PROOF OF THE PROJECTIVE NULLSTELLENSATZ

SACHA DE POYEN

Abstract. This paper aims to motivate the correspondence between algebraic sets and radical ideals by explaining why a more general correspondence between sets of n-tuples and sets of polynomials in n variables fails. To do this, we introduce the necessary ideas, including ideals, varieties, then prove the Nullstellensatz in both an affine and projective situation. The first part introduces readers to ideals and varieties, as well as affine and projective spaces. The second proves the Nullstellensatzes, using the Rabinschowitz trick for the affine case; and uses the affine case, as well as some facts about projective ideals to prove the projective nullstellensatz case.

Contents

1. Ideals and Varieties

Definition 1.1. $\mathbb{A}^n(k)$ is the set of to n-tuples of elements of the field k. If the field is clear from the context, then we denote it by $\mathbb{A}^n$.

It is natural to ask if there is a correspondence between subsets of $\mathbb{C}[x_1, ..., x_n]$ and $\mathbb{A}^n$, and if so, what would such a correspondence look like. In a perfect world we would have something of the following form:

$$\{\text{sets of polynomials}\} \leftrightarrow \{\text{subsets of } \mathbb{A}^n\}.$$

A strong candidate arises when examining the relationship between sets of polynomials and their solution sets. We define a set map

$$V : \{\text{sets of polynomials}\} \to \{\text{subsets of } \mathbb{A}^n\},$$
$$V(S) = \{x \in \mathbb{A}^n | f(x) = 0 \text{ for all } f \in S\},$$

and another map

$$I : \{\text{subsets of } \mathbb{A}^n\} \to \{\text{sets of polynomials}\},$$
$$I(V) = \{f \in \mathbb{C}[x_1, ..., x_n] | f(y) = 0 \text{ for all } y \in V\}.$$

These maps have an interesting property called reverse inclusion. If $I \subset J$, then $V(J) \subset V(I)$, and if $V \subset W$, then $I(W) \subset I(V)$. Unfortunately V isn't injective; the sets $\{x\}$ and $\{x^2\}$ have the same set of zeroes and thus have the same image under V. Nor is it surjective; no set of polynomials has $\mathbb{Z}$ as its solution set. The same is true for I; the same examples prove this. To show that I isn't injective, take the sets $\mathbb{Z}$ and $\mathbb{A}$. Their images under I are both $\{0\}$ as no other polynomial in one variable has infinitely many solutions. Let $f \in I(S)$, then $f^2 \in I(S)$ as well. If $f \neq 0$, then $f^2 \neq f$, so $I(S) \neq \{f\}$. As there is no set S such that $I(S) = \{f\}$, I isn't surjective on $\mathbb{C}[x_1, ..., x_n]$.

Definition 1.2. A subset X of $\mathbb{A}^n$ is called algebraic if there exists some set F of polynomials such that $f(x) = 0$ for all $f \in F$ and $x \in X$.

Restricting the codomain of V from all subsets of $\mathbb{A}^n$ to the set of algebraic sets makes V surjective.

$$\{\text{sets of polynomials}\} \to \{\text{algebraic subsets of } \mathbb{A}^n\}.$$

If we want V to be injective, we also need to introduce the concept of an ideal.

Definition 1.3. We say a subset I of a ring R is an ideal if:
1. $i + j \in I$ for all $i, j \in I$
2. $ri \in I$ for all $i \in I$ and $r \in R$

Lemma 1.4. *$I(V)$ is an ideal.*

Proof. It suffices to show $I(V)$ is closed under addition and $h \cdot f \in I(V)$ for all $f \in I(V)$ and all $g \in \mathbb{C}[x_1, ..., x_n]$.

Let $f, g \in I(V)$ and $h \in k[x_1, ..., x_n]$. Then for all $y \in V, (f + g)(y) = f(y) + g(y) = 0$.

Further, $fh(y) = 0 \cdot h(y) = 0$, so $fh \in I(V)$ as well. □

We can restrict V to ideals without losing any algebraic sets, as the vanishing set of a set of polynomials is the same as the vanishing set of the ideal generated by those polynomials.

