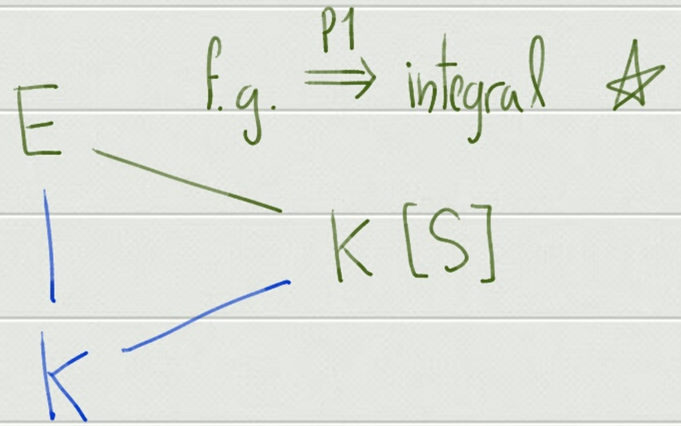
Lecture 15 Proof of Hilbert's Nullstellensatz

Theorem 3 (Zariski's lemma) If E/K is a field extn then

$$E = K[x_1, \ldots, x_n] \Rightarrow [E:K] < \infty$$

Proof

By the Noether normalisation lemma, $\exists$ finite Al $S \subseteq E$ s.t.



$(E \text{ is a field } \& \text{ ☆}) \overset{L2}{\Rightarrow} K[S] \text{ is a field} \Rightarrow K[S] = K \Rightarrow [E:K] < \infty$ □

The above thm was proved by Zariski.* It may be regarded as a generalisation of the basic fact that whenever $x \in E$ is s.t. $K[x] = E$, where E / K is a field extn, then the K-algebra homomorphism

$$K[X] \longrightarrow K[x]$$

$$f(X) \longmapsto f(x)$$

has nontrivial kernel and thus $[E : K] = \deg\left(p_{x/K}(X)\right) < \infty$.

---

* Zariski, O., *A new proof of Hilbert's Nullstellensatz*, Bulletin of the American Mathematical Society 53, pp 362-368, 1947.

Recall that for each ideal $I \subseteq K[X_1, \ldots, X_n]$ we have the algebraic set

$$V(I) := \{P \in \mathbb{A}^n \mid \forall f \in I : f(P) = 0\},$$

and for each subset $V \subseteq \mathbb{A}^n := \overline{K}^n$ we defined the ideal

$$\mathcal{I}(V) := \{f \in K[X_1, \ldots, X_n] \mid \forall P \in V : f(P) = 0\},$$

which is s.t. $\operatorname{rad}(\mathcal{I}(V)) = \mathcal{I}(V)$, where

$$\operatorname{rad}(I) = \{x \in R \mid \exists n \in \mathbb{Z}_{>0} : x^n \in I\}$$

is known as the *radical* of the ideal I of a ring R, itself an ideal of R.

Lemma 4 We have a canonical isomorphism

$$R_f \xrightarrow{\sim} R[T]/\langle fT-1\rangle$$

Proof

Any ring homomorphism $\sigma : R \to S$ s.t. $\varphi(f) =: f^\sigma \in S^\times$ extends uniquely to a ring homomorphism

