SFU Math 441 Commutative Algebra and Algebraic Geometry
Lecturer: Katrina Honigs
Written by: Grayson Davis

MT Notes (Part 1)

February 27, 2024 8:02 PM

All rings are commutative with unity.

Rings and Ideals

Def'n: An integral domain (or domain) is a ring with no zero divisors.

A domain R equipped with a size function $\sigma: R\setminus\{0\} \longrightarrow \mathbb{Z}_{\geq 0}$ is called a Euclidean domain if for every $a, b \in R$ there are $q, r \in R$ such that $b = aq + r$ and $r = 0$ or $\sigma(r) < \sigma(a)$.

Def'n: Let R be a ring. A subset $I \subseteq R$ is an ideal if:

- $0 \in I$;
- $a - b \in I$ whenever $a, b \in I$;
- $ar \in I$ whenever $a \in I, r \in R$.

Remark: If $a_1, \dots, a_n \in R$, then $(a_1, \dots, a_n) := \{r_1a_1 + \dots + r_na_n \mid (r_1, \dots, r_n) \in R^n\}$ is an ideal. We call $(a_1, \dots, a_n)$ the ideal generated by $\{a_1, \dots, a_n\}$.

More generally, if $S \subseteq R$ is a set, $(S) = \{r_1s_1 + \dots + r_ns_n \mid r_i \in R, n \in \mathbb{N}\}$ is an ideal.

Def'n: A principal ideal is an ideal that can be generated by a single element.

We call a domain a principal ideal domain (PID) if all its ideals are principal.

Theorem: Any Euclidean domain is a PID.

Proof: Let R be a Euclidean domain with size function σ.

Let $I \subseteq R$ be an ideal. Assume $I \neq (0)$.

Choose $a \in I$ such that $\sigma(a) \leq \sigma(b)$ for all $b \in I$.

We claim that $I = (a)$. The reverse inclusion is immediate.

Let $b \in I$. Then $b = qa + r$ for some $q, r \in R$, $r = 0$ or $\sigma(r) < \sigma(a)$.

But $\sigma(a)$ is minimal, so $r = 0$. Hence $b \in (a)$. $\square$

Def'n: Let R be an integral domain.

(a) $a, b \in R$ are associates if there is a unit $u \in R$ such that $a = ub$.

Def'n. Let R be an integral domain.

(a) $a, b \in R$ are associates if there is a unit $u \in R$ such that $a = ub$.

(b) $a \in R$ is irreducible if a is not a unit and $a = bc$ for some $b, c \in R$

implies b or c is a unit.

(c) $a \in R$ is prime if $a = bc$ implies $a \mid b$ or $a \mid c$.

(d) A proper ideal $P \subseteq R$ is prime if $ab \in P$ implies $a \in P$ or $b \in P$.

(e) A proper ideal $M \subseteq R$ is maximal if for any ideal $M \subseteq I \subseteq R$, then $I = M$ or $I = R$.

Proposition: Let R be a domain and $I \subseteq R$ an ideal.

(a) I is prime if and only if R/I is a domain.

(b) I is maximal if and only if R/I is a field.

Proof:

(a) Suppose I is prime.

Suppose $ab = 0$ for some $a, b \in R/I$. Then $a \in I$ or $b \in I$.

Hence, R/I is a domain. The converse is similar.

(b) Suppose I is maximal. We have that R/I is a field if and only if its only

non-zero ideal is R/I. Let $\tilde{J} \subseteq R/I$ be an ideal. Then we can lift

$\tilde{J}$ to an ideal $J \subseteq R$ containing I. If I is maximal, then $J = I$ or $J = R$.

If R/I is a field, then we can start with J to get $\tilde{J} = (0) = I$ or $\tilde{J} = R/I$.

Hence I is maximal. $\square$

Corollary: Any maximal ideal is prime.

Def'n: Let R be a ring. The spectrum of R is $\mathrm{Spec}(R) = \{P \subseteq R \mid P \text{ is prime}\}$.

The underlying set forms a topology, which we call the Zariski topology.

Multivariate Polynomials

Let k be a field.

Def'n: A monomial $x^\alpha \in k[x_1, \dots, x_n]$ is a polynomial of the form

Def'n: A monomial $x^\alpha \in k[x_1,\dots,x_n]$ is a polynomial of the form

$x_1^{\alpha_1}\cdots x_n^{\alpha_n}$ for some $\alpha = (\alpha_1,\dots,\alpha_n) \in \mathbb{Z}_{\geq 0}$.

The total degree of x^α is $|\alpha| = \alpha_1 + \dots + \alpha_n$.

The degree of a polynomial $p(x) = \sum_{i=1}^{m} x^{\alpha_i}$ is $\deg(p) = \max_{i=1\dots m}(|\alpha_i|)$.

Def'n: A monomial ordering on $k[x_1,\dots,x_n]$ is a total ordering of monomials so that

(a) $<$ is well-ordered;

(b) if $x^\alpha < x^\beta$, then $x^\alpha x^\gamma < x^\beta x^\gamma$ for all $\gamma \in \mathbb{Z}_{\geq 0}$.

Examples:

(1) Lexicographic Ordering: $x^\alpha <_{Lex} x^\beta$ if and only if the first non-zero entry of $\beta - \alpha$ is positive.

(2) Graded Lexicographic Ordering: $x^\alpha <_{GrLex} x^\beta$ if and only if $|\alpha| < |\beta|$ or $|\alpha| = |\beta|$ and $x^\alpha <_{Lex} x^\beta$.

(3) Reverse Graded Lex.: $x^\alpha < x^\beta$ if and only if $|\alpha| < |\beta|$ or $|\alpha| = |\beta|$ and the rightmost non-zero entry of $\beta - \alpha$ is positive.

Def'n: Let $p \in k[x_1,\dots,x_n]$ and fix a monomial order $<$.

The multidegree of p is $\mathrm{mdeg}(p)$, the largest exponent of the monomials in p.

Define the leading monomial of p, $LM(p)$, as the corresponding monomial.

If $c \in k$ is the coefficient of this monomial, the leading term of p is $LT(p) = c\,LM(p)$.

Gröbner Bases and the Division Algorithm

The division algorithm for multivariate polynomials is dividing the leading monomials and subtracting: let $f, g \in k[x_1,\dots,x_n]$. Set $g_0 = g$, and $g_n = g_{n-1} - \frac{LT(g)}{LT(f)} f$.

Def'n: A monomial ideal is an ideal generated by monomials

Given an ideal $I \subseteq k[x_1,\dots,x_n]$, the leading term ideal of I is $LT(I) := (x^\alpha \mid x^\alpha = LM(f) \text{ for some } f \in I)$.

We say that $f_1,\dots,f_r$ is a Gröbner basis of I if $LT(I) = (LT(f_1),\dots,LT(f_r))$.

Key Lemma: Let $I = (x^\alpha)_{\alpha\in\Gamma}$ be a monomial ideal. If $x^\beta \in (x^\alpha)_{\alpha\in\Gamma}$, then $x^\alpha \mid x^\beta$ for some $\alpha \in \Gamma$.