Lemma 1.5. *$V(S) = V(I)$ where I is the ideal generated by S.*

Proof. Let $y \in V(S)$ and $f \in I$. I is generated by S, so $f = a_1g_1 + a_2g_2 + ... + a_ng_n$ for some $\{g_1, ..., g_n\}$ in S. It follows that $f(y) = \sum_{1 \leq i \leq n} a_ig_i(y)$. Each $g_i \in S$, so $g_i(y) = 0$ for all y. Then $f(y) = 0$. □

In fact, the reason why this map is denoted by the letter I is because $I(V)$ is the ideal corresponding to V. But even then, the ideals (x) and (x^2) still correspond to the same algebraic set, so the function isn't injective.

Lets investigate why two ideals (f) and (g) might generate the same algebraic set. In the case of (x) and (x^2), we have that $x|x^2$, and one might assume that is a sufficient condition, but that isn't true. Take for example $f = (x - a)$ and $g = (x - a)(x - b)$, then $V(f) \subsetneq V(g)$. The example of (x) and (x^2) gives us another important clue, namely that $V(f) = V(f^n)$ for all n. Combining the two insights above, we realize that (f) and (g) generate the same set when $f|g^n$ and $g|f^m$. To generalize this to non-principal ideals, $V(f_1, ..., f_n) = V(g_1, ..., g_m)$ when there exists an N such that $f_i^N \in (g_1, ..., g_m)$ and M such that $f_j^M \in (f_1, ..., f_n)$.

Proof. To see this apply the fact that g^n has the same set of solutions as g, and that $f|g^n$ implies that $V(f) \subset V(g^n) = V(g)$. As $g|f^m$ we also have $V(g) \subset V(f^m) = V(f)$, thus they are equal. □

Not all ideals are principal, and for non-principal ideals, Then we can eliminate this "double counting" by only considering ideals which are *radical*.

Definition 1.6. For some ideal I, $\sqrt{I} = \{a | a^n \in I \text{ for some } n \in \mathbb{N}\}$

Definition 1.7. An ideal M is called *radical* if $\sqrt{I} = I$.

This gives us the desired bijection, but to show that, we must first prove Hilbert's nullstellensatz, which we will return to later. In the mean time, I would like to prove that for all algebraic sets X, $I(X)$ is a radical ideal.

Proof. Let X be an algebraic set, and suppose $f^n \in I(X)$, then $f^n(x) = 0$ for all $x \in X$, if $f^n(x) = 0$, suppose for contradiction that $f(x) = a \neq 0$, then $f^{n-1}(x) = 0$, and by induction $f^2(x) = 0$. Yet $0 = f^2(x) = f(x)f(x) = a^2$ for some $a \neq 0$, yielding a contradiction as the product of nonzero numbers is nonzero (over $\mathbb{C}$). □

We should turn our attention to the other map, that from algebraic sets to ideals. There are cases where $U \neq V(I(U))$, like the aforementioned $\mathbb{Z}$ case. One can find other examples of this by subtracting a single (or finite number) of points from an algebraic set. Then if we limit ourselves to sets of the form $V(I(U))$, we have no double counting, and each thing of the form $V(I(U))$ is also an algebraic set. The same prodcedure that makes I surjective, makes V injective.

Lemma 1.8. $I(U) = I(V(I(U)))$

Proof. Consider some point $x \in U$, then $f(x) = 0$ for all $f \in I(U)$, and thus $x \in V(I(U))$. Thus $U \subset V(I(U))$.

Consider some $f \in J$, then $f(x) = 0$ for all $x \in V(J)$, thus $f \in I(V(J))$. Thus $J \subset I(V(J))$.

Then consider $I(V(I(U)))$. On the one hand $U \subset V(I(U))$ so $I(U) \supset I(V(I(U))$, on the other hand, $I(U) \subset I(V(I(U))$. Then they are equal. □

From this, we conclude that for two subsets of U, W of $\mathbb{A}^n$, $I(U) = I(W) = I(V(I(U))$. Considering only elements of the form $V(I(U))$ eliminates the possibility of double counting.

