MAXIMAL IDEALS IN POLYNOMIAL RINGS

KEITH CONRAD

1. Introduction

Our goal here is to prove three results about maximal ideals in polynomial rings: describe the maximal ideals in $K[x_1, \ldots, x_n]$ when K is an algebraically closed field, the maximal ideals in $K[x_1, \ldots, x_n]$ when K is an arbitrary field, and the maximal ideals in $\mathbf{Z}[x]$. The first result has a particularly simple answer (even if the proof requires a fair bit of preliminary work), the second result is a combination of the first result and a group action, and the third result ties together $\mathbf{Z}$ and finite fields (not just fields of prime order).

The proofs of these theorems will use properties of integral ring extensions, which are a generalization of algebraic field extensions to the setting of rings, so we develop a few results about integral ring extensions first in Section 2. We'll describe maximal ideals in $K[x_1, \ldots, x_n]$ for all fields K in Section 3, use that description for algebraically closed K to prove the Nullstellensatz in Section 4, and describe maximal ideals in $\mathbf{Z}[x]$ in Section 5.

2. Integral extensions

For a field extension L/K, we call α in L algebraic over K when α is the root of a nonconstant polynomial $f(x)$ in $K[x]$. Scaling f by a nonzero constant in K does not change its roots, so we can assume $f(x)$ is monic by dividing $f(x)$ by its leading coefficient. If the coefficients of the polynomials do not form a field then saying something is the root of a monic polynomial is a more restrictive condition than it being the root of a general (nonconstant) polynomial. The more restrictive condition (root of a monic polynomial) has many of the useful properties of algebraic extensions.

Definition 2.1. Let B/A be an extension of commutative rings.[1] We call $b \in B$ *integral* over A if there is a monic $f(x) \in A[x]$ such that $f(b) = 0$. The ring B is called *integral* over A or an *integral ring extension* of A if each element of B is integral over A.

Example 2.2. In $\mathbf{Q}(\sqrt{5})$, numbers $a + b\sqrt{5}$ with $a, b \in \mathbf{Z}$ are integral over $\mathbf{Z}$ since $a + b\sqrt{5}$ is a root of

$$(x - (a + b\sqrt{5}))(x - (a - b\sqrt{5})) = x^2 - 2ax + (a^2 - 2b^2),$$

which is monic in $\mathbf{Z}[x]$. Other numbers in $\mathbf{Q}[\sqrt{5}]$ can be integral over $\mathbf{Z}$. For example, $(1 + \sqrt{5})/2$ is not in $\mathbf{Z}[\sqrt{5}]$ but is integral over $\mathbf{Z}$ since it is a root of $x^2 - x - 1$.

Example 2.3. In a ring extension B/A, every $a \in A$ is integral over A since a is a root of $x - a$.

Example 2.4. The number $1/2$ is a root of $2x - 1$ in $\mathbf{Z}[x]$, but this does not directly say whether or not $1/2$ integral over $\mathbf{Z}$ since $2x - 1$ is not monic. In fact, $1/2$ is *not* integral over $\mathbf{Z}$ using an argument by contradiction: if some monic $f(x)$ in $\mathbf{Z}[x]$ has $f(1/2) = 0$ and we write $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, then

$$0 = f\left(\frac{1}{2}\right) = \frac{1}{2^n} + \frac{a_{n-1}}{2^{n-1}} + \cdots + \frac{a_1}{2} + a_0,$$

[1] All rings here will be commutative, so we will henceforth stop using the label "commutative" each time.

so multiplying through by 2^n gives us

$$0 = 1 + 2a_{n-1} + \cdots + 2^{n-1}a_1 + 2^n a_0,$$

which is impossible since the number on the right side is odd. In a similar way, a rational number is integral over $\mathbf{Z}$ if and only if it is an integer: if a/b is rational in reduced form and it is integral over $\mathbf{Z}$, then running through an argument like the one we made with $1/2$ shows $b \mid a^n$, so $b = \pm 1$ since $(a, b) = 1$. (This is essentially the rational roots theorem.)

By similar reasoning, if A is a UFD with fraction field F, the only elements of F that are integral over A are the elements of A. For example, taking $A = \mathbf{Z}[1/N]$ for $N \in \mathbf{Z}^+$ and $F = \mathbf{Q}$, the only rational numbers integral over $\mathbf{Z}[1/N]$ are those in $\mathbf{Z}[1/N]$.

Example 2.5. In $\mathbf{Q}(\sqrt{5})$, $(2+\sqrt{5})/3$ is a root of $f(x) = x^2 - (4/3)x - 1/9$, which is monic. This does not tell us whether or not $(2 + \sqrt{5})/3$ is integral over $\mathbf{Z}$ (it really isn't), but we can say $(2 + \sqrt{5})/3$ is integral over $\mathbf{Z}[1/3]$ since $f(x)$ is monic with coefficients in $\mathbf{Z}[1/3]$.[2]

Example 2.6. If L/K is a field extension, then elements of L are integral over K if and only if they are algebraic over K because a polynomial in $K[x]$ can be scaled within $K[x]$ to become monic without changing its roots.

We will prove two important properties of integrality for a ring extension B/A:

- if B/A is an integral ring extension where A and B are integral domains, then A is a field if and only if B is a field (Theorem 2.7),
- the elements of B that are integral over A form a subring (Corollary 2.10).

Theorem 2.7. *Let B/A be an integral ring extension of integral domains. Then B is a field if and only if A is a field.*

Proof. Suppose A is a field. For nonzero $b \in B$, we want to show b has a multiplicative inverse in B, Let b be a root of a monic polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ in $A[x]$ and pick n to be as small as possible. Then the constant term a_0 can't be 0: if $a_0 = 0$ then

$$0 = f(b) = b^n + a_{n-1}b^{n-1} + \cdots + a_1 b = b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1),$$

so $b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1 = 0$ since B is an integral domain and $b \neq 0$. That equation contradicts the minimality of n, so $a_0 \neq 0$.

Isolate the constant term in the equation $f(b) = 0$:

$$0 = b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 \Longrightarrow b(b^{n-1} + a_{n-1}b^{n-2} + \cdots + a_1) = -a_0.$$

Since $a_0 \neq 0$ in A and A is a field, $-a_0$ has an inverse a'. Multiplying through the last equation by a',

$$b(a'b^{n-1} + a'a_{n-1}b^{n-2} + \cdots + a'a_1) = 1.$$

Thus b has an inverse in $A[b] \subset B$. Since this holds for all nonzero b in B, B is a field.

Now suppose B is a field. Each nonzero $a \in A$ has a multiplicative inverse b in B. We will show $b \in A$. Since b is integral over A, we have a relation

$$b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$$

for some $n \geq 1$ and $a_0, \ldots, a_{n-1} \in A$. Multiplying through the equation by a^{n-1} and using the relation $ab = 1$ kills off all powers of b except a single b in the first term:

$$b(ab)^{n-1} + a_{n-1}(ab)^{n-1} + \cdots + a_1 a^{n-2}(ab) + a^{n-1}a_0 = 0,$$

so

$$b + a_{n-1} + \cdots + a_1 a^{n-2} + a^{n-1}a_0 = 0.$$

All terms on the left after b are in A, so $b \in A$. □

[2]Note the common denominator of the coefficients is 9 and $\mathbf{Z}[1/3] = \mathbf{Z}[1/9]$ since $1/3 = 3(1/9)$.

To prove that the elements of B integral over A form a subring, we will need a characterization of integrality that is linearized (*i.e.*, formulated in terms of modules). It is analogous to the theorem that in a field extension L/K, elements of L are algebraic over K if and only if they lie in an intermediate field extension that is finite-dimensional over K.

Theorem 2.8. *For a ring extension B/A and $b \in B$, the following are equivalent:*

(*i*) *b is integral over A;*
(*ii*) *the subring $A[b]$ is a finitely generated A-module;*
(*iii*) *there is a subring of B containing A and b that is a finitely generated A-module.*

Proof. (*i*) $\Rightarrow$ (*ii*): Say $b^n + a_{n-1}b^{n-1} + \cdots + a_1 b + a_0 = 0$, where $a_i \in A$. Then

$$b^n = -a_0 - a_1 b - \cdots - a_{n-1}b^{n-1} \in A + Ab + \cdots + Ab^{n-1},$$

so

$$b^{n+1} \in Ab + Ab^2 + \cdots + Ab^n \subset A + Ab + \cdots + Ab^{n-1}$$

since $b^n \in \sum_{i=0}^{n-1} Ab^i$. By induction, $b^m \in A + Ab + \cdots + Ab^{n-1}$ for all $m \geq n$, so

$$A[b] = \sum_{i \geq 0} Ab^i = A + Ab + \cdots + Ab^{n-1}.$$

(*ii*) $\Rightarrow$ (*iii*): Use the subring $A[b]$.
(*iii*) $\Rightarrow$ (*i*): Say R is a ring where $A \subset R \subset B$ with $b \in R$, and

$$R = Ax_1 + Ax_2 + \cdots + Ax_n.$$

The x_i's are not all 0, since $1 \in R$ and $1 \neq 0$. (We're bypassing the trivial case that A is the zero ring, whose only ring extension is itself. The theorem is obvious in that case.) Multiplication by b sends R back to R, so

$$bx_i = a_{i1}x_1 + \cdots + a_{in}x_n, \qquad a_{ij} \in A.$$

Collect those equations over all i into a vector-matrix equation

$$\begin{pmatrix} bx_1 \\ bx_2 \\ \vdots \\ bx_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}.$$

Thus

$$b \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix},$$

which implies

$$(bI_n - (a_{ij})) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}. \tag{2.1}$$

Since the vector $(x_1, \ldots, x_n)$ is not zero, (2.1) says the matrix $bI_n - (a_{ij}) \in \mathrm{M}_n(B)$ is not one-to-one on B^n. If B were an integral domain, then by looking at (2.1) over the fraction field of B would tell us the matrix $bI_n - (a_{ij})$ has determinant 0. Since that determinant is a monic polynomial expression in b with coefficients in A, the equation $\det(bI_n - (a_{ij})) = 0$ would show us b is integral over A.

When B is not an integral domain, so B has zero divisors, the determinant of a square matrix over B that is not injective (that is, it kills a nonzero vector) need not be 0. It turns out that nevertheless $\det(bI_n - (a_{ij}))$, which is a monic polynomial in b with coefficients in A does equal 0, but we will need a result from linear algebra over rings to explain this.

In linear algebra, there is a "universal" formula for inverting a square matrix M: $M^{-1} = \frac{1}{\det M}\mathrm{adj}(M)$, where $\mathrm{adj}(M)$, called the classical adjoint of M, has (i,j) entry equal to the determinant of the matrix M with row j and column i removed, multiplied by $(-1)^{i+j}$. (For example, $\mathrm{adj}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)$.) This universal inverse formula doesn't always make sense, since the scalar $\det M$ might not be invertible, but $\mathrm{adj}(M)$ always makes sense since its entries are just polynomials in the entries of M. Multiplying through the inverse matrix formula by $\det M$ and by M gives the algebraic identity

$$\mathrm{adj}(M)M = (\det M)I_n.$$

This formula is valid for all square matrices over all (commutative) rings. It says we can multiply each square matrix M by a particular second matrix to produce a diagonal matrix with the number $\det M$ on the diagonal.

Let $D(b) = \det(bI_n - (a_{ij}))$ and multiply both sides of (2.1) on the left by $\mathrm{adj}(bI_n - (a_{ij}))$ to get

$$D(b)I_n \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \Longrightarrow D(b) \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Comparing coordinates,

$$D(b)x_i = 0 \text{ for all } i.$$

Since $R = Ax_1 + \cdots + Ax_n$,

$$D(b)r = 0 \text{ for all } r \in R.$$

Using $r = 1$, we get $D(b) = 0$. Since $D(b)$ is a monic polynomial in b with coefficients in A, b is integral over A. □

Remark 2.9. The proof of $(iii) \Rightarrow (i)$ had a simpler ending when B is an integral domain (no need for classical adjoint matrices), and this is the only case we will be using later.

Corollary 2.10. *In a ring extension B/A, the elements of B that are integral over A form a subring containing A.*

Proof. Let R be the set of elements of B that are integral over A, so $A \subset R$. To show R is a subring of B, we need to show for b and b' in R that $b \pm b'$ and bb' are in R. Since b and b' are integral over R, the subrings $A[b]$ and $A[b']$ are finitely generated A-modules, say

$$A[b] = A + Ab + \cdots + Ab^{m-1}, \quad A[b'] = A + Ab' + \cdots + Ab'^{n-1},$$

where b is the root of a monic polynomial in $A[x]$ of degree m and b' is the root of a monic polynomial in $A[x]$ of degree n. Then the subring $A[b, b']$ is finitely generated as an A-module:

$$A[b, b'] = \sum_{i,j \geq 0} Ab^i b'^j = \sum_{\substack{i \leq m-1 \\ j \leq n-1}} Ab^i b'^j.$$

Since this subring of B contains $b \pm b'$ and bb', and $A[b, b']$ is a finitely generated A-module, $b \pm b'$ and bb' are integral over A by $(iii) \Rightarrow (i)$ in Theorem 2.8. □

Our next and final result on integral ring extensions is about finitely generated algebras, rather than finitely generated modules. Let's recall the difference in the two meanings of "finitely generated" for A-modules and associative A-algebras.

- A finitely generated A-module is $A\alpha_1 + \cdots + A\alpha_n$: all elements of the module come from finitely many elements $\alpha_1, \ldots, \alpha_n$ by using their A-linear combinations.
- A finitely generated associative A-algebra has the form $A[\alpha_1, \ldots, \alpha_n]$: all elements of the A-algebra come from finitely many elements $\alpha_1, \ldots, \alpha_n$ by using their polynomial expressions with A-coefficients.

Finite generatedness of an A-module is about *linear combinations* of finitely many elements with coefficients in A, while finite generatedness for an associative A-algebra is about *polynomials* in finitely many elements with coefficients in A. For example, $\mathbf{Z}[x]$ is a finitely generated $\mathbf{Z}$-algebra but is not a finitely generated $\mathbf{Z}$-module since linear combinations of finitely many polynomials don't give us polynomials of arbitrarily large degree.

Theorem 2.11 (Zariski)**.** *Let L/K be a field extension such that L is a finitely generated K-algebra. Then L is finite-dimensional over K. In particular, L/K is an algebraic extension.*

Proof. We present an argument of Azarang [1]. We will induct on the number of generators of the top field as an algebra over the bottom field. Write $L = K[\alpha_1, \ldots, \alpha_n]$. We will show that if L is a finitely generated K-algebra then each α_i is algebraic over K, as that implies $\dim_K(L)$ is finite (only finitely many powers of each α_i are needed) and that in turn implies each element of L is algebraic over K.

Base case $n = 1$. If $n = 1$ then $L = K[\alpha]$ for some α. If α is not algebraic over K then $K[\alpha] \cong K[t]$ (polynomial ring over K in one indeterminate t transcendental over K) and this is not a field. Therefore if $K[\alpha]$ is a field then α *must* be algebraic over K. This theorem we are proving is a generalization of the observation about α being algebraic over K is equivalent to $K[\alpha]$ being finite-dimensional over K.

The case $n = 2$. We will derive the case $n = 2$ from $n = 1$ since all the key ideas for the general inductive step are used when $n = 2$ but the notation is a little simpler.

Suppose the theorem is proved for $n = 1$ with arbitrary base fields. If $L = K[\alpha, \beta]$ is a field, we want to show α and β are algebraic over K. We will prove this by contradiction: assume α or β is not algebraic over K, say β is transcendental over K. Rewrite β as t so it looks transcendental over K. Then

$$L := K[t][\alpha] \subset K(t)[\alpha] \subset L$$

since L is a field. Thus

$$L = K(t)[\alpha],$$

which shows L is a field generated as a $K(t)$-algebra by 1 element. By the base case, α is algebraic over the field $K(t)$: $f(\alpha) = 0$ for some monic $f(x) \in K(t)[x]$.

The coefficients of $f(x)$ are ratios of elements of $K[t]$. Let $d(t) \in K[t]$ be a common denominator of the coefficients of $f(x)$, so $f(x)$ is monic in $K[t, 1/d(t)][x]$. Thus the condition $f(\alpha) = 0$ tells us α is *integral* over the ring

$$R := K\left[t, \frac{1}{d(t)}\right].$$

Since $L = K[t][\alpha]$, L is a field, and $K[t] \subset R \subset L$, $L = R[\alpha]$. That α is integral over R implies L is an integral ring extension of R (Corollary 2.10). Then L being a field implies R is a field (Theorem 2.7). From $K[t] \subset R \subset K(t)$, we conclude $R = K(t)$.

We will show $R \neq K(t)$. All elements of R have denominators that are powers of $d(t)$, and $d(t)$ has finitely many *monic irreducible* factors in $K[t]$. Since $K[t]$ has *infinitely many* monic irreducibles (mimic Euclid's proof of the infinitude of primes in $\mathbf{Z}^+$), some monic irreducible $p(t)$ in $K[t]$ is not a factor of $d(t)$. Then $\boxed{1/p(t) \in K(t)}$ but unique factorization in $K[t]$ implies $\boxed{1/p(t) \notin R}$ (if $1/p(t) \in R$ then $p(t)$ divides $d(t)$). This contradiction implies α and β are algebraic over K, so $L = K[\alpha, \beta]$ is finite-dimensional over K.

General inductive step. Suppose $L = K[\alpha_1, \ldots, \alpha_n]$ where $n \geq 2$ and the theorem is proved for all field extensions where the top field is finitely generated as an algebra over the bottom field and the number of algebra generators is $n-1$. To prove each α_i is algebraic over K, we argue by contradiction: assume some α_i is not algebraic over K, and without loss of generality let it be α_n. Rewrrite α_n as t. Then

$$L = K[t][\alpha_1, \ldots, \alpha_{n-1}] \subset K(t)[\alpha_1, \ldots, \alpha_{n-1}] \subset L,$$

so

$$L = K(t)[\alpha_1, \ldots, \alpha_{n-1}].$$

Therefore L is a field generated as a $K(t)$-algebra by $n-1$ elements, so $\alpha_1, \ldots, \alpha_{n-1}$ are all algebraic over $K(t)$ by induction: $f_j(\alpha_j) = 0$ for monic $f_j(x) \in K(t)[x]$.