Key Lemma: Let $I = (x^\alpha)_{\alpha \in \Gamma}$ be a monomial ideal. If $x^\beta \in (x^\alpha)_{\alpha \in \Gamma}$, then $x^\alpha \mid x^\beta$ for some $\alpha \in \Gamma$.

Proof: Write $x^\beta = \sum_{i=1}^{N} x^{\alpha_i} p_i$ for some $\alpha_i \in \mathbb{Z}^n_{\geq 0}$, $p_i \in k[x_1, \dots, x_n]$.

Then x^β occurs in some $x^{\alpha_i} p_i$, so $x^{\alpha_i} \mid x^\beta$. $\square$

Proposition: Let $<$ be a monomial order and $I \subseteq k[x_1, \dots, x_n]$ an ideal.

Suppose $f_1, \dots, f_r$ is a Gröbner basis of I. If $LT(g)$ is not divisible by $LT(f_1), \dots, LT(f_r)$,

then $LT(g) \notin LT(I)$.

Proof: If $LT(g) \in LT(I)$, then by the key lemma $LT(f_i) \mid LT(g)$ for some $i = 1, \dots, r$. $\square$

Remark: This proposition implies $g \notin I$.

Lemma: Let $I \subseteq k[x_1, \dots, x_n]$ be an ideal. If $x^\beta \in LT(I)$, then there is $f \in I$

such that $x^\beta = LM(f)$.

Proof: By the key lemma, $x^\beta \in LT(I)$ gives the existence of $x^\alpha \in \{x^\alpha \mid \exists g \in I, x^\alpha = LM(g)\}$

such that $x^\beta = x^\alpha x^\gamma$ for some $\gamma \in \mathbb{Z}^n_{\geq 0}$. Then $x^\beta = LM(x^\gamma g)$. $\square$

Theorem: Let $f_1, \dots, f_r \in k[x_1, \dots, x_n]$ and fix a monomial order $<$. Suppose $I \subseteq k[x_1, \dots, x_n]$ is an ideal.

Then $f_1, \dots, f_r$ is a Gröbner basis for I if and only if for all $g \in I$, dividing g by $f_1, \dots, f_r$ returns zero.

Proof: "$\Rightarrow$" Suppose $g \in I$ does not return 0 when divided by $f_1, \dots, f_r$.

Let $r \in k[x_1, \dots, x_n]$ be the remainder. Then $r \in I$ by the division algorithm, but $LT(r)$

is not divisible by each $LT(f_i)$. By the proposition, $r \notin I$, a contradiction.

"$\Leftarrow$" Suppose instead $f_1, \dots, f_r$ is not a Gröbner basis of I.

Then we may choose $g \in LT(I) \setminus (LT(f_1), \dots, LT(f_r))$ a monomial. By the lemma, there is $h \in I$

so that $g = LT(h)$. By assumption, dividing h by $f_1, \dots, f_r$ gives 0 remainder, a contradiction. $\square$

MT Notes (Part 2)

March 2, 2024 12:53 PM

Normal Forms: Uniqueness of the Remainder

Theorem: Let $I \subseteq k[x_1,\dots,x_n]$ be an ideal and fix a monomial ordering $<$.

Suppose I has a Gröbner basis. Then for every $g \in k[x_1,\dots,x_n]$ there is

a unique finite sum $\sum_{i=1}^{N} c_i x^{\alpha_i}$, where $c_i \in k$, $x^{\alpha_i} \notin LT(I)$, such that $g \equiv \sum_{i=1}^{N} c_i x^{\alpha_i} \pmod I$.

This finite sum is called the normal form of g.

Proof:

Existence: Suppose $g \in I$ has no normal form. Then the set $S = \{LM(h) \mid h \text{ has no normal form}\}$

is non-empty. Choose $x^\beta = LM(h) \in S$ minimal. Either $x^\beta \in LT(I)$ or $x^\beta \notin LT(I)$.

In the first case, we may choose $\tilde{h} \in I$ so that $x^\beta = LT(\tilde{h})$.

Then $\hat{h} = h - \frac{LT(h)}{LT(\tilde{h})}\tilde{h}$ has multidegree strictly less than h and $h \equiv \hat{h} \pmod I$.

The former fact gives that $\hat{h}$ must have a normal form. But then $h \equiv \hat{h} \pmod I$

gives that h has a normal form, a contradiction.

Assume now that $x^\beta \notin LT(I)$. Let $h_* = h - LT(h)$. Then h_* has a normal form.

Let $\sum_{i=1}^{N} c_i x^{\beta_i}$ be a normal form of h_*. Then $LT(h) + \sum_{i=1}^{N} c_i x^{\beta_i}$ is a normal form

of g, a contradiction. Hence, g has a normal form.

Uniqueness: Let $\sum_\alpha c_\alpha x^\alpha, \sum_\alpha d_\alpha x^\alpha$ be normal forms of g.

If some $c_\alpha - d_\alpha \neq 0$, then $x^\alpha \in LT(I)$, which is impossible. $\square$

Noetherian Rings: Existence of a Gröbner basis.

Def'n: A ring R is Noetherian if it satisfies the ascending chain condition (ACC).

Theorem: Let R be a ring. Then R is Noetherian if and only if each ideal

in R is finitely generated.

Proof: "$\Longrightarrow$" Suppose R is Noetherian and let $I \subseteq R$ be an ideal.

Proof: "$\Longrightarrow$" Suppose R is Noetherian and let $I \subseteq R$ be an ideal.

Write $I = (f_\alpha)_{\alpha \in \Gamma}$ for some set of generators. Assume I is not finitely generated. Then given finitely many f_α, say $(f_{\alpha_1}, \ldots, f_{\alpha_n})$, we can find $f_{\alpha_{n+1}}$ so that $(f_{\alpha_1}, \ldots, f_{\alpha_n}) \subsetneq (f_{\alpha_1}, \ldots, f_{\alpha_n}, f_{\alpha_{n+1}})$, as if not, then $I = (f_{\alpha_1}, \ldots, f_{\alpha_n})$.

But R is Noetherian, so this process terminates.

"$\Longleftarrow$" Let $I_1 \subseteq \ldots \subseteq I_n \subseteq \ldots$ be an increasing chain of ideals in R.

Then $I = \bigcup_{i=1}^{\infty} I_i$ is an ideal. Hence $I = (a_1, \ldots, a_k)$ for some $a_i \in R$.

Hence R is Noetherian. $\square$

Theorem (Hilbert's Basis Theorem): If R is Noetherian, then so is $R[x]$.

The proof is omitted.

Proposition: Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal with Gröbner basis $f_1, \ldots, f_r$. Then $I = (f_1, \ldots, f_r)$.

Proof: This is immediate by running the division algorithm on $g \in I$ using $f_1, \ldots, f_r$. $\square$

Theorem (Dickson's Lemma): Every monomial ideal in $k[x_1, \ldots, x_n]$ has a finite set of monomial generators.

The proof is omitted. We immediately get the following corollary:

Corollary: Every ideal $I \subseteq k[x_1, \ldots, x_n]$ has a Gröbner basis.

