Here are some Lemmas which are referenced throughout the problems.

Lemma 1 (Sum of Ideals is an Ideal). *If I,J are ideals of a ring R, then $I+J=\{i+j \mid i\in I, j\in J\}$ is also an ideal of R.*

Proof. $\forall (i_1+j_1),(i_2+j_2)\in I+J$, $(i_1+j_1)-(i_2+j_2)=(i_1-i_2)+(j_1-j_2)\in I+J \implies I+J\leq_+ R$. Next for all $r\in R$ and all $(i+j)\in I+J$, $r(i+j)=ri+rj, (i+j)r=ir+jr\in I+J$ since $ir, ri\in I$ and $rj, jr\in J$. Thus,

$$\text{If } I,J \text{ are ideals of } R\text{, then } I+J \text{ is an ideal of } R.$$

□

Lemma 2 (Inclusion Mapping is Ring Embedding). *If $S\subseteq R$ is a subring of a ring R, then the inclusion mapping $\iota : S\hookrightarrow R$ defined via $\iota(s)=s$ is a ring embedding (an injective ring homomorphism).*

Proof. For all $a,b\in S$,

$$\begin{aligned}
&\iota(a+b)=a+b=\iota(a)+\iota(b)\\
&\iota(ab)=ab=\iota(a)\iota(b)\\
&\iota(1_S)=1_S=1_R\\
&\iota(a)=\iota(b)\implies a=b \text{ by definition.}
\end{aligned}$$

□

Lemma 3 (Evaluation Mapping to coefficient ring is a Surjective Ring Homomorphism). *The evaluation homomorphism $\varepsilon_a : R[x]\to R$ defined by $\varepsilon_a(f(x))=f(a)$ is a surjective ring homomorphism for any $a\in R$.*

Proof. For all $f(x),g(x)\in R[x]$,

$$\begin{aligned}
&\varepsilon_a(f(x)+g(x))=f(a)+g(a)=\varepsilon_a(f(x))+\varepsilon_a(g(x))\\
&\varepsilon_a(f(x)g(x))=f(a)g(a)=\varepsilon_a(f(x))\varepsilon_a(g(x))\\
&\varepsilon_a(1_{R[x]})=1_R\\
&\text{For any } r\in R,\ \varepsilon_a(r)=r \text{ so } \varepsilon_a \text{ is surjective.}
\end{aligned}$$

□

Lemma 4 (Telescoping Identity). *For any $k\in\mathbb{N}$ and any polynomial x^k-y^k over a commutative ring R where x,y may either be indeterminates or elements of R, we have that:*

$$x^k-y^k=(x-y)\sum_{\substack{i+j=k-1\\ i,j\in\mathbb{N}}} x^i y^j.$$

Proof.

$$
\begin{aligned}
x\sum_{\substack{i+j=k-1\\ i,j\in\mathbb{N}}} x^iy^j &= x(x^{k-1}+x^{k-2}y+\cdots+xy^{k-2}+y^{k-1}) = x^k+(x^{k-1}y+\cdots+x^2y^{k-2}+xy^{k-1})\\
y\sum_{\substack{i+j=k-1\\ i,j\in\mathbb{N}}} x^iy^j &= y(x^{k-1}+x^{k-2}y+\cdots+xy^{k-2}+y^{k-1}) = (yx^{k-1}+x^{k-2}y^2+\cdots xy^{k-1})+y^k\\
&= (x^{k-1}y+x^{k-2}y^2+\cdots+xy^{k-1})+y^k\\
\implies (x-y)\sum_{\substack{i+j=k-1\\ i,j\in\mathbb{N}}} x^iy^j &= x^k+(x^{k-1}y+\cdots+x^2y^{k-2}+xy^{k-1})-(x^{k-1}y+x^{k-2}y^2+\cdots+xy^{k-1})-y^k\\
&= x^k-y^k.
\end{aligned}
$$

□

Lemma 5 (Polynomials over fields have division algorithm)**.** *If $\mathbb{K}$ is a field, then for all $f(x), g(x) \in \mathbb{K}[x]$, where $g(x)$ is non-zero there exists $q(x), r(x) \in \mathbb{K}[x]$ such that either $r(x) = 0$ or $\deg(r(x)) < \deg(g(x))$ and then $f(x) = q(x)g(x) + r(x)$.*

Proof. Let $f(x) = \sum_{i=1}^{n} a_i x^i, g(x) = \sum_{j=1}^{m} b_j x^j \in \mathbb{K}[x]$ have degrees m, n, respectively, such that $g(x)$ is non-zero. Since $\mathbb{K}$ is a field, all non-zero coefficients are units. Note that leading terms must be non-zero.

If $f(x) = 0$, then $f(x) = 0 = 0g(x) + 0$ and so we have $q(x) = 0, r(x) = 0$ such that $f(x) = q(x)g(x) + r(x)$, which satisifies the statement. If $\deg(f(x)) = n < m = \deg(g(x))$, then set $q(x) = 0, r(x) = f(x)$, and then $f(x) = q(x)g(x) + r(x) = 0(g(x)) + f(x)$ satisfies the statement since $\deg(r(x)) = \deg(f(x)) < \deg(g(x))$.

Lastly, if $\deg(f(x)) = n \geq m = \deg(g(x))$, set $t(x) = a_n b_m^{-1} x^{n-m}$. Then we have that the leading term of $t(x)g(x)$ is $(a_n b_m^{-1} x^{n-m})(b_m x^m) = a_n x^n$, which is leading term of $f(x)$.

Now set $f_1(x) = f(x) - t(x)g(x)$. Then the n-coefficient will vanish; $[x^n](f(x) - t(x)g(x)) = [x^n]f(x) - [x^n]t(x)g(x) = a_n - a_n = 0$ and so $\deg(f_1(x)) < \deg(f(x)) = n$. If $\deg(f_1(x)) < m = \deg(g(x))$ then we have $f(x) = t(x)g(x) + f_1(x)$, which satisfies the statement.