Additionally, restricting to radical ideals makes this map surjective. If R is a radical ideal, then $V(R)$ is an algebraic set, and $I(V(R)) = R$ (again by Hilbert's nullstellensatz), thus every radical ideal has a preimage under V.

We can then use ideals instead of sets, as no useful information is lost in doing so. Restricting ourselves to ideals in place of sets goes a long way to giving us a correspondence between $k[x_1, ..., x_n]$ and $\mathbb{A}^n$, but this relationship is still not bijective. The second direction of the previous proof touches on an important property of this ideal-variety correspondence, namely reverse inclusion. If $I \subset J$, then $V(J) \subset V(I)$. This type reverse inclusion will be familiar to anyone who knows of the Galois correspondence, where a subset of the Galois group corresponds fixes a larger Galois extension. There are also specific types of ideals that the reader should be familiar with:

Definition 1.9. An ideal P is called *prime* if $ab \in P$ if and only if $a \in P$ or $b \in P$.

Definition 1.10. An ideal M is called *maximal* if it isn't contained in any proper ideal.

Also here is a theorem that one should know:

Theorem 1.11. *For P prime, R/P is an integral domain, for M maximal R/M is a field.*

Knowledge of this is necessary for some proofs in this paper. See Dummit and Foote for further details. The following may be new to a reader:

Lemma 1.12. *Let K be an algebraic extension of F. If F is algebraically closed, then $F \cong K$.*

Proof. If K is algebraic of F, then for all $k \in K$, there exists $f \in F[x]$ such that $f(k) = 0$. Then $k \in F$, as F contains its roots. □

Theorem 1.13. *$V(I(X)) \supset X$ and $I(V(S)) \supset S$.*

Proof. Let $x \in X$, then for all $f \in I(X)$, $f(x) = 0$, thus $x \in V(I(X)$. Similarly, let $f \in S$, then for all $x \in V(S), f(x) = 0$, then $f \in I(V(S))$. □

Theorem 1.14. *If X is algebraic, $V(I(X)) = X$.*

Proof. If X is algebraic, then $X = V(J)$ for some ideal J, and $V(I(X)) = V(I(V(J))$. As $I(V(J)) \supset J$, $V(I(V(J))) \subset V(J)$. On the other hand, $V(I(V(J)) \supset V(J)$. □

Theorem 1.15. *Every prime ideal is radical.*

Proof. Let P be a prime ideal; suppose for contradiction that it isn't radical. Then there exists some $a \notin P$ and $n \in N$ such that $a^n \in P$. If $a^k \in P$ and $a \notin p$, then $a^{k-1} \in P$ as P is prime. By induction, $a \in P$, yielding a contradiction. □

Theorem 1.16. *V is irreducible if and only if $I(V)$ is prime.*

Proof. Suppose V is reducible, then there exist U, W such that $U \cup W = V$, then $I(V) \subset I(U)$ and $I(V) \subset I(W)$. Pick $F \in I(U) - I(V)$ and $G \in I(W) - I(V)$, then $V(FG) = V(F) \cup V(G) \supset U \cup W = V$. Thus $FG \in I(V)$.

Suppose $I(V)$ isn't prime, then there exist $F, G \notin I(V)$ such that $FG \in I(V)$, and consider the ideals $(I(V), F)$ and $(I(V), G)$. Both ideals contain $I(V)$ so $V(I(V), F) \subset V$ and $V(I(V), G) \subset V$ so $V(I(V), F) \cup V(I(V), G) \subset V$. Further, $Vevery \subset V(I(V), F) \cup V(I(V), G)$ as for all $y \in V$, $fg(y) = 0$ implies either $f(y) = 0$ or $g(y) = 0$. [2] (1.5) □

In fact, it is true in general that $V(IJ) = V(I) \cup V(J)$.

Theorem 1.17. *The ideal $(x_1 - a_1, x_2 - a_2, ..., x_n - a_n)$ is maximal.*

Proof. Suppose that $I = (x_1 - a_1, ..., x_n - a_n)$ isn't maximal. Then there exists some ideal J satisfying $I \subsetneq J$. $I \subsetneq J$ implies that $V(J) \subsetneq V(I)$, but $V(I) = \{(a_1, a_2, ..., a_n)\}$ consists of only one point, so $V(J) = \emptyset$. We conclude that $J = \mathbb{C}[x_1, ..., x_n]$.

