# ALGEBRA HW 9

CLAY SHONKWILER

## 1

Let $I_1, \ldots, I_n \subset R$ be ideals in a commutative ring $R$.

**(a):** Show that $\prod_{j=1}^n I_j = \bigcap_{j=1}^n I_j$ if the ideals are pairwise relatively prime. Explain this assertion geometrically in the case $R = \mathbb{C}[x, y]$.

*Proof.* By induction. Note that

$$\prod_{j=1}^n I_j \subset \bigcap_{j=1}^n I_j,$$

so we need only show the reverse inclusion. Now, recall that we showed in class that, if $I, J$ relatively prime, then there exist $i \in I$, $j \in J$ such that $i + j = 1$ and so, if $a \in I \cap J$,

$$a = a(i + j) = ai + aj \in IJ.$$

For the induction step, suppose that for all collections $I_1, \ldots, I_k$ of pairwise relatively prime ideals that $\bigcap_{j=1}^n I_j \subset \prod_{j=1}^n I_j$. Then let $I_1, \ldots, I_{k+1}$ be a collection of pairwise relatively prime ideals. Then

$$\bigcap_{j=1}^{k+1} I_j = \left( \bigcap_{j=1}^{n} I_j \right) \cap I_{k+1} = \left( \prod_{j=1}^{k} I_j \right) \cap I_{k+1}$$

by the inductive hypothesis. Now, since the $I_j$ are pairwise relatively prime, there exist $a_i \in I_i$ and $b_i \in I_{k+1}$ such that

$$a_i + b_i = 1$$

for all $i = 1, \ldots, k$. Then

$$1 = \prod_{i=1}^{k} (a_i + b_i) = a_1 \cdots a_k + B$$

where $B$ is a summation. Now, each term in the summation $B$ has some $b_j$ as a factor, so $B \in I_{k+1}$. Now, if $a \in \bigcap_{j=1}^{k+1} I_j$, then

$$a = a(a_1 \cdots a_k + B) = a a_1 \cdots a_k + aB \in \prod_{j=1}^{k+1} I_j.$$

Therefore, we conclude, by induction, that $\bigcap_{j=1}^n I_j \subset \prod_{j=1}^n I_j$ for all $n$, which suffices to show that

$$\prod_{j=1}^{n} I_j = \bigcap_{j=1}^{n} I_j.$$

In $\mathbb{C}[x, y]$, this means that if the union of the zero loci of relatively prime polynomials is equal to the zero locus of the the product of the polynomials. For example, if we consider the relatively prime ideals $(x)$ and $(y)$, then the zero loci of these polynomials are the $y$-axis and the $x$-axis. The product ideal is $(xy)$, which has as its zero locus the union of the $y$-axis and the $x$-axis. □

**(b):** Let $\phi : R \to \prod_{j=1}^n R/I_j$ be the map obtained by reducing modulo each $I_j$. Must this map be injective? surjective? an isomorphism? Give examples to show the possibilities, and prove a necessary and sufficient condition for $\phi$ to be an isomorphism.

**Answer:** In general, the answer to all these questions is no, but there are cases for which the answer is yes. To see that $\phi$ is not necessarily injective, consider $R = \mathbb{Z}$ and $I_1 = 2\mathbb{Z}$. Then $\phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ is just reduction modulo 2, so $\phi(1) = \phi(3) = 1$, so this map is not injective, though it is surjective.

To see that $\phi$ is not necessarily surjective, consider $R = \mathbb{Z}$, $I_1 = 2\mathbb{Z}$, $I_2 = 4\mathbb{Z}$. Then $\phi : \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is just reduction modulo 2 and 4, respectively, in each coordinate. Now, there is no element $a \in \mathbb{Z}$ such that

$$\phi(a) = (1, 2),$$

as this would necessitate that $a \equiv 1 \mod 2$ and $a \equiv 2 \mod 4$, which is clearly imposible. This map isn't injective either, as $\phi(1) = (1, 1) = \phi(5)$.

Clearly, neither of the above maps is an isomorphism. On the other hand, if $R = \mathbb{Z}/6\mathbb{Z}$ and $I_1 = (2)$, $I_2 = (3)$, then we see that

$$R/I_1 \times R/I_2 = (\mathbb{Z}/6\mathbb{Z})/(2) \times (\mathbb{Z}/6\mathbb{Z})/(3) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

so certainly $R \simeq R/I_1 \times R/I_2$. In fact,

$$\begin{aligned} \phi(0) &= (0, 0) \\ \phi(1) &= (1, 1) \\ \phi(2) &= (0, 2) \\ \phi(3) &= (1, 0) \\ \phi(4) &= (0, 1) \\ \phi(5) &= (1, 2), \end{aligned}$$

so $\phi$ is bijective. Furthermore, since addition and multiplication are preserved by modular arithmetic, this is, in fact, an isomorphism.

Now, we prove the following proposition:

**Proposition 0.1.** *$\phi$ is an isomorphism if and only if the $I_j$ are pairwise relatively prime and $\bigcap_{j=1}^n I_j = 0$.*

*Proof.* Note, first of all that $\phi$ is certainly a ring homomorphism since it is just the natural projection of $R$ onto $R/I_j$ in each component, so it suffices to show bijectivity. Furthermore, if $\phi(a) = 0$, then $a \in I_j$ for all $j = 1, \ldots, n$, so $\ker \phi = \bigcap_{j=1}^n I_j$. Therefore, if $\phi$ is injective, then $\bigcap_{j=1}^n I_j = 0$ and, conversely, if $\bigcap_{j=1}^n I_j = 0$, then $\phi$ is injective. Hence, it remains only to show surjectivity in the reverse direction and that the $I_j$ are relatively prime in the forward direction, which we will do by induction.