Otherwise if $\deg(f_1(x)) < m = \deg(g(x))$, we repeat the process. For each step $i \geq 1$, let $d_i = \deg(f_i(x))$ set $t_i(x) = ([x^{d_i}]f_i(x))(b_m^{-1})\, x^{m-d_i}$. Now set $f_{i+1}(x) = f_i(x) - t_i(x)g(x)$. Then

$$[x^{d_i}]f_{i+1}(x) = ([x^{d_i}]f_i(x)) - ([x^{d_i}]f_i(x))b_m^{-1} = 0 \text{ and } f_i(x) = t_i(x)g(x) + f_{i+1}$$

So we see that by recursion, at each step $i \mapsto i+1$, $\deg(f_{i+1}(x)) < \deg(f_i(x))$. Suppose our process terminates at some $i = k$ such that $f_k(x)$ has degree $\mu \geq m$. That is $f_{k+1}(x)$ is not an acceptable polynomial in $\mathbb{K}[x]$; it has negative powers of x. So $f(x) = t(x)g(x) + \sum_{i=1}^{k} f_i(x) = (t(x) + \sum_{i=1}^{k-1} t_i(x))g(x) + f_k(x)$. Well, $t_k(x) = ([x^\mu]f_k(x))(b_m^{-1})\, x^{m-\mu}$ must have positive degree, and so $t_k(x)g(x)$ has the same leading coefficient as $f_k(x)$. But then $f_{k+1}(x)$ is a polynomial in $\mathbb{K}[x]$ with $\deg(f_{k+1}(x)) < \deg(f_k(x))$. So our process must terminate with at some $i = r$ such that $f_r(x)$ has degree strictly less than m. That is:

$$f(x) = t(x)g(x) + \sum_{i=1}^{r} f_r(x) = (t(x) + \sum_{i=1}^{r-1} t_i(x))g(x) + f_r(x) \text{ where } \deg(f_r(x)) < m = \deg(g(x)).$$

Which satisfies the statement. By exhaustion, the statement is proven. □

Lemma 6. *Let R be a commutative ring with unity. R/I is a field if and only if I is a maximal ideal of R.*

Proof. ($\Longleftarrow$) For any non-zero $\overline{q} \in R/I$ there exists some non-zero reduced representative $q \in R \setminus I$ such that $\overline{q} = [q]_I$. If I is maximal, then it's proper and then $I \subset I + \langle q \rangle \subseteq R \implies I + \langle q \rangle = R$, since I is maximal. So $1 \in I + \langle q \rangle$ and therefore $\exists i \in I, \exists pq \in \langle q \rangle$ such that

$$1 = i + pq \implies [1]_I = [i + pq]_I = [0]_I + [p]_I [q]_I \in R/I.$$

So $[q]_I$ is a unit. Therefore, we see all non-zero elements of R/I are units and so R/I is a field.

($\Longrightarrow$) If R/I is a field, let J be an ideal of R with $I \subseteq J \subseteq R$. Then $J/I = \{j + I : j \in J\}$ is an ideal of R/I by the **Third Isomorphism Theorem**. Well, since R/I is a field, its only ideals are $\{0\}$ and R/I, so $J/I = \{0\}$ or $J/I = R/I$.

If $J/I = \{0\}$, then $J = I$. Otherwise, If $J/I = R/I$, then $[1]_I \in J/I$, so there exists $j \in J$ with $[1]_I = [j]_I$. That is, $j - 1 \in J$. So then $j - (j - 1) = 1 \in J \implies r(1) = r \in J, \forall r \in R \implies J = R$. So $J = I$ or $j = R$ and therefore I is maximal.

Thus,

If R is a commutative ring with unity, then R/I is a field if and only if I is a maximal ideal of R.

$\square$

Lemma 7 (Zorn's Lemma)**.** *Let $(P, \leq)$ be a partially ordered set. If every chain in P has an upper bound in P, then P contains a maximal element.*

Theorem 8 (Problem $8(c)$ from HW 1)**.** *If R is a commutative ring with unity, then any $A(x)$ is a unit in $R[[x]]$ is a unit if and only if its constant term $[x^0]A(x)$ is a unit in R.*

Lemma 9 (Maximal ideals contain no units)**.** *If M is a maximal (two-sided) ideal of a ring R, then M contains no units of R.*

Proof. Suppose u is a unit in M with inverse $u^{-1} \in R$. Then $uu^{-1} = 1 \in M$. But then $1(r) = r \in M$ for all $r \in R$, and $M = R$ is not proper, a contradiction.

Thus,

A M is a maximal ideal of a ring R contains no units.

$\square$

Lemma 10. *A subring with unity, of an integral domain R is an integral domain.*

Proof. Let S be a unital subring of an integral domain R. Then for any $a, b \in S \subseteq R$, $ab = ba$, since R is commutative and $ab = 0$ with $a \neq 0 \implies b = 0$ immediately since R is an integral domain. So S is an integral domain.

$\square$

Problem 1. In the following problems, we investigate the relationship between integral domains and fields.

(a) Prove that every field is an integral domain.

(b) Prove that if R is a finite integral domain, then R is a field. **Hint:** Consider the set function $a : R \to R$ given by multiplication by an element a (it will not be a ring homomorphism). If a is a non-zero-divisor, prove this is an injective function, and so must also be surjective since R has finitely many elements.

(c) Find an example of an integral domain which is not a field.

Proof. **(a)** Let $\mathbb{K}$ be a field, and suppose it contains some non-zero zero divisor $b \in \mathbb{K} \setminus \{0\}$. Then there exists some $a \in \mathbb{K} \setminus \{0\}$ such that $ab = ba = 0$. Since $a, b \in \mathbb{K} \setminus \{0\}$, they are both units and so there exist $a^{-1}, b^{-1} \in \mathbb{K}$ such that $a^{-1}a = bb^{-1} = 1 \implies a^{-1}(ab)b^{-1} = 1 = a^{-1}(0)b^{-1} = 0 \implies 1 = 0$. But then $\mathbb{K} = \{0\}$ which is not a field, a contradiction. Therefore, all non-zero elements are not zero divisors and so $\mathbb{K}$ is a commutative ring with unity and no zero divisors, which is the definition of an integral domain.

