4/8/14

HW 4 due Thurs Apr 17

NO CLASS THIS THURSDAY

Final Exam Thurs May 1, 2–4:30 pm

Last time we proved* Hilbert's NSS:

If K is algebraically closed then every maximal ideal $\mathfrak{m} < K[x_1, \cdots, x_n]$ has the form

$$\mathfrak{m} = \mathfrak{m}_{\underline{a}} = (x_1 - a_1, \cdots, x_n - a_n)$$

for some point $\underline{a} \in K^n$.

This is the key fact that allows us to construct "geometry" out of polynomial functions.

Recall that a variety is a set of the form

$$V = V(J) = \{ \underline{a} \in K^n : f(\underline{a}) = 0 \ \forall \ f \in J \}$$

for some ideal $J \leq K[x_1, \cdots, x_n]$. By Hilbert's Basis theorem $\exists \ f_1, \cdots, f_m \in J$ such that

$$J = (f_1, f_2, \cdots, f_m)$$

and so $\underline{a} \in V$ if and only if

$$\left.\begin{aligned} f_1(\underline{a}) &= 0 \\ f_2(\underline{a}) &= 0 \\ &\vdots \\ f_m(\underline{a}) &= 0 \end{aligned}\right\}$$

Definition: We say $V \subseteq K^n$ is a hypersurface if

$$V = V(f) = \{ \underline{a} \in K^n : f(\underline{a}) = 0 \}$$

for some $K[\underline{x}]$. Example: An affine hyperplane is a hypersurface.

We can thus say:

"variety" $\equiv$ an intersection of hypersurfaces

Q: What do varieties "look like"?

Definition: We say that variety $X \subseteq K^n$ is irreducible if for all varieties $X_1, X_2 \subseteq K^n$ we have

$$X = X_1 \cup X_2 \implies X = X_1 \text{ OR } X = X_2$$

Theorem: Let $X \subseteq K^n$ be a variety. Then

X is irreducible $\iff$ $I(X) < K[x]$ is prime.

Proof: Let $I := I(X)$. If I is NOT prime then $\exists\, f_1, f_2 \in K[x] \setminus I$ with $f_1 f_2 \in I$. Define $X_1 := V(I + (f_1))$. Then

$$I \leq I + (f_1)$$
$$\Rightarrow \quad V(I) \supseteq V(I + (f_1))$$
$$\Rightarrow \quad X \supseteq X_1$$

[Recall $V(I) = V(I(X)) = X$ because X is a variety, i.e., $X = V(J)$ for some ideal J.].

But since $f_1 \notin I$, $\exists\, a \in X$ such that $f_1(a) \neq 0$, and hence $a \notin X_1$. We conclude that $X_1 \subsetneq X$.

Similarly, we have $X_2 \subsetneq X$ where $X_2 := V(I + (f_2))$.

Since $X_1, X_2 \subseteq X$ we have

$$X_1 \cup X_2 \subseteq X.$$

But for all $a \in X$ we have $f_1 f_2(a) = 0$ because $f_1 f_2 \in I$, and hence

$$0 = f_1 f_2(a) = f_1(a) f_2(a)$$

$\Rightarrow f_1(a) = 0$ or $f_2(a)$.

Since $f(a) = 0 \ \forall f \in I$ this implies

$a \in X_1$ or $a \in X_2$.

Hence $X \subseteq X_1 \cup X_2$, and we have

$X = X_1 \cup X_2$ with $X \neq X_1$ and $X \neq X_2$.

i.e., X is NOT irreducible.

Conversely, suppose $\exists$ varieties X_1, X_2 such that

$X = X_1 \cup X_2$ with $X \neq X_1$ and $X \neq X_2$

and let $I_1 := I(X_1)$, $I_2 := I(X_2)$.

We have $X_1 \subseteq X$

$\Rightarrow I(X_1) \supseteq I(X)$.

But if $I(X_1) = I(X)$ then

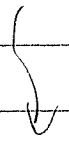
$$X_1 = V(I(X_1)) = V(I(X)) = X,$$

contradiction. Hence $\exists f_1 \in I_1 \setminus I$ and similarly $\exists f_2 \in I_2 \setminus I$.

But then for all $a \in X = X_1 \cup X_2$ we have $a \in X_1$ (hence $f_1(a) = 0$) or $a \in X_2$ (hence $f_2(a) = 0$) and hence $f_1 f_2(a) = f_1(a) f_2(a) = 0$.

We conclude that $f_1, f_2 \notin I$ but $f_1 f_2 \in I$, so I is NOT prime.

Furthermore, every variety decomposes into irreducibles is a unique way.



Theorem: Let $X \subseteq K^n$ be a variety. Then we have a unique decomposition

$$X = X_1 \cup X_2 \cup \cdots \cup X_r$$

where X_i are irreducible varieties and $i \neq j \Rightarrow X_i \not\subseteq X_j$

Proof: First note that varieties satisfy the d.c.c.: If $\exists$ an infinite descending chain of varieties

$$X_1 \supsetneq X_2 \supsetneq X_3 \supsetneq \cdots,$$

then applying the map I gives an infinite ascending chain of ideals

$$I(X_1) < I(X_2) < I(X_3) < \cdots$$

contradicting the fact that $K[\underline{x}]$ is Noetherian (HBT). [Why does $X_i \neq X_{i+1} \Rightarrow I(X_i) \neq I(X_{i+1})$?]

Now let $\Sigma = \{$ varieties $X \subseteq K^n$ that have no decomposition $\}$

We want to show that $\Sigma = \emptyset$. ...