Taking the reverse direction first, suppose $I, J$ are relatively prime and that $(a \mod I, b \mod J) \in R/I \times R/J$. Since $I$ and $J$ are relatively prime, there exist $x \in I$, $y \in J$ such that $x + y = 1$. Then $x = 1 - y \equiv 1 \mod J$ and $y = 1 - x \equiv 1 \mod I$, so

$$\phi(x) = (0, 1) \quad \phi(y) = (1, 0).$$

Hence, since $\phi$ is a ring homomorphism,

$$\begin{aligned} \phi(bx + ay) &= \phi(b)\phi(x) + \phi(a)\phi(y) \\ &= (b \mod I, b \mod J)(0, 1) + (a \mod I, a \mod J)(1, 0) \\ &= (0, b \mod J) + (a \mod I, 0) \\ &= (a \mod I, b \mod J), \end{aligned}$$

so $\phi$ is, indeed, surjective.

The induction follows directly from what we showed in part (a). To see why, suppose we have relatively prime ideals $I_1, \ldots, I_n$. Then $I = I_1$ and $J = \bigcap_{j=2}^n I_j$ are relatively prime by what we showed in the proof of (a) so we simply repeat the base case above for these values of $I$ and $J$. Therefore, we see that if $\bigcap_{j=1}^n I_j = 0$ and the $I_j$ are relatively prime, then $\phi$ is a surjection and, hence, an isomorphism.

On the other hand, we want to show that if$\phi : R \to \prod_{j=1}^n R/I_j$ is an isomorphism then $\bigcap_{j=1}^n I_j = 0$ and the $I_j$ are pairwise relatively prime. We already showed the first above, using only the fact that $\phi$ is injective. To show the second, let us prove the contrapositive. Suppose the $I_j$ are not pairwise relatively prime. Then there exist $i, j$ such that $I_i$, $I_j$ are not relatively prime. That is, there is no solution to the equation $x + y = 1$ for $x \in I_i$, $y \in I_j$. Specifically, this means that there is no element $x \in I_i$ such that $x = 1 + y$ for any $y \in I_j$, because if there were, then $x + (-y) = (1 + y) - y = 1$. Hence, there is no $a \in R$ such that

$$\phi(a) = (0, \ldots, 0, 1, 0, \ldots, 0)$$

where the single 1 is in the $j$th spot, because if there were, it would be the case that $a \in I_i$ and $a = 1 + y$ for some $y \in I_j$. Therefore, we see that $\phi$ is not surjective and thus not an isomorphism. Hence,

we conclude that if $\phi$ is an isomorphism, then the $I_j$ are relatively prime. □

## 2

If $I, J \subset R$ are ideals in a commutative ring, define the *ideal quotient* $(I : J) \subset R$ to be $\{a \in R | aJ \subset I\}$. Show that this is an ideal. If $R = \mathbb{Z}$, prove that $((m) : (n)) = (m/\gcd(m, n))$.

*Proof.* Let $a \in (I : J)$ and $b \in R$. Since $R$ is commutative,

$$abJ = baJ = b(aJ) \subset bI \subset I,$$

so $ab = ba \in (I : J)$, so $(I : J)$ is an ideal.

Now, suppose $R = \mathbb{Z}$ and $m, n \in \mathbb{Z}$. Then, if $d = \gcd(m, n)$, suppose $a \in (m/d)$. Then $a = \frac{bm}{d}$ for some $b \in \mathbb{Z}$. Furthermore, $m/d = c$ for some integer $c$, so

$$a(n) = \frac{bm}{d}(n) = bc(n) \subset (n),$$

so $a \in ((m) : (n))$ and, hence, $(m/d) \subset ((m) : (n))$.

On the other hand, if $a \in ((m) : (n))$, then $a(n) \subset (m)$, so there exists $c \in \mathbb{Z}$ such that $an = cm$. Hence, $a = \frac{cm}{n}$. Now, if $n$ divides $c$, then this implies that $a \subset (m) \subset (m/d)$. On the other hand, if $n$ does not divide $c$, then it must be the case that $n = xy$ where $x$ divides $c$ and $y$ divides $m$. Then $c/x = z$ for some integer $z$, so

$$a = z\frac{m}{y} \in (m/y) \subset (m/d),$$

since $d$ is the gcd of $m$ and $n$ and must, therefore, divide the common divisor $y$. This, then, demonstrates that $((m) : (n)) \subset (m/d)$; since containment holds both ways, we conclude that $((m) : (n)) = (m/d)$. □

## 3

**(a):** Is the Jacobsen radical always a radical ideal? Is the nilradical?

**Answer:** Let $R$ be a ring and let Jac $R$ denote the Jacobson radical. Then

$$\text{Jac } R = \bigcap_{\mathfrak{m} \text{ maximal in } R} \mathfrak{m}.$$

Now, suppose $a \in$ Jac $R$. Then $a^1 \in$ Jac $R$, so $a \in \sqrt{\text{Jac } R}$, so Jac $R \subset \sqrt{\text{Jac } R}$. On the other hand, suppose $a \in \sqrt{\text{Jac } R}$. Then $a^n \in$ Jac $R$ for some $n > 0$. Hence, $a^n \in \cap_{\mathfrak{m}}\mathfrak{m}$, so $a^n \in \mathfrak{m}$ for all maximal ideals $\mathfrak{m}$. Since maximal ideals are prime, this implies that $a \in \mathfrak{m}$ for all maximal $\mathfrak{m}$, so $a \in \cap_{\mathfrak{m}}\mathfrak{m} =$ Jac $R$. Therefore, $\sqrt{\text{Jac } R} \subset$ Jac $R$. Since containment goes both ways, we see that Jac $R = \sqrt{\text{Jac } R}$, so the Jacobson radical is a radical ideal.

