Algebra: Chapter 0 Exercises

Chapter 3, Section 4

Ideals and quotients: Remarks and examples. Prime and maximal ideals

David Melendez

September 6, 2018

Problem 4.1. Let R be a ring, and let $\{I_\alpha\}_{\alpha \in A}$ be a family of ideals of R. We let

$$\sum_{\alpha \in A} I_\alpha = \left\{ \sum_{\alpha \in A} r_\alpha \text{ such that } r_\alpha \in I_\alpha \text{ and } r_\alpha = 0 \text{ for all but finitely many } \alpha \right\}$$

Prove that $J = \sum_\alpha I_\alpha$ is an ideal of R and that it is the smallest ideal containing all of the ideals I_α.

Solution. First we prove that J is an ideal of R.

Proof. Let $a, b \in J$, so that

$$a = \sum_{\alpha \in A} r_\alpha$$
$$b = \sum_{\alpha \in A} s_\alpha,$$

where each $r_\alpha, s_\alpha \in I_\alpha$ and all but finitely many r_α and s_α are nonzero. We then have:

$$\begin{aligned} a + b &= \sum_{\alpha \in A} r_\alpha + \sum_{\alpha \in A} s_\alpha \\ &= \sum_{\alpha \in A} r_\alpha + s_\alpha. \end{aligned}$$

Each term $r_\alpha + s_\alpha$ is in I_α since $r_\alpha, s_\alpha \in I_\alpha$ and I_α is an ideal, and clearly all but finitely many $r_\alpha + s_\alpha$ are nonzero since $(r_\alpha)_{\alpha \in A}$ and $(s_\alpha)_{\alpha \in A}$ both have that property, so $a + b \in J$.

Additionally, if $s \in R$ and $r \in J$ so that $r = \sum_{\alpha \in A} r_\alpha$ (where all but finitely many r's are zero), then we have

$$\begin{aligned} rs &= \left(\sum_{\alpha \in A} r_\alpha \right) s \\ &= \sum_{\alpha \in A} r_\alpha s \\ &\in J, \end{aligned}$$

where the last line is true because each $r_\alpha s \in I_\alpha$ as a result of each I_α being a right-ideal of R, and the fact that if r_α is zero then $r_\alpha s$ is also zero, implying that there are cofinitely many zero terms in this resulting sum as well. A similar argument shows that J is a left-ideal of R if each I_α is also a left-ideal. □

Now, we will show that $J = \sum_{\alpha \in A} I_\alpha$ is the smallest ideal of R containing each of the ideals I_α for $\alpha \in A$.

Proof. We just proved that J is an ideal of R, so now we just need to show that J is a subset of any ideal containing each of the ideals I_α. This is immediate: if $r \in J$ is such that $r = \sum_{\alpha \in A} r_\alpha$ for $r_\alpha \in I_\alpha$, then of course any ideal of R containing each I_α contains r, since such an ideal is closed under addition. □

■

Problem 4.2. Prove that the homomorphic image of a Noetherian ring is Noetherian. That is, prove that if $\varphi : R \to S$ is a surjective ring homomorphism and R is Noetherian, then S is Noetherian.

Solution. Suppose $I = (a_1, \ldots, a_n)$ is an ideal of R and $\varphi : R \to S$ is surjective. Then we have

$$\begin{aligned}\varphi(I) &= \varphi\left(\sum_{i=1}^{n} (a_i)\right) \\ &= \sum_{i=1}^{n} \varphi((a_i)) \\ &= \sum_{i=1}^{n} (\varphi(a_i)),\end{aligned}$$

and so $\varphi(I)$ is finitely generated.

To see that these operations are justified, note that if $g \in R$ and $J = (g)$ is an ideal, then we have

$$\begin{aligned}\varphi(J) &= \varphi\left(\{rg : r \in R\}\right) \\ &= \{\varphi(r)\varphi(g) : r \in R\} \\ &= \{r\varphi(g) : r \in R\} \\ &= (\varphi(g)),\end{aligned}$$

where the third equality follows from the surjectivity of φ.