If $\Sigma \neq \emptyset$ then by Zorn's Lemma Σ has a minimal element $X \in \Sigma$.

Since X is not irreducible we have

$X = X_1 \cup X_2$ with $X_1 \subsetneq X$ and $X_2 \subsetneq X$.

But then $X_1, X_2 \notin \Sigma$ imply that X_1, X_2 have decompositions. Hence so does X. ///

To show uniqueness, suppose

$$X_1 \cup \cdots \cup X_k = X_1' \cup \cdots \cup X_\ell'$$

for X_i, X_j' irreducible with $i \neq j$

$\Rightarrow X_i \not\subseteq X_j$ and $X_i \not\subseteq X_j'$.

Since $X_1 \subseteq X_1' \cup \cdots \cup X_\ell'$ we have

$$X_1 = X_1 \cap (X_1' \cup \cdots \cup X_\ell')$$

$$X_1 = (X_1 \cap X_1') \cup \cdots \cup (X_1 \cup X_\ell')$$

by distributivity.

Since X_1 is irreducible this implies

$$X_1 = X_1 \cap X_j', \text{ i.e., } X_1 \subseteq X_j'$$

for some j. By symmetry we also have $X_j' \subseteq X_i$ for some i. If $i \neq 1$ then

$$X_1 \subseteq X_j' \subseteq X_i$$

is a contradiction, so we have $i = 1$ and $X_1 = X_j'$. Now use induction

∎

[Remark: The same proof works to show unique decomposition in any distributive lattice satisfying the d.c.c.]

Q: What do varieties "look like"?

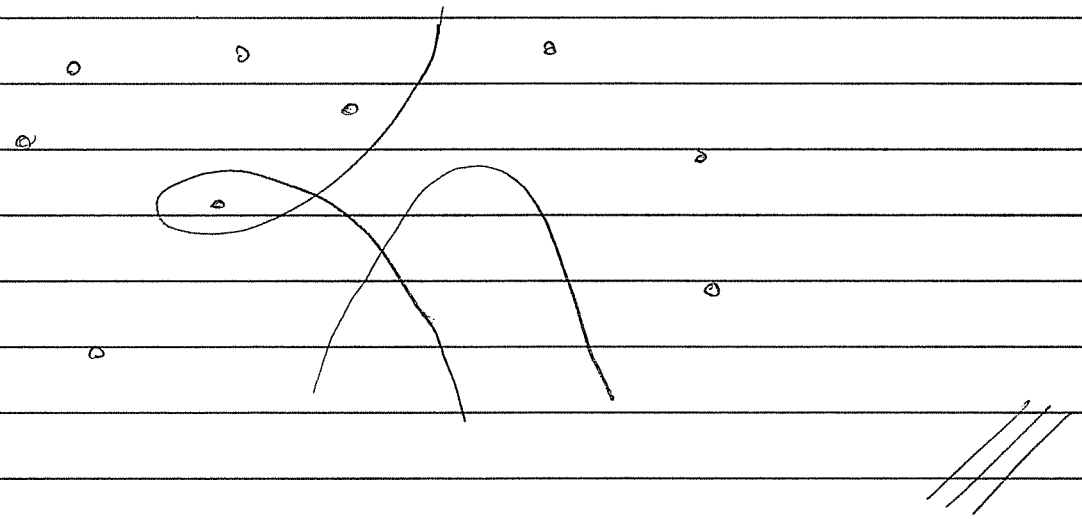
A: If K is algebraically closed then we know that the prime ideals of $K[x,y]$ are.

- (0)
- $(f(x,y))$ for irreducible $f \in K[x,y]$
- $(x-\alpha, y-\beta)$ for $(\alpha,\beta) \in K^2$.

Thus the irreducible varieties in K^2 are.

- $V(0) = K^2$
- $V(f)$ = a curve/hypersurface in K^2
- $V(x-\alpha, y-\beta)$ = the point (α, β).

A general variety in K^2 is a union of these:



Example: Let

$$f(x,y) = (y^2 - x + 1)(y - x)$$

Then since $K[x,y]$ is a domain we have

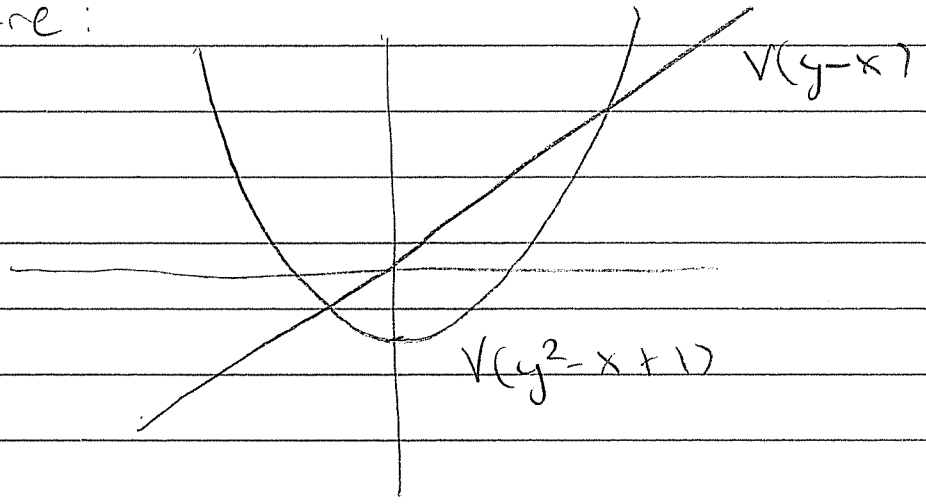
$$f(x,y) = 0 \iff y^2 = x - 1 \text{ OR } y = x.$$

In other words,

$$V(F) = V(y^2 - x + 1) \cup V(y - x)$$

Claim: $y^2 - x + 1$ & $y - x$ are irreducible so these are the irreducible components.

