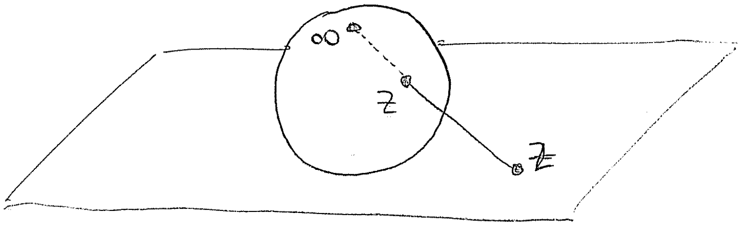
Math 662 — Spring 2014
Homework 4 — Drew Armstrong

Problem 0. (Drawing Pictures) We have drawn algebraic curves in $\mathbb{R}^2$, $\mathbb{C}^2$ and $\mathbb{R}P^2$. Now we will try to draw an algebraic curve in $\mathbb{C}P^2$. Let $\alpha, \beta, \gamma \in \mathbb{C}$ be distinct complex numbers and consider the polynomial

$$f(x, y) := y^2 - (x - \alpha)(x - \beta)(x - \gamma) \in \mathbb{C}[x, y].$$

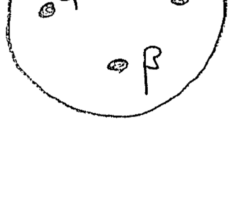
We can identify the complex projective line $\mathbb{C}P^1 := \{[x_0 : x_1] : x_0, x_1 \in \mathbb{C} \text{ not both zero}\}$ with the real 2-sphere by stereographic projection. (The points $[1 : x] \in \mathbb{C}P^1$ correspond to finite points $x \in \mathbb{C}$, and the point at infinity $\infty := [0 : 1] \in \mathbb{C}P^1$ is the north pole.) Let $S \subseteq \mathbb{C}P^2$ denote the set of points $(x, y) \in \mathbb{C}P^2$ satisfying $f(x, y) = 0$. (Technically we should homogenize the polynomial $f(x, y)$ to have 3 complex variables, but don't worry about it. Our pictures will not be precise anyway!) Note that for each $x \in \mathbb{C}P^1 \setminus \{\alpha, \beta, \gamma, \infty\}$ the equation $f(x, y) = 0$ has exactly two solutions for $y \in \mathbb{C}P^1$. Thus S can be thought of as a double cover of the sphere $\mathbb{C}P^1$, possibly branched at the four points $\{\alpha, \beta, \gamma, \infty\}$. One can show in fact that there is a single point of S above each $x \in \{\alpha, \beta, \gamma, \infty\}$, instead of two. **Perform cut-and-paste to show that S is topologically equivlalent to a torus.** [Hint: "Cut" from α to β and from γ to ∞. Take the two sheets apart and "paste" them back together. You may assume that Riemann surfaces are orientable (which can be proved using complex analysis), so S is not a Klein bottle.]

Proof. First recall that by stereographic projection we can identify $\mathbb{C}$ with the real 2-sphere:

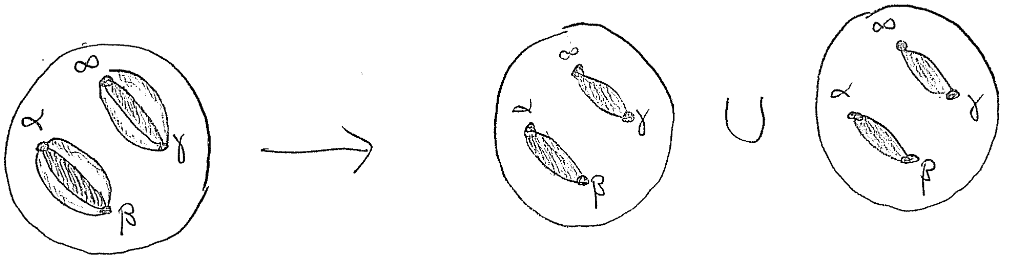


The north pole corresponds to the "point at infinity". We will call this the Riemann sphere (if we're feeling analytic) or $\mathbb{C}P^1$ (if we're feeling algebraic). We would like to think of the equation $f(x, y) = 0$ as defining $y \in \mathbb{C}P^1$ as a function of $x \in \mathbb{C}P^1$. Unfortunately we can't do this because for some values of $x \in \mathbb{C}P^1$ there are **two** values of $y \in \mathbb{C}P^1$ such that $f(x, y) = 0$. So instead we define $S \subseteq \mathbb{C}P^2$ as the set of points $(x, y) \in \mathbb{C}P^2$ such that $f(x, y) = 0$. Then we **can** think of $y \in S$ as a function of $x \in \mathbb{C}P^1$. What does S "look like" (i.e. topologically)?

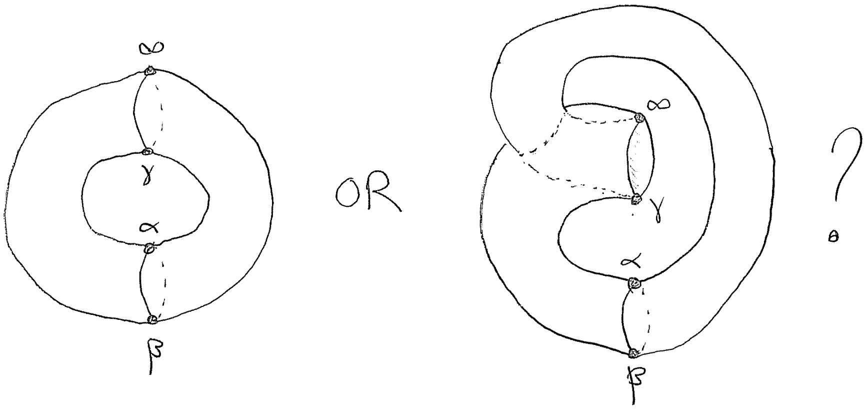
Well, the "x-axis" looks like this:



Above each $x \in \mathbb{C}P^1$ (except possibly $x \in \{\alpha, \beta, \gamma, \infty\}$) there are exactly **two** points $(x, y) \in S$. Thus we can think of S as a "double cover" of $\mathbb{C}P^1$. What happens over the points $x \in \{\alpha, \beta, \gamma, \infty\}$? Above each of these points there is exactly **one** point $(x, y) \in S$. This means that if we cut open the surface (say with a vertical laser) from α to β and from γ to ∞ we get something that looks like this:



(Of course this picture is only true topologically. The real picture is far too big to see accurately.) These two cuts disconnect S into two pieces that are much easier to visualize. Now we can try to think carefully about how they were originally connected. We realize that there are topologically only two ways that they could have been joined up, either as a torus or a Klein bottle:



How do we know which is the correct picture? We can either analyze the branch points a bit more carefully or we can use complex analysis to show that S must be orientable (multiplication by i rotates **counterclockwise** by 90°). Since S is orientable it can not be a Klein bottle. Hence it's a torus. □

[Remark: Maybe you find that hard to swallow because it's not rigorous; but there's no denying that it's useful. Welcome to topology.]

Problem 1. (The prime ideals of $\mathbb{Z}[y]$ and $K[x, y]$) Let R be a PID and let $P \leq R[y]$ be a **prime** ideal. You will show that P is one of the following:

- (0),
- (g) for irreducible $g \in R[y]$,
- (p, f) where $p \in R$ is prime, $f \in R[y]$, and the reduction $\bar{f} \in R/(p)[y]$ is irreducible.

Furthermore, the third kind ideals are the **maximal** ideals of $R[y]$.

(a) If P is principal, show that we have $P = (0)$ or $P = (g(y))$ for $g(y) \in R[y]$ irreducible.

(b) If P is not principal, show that P contains f_1, f_2 with no common prime factor in $R[y]$.

(c) Let $K = \text{Frac}(R)$. Show that the $f_1, f_2 \in P$ from part (b) also have no common factor in $K[y]$.

(d) If P is not principal, show that $R \cap P = (p)$ for some nonzero prime $p \in R$.