(b) Let R be a finite integral domain, and let a be some non-zero divisor $a \in R \setminus \{0\}$. We show the mapping $a : R \to R$ via $a(x) = ax$, $\forall x \in R$ is a bijection. For all $x, y \in R$,

[1-1] $a(x) = a(y) \implies ax = ay \implies ax - ay = a(x-y) = 0 \implies x = y$
otherwise a is a zero divisor, and we get a contradiction.
[Onto] $a : R \hookrightarrow R \implies$ the domain is in bijection with its image $\implies |R| = |a(R)|$
and since $a(R) \subseteq R$ (the domain is equal to the codomain), we must have that $a(R) = R$.

(This image is just the orbit of a in the canonical multiplicative monoid action of R on itself.) So then for each non-zero zero divisor $a \in R \setminus \{0\}$, $\exists x \in R$ such that $a(x) = ax = 1$. That is, each non-zero zero divisor, which is just all of $R \setminus \{0\}$ is a unit. Therefore, R is a commutative ring with unity and inverses for all non-zero elements, which is the definition of a field.

(c) $\mathbb{Z}$ is an integral domain but not a field.

$\square$

Problem 2. Let I, J be ideals in a commutative ring R such that $I + J = (1)$. Prove that $IJ = I \cap J$.

Proof. $(\subseteq)$ Recall that since I, J are ideals of R, $ir \in I$ and $rj \in J$, $\forall i \in I, \forall j \in J, \forall r \in R$. So then for all $ij \in IJ$, we have that $(i)j \in I$ and $i(j) \in J \implies ij \in I \cap J \implies IJ \subseteq I \cap J$.

$(\supseteq)$ $I + J = \langle 1 \rangle \implies \hat{i} + \hat{j} = 1$ for some $\hat{i} \in I, \hat{j} \in J$. Then for all $a \in I \cap J$, $a = a(1) = (1)a = a(\hat{i} + \hat{j}) = a\hat{i} + a\hat{j} \in IJ + JI = IJ$, since commutativity in R implies $IJ = JI$. Therefore, $I \cap J \subseteq IJ$.

Thus,

$$IJ = I \cap J$$

.

$\square$

Problem 3. Let $\varphi : R \to S$ be a ring homomorphism, and let J be an ideal of S. Prove that $I = \varphi^{-1}(J) = \{i \in R \mid \varphi(i) \in J\}$ is an ideal of R.

Proof. $\forall a, b \in \varphi^{-1}(J),\ \varphi(a), \varphi(b) \in J$ and so $\varphi(a-b) = \varphi(a) - \varphi(b) \in J$. So then $a - b \in \varphi^{-1}(J)$ and $\varphi^{-1}(J) \leq_+ R$.

Next, for any $r \in R$ and any $i \in \varphi^{-1}(J),\ \varphi(ri) = \varphi(r)\varphi(i) \in J$ and $\varphi(ir) = \varphi(i)\varphi(r) \in J$, since J is an ideal of S. So then $ri, ir \in \varphi^{-1}(J)$.

Thus,

$$\text{If } \varphi : R \to S \text{ is a ring homomorphism and } J \text{ is an ideal of } S\text{, then } \varphi^{-1}(J) \text{ is an ideal of } R.$$

$\square$

Problem 4. Let $\varphi : R \to S$ be a ring homomorphism, and let J be an ideal of R.

(a) Prove that $\varphi(J) = \{\varphi(j) \mid j \in J\}$ need not be an ideal of S.

(b) Prove that if φ is surjective, then $\varphi(J)$ is an ideal of S.

(c) Prove that if φ is surjective, and $I = \ker \varphi$, then $S \cong R/I$ and if we let $\overline{J} \subseteq R/I$ be the image of $\varphi(J)$ under this isomorphism, then

$$(R/I)/\overline{J} \cong R/(I+J).$$

Proof. **(a)** Consider the inclusion map $\iota : \mathbb{Z} \hookrightarrow \mathbb{R}$ defined by $\iota(n) = n \in R$, $\forall n \in \mathbb{Z}$. This is a ring embedding by **Lemma** 2. Now look at $2 \in 2\mathbb{Z}$, which is a well-known ideal of $\mathbb{Z}$. Well, $\pi \in \mathbb{R}$ but $2\pi = \pi 2 \notin \iota(2\mathbb{Z}) = 2\mathbb{Z}$. So then $\iota(2\mathbb{Z})$ is not an ideal and we see that the ring homomorphic image of an ideal need not be an ideal of the codomain.

(b) For all $\varphi(a), \varphi(b) \in \varphi(J)$ with preimages $a, b \in J$, $\varphi(a) - \varphi(b) = \varphi(a-b) \in \varphi(J)$ since $a - b \in J$. Therefore $\varphi(J) \leq_+ S$. Next, since φ is surjective, for any $s \in S$, $\exists r \in R$ such that $s = \varphi(r)$. So then $s\varphi(a) = \varphi(r)\varphi(a) = \varphi(ra)$ and $\varphi(a)s = \varphi(a)\varphi(r) = \varphi(ar)$ which must both belong to $\varphi(J)$ since $J \subseteq R$ is an ideal $\implies ar, rs \in J$. Therefore, $\varphi(J)$ is an ideal of S. That is, a surjective ring homomorphic image of an ideal is in fact an ideal of the codomain.

(c) φ is surjective, so by the First Isomorphism Theorem $R/\ker \varphi = R/I \cong \varphi(R) = S$ and so $S \cong R/\ker \varphi = R/I$. Let $\psi : S \to R/I$ be this pullback isomorphism. That is,

$$\overbrace{r}^{R} \overset{\varphi}{\mapsto} \overbrace{\varphi(r) = s}^{S} \overset{\psi}{\longleftrightarrow} \overbrace{[r]_I = [r]_{\ker \varphi}}^{R/I = R/\ker \varphi} \tag{1}$$

$$\text{So: } \psi(s) = \psi(\varphi(r)) = [r]_I \in R/I, \text{ for each } s = \varphi(r) \in \varphi(R) = S \tag{2}$$

$$\implies \psi(\varphi(j)) = [j]_I \in R/I \text{ for each } j \in J \tag{3}$$

$$\text{Now let: } \overline{J} = \psi(\varphi(J)) = \{\psi(\varphi(j)) = [j]_I \mid j \in J\} \subseteq R/I \tag{4}$$

Recall the Third Isomorphism Theorem. For ideals A, B of a ring R where $A \subseteq B$ is a subset:

$$① \ B/A \text{ is an ideal of } R/A \text{ and } ② \ \frac{(R/A)}{(B/A)} \cong \frac{R}{B}.$$

By **Lemma** 1, $I + J$ is an ideal of R since I, J are ideals of R. Also, $I \subseteq I + J$ is a subset. Well, we can simply compute that $(I+J)/I = \{(i+j) + I \mid (i+j) \in I + J\} = \{j + I = [j]_I \mid j \in J\} = \overline{J}$ by (4).

