1. In this problem we will prove that $\sqrt{\langle x^2(x+1), y\rangle} = \langle x(x+1), y\rangle$.

(a) Explain why we have the containment $\langle x(x+1), y\rangle \subseteq \sqrt{\langle x^2(x+1), y\rangle}$.

From part (a), in order to show equality it is enough to show the reverse containment. Let f be any element of $\sqrt{\langle x^2(x+1), y\rangle}$.

(b) Explain why we know that there is an $n \geqslant 1$ and polynomials $h_1, h_2 \in k[x,y]$ such that

$$f^n = x^2(x+1)h_1 + yh_2. \tag{b1}$$

(c) Let $\psi\colon k[x,y] \longrightarrow k[x]$ be the ring homomorphism given by setting $y=0$, and set $\overline{f} = \psi(f)$. Looking at the image of (b1) under ψ, and using unique factorization in the ring $k[x]$, explain why we know that there is a polynomial $h_3 \in k[x]$ so that

$$\overline{f} = x(x+1)h_3.$$

(d) Using part (c), explain why we know that there is a polynomial $h_4 \in k[x,y]$ so that $f - x(x+1)h_4$ is in the kernel of ψ.

(e) What is the kernel of ψ?

(f) Complete the problem by showing that $f \in \langle x(x+1), y\rangle$.

Solutions.

(a) Let $I = \langle x^2(x+1), y\rangle$. We always have the inclusion $I \subseteq \sqrt{I}$, and therefore since $y \in I$ we have $y \in \sqrt{I}$. Set $f = x(x+1)$. Since $f^2 = x^2(x+1)^2 = (x+1)\cdot(x^2(x+1)) \in I$ we have $f \in \sqrt{I}$ by definition of $\sqrt{I}$. Since both y and $x(x+1)$ are in the ideal $\sqrt{I}$, the ideal $\langle x(x+1), y\rangle$ is also contained in $\sqrt{I}$.

(b) By the definition of the radical if $f \in \sqrt{I}$ there is an $n \geqslant 1$ so that $f^n \in I$. Since I is generated by $x^2(x+1)$ and y this means that there are $h_1, h_2 \in k[x,y]$ with $f^n = x^2(x+1)h_1 + yh_2$.

(c) Let $\overline{h}_1$ be the image of h_1 under ψ. Applying ψ to (b1) we get

(c2)
$$\overline{f}^n = x^2(x+1)\overline{h}_1.$$

Any polynomial in $k[x]$ can be factored as a product of linear factors (or irreducible factors, if k is not algebraically closed). Since x divides the right hand side of (c2) it must also divide $\overline{f}^n$, and therefore must divide $\overline{f}$. Similarly, since $x+1$ divides the right hand side of (c2) $x+1$ must also divide $\overline{f}^n$ and hence also divide $\overline{f}$. Since x and $(x+1)$ are relatively prime, their product must also divide $\overline{f}$. By definition (of 'divides') this means that there is a polynomial $h_3 \in k[x]$ so that $\overline{f} = x(x+1)h_3$.

(d) Let $h_4 \in k[x,y]$ be the polynomial h_3, now also considered as a polynomial in x, y (but with no y's). Then $\psi(h_4) = h_3$, so

$$\psi\Big(f - x(x+1)h_4\Big) = \psi(f) - x(x+1)\psi(h_4) = \overline{f} - x(x+1)h_3 = 0,$$

and so $f - x(x+1)h_4 \in \mathrm{Ker}(\psi)$.

(e) The map ψ corresponds to "restriction to the x-axis", and has kernel $\langle y \rangle$.

(f) Since $f - x(x+1)h_4 \in \mathrm{Ker}(\psi) = \langle y \rangle$ there is a polynomial $h_5 \in k[x,y]$ so that $f - x(x+1)h_4 = yh_5$. But then $f = x(x+1)h_4 + yh_5$, so that $f \in \langle x(x+1), y \rangle$.

2. In this problem we will explore other questions about the radical.

(a) Let A be any ring, $I \subset A$ and ideal, and $f \in I$. Suppose that $f = f_1^{e_1} f_2^{e_2} \cdots f_r^{e_r}$ for some $f_1, \ldots, f_r \in A$, and some $e_1, \ldots e_r \geqslant 1$. Show that $f_1 f_2 \cdots f_r \in \sqrt{I}$.

(b) Let $I \subset \mathbb{Z}$ be an ideal. We know that every ideal in $\mathbb{Z}$ is generated by a single element, so $I = \langle n \rangle$ for some $n \in \mathbb{Z}$. Assume that $n \neq 0$ (i.e, $I \neq (0)$) and let $n = p_1^{e_1} \cdots p_r^{e_r}$ be the prime factorization of n. Show that $\sqrt{I} = \langle p_1 p_2 \cdots p_r \rangle$.