Since the coefficients of $f_j(x)$ are ratios of elements of $K[t]$, write $d(t)$ for a common denominator of the coefficients of $f_1(x), \ldots, f_{n-1}(x)$. That makes each $f_j(x)$ monic in $K[t, 1/d(t)][x]$, so $\alpha_1, \ldots, \alpha_{n-1}$ are all *integral* over the ring

$$R := K\left[t, \frac{1}{d(t)}\right].$$

Since $L = K[t][\alpha_1, \ldots, \alpha_{n-1}]$, L is a field, and $K[t] \subset R \subset L$, $L = R[\alpha_1, \ldots, \alpha_{n-1}]$. From $\alpha_1, \ldots, \alpha_{n-1}$ all being integral over R, L is an integral extension of R (Corollary 2.10), so L being a field implies R is a field (Theorem 2.7). Thus $K[t] \subset R \subset K(t)$ implies $R = K(t)$, so $K[t, 1/d(t)] = K(t)$. This is a contradiction (see $n = 2$), so $\alpha_1, \ldots, \alpha_n$ are algebraic over K and $L = K[\alpha_1, \ldots, \alpha_n]$ is finite-dimensional over K. □

Theorem 2.11 is called Zariski's lemma and was proved by Zariski in 1947 [10]. Its significance is that it shows for field extensions L/K, the linear and ring-theoretic notions of finiteness are equivalent: L is a finitely generated K-algebra if and only if L is a finite-dimensional K-vector space. It is easy to see that if $\dim_K(L)$ is finite then L is a finitely generated K-algebra (if $L = \sum_{i=1}^n K\alpha_i$ then $L = K[\alpha_1, \ldots, \alpha_n]$ since L is a ring). The less clear converse direction is Zariski's lemma. Our proof of Zariski's lemma is similar to the one in Fulton's book [2, Sect. 1.10] except for the way integrality properties are applied.

Corollary 2.12. *For every maximal ideal $\mathfrak{m}$ in $K[x_1, \ldots, x_n]$, where K is a field, the field $K[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite extension K.*

Proof. In $L := K[x_1, \ldots, x_n]/\mathfrak{m}$, set $\overline{x}_i = x_i \bmod \mathfrak{m}$. Then $L = K[\overline{x}_1, \ldots, \overline{x}_n]$, so L is a field (since $\mathfrak{m}$ is a maximal ideal) and is finitely generated as a K-algebra. By Theorem 2.11, $[L : K]$ is finite. □

3. Maximal ideals in polynomial rings over a field

Armed with Zariski's lemma, or more precisely the corollary to it, we are ready to describe the maximal ideals in $K[x_1, \ldots, x_n]$ for a field K. We will first treat the case when K is an algebraically closed field, where the description is especially simple.

Theorem 3.1. *Let K be a field.*

1. *For $c_1, \ldots, c_n \in K$, the ideal $(x_1 - c_1, \ldots, x_n - c_n)$ in $K[x_1, \ldots, x_n]$ is maximal.*
2. *If K is an algebraically closed field then each maximal ideal of $K[x_1, \ldots, x_n]$ has the form $(x_1 - c_1, \ldots, x_n - c_n)$ for unique $c_1, \ldots, c_n \in K$.*

In particular, for algebraically closed K the maximal ideals in $K[x_1, \ldots, x_n]$ are the polynomials in $K[x_1, \ldots, x_n]$ vanishing at some point in K^n and this sets up a bijection between maximal ideals in $K[x_1, \ldots, x_n]$ and points in K^n.

Proof. (1) Let $I = (x_1 - c_1, \ldots, x_n - c_n)$. Since $x_i \equiv c_i \bmod I$,

$$f(x_1, \ldots, x_n) \equiv f(c_1, \ldots, c_n) \bmod I$$

for all f in $K[x_1, \ldots, x_n]$. Thus $f(c_1, \ldots, c_n) = 0$ if and only if $f(x_1, \ldots, x_n) \in I$, so the evaluation homomorphism $K[x_1, \ldots, x_n] \to K$ where $f(x_1, \ldots, x_n) \mapsto f(c_1, \ldots, c_n)$ has kernel I. This homomorphism is surjective (elements of K map to themselves), so $K[x_1, \ldots, x_n]/I \cong K$. The right side K is a field, so I is maximal in $K[x_1, \ldots, x_n]$.

(2). Let $\mathfrak{m}$ be a maximal ideal of $K[x_1, \ldots, x_n]$ when K is algebraically closed. The field $K[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite extension of K by Corollary 2.12. Since K is algebraically closed, its only finite extension is itself. Therefore $K[x_1, \ldots, x_n]/\mathfrak{m}$ has degree 1 over K, so each coset mod $\mathfrak{m}$ is represented by an element of K. Thus $x_i \equiv c_i \bmod \mathfrak{m}$ for some $c_i \in K$. Then $x_i - c_i \in \mathfrak{m}$, so $(x_1 - c_1, \ldots, x_n - c_n) \subset \mathfrak{m}$. That containment must be equality since the ideal $(x_1 - c_1, \ldots, x_n - c_n)$ is maximal by (a).

If the ideals $(x_1 - c_1, \ldots, x_n - c_n)$ and $(x_1 - c_1', \ldots, x_n - c_n')$ in $K[x_1, \ldots, x_n]$ are equal then $c_i - c_i'$ is contained in the ideal since it equals $(c_i - x_i) - (c_i' - x_i)$. A proper ideal in $K[x_1, \ldots, x_n]$ can't contain an element of $K^\times$, so $c_i - c_i' = 0$ for all i. Thus $c_i = c_i'$. □

Example 3.2. Every maximal ideal in $\mathbf{C}[x_1, \ldots, x_n]$ has the form $(x_1 - c_1, \ldots, x_n - c_n)$ for unique $c_1, \ldots, c_n \in \mathbf{C}$. That $\mathbf{C}$ is algebraically closed is equivalent to saying all maximal ideals of $\mathbf{C}[x]$ have the form $(x - c)$ for $c \in \mathbf{C}$. Therefore the description of maximal ideals in $\mathbf{C}[x_1, \ldots, x_n]$ for all n could be considered a generalization of the fundamental theorem of algebra to multivariable polynomial rings over $\mathbf{C}$.[3]

Remark 3.3. The bijection between points in $\mathbf{C}^n$ and maximal ideals in $\mathbf{C}[x_1, \ldots, x_n]$ is an important intuition in mathematics: in a commutative ring, think about its maximal ideals as the points in a space. Besides $\mathbf{C}[x_1, \ldots, x_n]$, two more rings where this intuition holds are $C(X, \mathbf{R})$ and $C(X, \mathbf{C})$ – the continuous real-valued and complex-valued functions on a compact Hausdorff space X. The maximal ideals in each ring come from points of X: $\mathfrak{m}_x = \{f : f(x) = 0\}$. Moreover, X up to homeomorphism is determined by $C(X, \mathbf{R})$ and $C(X, \mathbf{C})$ up to isomorphism (as a ring and as a C^*-algebra, respectively). This is called the Gelfand–Kolmogorov theorem for $C(X, \mathbf{R})$ and the Gelfand–Naimark theorem for $C(X, \mathbf{C})$.

When K is not algebraically closed, maximal ideals in $K[x_1, \ldots, x_n]$ need not have the form $(x_1 - c_1, \ldots, x_n - c_n)$ for some $c_i \in K$. For example, if $p(x)$ is irreducible in $K[x]$ with $\deg p > 1$ (there are always such irreducibles when K is not algebraically closed), the ideal $(p(x))$ in $K[x]$ is maximal and not of the form $(x - c)$ where $c \in K$. But there is a connection between $(p(x))$ in $K[x]$ and the maximal ideal $(x - c)$ in $\overline{K}[x]$ where c is a root of $p(x)$: $(p(x)) = (x - c) \cap K[x]$, where $(x - c)$ is an ideal in $\overline{K}[x]$. Consider the maximal ideal $(x^2 + 1)$ in $\mathbf{R}[x]$: $x^2 + 1$ has roots $\pm i$ and $(x^2 + 1) = (x - i) \cap \mathbf{R}[x] = (x + i) \cap \mathbf{R}[x]$, where $(x \pm i)$ are ideals in $\mathbf{C}[x]$. Indeed, a polynomial in $\mathbf{R}[x]$ has root i or $-i$ if and only if it is divisible by $x^2 + 1$ in $\mathbf{R}[x]$ (the minimal polynomial of $\pm i$ over $\mathbf{R}$). This idea carries over to maximal ideals in a polynomial ring over an arbitrary field K and its algebraic closure $\overline{K}$.

Theorem 3.4. *Let K be a field and $\overline{K}$ be an algebraic closure of K.*

(1) *For each $\mathbf{c} = (c_1, \ldots, c_n)$ in $\overline{K}^n$, set $\mathfrak{m}_\mathbf{c} = (x_1 - c_1, \ldots, x_n - c_n)$ in $\overline{K}[x_1, \ldots, x_n]$. The intersection*

$$\mathfrak{m}_\mathbf{c} \cap K[x_1, \ldots, x_n] = \{f \in K[x_1, \ldots, x_n] : f(\mathbf{c}) = 0\}$$

is a maximal ideal of $K[x_1, \ldots, x_n]$.

(2) *Every maximal ideal in $K[x_1, \ldots, x_n]$ arises in the above way.*

[3] A simpler generalization of the fundamental theorem of algebra to $\mathbf{C}[x_1, \ldots, x_n]$ is that every nonconstant polynomial equation $f(x_1, \ldots, x_n) = 0$ in $\mathbf{C}[x_1, \ldots, x_n]$ has a complex zero.

Proof. (1) Evaluation at $\mathbf{c}$ is a homomorphism $K[x_1, \ldots, x_n] \to \overline{K}$ with image $K[c_1, \ldots, c_n]$, which is $K(c_1, \ldots, c_n)$ since all c_i are algebraic over K. The kernel is $\mathfrak{m}_{\mathbf{c}} \cap K[x_1, \ldots, x_n]$, so

$$K[x_1, \ldots, x_n]/(\mathfrak{m}_{\mathbf{c}} \cap K[x_1, \ldots, x_n]) \cong K(c_1, \ldots, c_n). \tag{3.1}$$

The right side is a field, so $\mathfrak{m}_{\mathbf{c}} \cap K[x_1, \ldots, x_n]$ is a maximal ideal in $K[x_1, \ldots, x_n]$.

(2) Let $\mathfrak{m}$ be a maximal ideal in $K[x_1, \ldots, x_n]$. Then $K[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite extension of K (Corollary 2.12), so it is K-isomorphic to a subfield of $\overline{K}$: there is an embedding $\varphi\colon K[x_1, \ldots, x_n]/\mathfrak{m} \to \overline{K}$ fixing all of K. Set $c_i = \varphi(x_i \bmod \mathfrak{m})$. The composition

$$K[x_1, \ldots, x_n] \to K[x_1, \ldots, x_n]/\mathfrak{m} \xrightarrow{\varphi} \overline{K},$$

where the first map is reduction mod $\mathfrak{m}$, is a ring homomorphism that is the identity on K and sends each x_i to c_i, so the composite homomorphism $K[x_1, \ldots, x_n] \to \overline{K}$ is evaluation at $(c_1, \ldots, c_n)$. Therefore the composite map has kernel $\mathfrak{m}_{\mathbf{c}} \cap K[x_1, \ldots, x_n]$. Also the composite map has kernel $\mathfrak{m}$ since φ is injective, so $\mathfrak{m} = \mathfrak{m}_{\mathbf{c}} \cap K[x_1, \ldots, x_n]$. □

That maximal ideals in $K[x_1, \ldots, x_n]$ are $\{f \in K[x_1, \ldots, x_n] : f(\mathbf{c}) = 0\}$ for some $\mathbf{c} \in \overline{K}^n$ gives two concrete descriptions of maximal ideals in $K[x_1, \ldots, x_n]$ for arbitrary K:

- the set of all polynomials in $K[x_1, \ldots, x_n]$ vanishing at some point $\mathbf{c}$ in $\overline{K}^n$,
- kernels of K-algebra homomorphisms from $K[x_1, \ldots, x_n]$ to finite extensions of K.

These generalize the description of maximal ideals of $K[x_1, \ldots, x_n]$ when K is algebraically closed, in which case $\overline{K} = K$ and the only finite extension of K is K. By (3.1), for a maximal ideal $\mathfrak{m}$ in $K[x_1, \ldots, x_n]$ the residue field $K[x_1, \ldots, x_n]/\mathfrak{m}$ has degree 1 over K if and only if $\mathfrak{m} = \mathfrak{m}_{\mathbf{c}}$ when $\mathbf{c} \in K^n$, which means $\mathfrak{m} = (x_1 - c_1, \ldots, x_n - c_n)$ with $c_i \in K$. Other maximal ideals have a residue field with K-degree bigger than 1.

When K is not algebraically closed, different maximal ideals in $\overline{K}[x_1, \ldots, x_n]$ could lead to the same maximal ideal in $K[x_1, \ldots, x_n]$: for different $\mathbf{a}$ and $\mathbf{b}$ in $\overline{K}^n$, $\mathfrak{m}_{\mathbf{a}}$ and $\mathfrak{m}_{\mathbf{b}}$ could intersect $K[x_1, \ldots, x_n]$ in the same way. For example, when passing from $\mathbf{C}[x]$ to $\mathbf{R}[x]$, $(x - i) \cap \mathbf{R}[x] = (x^2 + 1) = (x + i) \cap \mathbf{R}[x]$. (This is saying elements of $\mathbf{R}[x]$ that vanish at i and at $-i$ are the same, even though $i \neq -i$.) We can relate i and $-i$ by $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$: they are in the same Galois orbit. It turns out the same kind of relation occurs between $\mathbf{a}$ and $\mathbf{b}$ whenever $\mathfrak{m}_{\mathbf{a}}$ and $\mathfrak{m}_{\mathbf{b}}$ intersect $K[x_1, \ldots, x_n]$ in the same way. The group $\mathrm{Aut}(\overline{K}/K)$ will replace $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$, and we don't write $\mathrm{Gal}(\overline{K}/K)$ since K might have inseparable extensions.

Theorem 3.5. *For* $\mathbf{a}$ *and* $\mathbf{b}$ *in* $\overline{K}^n$,

$$\mathfrak{m}_{\mathbf{a}} \cap K[x_1, \ldots, x_n] = \mathfrak{m}_{\mathbf{b}} \cap K[x_1, \ldots, x_n] \Longleftrightarrow \mathbf{b} = \sigma(\mathbf{a})$$

for some $\sigma \in \mathrm{Aut}(\overline{K}/K)$, *where* $\sigma(a_1, \ldots, a_n) := (\sigma(a_1), \ldots, \sigma(a_n))$.

Proof. ($\Leftarrow$) If $\mathbf{b} = \sigma(\mathbf{a})$ for some $\sigma \in \mathrm{Aut}(\overline{K}/K)$ then

$$f \in \mathfrak{m}_{\mathbf{a}} \cap K[x_1, \ldots, x_n] \Longrightarrow f(\mathbf{a}) = 0 \Longrightarrow \sigma(f(\mathbf{a})) = \sigma(0) = 0.$$

Since f has coefficients in K, $\sigma(f(\mathbf{a})) = f(\sigma(\mathbf{a})) = f(\mathbf{b})$, so $f(\mathbf{b}) = 0$. Thus

$$\mathfrak{m}_{\mathbf{a}} \cap K[x_1, \ldots, x_n] \subset \mathfrak{m}_{\mathbf{b}} \cap K[x_1, \ldots, x_n].$$

Since $\mathbf{a} = \sigma^{-1}(\mathbf{b})$, the reverse containment also holds.

($\Rightarrow$) Let $\mathfrak{m}$ denote the common maximal ideal $\mathfrak{m}_{\mathbf{a}} \cap K[x_1, \ldots, x_n]$ and $\mathfrak{m}_{\mathbf{b}} \cap K[x_1, \ldots, x_n]$. From the end of the proof of Theorem 3.4, evaluation at $\mathbf{a}$ and at $\mathbf{b}$ give us two embeddings of $K[x_1, \ldots, x_n]/\mathfrak{m}$ into $\overline{K}$ that fix K pointwise. The images of these embeddings are $K(a_1, \ldots, a_n)$ and $K(b_1, \ldots, b_n)$, mapping $x_i \bmod \mathfrak{m}$ to a_i and to b_i for all i. Since $K[x_1, \ldots, x_n]/\mathfrak{m}$ is K-isomorphic to $K(a_1, \ldots, a_n)$ and $K(b_1, \ldots, b_n)$, composing one of these isomorphisms with the inverse of the other is a K-isomorphism $\sigma\colon K(a_1, \ldots, a_n) \to$

$K(b_1, \ldots, b_n)$, where $\sigma(a_i) = b_i$ for all i. Both $K(a_1, \ldots, a_n)$ and $K(b_1, \ldots, b_n)$ have algebraic closure $\overline{K}$, so by Zorn's lemma σ extends (in many ways) to an automorphism of $\overline{K}$. Denoting one of these extensions still by σ, we have $\sigma \in \mathrm{Aut}(\overline{K}/K)$ and $\sigma(\mathbf{a}) = \mathbf{b}$. □

Theorem 3.4 says each maximal ideal in $K[x_1, \ldots, x_n]$ comes from a point in $\overline{K}^n$, and Theorem 3.5 says different points in $\overline{K}^n$ lead to the same maximal ideal in $K[x_1, \ldots, x_n]$ exactly when they are in the same orbit of $\mathrm{Aut}(\overline{K}/K)$. So the maximal ideals of $K[x_1, \ldots, x_n]$ for an arbitrary field K are in bijection not with K^n, but with the orbits of the group $\mathrm{Aut}(\overline{K}/K)$ acting componentwise on $\overline{K}^n$. This illustrates how theorems about algebraically closed fields may generalize to all fields with the help of a group action by $\mathrm{Aut}(\overline{K}/K)$.

Starting from Zariski's lemma, we found properties of maximal ideals in $K[x_1, \ldots, x_n]$ for all fields K. The reasoning can be brought back to the start for a cycle of equivalences.

Theorem 3.6. *The following properties of fields are equivalent.*

(1) *Zariski's lemma: for every field K, a finitely generated K-algebra that is a field is finite-dimensional over K. (Theorem 2.11)*
(2) *For every field K and maximal ideal $\mathfrak{m}$ in $K[x_1, \ldots, x_n]$, $K[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite-dimensional over K (Corollary 2.12).*
(3) *For every field K, each maximal ideal of $K[x_1, \ldots, x_n]$ is the set of all polynomials vanishing at some point in $\overline{K}^n$ (Theorem 3.4).*
(4) *For every field K, each maximal ideal of $K[x_1, \ldots, x_n]$ is the kernel of a surjective K-algebra homomorphism $K[x_1, \ldots, x_n] \to L$ where L is a field such that $[L : K] < \infty$.*

Proof. (1) ⇒ (2): see the proof of Corollary 2.12.

(2) ⇒ (3): see the proof of Theorem 3.4.