(e) Let P be nonprincipal and consider $(p) = R \cap P$ as in part (d). Let $f \mapsto \bar{f}$ be the reduction homomorphism $R[y] \to R/(p)[y]$ and let $\bar{P} \leq R/(p)[y]$ be the image of P under reduction. Show that $\bar{P}$ is a prime ideal of $R/(p)[y]$, and conclude that $P = (p, f)$ for some $f \in R[y]$ such that $\bar{f} \in R/(p)[y]$ is irreducible.

(f) Finally, given any irreducible $p \in R$ and $f \in R[y]$ such that $\bar{f} \in R/(p)[y]$ is irreducible, show that $(p, f) < R[y]$ is a **maximal ideal**. Show that any principal ideal $(g) \leq R[y]$ is **not maximal**.

[I deleted the hints from the problem to make it more readable and to save space.]

Proof. **(a):** Let $P < R[y]$ be prime and principal. Then either $P = (0)$ or $P = (g(y))$ where $g(y) \in R[y]$ is a prime element. Since $R[y]$ is a domain we know that $g(y)$ is also irreducible. In particular, $g(y)$ is primitive (the gcd of its coefficients is 1).

(b): Now let $P < R[y]$ be prime and **not principal**. Then P contains an irreducible element. Indeed, since $P \neq (0)$ we can choose some nonzero, nonunit $f \in P$. Since $R[y]$ is a UFD we can factor f into irreducibles, and then one of these irreducibles must be in P. (If not then f is a product of elements outside the prime ideal P, hence $f \notin P$.) /// So let $f_1 \in P$ be irreducible. Since P is not principal there exists $f_2 \in P \setminus (f_1)$. We claim that f_1 and f_2 are coprime. Indeed, if g is any common divisor of f_1 and f_2 then in particular g divides f_1. Since f_1 is irreducible this implies that g is a unit or associate to f_1. But if g is associate to f_1 (say $f_1 = ug$ for $u \in R[y]^\times$) then since g also divides f_2 (say $f_2 = hg$) we find that $f_2 = (hu^{-1})f_1 \in (f_1)$. Contradiction.

(c): Now let $K = \text{Frac}(R)$ and consider the coprime $f_1, f_2 \in P$ from part (b). We claim that f_1, f_2 are also coprime in $K[y]$. Indeed, suppose that $f_1 = hg_1$ and $f_2 = hg_2$ for some nonunit $h, g_1, g_2 \in K[y]$. We can multiply each by a common denominator and then factor out gcd of its coefficients to obtain $h = \alpha h_0$, $g_1 = b_1\gamma_1$, $g_2 = b_2\gamma_2$ where $a, b_1, b_2 \in K$ and $h_0, \gamma_1, \gamma_2 \in R[y]$ are **primitive**. Then we have $f_1 = hg_1 = (ah_0)(b_1\gamma_1) = (ab_1)(h_0\gamma_1)$ where $ab_1 \in K$ and the product $h_0\gamma_1 \in R[y]$ is **primitive**. By Gauss' Lemma in a PID ($K[y]$ is a PID) we must also have $ab_1 \in R$; similarly, $ab_2 \in R$. Finally, since $f_1 = (ab_1\gamma_1)h_0$ and $f_2 = (ab_2\gamma_2)h_0$ with $ab_1\gamma_1, ab_2\gamma_2 \in R[y]$ we conclude that h_0 is a nontrivial common factor of f_1, f_2 in $R[y]$. Contradiction.

(d): If $P < R[y]$ is prime and **not principal**, we will show that $R \cap P = (p)$ for some nonzero prime $p \in R$. First note that $R \cap P$ is a prime ideal of the subring R. Indeed, given $a \in R$ and $b \in P$ we have $ab \in R$ since R is a subring and $ab \in P$ since P is an ideal, hence $ab \in R \cap P$ and we see that $R \cap P$ is an ideal of R. Then given $a, b \in R \setminus P$ we have $ab \in R$ since R is a subring and $ab \notin P$ since P is prime, hence $ab \in R \cap P$ and we see that $R \cap P$ is prime in R. /// Now consider two coprime elements $f_1, f_2 \in P$, which exist by part (b). By part (c) we know that f_1, f_2 are also coprime in $K[y]$. Since $K[y]$ is a PID there exist $g, h \in K[y]$ such that $1 = gf_1 + hf_2$. If $0 \neq a \in R$ is a common denominator of all the coefficients of $g(y)$ and $h(y)$ then we have $ag, ah \in R[y]$ and hence $0 \neq a = (ag)f_1 + (ah)f_2 \in R \cap P$. Since $R \cap P$ is a nonzero prime ideal of the PID R we conclude that $R \cap P = (p)$ for some prime $p \in R$.