Additionally, if I, J are ideals of R, then we also have

$$\begin{aligned}\varphi(I + J) &= \varphi(\{i + j : i \in I, j \in J\}) \\ &= \{\varphi(i) + \varphi(j) : i \in I, j \in J\} \\ &= \varphi(I) + \varphi(J)\end{aligned}$$

Note, then, that if J is an ideal of S, then $\varphi^{-1}(J)$ is an ideal of R, allowing us to see that $J = \varphi(\varphi^{-1}(J))$ is finitely generated. Therefore, every ideal of S is finitely generated, and so S is Noetherian. ■

Problem 4.3. Prove that the ideal $(2, x)$ of $\mathbb{Z}[x]$ is not principal.

Solution. First, we (quite clumsily) compute the ideal $(2, x)$ as follows:

$$\begin{aligned}(2, x) &= \{2p + xq : p, q \in \mathbb{Z}[x]\} \\ &= \{(2a_0 + 2a_1x + \cdots + 2a_nx^n) + (b_1x + b_2x^2 + \cdots + b_mx^m) : a_j, b_j \in \mathbb{Z}\} \\ &= \{2a_0 + a_1x + a_2x^2 + \cdots + a_nx^n : a_j \in \mathbb{Z}\}.\end{aligned}$$

In other words, the ideal $(2, x)$ consists of all the polynomials in $\mathbb{Z}[x]$ with an even constant term.

Note, then, if $(2, x) = (g)$ for some polynomial $g \in \mathbb{Z}[x]$, then there must be a polynomial $p \in \mathbb{Z}[x]$ such that $2 = gp$, since $2 \in (2, x)$. If this is the case, then we have $\deg g + \deg p = 0$, and so $\deg g = \deg p = 0$. This means that g is constant, and hence is either 1 or 2. In the former case, (g) is the whole ring $\mathbb{Z}[x]$, and in the latter case, (g) is the ideal $2\mathbb{Z}[x]$. Neither of these ideals equal the ideal of $(2, x)$, leading us to conclude that no single polynomial in $\mathbb{Z}[x]$ generates the ideal $(2, x)$. ■

Problem 4.4. Prove that if k is a field, then $k[x]$ is a PID. (Hint: Polynomial divison with remainder)

Solution. Let $I \subseteq k[x]$ be an ideal. If $I = 0 = (0)$, then clearly it is principal. Otherwise, let $p \in I$ be a monic polynomial of minimal degree d Let $I \subseteq k[x]$ be an ideal. If $I = 0 = (0)$, then clearly it is principal.

Otherwise, let $g \in I$ be a monic polynomial of minimal degree d. If $p \in I$, then we can apply division with remainder to find polynomials $q, r \in k[x]$ such that

$$p = gq + r,$$

where $\deg r < d$. Note that since $p \in I$ and $gq \in I$ by (right-) absorption, we then can see that $r = p - gq \in I$, since I is closed under addition. But d is the smallest degree of any nonzero polynomial in I and $\deg r < d$; it then follows that $r = 0$, and so

$$p = gq,$$

showing us that $I \subseteq (g)$.

Of course $(g) \subseteq I$, so we then have $I = (g)$, as desired. ■

Problem 4.5. Let I, J be ideals in a commutative ring R, such that $I + J = (1)$. Prove that $IJ = I \cap J$.

Solution. The simple fact that $IH \subseteq I \cap J$ was already proven in the text, so suppose $r \in I \cap J$. Since $I + J = (1) = R$, we know there exists an $i \in I$ and a $j \in J$ such that $1 = i + j$. Note, then, that:

$$\begin{aligned}r &= r \cdot 1 \\ &= r \cdot (i + j) \\ &= r \cdot i + r \cdot j.\end{aligned}$$

Since $r \in J$ and R is commutative, we know that $ri \in IJ$, and since $r \in J$, we also know that $rj \in IJ$. Hence $r = ri + rj \in IJ$, and so $I \cap J \subseteq IJ$. Therefore, $IJ = I \cap J$, as desired. ■

Problem 4.6. Let I, J be ideals in a commutative ring R. Assume that $R/(IJ)$ is reduced (that is, it has no nonzero nilpotent elements). Prove that $IJ = I \cap J$.