(3) ⇒ (4): let $\mathfrak{m}$ be a maximal ideal in $K[x_1, \ldots, x_n]$. By (3), there is a point $(c_1, \ldots, c_n) \in \overline{K}^n$ such that $\mathfrak{m}$ is the kernel of the evaluation map $\varphi\colon K[x_1, \ldots, x_n] \to \overline{K}$ at $(c_1, \ldots, c_n)$. Set $\alpha_i = \varphi(x_i)$ in $\overline{K}$. The image of φ in $\overline{K}$ is $L := K[\alpha_1, \ldots, \alpha_n]$, which is a finite extension of K since each α_i is algebraic over K. Therefore $\mathfrak{m}$ is the kernel of the surjective K-algebra homomorphism $K[x_1, \ldots, x_n] \to L$ and $[L : K] < \infty$.

(4) ⇒ (1): Let F be a finitely generated K-algebra that is a field and $\alpha_1, \ldots, \alpha_n$ be a finite set of K-algebra generators of F, so $F = K[\alpha_1, \ldots, \alpha_n]$. Evaluation of polynomials in $K[x_1, \ldots, x_n]$ at $(\alpha_1, \ldots, \alpha_n)$ in F^n is a K-algebra homomorphism $\varphi\colon K[x_1, \ldots, x_n] \to F$ that is surjective since the image of φ contains K and each α_i. Since the image of φ is a field, $\mathfrak{m} := \ker \varphi$ is a maximal ideal, so by (4) there is a surjective K-algebra homomorphism $\psi\colon K[x_1, \ldots, x_n] \to L$ with kernel $\mathfrak{m}$ where L is a finite extension field of K, so

$$L = \psi(K[x_1, \ldots, x_n]) \cong K[x_1, \ldots, x_n]/\mathfrak{m} \cong F$$

as K-algebras. Thus $\dim_K(F) = \dim_K(L) < \infty$. □

4. The Nullstellensatz

Let K be an algebraically closed field. Polynomials in $K[x_1, \ldots, x_n]$ define functions $K^n \to K$ by substitution of coordinates of a point in K^n for $x_1, \ldots, x_n$. We link algebra (polynomials) and geometry (subsets of K^n) by associating to each subset X of K^n the polynomials vanishing on all of X, and to each subset S of $K[x_1, \ldots, x_n]$ its zero set in K^n.

$$I(X) := \{f \in K[x_1, \ldots, x_n] : f(\mathbf{a}) = 0 \text{ for all } \mathbf{a} \in X\},$$
$$Z(S) := \{\mathbf{a} \in K^n : f(\mathbf{a}) = 0 \text{ for all } f \in S\}.$$

Example 4.1. For each point $\mathbf{c} = (c_1, \ldots, c_n)$ in K^n,

$$I(\mathbf{c}) = (x_1 - c_1, \ldots, x_n - c_n) \tag{4.1}$$

by the proof of Theorem 3.1(1) and

$$Z(x_1 - c_1, \ldots, x_n - c_n) = \{\mathbf{c}\} \tag{4.2}$$

since the polynomials $x_1 - c_1, \ldots, x_n - c_n$ all vanish at point $\mathbf{a} = (a_1, \ldots, a_n)$ if and only if $a_i = c_i$ for all i. Two more examples: $Z(0) = K^n$ and $Z(1) = \emptyset$.

It's easy to see for non-empty subsets X and Y in K^n that $\boxed{X \subset Y \Rightarrow I(Y) \subset I(X)}$. We define $I(\emptyset) = K[x_1, \ldots, x_n]$ so that the implication holds even with the empty set. For subsets S and T of $K[x_1, \ldots, x_n]$, $\boxed{S \subset T \Rightarrow Z(T) \subset Z(S)}$. Therefore the operations $X \rightsquigarrow I(X)$ and $S \rightsquigarrow Z(S)$ both reverse containments.

Note that $I(X)$ is always an *ideal* in $K[x_1, \ldots, x_n]$ (hence the notation): if f and g in $K[x_1, \ldots, x_n]$ vanish at all points of X then so do $f \pm g$ and hf for all $h \in K[x_1, \ldots, x_n]$. For a subset S of $K[x_1, \ldots, x_n]$, $Z(S) = Z(\langle S \rangle)$, where $\langle S \rangle$ is the ideal generated by S. Therefore in practice we will only look at zero sets of ideals in $K[x_1, \ldots, x_n]$. For example, $Z(f) = Z((f))$: an individual polynomial has the same zero set as the ideal it generates.

The most basic reason it is useful to work with ideals is that all ideals in $K[x_1, \ldots, x_n]$ are finitely generated. Therefore each zero set $Z(S)$ in K^n is always the zero set of finitely many polynomials: $Z(S) = Z(f_1, \ldots, f_r)$ when $\langle S \rangle = (f_1, \ldots, f_r)$.

Definition 4.2. A subset V of K^n is called a *variety* when it is the zero set in K^n of a set of polynomials in $K[x_1, \ldots, x_n]$: $V = Z(S)$ for some $S \subset K[x_1, \ldots, x_n]$.[4]

Example 4.3. In $K = K^1$, the varieties are finite or all of K since every ideal in $K[x]$ is principal and the zero set in K of a polynomial in $K[x]$ is finite or all of K (zero set of the polynomial 0). Conversely, each finite set $\{r_1, \ldots, r_d\}$ in K is $Z(f)$ where $f(x) = (x - r_1) \cdots (x - r_d)$.

We have a mapping from varieties in K^n to ideals in $K[x_1, \ldots, x_n]$ and conversely by $V \rightsquigarrow I(V)$ and $J \rightsquigarrow Z(J)$, and these are inclusion-reversing. If we apply these twice then we have easy containments

$$J \subset I(Z(J)), \quad V \subset Z(I(V)) \tag{4.3}$$

since polynomials in J vanish at the zero set of all polynomials in J and points in V are zeros of all the polynomials that vanish on V. Are the containments equalities? For the second containment, the answer is yes.

Theorem 4.4. *For varieties V in K^n, $Z(I(V)) = V$.*

Proof. We already saw $V \subset Z(I(V))$, so it remains to show $Z(I(V)) \subset V$.

Since V is a variety in K^n, $V = Z(J)$ for some ideal J of $K[x_1, \ldots, x_n]$. (Recall $Z(S) = Z(\langle S \rangle)$ for subsets S of $K[x_1, \ldots, x_n]$.) Then $J \subset I(V)$ by the first containment in (4.3). For each $\mathbf{a}$ in $Z(I(V))$, $f(\mathbf{a}) = 0$ for all $f \in I(V)$. From $J \subset I(V)$, we get $f(\mathbf{a}) = 0$ for all $f \in J$, so $\mathbf{a} \in Z(J)$, and thus $\mathbf{a} \in V$. □

We said at the start of the section that K is algebraically closed, but the notation and terminology we introduced all make sense for arbitrary fields. Theorem 4.4 holds for all fields K. In the following theorems, however, it is essential that K be algebraically closed.

Theorem 4.5. *When K is algebraically closed, a variety V in K^n is a point if and only if $I(V)$ is a maximal ideal in $K[x_1, \ldots, x_n]$.*

[4]The term "variety" means an algebraic analogue of a manifold. Most languages besides English and German use a cognate of the word "variety" for both varieties and manifolds. Context usually makes it clear what is meant, but terms such as "algebraic variety" or "analytic/differentiable variety" could be used to make a distinction.

Proof. If $V = \{\mathbf{c}\}$ is a point then $I(V) = (x_1 - c_1, \ldots, x_n - c_n)$ by (4.1).

If $I(V)$ is a maximal ideal then $I(V) = (x_1 - c_1, \ldots, x_n - c_n)$ for some $c_1, \ldots, c_n \in K$ by Theorem 3.1. Polynomials in $I(V)$ vanish on V by the definition of $I(V)$, so $V \subset Z(I(V))$. By (4.2), $Z(x_1 - c_1, \ldots, x_n - c_n) = \{\mathbf{c}\}$, so $V \subset \{\mathbf{c}\}$. Thus V is a point or $V = \emptyset$. If $V = \emptyset$ then $I(V) = I(\emptyset) = K[x_1, \ldots, x_n]$ by definition, which is not a maximal ideal. Therefore $V = \{\mathbf{c}\}$. □

Theorem 4.6 (Weak Nullstellensatz)**.** *Let K be algebraically closed. If J is a proper ideal in $K[x_1, \ldots, x_n]$ then $Z(J) \neq \emptyset$. That is, the polynomials in a proper ideal of $K[x_1, \ldots, x_n]$ all vanish at some common point in K^n.*

Proof. Since J is a proper ideal, by Zorn's lemma there is a maximal ideal $\mathfrak{m}$ in $K[x_1, \ldots, x_n]$ such that $J \subset \mathfrak{m}$. Then $Z(\mathfrak{m}) \subset Z(J)$, so we're reduced to showing $Z(\mathfrak{m}) \neq \emptyset$ for maximal ideals $\mathfrak{m}$. By Theorem 3.1, $\mathfrak{m} = (x_1 - c_1, \ldots, x_n - c_n)$, and $Z(\mathfrak{m}) = (c_1, \ldots, c_n)$ by (4.2). □

The weak Nullstellensatz tells us that over an algebraically closed field K, a system of polynomial equations $f_1 = 0, \ldots, f_r = 0$ in $K[x_1, \ldots, x_n]$ has a common solution in K^n if and only if the ideal $(f_1, \ldots, f_r)$ in $K[x_1, \ldots, x_n]$ is a proper ideal.

To illustrate the close relation between generating sets of ideals and solving systems of equations, we can reinterpret Gaussian elimination in linear algebra as a procedure to find a nice generating set for an ideal generated by linear polynomials in several variables. For example, the process of Gaussian elimination

$$\begin{array}{l} x + 2y = 5 \\ 3x - y = 4 \end{array} \rightsquigarrow \begin{array}{r} x + 2y = 5 \\ -7y = -11 \end{array} \rightsquigarrow \begin{array}{r} x + 2y = 5 \\ y = 11/7 \end{array} \rightsquigarrow \begin{array}{l} x = 13/7 \\ y = 11/7 \end{array}$$

corresponds to finding new generators for an ideal in $\mathbf{Q}[x, y]$:

$$(x+2y-5, 3x-y-4) = (x+2y-5, -7y+11) = (x+2y-5, y-11/7) = (x-13/7, y-11/7).$$

Some systems of polynomial equations over an algebraically closed field K have no solution in K. Linear algebra offers many examples. For a higher-degree example, if $f(x, y) = x^3 + 2x^2y + 3xy^2 + y^3 + c$, $g(x, y) = x^2 + 2xy$, and $h(x, y) = y^2 + 3xy$, then

$$f(x, y) - xg(x, y) - yh(x, y) = c,$$

so when $c \in K^\times$ there is no solution to $f = 0$, $g = 0$, and $h = 0$ in K^2 and no solution in L^2 for every field L containing K. The weak Nullstellensatz implies that checking for solvability of a system of polynomial equations with coefficients in K in a larger field L is the same as checking for a solution in K when K is algebraically closed.

Corollary 4.7. *Let K be an algebraically closed field. If a system of polynomial equations $f_1 = 0, \ldots, f_r = 0$ in $K[x_1, \ldots, x_n]$ has a solution in some field extension L/K then the system has a solution in K.*

Proof. In $K[x_1, \ldots, x_n]$, the ideal $(f_1, \ldots, f_r)$ can't be (1), since then $f_1g_1 + \cdots + f_rg_r = 1$ for some $g_i \in K[x_1, \ldots, x_n]$ and that prevents the system of equations $f_1 = 0, \ldots, f_r = 0$ from having a solution in a field L containing K. Since $(f_1, \ldots, f_r)$ is a proper ideal in $K[x_1, \ldots, x_n]$, the system of equations $f_1 = 0, \ldots, f_r = 0$ has a solution in K by the weak Nullstellensatz.

In more detail, the ideal $(f_1, \ldots, f_r)$ is in a maximal ideal $\mathfrak{m}$ and $\mathfrak{m} = (x_1 - c_1, \ldots, x_n - c_n)$ for some $c_i \in K$, so $(c_1, \ldots, c_n)$ is a common solution to the system of equations $f_1 = 0, \ldots, f_r = 0$. □

Example 4.8. Let $f_1, \ldots, f_r$ be polynomials in $\mathbf{Q}[x_1, \ldots, x_n]$. If the system of polynomial equations $f_1 = 0, \ldots, f_r = 0$ has a complex solution (in $\mathbf{C}^n$) then it has an algebraic solution (in $\overline{\mathbf{Q}}^n$). That comes from applying Corollary 4.7 to the algebraically closed field $K = \overline{\mathbf{Q}}$:

in brief, the ideal $(f_1, \ldots, f_r)$ in $\overline{\mathbf{Q}}[x_1, \ldots, x_n]$ can't be (1) since that would forbid a solution in $\mathbf{C}^n$. Thus $(f_1, \ldots, f_r)$ is in a maximal ideal of $\overline{\mathbf{Q}}[x_1, \ldots, x_n]$, which gives us a solution to the system of equations in $\overline{\mathbf{Q}}^n$ from the description of maximal ideals in $\overline{\mathbf{Q}}[x_1, \ldots, x_n]$.

We are not saying a complex solution to $f_1 = 0, \ldots, f_r = 0$ can somehow be converted into a solution in $\overline{\mathbf{Q}}$, but only that the existence of a complex solution forces the existence of an algebraic solution. Such a result may seem surprising, but if the f_j are all linear then it follows from linear algebra: a system of linear equations with $\mathbf{Q}$-coefficients that has a solution in a larger field has a $\mathbf{Q}$-solution. It is essential that we are looking at polynomial equations. The transcendental equation $\sin x - 1 = 0$ has rational coefficients and complex solutions $\{\pm\pi/2 + 2\pi k : k \in \mathbf{Z}\}$, but no algebraic solutions.

We will use the weak Nullstellensatz later in its contrapositive form: if $Z(J) = \emptyset$ then $1 \in J$. That is, for algebraically closed K, a system of equations $f_1 = 0, \ldots, f_r = 0$ in $K[x_1, \ldots, x_n]$ can fail to have a solution in K^n *only* because $f_1 g_1 + \cdots + f_r g_r = 1$ for some $g_i \in K[x_1, \ldots, x_n]$. That need not be a valid explanation when K is not algebraically closed. For example, $x^2 + y^2 + 1$ has no zeros in $\mathbf{R}^2$ but this is *not* because $(x^2 + y^2 + 1)g(x, y) = 1$ for some $g(x, y) \in \mathbf{R}[x, y]$.

Returning to the question about whether the containments in (4.3) are equalities, Theorem 4.4 says "yes" for the second containment, but the answer to the first containment is "no." An ideal J can be a proper subset of $I(Z(J))$. Here are two examples.

Example 4.9. In $K[x, y]$ let $J = (x^2, xy, y^2)$. Then $Z(J) = \{(0, 0)\}$, which is a point, so $I(Z(J)) = (x, y)$, which is strictly bigger than J. In terms of multiplication of ideals, $J = (x, y)^2$.

Example 4.10. In $K[x]$, let $J_k = (x^k)$ for a positive integer k. Then $Z(J_k) = \{0\}$ and $I(Z(J_k)) = (x)$, which is strictly bigger than J_k when $k \geq 2$.

While each subset X of K^n leads to an ideal $I(X)$, these ideals are not completely arbitrary. They have a special property: if $f \in K[x_1, \ldots, x_n]$ and $f^m \in I(X)$ then $f \in I(X)$. Indeed, if $f(\mathbf{a})^m = 0$ for all $\mathbf{a} \in X$ then $f(\mathbf{a}) = 0$ for all $\mathbf{a} \in X$, so $f \in I(X)$.

Definition 4.11. An ideal J in a ring A is called a *radical ideal* when the following property holds for all $a \in A$: if $a^m \in J$ for some $m \geq 1$ then $a \in J$.

Example 4.12. We saw above that for every subset X of K^n, $I(X)$ is a radical ideal.

Example 4.13. In the ring $\mathbf{Z}$, where every ideal is principal, a nonzero ideal $n\mathbf{Z}$ is a radical ideal if and only if n is squarefree (not divisible by the square of a prime number).

Example 4.14. Prime ideals are radical ideals: $a^m \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ by the definition of an ideal $\mathfrak{p}$ being prime. Since maximal ideals are prime ideals, maximal ideals are radical ideals. It's easy to see that an intersection of radical ideals is a radical ideal, so an intersection of prime ideals is a radical ideal even though an intersection of prime ideals is usually not a prime ideal, *e.g.*, in $\mathbf{Z}$, $3\mathbf{Z} \cap 5\mathbf{Z} = 15\mathbf{Z}$ is a radical ideal but not a prime ideal.

An ideal that is not a radical ideal has a canonical radical ideal associated to it.

Definition 4.15. For an ideal J in the ring A, the *radical of* J is

$$\operatorname{Rad} J = \{a \in A : a^m \in J \text{ for some } m \geq 1\}.$$

It is not hard to show $\operatorname{Rad} J$ is an ideal (it is additively closed by the binomial theorem). Clearly J is a radical ideal if and only if $\operatorname{Rad} J = J$. Another notation for $\operatorname{Rad} J$ is $\sqrt{J}$.

Theorem 4.16. *For an ideal J, $\operatorname{Rad} J$ is the smallest radical ideal containing J.*

Proof. It's easy to see that $J \subset \operatorname{Rad} J$. If J' is a radical ideal that contains J and $a \in \operatorname{Rad} J$, so $a^m \in J$ for some $m \geq 1$, then $a^m \in J'$, so $a \in J'$ since J' is a radical ideal. Since this holds for all $a \in \operatorname{Rad} J$, we get $\operatorname{Rad} J \subset J'$. □

Let's return to the containment $J \subset I(Z(J))$ in (4.3). It is not necessarily an equality (Examples 4.9 and 4.10) and we can refine it in two ways using radicals of ideals.

- Since $I(Z(J))$ is a radical ideal containing J, Theorem 4.16 tells us $\operatorname{Rad} J \subset I(Z(J))$. Perhaps $I(Z(J)) = \operatorname{Rad} J$ for each ideal J?
- Since a polynomial $f \in K[x_1, \ldots, x_n]$ and its powers vanish at the same points in K^n, $Z(J) = Z(\operatorname{Rad} J)$, so each zero set of an ideal can be described as the zero set of a radical ideal. Perhaps $I(Z(J)) = J$ when J is a radical ideal?

The answer to both questions turns out to be yes, and this is Hilbert's Nullstellensatz [4, p. 320]. This German term is two words: "Nullstellen + Satz" or "Zeros + theorem", so "Theorem about zeros". It is the starting point of classical algebraic geometry.