(e): Let $P < R[y]$ be prime and **not principal**. By part (d) we know that $R \cap P = (p)$ for some prime $p \in R$. Let $f \mapsto \bar{f}$ be the reduction homomorphism $R[y] \to R/(p)[y]$ and let $\bar{P} \subseteq R/(p)[y]$ be the image of P under reduction. We claim that $\bar{P}$ is a prime ideal of $R/(p)[y]$. To show this, first note that the kernel of the reduction map is contained in P. Indeed, if $\bar{\alpha}(y) = 0$ then $\alpha(y) = p \cdot \beta(y)$ for some $\beta(y)$. Since $p \in P$ and $P < R[y]$ is an ideal this implies $\alpha(y) \in P$. /// Now for any $F, G \in R/(p)[y]$ there exist (nonunique) $f, g \in R[y]$ such that $\bar{f} = F$ and $\bar{g} = G$. If $F, G \in \bar{P}$ then we can choose $f, g \in P$ and hence $f - g \in P$ which implies that $F - G = \bar{f} - \bar{g} = \overline{f - g} \in \bar{P}$. If $F \notin \bar{P}$ and $G \in \bar{P}$ then we can choose $g \in P$, hence $fg \in P$ and $FG = \bar{f}\bar{g} = \overline{fg} \in \bar{P}$. If $FG \in \bar{P}$ then there exists $h \in P$ such that $\bar{h} = FG = \bar{f}\bar{g} = \overline{fg}$, hence $0 = \bar{h} - \overline{fg} = \overline{h - fg}$. Since $h - fg$ is in the kernel we have $h - fg \in P$ and since $h \in P$ this implies $fg \in P$. Finally, since P is prime this implies $f \in P$ or $g \in P$, hence $F \in \bar{P}$ or $G \in \bar{P}$. We conclude that $\bar{P}$ is a prime ideal. ///

(e'): Continuing from part (e), since $\bar{P} < R/(p)[y]$ is a prime ideal and since $R/(p)[y]$ is a PID (because $R/(p)$ is a field, because $p \in R$ is prime in the PID R, because etc.), we have $\bar{P} = (F)$ where we can choose $f \in P$ such that $F = \bar{f}$ is irreducible in $R/(p)[y]$. Thus, given any $\varphi \in P$ we have $\bar{\varphi} = \bar{f}\bar{g}$ for some $g \in R[y]$, hence $0 = \bar{\varphi} - \bar{f}\bar{g} = \bar{\varphi} - \overline{fg} = \overline{\varphi - fg}$. Since $\varphi - fg$ is in the kernel of the reduction we have $\varphi(y) - f(y)g(y) = p \cdot h(y)$ for some $h(y)$. Finally, we conclude that $\varphi(y) = p \cdot h(y) + f(y)g(y) \in (p, f)$, and hence $P \leq (p, f)$. On the other hand, since p and f are in P we have $(p, f) \leq P$. **We conclude that any nonprincipal prime $P < R[y]$ has the form $P = (p, f)$ where $p \in R$ is prime and the reduction $\bar{f} \in R/(p)[y]$ is irreducible.**