Proof: By Dickson's Lemma, we can write $I = (x^{\alpha_1}, \ldots, x^{\alpha_k})$.

Lifting these generators to $f_i \in I$ such that $LM(f_i) = x^{\alpha_i}$ completes the proof. $\square$

Buchberger's Criterion

Def'n: The least common multiple of monomials x^α, x^β is $LCM(x^\alpha, x^\beta) = x_1^{\max(\alpha_1, \beta_1)} \cdots x_n^{\max(\alpha_n, \beta_n)}$.

For $f_1, f_2 \in k[x_1, \ldots, x_n]$, we define the S-polynomial of f_1 and f_2 as

$$S(f_1, f_2) = \frac{x^\gamma}{LM(f_1)} f_1 - \frac{x^\gamma}{LM(f_2)} f_2, \text{ where } x^\gamma = LCM(LM(f_1), LM(f_2)).$$

Theorem (Buchberger's Criterion): Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. Write $I = (f_1, \ldots, f_r)$. Then

Theorem (Buchberger's Criterion): Let $I \subseteq k[x_1,\dots,x_n]$ be an ideal. Write $I=(f_1,\dots,f_r)$. Then $f_1,\dots,f_r$ is a Gröbner basis of I if and only if $S(f_i,f_j)$ is divisible by $f_1,\dots,f_r$ with zero remainder.

In particular, we need not check divisibility of all polynomials in I.

We omit the proof.

Buchberger's Algorithm comes from this theorem.

To construct a Gröbner basis, we may repeatedly add S-polynomials of the generators until it forms a Gröbner basis. This procedure terminates since $k[x_1,\dots,x_n]$ is Noetherian.

Spec and Vanishing Sets

Let A be a ring. We noted that $\operatorname{Spec}(A)$ is a topological space.

Def'n: Let X be a non-empty set. We call $\mathcal{T}$ a topology on X if

(1) $\emptyset, X \in \mathcal{T}$,

(2) $\bigcap_{i=1}^{N} A_i \in \mathcal{T} \ \forall A_i \in \mathcal{T},\ N \in \mathbb{N}$,

(3) $\bigcup_{\alpha\in\Gamma} A_\alpha \in \mathcal{T} \ \ \forall \{A_\alpha\}_{\alpha\in\Gamma} \subseteq \mathcal{T}$.

A set in $\mathcal{T}$ is called open.

The complement of an open set is called closed.

The standard topology on $\operatorname{Spec}(A)$ is called the Zariski topology, where closed sets are of the form $V(S)=\{P\in\operatorname{Spec}(A) \mid S\subseteq P\}$ for any set $S\subseteq P$. We call $V(S)$ the vanishing set of S.

Def'n: Any topological space of the form $\operatorname{Spec}(A)$ is called an affine scheme with coordinate ring A. For $A=k[x_1,\dots,x_n]$, we call $\operatorname{Spec}(A)=\mathbb{A}^n_k$ affine n-space.

More generally, if $I\subseteq A$ is an ideal, we call $\operatorname{Spec}(A/I)$ an affine variety.

Remark: Let $f_1,\dots,f_k \in k[x_1,\dots,x_n]$. Then $V(f_1,\dots,f_k)=V(f_1)\cap\dots\cap V(f_k)$.

Proof: Let $P \in V(f_1,\dots,f_k)$. Then $(f_1,\dots,f_k) \subseteq P$. Immediately, $(f_i) \subseteq P$ for all $i=1,\dots,k$.

Conversely, if $P \in V(f_1)\cap\dots\cap V(f_k)$, then $(f_i) \subseteq P$ for each $i=1,\dots,k$.

Then $(f_1,\dots,f_k) \subseteq P$, so $P \in V(f_1,\dots,f_k)$. $\square$

Def'n: Let $m \in Spec(A)$ be maximal. We call A/m the residue field of m.

Remark: Evaluating polynomials in $A = k[x_1,\dots,x_n]$ can be thought of as looking at the image of the polynomial in the coefficient ring.

Theorem: The Zariski topology is a topology, where the vanishings are the closed sets.

Proof: We show three things:

(1) $\emptyset$, $Spec(A)$ are closed: We have $V(A) = \emptyset$, so $\emptyset$ is closed.

Also, $Spec(A) = V(\emptyset)$, so $Spec(A)$ is closed.

(2) $Spec(A)$ is closed under intersections: Let $\{V(S_\alpha)\}_{\alpha\in\Gamma} \subseteq Spec(A)$ be closed.

Then $\bigcap_{\alpha\in\Gamma} V(A_\alpha) = V\left(\bigcup_{\alpha\in\Gamma} A_\alpha\right)$, so $\bigcap_{\alpha\in\Gamma} V(A_\alpha)$ is closed.

(3) $Spec(A)$ is closed under finite unions: Let $V(A_1),\dots,V(A_N) \in Spec(A)$.

Then $\bigcup_{i=1}^{N} V(A_i) = V\left(\bigcap_{i=1}^{N} A_i\right)$. $\square$

Remark: (a) Let $S \subseteq A$ and $I = (S)$. Then $V(S) = V(I)$.

(b) Let $I, J \subseteq A$ be ideals. Then $V(I+J) = V(I) \cap V(J)$.

(c) $V(I) \cup V(J) = V(I\cap J) = V(IJ)$.

Proof: (a) is immediate.

(b) follows from noticing that $I \subseteq I+J \subseteq P$.

(c) We have that $I \cap J \supseteq IJ$, so $V(I\cap J) \subseteq V(IJ)$.

Assume $P \in V(IJ)$ but $P \notin V(I\cap J)$. Then there is $a \in (I\cap J)\setminus P$.

But $a^2 \in P$, so $a \in P$, a contradiction. $\square$

MT Notes (Part 3)

March 2, 2024 9:31 PM

Zariski Closure

Let A be a ring.

Def'n: The closure of a set S in a topological space is $\bar{S}$:

- the smallest closed set containing S.
- the intersection of all closed supersets of it.

Def'n: The Zariski closure of $Z \in \mathrm{Spec}(A)$ is $\bar{Z} = \bigcap_{\substack{Z \subseteq V(J) \\ J \subseteq A \text{ ideal}}} V(J)$.

We have: $Z \subseteq V(J) \iff P \in V(J)$ for all $P \in Z$

$\iff J \subseteq P$ for all $P \in Z$

$\iff J \subseteq \bigcap_{P \in Z} P$.

Thus, $\bar{Z} = \bigcap_{J \subseteq \bigcap_{P\in Z} P} V(J)$. But $\bigcap_{P \in Z} P$ is an ideal, so $V(\bigcap_{P\in Z} P) \subseteq V(J)$.

Hence, $\bar{Z} = V(\bigcap_{P \in Z} P)$.

Def'n: For any $Z \subseteq \mathrm{Spec}(A)$, define $I(Z) = \bigcap_{P \in Z} P$, so that $\bar{Z} = V(I(Z))$.

Vanishings and Affine n-space.

Consider $A = \mathbb{C}[x_1, \dots, x_n]$.

Let $S \subseteq A$. Define $V(S) = \{(a_1, \dots, a_n) \in \mathbb{C}^n \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in S\}$.