Now, the nilradical Nil $R = \sqrt{(0)}$, and, since $\sqrt{\cdot}$ is a closure operator,

$$\sqrt{\text{Nil } R} = \sqrt{\sqrt{(0)}} = \sqrt{(0)} = \text{Nil } R,$$

so the nilradical is a radical ideal.

♣

**(b):** In each of the following rings, find the Jacobsen radical, the nilradical, and the set of units. Also determine if the ring is local. $\mathbb{R}[x,y]$, $\mathbb{R}[[x,y]]$, $\mathbb{R}[x,y]/(y^3)$, $\mathbb{R}[x,y]/(xy)$, $\mathbb{R}[x,y]/(xy,y^3)$, $\mathbb{R}[x][[y]]$, $\mathbb{R}[[y]][x]$.

**Answer:** $\mathbb{R}[x,y]$: Since $\mathbb{R}[x,y]$ is an integral domain, its nilradical is zero. Furthermore, since any ideal of the form $(f(x,y), g(x,y))$ where $f$ and $g$ are irreducible and have no relations between them is maximal, we see that the intersection of the maximal ideals is just the zero ideal, so the Jacobson radical is also (0). Finally, the units in $\mathbb{R}[x,y]$ are simply the non-zero elements of $\mathbb{R}$. Furthermore, it's clear that $\mathbb{R}[x,y]$ is not local, since we just saw that there are lots of maximal ideals

$\mathbb{R}[[x,y]]$: Elements in $\mathbb{R}[[x,y]]$ are of the form

$$\sum_{i,j} a_{i,j} x^i y^j;$$

define the order of $f$ to be $i_0 + j_0$ where $i_0 + j_0$ is the smallest such sum such that $a_{i_0,j_0} \neq 0$ (this may well be non-unique). Then, just as in PS6#4(a), if $f, g \in \mathbb{R}[[x,y]]$, $\text{ord}(f \cdot g) = \text{ord}(f) + \text{ord}(g)$. Note that $\text{ord}(1) = 0$. Then any invertible element in $\mathbb{R}[[x,y]]$ must have order 0. On the other hand, let $f \in \mathbb{R}[[x,y]]$ have order 0; we want to show that $f$ has an inverse. Let $g \in \mathbb{R}[[x,y]]$. Then

$$f = \sum_{i,j} a_{i,j} x^i y^j$$

with $a_{0,0} \neq 0$ and

$$g = \sum_{i,j} b_{i,j} x^i y^j$$

Then

$$fg = \left(\sum_{i,j} a_{i,j} x^i y^j\right)\left(\sum_{i,j} b_{i,j} x^i y^j\right) = \sum_{i,j} \sum_{k=0}^{i} \sum_{n=0}^{j} a_{k,n} b_{i-k,j-n} x^i y^j.$$

Now, if $fg = 1$, then

$$\begin{aligned} a_{0,0}b_{0,0} &= 1 \\ a_{0,0}b_{0,1} + b_{0,0}a_{0,1} &= 0 \\ a_{0,0}b_{1,0} + b_{0,0}a_{1,0} &= 0 \\ &\vdots \end{aligned}$$

Now, we can solve for $b_{0,0} = a_{0,0}^{-1}$ and then solve for $b_{0,1}$, $b_{1,0}$, etc. Hence, there is such a $g$, and so $f$ is invertible. Therefore we conclude that the units of $\mathbb{R}[[x,y]]$ are precisely those elements with non-zero constant terms. Therefore, all non-units must be contained in $(x,y)$, which is, therefore, the unique maximal ideal. Hence, $\mathbb{R}[[x,y]]$ is local and has Jacobson radical $(x,y)$. However, since $\mathbb{R}[[x,y]]$ is an integral domain, it has nilradical (0).

$\mathbb{R}[x,y]/(y^3)$: Note, first off, that $(y) \subset \text{Nil } \mathbb{R}[x,y]/(y^3)$, since $y^3 = 0$ in this ring. Furthermore, any polynomial with $x$ in it or a non-zero constant term cannot be in the nilradical, since the $x$ or the non-zero constant term will propagate through all powers, so the nilradical is exactly $(y)$. Now, suppose $ay^2 + by + c \in \mathbb{R}[x,y]/(y^3)$ such that $c \neq 0$. Then

$$\frac{-a}{c}\left(\frac{b}{a}y - \frac{c}{a}\right)(ay^2+by+c) = \frac{-a}{c}\left(by^3 + by^2 - by^2 + \frac{bc}{a}y - \frac{bc}{a}y - \frac{c}{a}\right) = \frac{-a}{c}\frac{-c}{a} = 1,$$

so all elements $f(y) \in \mathbb{R}[x,y]/(y^3)$ with non-zero constant term are units. Clearly no polynomials containing an $x$ can be units, so the set of units is simply $\mathbb{R} \cup (y)$. Hence, any ideal of the form $(g(x), y)$ with $g(x)$ irreducible is maximal, so the Jacobson radical is simply $(y)$. The fact that there are many maximal ideals demonstrates that this ring is not local.