Therefore, since $I, (I+J)$ are ideals of R with $I \subseteq (I+J)$, by the Third Isomorphism Theorem we have that

$$① \ \overline{J} = (I+J)/I \text{ is an ideal of } (R/I) \text{ and } ② \ \frac{(R/I)}{\overline{J}} = \frac{(R/I)}{(I+J)/I} \cong \frac{R}{(I+J)}.$$

□

Problem 5. Let R be a commutative ring, $a \in R$, and let $f_1(x), \dots, f_r(x) \in R[x]$.

(a) Prove that $R[x]/(x-a) \cong R$.

(b) Prove the equality of ideals

$$(f_1(x), \dots, f_n(x), x-a) = (f_1(a), \dots, f_n(a), x-a).$$

(c) Prove the useful substitution trick

$$R[x]/(f_1(x), \dots, f_n(x), x-a) \cong R/(f_1(a), \dots, f_n(a)).$$

Hint: Use part (c) of the previous problem.

Proof. **(a)** Consider $\varepsilon_a : R[x] \to R$ defined by $\varepsilon_a(f(x)) = f(a)$, an evaluation which was proven to be a *surjective homomorphism* in **Lemma** 3. We show that $\ker \varepsilon_a = \langle x-a \rangle = \{f(x)(x-a) \mid f(x) \in R[x]\}$.

($\subseteq$) For any $B(x) = \sum_{k=0}^{n} b_k x^k \in \ker \varepsilon_a$, $B(a) = 0$. Well, $B(x) - B(a) = (\sum_{k=0}^{n} b_k x^k) - (\sum_{k=0}^{n} b_k a^k) = \sum_{k=0}^{n} b_k$ $(x^k - a^k) = \sum_{k=1}^{n} b_k (x^k - a^k)$. Then by **Lemma** 4, $(x^k - a^k) = (x-a) \sum_{i+j=k-1} x^i y^j$ for each $1 \le k \le n$. Therefore,

$$B(x) - B(a) = \sum_{k=1}^{n} b_k (x^k - a^k) = \sum_{k=1}^{n} b_k ((x-a) \sum_{i+j=k-1} x^i a^j) = (x-a) \sum_{k=1}^{n} b_k (\sum_{i+j=k-1} x^i a^j)$$

and since in fact $B(a) = 0$, we have that $B(x) = (x-a) \sum_{k=1}^{n} b_k (\sum_{i+j=k-1} x^i a^j) \in \langle x-a \rangle$ since $\sum_{k=1}^{n} b_k (\sum_{i+j=k-1} x^i y^j)$ belongs to $R[x]$. So then $\ker \varepsilon_a \subseteq \langle x-a \rangle$.

($\supseteq$) $\forall C(x) = f(x)(x-a) \in \langle x-a \rangle$ obviously $C(a) = f(a)(a-a) = 0 \implies C(x) \in \ker \varepsilon_a$. So then $\langle x-a \rangle \subseteq \ker \varepsilon_a$.. Thus, by the **First Isomorphism Theorem**,

$$R[x]/\ker \varepsilon_a = R[x]/\langle x-a \rangle \cong \varepsilon_a(R[x]) = R.$$

(b) For each $1 \le m \le n$, there exist $b_{m,0}, \dots, b_{m,d_m} \in R$ and $d_m \in \mathbb{N}$ such that $f_m(x) = \sum_{k=0}^{d_m} b_{m,k} x^k$. Now we use a result obtained in **(a)**:

$$f_k(x) - f_k(a) = (x-a) \sum_{k=1}^{d_m} b_{m,k} (\sum_{i+j=k-1} x^i a^j) \implies f_k(x) = f_k(a) + (x-a) \sum_{k=1}^{d_m} b_{m,k} (\sum_{i+j=k-1} x^i a^j)$$

So then

$$f_k(x) \in \langle f_k(a), x-a \rangle \subseteq \langle f_1(a), \dots, f_n(a), x-a \rangle, \ \forall 1 \le k \le n$$

and

$$f_k(a) \in \langle f_k(x), x-a \rangle \subseteq \langle f_1(x), \dots, f_n(x), x-a \rangle, \ \forall 1 \le k \le n$$

Therefore, all generators of $\langle f_1(x), \dots, f_n(x), x-a \rangle$ belong to $\langle f_1(a), \dots, f_n(a), x-a \rangle$ and vice versa. So the ideals are equal.

$\square$

Proof. **(c)** In **(a)** we used the surjective homomorphism $\varepsilon_a : R[x] \to R$ defined by $\varepsilon_a(h(x)) = h(a)$ to show that $R[x]/\langle x-a\rangle = R[x]/I \cong R$ by the **First Isomorphism Theorem** where $I = \ker\varepsilon_a = \langle x-a\rangle$. Much like in **Problem 4** let $\psi : R \to R[x]/I$ be the pullback isomorphism and let $J = \langle f_1(x),\ldots,f_n(x),x-a\rangle \subseteq R[x]$. Then:

$$\overbrace{r(x)}^{R[x]} \overset{\varepsilon_a}{\mapsto} \overbrace{\varepsilon_a(r(x)) = r(a)}^{R} \overset{\psi}{\longleftrightarrow} \overbrace{[r(x)]_I = [r(x)]_{\ker\varepsilon_a}}^{R[x]/I=R[x]/\ker\varepsilon_a} \tag{1}$$

$$\text{So: } \psi(r) = \psi(\varepsilon_a(r(x))) = [r(x)]_I \in R[x]/I, \text{ for each } r = \varepsilon_a(r(x)) \in \varepsilon_a(R[x]) = R(\text{ use } r(x) = r) \tag{2}$$

$$\Longrightarrow \psi(\varepsilon_a(j(x))) = [j(x)]_I \in R[x]/I \text{ for each } j(x) \in J \tag{3}$$

$$\text{Now let: } \bar{J} = \psi(\varepsilon_a(J)) = \{\psi(\varepsilon_a(j)) = [j(x)]_I \mid j(x) \in J\} = J/I \subseteq R[x]/I \text{ *an ideal of } R[x]/I\text{*} \tag{4}$$