(f): (Tying up loose ends.) It remains to show that any such ideal is prime. So choose any prime $p \in R$ and any $f \in R[y]$ such that $\bar{f} \in R/(p)[y]$ is irreducible. One can check that $R[y]/(p, f) \approx (R/(p)[y])/(\bar{f})$. (You didn't think I was going to prove absolutely **everything**, did you? I'm tired.) Since $\bar{f}$ is irreducible in the PID $R/(p)[y]$ we know that $(\bar{f})$ is a maximal ideal, hence $(R/(p)[y])/(\bar{f})$ is a field. Thus $R[y]/(p, f)$ is a field and we conclude that $(p, f) < R[y]$ is a **maximal ideal**. Could it possibly be a principal ideal? No. If $(g) < R[y]$ is any proper principal ideal, we will show that (g) is not maximal. First suppose that $g \in R$ is a constant and let $p \in R$ be any prime divisor of g. Then we have a strict inclusion $(g) < (p, y)$. (It's an inclusion because $g = pk \in (p, y)$ for some $k \in R$ and it's strict because the variable y is not in (g).) We also know that $(p, y) \neq R[y]$ because $R[y]/(p, y) \approx (R/(p)[y])/(y) \approx R/(p)$ is not the zero ring. Next suppose that $g(y) \in R[y]$ is not a constant and choose a prime p that does **not** divide the leading coefficient of $g(y)$. Then the reduction $\bar{g}(y)$ is not a unit in $R/(p)[y]$ because it is not a constant in $R/(p)[y]$ (the units of $R/(p)[y]$ are constants because $R/(p)$ is a domain). Hence $(\bar{g}(y)) < R/(p)[y]$ is a proper ideal and $R[y]/(p, g(y)) \approx (R/(p)[y])/(\bar{g}(y))$ is not the zero ring. This gives us strict inclusioins $(g(y)) < (p, g(y)) < R[y]$ and we conclude that $(g(y))$ is not maximal.

In summary, we have classified all the maximal and prime ideals of $R[y]$ when R is a PID. This includes the cases $\mathbb{Z}[y]$ and $K[x, y]$ where K is a field. □

[Apology: Believe it or not, this is the shortest proof I could find. It seems that further progress in this subject will require a more casual relationship with the notion of proof.]

[Remark: Since $y^4 + 1 \in \mathbb{Z}[y]$ is an irreducible polynomial (I won't prove this) we know that $(y^4 + 1) < \mathbb{Z}[y]$ is a prime ideal. But it is not a maximal ideal because the prime 2 does not divide the leading coefficient so we have strict inclusions $(y^4 + 1) < (2, y^4 + 1) < \mathbb{Z}[y]$. This does **not** mean, however, that $(2, y^4 + 1)$ is maximal. It's not even prime. Since $y^4 + 1 = (y + 1)^4 \bmod 2$ we have $(2, y^4 + 1) < (2, y + 1)$, which **is** maximal because $y + 1$ is irreducible mod 2. In fact, Hilbert showed that $y^4 + 1 \in \mathbb{Z}[y]$ is **reducible** mod p for any prime p! So there is **no** maximal ideal of the form $(p, y^4 + 1)$. The ideal theory of $\mathbb{Z}[y]$ encodes all information about which polynomials are reducible modulo which primes. However, it also has a strong resemblance to the ideal theory of $K[x, y]$ so it resembles in some way the theory of algebraic curves in the plane K^2. Weird.]

Problem 2. **($K[x,y]$ for algebraically closed K)** Now let K be an algebraically closed field and let $\mathfrak{m} < K[x,y]$ be a maximal ideal. By Problem 1 we know that $\mathfrak{m} = (p, f)$, where: $p \in K[x]$ is irreducible, $f \in K[x,y]$, and $\bar{f} \in (K[x]/(p))[y]$ irreducible.

(a) Show that $p = x - \alpha$ for some $\alpha \in K$.
(b) Show that $K[x]/(x-\alpha) \approx K$.
(c) Conclude that $f = y - \beta$ for some $\beta \in K$ and hence

$$\mathfrak{m} = (x - \alpha, y - \beta).$$

(d) Find a maximal ideal in $\mathbb{R}[x,y]$ that does **not** look like this. [Hint: Let $p = x^2 + 1$.]