Picture:



Q: How can we determine the "dimension" of a variety?

A: Given an irreducible variety $X \subseteq K^n$ we define the dimension $\dim(X)$ as the maximum d such that there exist irreducible varieties

$$X = X_0 \supsetneq X_1 \supsetneq \cdots \supsetneq X_d.$$

If X is reducible, say

$$X = X_1 \cup X_2 \cup \cdots \cup X_k,$$

then we define

$$\dim(X) = \max\{\dim(X_i)\}$$

Analogously, given an ideal $J \subsetneq R$ in a ring we define the depth of J as the maximum d such that there exist prime ideals

$$J \subseteq P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d$$

We define the Krull dimension of R as the depth of (0):

$$\dim(R) := \{\max d : \text{there exists primes } P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_d \subsetneq R\}.$$

4/15/14

HW 4 due this Thurs Apr 17

Final Exam Thurs May 1, 2–4:30pm

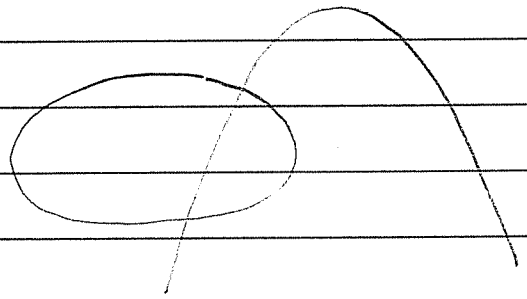
Let K be a field. Recall: We say $X \subseteq K^n$ is a variety if

$$X = V(J) = \{\underline{a} \in K^n : f(\underline{a}) = 0 \ \forall \ f \in J\}$$

for some ideal $J \subseteq K[x_1, \dots, x_n]$. We say that a variety X is irreducible if for all varieties $X_1, X_2 \subseteq K^n$ we have

$$X = X_1 \cup X_2 \implies X = X_1 \text{ OR } X = X_2 .$$

Picture:



This variety is reducible with two irreducible components.

Last time we proved that

$\downarrow$

X is irreducible $\iff$ $I(X) < K[x]$ is prime

[Convention: $X = \emptyset$ is not irreducible.]

We also proved that every variety has a unique decomposition

$$X = X_1 \cup X_2 \cup \cdots \cup X_r$$

where X_i are irreducible and $i \neq j \Rightarrow X_i \not\subseteq X_j$.

What does this tell us about ideals?

If $X \subseteq K^n$ is a variety, say $X = V(J)$, then we have

$$X = V(J) = V(I(V(J)))$$
$$X = V(I(X))$$

Thus if X is irreducible then we have $X = V(P)$ where P is prime (just take $P = I(X)$.)

Now let $J \subseteq K[x_1, \cdots, x_n]$ &c any ideal

{

We can decompose $V(J)$ into irreducibles

$$V(J) = X_1 \cup X_2 \cup \cdots \cup X_r$$
$$= V(P_1) \cup V(P_2) \cup \cdots \cup V(P_r)$$

where $P_1, \ldots, P_r \leq K[\underline{x}]$ are prime ideals. But recall that for any ideals J_1, J_2 we have $V(J_1) \cup V(J_2) = V(J_1 \cap J_2)$. Hence

$$V(J) = V(P_1 \cap P_2 \cap \cdots \cap P_r).$$

Applying I gives

$$I(V(J)) = I(V(P_1 \cap \cdots \cap P_r))$$

But we will show that $P_1 \cap \cdots \cap P_r$ is a closed ideal and hence

$$I(V(J)) = P_1 \cap P_2 \cap \cdots \cap P_r$$

In words: The closure of J is the intersection of the minimal prime ideals containing J.

However, to prove this we need K algebraically closed.

✡ **Theorem (Strong Nullstellensatz):**

Let K be algebraically closed and let $J \leq K[\underline{x}]$ be any ideal. Then we have

$$I(V(J)) = \sqrt{J}$$
$$:= \{ f \in K[\underline{x}] : f^m \in J \text{ for some } m \}.$$

"closure = radical"

Proof: This is a consequence of the "weak Nullstellensatz" (i.e., the fact that $V(J) = \emptyset \Rightarrow J = K[\underline{x}]$) and a trick of Rabinowitch (1929).

Given $f \in I(V(J))$ (i.e. $f(\underline{a}) = 0$ for all $\underline{a} \in V(J)$) we want to show that $f^m \in J$ for some m.

Now consider the ideal

$$J' := (J, fy - 1) \leq K[x_1, \ldots, x_n, y].$$

Note that $\alpha = (a_1, \cdots, a_n, \beta) \in K^{n+1}$ is in $V(J')$ if and only if

$\alpha \in V(J)$ and $\alpha \in V(fy-1)$

(i.e. $f(a_1, \cdots, a_n) = 0$) (i.e. $\beta \cdot f(a_1, \cdots a_n) = 1$).

But this is impossible, hence $V(J') = \emptyset$ and weak Nullstellensatz implies that $J' = K[x_1, \cdots, x_n, y]$.

Since $1 \in J'$ (and since J is f.g. by HBT) we can write

$$(*) \qquad 1 = g_0(fy-1) + \sum_i g_i h_i$$

for some $h_i \in J$ and $g_i \in K[x_1, \cdots, x_n, y]$.