$\mathbb{R}[x,y]/(xy)$: Note that, for $f(x), g(y)$ irreducible, $(f(x), g(y))$ is maximal, so the intersection of all maximal ideals, the Jacobson radical, must be (0). Hence, since the nilradical is contained in the Jacobson radical, the nilradical is also (0). The fact that there are many maximal ideals demonstrates that this ring is not local. Finally, since elements of $\mathbb{R}[x,y]/(xy)$ are simply polynomials either purely in $x$ or purely in $y$ or sums of such, there are no units in this ring except the non-zero scalars.

$\mathbb{R}[x,y]/(xy,y^3)$: Note that

$$\mathbb{R}[x,y]/(xy,y^3) = (\mathbb{R}[x,y]/(y^3))/(xy).$$

Since the nilradical in $\mathbb{R}[x,y]/(y^3)$ is $(y)$ and modding out by $(xy)$ does not introduce any new elements to the nilradical, the nilradical of this ring is also $(y)$. Similarly, since the units of $\mathbb{R}[x,y]/(y^3)$ are $\mathbb{R} \cup (y)$ and modding out by $(xy)$ doesn't introduce any new units, the units of $\mathbb{R}[x,y]/(xy,y^3)$ are just $\mathbb{R} \cup (y)$. Thus, ideals of the form $(f(x), y)$ for irreducible $f$ are maximal, so the Jacobson radical is also $(y)$. Finally, since we've just exhibited multiple maximal ideals, we see that this ring is not local.

$\mathbb{R}[x][[y]]$: Since $\mathbb{R}[x]$ is an integral domain, so is $\mathbb{R}[x][[y]]$, so the nilradical is (0). The proof given in PS6#4(b) that the units in $\mathbb{R}[[x]]$ are those elements with non-zero constant term only depended on the fact that the constant term was invertible; hence, the same proof

demonstrates the the units in $\mathbb{R}[x][[y]]$ are precisely those elements with invertible constant term. More precisely, suppose $f \in \mathbb{R}[x][[y]]$ has invertible constant term. Then

$$f = \sum_{i=0}^{\infty} f_i(x)y^i$$

where $f_0(x)$ is a non-zero constant $c$. Then, for $g = \sum g_i(x)y^i$,

$$fg = \left(\sum_{i=0}^{\infty} f_i(x)y^i\right)\left(\sum_{i=0}^{\infty} g_i(x)y^i\right) = \sum_{i=0}^{\infty}\left(\sum_{k=0}^{i} f_k(x)g_{i-k}(x)y^i\right).$$

Form the following system of equations:

$$\begin{aligned} cg_0(x) &= 1 \\ f_1(x)g_0(x) + f_0(x)g_1(x) &= 0 \\ &\vdots \\ \textstyle\sum_{k=0}^{i} f_k(x)g_{i-k}(x) &= 0 \end{aligned}$$

Then we can solve for $g_0(x) = c^{-1}$, since $c \neq 0$. Then

$$g_1(x) = \frac{-f_1(x)g_0(x)}{c^{-1}} = \frac{-f_1(x)c^{-1}}{c^{-1}} = -f_1(x)c^{-2}.$$

By induction, if $g_0, \ldots, g_{k-1}$ are determined in terms of the $f_i$, then

$$g_k(x) = c^{-1}(-f_1(x)g_{k-1}(x) - \ldots - f_k(x)g_0(x)).$$

Hence the above system admits a solution, which gives an inverse for $f$. Conversely, it's clear that any invertible element of $\mathbb{R}[x][[y]]$ must have invertible constant term, so we see that the units of $\mathbb{R}[x][[y]]$ are those elements with a non-zero constant polynomial for their constant term. Thus, maximal ideals in this ring are of the form $(f(x), y)$ where $f$ is irreducible, so $\mathbb{R}[x][[y]]$ has Jacobson radical equal to $(y)$ but is not a local ring.

$\mathbb{R}[[y]][x]$: Since $\mathbb{R}[[y]]$ is an integral domain, so is $\mathbb{R}[[y]][x]$, so the nilradical is (0). Now, for any commutative ring $R$, we know that the units in $R[x]$ are simply constant polynomials which are invertible in $R$. Hence, since the invertible elements of $\mathbb{R}[[y]]$ are those power series in $y$ with non-zero constant term, the units in $\mathbb{R}[[y]][x]$ are also simply power series in $y$ with non-zero constant term. Now, the only maximal ideal in $\mathbb{R}[[y]]$ is $(y)$; hence, all ideals of the form $(f(x), y)$ where $f(x) \in \mathbb{R}[[y]][x]$ is irreducible are maximal, so the Jacobson radical is contained in $(y)$. On the other hand, any maximal ideal in $\mathbb{R}[[y]][x]$ must contain $(y)$, else we could add in $(y)$ to get a proper ideal containing the original one. Hence, the Jacobson radical contains $(y)$. Since containment goes both ways, we see that the Jacobson radical is precisely $(y)$.