Solution. We will proceed by proving the contrapositive. Since we already know that $IJ \subseteq I \cap J$ for any ideals I, J, assume that $I \cap J \not\subseteq IJ$. There then exists an $r \in I \cap J$ with $r \notin IJ$; that is, such that the coset $r + (IJ)$ is nonzero in $R/(IJ)$. Note, then, that $r^2 = rr \in IJ$, since $r \in I$ and $r \in J$, and so $(r + IJ)^2 = 0$ in the ring $R/(IJ)$. Hence $R/(IJ)$ is not reduced, as desired.

Therefore, if $R/(IJ)$ is reduced, then $I \cap J \subseteq IJ$, and therefore $I \cap J = IJ$. ■

Problem 4.7. Let $R = k$ be a field. Prove that every nonzero (principal) ideal in $k[x]$ is generated by a unique monic polynomial.

Solution. Let I be an ideal of $k[x]$. Then, by exercise 4.4, there is a monic polynomial $p_1 \in k[x]$ such that $I = (p_1)$. Let $p_2 \in k[x]$ be such that $(p_2) = (p_1) = I$. Then, since $p_1 \in (p_2)$ and $p_2 \in (p_2)$, there exist q_1 and q_2 such that

$$p_1 = q_1 p_2$$

and

$$p_2 = q_2 p_1.$$

We then have

$$p_1 = q_1 q_2 p_1,$$

and hence $q_1 q_2 = 1$, as $k[x]$ is an integral domain.

Note, then, that

$$\begin{aligned} 0 &= \deg(q_1 q_2) \\ &=^1 \deg(q_1) + \deg(q_2), \end{aligned}$$

where equality (1) follows from $k[x]$ being an integral domain and thus having no nonzero zero divisors. Therefore, q_1 and q_2 are both degree 0, that is, constants.

It then follows that if p_2 is monic, then $q_1 = 1$ and so $p_1 = p_2$, showing that I is generated by a unique *monic* polynomial as desired. ■

Problem 4.8. Let R be a ring and $f(x) \in R[x]$ a monic polynomial. Prove that $f(x)$ is not a (left- or right-) zero divisor.

Solution. Let $g(x) \in R[x]$, be a nonzero polynomial and a be the leading coefficient of $g(x)$. Since $f(x)$ is monic, the leading coefficient of $f(x)g(x)$ and $g(x)f(x)$ is $1 \cdot a = a \cdot 1 = a$. Hence, if either one of these polynomials is zero, then $a = 0$. Since $a \neq 0$ as $g(x)$ is nonzero, neither of these polynomials is zero. Hence $f(x)$ is not a left- or right- zero divisor. ■

Problem 4.10. Let d be an integer that is not the square of an integer, and consider the subset of $\mathbb{C}$ defined by

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

(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 $z \in \mathbb{Q}(\sqrt{d}), z \neq 0$.

The function N is a 'norm'; it is very useful in the study of $\mathbb{Q}(\sqrt{d})$ and of its subrings.

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

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

Solution. First, we prove that $\mathbb{Q}(\sqrt{d})$ is a subring of $\mathbb{C}$. If $a+b\sqrt{d}$ and $x+y\sqrt{d}$ are elements of $\mathbb{Q}(\sqrt{d})$, then we have

$$\begin{aligned}(a + b\sqrt{d}) + (x + y\sqrt{d}) &= (a + b) + (x + y)\sqrt{d} \\ &\in \mathbb{Q}(\sqrt{d})\end{aligned}$$

and

$$\begin{aligned}(a + b\sqrt{d})(x + y\sqrt{d}) &= ax + ay\sqrt{d} + bx\sqrt{d} + bdy \\ &= (ax + bdy) + (ay + bx)\sqrt{d} \\ &\in \mathbb{Q}(\sqrt{d}).\end{aligned}$$

Of course $1 = 1 + 0\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, so $\mathbb{Q}(\sqrt{d})$ is a ring.

