb{D}[x]/(x) \) is a field. So we need to see that \( \mathbb{D} \cong \mathbb{D}[x]/(x) \). Let \( h \) be the (unique) homomorphism from \( \mathbb{D}[x] \) into \( \mathbb{D} \) that fixes each element of \( \mathbb{D} \) (that is \( h(d) = d \) for all \( d \in \mathbb{D} \) and sends \( x \) to \( 0 \). So \( h \) maps \( \mathbb{D}[x] \) onto \( \mathbb{D} \). Since \( h(d_0 + d_1x + \cdots + d_nx^n) = d_0 \) for any polynomial \( d_0 + d_1x + \cdots + d_nx^n \), we see that \( d_0 + d_1x + \cdots + d_nx^n \in \ker h \) iff \( d_0 = 0 \) iff \( d_0 + d_1x + \cdots + d_nx^n \in (x) \). So \((x) = \ker h \). By the Homomorphism Theorem, we see that \( \mathbb{D}[x]/(x) \cong \mathbb{D} \). So \( \mathbb{D} \) is a field.

**Here is a second solution:**

We only need to see that every nonzero element of \( \mathbb{D} \) has a multiplicative inverse. So let \( d \in \mathbb{D} \) with \( d \neq 0 \). Now the ideal \((d, x)\) of \( \mathbb{D}[x] \) generated by \( \{d, x\} \) is principal. Say it is generated by the polynomial \( f(x) \). Then \( d = f(x)g(x) \) for some polynomial \( g(x) \). This entails that the degree of \( f(x) \) is \( 0 \). Say \( f(x) = a \). Now there must also be a polynomial \( h(x) \) so that \( x = f(x)h(x) = ah(x) \). So evidently \( h(x) = cx \) and \( ac = 1 \). This means that \( a \) is a unit. Because \( \mathbb{D}[x] \) is a principal ideal domain, there must be polynomials \( u(x) \) and \( w(x) \) such that \( a = du(x) + xw(x) \). Let \( b \) be the constant term of \( u(x) \). It must turn out that \( a = db \). So we find that \( a \) and \( d \) are associates. So \( d \) must also be a unit. This means \( d \) is invertible, as desired.
**Problem 15.**
Is the polynomial $y^3 - x^2y^2 + x^3y + x + x^4$ irreducible in $\mathbb{Z}[x, y]$?

**Solution**

Construe $y^3 - x^2y^2 + x^3y + x + x^4$ as a polynomial (in $y$) with coefficients from $\mathbb{Z}[x]$. Thus the coefficients of this polynomial are $1, -x^2, x^3, x^4 + x$. Since these coefficients have no common irreducible factor (in $\mathbb{Z}[x]$) our polynomial is primitive. Now $x \in \mathbb{Z}[x]$ is irreducible and $x \nmid 1, x \mid -x^2, x \mid x^3, x \mid x^4 + x$, and $x^2 \nmid x^4 + x = (x^4 + 1)x$.

This means that Eisenstein Criterion applies, and our polynomial is irreducible.

**Problem 16.**
Let $R$ be a principal ideal domain, and let $I$ and $J$ be ideals of $R$. $IJ$ denotes the ideal of $R$ generated by the set of all elements of the form $ab$ where $a \in I$ and $b \in J$. Prove that if $I + J = R$, then $I \cap J = IJ$.

**Solution**
In any case, $IJ \subseteq I$ and $IJ \subseteq J$ since $I$ and $J$ are ideals. This means that $IJ \subseteq I \cap J$. We need to work for the reverse inclusion.

Let $I = (a)$ and $J = (b)$. In a principal ideal domain we see that $(d) = (a) \cap (b)$ means the same thing as $d$ is a least common multiple of $a$ and $b$.

On the other hand, $ra$ and $sb$ are arbitrary elements of $I$ and $J$ and $(ra)(sb) = (rs)(ab)$. So the product of an element of $I$ with an element of $J$ turns a multiple of $ab$. From this it is easy to see that $IJ = (ab)$. So we would be done, if we could prove that $ab$ is a least common multiple of $a$ and $b$. This is where the hypothesis $I + J = R$ comes in. We could restate this as $(a) + (b) = (1)$. Another way to say it is that $a$ and $b$ are relatively prime. For $a$ and $b$ have no common prime factors. For any prime $p$ the number of times it occurs as a factor in $d$ must be the sum of the number of times it occurs in $a$ and the number of times it occurs in $b$. So $d$ and $ab$ must be associates.