Well, $(I+J)/I = (\langle x-a\rangle + \langle f_1(x),\ldots,f_n(x),x-a\rangle)/\langle x-a\rangle = \langle f_1(x),\ldots,f_n(x),x-a\rangle/\langle x-a\rangle = J/I = \bar{J}$. Since $I,(I+J)$ are ideals of $R[x]$ with $I \subseteq (I+J)$, by the **Third Isomorphism Theorem** we have that

$$① \ \bar{J} = (I+J)/I \text{ is an ideal of } (R[x]/I) \text{ and } ② \ \frac{(R[x]/I)}{\bar{J}} = \frac{(R[x]/I)}{(I+J)/I} \cong \frac{R[x]}{I+J} = R[x]/J.$$

Let $K = \langle f_1,\ldots,f_n\rangle$ and $\Phi : R[x]/I \to \frac{R}{\langle f_1(a),\ldots,f_n(a)\rangle} = R/K$ defined via $\Phi([h(x)]_I) = \psi^{-1}([h(x)]_I) + K$.

Obviously this is well defined since ψ^{-1} is an isomorphism, and then for all $[A(x)]_I, [B(x)]_I \in R[x]/I$,

$$\begin{aligned}
&\Phi([I]_{1_R}) = \phi^{-1}([1_R]_I) + K = 1_R + K = 1_{R/K}\\
&\Phi([A(x)]_I) + \Phi([B(x)]_I) = \psi^{-1}([A(x)]_I) + \psi^{-1}([B(x)]_I) + K = \psi^{-1}([A(x)]_I + [B(x)]_I) + K\\
&= \Phi([A(x)]_I + [B(x)]_I)\\
&\Phi([A(x)]_I)\Phi([B(x)]_I) = (\psi^{-1}([A(x)]_I))(\psi^{-1}([B(x)]_I)) + K = \psi^{-1}([A(x)]_I[B(x)]_I) + K\\
&= \Phi([A(x)]_I[B(x)]_I)\\
&\forall (r+K) \in R/K\ , \exists \psi(r) = [r]_I \in R/I \text{ such that } \Phi(\psi(r)) = \psi^{-1}(\psi(r)) + K = r + K.
\end{aligned}$$

So Φ is an surjective ring homomorphism. We show $\ker\Phi = \bar{J}$. ($\subseteq$) For any $j(x) \in J = \langle f_1(a),\ldots,f_n(a),x-a\rangle$ is of the form $j(x) = j_0(a)(x-a) + \sum_{i=1}^n j_i(x)f_i(a)$ for some $j_0(x),\ldots,j_n(x) \in R[x]$, and so $j(a) = \sum_{i=1}^n j_i(a)f_i(a)$. Therefore, for any $[j(x)]_I \in \bar{J}$, $\Phi([j(x)]_I) = \psi^{-1}([j(x)]_I) + K = j(a) + K = K \Longrightarrow [j(x)]_I \in \ker\Phi \subseteq \ker\Phi$.

($\supseteq$) On the other hand, for any $[r(x)]_I$, $r(a) \in K$ and so $r(a) = \sum_{i=1}^n r_i f_i(a)$ for some $r_1,\ldots,r_k \in R$ and then $r(x) = r_0(x)(x-a) + \sum_{i=1}^n r_i(x)f_i(x)$ for some $r_0(x), r_1(x),\ldots,r_n(x) \in R[x]$ such that $r_i(a) = r_i$ for each $1 \le i \le n$. Therefore, $r(x) \in J$ and so $[r(x)]_I \in \bar{J} \Longrightarrow \ker\Phi \subseteq \bar{J}$. So $\ker\Phi = \bar{J}$, and by the **First Isomorphism Theorem** ③ $\frac{R[x]/I}{\ker\Phi} = \frac{R[x]/I}{\bar{J}} \cong \Phi(R[x]/I) = R/J$.

Thus, by ② and ③,

$$\frac{R[x]}{\langle f_1(x),\ldots,f_n(x),x-a\rangle} = R[x]/J \cong \frac{R[x]/I}{\bar{J}} \cong R/K = \frac{R}{\langle f_1(a),\ldots,f_n(a)\rangle}$$

$\square$

Problem 6. If $\Bbbk$ is an algebraic closed field, then the only maximal ideals of $\Bbbk[x]$ are of the form $(x-a)$ where $a \in \Bbbk$. In this problem, we'll see that this is not true when $\Bbbk$ is not algebraically closed.

(a) Use the first isomorphism theorem to show that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

(b) Prove that (x^2+1) is a maximal ideal of $\mathbb{R}[x]$.