♣

**(c):** Prove that $\mathbb{R}[x]_{(x)} \subset \mathbb{R}[[x]]$, $\mathbb{R}[x,y]_{(x,y)}$, and $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$, but that $\mathbb{R}[x,y]_{(y)}$ is not a subring of the completion $\mathbb{R}[x][[y]]$. Explain.

*Proof.* Consider first $\mathbb{R}[x]_{(x)} = \mathbb{R}[x][\frac{1}{f(x)}|x \text{ does not divide } f(x)]$. Now, for it to be the case that $x$ does not divide $f(x)$, it must be the case that $f(x)$ has non-zero constant term. Since the units of $\mathbb{R}[[x]]$ are precisely those elements with non-zero constant term and $f$ is naturally an element of $\mathbb{R}[[x]]$, we see that $\frac{1}{f(x)} \in \mathbb{R}[[x]]$, so adjoining such terms to $\mathbb{R}[x] \subset \mathbb{R}[[x]]$ doesn't introduce any new elements, so $\mathbb{R}[x]_{(x)} \subset \mathbb{R}[[x]]$.

Next, consider $\mathbb{R}[x,y]_{(x,y)} = \{\frac{f(x)}{g(x)}|f,g \in \mathbb{R}[x,y], g \notin (x,y)\}$. Then the fact that $g \notin (x,y)$ means that $g$ necessarily has non-zero constant term. Again, since as we said above, the units of $\mathbb{R}[[x,y]]$ are precisely those with non-zero constant term, $\frac{1}{g} \in \mathbb{R}[[x,y]]$, so each term of the form $\frac{f}{g} \in \mathbb{R}[[x,y]]$ and so $\mathbb{R}[x,y]_{(x,y)} \subset \mathbb{R}[[x,y]]$.

Now, consider $\mathbb{Z}_{(p)} = \mathbb{Z}[\frac{1}{n}|p \text{ does not divide } n]$. If $n \in \mathbb{Z}$ such that $p$ does not divide $n$, then $n \in \mathbb{Z}_p$ and can be viewed as the following tuple:

$$(n \mod p, n \mod p^2, n \mod p^3, \ldots).$$

We know the unique maximal ideal in $\mathbb{Z}_p$ is $(p)$; hence, the ideal generated by $n$ in $\mathbb{Z}_p$ must be the unit ideal. Hence, $n$ has an inverse in $\mathbb{Z}_p$, $\frac{1}{n}$ (in fact, this shows that any element in $\mathbb{Z}_p$ represented by an infinite tuple with non-zero first term is invertible in $\mathbb{Z}_p$). Therefore, since $\frac{1}{n} \in \mathbb{Z}_p$ for all $n$ not divisible by $p$, we see that an arbitrary element of $\mathbb{Z}_{(p)}$, $\frac{a}{n}$ where $n$ is not divisible by $p$, is in $\mathbb{Z}_p$, so $\mathbb{Z}_{(p)} \subset \mathbb{Z}_p$.

Finally, consider $\mathbb{R}[x,y]_{(y)} = \{\frac{f}{g}|f,g \in \mathbb{R}[x,y], g \notin (y)\}$. Now, $x \notin (y)$, so it's clear that $\frac{1}{x} \in \mathbb{R}[x,y]_{(y)}$. However, as we saw in part (b) above, the units in the completion $\mathbb{R}[x][[y]]$ are those power series in $y$ with a non-zero constant polynomial as their constant term. Now, $x$ is a power series in $y$ with a non-constant polynomial as its constant term, so $x$ is not invertible in $\mathbb{R}[x][[y]]$, and so $\frac{1}{x} \notin \mathbb{R}[x][[y]]$, even though $\frac{1}{x} \in \mathbb{R}[x,y]_{(y)}$. Therefore, we see that $\mathbb{R}[x,y]_{(y)} \not\subset \mathbb{R}[x][[y]]$. There are a couple of differences between this last and the first three rings considered. First of all, in this last example, we're not localizing at an ideal that was maximal in the original ring, since $(y)$ is not maximal in $\mathbb{R}[x,y]$, whereas in the first three we were localizing at a maximal ideal. Secondly, the completion $\mathbb{R}[x][[y]]$ is not a local ring, since all ideals of the form $(x-a,y)$ are maximal. In fact, $\mathbb{R}[x,y]_{(y)}$ is not local either, since, again, ideals of the form $(x-a,y0$ are all maximal. In the first three examples, on the other hand, both the localization and the completion *were* local rings. □

## 4

If $R \subset S$ are commutative rings and $I \subset R$ is an ideal of $R$, call $IS \subset S$ the *extension* of $I$ to $S$. If $J \subset S$ is an ideal of $S$, call $J \cap R \subset R$ the *contraction* of $J$ to $R$.

**(a):** Are extensions and contractions always ideals? Are extension and contraction inverse operations?

**Answer:** Suppose $I \subset R$ is an ideal. Let $a \in IS$. Then $a = bs$ for some $b \in I$, $s \in S$. If $t \in S$, then

$$at = (bs)t = b(st) \in IS.$$

Therefore, since $IS$ is, by definition, a group under addition and $S$ is commutative, this suffices to show that $IS \subset S$ is an ideal.