Suppose y^m is the highest power of y appearing in any g_i. Multiply both sides of $(*)$ by f^m to get

$$(**) \qquad f^m = G_0(x_1, \cdots, x_n, fy)(fy-1) + \sum_i G_i(x_1, \cdots, x_n, fy)\, h_i$$

where $G_i \in K[x_1, \cdots, x_n, x_{n+1}]$.

Since (**) is an identity of polynomials, it remains true if we substitute $y = f^{-1}$. Doing this gives

$$f^m = G_0(x_1, \dots, x_n, 1) \cdot 0 + \sum_i G_i(x_1, \dots, x_n, 1) h_i \in J$$

as desired. ∎

[Remark: Geometrically, Rabinowitch's trick means the following. Given $f \in K[x_1, \dots, x_n]$ we consider the complement of the hypersurface

$$U_f := \{ a \in K^n : f(a) \neq 0 \} \subseteq K^n.$$

This is not a variety in K^n, but it is isomorphic to a variety in K^{n+1}. Namely we define

$$\overline{U}_f := \{ a \in K^{n+1} : a_{n+1} f(a_1, \dots, a_n) = 1 \}.$$

This is a variety, so we can apply the weak NSS in $\overline{U}_f$ and then map back down to K^n.

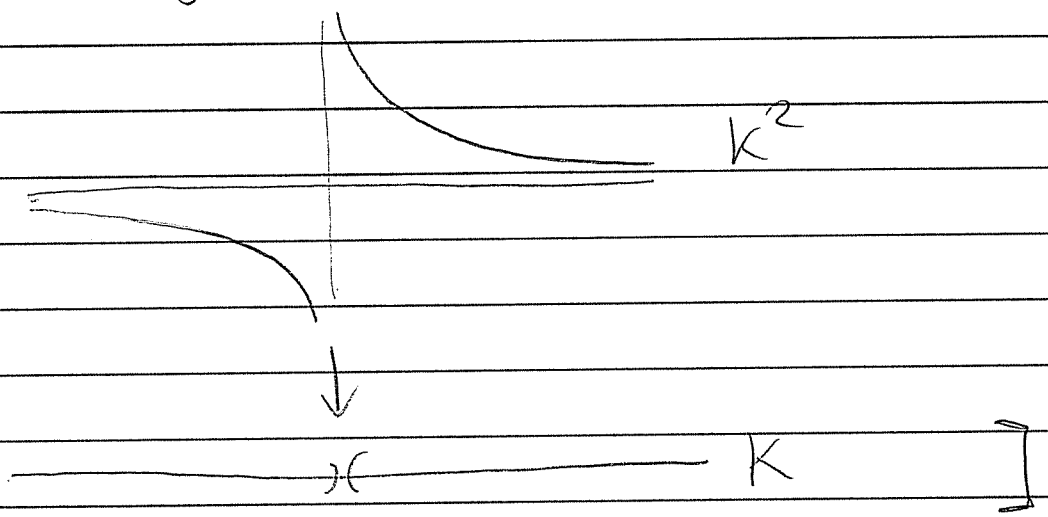
Picture: Let $f(x) = x \in K[x]$. The set

$$U_f = \{ \alpha \in K : \alpha \neq 0 \} \subseteq K$$

is not a variety but the set

$$\overline{U}_f = \{ (\alpha, \beta) \in K^2 : \alpha\beta = 1 \} \subseteq K^2$$

is a variety



We just proved that

$$f \in I(V(J)) \Rightarrow f^m \in J \text{ for some } m.$$

"If f vanishes where J vanishes, then some power of f is in J".

Conversely, suppose $f^m \in J$ for some m, and consider any $\underline{a} \in V(J)$. Then we have

$$f^m(\underline{a}) = 0 \implies f(\underline{a}) = 0$$

and hence $f \in I(V(J))$.
We conclude that

$$I(V(J)) = \sqrt{J}.$$

Notation: We say an ideal J is radical if

$$J = \sqrt{J}.$$

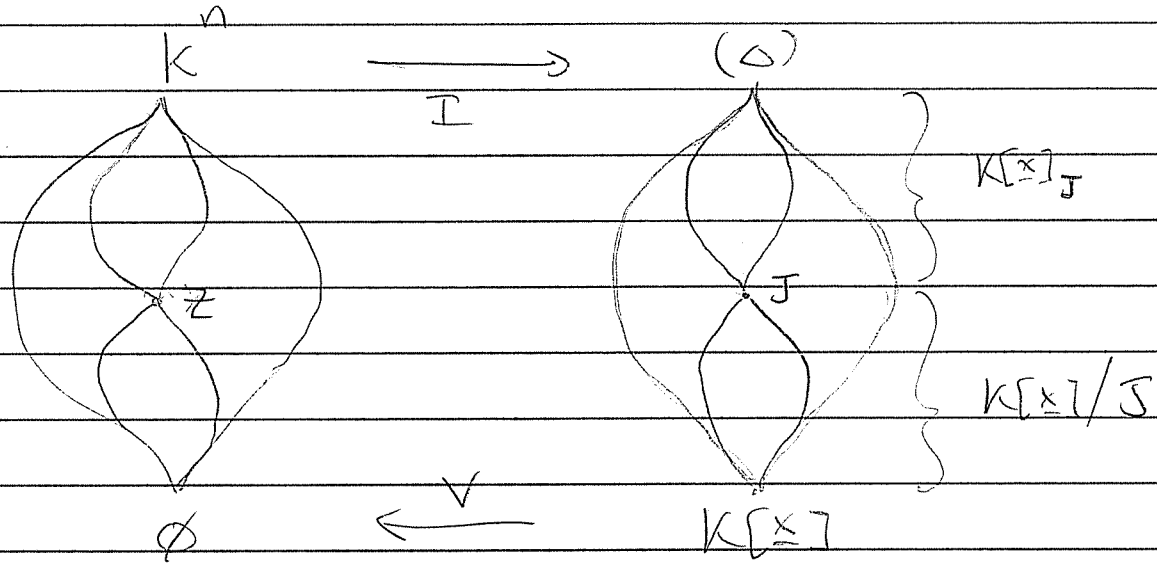
This allows us to complete our description of Hilbert's "Galois connection".