Proof. **(a)**Let $\varepsilon_i : \mathbb{R}[x] \to \mathbb{C}$ be defined via $\varepsilon_i(f(x)) = f(i)$ for all $f(x) \in \mathbb{R}[x]$. We show this is a surjective ring homomorphism. For any $A(x), B(x) \in \mathbb{R}[x]$,

$$\begin{aligned}
&\varepsilon_i(1(x)) = 1(a) = 1_{\mathbb{R}} = 1_{\mathbb{C}} \\
&\varepsilon_i(A(x)) + \varepsilon_i(B(x)) = A(i) + B(i) = (A+B)(i)\varepsilon_i((A+B)(x)) = \varepsilon_i(A(x)+B(x)) \\
&\varepsilon_i(A(x))\varepsilon_i(B(x)) = A(i)B(i) = (AB)(i)\varepsilon_i((AB)(x)) = \varepsilon_i(A(x)B(x)) \\
&\forall(\alpha+\beta i) \in \mathbb{C},\ \varepsilon_i(\alpha+\beta x) = \alpha+\beta i
\end{aligned}$$

Next, we show that $\ker \varepsilon_i = \langle x^2+1 \rangle$. $(\subseteq)$ Consider any $C(x) \in \ker \varepsilon_i$. **By Lemma** 5 we have the division algorithm for polynomials over fields. So $C(x) = q(x)(x^2+1) + r(x)$ where $r(x) = 0$ or $\deg(r(x)) < 2 = \deg(x^2+1)$. Well, $0 = C(i) = q(i)(i^2+1) + r(i) \implies r(i) = 0$ and so it can't be linear otherwise $r(i)$ wouldn't vanish; $r(x) = ax+b$ is linear implies $a \neq 0$ and then $r(i) = ai + b \neq 0$ since $i \neq 0$ and $ai = -b \implies b \notin \mathbb{R}$. So then $r(x)$ must be some constant r. So then $r(i) = r(x) = r = 0$. So x^2+1 divides $C(x) \implies C(x) \in \langle x^2+1 \rangle$. $(\supseteq)$ Trivially, any $f(x) = r(x)(x^2+1)$ belongs to $\ker \varepsilon_i$ since then $f(i) = r(i)(i^2+1) = 0$.

So then $\ker \varepsilon_i = \langle x^2+1 \rangle$ and by the **First Isomorphism Theorem**

$$\mathbb{R}[x]/\langle x^2+1 \rangle = \mathbb{R}[x]/\ker \varepsilon_i \cong \varepsilon_i(\mathbb{R}[x]) = \mathbb{C}.$$

(b) $\mathbb{R}[x]/\langle x^2+1 \rangle \cong \mathbb{C}$, so $\mathbb{R}[x]/\langle x^2+1 \rangle$ is a field and then by **Lemma** 6, $\langle x^2+1 \rangle$ must be maximal.

$\square$

Problem 7. Let R be a commutative ring with $0 \neq 1$. In this problem, we will prove that every proper ideal of R is contained in some maximal ideal.

(a) Look up Zorn's Lemma and record it here.

(b) Define $S = \{J \mid J \text{ is a proper ideal of } R \text{ and } J \supseteq I\}$. Explain why S is a partially ordered set (what is the ordering?).

(c) Given a chain C in S, prove that $\bigcup_{J \in C} J$ is an ideal of R (you will use that C is totally ordered), and further that this ideal is in the set S.

(d) Conclude using Zorn's Lemma that S has a maximal element.

(a)

Lemma 7 (Zorn's Lemma)**.** *Let $(P, \leq)$ be a partially ordered set. If every chain in P has an upper bound in P, then P contains a maximal element.*

Proof. **(b)** (1) $A \subseteq A$, $\forall A \in S$. (2) $A \subseteq B$ and $A \neq B \implies A \subset B \implies B \not\subseteq A$ (3) $A \subseteq B$ and $B \subseteq C \implies A \subseteq C$. So $(J, \subseteq)$ is a poset.

(c) Let C be a chain in S and consider $U_C = \bigcup_{J \in C} J$. We show this is an ideal of R.

For any $a, b \in U_C$, $\exists J_a, J_b \in C$ such that $a \in J_a$ and $b \in J_b$, and then $a, b \in J_a \cup J_b$. Since C is totally ordered, $(J_a \subseteq J_b \implies J_a \cup J_b = J_b)$ or $(J_b \subseteq J_a \implies J_a \cup J_b = J_a)$. Therefore,

$$a, b \in \begin{cases} J_b, & \text{if } J_a \subseteq J_b \\ J_a, & \text{if } J_b \subseteq J_a \end{cases} \implies a - b \in J_b \subseteq U_c \text{ or } a - b \in J_a \subseteq U_c \implies U_c \leq_+ R.$$

Now, for any $u \in U_C, \exists J_u \in C$ such that $u \in J_u$, and since J_u is an ideal, for any $r \in R$, $ru = ur \in J_u \subseteq U_C$. So U_C is an ideal of R.

Now, suppose $1 \in U_C$. Then there exists some $J_1 \in C$ such that $1 \in J_1$. So $r(1) = r \in J_1$, $\forall r \in R$, and $J_1 = R$. But then $\exists J_1 \in C$ which isn't proper, a contradiction. Therefore, $1 \notin U_C \implies U_C$ is a proper ideal of R. Finally, since I is contained in all ideals J in S, of course I is contained in any arbitrary union of ideals in S, and so of course $U_C = \bigcup_{J \in C \subseteq S} J$ contains I. Thus, $U_C \in S$.

(d) For any chain C in S, by **(c)** we have that $U_C = \bigcup_{J \in C} J \in S$ and since $J \subseteq U_C, \forall J \in C$, U_C is an upper bound for C in S. So any chain has an upperbound in S and by **Zorn's Lemma** (Lemma 7), S contains a maximal element. That is, there exists some maximal ideal of R which contains all proper ideal that contain I, or equivalently, every proper ideal I of R is contained in some maximal ideal of R.

□

Problem 8. Let $\mathbb{K}$ be a field. In this problem, we will prove that the only maximal ideal of $\Bbbk[[x]]$ is $\langle x\rangle$, which makes $\mathbb{K}[[x]]$ a local ring.

(a) Explain why $(x) = \{f \in \mathbb{K}[[x]] \mid f \text{ has no constant term}\}$.

(b) Compute $\mathbb{K}[[x]]/(x)$, and then explain why (x) is a maximal ideal.

(c) You may freely use the following result from the optional hint last week: $f \in \mathbb{K}[[x]]$ is a unit if and only f has a nonzero constant term. Use Proposition 1.41 to show that the only maximal ideal of $\mathbb{K}[[x]]$ is (x).