Proof. Since $p \in K[x]$ is an irreducible polynomial and since K is algebraically closed we know that $p = x - \alpha$ for some $\alpha \in K$. (It makes no difference to assume that the leading coefficient is 1.) This proves (a). For (b) we consider the evaluation map $\mathsf{ev}_\alpha : K[x] \to K$. This map is surjective because $\mathsf{ev}_\alpha(c) = c$ for all $c \in K$. Since the kernel is $(x - \alpha)$ we conclude by the First Isomorphism Theorem that $K[x]/(x - \alpha) \approx K$. Then since $\bar{f} = f$ is irreducible in $K[x]/(x-\alpha)[y] \approx K[y]$ we conclude that $f = y - \beta$ for some β, proving (c). For part (d) note that $p := x^2 + 1$ is irreducible in $\mathbb{R}[x]$ and that $\mathbb{R}[x]/(x^2+1) \approx \mathbb{C}$ (where i is the image of x). Thus we only need to find an irreducible polynomial $\bar{f}(y) \in \mathbb{C}[y]$. Any degree 1 polynomial will do; I'll choose $\bar{f}(y) = y + i \in \mathbb{C}[y]$ so that $f(y) = y + x \in \mathbb{R}[x,y]$. We conclude that $(x^2 + 1, y + x)$ is a maximal ideal of $\mathbb{R}[x,y]$. □

[Congratulations. We just proved the 2-dimensional Nullstellensatz. Which proof do you like better: this one or the one using Noether Normalization and Zariski's Lemma?]

Problem 3. **(Zorn's Lemma)** In a partially ordered set $(\mathcal{P}, \leq)$ we say that $C \subseteq \mathcal{P}$ is a chain if for all $c_1, c_2 \in C$ we have $c_1 \leq c_2$ or $c_2 \leq c_1$. "Zorn's Lemma" is actually an **axiom** which is equivalent to the Axiom of Choice. It says the following:

> *Let $(\mathcal{P}, \leq)$ be* **nonempty**. *If every chain $C \subseteq \mathcal{P}$ has an upper bound (i.e., there exists $u \in \mathcal{P}$ such that $c \leq u$ for all $c \in C$) then $\mathcal{P}$ contains a maximal element (i.e., there exists $m \in P$ such that $p \leq m$ for all $p \in \mathcal{P}$).*

Now let R be a ring, let $I < R$ be a proper ideal, and let $S \subseteq (R, \times, 1)$ be a subsemigroup that is disjoint from I. (Note that we always have $1 \in S$.)

(a) Use Zorn's Lemma to prove that the set of ideals containing I and disjoint from S has a maximal element. [Remark: If $S = \{1\}$, this result implies that every proper ideal is contained in a maximal ideal.]
(b) Prove that this maximal element is a prime ideal. [Hint: Let $P < R$ be a maximal element. If $f, g \notin P$ then the ideals $P + (f)$ and $P + (g)$ are strictly bigger than P, hence they both intersect S. Use this fact to show that $fg \notin P$.]

Proof. For part (a), let $\mathcal{P}$ be the set of ideals $J < R$ such that $I \leq J$ and $J \cap S = \emptyset$. Note that $I \in \mathcal{P}$ by assumption so that $\mathcal{P} \neq \emptyset$. If $J_1 \leq J_2 \leq \cdots$ is a chain of ideals in $\mathcal{P}$ then we define $J := \cup_i J_i$. Note that J is an ideal of R since given any $a, b \in J$ and $r \in R$ there exists some n such that a and b are in J_n, and then $a - rb \in J_n \subseteq J$. Note also that J is disjoint from S because if there exists some $a \in J \cap S$ then this a is in $J_n \cap S$ for some n, contradicting the fact that $J_n \cap S = \emptyset$. Hence $J \in \mathcal{P}$ is an upper bound for the chain and Zorn's Lemma implies that $\mathcal{P}$ has a maximal element.