Now, define $N : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}$ as in the question. Let $z = z_1 + z_2\sqrt{d}$ and $w = w_1 + w_2\sqrt{d}$. We then have:

$$\begin{aligned}N(zw) &= N((z_1w_1 + z_2w_2d) + (z_1w_2 + z_2w_1)\sqrt{d}) \\ &= (z_1w_1 + z_2w_2)^2 - (z_1w_2 + z_2w_1)^2 d \\ &= z_1^2w_1^2 - z_1^2w_2^2d - z_2^2w_1^2d + z_2^2w_2^2d^2 \\ &= (z_1^2 - z_2^2d)(w_1^2 - w_2^2d) \\ &= N(z)N(w).\end{aligned}$$

Of course $z = 0$ implies $N(z) = 0$, so $N(z) \neq 0$ implies $z \neq 0$.

For part (c), let $z = a + b\sqrt{d}$ be a nonzero element of $\mathbb{Q}(\sqrt{d})$. Since $N(z) \in \mathbb{Q}$ and is nonzero because z is nonzero, we know that

$$\begin{aligned}w &= \frac{a - b\sqrt{d}}{N(z)} \\ &= \frac{a}{N(z)} - \frac{b}{N(z)}\sqrt{d} \\ &\in \mathbb{Q}(\sqrt{d}),\end{aligned}$$

and so we find that

$$\begin{aligned} zw &= \left(a + b\sqrt{d}\right)\left(\frac{a - b\sqrt{d}}{N(z)}\right) \\ &= \frac{N(z)}{N(z)} \\ &= 1, \end{aligned}$$

showing that w is a multiplicative inverse of z, and hence that $\mathbb{Q}(\sqrt{d})$ is a field.

Any subfield of $\mathbb{C}$ that conatins $\mathbb{Z}$ and $\sqrt{d}$ must contain $\mathbb{Q}(\sqrt{d})$, since subfields must be closed under the field operations. Hence $\mathbb{Q}(\sqrt{d})$ is the smallest such subfield.

Finally, Let $\varphi : \mathbb{Q}[x] \to \mathbb{Q} \oplus \mathbb{Q}$ be the group homomorphism (defined in the book) that sends $g(x) \in \mathbb{Q}[x]$ to the pair (r_0, r_1), where r_0, r_1 come from the remainder $r_0 + r_1 x$ when dividing $g(x)$ by the polynomial $x^2 - d$.

An argument in the book establishes that φ is surjective with kernel equal to the principle ideal $(x^2 - d)$, and so we have

$$\frac{\mathbb{Q}[x]}{(x^2 - d)} \cong \mathbb{Q} \oplus \mathbb{Q},$$

as abelian groups.

All we need to do, now, is endow $\mathbb{Q} \oplus \mathbb{Q}$ with a ring structure that makes φ a homomorphism, and show that this ring is isomorphic to $\mathbb{Q}(\sqrt{d})$. Define an operation $\cdot$ on $\mathbb{Q} \oplus \mathbb{Q}$, then, by

$$(a_0, a_1) \cdot (b_0, b_1) = \varphi\left(\varphi^{-1}(a_0, a_1) \cdot \varphi^{-1}(b_0, b_1)\right),$$

where $\overline{p(x)}$ is the coset of $p(x)$ in the quotient ring $\mathbb{Q}[x]/(x^2 - d)$. Note that this is well-defined because φ is a bijection.

To prove that φ is then a ring homomorphism $\dfrac{\mathbb{Q}[x]}{(x^2 - d)} \to \mathbb{Q} \oplus \mathbb{Q}$, note that:

$$\begin{aligned} \varphi^{-1}(a \cdot b) &= \varphi^{-1}\left(\varphi(\varphi^{-1}(a) \cdot \varphi^{-1}(b))\right) \\ &= \varphi^{-1}(a) \cdot \varphi^{-1}(b), \end{aligned}$$

from which it then follows that φ preserves multiplication.

The reader way wish to note, additionally, that the identity with respect to this multiplication defined on $\mathbb{Q} \oplus \mathbb{Q}$, is the pair $(0, 1)$, as we have, for $a_0, a_1 \in \mathbb{Q}$:

$$\begin{aligned} (1, 0) \cdot (a_0, a_1) &= \varphi\left(\varphi^{-1}(0, 1) \cdot \varphi^{-1}(a_0, a_1)\right) \\ &= \varphi((\overline{1}) \cdot (\overline{a_0 + a_1 x})) \\ &= \varphi(\overline{1(a_0 + a_1 x)}) \\ &= \varphi(a_0 + a_1 x) \\ &= (a_0, a_1), \end{aligned}$$

where each step follows from simple considerations concerning polynomial division by a polynomial of degree 2, and the properties of ideals with respect to the ring operations.