Theorem 4.17 (Nullstellensatz)**.** *When K is algebraically closed. $I(Z(J)) = \operatorname{Rad} J$ for each ideal J in $K[x_1, \ldots, x_n]$. Equivalently, $I(Z(J)) = J$ for radical ideals J.*

Writing $J = (f_1, \ldots, f_r)$, the harder containment $I(Z(J)) \subset \operatorname{Rad} J$ is saying that if a polynomial $g \in K[x_1, \ldots, x_n]$ vanishes on K^n wherever the polynomials $f_1, \ldots, f_r$ all vanish, then $g^m \in (f_1, \ldots, f_r)$ for some $m \geq 1$.

Proof. Since $Z(J) = Z(\operatorname{Rad} J)$, the formulas $I(Z(J)) = \operatorname{Rad} J$ for all ideals J or $I(Z(J)) = J$ for radical ideals J are equivalent. We will prove $I(Z(J)) = \operatorname{Rad} J$ for all J.

Before the theorem we saw that $\operatorname{Rad} J \subset I(Z(J))$. To prove $I(Z(J)) \subset \operatorname{Rad} J$, write $J = (f_1, \ldots, f_r)$ since ideals in $K[x_1, \ldots, x_n]$ are finitely generated. Pick $g \in I(Z(J))$ with $g \neq 0$. Pass to an ideal in $K[x_1, \ldots, x_n, x_{n+1}]$: set $J' = (f_1, \ldots, f_r, x_{n+1}g - 1)$ (the "Rabinowitsch[5] trick[6] "). Since g vanishes on K^n wherever all the f_i vanish, g vanishes on K^{n+1} wherever all f_i vanish (the new last coordinate in K^{n+1} doesn't affect their values). So $x_{n+1}g - 1$ doesn't vanish anywhere that all f_i vanish (its value at such a point is -1). That means $Z(J') = \emptyset$, so the weak Nullstellensatz says $J' = K[x_1, \ldots, x_{n+1}]$. Thus $1 \in J'$:

$$1 = \sum_{j=1}^{r} h_j(x_1, \ldots, x_n, x_{n+1}) f_j(x_1, \ldots, x_n) + h(x_1, \ldots, x_n, x_{n+1})(x_{n+1}g - 1)$$

for some $h_1, \ldots, h_r, h$ in $K[x_1, \ldots, x_{n+1}]$. In this polynomial identity, set $x_{n+1} = 1/g$ (we can do that since $g \neq 0$) to get an equation in $K[x_1, \ldots, x_n, 1/g]$ that kills off the last term on the right:

$$1 = \sum_{j=1}^{r} h_j(x_1, \ldots, x_n, 1/g) f_j(x_1, \ldots, x_n).$$

Multiply both sides by a power of g to clear the reciprocal powers of g from the right side. When the powers of $1/g$ are cleared out on the right, we get $g^m \in (f_1, \ldots, f_r) = J$ for some $m \geq 1$, so $g \in \operatorname{Rad} J$. □

Example 4.18. For algebraically closed K, let f be irreducible in $K[x_1, \ldots, x_n]$. A polynomial g in $K[x_1, \ldots, x_n]$ vanishes at all points in K^n where f vanishes if and only if f is a factor of g: the polynomials that vanish where f vanishes are the elements of $I(Z(f))$, and

[5]People say Rabinowitsch was George Rainich, but this is dubious: Rainich was a mathematical physicist. See the answer by Georges Elencwajg and comments below it at https://mathoverflow.net/questions/45185/pseudonyms-of-famous-mathematicians/45195.

[6]A conceptual explanation of this trick is at https://mathoverflow.net/questions/90661/the-rabinowitz-trick. Earlier proofs were much longer. Hilbert called his own proof "very cumbersome" [3, p. 10].

the Nullstellensatz says $I(Z(f)) = \mathrm{Rad}(f)$, which is (f) since f is irreducible. Therefore $g \in I(Z(f))$ is equivalent to $g \in (f)$, which means $f \mid g$.

Example 4.19. For algebraically closed K, let $J = (x^2, xy, z^2)$ in $K[x, y, z]$. Then $Z(J) = \{(0, b, 0) : b \in K\}$, so $I(Z(J)) = \{g \in K[x, y, z] : g(0, b, 0) = 0 \text{ for all } b \in K\}$. What is a generating set of polynomials for this ideal? It contains x and z, so $(x, z) \subset I(Z(J))$. We will show the reverse containment $I(Z(J)) \subset (x, z)$ in two ways, so $I(Z(J)) = (x, z)$.

Method 1. Write a polynomial $g(x, y, z)$ as a polynomial in x and z whose coefficients are polynomials in y (that is, $K[x, y, z] = K[y][x, z]$). Say $g = \sum_{i,j} c_{ij}(y)x^i z^j$ (a finite sum) where $c_{ij}(y) \in K[y]$. The only term not divisible by x or z is the "constant term" $c_{00}(y)$. For $b \in K$, $g(0, b, 0) = c_{00}(b)$. Therefore if $g(0, b, 0) = 0$ for all $b \in K$, $c_{00}(b) = 0$ for all b. That implies $c_{00}(y) = 0$ since K is infinite, so $g(x, y, z) \in (x, z)$.

Method 2. Since $Z(I(J)) = \mathrm{Rad}(J)$ (Nullstellensatz), we will show $\mathrm{Rad}(x^2, xy, z^2) \subset (x, z)$. If $g \in \mathrm{Rad}(x^2, xy, z^2)$ then $g^m \in (x^2, xy, z^2) \subset (x, z)$ for some $m \geq 1$. The ideal (x, z) in $K[x, y, z]$ is a prime ideal since $K[x, y, z]/(x, z) \cong K[y]$ is an integral domain, so from $g^m \in (x, z)$ we get $g \in (x, z)$.

The Nullstellensatz gives us a bijection between varieties in K^n and radical ideals in $K[x_1, \ldots, x_n]$ if K is algebraically closed. This is called the *variety–ideal correspondence*.

Theorem 4.20. *For algebraically closed fields K, the mappings $V \rightsquigarrow I(V)$ and $J \rightsquigarrow Z(J)$ between varieties in K^n and radical ideals in $K[x_1, \ldots, x_n]$ are inclusion-reversing bijections that are inverses: $Z(I(V)) = V$ for varieties V and $I(Z(J)) = J$ for radical ideals J.*

Proof. We have seen before that $I(V)$ is a radical ideal for each variety V, and $Z(J)$ is a variety in K^n by the definition of varieties. Since $Z(J) = Z(\mathrm{Rad}\, J)$, varieties have the form $Z(J)$ for radical ideals J. Therefore the mappings $V \rightsquigarrow I(V)$ and $J \rightsquigarrow Z(J)$ pass from varieties to radical ideals and conversely.

We saw before that these mappings are inclusion-reversing: $V \subset V' \Rightarrow I(V') \subset I(V)$ and $J \subset J' \Rightarrow Z(J') \subset Z(J)$. Theorem 4.4 tells us $Z(I(V)) = V$.

So far nothing we have mentioned requires K to be algebraically closed. The final step, that $I(Z(J)) = J$ for radical ideals J, is the Nullstellensatz and here we rely on K being algebraically closed. □

Remark 4.21. When K is not algebraically closed, the mappings $V \rightsquigarrow I(V)$ and $J \rightsquigarrow Z(J)$ between varieties in K^n and radical ideals in $K[x_1, \ldots, x_n]$ make sense, are inclusion-reversing, and $Z(I(V)) = V$ for all V by Theorem 4.4, but $J \neq I(Z(J))$ for some radical ideals J. For example, if $f(x) \in K[x]$ is irreducible with $\deg f > 1$ (such $f(x)$ exist since K is not algebraically closed) then $J := (f(x_1))$ in $K[x_1, \ldots, x_n]$ is prime since $f(x_1)$ is irreducible in $K[x_1, \ldots, x_n]$ and $Z(J) = \emptyset$ in K^n: if some $(c_1, \ldots, c_n) \in K^n$ is in $Z(J)$ then $f(c_1) = 0$, contradicting irreducibility of $f(x_1)$ since $\deg f > 1$. Thus $I(Z(J)) = I(\emptyset) = K[x_1, \ldots, x_n]$. The ideal J is radical since J is prime, and $J \neq (1)$ since $f(x_1)$ is nonconstant, so $J \neq I(Z(J))$.

The variety–ideal correspondence in Theorem 4.20 has a striking similarity to the Galois correspondence between intermediate fields M in a finite Galois extension E/F and subgroups H of $\mathrm{Gal}(E/F)$. Let's examine this similarity further.

- The condition $f(\mathbf{a}) = 0$ (all f as $\mathbf{a}$ runs over V, or all $\mathbf{a}$ as f runs over J) is analogous to the condition $\sigma(\alpha) = \alpha$ (all σ as α runs over M, or all α as σ runs over H).
- The mappings between varieties in K^n and radical ideals in $K[x_1, \ldots, x_n]$ can be defined without assuming K is algebraically closed, and the two mappings in the Galois correspondence can be defined without assuming E/F is a Galois extension (the group $\mathrm{Aut}(E/F)$ is finite when $[E : F]$ is finite).

- Iterating the Z and I mappings from Theorem 4.20 in the order $V \rightsquigarrow I(V) \rightsquigarrow Z(I(V))$ returns us to the starting point V without assuming K is algebraically closed (we have $Z(I(V)) = V$ by Theorem 4.4), and iterating the Galois correspondence in the order $H \rightsquigarrow E^H \rightsquigarrow \mathrm{Aut}(E/E^H)$ returns us to the starting point H without assuming E/F is Galois ($\mathrm{Aut}(E/E^H) = H$ by Artin's theorem about finite groups of automorphisms of a field).
- The iterations $J \rightsquigarrow Z(J) \rightsquigarrow I(Z(J))$ and $M \rightsquigarrow \mathrm{Aut}(E/M) \rightsquigarrow M^{\mathrm{Aut}(E/M)}$ lead to containments: $J \subset I(Z(J))$ and $M \subset M^{\mathrm{Aut}(E/M)}$. Turning these containments into equalities ($J = I(Z(J))$ and $M = M^{\mathrm{Aut}(E/M)}$ for all J and M) genuinely needs an extra assumption: to have $I(Z(J)) = J$ for all radical ideals J in $K[x_1, \ldots, x_n]$ requires K to be algebraically closed (there are always counterexamples when K is not algebraically closed – see Remark 4.21) and to have $M^{\mathrm{Aut}(E/M)} = M$ for all intermediate fields M in E/F requires E/F to be Galois (that $E^{\mathrm{Aut}(E/F)} = F$ is equivalent to E/F being Galois).

From those comparisons, we assemble analogies in Table 1.

Variety–Ideal Correspondence	Galois Correspondence
$K[x_1, \ldots, x_n]$ for alg. closed K	Galois extension E/F
Varieties V in K^n	Subgroups H of $\mathrm{Gal}(E/F)$
K^n (the biggest variety in K^n)	$\mathrm{Gal}(E/F)$ (the biggest subgroup)
Radical ideals J in $K[x_1, \ldots, x_n]$	Intermediate fields M in E/F
$V \rightsquigarrow I(V) = \{f : f(\mathbf{a}) = 0 \text{ for } \mathbf{a} \in V\}$	$H \rightsquigarrow E^H = \{\alpha : \sigma(\alpha) = \alpha \text{ for } \sigma \in H\}$
$J \rightsquigarrow Z(J) = \{\mathbf{a} : f(\mathbf{a}) = 0 \text{ for } f \in J\}$	$M \rightsquigarrow \mathrm{Gal}(E/M) = \{\sigma : \sigma(\alpha) = \alpha \text{ for } \alpha \in M\}$
$Z(I(V)) = V$ (Theorem 4.4)	$\mathrm{Gal}(E/E^H) = H$ (Artin's theorem)
$I(Z(J)) = J$	$M^{\mathrm{Gal}(E/M)} = M$

TABLE 1. Analogous correspondences

Remark 4.22. Two further examples in mathematics where inclusion-reversing bijections occur between two partially ordered sets are (1) covering spaces and subgroups of a fundamental group in topology and (2) subspaces of a vector space V and its dual space $V^\vee$ (associate to $W \subset V$ all $\varphi \in V^\vee$ such that $\varphi(w) = 0$ for all $w \in W$, and to each subspace U of $V^\vee$ all $w \in V$ such that $\varphi(w) = 0$ for all $\varphi \in U$).

We saw earlier that for an arbitrary subset S of $K[x_1, \ldots, x_n]$, $Z(S) = Z(J)$ where $J = \langle S \rangle$ is the ideal generated by S. We can go further and replace J with $\mathrm{Rad}(J)$ without changing the zero set in K^n, so $Z(S) = Z(\mathrm{Rad}(\langle S \rangle))$. This tells us how to write the zero set of an arbitrary subset S of $K[x_1, \ldots, x_n]$ as the zero set of a radical ideal: use the radical of the ideal generated by S.

Going the other way, if we start with an arbitrary subset X of K^n, then $J := I(X)$ is a radical ideal, so by the Nullstellensatz $J = I(V)$ for a unique variety V in K^n and $V = Z(J) = Z(I(X))$. Thus each subset X of K^n leads to a variety V where $X \subset V$ and the same polynomials in $K[x_1, \ldots, x_n]$ vanish on both X and V: $I(X) = J = I(V)$. How is V "generated" from X? It is the *smallest variety in K^n containing X*. Indeed, if W is a variety in K^n and $X \subset W$ then

$$X \subset W \Longrightarrow I(W) \subset I(X) = I(V) \Longrightarrow Z(I(V)) \subset Z(I(W)) \Longrightarrow V \subset W,$$

where the last step is the Nullstellensatz. We can express this relation between V and X using a topological language for subsets of K^n. The varieties in K^n satisfy the axioms of closed sets for a topology: both K^n and $\emptyset$ are varieties, and varieties in K^n are closed under finite unions and arbitrary intersections since $Z(J) \cup Z(J') = Z(JJ')$ and $\bigcap_\alpha Z(J_\alpha) =$

$Z(\sum_\alpha J_\alpha)$. For algebraically closed K, the topology on K^n whose closed sets are the varieties in K^n is called the *Zariski topology* on K^n. It was introduced by Zariski [9] in 1944. Open sets for the Zariski topology are the complements in K^n of varieties.[7] That V is the smallest variety in K^n containing X can now be described by saying V is the Zariski closure of X: $V = \overline{X}$ in the Zariski topology on K^n. That is how V is "generated" by X, analogous to $[0,1]$ being generated from $(0,1)$ in $\mathbf{R}$ by passing to the closure in the usual Euclidean topology on $\mathbf{R}$.

Example 4.23. A polynomial in $K[x]$ is a continuous function $K \to K$ using the Zariski topology since the inverse image of closed sets are closed: obviously $f^{-1}(K) = K$, and if $\{a_1, \ldots, a_m\}$ is a finite subset of K then its inverse image $f^{-1}(a_1) \cup \cdots \cup f^{-1}(a_m)$ in K is finite since each polynomial equation $f(x) = a_i$ has finitely many solutions in K. Let's compute a Zariski closure (closure of a subset in the Zariski topology). If X is an infinite subset of K then $\overline{X} = K$ in the Zariski topology since the varieties in K are $\emptyset$, K, and finite subsets[8]: the only variety in K containing an infinite subset is K. This means each infinite subset of K is a dense subset in the Zariski topology on K. In case that sounds weird, it is really just a topological expression of the familiar fact that polynomials in $K[x]$ are completely determined by their values on an infinite subset of K: if $f(x)$ and $g(x)$ in $K[x]$ are equal on an infinite subset of K then $f(x) - g(x)$ has infinitely many roots, so $f(x) - g(x) = 0$ in $K[x]$. This says that if $f(a) = g(a)$ for infinitely many $a \in K$ then $f(a) = g(a)$ for all $a \in K$; doesn't that make an infinite subset of K look "dense" for a topology on K when polynomials in $K[x]$ are continuous for that topology on K?

Putting a topology on K^n, like the Zariski topology, is extremely important in algebraic geometry (not so much for taking limits as in calculus, but for topological constructions like sheaves) and this is another example of the analogy with the Galois correspondence. We said above that varieties in K^n are analogous to subgroups of a Galois group. When Galois theory is generalized to infinite algebraic field extensions, it is important to put a topology on the infinite Galois group, called the Krull topology. (The Krull topology on finite Galois groups is discrete, and thus of no interest.) The subgroups of the Galois group that are relevant to the Galois correspondence for infinite-degree extensions are the subgroups that are closed in the Krull topology, which is analogous to the varieties in K^n being (by definition) the closed subsets of K^n for the Zariski topology. The Krull topology on an infinite Galois group makes the Galois group compact, and K^n in the Zariski topology is also compact, a property related to ideals in $K[x_1, \ldots, x_n]$ being finitely generated.

We assumed K is algebraically closed to show the maximal ideals in $K[x_1, \ldots, x_n]$ have an especially simple form, to prove the weak Nullstellensatz, and to prove the Nullstellensatz. In fact, all of these properties of a field K are equivalent.

Theorem 4.24. *Fix an integer $n \geq 1$. For a field K, the following properties are equivalent.*

1. *K is algebraically closed.*
2. *Each maximal ideal in $K[x_1, \ldots, x_n]$ is $(x_1 - c_1, \ldots, x_n - c_n)$ for some $c_i \in K$.*
3. *(Weak Nulllstellensatz) For each proper ideal J in $K[x_1, \ldots, x_n]$, $Z(J) \neq \emptyset$.*
4. *(Nullstellensatz) For each ideal J in $K[x_1, \ldots, x_n]$, $I(Z(J)) = \operatorname{Rad} J$.*

Proof. (1) $\Rightarrow$ (2): see the proof of Theorem 3.1.

[7] We do *not* use the Zariski topology on K^n when K is not algebraically closed. Algebraic geometry over non-algebraically closed fields requires a reconsideration of what a variety should be, analogous to the contrast between Theorems 3.1(2) and 3.4.

[8] For $n \geq 2$, the Zariski topology on K^n is *not* the product topology: the diagonal $\{(c,c) : c \in K\} = Z(y - x)$ is closed in the Zariski topology on K^2 but not in the product topology of the Zariski topologies on the two axes.

(2) $\Rightarrow$ (3): see the proof of the weak Nullstellensatz (Theorem 4.6), which is based on the description of maximal ideals in $K[x_1, \ldots, x_n]$ rather than an explicit assumption of K being algebraically closed.

(3) $\Rightarrow$ (4): see the proof of Theorem 4.17, which depends only the weak Nullstellensatz.