On the other hand, suppose $a, b \in J \cap R$. Then $a, b \in J$ and $a, b \in R$. Let $r \in R$. Then certainly $ar, br \in R$ and, since $r \in S$, $ar, br \in J$. Hence, $(a + b)r = ar + br \in J \cap R$, so, since $R$ is commutative, this suffices to show that $J \cap R$ is an ideal in $R$.

To see that extension and contraction are not inverse operations, let $R = \mathbb{Z}$ and $S = \mathbb{Q}$. Let $I = 2\mathbb{Z}$. Then

$$IS = (2\mathbb{Z})\mathbb{Q} = \mathbb{Q}$$

and

$$(IS) \cap R = (\mathbb{Q}) \cap \mathbb{Z} = \mathbb{Z} \neq 2\mathbb{Z}.$$

♣

**(b):** For which prime ideals of $\mathbb{Z}$ is the extension to $\mathbb{Z}[i]$ also prime? For those that are not, which extensions ae the product of two distinct prime ideals, and which are the square of a prime ideal of $\mathbb{Z}[i]$? (Of thse two cases, the former case is called *split* and the latter case is called *ramified*

**Answer:** Note that the only prime ideals of $\mathbb{Z}$ are $(0)$ and $p\mathbb{Z}$ for $p$ prime in $\mathbb{Z}$. Also, it's clear that the zero ideal in $\mathbb{Z}[i]$ contracts to the zero ideal in $\mathbb{Z}$. Suppose, first of all, that $p \in \mathbb{Z}$ is a prime congruent to 3 modulo 4. Then, as we saw on PS8#5(b), $p$ remains prime in $\mathbb{Z}[i]$. Hence, if

$$ab \in (p\mathbb{Z})\mathbb{Z}[i] = p\mathbb{Z}[i],$$

then $p|ab$, which means that $p|a$ or $p|b$, so either $a$ or $b$ is in $p\mathbb{Z}[i]$. Thus, $p\mathbb{Z}[i]$ is a prime ideal.

On the other hand, if $p$ is an odd prime congruent to 1 modulo 4, then we saw in PS*#5(a) that $p$ is the product of two distinct primes $\beta, \gamma \in \mathbb{Z}[i]$. Hence, $\beta\gamma \in (p\mathbb{Z})\mathbb{Z}[i] = p\mathbb{Z}[i]$ even though neither $\beta$ nor $\gamma$ is divisible by $p$ and, thus, neither is in $p\mathbb{Z}[i]$. Therefore, $p\mathbb{Z}[i]$ is not prime. However, since $\beta, \gamma$ are prime in $\mathbb{Z}[i]$, $\beta\mathbb{Z}[i]$ and $\gamma\mathbb{Z}[i]$ are distinct prime ideals and $p\mathbb{Z}[i] = (\beta\mathbb{Z}[i])(\gamma\mathbb{Z}[i])$.

Finally, if $p = 2$, then, as we saw in PS8#5(c),

$$2 = -i(1+i)^2$$

and $1 + i$ is prime in $\mathbb{Z}[i]$. Hence, $(2\mathbb{Z})\mathbb{Z}[i] = 2\mathbb{Z}[i]$ is not prime; instead, it is the square of the prime ideal $(1 + i)\mathbb{Z}[i]$.

♣

**(c):** Show that taking contraction induces a surjection from the prime ideals of $\mathbb{Z}[i]$ to the prime ideals of $\mathbb{Z}$. Is it injective?

*Proof.* Note that the contraction of the zero ideal yields the zero ideal. For the more interesting cases, suppose $p\mathbb{Z}$ is a prime ideal in $\mathbb{Z}$. If $p \equiv 3 \mod 4$, then $p\mathbb{Z}[i] = \{pa + pbi | a, b \in \mathbb{Z}\}$, so

$$p\mathbb{Z}[i] \cap \mathbb{Z} = \{pa + pbi | a \in \mathbb{Z}, b = 0\} = \{pa | a \in \mathbb{Z}\} = p\mathbb{Z}.$$

If $p \equiv 1 \mod 4$, then $p = \beta\gamma$ for prime $\beta, \gamma \in \mathbb{Z}[i]$ as above. Now, recall that we showed in PS8#5(a) that $N(\gamma) = p$. Now,

$$\gamma\mathbb{Z}[i] \cap \mathbb{Z} = \{\gamma z | z \in \mathbb{Z}[i], \gamma z \in \mathbb{Z}\}.$$

Now, suppose $z \in \mathbb{Z}[i]$ such that $\gamma z \in \mathbb{Z}$. Since $\gamma z \in \mathbb{Z}$, $N(\gamma z) = (\gamma z)^2$. Hence,

$$(\gamma z)^2 = N(\gamma z) = N(\gamma)N(z) = pN(z).$$

Since $p|(\gamma z)^2$ it must be that $p|\gamma z$, so $\gamma z \in p\mathbb{Z}$. Since $\beta\gamma = p$, we know that $p \in \gamma\mathbb{Z}[i] \cap \mathbb{Z}$, so we conclude that, in fact, the contraction of $\gamma\mathbb{Z}[i]$ is, in fact, $p\mathbb{Z}$.

Finally, if $p = 2$, then the same argument given above (substituting $(1 + i)$ for $\gamma$ and $-i(1 + i)$ for $\beta$) shows that $(1 + i)\mathbb{Z}[i]$ contracts to $2\mathbb{Z}$ (the same argument works because nowhere did we use the fact that $\beta$ and $\gamma$ are distinct primes).