Since the remainder when dividing 1 by the polynomial $x^2 - d$ is 1, we then know that $\varphi(1) = (1, 0)$, showing that φ preserves the identity with respect to multiplication.

Since φ is a bijection that preserves addition, multiplication, and the identity as defined on $\mathbb{Q} \oplus \mathbb{Q}$, we then know that $\mathbb{Q} \oplus \mathbb{Q}$ is a ring isomorphic to the ring $\mathbb{Q}[x]/(x^2 - d)$.

To characterize this multiplication on $\mathbb{Q} \oplus \mathbb{Q}$, we find with some algebra that

$$\begin{aligned}
(a_0 + a_1) \cdot (b_0 + b_1) &= \varphi\left(\varphi^{-1}(a_0, a_1) \cdot \varphi^{-1}(b_0, b_1)\right) \\
&= \varphi\left((\overline{a_0 + a_1x}) \cdot (\overline{b_0 + b_1x})\right) \\
&= \varphi\left(\overline{(a_0 + a_1x)(b_0 + b_1x)}\right) \\
&= \varphi(\overline{a_0b_0 + (a_0b_1 + a_1b + 0)x + a_1b_1x^2}) \\
&= \varphi(\overline{(a_0b_0 + a_1b_1d) + (a_0b_1 + a_1b_0)x + (x^2 - d)(a_1b_1)}) \\
&= \varphi(\overline{(a_0b_0 + a_1b_1d) + (a_0b_1 + a_1b_0)x}) \\
&= (a_0b_0 + a_1b_1d, a_0b_1 + a_1b_0).
\end{aligned}$$

Inspection of the product $(a_0 + a_1\sqrt{d})(b_0 + b_1\sqrt{d})$ quite easily shows that the mapping $(a_0, a_1) \mapsto a_0 + a_1\sqrt{d}$ is a ring isomorphism $\mathbb{Q} \oplus \mathbb{Q} \to \mathbb{Q}(\sqrt{d})$, and so we therefore get the isomorphism $\mathbb{Q}[x]/(x^2 - d) \cong \mathbb{Q}(\sqrt{d})$, as desired. ■

Problem 4.11. Let R be a commutative ring, $a \in R$, and $f_1(x), \ldots, f_r(x) \in R[X]$.

(a) Prove the equality of ideals

$$(f_1(x), \ldots, f_r(x), x - a) = (f_1(a), \ldots, f_r(a), x - a)\,.$$

(b) Prove the useful substitution trick

$$\frac{R[x]}{(f_1(x), \ldots, f_r(x), x - a)} \cong \frac{R}{(f_1(a), \ldots, f_r(a))}.$$

Solution. First, suppose $f(x) \in R[x]$ and $a \in R$. If we divide $f(x) - f(a)$ by the polynomial $x - a$, we find that

$$f(x) - f(a) = q(x)(x - a) + r(x),$$

where $q(x), r(x) \in R[x]$ and $\deg r(x) = 0$. Evaluating both sides at a, we then can see that

$$\begin{aligned}
f(a) - f(a) &= q(a)(a - a) + r(a) \\
\Rightarrow 0 &= r(a),
\end{aligned}$$

meaning $r(x)$ must be the zero polynomial since it has degree zero and evaluates to zero at a. Thus, we have:

$$f(x) = q(x)(x - a) + f(a)$$

for all $f(x) \in R[x], a \in R$ and some polynomial $q(x)$.

Applying this to our problem, we then have polynomials q_j such that

$$f_j(x) = q_j(x)(x - a) + f_j(a),$$

for all $1 \leq j \leq r$.