(4) $\Rightarrow$ (1): The contrapositive is proved (by example) in Remark 4.21: if K is not algebraically closed then there is a radical (in fact prime) ideal J in $K[x_1, \ldots, x_n]$ such that $I(Z(J)) \neq J$. □

5. Maximal ideals in $\mathbf{Z}[x]$

We now switch our attention to a polynomial ring over $\mathbf{Z}$: what are the maximal ideals in $\mathbf{Z}[x]$? We will first prove a result analogous to Zariski's lemma (Theorem 2.11) for all finitely generated $\mathbf{Z}$-algebras (rings of the form $\mathbf{Z}[\alpha_1, \ldots, \alpha_n]$, even if the subring generated by 1 is $\mathbf{Z}/m\mathbf{Z}$ rather than $\mathbf{Z}$). We'll apply the result to $\mathbf{Z}[x]$ in order to give construction maximal ideals in $\mathbf{Z}[x]$ and show the construction yields all maximal ideals.

Theorem 5.1. *If L is a field that is a finitely generated $\mathbf{Z}$-algebra then L is a finite field.*

Proof. Since L is a finitely generated $\mathbf{Z}$-algebra, $L = \mathbf{Z}[\alpha_1, \ldots, \alpha_n]$ for some $\alpha_1, \ldots, \alpha_n$ in L. The (unique) ring homomorphism $\mathbf{Z} \to L$ has kernel that is a prime ideal in $\mathbf{Z}$ (subrings of L are integral domains), so the kernel is (0) or $p\mathbf{Z}$ for prime p.

Case 1: The kernel of $\mathbf{Z} \to L$ is $p\mathbf{Z}$. Then L has characteristic p, so $L = \mathbf{F}_p[\alpha_1 \ldots, \alpha_n]$. This shows L is a field that is a finitely generated algebra over the field $\mathbf{F}_p$, so by Zariski's lemma, L is a finite extension of $\mathbf{F}_p$ and thus L is finite.

Case 2: The kernel of $\mathbf{Z} \to L$ is (0). Then L has characteristic 0, so $\mathbf{Z} \subset L$ and thus $\mathbf{Q} \subset L$ (since L is a field). We will show this case is impossible.

Since L is a field,

$$L = \mathbf{Z}[\alpha_1, \ldots, \alpha_n] \subset \mathbf{Q}[\alpha_1, \ldots, \alpha_n] \subset L,$$

so $L = \mathbf{Q}[\alpha_1, \ldots, \alpha_n]$. Thus L is a finitely generated $\mathbf{Q}$-algebra that is a field, so $L/\mathbf{Q}$ is a finite extension by Zariski's lemma. Therefore each α_i is algebraic over $\mathbf{Q}$: α_i is the root of a monic (irreducible) $f_i(x) \in \mathbf{Q}[x]$.

Let d in $\mathbf{Z}^+$ be a common denominator of the coefficients of $f_1(x), \ldots, f_n(x)$, so each $f_i(x)$ is monic in $\mathbf{Z}[1/d][x]$. Therefore each α_i is *integral* over $\mathbf{Z}[1/d]$ for $i = 1, \ldots, n$. From

$$L = \mathbf{Z}[\alpha_1, \ldots, \alpha_n] \subset \mathbf{Z}[1/d][\alpha_1, \ldots, \alpha_n] \subset L$$

we have $L = \mathbf{Z}[1/d][\alpha_1, \ldots, \alpha_n]$, so L is integral over $\mathbf{Z}[1/d]$ (Corollary 2.10). Since L is a field, $\mathbf{Z}[1/d]$ must be a field (Theorem 2.7), so $\mathbf{Z}[1/d] = \mathbf{Q}$. This is impossible: pick a prime p that doesn't divide d, so $1/p \in \mathbf{Q}$ but $1/p \notin \mathbf{Z}[1/d]$. Thus Case 2 can't occur. □

Note the similarity between the way a contradiction is reached at the end of Case 2 and at the end of the proof of Zariski's lemma: we can't have $\mathbf{Q} = \mathbf{Z}[1/d]$ for a positive integer d and for fields K we can't have $K(t) = K[t][1/d(t)]$ for a monic $d(t) \in K[t]$.

Corollary 5.2. *If R is a nonzero ring that is a finitely generated $\mathbf{Z}$-algebra then $R/\mathfrak{m}$ is a finite field for every maximal ideal $\mathfrak{m}$ of R. In particular, every maximal ideal of R is the kernel of a ring homomorphism from R onto a finite field.*

Proof. Since R is a finitely generated $\mathbf{Z}$-algebra, $R = \mathbf{Z}[\alpha_1, \ldots, \alpha_n]$ for some $\alpha_1, \ldots, \alpha_n$ in R. The quotient ring $R/\mathfrak{m}$ is $\mathbf{Z}[\overline{\alpha}_1, \ldots, \overline{\alpha}_n]$, where $\overline{\alpha}_i = \alpha_i \bmod \mathfrak{m}$, so $R/\mathfrak{m}$ is a field that is a finitely generated $\mathbf{Z}$-algebra. By Theorem 5.1, $R/\mathfrak{m}$ is finite.

Since $R/\mathfrak{m}$ is finite, $\mathfrak{m}$ is the kernel of reduction $R \to R/\mathfrak{m}$, which is a ring homomorphism from R onto a finite field. □

Theorem 5.3. *Here is a classification of maximal ideals in $\mathbf{Z}[x]$.*

(1) *For a prime p and monic $f(x) \in \mathbf{Z}[x]$ such that $f(x) \bmod p$ is irreducible in $\mathbf{F}_p[x]$, the ideal $(p, f(x))$ in $\mathbf{Z}[x]$ is maximal.*
(2) *For two maximal ideals $(p, f(x))$ and $(q, g(x))$ in $\mathbf{Z}[x]$ in the form described in (1), we have $(p, f(x)) = (q, g(x))$ if and only if $p = q$ and $\overline{f}(x) = \overline{g}(x)$ in $\mathbf{F}_p[x]$.*
(3) *All maximal ideals in $\mathbf{Z}[x]$ arise in the above way. In particular, maximal ideals in $\mathbf{Z}[x]$ have prime-power index, and for each prime power p^d the number of maximal ideals in $\mathbf{Z}[x]$ with index p^d is the number of monic irreducibles of degree d in $\mathbf{F}_p[x]$.*

For example the maximal ideals in $\mathbf{Z}[x]$ with prime index p are $(p, x-a)$ for $0 \leq a \leq p-1$, the maximal ideals with index 8 are $(2, x^3 + x + 1)$ and $(2, x^3 + x^2 + 1)$, and the maximal ideals with index 9 are $(3, x^2 + 1)$, $(3, x^2 + x + 2)$, and $(3, x^2 + 2x + 2)$.

Proof. (1) If p is prime and $f(x) \in \mathbf{Z}[x]$ is monic such that $\overline{f}(x) := f(x) \bmod p$ is irreducible in $\mathbf{F}_p[x]$ then $\mathbf{Z}[x]/(p, f(x)) \cong \mathbf{F}_p[x]/(\overline{f}(x))$, which is a field since the ideal generated by an irreducible in $\mathbf{F}_p[x]$ is maximal. Thus $(p, f(x))$ is a maximal ideal in $\mathbf{Z}[x]$.

(2) Suppose $(p, f(x)) = (q, g(x))$, where $f(x)$ and $g(x)$ are monic in $\mathbf{Z}[x]$ with $f(x) \bmod p$ irreducible in $\mathbf{F}_p[x]$ and $g(x) \bmod q$ irreducible in $\mathbf{F}_q[x]$. Necessarily $p = q$ since a proper ideal in $\mathbf{Z}[x]$ can't contain two different primes (otherwise it contains 1, which is a contradiction). If $\overline{f}(x) \neq \overline{g}(x)$ in $\mathbf{F}_p[x]$ then some $\mathbf{F}_p[x]$-linear combination of $\overline{f}(x)$ and $\overline{g}(x)$ is 1 (different monic irreducibles in $\mathbf{F}_p[x]$ generate the unit ideal in $\mathbf{F}_p[x]$). Therefore $f(x)u(x) + g(x)v(x) = 1 + ph(x)$ for some $u(x), v(x), h(x) \in \mathbf{Z}[x]$. Since $f(x), g(x)$, and p are all in $(p, f(x))$, we get $1 = fu + gv - ph \in (p, f(x))$, which contradicts $(p, f(x))$ being a proper ideal. Therefore $\overline{f}(x) = \overline{g}(x)$ in $\mathbf{F}_p[x]$.

Conversely, if $p = q$ and $\overline{f}(x) = \overline{g}(x)$ in $\mathbf{F}_p[x]$ then $g(x) \in (p, f(x))$, so $(p, g(x)) \subset (p, f(x))$, which implies $(p, g(x)) = (p, f(x))$ since both ideals are maximal in $\mathbf{Z}[x]$.

(3) Let M be a maximal ideal in $\mathbf{Z}[x]$. We want to prove $M = (p, f(x))$ for a prime p and monic $f(x) \in \mathbf{Z}[x]$ such that $f(x) \bmod p$ is irreducible in $\mathbf{F}_p[x]$. By Corollary 5.2, $\mathbf{Z}[x]/M$ is a finite field, so it has positive characteristic: $p = 0$ in $\mathbf{Z}[x]/M$, for a prime p, so $p \in M$.

Since M contains p, the surjective reduction homomorphism $\mathbf{Z}[x] \to \mathbf{Z}[x]/M$ kills p and thus it induces a surjective ring homomorphism $\mathbf{Z}[x]/(p) \to \mathbf{Z}[x]/M$, or equivalently

$$\varphi\colon \mathbf{F}_p[x] \to \mathbf{Z}[x]/M.$$

The kernel of this surjective homomorphism φ has to be a maximal ideal in $\mathbf{F}_p[x]$, so it is $(\pi(x))$ for some monic irreducible $\pi(x)$ in $\mathbf{F}_p[x]$. Let $f(x)$ be a monic lifting of $\pi(x)$ to $\mathbf{Z}[x]$: $f(x)$ is monic and $\pi(x) = \overline{f}(x)$ in $\mathbf{F}_p[x]$. That $\varphi(\pi(x)) = 0$ in $\mathbf{Z}[x]/M$ implies $f(x) \equiv 0 \bmod M$, so $f(x) \in M$ in $\mathbf{Z}[x]$. Thus $(p, f(x)) \subset M$. The ideal $(p, f(x))$ is maximal by part (1) since $f(x) \bmod p$ is irreducible in $\mathbf{F}_p[x]$, so the containment $(p, f(x)) \subset M$ implies $M = (p, f(x))$. □

The most important step in the proof of part (3) is that $M \cap \mathbf{Z}$ contains a prime number. Our proof of that relies on Corollary 5.2, which depends on Theorem 5.1, which depends on Zariski's lemma. It's reasonable to ask if we can prove $M \cap \mathbf{Z}$ contains a prime number without having to prove Zariski's lemma first. Since $M \cap \mathbf{Z}$ is a prime ideal in $\mathbf{Z}$, $M \cap \mathbf{Z}$ is (0) or $p\mathbf{Z}$ for a prime p. Here is a proof of $M \cap \mathbf{Z} \neq (0)$ that doesn't depend on Zariski's lemma, but it has common features with the proof we gave of Zariski's lemma.

We argue by contradiction. Assume $M \cap \mathbf{Z} = (0)$. The natural composite homomorphism $\mathbf{Z} \to \mathbf{Z}[x] \to \mathbf{Z}[x]/M$ has kernel $M \cap \mathbf{Z}$, which is (0), so the map is injective. Thus $\mathbf{Z}$ is a subring of $\mathbf{Z}[x]/M$. Set

$$F = \mathbf{Z}[x]/M, \quad \alpha = x \bmod M.$$

Then $F = \mathbf{Z}[\overline{x}] = \mathbf{Z}[\alpha]$ as a ring. Since F is a field (it's a ring modulo a maximal ideal) and it contains $\mathbf{Z}$, F also contains $\mathbf{Q}$. Define a ring homomorphism $\varphi\colon \mathbf{Q}[y] \to F$ to be evaluation a α: $\varphi(f(y)) = f(\alpha)$ for all $f(y) \in \mathbf{Q}[y]$.

Since $\mathbf{Z} \subset \mathbf{Q} \subset F$ and F is generated as a ring by $\mathbf{Z}$ and α, F is generated as a ring by $\mathbf{Q}$ and α:

$$F = \mathbf{Z}[\alpha] = \mathbf{Q}[\alpha]. \tag{5.1}$$

(This should already seem weird!) The map $\varphi\colon \mathbf{Q}[y] \to F$ is onto since $F = \mathbf{Q}[\alpha]$. Since F is a field, $\ker\varphi$ is a maximal ideal in $\mathbf{Q}[y]$, so $\ker\varphi = (\pi(y))$ for a monic irreducible $\pi(y) \in \mathbf{Q}[y]$. That $\pi(y) \in \ker\varphi$ implies $0 = \varphi(\pi(y)) = \pi(\alpha)$ in F.

Let $d \in \mathbf{Z}^+$ be a common denominator of the coefficients of $\pi(y)$, so $\pi(y)$ is monic with coefficients in $\mathbf{Z}[1/d]$. Thus the equation $\pi(\alpha) = 0$ tells us α is *integral* over the ring $\mathbf{Z}[1/d]$. Since $\mathbf{Z} \subset \mathbf{Z}[1/d] \subset \mathbf{Q}$, (5.1) implies $F = \mathbf{Z}[1/d][\alpha]$. Since α is integral over $\mathbf{Z}[1/d]$, F is an integral extension of $\mathbf{Z}[1/d]$ (Corollary 2.10). Since F is a field, $\mathbf{Z}[1/d]$ is also a field (Theorem 2.7), That tells us $\mathbf{Q} = \mathbf{Z}[1/d]$, which is impossible: for a prime p not dividing d, $1/p \in \mathbf{Q}$ but $1/p \notin \mathbf{Z}[1/d]$.[9] Thus $M \cap \mathbf{Z} \neq (0)$.

The next theorem applies the description of maximal ideals in finitely generated $\mathbf{Z}$-algebras.

Theorem 5.4. *Let $f_1, \ldots, f_r$ be polynomials in $\mathbf{Z}[x_1, \ldots, x_n]$. The following conditions are equivalent.*

1. *For every prime p, the reductions $\overline{f}_1, \ldots, \overline{f}_r$ in $\mathbf{F}_p[x_1, \ldots, x_n]$ have no common zero in $\overline{\mathbf{F}}_p^{\,n}$.*
2. *$(f_1, \ldots, f_r) = (1)$ in $\mathbf{Z}[x_1, \ldots, x_n]$.*

Proof. (2) $\Rightarrow$ (1): If $f_1g_1 + \cdots + f_rg_r = 1$ in $\mathbf{Z}[x_1, \ldots, x_n]$ then $\overline{f}_1\overline{g}_1 + \ldots + \overline{f}_r\overline{g}_r = \overline{1}$ in $\mathbf{F}_p[x_1, \ldots, x_n]$ for each prime p, so there is no common zero of the reductions $\overline{f}_i$ in $\overline{\mathbf{F}}_p^{\,n}$.

(1) $\Rightarrow$ (2): We will prove the contrapositive. If $(f_1, \ldots, f_r) \neq (1)$ then we will show there is a prime p such that $\overline{f}_1, \ldots, \overline{f}_r$ have a common zero in $\overline{\mathbf{F}}_p^{\,n}$.

Since $(f_1, \ldots, f_r) \neq (1)$ there is a maximal ideal $\mathfrak{m}$ in $\mathbf{Z}[x_1, \ldots, x_n]$ such that $(f_1, \ldots, f_r) \subset \mathfrak{m}$. By Corollary 5.2, $\mathfrak{m}$ is the kernel of a homomorphism φ from $\mathbf{Z}[x_1, \ldots, x_n]$ onto a finite field $\mathbf{F}$. Set $\alpha_i = \varphi(x_i)$, so $(\alpha_1, \ldots, \alpha_n) \in \mathbf{F}^n$ is an n-tuple in the finite field $\mathbf{F}$ and for each $f \in \mathbf{Z}[x_1, \ldots, x_n]$,

$$\varphi(f(x_1, \ldots, x_n)) = f(\varphi(x_1), \ldots, \varphi(x_n)) = \overline{f}(\alpha_1, \ldots, \alpha_n) \in \mathbf{F},$$

where $\overline{f}$ has the integral coefficients of f reduced mod p where p is the characteristic of $\mathbf{F}$. Therefore φ is evaluation at $(\alpha_1, \ldots, \alpha_n)$, and the fact that $(f_1, \ldots, f_r) \subset \mathfrak{m} = \ker(\varphi)$, tells us $\overline{f}_i(\alpha_1, \ldots, \alpha_n) = 0$ in $\mathbf{F}$ for all i, so the polynomials $\overline{f}_1, \ldots, \overline{f}_n$ in $\mathbf{F}_p[x_1, \ldots, x_n]$ have the common zero $(\alpha_1, \ldots, \alpha_n)$ in $\mathbf{F}^n \subset \overline{\mathbf{F}}_p^{\,n}$. □

Example 5.5. Let $f(x) = x^4 - 2$ and $g(x) = x^3 + x + 5$. They are relatively prime in $\mathbf{Q}[x]$, so a $\mathbf{Q}[x]$-linear combination is 1. After working out such a relation with Euclid's algorithm and clearing the denominator, we get

$$(8x^2 - 5x + 17)f(x) - (8x^3 - 5x^2 + 9x - 35)g(x) = 141 = 3 \cdot 47$$

in $\mathbf{Z}[x]$. So there is no common zero of $f(x)$ mod p and $g(x)$ mod p in $\overline{\mathbf{F}}_p$ when $p \neq 3$ or 47. In $\mathbf{F}_3[x]$, $\overline{f}(x) = (x^2 + x + 2)(x^2 + 2x + 2)$ and $\overline{g}(x) = (x + 1)(x^2 + 2x + 2)$, so $\overline{f}(x)$ and $\overline{g}(x)$ have a common root in $\mathbf{F}_9$ (a root of $x^2 + 2x + 2$ in characteristic 3). In $\mathbf{F}_{47}[x]$, $\overline{f}(x) = (x - 17)(x - 30)(x^2 + 7)$ and $\overline{g}(x) = (x - 17)(x^2 + 17x + 8)$, so $\overline{f}(x)$ and $\overline{g}(x)$ have the common root 17 in $\mathbf{F}_{47}$. Therefore the only maximal ideals in $\mathbf{Z}[x]$ containing $f(x)$ and

[9] Note the similarity to the end of the proof of Zariski's lemma.