□

2. Projective Space

Before progressing to the Nullstellensatz, we should also introduce the concept of projective space. Consider some points a and b of $\mathbb{A}^{n+1}$. Each of these points defines a line passing through the origin. Define a relation where $a\ b$ if $(0, a, b)$ are colinear, or equivalently $a = \lambda b$ for some $\lambda \in \mathbb{R}$. This relation is:
(i) Symmetric, as $a = \lambda b$ implies $b = \frac{1}{\lambda}a$.
(ii) Reflexive, as $a = 1 \cdot a$
(iii) Transitive, as $a = \lambda_1 b$ and $b = \lambda_2 c$ implies $a = \lambda_1\lambda_2 c$.
Then this is an equivalence relation. Let $\mathbb{P}^n$ denote the set of equivalence classes of $\mathbb{A}^{n+1}$ under this relation. $\mathbb{P}^n$ can be though of as the set of lines in $\mathbb{A}^{n+1} \setminus 0$ that pass through the origin.

Any point $P \in \mathbb{P}^n$, can be written $P = [x_1 : x_2 : ... : x_n : x_{n+1}]$. Fulton notes that the values of x_i are not well defined, but that the ratios $x_i : x_j$ are well defined for all $x_j \neq 0$. In essence $P = [x_1 : x_2 : ... : x_{n+1}] = [\lambda x_1 : \lambda x_2 : ... : \lambda x_{n+1}]$ for all $\lambda \in \mathbb{R} - 0$. Note that $x_i = 0$ if and only if $\lambda x_i = 0$, so the zeroes are the same regardless of the choice of λ.

In this way, $\mathbb{P}^n$ can be divided into two (disjoint) sets, namely the set of points whose x_i coordinate is non-zero, and those whose x_i coordinate is zero. Define $U_i = \{[x_1 : x_2 : ... : x_{n+1}] | x_i \neq 0\}$. As the choice of i is arbitary, we will consider only U_{n+1} going forward.

Every point $P \in U_{n+1}$ can be written in the form $[x_1 : ... : x_n : 1]$. This form suggests a natural bijection

$$\mathbb{A}^n \longrightarrow U_{n+1}$$
$$(x_1, x_2, ..., x_n) \to [x_1 : x_2 : ... : x_n : 1].$$

Denote $H_\infty = \mathbb{P}^n - U_{n+1} = \{[x_1 : ... : x_n : x_{n+1}] | x_{n+1} = 0\}$. H_∞ can be identified with $\mathbb{P}^{n-1}$.

It is natural to wonder why U_{n+1} is identified with $\mathbb{A}^n$ while H_∞ is identified with $\mathbb{P}^{n-1}$. The answer lies in the fact that for some point $P \in H_\infty$, $\lambda P = [\lambda x_1 : ... : \lambda x_n : \lambda \cdot 0] = [\lambda x_1 : ... : \lambda x_n : 0] = [x_1 : ... : x_n : 0]$, while for $P \in U_{n+1}$, $P = [x_1 : ... : x_n : 1] = [\lambda x_1 : ... : \lambda x_n : \lambda] \neq [\lambda x_1 : ... : \lambda x_n : 1]$.

Before progressing, we should ask ourselves what exactly it means for a $P \in \mathbb{P}^n$ to be a zero of a polynomial. There is no canonical $(n+1)$-tuple corresponding to P, instead, we say that $f(P) = 0$ if $f(\lambda x_1, ..., \lambda x_n) = 0$ for all $\lambda > 0$ where $x = [x_1 : ... : x_n : x_{n+1}]$ are homogeneous coordinates for P.

Definition 2.1. Given a set S, the *cone* of S is the set $\{\lambda x | \lambda > 0, x \in S\} \cup \{0\}$.

The cone of S is denoted $C(S)$. If you were to imagine that S was a circle over the origin, then $C(S)$ would be the cone with S as a base, and the origin as the vertex.