**Problem 17.**
Let $D$ be a unique factorization domain and let $I$ be a nonzero prime ideal of $D[x]$ which is minimal among all the nonzero prime ideals of $D[x]$. Prove that $I$ is a principal ideal.

**Solution**

We know that $D[x]$ is also a unique factorization domain. First pick a polynomial $p(x) \in I$ with $p(x) \neq 0$. Next factor $p(x)$ into primes. Because $I$ is a prime ideal, at least one of the prime factors of $p(x)$ must be in $I$. So it does no harm to suppose $p(x)$ is prime to begin with. Let $J$ be the ideal generated by $p(x)$. Because $p(x)$ is prime $J$ is a prime ideal. But $J \subseteq I$ and $I$ is minimal among nonzero prime ideals. So $J = I$. Since $J$ is principal, so is $I$. 
Problem 18.

a. Prove that \((2, x)\) is not a principal ideal of \(\mathbb{Z}[x]\).

b. Prove that \((3)\) is a prime ideal of \(\mathbb{Z}[x]\) that is not a maximal ideal of \(\mathbb{Z}[x]\).

Solution

For part (a) suppose otherwise. Pick \(f(x) \in (2, x)\) so that \(f(x)\) generates \((2, x)\). It is routine to check (and hard working grad students do it) that

\[
(2, x) = \{g(x) \mid g(x) \in \mathbb{Z}[x] \text{ and the constant term of } g(x) \text{ is even}\}.
\]

So we know that \(f(x)\) has an even constant term and that \(f(x)\mid 2\) and \(f(x)\mid x\) since both 2 and \(x\) must be multiples of \(f(x)\). Because \(f(x)\mid 2\) we see that \(f(x)\) must be one of 1, \(-1\), 2, or \(-2\). Since neither 1 nor \(-1\) is even we see that \(f(x)\) must be either 2 or \(-2\). But neither of these divides \(x\). So we have the desired contradiction.

For part (b) we first argue that \((3)\) is a prime ideal. Plainly

\[
(3) = \{f(x) \mid f(x) \in \mathbb{Z}[x] \text{ and all the coefficients of } f(x) \text{ are multiples of } 3\}.
\]

Suppose \(g(x)h(x) \in (3)\) and \(g(x) \notin (3)\). Let \(g(x) = b_0 + b_1x + \cdots + b_nx^n\) and \(h(x) = c_0 + c_1x + \cdots + c_mx^m\). We have to show that \(3 \mid c_j\) for all \(j\). Let \(k\) be as small as possible so that \(3 \nmid b_k\). Observe that the \(k\)th coefficient of \(g(x)h(x)\) is

\[
\sum_{i+j=k} b_ic_j = b_0c_j + b_1c_{j-1} + \cdots + b_{k-1}c_1 + b_kc_0.
\]

Now 3 this sum and it also divides the first \(k\) terms of the sum. Therefore it divides the last term as well. Since 3 is prime and \(3 \nmid b_k\), we conclude that \(3 \mid c_0\). We can continue in this way to see that \(3 \mid c_j\) for all \(j\). I’ll do one more step and leave it to you to reorganize the proof into a real proof by induction on \(j\). The \(k+1\)st coefficient of \(g(x)h(x)\) is

\[
\sum_{i+j=k+1} b_ic_j = b_0c_{k+1} + \cdots + b_kc_1 + b_{k+1}c_0.
\]

This time it is clear that 3 divides all the terms (the problem term is \(b_kc_1\) this time). Since \(3 \mid b_kc_1\) and since \(3 \nmid b_k\) we find that \(3 \mid c_1\). So after some more moves like this we find that \(3 \mid c_j\) for all \(j\). So \(h(x) \in (3)\) as desired. We conclude that \((3)\) is a prime ideal of \(\mathbb{Z}[x]\).

Finally, we have to argue that \((3)\) is not a maximal ideal. Consider the ideal \((3, x)\). It is clearly an ideal which is properly larger than \((3)\) and on the other hand it consists of all those polynomials with constant terms divisible by 3. Since this is not the whole ring \(\mathbb{Z}[x]\) we find that \((3)\) is a prime ideal which fails to be maximal.

Problem 19.

Show that any integral domain satisfying the descending chain condition on ideals is a field.
Solution
Let $D$ be an integral domain satisfying the descending chain condition. Let $0 \neq a \in D$. For each natural number $n$ let $I_n = (a^n)$. Then $D = I_0 \supsetneq (a) = I_1 \supsetneq (a^2) \supsetneq \ldots$ is a descending chain of ideals. By the descending chain condition, there is $m$ such that
\[ I_m = I_{m+1} = I_{m+2} = \ldots \]
This means, in particular that $a^m \in (a^{m+1})$. So there is $r \in D$ so that $a^m = ra^{m+1}$. But then $a^m \cdot 1 = a^m(ra)$. Since we are in an integral domain and $a \neq 0$, we see that $a^m \neq 0$. But in integral domains the cancellation law holds. So we get that $1 = ra$. This means that $r$ is a multiplicative inverse of $a$. Therefore, every nonzero element of $D$ has a multiplicative inverse. Hence $D$ is a field.