$g(x)$ are $(3, x^2+2x+2)$ and $(47, x-17)$. The ideals $(f(x))$ and $(g(x))$ in $\mathbf{Z}[x]$ are analogous to curves in the plane, and saying $(f(x), g(x))$ lies in two maximal ideals is like saying a pair of curves intersects in two points.

The description of maximal ideals in $\mathbf{Z}[x]$ extends to a description of prime ideals in $\mathbf{Z}[x]$.

Theorem 5.6. *Here are the prime ideals $\mathfrak{p}$ in $\mathbf{Z}[x]$ and their quotient rings $\mathbf{Z}[x]/\mathfrak{p}$.*

(*i*) $\mathfrak{p} = (0)$, *with quotient ring* $\mathbf{Z}[x]$.
(*ii*) $\mathfrak{p} = (p)$ *for a prime number* p *with quotient ring* $\mathbf{F}_p[x]$.
(*iii*) $\mathfrak{p} = (\pi(x))$ *for nonconstant irreducible* $\pi(x)$ *in* $\mathbf{Z}[x]$ *with quotient ring* $\mathbf{Z}[\alpha]$, *where* $\pi(\alpha) = 0$.
(*iv*) $\mathfrak{p} = (p, f(x))$ *for a prime number* p *and monic* $f(x) \in \mathbf{Z}[x]$ *such that* $f(x) \bmod p$ *is irreducible in* $\mathbf{F}_p[x]$, *with quotient ring the finite field* $\mathbf{F}_p[x]/(\overline{f}(x))$.

Example 5.7. Prime ideals of type (iii) include $(2x-1)$ with quotient ring $\mathbf{Z}[1/2]$, (x^2+1) with quotient ring $\mathbf{Z}[i]$, and $(3x^2 - 10x + 1)$ with quotient ring $\mathbf{Z}[(5+\sqrt{22})/3]$.

Proof. The intersection $\mathfrak{p} \cap \mathbf{Z}$ is a prime ideal in $\mathbf{Z}$, so it is (0) or $p\mathbf{Z}$ for a prime number p.

Case 1: $\mathfrak{p} \cap \mathbf{Z} = p\mathbf{Z}$ for a prime p. Such $\mathfrak{p}$ correspond under the reduction map $\mathbf{Z}[x] \to \mathbf{Z}[x]/(p)$ to prime ideals in $\mathbf{Z}[x]/(p) \cong \mathbf{F}_p[x]$. All $\mathfrak{p}$ of types (ii) and (iv) occur this way.

The prime ideals in $\mathbf{F}_p[x]$ are $(\overline{0})$ and maximal ideals $(\overline{f}(x))$ where $f(x) \in \mathbf{Z}[x]$ is monic with $\overline{f}(x) := f(x) \bmod p$ being irreducible in $\mathbf{F}_p[x]$. Lifting these back into $\mathbf{Z}[x]$, we get the prime ideal $(p) = p\mathbf{Z}[x]$ and the maximal ideal $(p, f(x))$, with respective quotient rings $\mathbf{F}_p[x]$ and $\mathbf{F}_p[x]/(\overline{f}(x))$.

Case 2: $\mathfrak{p} \cap \mathbf{Z} = (0)$. All $\mathfrak{p}$ of type (i) and (iii) occur this way. Henceforth suppose $\mathfrak{p} \neq (0)$.

Pick a nonzero element of $\mathfrak{p}$. It is not ± 1, so it has an irreducible factorization in $\mathbf{Z}[x]$ and thus an irreducible factor $\pi(x)$ is in $\mathfrak{p}$. The polynomial $\pi(x)$ is nonconstant since $\mathfrak{p} \cap \mathbf{Z} = (0)$. We will show $\mathfrak{p} = (\pi(x))$.

Since $\pi(x) \in \mathfrak{p}$, $(\pi(x)) \subset \mathfrak{p}$. To show $\mathfrak{p} \subset (\pi(x))$, assume some $g(x) \in \mathfrak{p}$ is not divisible by $\pi(x)$. Then a nonconstant irreducible factor of $g(x)$ is in $\mathfrak{p}$, say $\widetilde{\pi}(x)$. So $\pi(x)$ and $\widetilde{\pi}(x)$ are two nonconstant irreducible polynomials in $\mathfrak{p}$, and $\widetilde{\pi}(x) \neq \pm\pi(x)$ since $\pi(x) \nmid g(x)$.

At this point we bring in a description of the nonconstant irreducibles in $\mathbf{Z}[x]$: they are precisely the primitive polynomials in $\mathbf{Z}[x]$ (gcd of coefficients is 1) that are irreducible in $\mathbf{Q}[x]$. Thus $\pi(x)$ and $\widetilde{\pi}(x)$ are irreducible in $\mathbf{Q}[x]$ and are not constant multiples of each other in $\mathbf{Q}[x]$ (since they are primitive and not equal up to sign). Thus $\pi(x)$ and $\widetilde{\pi}(x)$ are relatively prime irreducibles in $\mathbf{Q}[x]$, so $\pi(x)u(x) + \widetilde{\pi}(x)v(x) = 1$ where $u(x)$ and $v(x)$ are in $\mathbf{Q}[x]$. Clearing denominators, $\pi(x)a(x) + \widetilde{\pi}(x)b(x) = c$ where $a(x)$ and $b(x)$ are in $\mathbf{Z}[x]$ and c is a nonzero integer. Since $\pi(x)$ and $\widetilde{\pi}(x)$ are in $\mathfrak{p}$ we get $c \in \mathfrak{p}$, which contradicts the assumption that $\mathfrak{p} \cap \mathbf{Z} = (0)$. Thus $\mathfrak{p} \subset (\pi(x))$, so $\mathfrak{p} = (\pi(x))$.

It remains to show for each nonconstant irreducible $\pi(x)$ in $\mathbf{Z}[x]$ that the ideal $(\pi(x))$ in $\mathbf{Z}[x]$ is a prime ideal and to compute the quotient ring $\mathbf{Z}[x]/(\pi(x))$. Since $\mathbf{Z}[x]$ has unique factorization, if $\pi(x) \mid g(x)h(x)$ in $\mathbf{Z}[x]$ then $\pi(x) \mid g(x)$ or $\pi(x) \mid h(x)$, so $(\pi(x))$ is a prime ideal in $\mathbf{Z}[x]$. (It is not a maximal ideal because $(\pi(x)) \cap \mathbf{Z} = (0)$ and we saw in Theorem 5.3 that every maximal ideal in $\mathbf{Z}[x]$ contains a prime number.)

Let α be a root of $\pi(x)$ in a field extension of $\mathbf{Q}$. Evaluation at α is a surjective ring homomorphism $\mathbf{Z}[x] \to \mathbf{Z}[\alpha]$. We will show the kernel is $(\pi(x))$: if $f(x) \in \mathbf{Z}[x]$ and $f(\alpha) = 0$ then $\pi(x) \mid f(x)$ in $\mathbf{Z}[x]$ (the converse is obvious). Since $\pi(x)$ is irreducible in $\mathbf{Q}[x]$ and $\mathbf{Q}$ is a field, if $f(x) \in \mathbf{Z}[x]$ and $f(\alpha) = 0$ then $\pi(x) \mid f(x)$ in $\mathbf{Q}[x]$: $f(x) = \pi(x)g(x)$ where $g(x) \in \mathbf{Q}[x]$. Let c be a common denominator of the coefficients of $g(x)$: $g(x) = G(x)/c$ where $G(x) \in \mathbf{Z}[x]$, so $cf(x) = \pi(x)G(x)$ in $\mathbf{Z}[x]$. Therefore $\pi(x) \mid cf(x)$ in $\mathbf{Z}[x]$, and $\pi(x)$ is not constant, so unique factorization in $\mathbf{Z}[x]$ implies $\pi(x) \mid f(x)$ in $\mathbf{Z}[x]$. $\square$

The nonzero non-maximal prime ideals (p) and $(\pi(x))$ in $\mathbf{Z}[x]$ (as p and $\pi(x)$ vary) have no containment relations among them, so the possible chains of prime ideals in $\mathbf{Z}[x]$ are

$$(0) \subset (p) \subset \mathfrak{m}, \quad (0) \subset (\pi(x)) \subset \mathfrak{m}$$

for maximal ideals $\mathfrak{m}$. The $\mathfrak{m}$ containing (p) have the form $(p, f(x))$ where p is prime and $f(x)$ mod p is irreducible, The $\mathfrak{m}$ containing $(\pi(x))$ have the form $(p, f(x))$ where p is prime, $f(x)$ mod p is irreducible, and the image of $\pi(x)$ in $\mathbf{F}_p[x]/(\overline{f}(x))$ is 0; this is equivalent to $\overline{f}(x) \mid \overline{\pi}(x)$ in $\mathbf{F}_p[x]$, so $\overline{f}(x)$ is an irreducible factor of $\overline{\pi}(x)$ in $\mathbf{F}_p[x]$. Describing the maximal ideals in $\mathbf{Z}[x]$ containing $(\pi(x))$ amounts to describing the irreducible factorization of $\pi(x)$ mod p in $\mathbf{F}_p[x]$ for each prime p.

Example 5.8. The maximal ideals in $\mathbf{Z}[x]$ containing $(2x-1)$ are all $(p, 2x-1)$ where p is an odd prime.

Example 5.9. The maximal ideals in $\mathbf{Z}[x]$ containing (x^2+1) are all $(p, f(x))$ where $\overline{f}(x) \mid (x^2+1)$ in $\mathbf{F}_p[x]$. We take cases depending on the irreducible factorization of x^2+1 mod p and there are three possibilities:

- $(2, x+1)$,
- $(p, x-r)$ and $(p, x+r)$ where $p \equiv 1 \bmod 4$ and $r^2 \equiv -1 \bmod p$,
- (p, x^2+1) where $p \equiv 3 \bmod 4$.

Pictures of all the prime ideals of $\mathbf{Z}[x]$ are famous in algebraic geometry, and can be found at https://pbelmans.ncag.info/blog/atlas/.

Appendix A. Nullstellensatz for non-algebraically closed fields

In this appendix we extend the Nullstellensatz from algebraically closed fields to arbitrary fields. For a field K, let C/K be an algebraically closed extension (*e.g.*, $C = \overline{K}$). This will be fixed throughout our discussion. We will obtain a bijection between the radical ideals in $K[x_1, \ldots, x_n]$ and the varieties in C^n "defined over K", which means being the zero set of polynomials with coefficients in K.

Definition A.1. A *K-variety* in C^n is the zero set in C^n of a subset S of $K[x_1, \ldots, x_n]$:

$$Z_{C^n}(S) = \{\mathbf{a} \in C^n : f(\mathbf{a}) = 0 \text{ for all } f \in S\}.$$

Replacing S with the ideal $\langle S \rangle$ or with the radical of the ideal $\langle S \rangle$ does not change the zero set, so we can always suppose a K-variety in C^n is the zero set in C^n of a finite set of polynomials in $K[x_1, \ldots, x_n]$ (ideals in this ring are finitely generated).

Example A.2. The polynomial x^2+y^2+1 defines an $\mathbf{R}$-variety in $\mathbf{C}^2$:

$$Z_{\mathbf{C}^2}(x^2+y^2+1) = \{(z.w) \in \mathbf{C}^2 : z^2+w^2+1 = 0\}.$$

This $\mathbf{R}$-variety in $\mathbf{C}^2$ has no solutions in $\mathbf{R}^2$, but it has many complex solutions.

Definition A.3. For each K-variety $V \subset C^n$, set

$$I_K(V) = \{f \in K[x_1, \ldots, x_n] : f(\mathbf{a}) = 0 \text{ for all } \mathbf{a} \in V\}.$$

This is a radical ideal in $K[x_1, \ldots, x_n]$.

Theorem A.4. *For K-varieties V in C^n, $Z_{C^n}(I_K(V)) = V$.*

This is a generalization of Theorem 4.4 and the proof will be the same except for some more care about polynomials having coefficients in K rather than C.

Proof. It's easy to see that $V \subset Z_{C^n}(I_K(V))$. To show the reverse containment, write $V = Z_{C^n}(J)$ for a radical ideal J in $K[x_1, \ldots, x_n]$. (This is how we use the condition that V is a K-variety.) Then $J \subset I_K(V) = I_K(Z_{C^n}(J))$. For $\mathbf{a} \in Z_{C^n}(I_K(V))$ and $f \in I_K(V)$, $f(\mathbf{a}) = 0$. In particular, for $\mathbf{a} \in Z_{C^n}(I_K(V))$ and $f \in J$, $f(\mathbf{a}) = 0$. Thus $\mathbf{a} \in Z_{C^n}(J) = V$, so $Z_{C^n}(I_K(V)) \subset V$. □

Here is a generalization of Theorem 4.5.

Theorem A.5. *For a K-variety V in C^n, $I_K(V)$ is a maximal ideal in $K[x_1, \ldots, x_n]$ if and only if V is the $\mathrm{Aut}(C/K)$-orbit of a point in $\overline{K}^n$, which is the same thing as an $\mathrm{Aut}(\overline{K}/K)$-orbit of a point in $\overline{K}^n$.*

Proof. First we address the relation between an $\mathrm{Aut}(C/K)$-orbit and $\mathrm{Aut}(\overline{K}/K)$-orbit of a point in $\overline{K}^n$, which is contained in C^n. For a point $\mathbf{a}$ in $\overline{K}^n$ and $\sigma \in \mathrm{Aut}(C/K)$, σ maps each coordinate of $\mathbf{a}$ to an element of $\overline{K}$ since σ preserves algebraic relations over K. Thus the $\mathrm{Aut}(C/K)$-orbit of $\mathbf{a}$ is inside $\overline{K}^n$ and it is the $\mathrm{Aut}(\overline{K}/K)$-orbit of $\mathbf{a}$ since the restriction mapping $\mathrm{Aut}(C/K) \to \mathrm{Aut}(\overline{K}/K)$ is surjective by Zorn's lemma (every K-isomorphism $\overline{K} \to \overline{K}$ extends to a K-isomorphism $C \to C$).

Let V be the $\mathrm{Aut}(C/K)$-orbit of some $\mathbf{a} \in \overline{K}^n$. Evaluation at $\mathbf{a}$ is a K-algebra homomorphism $K[x_1, \ldots, x_n] \to \overline{K}$ and its kernel $\mathfrak{m}$ (a maximal ideal: why?) contains each $f \in I_K(V)$. Thus $I_K(V) \subset \mathfrak{m}$. Conversely, if $f \in \mathfrak{m}$ then $f(\mathbf{a}) = 0$, so for all $\sigma \in \mathrm{Aut}(C/K)$,

$$0 = \sigma(f(\mathbf{a})) = f(\sigma(\mathbf{a}))$$

since f has coefficients in K. Thus $\mathfrak{m} \subset I_K(V)$, so $I_K(V) = \mathfrak{m}$.

Now let $I_K(V)$ be a maximal ideal in $K[x_1, \ldots, x_n]$. Then $I_K(V)$ is the kernel of an evaluation homomorphism $K[x_1, \ldots, x_n] \to \overline{K}$ at some point $\mathbf{a} \in \overline{K}^n$ by Theorem 3.4, so the polynomials in $I_K(V)$ are polynomials in $K[x_1, \ldots, x_n]$ that vanish at $\mathbf{a}$. Since V is a K-variety, Theorem A.4 tells us

$$V = Z_{C^n}(I_K(V)) = \{\mathbf{b} \in C^n : f(\mathbf{b}) = 0 \text{ when } f(\mathbf{a}) = 0\}. \tag{A.1}$$

We want to show each $\mathbf{b}$ in V has coordinates in $\overline{K}$ and $\mathbf{b} = \sigma(\mathbf{a})$ for some $\sigma \in \mathrm{Aut}(\overline{K}/K)$.

Write $\mathbf{a} = (a_1, \ldots, a_n)$ and $\mathbf{b} = (b_1, \ldots, b_n)$. Let a_i have minimal polynomial $\pi_i(x) \in K[x]$. Then $\pi_i(a_i) = 0$, so $\pi_i(x_i)$ is in $I_K(V)$ for $i = 1, \ldots, n$. Since $\mathbf{b} \in V$, $\pi_i(b_i) = 0$ by (A.1). Thus the coordinates of $\mathbf{b}$ are all in $\overline{K}$, so $\mathbf{b} \in \overline{K}^n$ and (A.1) says

$$\mathfrak{m}_{\mathbf{a}} \cap K[x_1, \ldots, x_n] \subset \mathfrak{m}_{\mathbf{b}} \cap K[x_1, \ldots, x_n].$$

Both intersections are maximal ideals by Theorem 3.4, so the containment is an equality and $\mathbf{b} = \sigma(\mathbf{a})$ for some $\sigma \in \mathrm{Aut}(\overline{K}/K)$. □

Comparing Theorem A.5 to Theorem 4.5 suggests that a "K-point of $\overline{K}^n$" should be an $\mathrm{Aut}(\overline{K}/K)$-orbit of a point in $\overline{K}^n$. When K is algebraically closed, so $\overline{K} = K$, this is the classical notion of a point in K^n since $\mathrm{Aut}(K/K)$ is trivial.

Example A.6. Returning to Example A.2, the $\mathbf{R}$-variety

$$Z_{\mathbf{C}^2}(x^2 + y^2 + 1) = \{(z.w) \in \mathbf{C}^2 : z^2 + w^2 + 1 = 0\}$$

has no classical real points. Pairs of complex-conjugate points, such as $\{(i, 0), (-i, 0)\}$, are the $\mathbf{R}$-points (of "degree 2" since it is a set of 2 related complex solutions).

Lemma A.7. *For a field extension L/K, let $\{e_\beta\}_{\beta \in B}$ be a K-basis: $L = \bigoplus_{\beta \in B} Ke_\beta$. Then $L[x_1, \ldots, x_n]$ is a free $K[x_1, \ldots, x_n]$-module with basis $\{e_\beta\}_{\beta \in B}$.*

For example, $\mathbf{C}[x, y] = \mathbf{R}[x, y] + i\mathbf{R}[x, y]$. If that seems obvious then you understand what the lemma is saying, except in general $[L : K]$ could be infinite (*e.g.*, $K = \mathbf{Q}$ and $L = \overline{\mathbf{Q}}$ or $L = \mathbf{C}$).

Proof. The set $\{e_\beta\}$ is a $K[x_1,\ldots,x_n]$-linear spanning set of $L[x_1,\ldots,x_n]$. Since each element of L is a finite K-linear combination of elements in $\{e_\beta\}$ and each polynomial $f \in L[x_1,\ldots,x_n]$ have finitely many coefficients, writing each of the coefficients of f in terms of the K-basis of L and then collecting monomials from $K[x_1,\ldots,x_n]$ that are multiplied by the same e_β shows f is a $K[x_1,\ldots,x_n]$-linear combination of $\{e_\beta\}$.