(c) Let J_1 and J_2 be ideals. Show that $J_1 \cap J_2$ is also an ideal.

(d) Let I_1 and I_2 be radical ideals. Show that $I_1 \cap I_2$ is also a radical ideal.

[Math 813 only] (e) For any $f \in k[x_1, \ldots, x_n]$ let $f = f_1^{e_1} \cdots f_r^{e_r}$ be its factorization into irreducibles, and define $\mathrm{Rad}(f)$ by the formula $\mathrm{Rad}(f) = f_1 f_2 \cdots f_r$. Show that if I is a principal ideal, $I = \langle f \rangle$, then $\sqrt{I} = \langle \mathrm{Rad}(f) \rangle$.

[Math 813 only] (f) Give an example of an ideal $I = \langle g_1, g_2 \rangle \subset k[x,y]$ such that $\sqrt{I} \neq \langle \mathrm{Rad}(g_1), \mathrm{Rad}(g_2) \rangle$. (One possibility: An ideal with this property has already appeared in class, but you can make up your own.)

Solution.

(a) Let $e = \max(e_1, e_2, \ldots, e_r)$. Then $(f_1 \cdots f_r)^e = f_1^{e-e_1} f_2^{e-e_2} \cdots f_r^{e-e_r} f \in I$. Therefore by definition of the radical we must have $f_1 \cdots f_r \in \sqrt{I}$.

(b) By part (a), $p_1 \cdots p_r \in \sqrt{I}$, so that $\langle p_1 \cdots p_r \rangle \subseteq \sqrt{I}$. We now want to show the opposite containment. Let m be any element of $\sqrt{I}$. By definition there is a positive integer n so that $m^n \in I = \langle p_1^{e_1} \cdots p_r^{e_r} \rangle$. Thus there is a number g so that $m^n = g \cdot p_1^{e_1} \cdots p_r^{e_r}$. But then each of p_1,..., p_r divides m^n, so each of p_1,..., p_r must also divide m. Since p_1,..., p_r are relatively prime, this implies that the product $p_1 p_2 \cdots p_r$ divids m, and therefore that $m = u \cdot p_1 \cdots p_r$ for some integer u. This is the same thing as saying that $m \in \langle p_1 \cdots p_r \rangle$. Since m was arbitrary, we conclude that $\sqrt{I} \subseteq \langle p_1 \cdots p_r \rangle$ and hence that $\sqrt{I} = \langle p_1 \cdots p_r \rangle$.

(c) Set $J = J_1 \cap J_2$. We need to show that J is closed under addition, and that J is "multiplicatively sticky".

Suppose that $f_1, f_2 \in J$. By the definition of J this means f_1 and f_2 are in each of I_1 and I_2. Since I_1 is an ideal we know that $f_1 + f_2 \in I_1$. Since I_2 is an ideal we know that $f_1 + f_2 \in I_2$. Therefore $f_1 + f_2 \in I_1 \cap I_2 = J$.

Similarly, suppose that $f \in J$ and that $a \in A$ (where A is the ring we are working in). Since $f \in I_1 \cap I_2$, we know that f is in I_1 and I_2. Since I_1 is an ideal $af \in I_1$. Since I_2 is an ideal $af \in I_2$. Therefore $af \in I_1 \cap I_2 = J$.

(d) By part (b) $I_1 \cap I_1$ is an ideal, so the only issue is to show that it is also a radical ideal. Set $J = I_1 \cap I_2$, and suppose that $f \in A$, and that $f^n \in J$ for some $n \geqslant 1$. Then we have $f^n \in I_1$ and $f^n \in I_2$ by the definition of J. Since both I_1 and I_2 are radical ideals, this implies that $f \in I_1$ and $f \in I_2$. Therefore $f \in I_1 \cap I_2 = J$, so J is a radical ideal.

[Math 813 only] (e) This argument works exactly like the argument in (b): Let $f = f_1^{e_1} \cdots f_r^{e_r}$ be the factorization of f into irreducibles. By part (a) we have $f_1 \cdots f_r \in \sqrt{I}$, so that $\langle f_1 \cdots f_r \rangle \subseteq \sqrt{I}$, and we need to show the opposite containment. Suppose that $g \in \sqrt{I}$. By definition that means that there is an $n \geqslant 1$ so that $g^n \in I$, so that $g^n = h f_1^{e_1} \cdots f_r^{e_r}$ for some $h \in k[x_1, \ldots, x_n]$. The equation shows that each of f_1,..., f_r divides g^n, hence since f_1,..., f_r are irreducible (and so prime), each of f_1,..., f_r divides g. Since f_1,..., f_r are relatively prime, the product $f_1 \cdots f_r$ also divides g. Therefore $g \in \langle f_1 \cdots f_r \rangle$, so that $\sqrt{I} = \langle f_1 \cdots f_r \rangle$.