Thus, having examined all four possible types of prime ideals in $\mathbb{Z}$ (i.e. $(0)$ and $p\mathbb{Z}$ for $p \equiv 3 \mod 4$, $p \equiv 1 \mod 4$ and $p = 2$), we conclude that, indeed, this correlation given by contraction is surjective.

However, this correlation is clearly not injective. To see why, simply note that for $p \equiv 3 \mod 4$, $p\mathbb{Z}[i] = \{pa + pbi | a, b \in \mathbb{Z}\}$, so

$$p\mathbb{Z}[i] \cap \mathbb{Z} = \{pa + pbi | a \in \mathbb{Z}, b = 0\} = \{pa | a \in \mathbb{Z}\} = p\mathbb{Z}.$$

On the other hand, we saw in PS8#7 that $pi$ is prime in $\mathbb{Z}[i]$. Now, $(pi)\mathbb{Z}[i] = \{(pi)a + (pi)bi | a, b \in \mathbb{Z}\}$, which we can simplify to $\{-pb + pai | a, b \in \mathbb{Z}\}$. Hence,

$$(pi)\mathbb{Z}[i] \cap \mathbb{Z} = \{-pb + pai | b \in \mathbb{Z}, pa = 0\} = \{-pb | b \in \mathbb{Z}\} = p\mathbb{Z}.$$

□

**(d):** Do your assertions in part (c) hold for an arbitrary extension of integral domains $R \subset S$?

**Answer:** As in part (a) above, we can demonstrate that the answer is "no" by considering the pathological counter-example where $R = \mathbb{Z}$ and $S = \mathbb{Q}$. The only prime ideal in $\mathbb{Q}$ is $(0)$, so taking contractions of prime ideals in $\mathbb{Q}$ certainly does not give a surjection onto the prime ideals of $\mathbb{Z}$. As a slightly less pathological counter-example, consider the case where $R = \mathbb{Z}$ and $S = \mathbb{R}[x]$. Then certainly $\mathbb{Z} \subset \mathbb{R}[x]$. However, the no ideal in $\mathbb{R}[x]$ contains any of the integers except zero, since all non-zero integers are units in $\mathbb{R}[x]$. Hence, if $\mathfrak{p} \subset \mathbb{R}[x]$ is a prime ideal, then $\mathfrak{p} \cap \mathbb{Z} = (0)$, so again contraction does not yield a surjection.

♣

## 5

Let $K$ be a field

**(a):** Find all $c \in K$ such that the vectors $(c, 1, 0), (1, c, 1), (0, 1, c) \subset K^3$ are linearly independent.

**Answer:** First, let us see for what values of $c$ these vectors are linearly dependent. That is, for what values of $a, b, c, d \in K$ is it the case that

$$a(c, 1, 0) + b(1, c, 1) + d(0, 1, c) = (0, 0, 0).$$

For this to be true, the following system holds:

$$\begin{aligned} ac + b &= 0 \\ a + bc + d &= 0 \\ b + dc &= 0. \end{aligned}$$

Hence, by the first and third equations,

$$ac = -b = dc.$$

Therefore,

$$a + d = -bc = ac^2 = dc^2.$$

That is,

$$\frac{a+d}{a} = c^2 = \frac{a+d}{d}.$$

In turn, this means that $a = d$, so $c^2 = a = d$ and so $b = -ac = -c^3$. Substituting into the second equation,

$$0 = a + bc + d = c^2 - c^4 + c^2 \Rightarrow c^2c^2 = c^4 = c^2 + c^2 \Rightarrow c^2 = \frac{2c^2}{c^2} = 2,$$

so $c = \pm\sqrt{2}$. Hence, for all other values of $c$ (or for all values of $c$ if $\sqrt{2} \notin K$), the given vectors are linearly independent.

♣

**(b):** Determine whether the vectors $(7,-1,5),(0,0,2) \in K^3$ can be expressed as a linear combination of $v=(3,-1,2)$ and $w=(1,1,1)$; do so explicitly in each case if possible.

**Answer:** Suppose $(7,-1,5)$ is a linear combination of the given vectors. Then there exist $a,b \in \mathbb{R}$ such that

$$(7,-1,5) = av+bw = a(3,-1,2)+b(1,1,1) = (3a,-a,2a)+(b,b,b) = (3a+b,b-a,2a+b).$$

That is, $a$ and $b$ are solutions of the system

$$\begin{aligned} 3a+b &= 7 \\ b-a &= -1 \\ 2a+b &= 5. \end{aligned}$$

Hence, $a=b+1$, so

$$7 = 3a+b = 3(b+1)+b = 4b+3 \Rightarrow b = 1 \Rightarrow a = 2.$$

Note that, with these values, $5 = 2a+b = 4+1$, and so we see that

$$2(3,-1,2)+(1,1,1) = (6,-2,4)+(1,1,1) = (7,-1,5).$$

On the other hand, if $(0,0,2)$ is a linear combination of the given vectors, then there exist $a,b \in \mathbb{R}$ such that

$$(0,0,2) = a(3,-1,2)+b(1,1,1) = (3a,-a,2a)+(b,b,b) = (3a+b,b-a,2a+b),$$

so $a$ and $b$ are solutions to the system

$$\begin{aligned} 3a+b &= 0 \\ b-a &= 0 \\ 2a+b &= 2. \end{aligned}$$

Hence, $a=b$, by the second equation, so

$$0 = 3a+b = 3b+b = 4b \Rightarrow a = b = 0.$$

However, this is inconsistent with the third equation, as $2(0)+0 \neq 2$, so we see that there are no such $a,b$, so $(0,0,2)$ cannot be written as a linear combination of the given vectors.