We take the following as a fact:

Fact: The maximal ideals of $\mathbb{C}[x_1, \dots, x_n]$ are of the form $(x-a_1, \dots, x_n - a_n)$, $a_i \in \mathbb{C}$.

Then $(a_1, \dots, a_n) \in V(S) \iff f(a_1, \dots, a_n) = 0$ for all $f \in S$

$\iff f \in (x_1 - a_1, \dots, x_n - a_n)$ for all $f \in S$

$\iff (x_1 - a_1, \dots, x_n - a_n) \in V(S)$.

Hence, we get a one-to-one correspondence between points in $\mathbb{C}^n$ and

Hence, we get a one-to-one correspondence between points in $\mathbb{C}^n$ and maximal ideals in $\mathbb{C}[x_1,\dots,x_n]$.

In this context, $I(E) = \{f \in \mathbb{C}[x_1,\dots,x_n] \mid f \in m_s$ for each maximal ideal corresponding to a point $s \in E\}$, where $E \subseteq \mathbb{C}^n$. This set is equivalent to the set $\bigcap_{s\in E} m_s$. i.e. points can be thought of as maximal ideals.

The Affine Plane $\mathbb{A}^2_{\mathbb{C}}$

We completely classify the prime ideals of $\mathbb{C}[x,y]$.

Proposition: Each element of $\mathbb{A}^2_{\mathbb{C}}$ is of one of the following forms:

(a) (0),

(b) $(x-a, y-b)$ for every $a, b \in \mathbb{C}$,

(c) (f) for any irreducible $f \in \mathbb{C}[x_1,\dots,x_n]$.

Before proving this, we need unique factorization domains (UFDs).

Def'n: A domain R is a UFD if: (a) Factoring of any $r \in R\setminus\{0\}$ terminates.

(b) Any factorization of R into irreducibles is unique up to associates.

Proposition: Let R be a UFD. If $r \in R$ is irreducible, then r is prime.

Proof: Let r be irreducible and suppose $r \mid ab$ for some $a, b \in R$.

Write $rs = ab$ for some $s \in R$. Since r is its own factorization, it must appear in either a or b. $\square$

Remark: Any PID is a UFD, and any Euclidean domain is a PID.

To summarize, we have:

(a) In a domain, prime implies irreducible.

(b) In a UFD, irreducible is equivalent to prime.

(b) In a UFD, irreducible is equivalent to prime.

(c) In a PID, prime ideals are maximal.

(d) In any domain, maximal ideals are prime.

(e) In any domain, irreducible is equivalent to maximal among principal ideals.

Def'n: Let k be a field. We call $k(x) = \mathrm{Frac}(K) = \{\frac{a(x)}{b(x)} \mid a, b \in k[x], b \neq 0\}$ the field of rational functions or fraction field over k.

Theorem (Gauss's Lemma): $f \in k[x_1, \ldots, x_n]$ is irreducible if and only if all its coefficients in $k[x_1, \ldots, x_{n-1}]$ do not share a common factor and f is irreducible in $k(x_1, \ldots, x_{n-1})[x_n]$.

Theorem: $\mathbb{A}^2_{\mathbb{C}} = \{(0)\} \cup \{(x-a, y-b) \mid a, b \in \mathbb{C}\} \cup \{(f) \mid f \in \mathbb{C}[x_1, \ldots, x_n] \text{ is irreducible}\}$.

Proof: We proceed in 2 steps.

1. We show each of these are prime.

Notice that $\mathbb{C}[x,y]/(0) \cong \mathbb{C}[x,y]$ and $\mathbb{C}[x,y]/(x-a, y-b) \cong \mathbb{C}$, so these cases are done.

Let $f \in \mathbb{C}[x,y]$ be irreducible. Then (f) is prime since $\mathbb{C}[x,y]$ is a UFD.

2. These are the only prime ideals.

Let $P \subseteq \mathbb{C}[x,y]$ be a non-trivial prime ideal.

If P is principal, then we are done. Assume P is not principal.

Since $\mathbb{C}[x,y]$ is Noetherian, we may write $P = (f_1, \ldots, f_r)$ for some $f_i \in P$.

Moreover, we may choose the f_i to be irreducible. Let $h = \gcd(f_1, f_2) \in \mathbb{C}(x)[y]$.

Since f_1, f_2 are irreducible, Gauss's Lemma gives that $h \in \mathbb{C}(x)$ as f_1, f_2 are irreducible in $\mathbb{C}(x)[y]$.

Choose $p_1, p_2 \in \mathbb{C}(x)[y]$ so that $h = p_1 f_1 + p_2 f_2$.

Clearing denominators, we have a new equation $\tilde{h} = \tilde{p}_1 f_1 + \tilde{p}_2 f_2 \in P$.

Since P is prime, some divisor $x-a$ of $\tilde{h}$ is in P.

Since P is prime, some divisor $x-a$ of h is in P.

Repeating this argument, $y-b \in P$ for some $b \in \mathbb{C}$. But $(x-a, y-b)$ is maximal, so $P = (x-a, y-b)$. $\square$

Localization

Def'n: Let R be a ring and $S \subseteq R$ a multiplicative set containing unity.
The localization of R at S is $R[S^{-1}] := \{\frac{r}{s} \mid r \in R, s \in S\}/\sim$, where
$\sim$ is the equivalence relation $\frac{r}{s} \sim \frac{r'}{s'}$ if and only if there is a $u \in S$
such that $u(rs' - r's) = 0$.

Proposition: $\sim$ is an equivalence relation.

Proof: Reflexivity and symmetry are immediate.
Let $\frac{r_1}{s_1} \sim \frac{r_2}{s_2}$ and $\frac{r_2}{s_2} \sim \frac{r_3}{s_3}$. Then there is $u, v \in S$ so that
$u(r_1s_2 - r_2s_1) = v(r_2s_3 - r_3s_2) = 0$, hence $s_3uv(r_1s_2 - r_2s_1) = s_1uv(r_2s_3 - r_3s_2) = 0$.
Thus, subtracting these gives $uv(r_1s_2s_3 - s_3\cancel{r_2}s_1 - s_1\cancel{r_2}s_3 + s_1r_3s_2) = uvs_2(r_1s_3 - r_3s_1) = 0$.
Since $uvs_2 \in S$, this gives $\frac{r_1}{s_1} \sim \frac{r_3}{s_3}$. $\square$

We define $\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1s_2 + r_2s_1}{s_1s_2}$ and $\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1r_2}{s_1s_2}$, so that $R[S^{-1}]$ is a ring.

Notation:

(a) For $x \in R$ and $S = \{1, x, x^2, \dots\}$, we let $R_x := R[S^{-1}] = \{\frac{r}{x^k} \mid r \in R, k \in \mathbb{Z}_{\geq 0}\}$.

(b) For $P \subseteq R$ a prime ideal, $S = R \setminus P$ is multiplicative. Denote $R_P := R[S^{-1}]$.

(c) If R is a domain, $R_{(0)} = \mathrm{Frac}(R)$ is the field of fractions of R.