$K[x_1,\ldots,x_n]$-linear independence of $\{e_\beta\}$. Assume $\sum_{\beta\in B} g_\beta e_\beta = 0$, where the sum has finitely many terms $g_\beta \in K[x_1,\ldots,x_n]$. Because there are finitely many terms, there is an upper bound on degrees of monomials appearing in each g_β, say degree d: $g_\beta = \sum_{|\mathbf{j}|\le d} a_{\beta\mathbf{j}}\mathbf{x}^{\mathbf{j}}$ where $\mathbf{j} = (j_1,\ldots,j_j)$ is an n-tuple, $\mathbf{x}^{\mathbf{j}} = x_1^{j_1}\ldots x_n^{j_n}$, and $a_{\beta\mathbf{j}} \in K$. Then in $L[x_1,\ldots,x_n]$,

$$0 = \sum_{\beta\in B} g_\beta e_\beta = \sum_{|\mathbf{j}|\le d}\left(\sum_\beta a_{\beta\mathbf{j}} e_\beta\right)\mathbf{x}^{\mathbf{j}},$$

so by the meaning of equality in $L[x_1,\ldots,x_n]$ we get $\sum_\beta a_{\beta\mathbf{j}} e_\beta = 0$ for each $\mathbf{j}$. Therefore by K-linear independence of $\{e_\beta\}$, $a_{\beta\mathbf{j}} = 0$ for all β and $\mathbf{j}$. Thus each g_β is 0. □

Theorem A.8. *For an ideal J in $K[x_1,\ldots,x_n]$ and field extension L/K, if the extended ideal $JL[x_1,\ldots,x_n]$ in $L[x_1,\ldots,x_n]$ equals $L[x_1,\ldots,x_n]$ then $J = K[x_1,\ldots,x_n]$.*

Proof. Let $\{e_\beta\}_{\beta\in B}$ be a K-basis and we may assume 1 is an element of this basis, say $1 = e_{\beta_0}$. The ideal $JL[x_1,\ldots,x_n]$ consists of finite sums of products of elements in J times elements in $L[x_1,\ldots,x_n]$. Since $L[x_1,\ldots,x_n]$ has $K[x_1,\ldots,x_n]$-basis $\{e_\beta\}_{\beta\in B}$ by Lemma A.7 and $JK[x_1,\ldots,x_n] \subset J$, we have

$$JL[x_1,\ldots,x_n] = \bigoplus_{\beta\in B} Je_\beta.$$

If $JL[x_1,\ldots,x_n] = L[x_1,\ldots,x_n]$ then $1 \in JL[x_1,\ldots,x_n]$, so $1 = \sum_{\beta\in B} g_\beta e_\beta$ (a finite sum) where $g_\beta \in J$. From the coefficient of e_{β_0} on both sides, $1 = g_{\beta_0} \in J$. So $J = K[x_1,\ldots,x_n]$. □

Theorem A.9 (Weak Nullstellensatz over K)**.** *If J is a proper ideal in $K[x_1,\ldots,x_n]$ then $Z_{C^n}(J) \neq \emptyset$ in C^n.*

Proof. Since $J \neq (1)$ in $K[x_1,\ldots,x_n]$, $JC[x_1,\ldots,x_n] \neq (1)$ in $C[x_1,\ldots,x_n]$ by Theorem A.8. Thus $JC[x_1,\ldots,x_n] \subset \mathfrak{m}$ for a maximal ideal $\mathfrak{m}$ in $C[x_1,\ldots,x_n]$, so $J \subset \mathfrak{m}$. Since C is algebraically closed, $\mathfrak{m} = (x_1 - c_1,\ldots,x_n - c_n)$ for $c_1,\ldots,c_n \in C$, so $(c_1,\ldots,c_n) \in Z_{C^n}(J)$. Thus $Z_{C^n}(J) \neq \emptyset$. □

Corollary A.10. *Let K be a field and $f_1,\ldots,f_r \in K[x_1,\ldots,x_n]$. The following conditions are equivalent.*

1. *The system of polynomial equations $f_1 = 0,\ldots,f_r = 0$ does not have a solution in C.*
2. *$(f_1,\ldots,f_r) = (1)$ in $K[x_1,\ldots,x_n]$.*

The key point in the second condition is that the ideal generated by the f_i in $K[x_1,\ldots,x_n]$ is the unit ideal, not just the ideal generated by the f_i in $C[x_1,\ldots,x_n]$.

Proof. It is obvious that the second condition implies the first condition. To show the first condition implies the second condition, set $J = (f_1,\ldots,f_r)$ in $K[x_1,\ldots,x_r]$. The first condition says $Z_{C^n}(J) = \emptyset$, so Theorem A.9 tells us that $J = (1)$: $f_1g_1 + \cdots + f_rg_r = 1$ for some $g_i \in K[x_1,\ldots,x_n]$. □

For example, if $f_1, \ldots, f_r \in \mathbf{Q}[x_1, \ldots, x_n]$, then in order for the system of equations $f_1 = 0, \ldots, f_r = 0$ not to have a solution in $\mathbf{C}^n$ or $\overline{\mathbf{Q}}^n$, it is necessary and sufficient that $f_1 g_1 + \cdots + f_r g_r = 1$ for some $g_i \in \mathbf{Q}[x_1, \ldots, x_n]$.

Theorem A.11 (Nullstellensatz over K)**.** *For each ideal J in $K[x_1, \ldots, x_n]$, $I_K(Z_{C^n}(J)) = \operatorname{Rad} J$.*

We can write $J = (f_1, \ldots, f_r)$ since ideals in $K[x_1, \ldots, x_n]$ are finitely generated. The more interesting containment $I_K(Z_{C^n}(J)) \subset \operatorname{Rad} J$ says that if $g \in K[x_1, \ldots, x_n]$ vanishes on C^n (not just K^n!) wherever $f_1, \ldots, f_r$ all vanish, then $g^m \in J$ for some $m \geq 1$.

Proof. It is easy to check that $\operatorname{Rad} J \subset I_K(Z_{C^n}(J))$. We will show $I_K(Z_{C^n}(J)) \subset \operatorname{Rad} J$ by the Rabinowitsch trick.

The ideal J can be written as $(f_1, \ldots, f_r)$. For $g \in I_K(Z_{C^n}(J))$ such that $g \neq 0$, define an ideal in $K[x_1, \ldots, x_n, x_{n+1}]$:

$$J' := (f_1, \ldots, f_r, x_{n+1}g - 1)$$

Because g vanishes on C^n wherever $f_1, \ldots, f_r$ all vanish, the generators of J' have no common zero in C^n. Therefore $Z_{C^n}(J') = \emptyset$, so the weak Nullstellensatz over K tells us $J' = K[x_1, \ldots, x_{n+1}]$. Thus $1 \in J'$:

$$1 = \sum_{j=1}^{r} h_j(x_1, \ldots, x_n, x_{n+1}) f_j(x_1, \ldots, x_n) + h(x_1, \ldots, x_n, x_{n+1})(x_{n+1}g - 1)$$

for some $h_1, \ldots, h_r, h$ in $K[x_1, \ldots, x_{n+1}]$. The rest of the proof proceeds just as in the proof of the Nullstellensatz over algebraically closed fields. □

Example A.12. For a field K, let f be irreducible in $K[x_1, \ldots, x_n]$. For $g \in K[x_1, \ldots, x_n]$, we'll show $g = 0$ at all points in $\overline{K}^n$ where $f = 0$ if and only if $f \mid g$ in $K[x_1, \ldots, x_n]$. The polynomials in $K[x_1, \ldots, x_n]$ that vanish in $\overline{K}^n$ where f vanishes form the ideal $I_K(Z_{\overline{K}^n}(f))$, and by the Nullstellensatz over K that ideal in $K[x_1, \ldots, x_n]$ is $\operatorname{Rad}(f)$, which equals (f) since f is irreducible in $K[x_1, \ldots, x_n]$. Thus $g \in I_K(Z_{\overline{K}^n}(f))$ is equivalent to $f \mid g$. We have generalized Example 4.18 from algebraically closed fields K to all fields K.

Consider $x^2 - 2y^2$ in $\mathbf{Q}[x, y]$. It is irreducible since, viewed in $\mathbf{Q}[y][x]$, it is quadratic in x with no root in $\mathbf{Q}[y]$ (think about the rational roots theorem over a UFD). If $g(x, y) \in \mathbf{Q}[x, y]$ satisfies $g(a, b) = 0$ for all $a, b \in \overline{\mathbf{Q}}$ such that $a^2 = 2b^2$ then $(x^2 - 2y^2) \mid g(x, y)$ in $\mathbf{Q}[x, y]$. Note $x^2 - 2y^2$ is not irreducible in $\overline{\mathbf{Q}}[x, y]$.

Example A.13. For a field K, set $J = (x^2, xy, z^2)$ in $K[x, y, z]$. Then

$$Z_{\overline{K}^3}(J) = \{(0, b, 0) : b \in \overline{K}\},$$
$$I_K(Z_{\overline{K}^3}(J)) = \{g \in K[x, y, z] : g(0, b, 0) = 0 \text{ for all } b \in \overline{K}\}.$$

As in Example 4.19, $(x, z) \subset I_K(Z_{\overline{K}^3}(J))$ and the reverse containment $I_K(Z_{\overline{K}^3}(J)) \subset (x, z)$ follows by either a concrete calculation (since $\overline{K}$ is infinite) or by using the Nullstellensatz over K (since (x, z) is a prime ideal in $K[x, y, z]$ for all fields K).

It is important to use the zero set $Z_{\overline{K}^3}(x^2, xy, z^2)$ in $\overline{K}^3$, not $Z_{K^3}(x^2, xy, z^2)$ in K^3. If $K = \mathbf{F}_p$ then $Z_{K^3}(x^2, xy, z^2) = \{(0, b, 0) : b \in \mathbf{F}_p\}$, so $y^p - y \in I_K(Z_{K^3}(x^2, xy, z^2))$ but $y^p - y \notin (x, z)$. When we look at zero sets in $\overline{K}^3$, or at least using fields strictly larger than $\mathbf{F}_p$, $y^p - y$ no longer vanishes at all $(0, b, 0)$ since there are more than p choices for b.

Here is a generalization of the ideal–variety correspondence from algebraically closed fields in Theorem 4.20 to all fields.

Theorem A.14. *The mappings $V \rightsquigarrow I_K(V)$ and $J \rightsquigarrow Z_{C^n}(J)$ between K-varieties in C^n and radical ideals J in $K[x_1, \ldots, x_n]$ are inclusion-reversing bijections that are inverses: $Z_{C^n}(I_K(V)) = V$ and $I_K(Z_{C^n}(J)) = J$.*

Proof. The mappings $V \rightsquigarrow I_K(V)$ and $J \rightsquigarrow Z_{C^n}(J)$ both make sense and it's easy to see

$$V \subset V' \Longrightarrow I_K(V') \subset I_K(V), \quad J \subset J' \Longrightarrow Z_{C^n}(J') \subset Z_{C^n}(J).$$

We have already seen that these mappings are inverses of each other: that $Z_{C^n}(I_K(V)) = V$ for all K-varieties V in C^n is Theorem A.4, and that $I_K(Z_{C^n}(J)) = J$ for radical ideals J in $K[x_1, \ldots, x_n]$ is immediate from the Nullstellensatz over K in Theorem A.11. □

We conclude with an application of the weak Nullstellensatz over $\mathbf{Q}$ to comparing irreducibility of polynomials over $\overline{\mathbf{Q}}$ and $\overline{\mathbf{F}}_p$. Polynomials in $\mathbf{Z}[x]$ that are irreducible in $\mathbf{Q}[x]$ need not be irreducible mod p for some p: $x^4 + 1$ is irreducible in $\mathbf{Q}[x]$ but it is reducible mod p for every p. However, if we compare irreducibility of a polynomial in $\mathbf{Z}[x_1, \ldots, x_n]$ over the algebraic closures $\overline{\mathbf{Q}}$ and $\overline{\mathbf{F}}_p$ then there is a connection by the following theorem of Noether [5].

Theorem A.15. *For nonconstant $f \in \mathbf{Z}[x_1, \ldots, x_n]$ of degree d, the following conditions are equivalent:*

(1) *f is irreducible in $\overline{\mathbf{Q}}[x_1, \ldots, x_n]$,*
(2) *for all but finitely many p, f mod p is irreducible in $\overline{\mathbf{F}}_p[x_1, \ldots, x_n]$ of degree d.*

When $n = 1$ this is a boring theorem, since irreducibility of single-variable polynomials over an algebraically closed field means the polynomial is linear.

Example A.16. Let $f(x, y) = x^2 + y^2 - 7$. This is irreducible in $\overline{\mathbf{Q}}[x, y]$ since in $\overline{\mathbf{Q}}[y][x]$ it is Eisenstein at $y - \sqrt{7}$. For the same reason, $f(x)$ mod p is irreducible in $\overline{\mathbf{F}}_p[x, y]$ when $p \neq 2, 7$. It is reducible in $\overline{\mathbf{F}}_2[x, y]$, where $f(x, y) = x^2 + y^2 + 1 = (x + y + 1)^2$, and in $\overline{\mathbf{F}}_7[x, y]$, where $f(x, y) = x^2 + y^2 = (x + iy)(x - iy)$ when $i^2 = -1$ in characteristic 7.

A few years before Noether proved Theorem A.15, Ostrowski [6] proved condition (1) implies that for all but finitely many p, f mod p is irreducible over $\mathbf{F}_p$ (not $\overline{\mathbf{F}}_p$).

Proof. The argument is based on considering "generic" factorizations of a polynomial into lower-degree polynomials. This will let us interpret the reducibility of a multivariable polynomial over a field F as the existence of a common zero in F to a certain system of multivariable polynomials.

When a prime p does not divide some nonzero coefficient of f, f mod p has the same degree as f, so $\deg(f \bmod p) = \deg f$ for all but finitely many p. Therefore the theorem is obvious if $d = 1$, since (i) all polynomials (in any number of indeterminates) of degree 1 over a field are irreducible and (ii) $\deg(f \bmod p) = \deg f$ for all but finitely many p. We may now suppose $d \geq 2$.

For a field F, a polynomial of degree d in $F[\mathbf{x}] := F[x_1, \ldots, x_n]$ is reducible when it is a product of two polynomials in $F[\mathbf{x}]$ with degree less than d. Let's look at a "universal" product of polynomials in n indeterminates of degree j and $d - j$, where $1 \leq j \leq d - 1$.[10] For an n-tuple of nonnegative integers $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_n)$, let $M_{\boldsymbol{\alpha}}(\mathbf{x}) = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ be the monomial with exponents from $\boldsymbol{\alpha}$ and let $|\boldsymbol{\alpha}| = \alpha_1 + \cdots + \alpha_n$ be the degree of $M_{\boldsymbol{\alpha}}(\mathbf{x})$. A pair of "generic polynomials" of degree j and $d - j$ in n indeterminates $x_1, \ldots, x_n$ is

$$g_j(\mathbf{u}, \mathbf{x}) = \sum_{|\boldsymbol{\alpha}| \leq j} u_{\boldsymbol{\alpha}} M_{\boldsymbol{\alpha}}(\mathbf{x}), \quad h_{d-j}(\mathbf{v}, \mathbf{x}) = \sum_{|\boldsymbol{\beta}| \leq d-j} v_{\boldsymbol{\beta}} M_{\boldsymbol{\beta}}(\mathbf{x}),$$

[10] We only need to consider $1 \leq j \leq d/2$.

where the coefficients $\{u_{\boldsymbol{\alpha}}, v_{\boldsymbol{\beta}} : |\boldsymbol{\alpha}| \leq j, |\boldsymbol{\beta}| \leq d-j\}$ are algebraically independent over $\mathbf{Q}$.[11] The product of these two polynomials involves monomials of degree up to d with coefficients in $\mathbf{Z}[\mathbf{u},\mathbf{v}] := \mathbf{Z}[\{u_{\boldsymbol{\alpha}}, v_{\boldsymbol{\beta}} : |\boldsymbol{\alpha}| \leq j, |\boldsymbol{\beta}| \leq d-j\}]$:

$$g_j(\mathbf{u},\mathbf{x})h_{d-j}(\mathbf{v},\mathbf{x}) = \sum_{|\boldsymbol{\gamma}|\leq d} w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v})M_{\boldsymbol{\gamma}}(\mathbf{x}), \tag{A.2}$$

where $w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) \in \mathbf{Z}[\mathbf{u},\mathbf{v}]$.

The coefficients $w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v})$ on the right side of (A.2) are polynomials in the indeterminate coefficients $u_{\boldsymbol{\alpha}}$ and $v_{\boldsymbol{\beta}}$ of the factors on the left side. For $f(\mathbf{x}) = \sum_{|\boldsymbol{\gamma}|\leq d} c_{\boldsymbol{\gamma}} M_{\boldsymbol{\gamma}}(\mathbf{x})$ in $R[\mathbf{x}]$, $f(\mathbf{x})$ is a product of polynomials of degree at most j and $d-j$ in $R[\mathbf{x}]$ if and only if the right side of (A.2) equals $f(\mathbf{x})$ for some $u_{\boldsymbol{\alpha}}$'s and $v_{\boldsymbol{\beta}}$'s in R. So when R is an integral domain,

> $f(\mathbf{x})$ is a product of polynomials of degree j and $d-j$ in $R[\mathbf{x}]$ if and only if all $w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) - c_{\boldsymbol{\gamma}}$ in $\mathbf{Z}[\mathbf{u},\mathbf{v}]$ for $|\boldsymbol{\gamma}| \leq d$ have a common zero with $u_{\boldsymbol{\alpha}}$ and $v_{\boldsymbol{\beta}}$ in R.

Strictly speaking, specializing the $u_{\boldsymbol{\alpha}}$'s and $v_{\boldsymbol{\beta}}$'s to elements of R makes $g_j(\mathbf{u},\mathbf{x})$ and $h_{d-j}(\mathbf{v},\mathbf{x})$ have degree *at most* j and $d-j$ in $R[\mathbf{x}]$, but when $\deg f = d$ and R is an integral domain, a decomposition of $f(\mathbf{x})$ into factors of degree at most j and $d-j$ in $R[\mathbf{x}]$ must use factors of degree j and $d-j$.

With this description of reducibility, we can prove the equivalence of (1) and (2) using $R = \overline{\mathbf{Q}}$ and $R = \overline{\mathbf{F}}_p$.