[Math 813 only] (f) Perhaps the easiest example is this: Suppose that k is not of characteristic 2 and let I be the ideal $I = \langle x^2 - y^2, x^2 + y^2 \rangle \subset k[x, y]$. Then $\mathrm{Rad}(x^2 - y^2) = x^2 - y^2$, $\mathrm{Rad}(x^2 + y^2) = x^2 + y^2$. However, $\langle x^2 - y^2, x^2 + y^2 \rangle = \langle x^2, y^2 \rangle$, so we see that $(x, y) \subseteq \sqrt{I}$. From this we deduce that $\langle x, y \rangle = \sqrt{I}$ since $\langle x, y \rangle$ is a maximal ideal, and $\sqrt{I} \neq k[x,y]$. However, $\langle x^2-y^2, x^2+y^2\rangle \neq \langle x,y\rangle$, so $\sqrt{\langle f,g\rangle} \neq \langle \mathrm{Rad}\, f, \mathrm{Rad}\, g\rangle$ when $f = x^2-y^2$, $g = x^2+y^2$.

An alternate example is the one we saw in class (and question 1). Let $I = \langle y, y^2 - x^3 - x^2\rangle$, i.e., $f = y$ and $g = y^2 - x^3 - x^2$. Then $\mathrm{Rad}(f) = f$, $\mathrm{Rad}(g) = g$, but since $I = \langle y, x^2(x+1)\rangle$ we have $\sqrt{I} = \langle y, x(x+1)\rangle \neq I$.

3. Let $\mathfrak{m} \subset \mathbb{C}[x,y,z]$ be the maximal ideal $\mathfrak{m} = \langle x-3, y-4, z-5\rangle$. Which of the following ideals are contained in $\mathfrak{m}$? And how do you know?

(a) $I_1 = \langle x^2+y^2-z^2\rangle$.

(b) $I_2 = \langle z^2 - 2xy\rangle$.

(c) $I_3 = \langle y^2 - x^2 - x - y, xyz - 3z^2 + 5x\rangle$.

(d) $I_4 = \langle x^2+y^2+z^2-xy-xz-yz, 7yz+4xz-8z^2\rangle$.

Solution. In class we have seen that for a maximial ideal of the form $\mathfrak{m} = \langle x_1 - a_1, \ldots, x_n - a_n\rangle \subset k[x_1,\ldots,x_n]$, that a polynomial $g \in k[x_1,\ldots,x_n]$ is in $\mathfrak{m}$ if and only if $g(a_1,\ldots,a_n) = 0$. (We saw this in two different ways, one of which was identifying $\mathfrak{m}$ as the kernel of the evaluation map $k[x_1,\ldots,x_n] \longrightarrow k$ sending each g to $g(a_1,\ldots,a_n)$, and the other was by considering the "Taylor expansion" of g around $(a_1,\ldots,a_n)$.)

In this problem we are considering the maximal ideal $\mathfrak{m} = \langle x-3, y-4, z-5\rangle$.

(a) The ideal $I_1 = \langle x^2+y^2-z^2\rangle$ is generated by $g_1 = x^2+y^2-z^2$. Since $g_1(3,4,5) = 3^2+4^2-5^2 = 0$, we see that $g_1 \in \mathfrak{m}$. Since $g_1 \in \mathfrak{m}$, the ideal $I_1 = \langle g_1\rangle$ is also contained in $\mathfrak{m}$.

(b) The ideal $I_2 = \langle z^2-2xy\rangle$ is generated by $g_2 = z^2 - 2xy$. Since $g_2(3,4,5) = 5^2 - 2\cdot 3\cdot 4 = 25 - 24 = 1 \neq 0$, we see that $g_2 \notin \mathfrak{m}$, and so $I_2 \not\subset \mathfrak{m}$.

(c) The ideal $I_3 = \langle y^2-x^2-x-y, xyz-3z^2+5x\rangle$ is generated by $g_3 = y^2-x^2-x-y$ and $h_3 = xyz - 3z^2 + 5x$. We have

$$\begin{aligned} g_3(3,4,5) &= 4^2 - 3^2 - 3 - 4 = 16 - 9 - 3 - 4 = 0, \text{ and} \\ h_3(3,4,5) &= 3\cdot 4\cdot 5 - 3\cdot 5^2 + 5\cdot 3 = 60 - 75 + 15 = 0 \end{aligned}$$

and therefore both g_3 and h_3 are in $\mathfrak{m}$. We conclude that $I_3 = \langle g_3, h_3\rangle \subset \mathfrak{m}$.