Let K be an algebraically closed field. Then the maps

$$I : 2^{K^n} \to 2^{K[\underline{x}]}$$
$$V : 2^{K[\underline{x}]} \to 2^{K^n}$$

set up an order reversing bijection:

$$\{\text{varieties} \subseteq K^n\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{radical ideals} \subseteq K[\underline{x}]\}$$



The bijection matches irreducible varieties to prime ideals.

Furthermore,

- Every variety is the union of the finitely many maximal irreducible subvarieties it contains.

- Every radical ideal is the intersection of the finitely many minimal prime ideals that contain it.

///

Suppose Z, J is a variety, rad. ideal pair. Then we have a bijection between

$$\{\text{subvarieties of } Z\} \longleftrightarrow \{\text{rad. ideals of } K[\underline{x}]/J\}$$

Notation:

$$K[Z] := K[\underline{x}]/I(Z)$$

"The coordinate ring of Z"

Note that $K[Z]$ is a domain if and only if Z is irreducible. In this case $I(Z)$ is prime and we can also consider the localization

$$K[\underline{x}]_{I(Z)} = \left\{ \frac{f}{g} : f, g \in K[\underline{x}], g \notin I(Z) \right\}.$$

That is, $\frac{f}{g} \in K[\underline{x}]_{I(Z)}$ if g never vanishes on Z so that f/g defines a function on Z.

We have a bijection

$$\{\text{varieties } \supseteq Z\} \longleftrightarrow \{\text{rad. ideals of } K[\underline{x}]_{I(Z)}\}.$$

The points of Z correspond to maximal ideals $m < K[Z]$.

The vector space m/m^2 is called the Zariski tangent space at the point m. The dimension

$$\dim_K(m/m^2)$$

tells us if m is a singular point. The set of singular points form a subvariety of Z called the singular locus.

If $K[Z]$ is normal (integrally closed in $\mathrm{Frac}(K[Z])$) then the singular locus has codimension ≥ 2.

Corollary: If Z is a curve (1D) and $K[Z]$ is normal then Z is smooth (i.e. nonsingular).

4/17/14

HW 4 due now (sorry no solutions yet).
Final Exam Thurs May 1, 2-4:30 pm.

We have seen the Nullstellensatz, but there is still something missing from the proof.

☆ Zariski's Lemma: Let K be a field and let $A \supseteq K$ be an algebra such that

- A is f.g. as a K-algebra
- A is a field.

Then A is algebraic over K and hence $[A : K] < \infty$.

Let's prove it now.

Let $A \supseteq K$ be an algebra. Recall that we say $a_1, a_2, \ldots, a_n \in A$ are algebraically independent if the evaluation homomorphism

↓

$$ev_{\underline{a}} : K[x_1, \ldots, x_n] \longrightarrow A$$
$$f(x_1, \ldots, x_n) \longmapsto f(a_1, \ldots, a_n)$$

is injective. That is, there does not exist $0 \neq f \in K[\underline{x}]$ such that

$$f(\underline{a}) = 0.$$

Now recall the analogy between K-algebras and K-modules.

K-module	K-algebra
linear dependence	algebraic dependence.

If V is a K-module we say that $\beta \subseteq V$ is a "basis" if it is a maximal linearly independent set.

Steinitz' Exchange Lemma proves that every basis has the same size!

$$\dim_K(V) = \text{size of any basis}$$

Q: Does there exist an analogous concept for K-algebras?

A: Yes.

Definition: Let $A \supseteq K$ be an algebra. (I assume A is a domain). We say $\beta = \{\beta_1, \beta_2, \dots, \beta_d\} \subseteq A$ is a transcendence basis if

- β is algebraically independent over K
- A is algebraic over the polynomial algebra

$$K[\beta_1, \dots, \beta_d] \approx K[x_1, \dots, x_d].$$

Equivalently, a transcendence basis is a maximal alg. independent subset of A.

Proof: Let $\beta = \{\beta_1, \dots, \beta_d\} \subseteq A$ be max. alg. ind. and consider any $\alpha \in A \setminus \beta$. Since $\{\beta_1, \dots, \beta_d, \alpha\}$ is not alg. ind. $\exists\ 0 \neq f \in K[x_1, \dots, x_{d+1}]$ such that

$$f(\beta_1, \dots, \beta_d, \alpha) = 0$$

$\}$

By collecting terms we can write

$$F(\beta_1, \cdots, \beta_d, \alpha) = \sum g_i(\beta_1, \cdots \beta_d) \alpha^i = 0$$

for some $g_i \in K[x_1, \cdots, x_d]$, which implies that α is algebraic over $K[\beta_1, \cdots, \beta_d]$.