Definition 2.2. A polynomial $p(x_1, x_2, ..., x_n)$ is called homogeneous in n variables, or simply homogeneous if all its terms are of the same degree. In his book, Fulton refers to homogeneous polynomials as forms.

Homogeneous polynomials have the following property:

$$F(\lambda(x_1, ..., x_n)) = \lambda^n F((x_1, ..., x_n)).$$

For homogeneous coordinates x and y corresponding to P, $F(y) = \lambda F(x)$, and $F(x)$ and $F(y)$ correspond to the same projective point. As a consequence, $F(P)$ is well defined for all $P \in \mathbb{P}^n$.

Definition 2.3. An ideal I is called homogeneous if its is generated by homogeneous polynomials.

Lemma 2.4. *$I_p(X) = I_a(C(X))$; if I homogeneous and $V_p(I) \neq \emptyset$, then $C(V_p(I)) = V_a(I)$.*

Proof. First suppose that $f(x) \in I_p(X)$, then $f(\lambda x) = 0$ for all $x \in X$, or equally $f(y) = 0$ for all $y \in C(X)$. Thus $f \in I_a(C(X))$.

Now suppose $f \in I_a(C(X))$, then $f(\lambda x) = 0$ for all $x \in X$. Thus $f \in I_p(X)$. Thus (1) is proved.

Now for (2). Let I be homogenous, and $V_p(I) \neq 0$. First note that if $x \in V_p(I)$, then $x \in V_a(I)$ as $f(x) = 0$ for all $f \in I$, thus $V_p(I) \subset V_a(I)$. Then, we know that I is homogeneous, so $f(\lambda x) = \lambda f(x)$, thus $C(V_p(I)) \subset V_a(I)$.

Additionally, $x \in V_a(I)$ implies $\lambda x \in V_a(I)$ as I homogeneous. Then $[x] \in V_p(I)$ so $x \in C(V_p(I))$. Thus $C(V_p(I)) = V_a(I)$ by mutual inclusion. □

3. Nullstellensatz(es)

To prove the Affine Nullstellensatz, better known as Hilbert's Nullstellensatz, we start by proving the weak Nullstellensatz, then use what is known as the Rabinowitsch trick.

Theorem 3.1. *Let k be a field with infinitely many elements, and let $A = k[a_1, ..., a_n]$, be a finitely generated k-algebra. If A is a field, then A is algebraic over k.*

Proof. Assume for contradiction that A is not algebraic over k, then there is some $t \in A$ such that t is transcendental over k. If A is a field, then $k[t] \subset A$ implies $k(t) \subset A$, but this poses a problem, namely that $k(t) \cong k(x)$, which is not a finitely generated k-algebra. To see this, assume there exists set $\{v_1, ..., v_m\}$ such that $k[v_1, ..., v_m] = k(x)$, then each $v_i = \frac{f_i}{g_i}$, so they have a common denominator $d = \prod g_i$. This implies that for all $z \in k[v_1, ..., v_m]$, there exists l such that $d^l z \in k[x]$ (in particular l is the degree of the minimal polynomial of z). But this isn't true for $k(x)$ as b is divisible by only finitely many prime (irreducible) elements of $k[t]$, while Euclid's theorem shows that there are infinitely many primes in $k[t]$, thus there are some elements of $k(t)$ whose denominators cannot be eliminated by any power of d. [1](Hulek 1.15, for alternative proof see Fulton 1.44) □

Theorem 3.2 (Weak Nullstellensatz)**.** *Let I be a proper ideal of $\mathbb{C}[x_1, ..., x_n]$, then $V(I) \neq 0$.*

Proof. As I is a proper ideal, it is contained in some maximal ideal J. $K = k[x_1, ..., x_n]/J$ is a field. By Theorem 3.1, we have that $k[x_1, ..., x_n]/J$ is an algebraic extension of k. By our assumptions, k is algebraically closed, so $k[x_1, ..., x_n]/J \cong k$. The first isomorphism theorem gives us a surjective homomorphism

$$\pi : k[x_1, ..., x_n] \longrightarrow k$$

with kernel J and an isomorphism

$$\varphi : k = k[x_1, ..., x_n] \longrightarrow k.$$

Suppose $\pi(x_i) = b_i$, and define $a_i = \varphi^{-1}(b_i)$ then $x_i - a_i \in J$. Thus $(x_1 - a_1, ..., x_n - a_n) \subset J$. But $(x_1 - a_1, ..., x_n - a_n)$ is a maximal ideal so $J = (x_1 - a_1, ..., x_n - a_n)$. Then $V(J) = \{a_i\}$, and $I \subset J$ implies $V(J) \subset V(I)$, so $V(I) \neq \emptyset$. [2] (Fulton 1.7) □