(d) For $k[x]$, we have $k(x) := k[x]_{(0)}$.

We define a ring homomorphism $\varphi: R \longrightarrow R[S^{-1}]$ by $\varphi(r) = \frac{r}{1}$ for all $r \in R$.

Proposition: φ is injective if and only if S has no zero divisors.

Proof: "$\Longrightarrow$" Let $s \in S$ be a zero divisor, with $rs = 0$ for some $r \in R \setminus \{0\}$.

Then $\ker(\varphi)=\{0,r\}$, so φ is not injective.

"$\Leftarrow$" If φ is not injective, then $\varphi(r)=0$ for some $r\in R\setminus\{0\}$.

Hence S has a zero divisor. $\square$

Theorem (Universal Property of Localization): Let R be a ring and $S\subseteq R$ a multiplicative set with unity. Let $\varphi: R\to R[S^{-1}]$, $r\mapsto \frac{r}{1}$. Let A be any ring and suppose $f:R\to A$ is a ring homomorphism such that $f(S)\subseteq R^*$.

Then there is a unique homomorphism $g:R[S^{-1}]\to A$ such that the diagram

$$\begin{tikzcd} & R \arrow[dl, "\varphi"'] \arrow[dr, "f"] & \\ R[S^{-1}] \arrow[rr, "g"'] & & A \end{tikzcd}$$

commutes. i.e. $f=g\circ\varphi$.

Proof: For each $\frac{r}{s}\in R[S^{-1}]$, define $g\left(\frac{r}{s}\right)=\frac{f(r)}{f(s)}$.

Well-defined: Let $\frac{r_1}{s_1}\sim\frac{r_2}{s_2}$. We show $f(r_1s_2-r_2s_1)=0$. Choose $u\in S$ so that $u(r_1s_2-r_2s_1)=0$.

Applying f gives $f(r_1s_2-r_2s_1)=0$.

Homomorphism: Let $\frac{r_1}{s_1},\frac{r_2}{s_2}\in R[S^{-1}]$. Then $g\left(\frac{r_1}{s_1}+\frac{r_2}{s_2}\right)=\frac{f(r_1s_2+r_2s_1)}{f(s_1s_2)}=\frac{f(r_1)}{f(s_1)}+\frac{f(r_2)}{f(s_2)}=g\left(\frac{r_1}{s_1}\right)+g\left(\frac{r_2}{s_2}\right)$.

Similarly, $g\left(\frac{r_1}{s_1}\cdot\frac{r_2}{s_2}\right)=g\left(\frac{r_1}{s_1}\right)g\left(\frac{r_2}{s_2}\right)$.

Uniqueness: The definition of g is forced by commutativity. $\square$

Theorem: Let $\beta\in R$. Then $R_\beta\cong R[x]/(x\beta-1)$.

Proof: Define a ring homomorphism $f:R\to R[x]/(xf-1)$ by $f(r)=[r]$. Then $f(\beta)$ is a unit (and all its powers too). By the universal property, there is a unique $g:R_\beta\to R[x]/(x\beta-1)$ so that $f=g\circ\varphi$. We can also define a homomorphism $\tilde{g}:R[x]/(x\beta-1)\to R_\beta$, as any ring homomorphism $R[x]\to R_\beta$ is determined by a homomorphism $R\to R_f$ (say φ) and a choice of where x is mapped. i.e. $\tilde{g}|_R=\varphi$ and $\tilde{g}(x)=\frac{1}{\beta}$ defines a homomorphism.

Then we can factor $\tilde{g}$ through the quotient $R[x]\xrightarrow{\pi}R[x]/(x\beta-1)\to R_\beta$.

But $x\beta-1\mapsto 0$ under these maps so we have $g\circ\tilde{g}=\tilde{g}\circ g=\mathrm{id}$

Then we can factor g through the quotient $R[x] \longrightarrow R[x]/(x\beta-1) \longrightarrow R_\beta$.

But $x\beta - 1 \longmapsto 0$ under these maps, so we have $g \circ \tilde{g} = \tilde{g} \circ g = id$. $\square$

Theorem: Let R be a ring and $S \subseteq R$ a multiplicative set.

Then there is a bijection between elements of $\mathrm{Spec}(R[S^{-1}])$ and prime ideals of R

that are disjoint from S.

Proof: Let $E = \{P \subseteq R \mid P \text{ is prime}, P \cap S = \varnothing\}$. We show $\mathrm{Spec}(R[S^{-1}]) \longleftrightarrow E$.

"$\longrightarrow$" We take $p \longmapsto \varphi^{-1}(p)$. Since preimages of prime ideals are prime, $\varphi^{-1}(p)$ is prime.

Let $s \in S \cap \varphi^{-1}(p)$. Then $\varphi(s)$ is a unit in p - a contradiction.

"$\longleftarrow$" We take $P \longmapsto (\varphi(P))$. Notice that each element of $(\varphi(P))$ is of the form

$\frac{a}{b}$ for some $a \in P$, $b \in S$. Take $\frac{a}{b} \cdot \frac{c}{d} \in (\varphi(P))$ for some $a, c \in R$, $b, d \in S$.

Then $\frac{ac}{bd} = \frac{e}{f}$ for some $e \in P$, $f \in S$. Then there is $u \in S$ so that $u(acf - bde) = 0$.

Hence $ac(uf) = bdue \in P$. Since $u, f \notin P$, we have $ac \in P$. But P is prime, so

at least one of a or b is in P.

Inverses: Notice, $(\varphi(\varphi^{-1}(p))) = (p) = p$.

Conversely, we show $\varphi^{-1}((\varphi(P))) = P$. The "$\supseteq$" direction is immediate.

Let $a \in \varphi^{-1}((\varphi(P)))$. Then $\varphi(a) = \frac{a}{1} = \frac{b}{c}$ for some $b \in P$, $c \in S$.

Choose $u \in S$ so that $a(uc) = bu \in P$. Since $u, c \notin P$, $a \in P$. $\square$

Elimination Theory

Def'n: A monomial order on $k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ is an elimination order for $x_1, \ldots, x_n$ if

each polynomial with leading monomial in $k[y_1, \ldots, y_m]$ is in $k[y_1, \ldots, y_m]$.

Theorem (Elimination Theorem): Let $J \subseteq k[x_1, \ldots, x_n, y_1, \ldots, y_m]$ be an ideal with Gröbner

basis $f_1, \ldots, f_r$ with respect to an elimination order $<$. Then $J \cap k[y_1, \ldots, y_m] = (f_i \mid f_i \in k[y_1, \ldots, y_m])$.

basis $f_1, \dots, f_r$ with respect to an elimination order $<$. Then $J \cap K[y_1, \dots, y_m] = (f_i \mid f_i \in K[y_1, \dots, y_m])$.

Proof: Assume instead there is $g \in J \cap K[y_1, \dots, y_m] \setminus (f_i \mid f_i \in K[y_1, \dots, y_m])$ with $LM(g)$ minimal.

Then $LM(g)$ is divisible by $LM(f_i)$ for some f_i. Since $LM(g)$ is minimal, $LM(g) \in K[y_1, \dots, y_m]$.