Conversely, suppose $A \supseteq K[\beta_1, \cdots, \beta_d]$ is algebraic and consider any $\alpha \in A \setminus \beta$. Then $\exists$ a relation

$$\sum g_i(\beta_1, \cdots, \beta_d) \alpha^i = 0.$$

and we conclude that $\{\beta_1, \cdots, \beta_d, \alpha\}$ is not alg. ind. ///

Lemma: Transcendence bases exist.

Proof (Zorn's lemma): Let Σ be the set of alg. ind. subsets of A. Given a chain

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots \text{ in } \Sigma$$

we verify $S := \bigcup S_i$ is an upper bound for the chain ($S_i \subseteq S \ \forall i$) and that S is algebraically independent (any finite subset of S is in some S_i). By Zorn's lemma we conclude that Σ has a maximal element. ///

[Remark: This is the same reason why a general vector space has a basis, i.e., because we say it does.]

Q: If $A \supseteq K$ is finitely generated, does it follow that every transcendence basis is finite?

A: Yes. In fact, if $A = K[u_1, \dots, u_n]$ for some $u_i \in A$ then every max. alg. ind. subset of $\{u_1, u_2, \dots, u_n\}$ is a transcendence basis.

Proof: Let $S \subseteq A$ be any set and consider the subring and subfield of $\mathrm{Frac}(A)$ generated by S:

$$K[S] \subseteq K(S) =: \mathrm{Frac}(K[S]) \subseteq \mathrm{Frac}(A).$$

Note that if $\alpha \in A$ is algebraic over $K[S]$ then it is trivially algebraic over $K(S)$. Conversely, suppose α is alg. over $K(S)$, i.e., we have

$$f(\alpha) = 0 \quad \text{for} \quad f(x) \in K(S)[x].$$

Then multiplying through by the lcm of denominators of coefficients in $f(x)$ shows that α is algebraic over $K[S]$.

In summary:

$$\text{alg. over } K[S] \iff \text{alg. over } K(S).$$

Now suppose $A = K[u_1, \ldots, u_n]$ and suppose $\{u_1, \ldots, u_d\}$ is a max. alg. ind. subset of $\{u_1, \ldots, u_n\}$. We must show that A is algebraic over $K[u_1, \ldots, u_d]$.

So consider the algebraic closure of the field $K(u_1, \ldots, u_d)$ in $\mathrm{Frac}(A)$:

$$\overline{K(u_1, \ldots, u_d)} \subseteq \mathrm{Frac}(A).$$

By assumption, $u_{d+1}, u_{d+2}, \ldots, u_n$ are algebraic over $K[u_1, \ldots, u_d]$ (by the maximality of $\{u_1, \ldots, u_d\}$) hence also over $K(u_1, \ldots, u_d)$, so that

$$A = K[u_1, \ldots, u_n] \subseteq K(u_1, \ldots, u_d) \subseteq \mathrm{Frac}(A).$$

because $K(u_1, \ldots, u_d)$ is a field. (Actually we only need it to be a ring.) We conclude that every element of A is algebraic over $K(u_1, \ldots, u_d)$, hence also over $K[u_1, \ldots, u_d]$. //

[Remark: We actually proved here that if $R \subseteq S$ is an extension of domains then the "algebraic closure" of R in S

$$\overline{R} = \{\alpha \in S : f(\alpha) = 0 \text{ for some } f(x) \in R[x]\}$$

is a subring of S. Maybe this can be done directly using resultants, but passing to the field of fractions seems more efficient.]

Q: So if $A \supseteq K$ is finitely generated then every trans. basis is finite, but do they all have the same size?

A: Yes. To prove this we need a K-algebra analogue of Steinitz Exchange.

☆ "Steinitz Exchange" for K-algebras (with no zero divisors):

Let $A \supseteq K$ be a K-algebra. Suppose that

- $\beta = \{\beta_1, \ldots, \beta_m\} \subseteq A$ is alg. ind over K
- A is algebraic over $K[\alpha_1, \ldots, \alpha_n]$.

Then $m \leq n$.

Proof: Since $\beta_1 \in A$ is alg. over $K[\alpha_1, \ldots \alpha_n]$ there is a nonzero polynomial f such that

$$f(\beta_1, \alpha_1, \ldots, \alpha_n) = 0$$

Because β is an alg. ind. set, note that some α_i must occur in this equation. WLOG suppose that α_1 occurs.

This means that α_1 is algebraic over $K[\beta_1, \alpha_2, \ldots, \alpha_n]$. Since the algebraic closure of $K[\beta_1, \alpha_2, \ldots, \alpha_n]$ in A is a ring (see above Remark) we know that $K[\beta_1, \alpha_1, \ldots, \alpha_n]$ is algebraic over $K[\beta_1, \alpha_2, \ldots, \alpha_n]$. Since A is algebraic over $K[\beta_1, \alpha_1, \ldots, \alpha_n]$ (the β_1 is not even necessary) we conclude that A is algebraic over $K[\beta_1, \alpha_2, \ldots, \alpha_n]$. (Algebraic over algebraic is algebraic. Why?)

Next since $\beta_2 \in A$ is alg. over $K[\beta_1, \alpha_2, \ldots, \alpha_n]$ there is a nonzero polynomial equation

$$g(\beta_1, \beta_2, \alpha_2, \ldots, \alpha_n) = 0$$

Again, since β is alg ind., some α_i occurs. WLOG say α_2 occurs. Then as above, $K[\beta_1, \beta_2, \alpha_2, \ldots, \alpha_n]$ is alg. over $K[\beta_1, \beta_2, \alpha_3, \ldots, \alpha_n]$. Since A is alg. over $K[\beta_1, \beta_2, \alpha_2, \ldots, \alpha_n]$ (the β_2 is not even necessary) we find that A is alg. over $K[\beta_1, \beta_2, \alpha_3, \ldots, \alpha_n]$.