Theorem 3.3 (Hilbert's Nullstellensatz)**.** $I(V(I)) = \sqrt{I}$

Note: Fulton says that $I(V(I)) = \sqrt{I}$ is equivalent to "if G vanishes whenever $F_1, ..., F_n$ vanish, then $G^n = a_1F_1 + ... + a_nF_n$". This is true for the following reason, which took me longer to grasp than I care to admit: if $F_1, ..., F_n$ be the generators of I, and G vanishes simulatneously with them, then $V(I) \subset V(G)$, which implies that $I(V(G)) \subset I(V(I)) = \sqrt{I}$. As $G \in I(V(G))$, $G \in \sqrt{I}$, so there exists n such that $G^n \in I$. As I is generated by the F_i, G^n be written as a sum of F_i.

Proof. Consider a set of polynomials such that G vanishes whenever all the F_i vanish, then consider the ideal $(F_1, ..., F_n, 1 - x_{n+1}G)$ of $k[x_1, ..., x_{n+1}]$. Note that if all the F_is are zero then so is G, thus $1 - x_{n+1}G = 1$. Thus this ideal has no shared solutions, of $V(F_1, ..., F_n, 1 - x_{n+1}G) = \emptyset$. Thus J cannot be a proper ideal of $k[x_{n+1}]$ by the weak nullstellensatz. Thus $1 \in J$, so 1 can be written as a linear combination of the F_i and G. Then

$$1 = A_1(x_1, ..., x_{n+1})F_1 + ... + A_n(x_1, ..., x_{n+1})F_n + B(x_1, ..., x_{n+1})(1 - x_{n+1}G)$$

. Substituting $x_{n+1} = \frac{1}{y}$ for some y, yields

$$1 = A_1(x_1, ..., \frac{1}{y})F_1 + ... + A_n(x_1, ..., \frac{1}{y})F_n + B(x_1, ..., \frac{1}{y})(1 - \frac{1}{y}G).$$

For sufficiently large n, the $\frac{1}{y}$ terms vanish, and

$$Y^n = A_1(x_1, ..., y)F_1 + ... + A_n(x_1, ..., y)F_n + B(x_1, ..., Y)(Y - G).$$

As Y is arbitrary, setting $Y = G$ gives

$$G^n = A_1(x_1, ..., y)F_1 + ... + A_n(x_1, ..., y)F_n$$

for sufficiently large n. [2] (Fulton 1.7) □

This has several corollaries, the most important of which are three bijections:

$$\{\text{radical ideals}\} \longleftrightarrow \{\text{varieties of } \mathbb{A}^n\},$$

$$\{\text{prime ideals}\} \longleftrightarrow \{\text{irreducible varieties } \mathbb{A}^n\}, \text{and}$$

$$\{\text{maximal ideals}\} \longleftrightarrow \{\text{points in } \mathbb{A}^n\}.$$

Proof. The forward direction of the first bijection follows from Theorem 1.14, and the reverse implication follows from Hilbert's nullstellensatz (Theorem 3.3). The second bijection is proved in Theorem 1.16. The third bijection comes from Theorem 1.17 and the reverse comes from the weak nullstellensatz (Theorem 3.2).

For some radical ideal J, $\sqrt{J} = J$, so $I(V(J)) = J$, and $V(I(X)) = X$ for any algebraic set X. When understood as functions V and I from the radical ideals of $\mathbb{C}[x_1, ..., x_n]$ to the algebraic sets of $\mathbb{A}^n$ and visa-versa, V and I are each other's inverse. In other words, we have built a one-to-one correspondence.