♣

**(c):** Let $T : K^3 \to K^3$ be the homomorphism taking $(1,0,0) \mapsto (1,4,7)$, $(0,1,0) \mapsto (2,5,8)$, and $(0,0,1) \mapsto (3,6,9)$. Describe the kernel and image of $T$ geometrically, find their dimensions, and find a basis for each.

**Answer:** Given what it does to the standard basis, we can represent this homomorphism $T$ by the matrix

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

We can determine the kernel of $T$ by row-reducing this matrix; as a first step, subtract 4 times the first row from the second and 7 times the first from the third, to get:

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{pmatrix}.$$

Scaling the second row and subtracting twice it from the third then yields

$$\begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{pmatrix}.$$

From this arises the system

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= 0 \\ x_2 + 2x_3 &= 0 \end{aligned}$$

Hence, $x_2 = -2x_3$ and

$$x_1 = -2x_2 - 3x_3 = -2(-2x_3) - 3x_2 = x_3$$

where $x_3$ is free. Therefore, we see that the vector $(1, -2, 1)$ serves as a basis for the kernel of $T$, which, therefore, has dimension 1 and consists simply of the line passing through the origin and the point $(1, -2, 1)$.

On the other hand, the image of $T$ is given by the span of the pivot columns of the associated matrix, so $\{(1, 4, 7), (2, 5, 8)\}$ is a basis for the image of $T$, which necessarily has dimension 2 and consists, geometrically, of the plane passing through the origin, $(1, 4, 7)$ and $(2, 5, 8)$.

♣

**(d):** Let $S : K^2 \to K^2$ be the homomorphism taking $(a, b) \mapsto (17a - 30b, 9a - 16b)$. Find all diagonal matrices $D$ such that $D$ is the matrix for $T$ with respect to some basis of $K^2$.

**Answer:** Now, the columns of the matrix of a vector space homomorphism are simply the images of whatever basis vectors we're considering. Hence, in order for the matrix of $T$ to be diagonal, it must be the case that $\{(a, b), (a', b')\}$ forms a basis for $K^2$ and

$$\begin{aligned} 17a - 30b &= d_1 \\ 9a - 16b &= 0 \\ 17a' - 30b' &= 0 \\ 9a' - 16b' &= d_2. \end{aligned}$$

Then $9a = 16b$, so $a = \frac{16b}{9}$. In turn, this means that

$$d_1 = 17a - 30b = 17\frac{16b}{9} - 30b = \frac{272b}{9} - \frac{270b}{9} = \frac{2}{9}b.$$

On the other hand, $17a' = 30b'$, so $a' = \frac{30b'}{17}$. Hence,

$$d_2 = 9a' - 16b' = 9\frac{30b'}{17} - 16b' = \frac{270b'}{17} - \frac{272b'}{17} = -\frac{2}{17}b'.$$

Now, $\{(\frac{16}{9}, 1), (\frac{30}{17}, 1)\}$ are linearly independent, so all multiples thereof form a basis for $K^2$, so such a matrix $D$ must be of the form

$$\begin{pmatrix} \frac{2}{9}b & 0 \\ 0 & \frac{-2}{17}b' \end{pmatrix}$$

for some $b, b' \in K$.

♣

## 6

**(a):** Let $A$ be a $3 \times 2$ matrix and let $B$ be a $2 \times 3$ matrix over some field $K$. Find $\det AB$. Explain.

**Answer:** Associated with $A$ and $B$ are linear maps $\phi : \mathbb{R}^2 \to \mathbb{R}^3$ and $\psi : \mathbb{R}^3 \to \mathbb{R}^2$, respectively, and $AB$ corresponds to the linear map $\phi \circ \psi : \mathbb{R}^3 \to \mathbb{R}^3$. Now, since the rank of $\phi$ is equal to the column rank of $A$, rank $\phi \leq 2$. Therefore, the dimension of $\text{Image}(\phi) \subset \mathbb{R}^3$ is at most 2. Now, since $\text{Image}(\phi \circ \psi) \subset \text{Image}(\phi)$, $\text{Image}(\phi \circ \psi)$ has dimension at most 2, and so $\phi \circ \psi$ has rank at most 2. Therefore, the column rank of $AB$ is at most 2; since a matrix must have full rank to have non-zero determinant, we see that $\det AB = 0$.

♣

**(b):** Let $A$ and $B$ be $n \times n$ matrices over $K$. Show that $AB$ is invertible if and only if both $A$ and $B$ are.

*Proof.* Suppose, first of all, that $AB$ is invertible. Then it must be the case that

$$0 \neq \det AB = \det A \det B$$

which means that $\det A \neq 0$ and $\det B \neq 0$, so $A$ and $B$ are invertible.

On the other hand, suppose $A$ and $B$ are invertible. Then $\det A \neq 0$ and $\det B \neq 0$, so

$$0 \neq \det A \det B = \det AB$$

since $K$ is a field and thus has no zero divisors. Therefore, $AB$ is invertible. □

DRL 3E3A, University of Pennsylvania
*E-mail address*: shonkwil@math.upenn.edu