If $m > n$ then by induction we find that A is algebraic over

$$K[\beta_1, \ldots, \beta_n].$$

But then β_{n+1} is algebraic over $K[\beta_1, \ldots, \beta_n]$, contradicting the fact that β is an alg. ind. set.

Hence $m \leq n$. ▨

Finally we have

☆ Corollary to Steinitz:

Let $A \supseteq K$ be a finitely generated K-algebra with no zero divisors. Then every transcendence basis of A has the same finite size.

Proof: Let α, β be two trans. bases. Applying Steinitz one way gives $|\alpha| \leq |\beta|$. Applying it the other way gives $|\beta| \leq |\alpha|$.

Hence $|\alpha| = |\beta|$. //

Since the size of a trans. basis is unique we should give it a name.

Definition:

Let $A \supseteq K$ be a f.g. K-alg. with no zero divisors let

$$tr.deg_K(A)$$

be the size of any trans. basis. We call this the transcendence degree of A over K.

Remark: Note that

$$[A:K] := \dim_K(A) \geq tr.deg_K(A)$$

because any algebraically independent set is also linearly independent. Actually we have

$$tr.deg_K(A) > 0 \implies [A:K] = \infty.$$

(α trans. $\implies 1, \alpha, \alpha^2, \ldots$ lin. ind.)

4/22/14

4/17 Lecture notes are improved.
Still no HW4 solutions
Review Thursday
Exam Thurs May 1 2–4:30 pm.

Today: The End.

Recall the analogy between linear independence and algebraic independence

Linear Algebra	Transcendence
lin. ind.	alg. ind.
$A \subseteq \text{span}(B)$	A algebraic over B
basis	trans. basis
dim	tr. deg

Now we will finish the proof of the NSS by proving

☆ Zariski's Lemma:

Let $A \supseteq K$ be a f.g. K-algebra. Then

A is a field $\Longrightarrow$ A algebraic over K.

Proof: Let A be a f.g. K-algebra so there exist $\alpha_1, \dots, \alpha_n \in A$ such that

$$K[x_1, \dots, x_n] \xrightarrow{ev} K[\alpha_1, \dots, \alpha_n] = A.$$

Let A be a field, we want to show that A is algebraic over K.

Let $\theta_1, \dots, \theta_d \in A$ be a transcendence basis so that A is algebraic over the polynomial algebra $B := K[\theta_1, \dots, \theta_d]$. We will be done if we can show that B is a field since then we have $d = 0$ hence $B = K$ and A is algebraic over K.

So consider $0 \neq \beta \in B$. Since A is a field we have $\beta^{-1} \in A$. Since A is algebraic over B there exist $b_0, b_1, \dots, b_m \in B$ such that

$$b_0 + b_1\beta^{-1} + b_2\beta^{-2} + \cdots + b_m\beta^{-m} = 0.$$

Multiply through by β^{m-1} to get

$$b_0\beta^{m-1} + b_1\beta^{m-2} + \cdots + b_{m-1}\beta^0 + b_m\beta^{-1} = 0$$

$$\Rightarrow b_m\beta^{-1} = -\left(b_m\beta^0 + \cdots + b_1\beta^{m-2} + b_0\beta^{m-1}\right) \in B.$$

We will be done if b_m is a unit in B?
But is it?

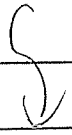
Oops. We need something stronger.
We know that

$$A \supseteq K[\theta_1, \ldots, \theta_d] = B$$

is an algebraic extension but we want it to be integral (i.e. every $a \in A$ satisfies a monic polynomial over B.)

To do this we might need to choose a "good" transcendence basis...

We will be done if we can prove



Noether Normalization:

Let $A \supseteq K$ be a f.g. K-algebra. Then there exists a transcendence basis $\theta_1, \dots, \theta_d \in A$ such that

$$A \supseteq K[\theta_1, \dots, \theta_d]$$

is an integral extension.

Proof: For simplicity we assume K is infinite (which it will be anyway if K is algebraically closed). Since A is f.g. there exist $a_1, \dots, a_n \in A$ such that

$$K[x_1, \dots, x_n] \xrightarrow{ev_a} K[a_1, \dots, a_n] = A.$$

Given any $f \in \ker(ev_a)$ we have

$$f(a_1, \dots, a_n) = 0. \qquad (*)$$

The idea is to replace $x_1, \dots, x_{n-1}$ be certain $x_1', \dots, x_{n-1}' \in K[x_1, \dots, x_n]$ so that $(*)$ becomes

a monic equation for α_n over $K[\alpha_1', \ldots, \alpha_{n-1}']$ where $\alpha_i' = ev_a(x_i')$. So we define

$$x_1' := x_1 - c_1 x_n$$
$$x_2' := x_2 - c_2 x_n$$
$$\vdots$$
$$x_{n-1}' := x_{n-1} - c_{n-1} x_n$$

for some constants $c_1, \ldots, c_{n-1} \in K$ (to be chosen later). Then (*) becomes

(**). $$f(\alpha_1' + c_1\alpha_n, \ldots, \alpha_{n-1}' + c_{n-1}\alpha_n, \alpha_n) = 0$$

Claim: for suitable choices of $c_1, \ldots, c_{n-1}$ the equation (**) is monic in α_n.

Assuming the claim, let

$$A' := K[\alpha_1', \ldots, \alpha_{n-1}']$$

By induction on n we know that there exists a transcendence basis $\theta_1, \ldots, \theta_d \in A'$ such that

$$A' \supseteq K[\theta_1, \ldots, \theta_d]$$

is an integral extension.