We then have, for all polynomials of the form shown on the left-hand side in the ideal $(f_1(x), \dots, f_r(x), x-a)$,

$$\begin{aligned}\left(\sum_{j=0}^{r} p_j(x)f_j(x)\right) + g(x)(x-a) &= \left(\sum_{j=0}^{r} p_j(x)(q_j(x)(x-a)) + f_j(a)\right) + g(x)(x-a)\\ &= \sum_{j=1}^{r} f_j(a) + \left(g(x) + \sum_{j=1}^{n} q_j(a)\right)(x-a),\end{aligned}$$

and so $(f_1(x), \dots, f_r(x), x-a) \subseteq (f_1(a), \dots, f_r(a), x-a)$. A nearly identical argument gives us the inclusion in the other direction, and so we have the desired equality of ideals.

With this shiny new lemma, we can now see that

$$\begin{aligned}\frac{R[x]}{(f_1(x), \dots, f_r(x), x-a)} &= \frac{R[x]}{(f_1(a), \dots, f_r(a), x-a)}\\ &= \frac{R[x]}{(f_1(a), \dots, f_r(a)) + (x-a)}\\ &\cong \frac{R[x]/(x-a)}{(f_1(a), \dots, f_r(a))}\\ &\cong \frac{R}{(f_1(a), \dots, f_r(a))},\end{aligned}$$

where the first equality follows from the lemma we just proved, the second equality follows from the definition of an ideal generated by multiple elements, the isomorphism in the third line follows from Exercise 3.3, and the isomorphism in the fourth line follows from the isomorphism

$$\frac{R[x]}{(x-a)} \cong R.$$

■

Problem 4.12. Let R be a commutative ring and $a_1, \dots, a_n$ elements of R. Prove that

$$\frac{R[x_1, \dots, x_n]}{(x_1 - a_1, \dots, x_n - a_n)} \cong R$$

Solution. We will proceed by induction. For the base case $n = 1$, the isomorphism

$$\frac{R[x]}{(x-a)}$$

has already been established. For the induction step, suppose we have the isomorphism

$$\frac{R[x_1, \dots, x_n]}{(x_1 - a_1, \dots, x_n - a_n)}$$

for $a_1, \dots, a_n \in R$, and let $a_{n+1} \in R$. We then have:

$$\begin{aligned}
\frac{R[x_1, \dots, x_n, x_{n+1}]}{(x_1 - a_1, \dots, x_n - a_n, x_{n+1} - a_{n+1})} &= \frac{R[x_1, \dots, x_n][x_{n+1}]}{(x_1 - a_1, \dots, x_n - a_n) + (x_{n+1} - a_{n+1})} \\
&\cong \frac{R[x_1, \dots, x_n][x_{n+1}]/(x_{n+1} - a_{n+1})}{(x_1 - a_1, \dots, x_n - a_n)} \\
&\cong \frac{R[x_1, \dots, x_n]}{(x_1 - a_1, \dots, x_n - a_n)} \\
&\cong R.
\end{aligned}$$

Here, the equality in the first line follows from the definition of multivariate polynomial rings and finitely generated ideals, the isomorphism in the second line follows from Exercise 3.3, the isomorphism in the third line follows from the general isomorphism $R[x]/(x-a) \cong R$, and the isomorphism in the fourth line follows from the inductive hypothesis. ■

Problem 4.13. Let R be an integral domain. For all $k = 1, \dots, n$, prove that $(x_1, \dots, x_k)$ is prime in $R[x_1, \dots, x_n]$.

Solution. This follows immediately from the previous exercise, and the fact that the ideal $I \subseteq R$ is prime iff R/I is an integral domain. ■

Problem 4.14. Prove 'by hand' that maximal ideals are prime, *without* using quotient rings.

Solution. We will assume that the ring R is commutative, since this is the only case in which the book deals with prime and maximal ideals (and because it makes things more convenient). We will also assume that R is nonzero, as the result is immediate otherwise.

Let I be a maximal ideal, and let J be the subset of R defined by

$$J = \{a \in R \mid (\exists b \in R \setminus I) : ab \in I\}$$

Since I is maximal, it does not contain the identity (by definition), and so $a \in I$ implies $a \cdot 1_R \in I$, making it clear that $I \subseteq J$.