(1) $\Rightarrow$ (2). Write $f(\mathbf{x}) = \sum_{|\boldsymbol{\gamma}|\leq d} c_{\boldsymbol{\gamma}} M_{\boldsymbol{\gamma}}(\mathbf{x})$ where $c_{\boldsymbol{\gamma}} \in \mathbf{Z}$. From the discussion above, $f(\mathbf{x})$ is a product of polynomials of degree j and $d-j$ over $\overline{\mathbf{Q}}$ if and only if the system of polynomials $\{w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) - c_{\boldsymbol{\gamma}} : |\boldsymbol{\gamma}| \leq d\}$ in $\mathbf{Z}[\mathbf{u},\mathbf{v}]$ has a common zero where each $u_{\boldsymbol{\alpha}}$ and $v_{\boldsymbol{\beta}}$ is in $\overline{\mathbf{Q}}$.

Since f is irreducible over $\overline{\mathbf{Q}}$, for each j from 1 to $d-1$ there is no decomposition of f into factors of degree j and $d-j$ over $\overline{\mathbf{Q}}$, so the system of polynomials $\{w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) - c_{\boldsymbol{\gamma}} : |\boldsymbol{\gamma}| \leq d\}$ for each j has *no* common zero with coordinates in $\overline{\mathbf{Q}}$. These polynomials have rational coefficients, so the weak Nullstellensatz over $\mathbf{Q}$ (not the weak Nullstellensatz over $\overline{\mathbf{Q}}$) tells us that the ideal generated by these polynomials in $\mathbf{Q}[\mathbf{u},\mathbf{v}]$ contains 1: we can write

$$1 = \sum_{|\boldsymbol{\gamma}|\leq d} q_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v})(w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) - c_{\boldsymbol{\gamma}}) \tag{A.3}$$

for some $q_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) \in \mathbf{Q}[\mathbf{u},\mathbf{v}]$.

To show $f(\mathbf{x})$ mod p is irreducible in $\overline{\mathbf{F}}_p[\mathbf{x}]$ for all but finitely many p, we want to reduce (A.3) mod p. The polynomials $w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) - c_{\boldsymbol{\gamma}}$ have $\mathbf{Z}$-coefficients but $q_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v})$ has $\mathbf{Q}$-coefficients, so let's clear out a common denominator b_j in $\mathbf{Z}^+$: $q_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) = Q_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v})/b_j$, where $Q_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) \in \mathbf{Z}[\mathbf{u},\mathbf{v}]$. Multiplying both sides of (A.3) by b_j,

$$b_j = \sum_{|\boldsymbol{\gamma}|\leq d} Q_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v})(w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) - c_{\boldsymbol{\gamma}}). \tag{A.4}$$

All coefficients here are integers, so we can reduce (A.4) mod p. We will use p not dividing the nonzero coefficients of $f(\mathbf{x})$, so $f(\mathbf{x})$ mod p has degree d.

If $f(\mathbf{x})$ mod p is reducible in $\overline{\mathbf{F}}_p[\mathbf{x}]$ then for some j in $\{1,\ldots,d-1\}$ it is a product of polynomials of degree j and $d-j$ in $\overline{\mathbf{F}}_p[\mathbf{x}]$, which implies the polynomials $w_{\boldsymbol{\gamma},j}(\mathbf{u},\mathbf{v}) - c_{\boldsymbol{\gamma}}$ over all $\boldsymbol{\gamma}$ with $|\boldsymbol{\gamma}| \leq d$ have a common zero $\{u_{\boldsymbol{\alpha}}, v_{\boldsymbol{\beta}}\}$ where all the coordinates are in $\overline{\mathbf{F}}_p$. Substituting these values for $u_{\boldsymbol{\alpha}}$ and $v_{\boldsymbol{\beta}}$ into the right side of (A.4) reduced mod p makes each term in the sum on the right vanish in $\overline{\mathbf{F}}_p$, so $b_j = 0$ in $\overline{\mathbf{F}}_p$. Thus $p \mid b_j$. So when p does not divide the nonzero coefficients of $f(\mathbf{x})$ and all of $b_1,\ldots,b_{d-1}$, $f(\mathbf{x})$ mod p has

[11] The exact number of n-tuples $\boldsymbol{\alpha}$ with $|\boldsymbol{\alpha}| = k$ is $\binom{k+n-1}{n-1}$.

degree d and has no factorization over $\overline{\mathbf{F}}_p$ into two smaller-degree polynomials. Therefore $f(\mathbf{x}) \bmod p$ is irreducible of degree d over $\overline{\mathbf{F}}_p$ for all but finitely many primes p.

(2) $\Rightarrow$ (1). We will prove the contrapositive: if f is reducible in $\overline{\mathbf{Q}}[\mathbf{x}]$ then $f(\mathbf{x}) \bmod p$ is reducible in $\overline{\mathbf{F}}_p[\mathbf{x}]$ for all but finitely many primes p. (Strictly speaking, the negation of (2) is the apparently weaker condition that $f(x) \bmod p$ is reducible in $\overline{\mathbf{F}}_p[\mathbf{x}]$ for infinitely many p.) Let $f(\mathbf{x}) = g(\mathbf{x})h(\mathbf{x})$ in $\overline{\mathbf{Q}}[\mathbf{x}]$ where $\deg g, \deg h < d$. We want to show this factorization can be reduced mod p for all but finitely many p.

Let $\{c_k\}$ be the set of all nonzero coefficients of $g(\mathbf{x})$ and $h(\mathbf{x})$. Each c_k is in $\overline{\mathbf{Q}}$ and therefore is the root of a monic polynomial $m_k(x)$ in $\mathbf{Q}[x]$. Intuitively, we should be able to make sense of c_k in $\overline{\mathbf{F}}_p$ as long as p doesn't divide a denominator of a coefficient of $m_k(x)$. We will use that idea to put the finitely many numbers c_k into a finitely generated $\mathbf{Z}$-algebra in which each c_k is a unit.

Let N be a positive integer that is divisible by

(i) all the denominators of the (rational) coefficients of all $m_k(x)$,
(ii) the numerators of the (nonzero!) constant terms of all $m_k(x)$.

Let R be the $\mathbf{Z}$-algebra generated by $1/N$ and all the nonzero coefficients c_k of $g(\mathbf{x})$ and $h(\mathbf{x})$, so $g(\mathbf{x})$ and $h(\mathbf{x})$ are in $R[\mathbf{x}]$. By (i), each $m_k(x)$ is monic in $\mathbf{Z}[1/N][x]$, so each c_k is *integral* over $\mathbf{Z}[1/N]$. Since$R$ is generated by the c_k's as a $\mathbf{Z}[1/N]$-algebra, integrality of the c_k's over $\mathbf{Z}[1/N]$ makes all elements of R integral over $\mathbf{Z}[1/N]$ (Corollary 2.10) and R is a finitely generated $\mathbf{Z}[1/N]$-module. By (ii), the constant term of each $m_k(x)$ is a unit in $\mathbf{Z}[1/N]$ and that makes each c_k a unit in R: the proof of Theorem 2.7 shows that when B/A is an integral ring extension and $b \in B$ is the root of a monic polynomial in $A[x]$ with constant term in $A^\times$, b is in $B^\times$. Use that with $A = \mathbf{Z}[1/N]$ and $B = R$.

From the factorization $f(\mathbf{x}) = g(\mathbf{x})h(\mathbf{x})$ in $R[\mathbf{x}]$ we will show $f(\mathbf{x}) \bmod p$ is reducible in $\overline{\mathbf{F}}_p[\mathbf{x}]$ for each prime p where $p \nmid N$.

When $p \nmid N$, $p \notin R^\times$: if $p \in R^\times$ then $1/p$ would be integral over $\mathbf{Z}[1/N]$, so $1/p \in \mathbf{Z}[1/N]$ (see the end of Example 2.4) and that's false since $p \nmid N$. Therefore R has a maximal ideal $\mathfrak{m}$ containing p (use for $\mathfrak{m}$ a maximal ideal of R containing the proper ideal pR). The field $R/\mathfrak{m}$ is finite by Corollary 5.2 and it has characteristic p since $p \in \mathfrak{m}$. Reducing the equation $f(\mathbf{x}) = g(\mathbf{x})h(\mathbf{x})$ in $R[\mathbf{x}]$ modulo $\mathfrak{m}$, $\overline{f}(\mathbf{x}) = \overline{g}(\mathbf{x})\overline{h}(\mathbf{x})$ in $(R/\mathfrak{m})[\mathbf{x}] \subset \overline{\mathbf{F}}_p[\mathbf{x}]$, so $f(x) \bmod p$ is reducible over $\overline{\mathbf{F}}_p$ as long as $\overline{g}(\mathbf{x})$ and $\overline{h}(\mathbf{x})$ are not constant in $(R/\mathfrak{m})[\mathbf{x}]$, and they are nonconstant mod $\mathfrak{m}$ since their nonzero coefficients in R are in $R^\times$ and thus the nonzero coefficients don't vanish mod $\mathfrak{m}$ no matter what maximal ideal $\mathfrak{m}$ is used in R. □

Corollary A.17. *For nonconstant $f \in \mathbf{Z}[x_1, \ldots, x_n]$, if $f \bmod p$ is irreducible over $\overline{\mathbf{F}}_p$ for infinitely many p then $f \bmod p$ is irreducible over $\overline{\mathbf{F}}_p$ for all but finitely many p.*

This is analogous to the fact that if F is an infinite field (like $\overline{\mathbf{F}}_p$) and $f(x) \in F[x]$ has $f(a) = 0$ for infinitely many $a \in F$ then $f(a) = 0$ for all $a \in F$ since a nonzero polynomial in $F[x]$ has only finitely many roots in F.

Proof. We will prove the contrapositive. If it's not true that $f \bmod p$ is irreducible over $\overline{\mathbf{F}}_p$ for all but finitely many p then $f(x_1, \ldots, x_n)$ is reducible over $\overline{\mathbf{Q}}$ by the contrapositive of (1) $\Rightarrow$ (2) in Theorem A.15. (Concerning the degree condition in (2), $\deg(f \bmod p) = \deg f$ for all but for all but finitely many p since only finitely many primes divide the nonzero coefficients of f.) Then $f \bmod p$ is reducible over $\overline{\mathbf{F}}_p$ for all but finitely many p by the method of proof of (2) $\Rightarrow$ (1) in Theorem A.15, so $f \bmod p$ can be irreducible over $\overline{\mathbf{F}}_p$ for only finitely many p. □

Remark A.18. It is very important in Corollary A.17 that the irreducibility is over the algebraic closure $\overline{\mathbf{F}}_p$. The result is completely false over the finite field $\mathbf{F}_p$. For instance,

$x^2 + 1 \mod p$ is irreducible in $\mathbf{F}_p[x]$ if $p \equiv 3 \bmod 4$ and reducible in $\mathbf{F}_p[x]$ if $p \not\equiv 3 \bmod 4$, and there are infinitely many primes of both types.

How large does p have to be so that $f \bmod p$ in Theorem A.15 is guaranteed to be absolutely irreducible over $\overline{\mathbf{F}}_p$ of degree d? A lower bound in [8, Corollary 2B, p. 193] is

$$p > (4||f||)^{k^{2^k}} \tag{A.5}$$

where $||f||$ is the sum of the absolute values of the coefficients of f and $k = \binom{n+d-1}{n}$. A smaller lower bound is given in [7] for polynomials in two indeterminates:

$$p > (a(b+1)b^2 + (a+1)(b-1)a^2)^{ab+(b-1)/2}H(f)^{2ab+b-1}, \tag{A.6}$$

where $H(f)$ is the maximum absolute value of the coefficients of f, a is the x-degree of f, and b is the y-degree of f.

Example A.19. The following example is taken from the start of [7]. Let

$$f(x,y) = x^9y - 9x^9 - 2x + 9y + 2.$$

This is irreducible in $\overline{\mathbf{Q}}[x,y]$ by looking at in $\overline{\mathbf{Q}}[x][y]$: $f(x,y) = (x^9+9)y + (-9x^9 - 2x + 2)$ is linear in y, so it is irreducible over $\overline{\mathbf{Q}}(x)$, and it remains irreducible in $\overline{\mathbf{Q}}[x][y]$ because its coefficients in $\overline{\mathbf{Q}}[x]$ are relatively prime (the coefficients have no common root). This is a special case of irreducibility of nonconstant polynomials in $R[y]$ when R is a UFD: it is necessary and sufficient that the polynomial is irreducible over the fraction field of R and be primitive (coefficients have gcd 1).

To apply (A.5) and (A.6) for a lower bound on p making $f(x,y) \bmod p$ irreducible over $\overline{\mathbf{F}}_p$, note $||f|| = 23$, $k = \binom{2+10-1}{2} = 55$, $H(f) = 9$, $a = 9$, and $b = 1$. Then (A.5) gives the shockingly large lower bound $92^{55^{2^{55}}}$ and (A.6) gives the lower bound $18^9 \cdot 9^{18}$, which is a 29-digit number. You may think the second lower bound is also absurdly large, but $f(x,y) \bmod p$ is reducible over $\overline{\mathbf{F}}_p$ for a much larger p than you might expect: the coefficients $x^9 + 9$ and $-9x^9 - 2x + 2$ have a common root $93470127633772547 \bmod p$ where p is the 18-digit prime 186940255267545011, so $f(93470127633772547, y) = 0$ in $\mathbf{F}_p[y]$. Therefore in $\overline{\mathbf{F}}_p[x,y]$, $f(x,y) \bmod p$ is reducible with factor $x - 93470127633772547$.

In [5], Noether showed that for a field F, irreducibility in $\overline{F}[\mathbf{x}]$ of polynomials of degree $d \geq 2$ is a "coefficient property": there is a set of multivariable polynomials $G_{\boldsymbol{\gamma}}(\mathbf{y})$, depending only on d, such that $f(\mathbf{x})$ in $\overline{F}[\mathbf{x}]$ is irreducible of degree d if and only if the polynomials $G_{\boldsymbol{\gamma}}(\mathbf{y})$ don't all vanish when the coefficients of $f(\mathbf{x})$ are substituted into the variables of all $G_{\boldsymbol{\gamma}}(\mathbf{y})$. (A simple analogue of this is $ax^2 + bx + c$ over a field being a separable quadratic if and only if $a \neq 0$ and $b^2 - 4ac \neq 0$.) This is different from how we worked with irreducibility over $\overline{F}$ in the proof of Theorem A.15, where we expressed it in terms of certain multivariable polynomials *depending on* $f(\mathbf{x})$ not vanishing at all points $(\mathbf{u}, \mathbf{v})$ with coordinates $u_{\boldsymbol{\alpha}}$ and $v_{\boldsymbol{\beta}}$ in $\overline{F}$.

The polynomials $G_{\boldsymbol{\gamma}}(\mathbf{y})$ arise from treating nonzero polynomials in $\overline{F}[\mathbf{x}]$ of degree at most d as points in a projective space using coefficients as coordinates, *e.g.*, $ax^2 + bx + c$ becomes $[a : b : c]$ in the projective plane. (This is sensible because reducibility of a polynomial over a field is unaffected by scaling the coefficients by a common nonzero factor.) For $1 \leq j \leq d-1$, let $P_{j,n}$ be the projective space of coefficients of nonzero polynomials in n indeterminates over $\overline{F}$ of degree at most j and let $\mu_j \colon P_{j,n} \times P_{d-j,n} \to P_{d,n}$ be multiplication of such polynomials (degree at most j times degree at most $d-j$ has degree at most d). Projective spaces can be given the Zariski topology (closed sets are zero sets of homogeneous polynomials) and the image of each μ_j turns out to be a Zariski closed subset of $P_{d,n}$ because projective spaces in algebraic geometry are proper (analogous to projective spaces over $\mathbf{R}$

and $\mathbf{C}$ being compact and Hausdorff in their classical topology), so the polynomials in $\overline{F}[\mathbf{x}]$ that are reducible of degree d or have degree less than d form the Zariski closed set $\bigcup_{1\leq j\leq d-1}\mu_j(P_{j,n}\times P_{d-j,n})$ in $P_{d,n}$. A Zariski closed set is defined by the vanishing of a finite set of polynomials, and that is what the polynomials $G_{\boldsymbol{\gamma}}(\mathbf{y})$ are.

Interpreting nonzero polynomials of degree at most d as a projective space with coefficients being coordinates, and reducible polynomials of degree d plus polynomials of degree less than d as a union of images of multiplication maps $\bigcup_{1\leq j\leq d-1}\mu_j(P_{j,n}\times P_{d-j,n})$, can be applied to real polynomials in one variable and leads to a proof of the Fundamental Theorem of Algebra purely in terms of $\mathbf{R}$, making no use of complex numbers. See Section 3 of https://kconrad.math.uconn.edu/blurbs/fundthmalg/propermaps.pdf.

References

[1] A. Azarang, *A simple proof of Zariski's lemma*, Bull. Iranian Math. Soc. **43** (2017), 1529–1530. Online at https://arxiv.org/abs/1506.08376.

[2] W. Fulton, "Algebraic Curves," Addison-Wesley, New York, 1989. Online at http://www.math.lsa.umich.edu/∼wfulton/CurveBook.pdf.

[3] J. Gray, *Algebraic geometry between Noether and Noether – a forgotten chapter in the history of algebraic geometry*, Revue d'histoire des mathématiques **3** (1997), 1–48. Online at http://www.numdam.org/article/RHM_1997__3_1_1_0.pdf.

[4] D. Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–373. Online at https://eudml.org/doc/157652.

[5] E. Noether, *Ein algebraisches Kriterium für absolute Irreduzibilität*, Math. Ann. **85** (1922), 26–33. Online at https://eudml.org/doc/158900.

[6] A. Ostrowski, *Zur arithmetischen Theorie der algebraischen Grössen*, Nachr. Ges. Wiss. Göttingen, Math.-Phys. Klasse (1919), 279–298. Online at https://eudml.org/doc/59056.

[7] W. M. Ruppert, *Reducibility of polynomials $f(x,y)$ modulo p*, J. Number Theory **77** (1999), 62–70. Online at https://arxiv.org/abs/math/9808021v1.

[8] W. M. Schmidt, "Equations over Finite Fields: an Elementary Approach," Lecture Notes in Mathematics 536, Springer-Verlag, Berlin, 1976.

[9] O. Zariski, *The compactness of the Riemann manifold of an abstract field of algebraic functions*, Bull. Amer. Math. Soc. **50** (1944), 683–691. Online at https://www.ams.org/journals/bull/1944-50-10/S0002-9904-1944-08206-2/S0002-9904-1944-08206-2.pdf.

[10] O. Zariski, *A new proof of Hilbert's Nullstellensatz*, Bull. Amer. Math. Soc. **53** (1947), 362–368. Online at https://www.ams.org/journals/bull/1947-53-04/S0002-9904-1947-08801-7/S0002-9904-1947-08801-7.pdf.