Then since $A = A'[\alpha_n]$ is integral over A' we conclude that

$$A \supseteq K[\theta_1, \ldots, \theta_d]$$

is integral. [Why? I'm skipping a little something here called the "determinant trick".]

Now we prove the claim. Suppose $\deg(f) = m$ and write

$$f = F_m + G \in K[x_1, \ldots, x_n]$$

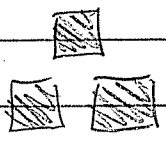
where F_m is homogeneous of degree m and $\deg(G) \leq m-1$. Then

$$f(x_1, \ldots, x_n) = f(x_1' + c_1 x_n, \ldots, x_{n-1}' + c_{n-1} x_n, x_n)$$

$$= F_m(c_1, \ldots, c_{n-1}, 1) x_n^m + (\text{lower terms})$$

Since $F_m \neq 0$ and since K is infinite we can choose the c_i such that

$$0 \neq F_m(c_1, \ldots, c_{n-1}, 1) \in K^\times.$$



That concludes the proof of the NSS.

Epilogue: The Big Picture.

Recall: If $V \subseteq K^n$ is a variety then the ideal $I(V)$ is radical (if $f^m \in I(V)$ for some m then $f \in I(V)$).

Hence the coordinate ring

$$K[V] := K[x_1, \ldots, x_n] / I(V)$$

has no nilpotents (we say $K[V]$ is reduced).

Summary: The coordinate ring of a variety is a finitely generated reduced K-algebra.

Conversely, let $A \supseteq K$ be any f.g. reduced K-algebra.

Q: Is A the coordinate ring of some variety?

A: Yes.

Since A is f.g. there exist $a_1, \ldots, a_n \in A$ such that

$$K[x_1, \ldots, x_n] \xrightarrow{\text{ev}_a} K[a_1, \ldots, a_n] = A$$

And then

$$A = K[x_1, \ldots, x_n] / I$$

where $I = \ker(\text{ev}_a)$. Since A is reduced we know that I is a radical ideal. Therefore $I = I(V)$ for some variety $V \subseteq K^n$ and hence $A = K[V]$.

Q: What does it mean to say that two varieties V, W are isomorphic?

A: We will say

$$V \approx W \iff K[V] \approx K[W]$$

as varieties $\qquad$ as K-algebras

To be precise, let A, B be f.g. reduced K-algebras, say $A = K[W]$ and $B = K[V]$.

Then given any K-algebra homomorphism

$$\Phi : K[W] \to K[V]$$

we define a function of varieties

$$f : V \to W$$

as follows. Now suppose that

$$K[W] = K[a_1, \dots, a_m] = K[x_1, \dots, x_n] / I(W)$$

We define $f_i := \Phi(a_i) \in K[V]$. Now consider the map $f : V \to K^m$ defined by

$$f(p) := (f_1(p), \dots, f_m(p)) \in K^m$$

for all $p \in V$.

Claim: $f(p) \in W$ for all $p \in V$.

$\wr$

Proof: Indeed, given any $G \in I(W) \subset K[x_1, \ldots, x_m]$ we have

$$G(a_1, \ldots, a_m) = 0 \text{ in } K[W]$$

$$\Rightarrow \Phi(G(a_1, \ldots, a_m)) = 0 \text{ in } K[V].$$

Since Φ is a K-algebra hom we have

$$\begin{aligned} 0 &= \Phi(G(a_1, \ldots, a_m)) \\ &= G(\Phi(a_1), \ldots, \Phi(a_m)) \\ &= G(f_1, \ldots, f_m) \text{ in } K[V]. \end{aligned}$$

Thus if we evaluate this function $\in K[V]$ at some $p \in V$ we get

$$\begin{aligned} 0 &= G(f_1, \ldots, f_m)(p) \\ &= G(f_1(p), \ldots, f_m(p)) \\ &= G(f(p)). \end{aligned}$$

For all $p \in V$ and $G \in I(W)$ we have $G(f(p)) = 0$. Therefore

$$f(p) \in V(I(W)) = W$$

///

Note that $f: V \to W$ is a "polynomial map" because it is defined by polynomial functions $f_1, \ldots, f_m$.

We obtain an equivalence of categories

$$\left\{\begin{array}{l}\text{varieties with} \\ \text{polynomial maps}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{f.g. reduced } K\text{-algebras} \\ \text{with } K\text{-algebra homs.}\end{array}\right\}$$

The ring $K[V]$ encodes the intrinsic properties of V independent of any particular embedding.

Theorem: Let $A = K[V]$ then

$$\dim V = \text{tr. deg}_K A.$$

Proof: Use Noether Normalization to write

$$A \supseteq K[\theta_1, \ldots, \theta_d].$$

Taking fields of fractions gives

$$\text{Frac}(A) \supseteq K(\theta_1, \ldots, \theta_d).$$

$\uparrow$

finite, separable

The Primitive Element Theorem of field theory says $\exists\ \alpha \in \mathrm{Frac}(A)$ separable over $K(\theta_1, \dots, \theta_d)$ such that

$$\mathrm{Frac}(A) = K(\theta_1, \dots, \theta_d, \alpha).$$

The equation $f(\alpha) = 0$ with

$$f(x) = K[\theta_1, \dots, \theta_d, x]$$

means V is isomorphic (on an open dense subset) to a hypersurface in K^{d+1}. Hence

$$\dim V = d = \mathrm{tr.deg}_K A.$$

THE END.