Note, then, that if $a \in J$ so that $b \in R \setminus I$ is such that $ab \in I$, then for any $r \in R$, we have:

$$\begin{aligned}
(ra)b &= r(ab) \\
&\in I,
\end{aligned}$$

and so J is actually an ideal of R. Because $1 \notin J$ (as $1r \in I$ implies $r \in I$), this means that $J = I$, since J contains I and I is maximal.

For the slam dunk, observe that if $a, b \in R$ are such that $ab \in I$ and $b \notin I$, then $a \in J$ by definition, and so $a \in I$, proving that I is a prime ideal. ■

Problem 4.15. Let $\varphi : R \to S$ be a homomorphism of commutative rings, and let $I \subseteq S$ be an ideal. Prove that if I is a prime ideal in S, then $\varphi^{-1}(I)$ is a prime ideal in R. Show that $\varphi^{-1}(I)$ is not necessarily maximal if I is maximal.

Solution. Let $J \subseteq R$ be the preimage of I, $J = \varphi^{-1}(I)$. Note that $r \in R, a \in J$ implies $\varphi(ra) = \varphi(r)\varphi(a) \in I$, and so J is an ideal of R. Then, if $a, b \in R$ are such that $ab \in J$, then $\varphi(ab) = \varphi(a)\varphi(b) \in I$, which implies $\varphi(a) \in I$ or $\varphi(b) \in I$ (since I is prime), which implies $a \in J$ or $b \in J$; hence J is prime. ■

Problem 4.16. Let R be a commutative ring, and let P be a prime ideal of R. Suppose 0 is the only zero-divisor of R contained in P. Prove that R is an integral domain.

Solution. Suppose R is not an integral domain. Then there exist $a, b \in R$, both nonzero, such that $ab = 0$. If P is a prime ideal in R, then $ab \in P$ since 0 is contained in every ideal of R, and so we know $a \in P$ or $b \in P$. Hence, 0 is not the only zero-divisor of R contained in P, proving the contrapositive of the desired result. ■

Problem 4.18. Let R be a commutative ring, and let N be its nilradical. Prove that N is contained in every prime ideal of R.

Solution. Let $a \in N$, so that $a^n = 0$ for some integer n. If P is a prime ideal of R, then we have

$$\begin{aligned} 0 &= (a^n + P) \\ &= (a + P)^n \end{aligned}$$

in the ring R/P, and so $(a + P) = 0$ as R/P is an integral domain, meaning $a \in P$. ■

Problem 4.19. Let R be a commutative ring, let P be a prime ideal in R, and let I_j be ideals of R.

(a) Assume that $I_1 \cdots I_r \subseteq P$; prove that $I_J \subseteq P$ for some j.

(b) By (a), if $P \supseteq \bigcap_{j=1}^{r} I_j$, then P contains one of the ideals I_j. Prove or disprove: if $P \supseteq \bigcap_{j=1}^{\infty} I_j$, then P contains one of the ideals I_j.

Solution. Let $I_2, \ldots, I_n$ be ideals that are not subsets of P, and assume $I_1, \ldots, I_n \subseteq P$, so that $i_1 \cdots i_n \in P$ for all $i_j \in I_j$. An argument by induction then shows that $i_j \in P$ for some j, since P is prime. If we fix $i_2, \ldots, i_n$ such that each of these are not in P (since $I_2, \ldots, I_n$ are not subsets of P), it then follows that $i_1 \in P$, for all $i_1 \in I_1$; hence $I_1 \subseteq P$.

On the other hand, if $I_1, I_2, \ldots$ are ideals of R and $P \supseteq \bigcap_{j=1}^{\infty} I_j$, then it does not necessarily follow that P contains one of the ideals j. For a counterexample, let $R = \mathbb{Z}$, let $\mathcal{I} = \{n\mathbb{Z} : n \text{ is odd}\}$ and let $P = 2\mathbb{Z}$. Then $\bigcap \mathcal{I} = \varnothing \subseteq P$, but P doesn't contain any of the ideals in $\mathcal{I}$. ■

Problem 4.20. Let Mbe a two-sided ideal in a (not necessarily commutative) ring R. Prove that M is maximal if and only if R/M is a simple ring.