(d) The ideal $I_4 = \langle x^2 + y^2 + z^2 - xy - xz - yz, 7yz + 4xz - 8z^2 \rangle$ is generated by $g_4 = x^2 + y^2 + z^2 - xy - xz - yz$ and by $h_4 = 7yz + 4xz - 8z^2$. We have

$$\begin{aligned} g_4(3,4,5) &= 3^2 + 4^2 + 5^2 - 3 \cdot 4 - 3 \cdot 5 - 4 \cdot 5 = 3, \text{ and} \\ h_4(3,4,5) &= 7 \cdot 4 \cdot 5 + 4 \cdot 3 \cdot 5 - 8 \cdot 5^2 = 0. \end{aligned}$$

Since $g_4(3,4,5) = 3 \neq 0$, $g \notin \mathfrak{m}$ and therefore $I_4 \not\subset \mathfrak{m}$.

[Math 813 only] 4. In order that maximal ideals are in one-to-one correspondence with points, we needed the condition that k be algebraically closed. In this problem we will see in a simple example what happens if k is not algebraically closed: Maximal ideals are in one-to-one correspondence with $\mathrm{Gal}(\overline{k}/k)$ orbits of points.

[Math 813 only] (a) Let $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$ be the Galois group of $\mathbb{C} = \overline{\mathbb{R}}$ over $\mathbb{R}$. Classify the orbits of G on $\mathbb{C}$.

[Math 813 only] (b) Classify the maximal ideals of $\mathbb{R}[x]$.

[Math 813 only] (c) Show that the maximal ideals of $\mathbb{R}[x]$ are in one-to-one correspondence with the orbits of $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ on $\mathbb{C}$.

Solutions.

[Math 813 only] (a) The Galois group is $G = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}_{\mathbb{C}}, \sigma\}$, where σ is complex conjugation. If $z \in \mathbb{R} \subseteq \mathbb{C}$ then z is fixed by G. If $z \in \mathbb{C} \setminus \mathbb{R}$ then the orbit of z is $\{z, \overline{z}\}$, of size 2. Thus an orbit of G consists of either a real number or a pair of conjugate complex numbers.

[Math 813 only] (b) The ring $\mathbb{R}[x]$ is a principal ideal domain, so every ideal $I \subseteq \mathbb{R}[x]$ is of the form $I = \langle f \rangle$ for a monic polynomial f. In order for I to be maximal we need f to be irreducible. The monic irreducible polynomials in $\mathbb{R}[x]$ are either linear, so of the form $x - z$ with $z \in \mathbb{R}$ or an irreducible quadratic polynomial $x^2 + bx + c$ with $b, c \in \mathbb{R}$ and $b^2 - 4c < 0$. The roots of the irreducible quadratic polynomial are the conjugate pair of complex numbers $\frac{1}{2}(-b \pm \sqrt{b^2 - 4c})$, while the root of the linear polynomial is the real number z.

[Math 813 only] (c) The maximal ideals of $\mathbb{R}[x]$ are in one-to-one with the G-orbits on $\mathbb{C}$: given $u \in \mathbb{C}$ we send u to the maximal ideal generated by $\prod_{z \in \mathrm{Orb}_G(u)} (x - z)$. Concretely, for $u \in \mathbb{R} \subset \mathbb{C}$ this means we send u to the ideal $\langle x - u \rangle$, and for $u \in \mathbb{C} \setminus \mathbb{R}$ we send u to the ideal $\langle (x-u)(x-\overline{u}) \rangle = \langle x^2 - (u + \overline{u})x + u\overline{u} \rangle$. Conversely, given a maximal ideal $\mathfrak{m} = \langle f \rangle \subset \mathbb{R}[x]$ we associate it to its set of roots. This gives a one-to-one correspondence between the two sets.

Note: The reason we looked at points of $\mathbb{C} = \mathbb{A}^1_{\mathbb{C}}$ is that $\mathbb{A}^1_{\mathbb{C}}$ is the variety associated to the ring of functions $\overline{\mathbb{R}}[x] = \mathbb{C}[x]$. More generally the maximal ideals of $k[x_1, \ldots, x_n]$ are in one to one corresopondence with the orbits of $\mathrm{Gal}(\overline{k}/k)$ acting on $\mathbb{A}^n_{\overline{k}}$. There is a similar statement for maximal ideals of a ring $R[X]$ where X is an affine variety defined over k (i.e., using equations in $k[x_1, \ldots, x_n]$). Thus working over a non-algebraically closed field k amounts to combining the geometric picture over $\overline{k}$ with the action of $\mathrm{Gal}(\overline{k}/k)$ on the points of the variety.