Problem 20.
Prove the following form of the Chinese Remainder Theorem: Let $R$ be a commutative ring with unit 1 and suppose that $I$ and $J$ are ideals of $R$ such that $I + J = R$. Then
\[ \frac{R}{I \cap J} \cong \frac{R}{I} \times \frac{R}{J}. \]

Solution
Define the map $\Phi : R \rightarrow R/I \times R/J$ via $\Phi(r) = (r/I, r/J)$ for all $r \in R$. The hardworking graduate student will carry out the details to prove that $\Phi$ is a homomorphism.

I contend that the kernel of $\Phi$ is $I \cup J$. Here is why:
\[ r \in \ker \Phi \iff \Phi(r) = (0/I, 0/J) \]
\[ \iff (r/I, r/J) = (0/I, 0/J) \]
\[ \iff r/I = 0/I \text{ and } r/J = 0/J \]
\[ \iff r \in I \text{ and } r \in J \]
\[ \iff r \in I \cap J \]

Now the idea is to apply the Homomorphism Theorem to obtain the desired isomorphism. But it remains to argue that $\Phi$ maps $R$ onto $R/I \times R/J$. To this end, pick $a, b \in R$ obtaining $(a/I, b/J)$, which is an arbitrary element of $R/I \times R/J$. To complete the solution to this problem, we must find $r \in R$ so that $r/I = a/I$ and $r/J = b/J$. Another way to phrase this is that we must find $r$ so that $r - a \in I$ and $r - b \in J$. Yet a third way is that we must find $r$ so that
\[ r \equiv a \pmod{I} \]
\[ r \equiv b \pmod{J} \]
Because $R = I + J$ we can pick $a_0, b_0 \in I$ and $a_1, b_1 \in J$ so that $a = a_0 + a_1$ and $b = b_0 + b_1$. Here is our value: $r = a_1 + b_0$. Then
\[ r - a = a_1 + b_0 - a_0 - a_1 = b_0 - a_0 \in I \]
\[ r - b = a_1 + b_0 - b_0 - b_1 = a_1 - b_1 \in J \]
In this way we have found the desired $r$ and established that $\Phi$ maps $R$ onto $R/I \times R/J$ with $\ker \Phi = I \cap J$. An appeal to the Homomorphism Theorem completes this solution.
PROBLEM 21.
Let $D$ be an integral domain and let $c_0, \ldots, c_{n-1}$ be $n$ distinct elements of $D$. Further let $d_0, \ldots, d_{n-1}$ be arbitrary elements of $D$. Prove there is at most one polynomial $f(x) \in D[x]$ of degree $n$ such that $f(c_i) = d_i$ for all $i < n$.

PROBLEM 22.
Let $F$ be a field and let $c_0, \ldots, c_{n-1}$ be $n$ distinct elements of $F$. Further let $d_0, \ldots, d_{n-1}$ be arbitrary elements of $F$. Prove there is at least one polynomial $f(x) \in D[x]$ of degree $n$ such that $f(c_i) = d_i$ for all $i < n$.

PROBLEM 23.
Let $R$ be the following subring of the field of rational functions in 3 variables with complex coefficients:

\[ R = \left\{ \frac{f}{g} : f, g \in \mathbb{C}[x, y, z] \text{ and } g(1, 2, 3) \neq 0 \right\} \]

Find 3 prime ideals $P_1, P_2, \text{ and } P_3$ in $R$ with

\[ 0 \subsetneq P_1 \subsetneq P_2 \subsetneq P_3 \subsetneq R. \]
Problem 24.
Let $A$ be the $4 \times 4$ real matrix

$$A = \begin{pmatrix}
1 & 1 & 0 & 0 \\
-1 & -1 & 0 & 0 \\
-2 & -2 & 2 & 1 \\
1 & 1 & -1 & 0
\end{pmatrix}$$

(a) Determine the rational canonical form of $A$.
(b) Determine the Jordan canonical form of $A$.

Problem 25.
Suppose that $N$ is a $4 \times 4$ nilpotent matrix over a field $F$ with minimal polynomial $x^2$. What are the possible rational canonical forms for $N$?