Solution. First suppose M is maximal. Then R/M is a field, which is simple.

Conversely, suppose R/M is a simple ring. Note that every ideal of R/M is of the form J/M for some ideal J of R containing M, and every ideal J of R containing M gives rise to an ideal J/M of R/M. With this correspondence in mind, we know that since R/M is simple, the only ideals of R/M are $\{0\}/M$ and R/M, and so the only ideals of R containing M are (0) and R itself. Hence M is maximal in R. ■

Problem 4.21. Let k be a algebraically closed field, and let $I \subseteq k[x]$ be an ideal. Prove that I is maximal if and only if $I = (x - c)$ for some $c \in k$.

Solution. One direction is obvious: If $I = (x - c)$ for some c, then $k[x]/(x - c) \cong k$ is a field, and so I is maximal.

On the other hand, since k is a field, we know $k[x]$ is a PID, and so there exists some $f(x) \in k[x]$ such that $I = (f(x))$. Assume, then, that $I \neq R$ and $\deg f(x) \neq 1$, and so $\deg f(x) > 1$. Since k is algebraically closed, the equation $f(x) = 0$ has a solution $c \in k$. Note, then, that if we divide $f(x)$ by the polynomial $x - c$, we obtain

$$f(x) = (x - c)q(x) + r(x)$$

for some $q(x), r(x) \in k[x]$ with $\deg r(x) = 0$. Evaluating each side at $x = c$, we find that $r(c) = 0$, and so $r(x) = 0$; hence $f(x) = (x - c)q(x)$.

Notice that from this equation, we can see that $\deg f(x) = \deg q(x) + 1$. Since k is a field and hence has no zero divisors, we can then conclude that

$$(f(x)) \subsetneq (q(x)),$$

as it is clear that $(f(x)) \subseteq (q(x))$, and we can see that $q(x) \notin (f(x))$ since $\deg q(x) > \deg f(x)$ and k is an integral domain. Therefore $(q(x))$ is an ideal that strictly contains I and is not equal to the whole ring R, meaning I is not maximal, giving us the contrapositive of the desired result. ■

Problem 4.22. Prove that $(x^2 + 1)$ is maximal in $\mathbb{R}[x]$.

Solution. The ring $\mathbb{R}[x]/(x^2+1)$ is isomorphic to $\mathbb{C}$, which is a field, so (x^2+1) is maximal. ■

Problem 4.23. A ring R has Krull dimension 0 if every prime ideal in R is maximal. Prove that fields and Boolean rings have Krull dimension 0.

Solution. Of course fields have Krull dimension 0, since the only proper ideal of a field is the zero ideal (0), which is prime and hence maximal as fields are PIDs.

If R is a boolean ring and P is a prime ideal of R, then R/P is an integral domain by definition. Since R is boolean, we have, for all $a \in R$,

$$\begin{aligned}(a + I)^2 &= a^2 + I \\ &= a + I,\end{aligned}$$

and so R/P is boolean as well. It then follows, by Exercise 3.15, $R/P \cong \mathbb{Z}/2\mathbb{Z}$ since R/P is a boolean integral domain. Hence R/P is a field, and so has Krull dimension 0 as desired. ■

Problem 4.24. Prove that the ring $\mathbb{Z}[x]$ has Krull dimension ≥ 2.

Solution. We consider the ideals (x) and (x, p) (for $p \in \mathbb{Z}$ prime) of $\mathbb{Z}[x]$. Note that:

$$\frac{\mathbb{Z}[x]}{x} \cong \mathbb{Z},$$

and

$$\begin{aligned}\frac{\mathbb{Z}[x]}{(x,p)} &\cong \frac{\mathbb{Z}[x]/(x)}{(p)}\\ &\cong \frac{\mathbb{Z}}{(p)}\\ &= \mathbb{Z}/p\mathbb{Z},\end{aligned}$$

and so (x) is prime and (x, p) is maximal (and thus prime).

The chain of proper inclusions of prime ideals

$$0 \subsetneq (x) \subsetneq (x, p)$$

then shows that $\mathbb{Z}[x]$ has Krull dimension at least 2. ■