Proof. **(a)** ($\subseteq$) Any $F(x) \in \langle x\rangle$ is of the form $F(x) = xQ(x)$ for some $Q(x) = \sum_{i=0}^{\infty} q_i x^i \in \mathbb{K}[[x]]$. So then $F(x) = xQ(x) = x\sum_{i=0}^{\infty} q_i x^i = \sum_{i=0}^{\infty} q_0 x^{i+1}$ has no constant term and therefore belongs to $\{f \in \mathbb{K}[[x]] \mid f \text{ has no constant term}\}$. Therefore, $\langle x\rangle \subseteq \{f \in \mathbb{K}[[x]] \mid f \text{ has no constant term}\}$.

($\supseteq$) Any $G(x) \in \{f \in \mathbb{K}[[x]] \mid f \text{ has no constant term}\}$ has no constant term and must be of the form $G(x) = \sum_{j=1}^{\infty} g_i x^i = x\sum_{i=1}^{\infty} g_i x^{i-1} \in \langle x\rangle$ since $\sum_{i=1}^{\infty} g_i x^{i-1} \in \mathbb{K}[[x]]$. So, $\{f \in \mathbb{K}[[x]] \mid f \text{ has no constant term}\} \subseteq \langle x\rangle$.

Thus,

$$\langle x\rangle = \{f \in \mathbb{K}[[x]] \mid f \text{ has no constant term}\}.$$

(b) Consider any non-zero $\overline{U(x)} \in \frac{\mathbb{K}[[x]]}{\langle x\rangle}$. There exists some non-zero $U(x) \in \mathbb{K}[[x]] \setminus \{0\}$ such that $\overline{U(x)} = U(x) + \langle x\rangle \neq \langle x\rangle$. That is, $U(x) \notin \langle x\rangle = \{f \in \mathbb{K}[[x]] \mid f \text{ has no constant term}\}$, and so $U(x)$ has a non-zero constant term $u_0 = [x^0]U(x) \in \mathbb{K}$.

Well, since $\mathbb{K}$ is a field, u_0 must be a unit in $\mathbb{K}$. Therefore by **Problem 8(c)**, the constant term $u_0 = [x^0]U(x)$ is a unit in $\mathbb{K} \implies U(x)$ is a unit in $\mathbb{K}[[x]]$. So there exists some $U^{-1}(x) \in \mathbb{K}[[x]]$ such that $U(x)U^{-1}(x) = 1$ and so

$$\left[U(x)\right]_{\langle x\rangle}\left[U^{-1}(x)\right]_{\langle x\rangle} = \left[U(x)U^{-1}(x)\right]_{\langle x\rangle} = [1]_{\langle x\rangle} = 1_{\frac{\mathbb{K}[[x]]}{\langle x\rangle}} \implies \overline{U(x)} = [U(x)]_{\langle x\rangle} \text{ is a unit in } \frac{\mathbb{K}[[x]]}{\langle x\rangle}.$$

Therefore, every non-zero element of $\frac{\mathbb{K}[[x]]}{\langle x\rangle}$ is a unit, and so $\frac{\mathbb{K}[[x]]}{\langle x\rangle}$ is a field.

Thus, by **Lemma** 6,

$$\langle x\rangle \text{ is a maximal ideal of } \mathbb{K}[[x]].$$

(c) Let M be a maximal ideal of $\mathbb{K}[[x]]$ and consider any $F(x) \in M$. By **Lemma** 9, since M is maximal, it contains no units. So then all elements of M are non-units and by the contrapositive of **Problem** 8**(c)**, all elements have no constant term. So $F(x) \in \langle x\rangle = \{f \in \mathbb{K}[[x]] \mid \text{f has no constant term}\}$. So $M \subseteq \langle x\rangle \subset \mathbb{K}[[x]]$. Well, since M is maximal, either $\langle x\rangle = \mathbb{K}[[x]]$ or $\langle x\rangle = M$. Therefore, since $\langle x\rangle \subset \mathbb{K}[[x]]$ is proper, we must have that $\langle x\rangle = M$.

Thus,

$$\langle x\rangle \text{ is the only maximal ideal of } \mathbb{K}[[x]].$$

$\square$

Problem 9. Let d be an integer which is not the square of an integer, and consider

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

(a) Prove that $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$.

(b) Define a function $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ by $N(a+b\sqrt{d}) = a^2 - b^2 d$. Prove that $N(zw) = N(z)N(w)$ and that $N(z) \neq 0$ if $z \neq 0$. This function is often called the norm.

(c) Prove that $\mathbb{Q}(\sqrt{d})$ is a field and is the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$ (use N).

(d) Prove that $\mathbb{Q}(\sqrt{d}) \cong \mathbb{Q}[x]/(x^2 - d)$.

Proof. $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$ since $\forall a, b \in \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$, $a + b\sqrt{d} \in \mathbb{C}$.

Next, for any $r_1 = a_1 + b_1\sqrt{d}, r_2 = a_2 + b_2\sqrt{d} \in \mathbb{Q}(\sqrt{d})$,

$$\begin{aligned}
&1 \in \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d}) \\
&r_1 - r_2 = (a_1 - a_2) + (b_1 - b_2)\sqrt{d} \in \mathbb{Q}(\sqrt{d}) \\
&r_1 r_2 = (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) = (a_1 a_2 + b_1 b_2 d) + (a_1 b_2 + b_1 a_2)\sqrt{d} \in \mathbb{Q}(\sqrt{d})
\end{aligned}$$

So $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$, and since $\mathbb{C}$ is an integral domain, by **Lemma** 10 so is $\mathbb{Q}(\sqrt{d})$.

(b) Next, $N(r_1)N(r_2) = (a_1^2 - b_1^2 d)(a_2^2 - b_2^2 d) = a_1^2 a_2^2 - (a_1^2 b_2^2 + b_1^2 a_2^2)d + b_1^2 b_2^2 d^2$. Recall that $\mathbb{Q}$ is a field.