Since $<$ is an elimination order, $f_i \in K[y_1, \dots, y_m]$.

Then $\tilde{g} = g - \frac{LT(g)}{LT(f_i)} f_i$ contradicts minimality of g. $\square$

This helps us find solutions to systems of polynomial equations, as we can isolate variables when computing a Gröbner basis of a given ideal.

Final Notes (Part 1)

April 8, 2024 8:04 PM

Morphisms of Schemes

Def'n: Let A be a ring, k a field, and $I \subseteq k[x_1,\dots,x_n]$ an ideal. We define an

(i) affine scheme as $\operatorname{Spec} A$,

(ii) affine n-space as $\operatorname{Spec}(k[x_1,\dots,x_n])$,

(iii) affine variety as $\operatorname{Spec}(k[x_1,\dots,x_n]/I)$.

Def'n: A morphism of schemes $\operatorname{Spec} A \longrightarrow \operatorname{Spec} B$ consists of:

(i) a ring homomorphism $\phi^*: B \longrightarrow A$ - the pullback map, and

(ii) a continuous (with respect to the Zariski topology) map $\phi: \operatorname{Spec} A \longrightarrow \operatorname{Spec} B$.
$$P \longmapsto \phi^{*-1}(P)$$

Remark: ϕ is induced by ϕ^* and is necessarily continuous.

Proof: Let $V(I)$ be closed in $\operatorname{Spec}(B)$, where $I \subseteq B$ is an ideal. Then

$\phi^{-1}(V(I)) = \{P \in \operatorname{Spec}(A) \mid I \subseteq \phi^{*-1}(P)\} = \{P \in \operatorname{Spec}(A) \mid \phi^*(I) \subseteq P\} = V(\phi^*(I))$.

Thus, ϕ is continuous. $\square$

We restrict our attention to affine space.

We consider pullback maps $\phi^*: k[y_1,\dots,y_m] \longrightarrow k[x_1,\dots,x_n]$ that fix k, so that ϕ is entirely determined by its action on the y_i. Let $y_i \longmapsto \phi_i(x_1,\dots,x_n)$ for some $\phi_1,\dots,\phi_m \in k[x_1,\dots,x_n]$.

Lemma: The morphism $\phi: \mathbb{A}^n \longrightarrow \mathbb{A}^m$ induced by ϕ^* is given by $\phi(a_1,\dots,a_n) = (\phi_1(a_1,\dots,a_n),\dots,\phi_m(a_1,\dots,a_n))$.

Likewise, any ϕ defined in this way induces a pullback map $\phi^*: k[y_1,\dots,y_m] \to k[x_1,\dots,x_n]$ given by $\phi^*(y_i) = \phi_i(x_1,\dots,x_n)$.

i.e., morphisms are in a one-to-one correspondence with homomorphisms of this type.

Proof: We show that $(\phi_1(x_1,\dots,x_n) - \phi_1(a_1,\dots,a_n),\dots,\phi_m(x_1,\dots,x_n) - \phi_m(a_1,\dots,a_n)) \subseteq (x_1 - a_1,\dots,x_n - a_n)$.

Consider the homomorphism $\pi: \mathbb{C}[x_1,\dots,x_n] \longrightarrow \mathbb{C}[x_1,\dots,x_n]/(x_1-a_1,\dots,x_n-a_n) \cong \mathbb{C}$. Then $\phi_i(x_1,\dots,x_n) - \phi_i(a_1,\dots,a_n) \in \ker(\pi)$,
$$x_i \longmapsto a_i$$
proving the claim. Thus, $(y_i - \phi(a_1,\dots,a_n),\dots,y_m - \phi_m(a_1,\dots,a_n)) = \phi((\phi_1(x_1,\dots,x_n) - \phi_1(a_1,\dots,a_n),\dots,\phi_m(x_1,\dots,x_n) - \phi_m(a_1,\dots,a_n)))$. $\square$

Note: We can think of $\mathbb{A}^n$ as points since $\sqrt{J} = \bigcap_{J \subseteq m} m$ for m maximal.

In the case of $k[x_1,\dots,x_n]$ for k algebraically closed, we have $m = (x_1 - a_1,\dots,x_n - a_n)$ for some $a_i \in k$.

Morphisms of Varieties

Let $V \subseteq \mathbb{A}^n$ be a variety, i.e., $V = \operatorname{Spec}(k[x_1,\dots,x_n]/I)$ for some ideal I. The pullback of a morphism $\phi: V \to \mathbb{A}^m$ is a ring homomorphism $\phi^*: k[y_1,\dots,y_m] \longrightarrow k[x_1,\dots,x_n]/I$.

$\phi: V \to \mathbb{A}^m$ is a ring homomorphism $\phi^*: k[y_1,\dots,y_m] \to k[x_1,\dots,x_n]/I$.

We can view the pullback as a composition $k[y_1,\dots,y_m] \xrightarrow{\phi^*} k[x_1,\dots,x_n] \xrightarrow{\pi} k[x_1,\dots,x_n]/I$.
$$y_i \longmapsto \phi_i \longmapsto [\phi_i]_I$$

Let $W = \mathrm{Spec}(k[y_1,\dots,y_m]/J) \subseteq \mathbb{A}^m$ be another variety.

How can we restrict a morphism $\phi: V \to \mathbb{A}^m$ to $\tilde{\phi}: V \to W$? Consider the following diagram:

$$\begin{tikzcd}
\mathbb{C}[y_1,\dots,y_m] \arrow[r, "\phi^*"] \arrow[dr, "\pi"'] & \mathbb{C}[x_1,\dots,x_n]/I \\
& \mathbb{C}[y_1,\dots,y_m]/J \arrow[u, dotted, "?\,\tilde{\phi}^*"']
\end{tikzcd}$$

The map $\tilde{\phi}^*$ exists if $J \subseteq \ker(\phi^*)$, giving a criterion for the existence of morphisms $V \to W$.

Rational Maps

Def'n: A rational map consists of a map $\rho: \mathbb{A}^n \dashrightarrow \mathbb{A}^m$ and a pullback $\rho^*: k[y_1,\dots,y_m] \to k(x_1,\dots,x_n)$ where $\rho^*(y_i) = \phi_i \in k(x_1,\dots,x_n)$ for each $i = 1,\dots,m$.

This can also be extended to varieties as in the case of morphisms.

Def'n: The resolution of a rational map $\rho: \mathbb{A}^n \dashrightarrow \mathbb{A}^m$ is the morphism $\eta: \mathbb{A}^n \to \mathbb{A}^m$ induced by the homomorphism $\eta^*: k[y_1,\dots,y_m] \to k[x_1,\dots,x_n]_g$, where g is the least common multiple of the denominators of the ϕ_i. We call $V(g)$ the indeterminacy locus of ρ.

Remark: We have that $k[x_1,\dots,x_n]_g \cong k[x_1,\dots,x_n,z]/(1-zg)$, so η^* uses z to eliminate the denominators.

Dominant Maps

Def'n: A morphism (rational map) of varieties $\phi: V \to W$ is dominant is $\phi(V)$ is dense in W.