Note that an ideal M generated by $\{x_1 - a_1, ..., x_i - a_i, ..., x_n - a_n\}$ corresponds to a variety consisting of a single point. Then consider $\mathbb{C}[x_1, ..., x_n]/M$. This is isomorphic to $\mathbb{C}$, thus M is maximal. Now suppose M is maximal, then it isn't contained in any proper ideals, by correspondence this means that $V(M)$ doesn't contain any proper algebraic subsets. Yet for all $x \in V(M)$ $\{x\}$ is an algebraic subset of $V(M)$, so $\{x\} = V(M)$.

Now consider some prime ideal P. □

Theorem 3.4 (Projective Nullstellensatz)**.**
(1) $V_p(I) = \emptyset$ if and only if there exists some integer N such that I contains all homogeneous polynomials of degree $\geq N$.
(2) If $V_p(I) \neq 0$, then $V_p(I_p(I)) = \sqrt{I}$.

Proof. We have four equivalent statements:

(i) $V_p(I) = \emptyset$
(ii) $V_a(I) \subset \{(0, 0, ..., 0)\}$
(iii) $Rad(I) = I_a(V_a(I)) \supset (X_1, ..., X_{n+1})$
(iv) $(X_1, ..., X_{n+1})^N \subset I$ for some N.

$(i) \Rightarrow (ii)$:
As shown above, $V_a(I) = C(V_p(I))$, thus if $V_p(I) = \emptyset$, then $C(V_a(I)) = C(\emptyset) \subset \{(0, 0, ..., 0)\}$.
$(ii) \Rightarrow (iii)$:
As $V_a(I) \subset \{(0, 0, ..., 0)\}$, then $I_a(V_a(I)) \supset I_a(\{(0, 0, ..., 0)\}$, or equally,
$\sqrt{I} \supset (X_1, ..., X_{n+1})$.
$(iii) \Rightarrow (iv)$:
As $(X_1, ..., X_{n+1}) \subset \sqrt{I}$, then we know that for all X_i, there exists n_i such that $X_i^{n_i} \in I$. Then let $N = \sum(n_i - 1) + 1$. Then an element $F \in (X_1, ..., X_{n+1})^N$ is the product $F = F_1F_2...F_N$ where each $F_j \in (X_1, ..., X_{n+1})$, so there is some X_i that divides F_j. We only need to consider the case where $F_j \in \{X_1, ..., X_{n+1}\}$, as if the product of the X_js is in I than so too is $\prod f_jX_j$. Assume that $F_1F_2...F_N \notin I$, then $F_1F_2...F_n = X_1^{n_1-1}X_2^{n_2-1}...X_{n+1}^{n_{n+1}-1}$ then regardless of our choice of X_N, we get that $F \in I$.
$(iv) \Rightarrow (i)$:
Suppose $(X_1, ..., X_{n+1})^N \subset I$, then let $p \in \mathbb{P}^n$. Then $V(I) \subset V_p(X_1, ..., X_{n+1}$, so it suffices to show that $V_p(X_1, ..., X_{n+1}) = \emptyset$. But the only common zero of $(X_1, ..., X_{n+1})$ is $(0, 0, ..., 0)$, which has no equivalent in a projective situation. Thus $V_p(X_1, ..., X_{n+1}) = \emptyset$ as desired.

We prove (2) in the following way $V_p(I) \neq \emptyset$, thus by Lemma 2.4, $I_p(V_p(I)) = I_a(C(V_p(I))) = I_a(V_a(I)) = \sqrt{I}$. [2] (Fulton 4.2)

□

Acknowledgements

I would like to thank Samanda Zhang for her excellent mentorship, as well as her patience. I would also like to thank Peter May for running this program and giving me the chance to participate in it this year.

References

[1] Klaus Hulek, Elementary Algebraic Geometry (American Mathematical Society, 2003)
[2] William Fulton, Algebraic Curves (3rd Edition, University of Michigan, 2008) https://dept.math.lsa.umich.edu/ wfulton/CurveBook.pdf
[3] Rabinowitsch, J.L. Zum Hilbertschen Nullstellensatz. Math. Ann. 102, 520 (1930). https://doi.org/10.1007/BF01782361