So on the other hand, $N(r_1 r_2) = N((a_1 a_2 + b_1 b_2 d) + (a_1 b_2 + b_1 a_2)\sqrt{d}) = (a_1 a_2 + b_1 b_2 d)^2 - (a_1 b_2 + b_1 a_2)^2 d$ $= ((a_1 a_2)^2 + 2(a_1 a_2 b_1 b_2)d + (b_1 b_2)^2 d^2) - ((a_1 b_2)^2 + 2(a_1 b_2 b_1 a_2) + (b_1 a_2)^2)d = a_1^2 a_2^2 + 2(a_1 a_2 b_1 b_2)d + b_1^2 b_2^2 d^2 - a_1^2 b_2^2 d - 2(a_1 a_2 b_1 b_2)d - b_1^2 a_2^2 d = a_1^2 a_2^2 - (a_1^2 b_2^2 + b_1^2 a_2^2)d + b_1^2 b_2^2 d^2 = N(r_1)N(r_2)$.

Finally, for any non-zero $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ suppose that $N(a + b\sqrt{d}) = a^2 - b^2 d = 0$. Then $a^2 = b^2 d$. Now, $d \neq 0$ since 0 is a square. So $a = 0 \implies b = 0$ and $b = 0 \implies a = 0$ since $\mathbb{Z}$ is an integral domain, and then both are contradictions since $z = a + b\sqrt{d} \neq 0$. So a and b must both be non-zero. But then $d = \frac{a^2}{b^2}$ is either the square of an integer, or not an integer at all, a contradiction. Therefore, $N(z) \neq 0$ if $z \neq 0$.

(c) Consider any non-zero $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$. By **(b)**, $N(z) = a^2 - b^2 d \neq 0$, and recall that $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$

$$z^{-1} = \frac{a - b\sqrt{d}}{N(z)} = \frac{a - b\sqrt{d}}{(a + b\sqrt{d})(a - b\sqrt{d})} \in \mathbb{Q}(\sqrt{d}) \implies zz^{-1} = z^{-1}z = \frac{(a + b\sqrt{d})(a - b\sqrt{d})}{(a + b\sqrt{d})(a - b\sqrt{d})} = 1$$

So every non-zero element of the integral domain $\mathbb{Q}(\sqrt{d})$ is a unit, and therefore $\mathbb{Q}(\sqrt{d})$ is a field.

Finally, consider any subfield $\mathbb{F}$ of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$. For any $a + b\sqrt{d}$, $a, b, \sqrt{d} \in \mathbb{F} \implies a + b\sqrt{d} \in \mathbb{F}$ and so $\mathbb{Q}(\sqrt{d}) \subseteq \mathbb{F}$ for any such subfield $\mathbb{F}$. Thus, $\mathbb{Q}(\sqrt{d})$ is the smallest subfield of $\mathbb{C}$ containing both $\mathbb{Q}$ and $\sqrt{d}$.

$\square$

We prove (d) on the next page.

Proof. **(d)** Let $\varepsilon_{\sqrt{d}} : \mathbb{Q}[x] \to \mathbb{Q}(\sqrt{d})$ be defined by $\varepsilon_{\sqrt{d}}(f(x)) = f(\sqrt{d})$, $\forall f(x) \in \mathbb{Q}[x]$.

We show this is a surjective ring homomorphism. For any $A(x), B(x) \in \mathbb{Q}[x]$,

$$\varepsilon_{\sqrt{d}}(1(x)) = 1(\sqrt{d}) = 1_{\mathbb{Q}} = 1_{\mathbb{Q}(\sqrt{d})}$$
$$\varepsilon_{\sqrt{d}}(A(x)) + \varepsilon_{\sqrt{d}}(B(x)) = A(\sqrt{d}) + B(\sqrt{d}) = (A+B)(\sqrt{d}) = \varepsilon_{\sqrt{d}}((A+B)(x)) = \varepsilon_{\sqrt{d}}(A(x)+B(x))$$
$$\varepsilon_{\sqrt{d}}(A(x))\varepsilon_{\sqrt{d}}(B(x)) = A(\sqrt{d})B(\sqrt{d}) = (AB)(\sqrt{d}) = \varepsilon_{\sqrt{d}}((AB)(x)) = \varepsilon_{\sqrt{d}}(A(x)B(x))$$
$$\forall (a+b\sqrt{d}) \in \mathbb{Q}(\sqrt{d}),\ \varepsilon_{\sqrt{d}}(a+bx) = a+b\sqrt{d}$$

We show $\ker \varepsilon_{\sqrt{d}} = \langle x^2 - d \rangle$. ($\subseteq$) for any $C(x) \in \ker \varepsilon_{\sqrt{d}}$, $C(\sqrt{d}) = 0$. By the **Division Algorithm** for polynomials over fields (**Lemma** 5), $C(x) = q(x)(x^2-d) + r(x)$ where $r(x) = 0$ or $\deg(r(x)) < 2 = \deg(x^2 - d)$. Well, $0 = C(\sqrt{d}) = q(\sqrt{d})(\sqrt{d}^2 - d) + r(\sqrt{d}) \implies r(\sqrt{d}) = 0$ and so it can't be linear otherwise $r(\sqrt{d})$ wouldn't vanish; $r(x) = ax+b$ is linear implies $a \neq 0$ and then $r(\sqrt{d}) = a\sqrt{d} + b \neq 0$ since $\sqrt{d} \neq 0$ and $b = a\sqrt{d} \implies b \notin \mathbb{Q}$. So $r(x)$ must be some constant $q \in \mathbb{Q}$, and then $r(\sqrt{d}) = r(x) = q = 0$. So $x^2 - d$ divides $C(x) \implies C(x) \in \langle x^2 - d \rangle$. ($\supseteq$) Trivially, any $f(x) = q(x)(x^2-d)$ belongs to $\ker \varepsilon_{\sqrt{d}}$ since then $f(\sqrt{d}) = r(\sqrt{d})(\sqrt{d}^2 - d) = 0$.

So then $\ker \varepsilon_{\sqrt{d}} = \langle x^2 - d \rangle$ and by the **First Isomorphism Theorem**

$$\mathbb{Q}[x]/\langle x^2 - d \rangle = \mathbb{Q}[x]/\ker \varepsilon_{\sqrt{d}} \cong \varepsilon_{\sqrt{d}}(\mathbb{Q}[x]) = \mathbb{Q}(\sqrt{d}).$$

$\square$