For part (b), let P be a maximal element of the set $\mathcal{P}$. We will show that P is a prime ideal of R. So consider any $f, g \in R$ such that $f, g \notin P$. The ideals $P + (f)$ and $P + (g)$ are strictly bigger than P so they both intersect S. Say we have $x, y \in S$ with $x = p_1 + r_1 f$ and $y = p_2 + r_2 g$ with $p_1, p_2 \in P$ and $r_1, r_2 \in R$, hence

$$xy = (p_1 + r_1 f)(p_2 + r_2 g) = p_1 p_2 + p_1 r_2 g + p_2 r_1 f + r_1 r_2 fg.$$

If $fg \in P$ then the above equation implies that $xy \in P$. But since S is closed under multplication we also know that $xy \in S$. Since $P \cap S = \emptyset$ we conclude that $xy \notin P$. □

Problem 4. (The Radical of an Ideal) Given a ring R we say that $f \in R$ is nilpotent if there exists n such that $f^n = 0$. We define the nilradical as the set of nilpotent elements:

$$\sqrt{0} := \{f \in R : f^n = 0 \text{ for some } n\}.$$

(a) Prove that $\sqrt{0}$ is an ideal. [Hint: Binomial Theorem.]

(b) Prove that $\sqrt{0}$ is the intersection of all prime ideals of R. [Hint: If $f \in R$ is nilpotent show that it belongs to every prime ideal. Conversely, suppose that $f \in R$ is **not** nilpotent. Since $0 \notin S = \{1, f, f^2, \ldots\}$, Problem 3 implies that there exists a prime ideal **not** containing f.]

(c) More generally, given any ideal $I \leq R$ we define its radical:

$$\sqrt{I} := \{f \in R : f^n \in I \text{ for some } n\}.$$

Prove that $\sqrt{I}$ is the intersection of all prime ideals containing I. [Hint: The "same" proof works.]

Proof. For part (a) consider $f, g \in \sqrt{0}$, say $f^m = 0$ and $g^n = 0$. Then for any $r \in R$ we have

$$(f - rg)^{m+n} = \sum_{i+j=m+n} \binom{m+n}{i} f^i (-r)^j g^j.$$

But note that every term in this sum is zero because for all $i + j = m + n$ we must have $i \geq m$ (hence $f^i = 0$) or $j \geq n$ (hence $g^j = 0$). Hence $f - rg \in \sqrt{0}$.

For parts (b) and (c), let $I < R$ be any proper ideal. First we will show that $\sqrt{I} \subseteq \bigcap \{P \text{ prime } : I \leq P\}$. So let $f \in \sqrt{I}$ and consider **any** prime P containing I. Since $f \in \sqrt{I}$ there exists n such that $f^n \in I \leq P$. Then since P is prime and $f = f \cdot f^{n-1} \in P$ we have $f \in P$ or $f^{n-1} \in P$. If $f^{n-1} \in P$ then we conclude by induction that $f \in P$. Next we will show that $\bigcap \{P \text{ prime } : I \leq P\} \subseteq \sqrt{I}$. So suppose that $f \notin \sqrt{I}$ and consider the multiplicative set $S = \{1, f, f^2, \ldots\}$. Since I is disjoint from S we know from Problem 3 that the set of ideals containing I and disjoint from S contains a maximal element. This maximal element is a **prime** ideal not containing f, hence $f \notin \bigcap \{P \text{ prime } : I \leq P\}$. □

[Remark: The general Nullstellensatz says that if K is an algebraically closed field and I is an ideal in $K[x_1, \ldots, x_n]$, then the set of polynomials (thought of as functions $K^n \to K$) that vanish everywhere that I does is exactly $\sqrt{I}$. In other words, if $f \in K[x_1, \ldots, x_n]$ vanishes on the set $V(I) = \{\alpha \in K^n : g(\alpha) = 0 \text{ for all } g \in I\}$ then $f^n \in I$ for some n. For example consider an irreducible polynomial $f(x, y) \in \mathbb{C}[x, y]$. If $g(x, y) \in \mathbb{C}[x, y]$ is any polynomial that vanishes on the curve $\{(x, y) \in \mathbb{C}^2 : f(x, y) = 0\}$ then $g(x, y) = f(x, y)h(x, y)$ for some $h(x, y) \in \mathbb{C}[x, y]$. This simple case of the Nullstellensatz is called Study's Lemma.]