Def'n: Let J be an ideal of $k[x_1,\dots,x_n]$. Define $V(J) = \{(a_1,\dots,a_n) \in \mathbb{A}^n \mid f(a_1,\dots,a_n) = 0 \ \forall f \in J\}$.

Let $V \subseteq \mathbb{A}^n$ be a variety. Define $I(V) = \{f \in k[x_1,\dots,x_n] \mid f(a_1,\dots,a_n) = 0 \ \forall (a_1,\dots,a_n) \in V\}$.

Proposition: ϕ is dominant if and only if ϕ^* is injective.

Proof: First assume ϕ is not dominant. Then there is Z closed so that $\phi(V) \subseteq Z \subsetneq W$.

In particular, $I(W) \subsetneq I(Z)$, so we may choose $f \in I(Z) \setminus I(W)$. Then $\bar{f} \in k[y_1,\dots,y_m]/I(W)$ is non-zero.

Observe that $\phi(V) \subseteq Z \subseteq W$ if and only if $\phi^*(I(Z)) \subseteq I(V)$.

Hence, $f \in \mathrm{Ker}(\phi^*)$.

Conversely, if ϕ^* is not injective, then there is $g \notin I(W)$ with $\phi^*(g) \in I(V)$.

Then $\phi^*(I(W) + (g)) \subseteq I(V)$. By the observation, $\phi(V) \subseteq W \cap \{a \in W \mid g(w) = 0\} \subsetneq W$. $\square$

Def'n: Two varieties V, W are birational if there are dominant rational maps $\rho: V \dashrightarrow W$, $\eta: W \dashrightarrow V$

Def'n: Two varieties V, W are birational if there are dominant rational maps $\rho: V \dashrightarrow W$, $\eta: W \dashrightarrow V$ so that $\eta \circ \rho = id_V$ and $\rho \circ \eta = id_W$.

Proposition: V and W are birational if and only if their field of fractions are isomorphic.

Implitization

Theorem: Let $\pi: \mathbb{A}^{n+m} \to \mathbb{A}^m$ be the projection morphism. Let $V \subseteq \mathbb{A}^{n+m}$ be a variety. Then $\overline{\pi(V)} = V(I(V) \cap k[y_1, \dots, y_m])$.

Proof: "$\subseteq$" Let $f \in I(V) \cap k[y_1, \dots, y_m]$ and $(b_1, \dots, b_m) \in \overline{\pi(V)}$. Then

There is $(a_1, \dots, a_n, b_1, \dots, b_m) \overset{\pi}{\mapsto} (b_1, \dots, b_m)$. We have $f(b_1, \dots, b_m) = f(a_1, \dots, a_n, b_1, \dots, b_m) = 0$.

"$\supseteq$" We show $I(\pi(V)) \subseteq I(V) \cap k[y_1, \dots, y_m]$. If $g \in I(\pi(V))$, then $g \in k[y_1, \dots, y_m]$, or else g does not vanish everywhere on $\overline{\pi(V)}$. Thus, g vanishes on V. $\square$

Def'n: Let $\phi: V \to W$ be a morphism of affine varieties. The graph of ϕ is $\Gamma_\phi = \{(a, \phi(a)) \mid a \in V\} \subseteq V \times W \subseteq \mathbb{A}^n \times \mathbb{A}^m \cong \mathbb{A}^{n+m}$.

To find $\overline{\phi(V)}$, we observe that $\overline{\phi(V)}$ is the projection of Γ_ϕ onto $\mathbb{A}^m$, namely, $I(\Gamma_\phi) \cap k[y_1, \dots, y_m]$.

Theorem: Let ϕ be as above. Then $I(\Gamma_\phi) \cong (I(V)) + (y_1 - \phi_1, \dots, y_m - \phi_m)$.

Proof: For any $f \in (I(V))$, we immediately have $f \in I(\Gamma_\phi)$. Moreover, each $y_i - \phi_i$ vanishes on Γ_ϕ by definition. Hence, the "$\supseteq$" direction is shown.

For the converse, let $f \in I(\Gamma_\phi)$. Consider the quotient maps

$$k[x_1, \dots, x_n, y_1, \dots, y_m] \to k[x_1, \dots, x_n, y_1, \dots, y_m] / (y_1 - \phi_1, \dots, y_m - \phi_m) \to k[x_1, \dots, x_n, y_1, \dots, y_m] / (I(V)) + (y_i - \phi_i)_{i=1}^m.$$

Then $f \mapsto f(x_1, \dots, x_n, \phi_1, \dots, \phi_m) \mapsto 0$. $\square$

Applying elimination theory lets us compute the image of morphisms.

Final Notes (Part 2)

April 11, 2024 7:59 PM

Nullstellensatz

Theorem (Weak Nullstellensatz I): The maximal ideals in $\mathbb{C}[x_1,\dots,x_n]$ are precisely of the form $(x_1-a_1,\dots,x_n-a_n)$, where $a_1,\dots,a_n \in \mathbb{C}$.

Proof: Since $\mathbb{C}[x_1,\dots,x_n]/(x_1-a_1,\dots,x_n-a_n) \cong \mathbb{C}$, we have that $(x_1-a_1,\dots,x_n-a_n)$ is maximal.

Let $M \subseteq \mathbb{C}[x_1,\dots,x_n]$ be another maximal ideal. Then $F = \mathbb{C}[x_1,\dots,x_n]/M$ is a field, and there is a surjective homomorphism $\pi: \mathbb{C}[x_1,\dots,x_n] \to F$ with $\ker(\pi) = M$. Let $\pi_1 = \pi|_{\mathbb{C}[x_1]}$.

Then $\operatorname{im}\pi_1$ is a domain, since F is a field. Hence, $\ker \pi_1$ is prime, thus maximal in $\mathbb{C}[x_1]$.

Write $\ker\pi_1 = (x_1-a_1)$ for some $a_1 \in \mathbb{C}$. Likewise, $\ker\pi_j = (x_j - a_j)$ for some $a_j \in \mathbb{C}$. Thus, $(x_1-a_1,\dots,x_n-a_n) \subseteq \ker\pi = M$, so the ideals are equal. $\square$

Theorem (Weak Version II): Let $J \subseteq \mathbb{C}[x_1,\dots,x_n]$ be an ideal. If $V(J) = \emptyset$, then $J = \mathbb{C}[x_1,\dots,x_n]$.

Theorem (Strong Nullstellensatz): Let $J \subseteq \mathbb{C}[x_1,\dots,x_n]$ be an ideal. Then $I(V(J)) = \sqrt{J}$.

Proposition: TFAE: (a) Weak Version I,

(b) Weak Version II,

(c) Strong Version.

Proof:

$(a) \Longrightarrow (b)$

Suppose $J \subsetneq \mathbb{C}[x_1,\dots,x_n]$. By vI and Zorn's Lemma, there is a maximal ideal $(x_1-a_1,\dots,x_n-a_n)$ containing J. In particular, $(a_1,\dots,a_n) \in V(J)$. //

$(b) \Longrightarrow (a)$ Let $M \subsetneq \mathbb{C}[x_1,\dots,x_n]$ be another maximal ideal. Then vII gives us that $V(M) \neq \emptyset$.

Let $(a_1,\dots,a_n) \in V(M)$. Then $M \subseteq (x_1-a_1,\dots,x_n-a_n)$. But M is maximal, so equality holds. //

$(b) \Longrightarrow (c)$ Let $f \in \sqrt{J}$. Then $f^m \in J$ for some $m \in \mathbb{N}$. But $\mathbb{C}$ is a domain, so $f \in I(V(J))$.

Conversely, let $g \in I(V(J))$ be non-zero. Since $\mathbb{C}[x_1,\dots,x_n]$ is Noetherian, we may choose $f_i \in J$ such that $J = (f_1,\dots,f_r)$. Define $\tilde{J} := (f_1,\dots,f_r, 1-zg) \subseteq \mathbb{C}[x_1,\dots,x_n,z]$. We claim that $V(\tilde{J}) = \emptyset$.

$J = (f_1, \dots, f_r)$. Define $\tilde{J} := (f_1, \dots, f_r, 1-zg) \subseteq \mathbb{C}[x_1, \dots, x_n, z]$. We claim that $V(\tilde{J}) = \emptyset$.

Let $(a_1, \dots, a_n, a_{n+1}) \in \mathbb{A}^{n+1}_{\mathbb{C}}$. If $(a_1, \dots, a_n) \notin V(J)$, then $(a_1, \dots, a_n, a_{n+1}) \notin V(\tilde{J})$.

Suppose $(a_1, \dots, a_n) \in V(J)$. Then $1 - a_{n+1} g(a_1, \dots, a_n) = 1 \neq 0$, so $(a_1, \dots, a_n, a_{n+1}) \notin V(\tilde{J})$.

Thus, $V(\tilde{J}) = \emptyset$, so $\tilde{J} = \mathbb{C}[x_1, \dots, x_n, z]$. Hence, there are $c_1, \dots, c_r, c \in \mathbb{C}[x_1, \dots, x_n, z]$ such that

$c_1 f_1 + \dots + c_r f_r + c(1-zg) = 1$, and evaluating z at $1/g$ gives $\sum_{i=1}^r c_i(x_1, \dots, x_n, \frac{1}{g}) f_i = 1$.

Clearing denominators, we have $g^m = \sum_{i=1}^r \tilde{c}_i(x_1, \dots, x_n) f_i \in J$ for some $m \in \mathbb{N}$. //

(c) $\Rightarrow$ (b) We have $V(J) = \emptyset$, so $\sqrt{J} = I(V(J)) = \mathbb{C}[x_1, \dots, x_n]$, by definition of $I(\emptyset)$.

In particular, $1 \in \sqrt{J}$, so $1 \in J$. Hence, $J = \mathbb{C}[x_1, \dots, x_n]$. $\square$

Essentially, Nullstellensatz is a way to go back and forth between ideals and their vanishings.

Irreducible Varieties

Def'n: A variety is reducible if it is the union of two smaller varieties.

A variety that is not reducible is called irreducible.

Proposition: Any variety is the union of finitely many irreducible varieties.

Proof: Let V be a reducible variety. Suppose $V = V_1 \cup V_2$ for some varieties $V_1, V_2 \subsetneq V$.

If V_1, V_2 are irreducible, then we are done. Suppose, without loss, that V_1 is reducible.

Continuing in this way, we find a decreasing sequence of varieties $V_1 = W_1 \supsetneq W_2 \supsetneq \dots$.

Thus, $I(W_1) \subsetneq I(W_2) \subsetneq \dots$ is an ascending chain of ideals. Since $\mathbb{C}[x_1, \dots, x_n]$ is Noetherian, we are done. $\square$

Proposition: An affine variety W is irreducible if and only if $I(W)$ is prime.

That is, W is irreducible if and only if $\mathbb{C}[x_1, \dots, x_n]/I(W)$ is an integral domain.

Proof: "$\Rightarrow$" Let $fg \in I(W)$. Then $W = I(V(W)) \subseteq V(fg) = V(f) \cup V(g)$.

Then $W = W \cap (V(f) \cup V(g)) = (W \cap V(f)) \cup (W \cap V(g))$. But W is irreducible, so

$V(f) \subseteq W$ or $V(g) \subseteq W$.

"$\Leftarrow$" Let $I(W)$ be prime and write $W = V_1 \cup V_2$ for some varieties $V_1, V_2 \subseteq W$, $V_1 \neq W$.

"$\Leftarrow$" Let $I(W)$ be prime and write $W = V_1 \cup V_2$ for some varieties $V_1, V_2 \subseteq W$, $V_1 \neq W$.

Then $I(W) \subsetneq I(V_1)$. Let $f \in I(V_1) \setminus I(W)$ and $g \in I(V_2)$. Then fg vanishes on W.

Hence, $fg \in I(W)$. But $I(W)$ is prime and $f \notin I(W)$, so $g \in I(W)$. Hence, $V_2 = W$. $\square$

Projective Space

Def'n: Projective n-space, $\mathbb{P}^n$, is in bijection with $(\mathbb{A}^{n+1} \setminus \{0\})/\sim$, where $[a_1, \ldots, a_{n+1}] \sim [b_1, \ldots, b_{n+1}]$ if there is $\lambda \in \mathbb{C}^*$ such that $[a_1, \ldots, a_{n+1}] = \lambda [b_1, \ldots, b_{n+1}]$.

In particular, $\mathbb{P}^n$ consists of lines in $(n+1)$-space intersecting but not attaining the origin.

Remark: Projective space is compact, whereas affine space is not.

We define the canonical injection of $\mathbb{A}^n$ into $\mathbb{P}^n$ by $(a_1, \ldots, a_n) \mapsto [a_1, \ldots, a_n, 1]$.

Def'n: The extension of a polynomial $f \in \mathbb{C}[x_1, \ldots, x_n]$ to a polynomial with solutions in $\mathbb{P}^n$ is the homogenization of f, $\tilde{f} \in \mathbb{C}[x_1, \ldots, x_n, z]$, where $\tilde{f}$ is the homogeneous polynomial formed by multiplying each monomial in f by suitable powers of z. i.e. $\tilde{f}|_{z=1} = f$.

Remark: Homogenization solves the issue of equivalence classes.

Def'n: The intersection multiplicity of $f, g \in \mathbb{C}[x,y]$ at a common zero $(a,b) \in \mathbb{C}^2$ is the dimension of the vector space $\left(\mathbb{C}[x,y]/(f,g)\right)_{(x-a,y-b)}$ over $\mathbb{C}$.

Remark: Localization "remembers" tangent information.

Theorem (Bezout): Let V, W be irreducible curves cut out by $f, g \in \mathbb{C}[x,y]$ respectively. i.e. $V = V(f)$, $W = V(g)$ in $\mathbb{P}^2$. Then, counting with multiplicity, the number of intersection points of f and g in $\mathbb{P}^2$ is $\deg(f) \cdot \deg(g)$.

Remark: $\mathbb{P}^2$ gives more solutions than in $\mathbb{A}^n$.