$$R[T] \xrightarrow{\tau} S$$

$$F(T) \mapsto F^\sigma\left(\frac{1}{f^\sigma}\right)$$

where

$$F(T) = a_d T^d + a_{d-1} T^{d-1} + \dots + a_0 \in R[T]$$

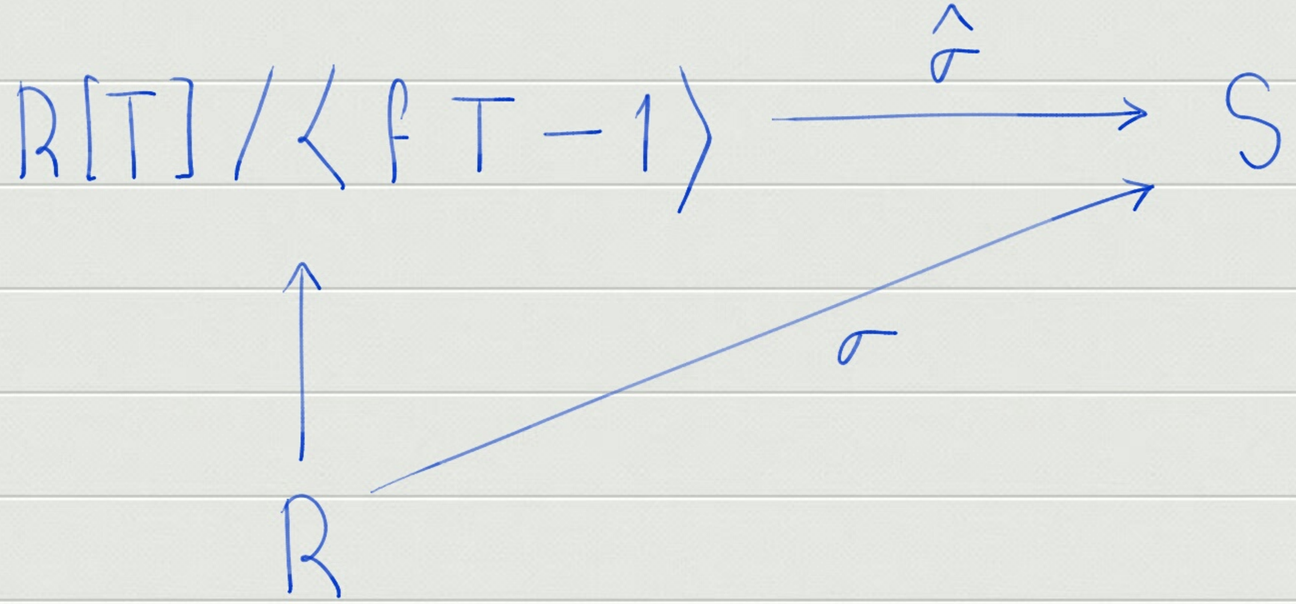
and

$$F^\sigma(T) := a_d^\sigma T^d + a_{d-1}^\sigma T^{d-1} + \dots + a_0^\sigma \in R^\sigma[T].$$

Since $f(T-1) \in \ker(\tau)$, we have a commutative diagram

$$\begin{array}{ccc} R[T] & \xrightarrow{\tau} & S \\ \downarrow{\scriptstyle \pi_f} & & \uparrow{\scriptstyle \hat{\tau}} \\ R[T]/\langle f(T-1)\rangle & \xrightarrow{\kappa} & R[T]/\ker(\tau) \end{array}$$

Thus $\hat{\sigma} := \hat{\tau} \circ \kappa$ is the unique ring homomorphism that makes



commute, i.e. $R[T]/\langle fT-1\rangle$ satisfies the same universal property as R_f, so $R_f \cong R[T]/\langle fT-1\rangle$ canonically.

Thm 4 The following are equivalent

(i) $\forall\ I \subseteq K[X_1, \ldots, X_n] : \mathcal{I}(\mathcal{V}(I)) = \mathrm{rad}(I)$

(ii) $\forall\ I \subseteq K[X_1, \ldots, X_n] : \mathcal{V}(I) = \emptyset \Rightarrow I = K[X_1, \ldots, X_n]$

(iii) $\forall$ field extn $E/K : E = K[x_1, \ldots, x_n] \Rightarrow [E : K] < \infty$

Proof

(i) $\Rightarrow$ (ii) : Let

$$\mathcal{I}_{rad,\,/K} := \{ I \text{ ideal of } K[X_1, \ldots, X_n] \mid \mathrm{rad}(I) = I \}.$$

Recall that $\mathrm{rad}(\mathcal{I}(V)) = \mathcal{I}(V)$ and also that $\mathcal{V}(\mathcal{I}(V)) = V$,

so we have an injective, inclusion reversing map

$$\mathcal{A}_{/K} \longrightarrow \mathcal{Y}_{\mathrm{rad},/K}$$

$$V \longmapsto \mathcal{I}(V)$$

Here $\mathcal{A}_{/K} := \{ \text{algebraic sets } V \subseteq \mathbb{A}^n \mid V \text{ is defined } /K \}$. So $\forall\, I \in \mathcal{Y}_{\mathrm{rad},/K}$

$$\mathcal{I}(\mathcal{V}(I)) \overset{(i)}{=} \mathrm{rad}(I) = I$$

Hence the above map is also onto and thus $\mathcal{V}(I) = \emptyset$ implies that $I = K[X_1, \ldots, X_n]$, that is (ii).

(ii) $\Rightarrow$ (i): We'll use Rabinowitsch's argument as in Mathoverflow.

It suffices to show that $\forall\, f \in I(V(I))\ \exists\, n \in \mathbb{Z}_{>0}$ s.t. $f^n \in I$.

Note that $f^n \in I \iff \underbrace{(K[X_1, \ldots, X_n]/I)_{\bar{f}} = 0}$

$\cong$ lemma 4

$$K[X_1, \ldots, X_n, T] / \langle I, fT - 1 \rangle$$

Claim We have $V(\langle I, fT-1\rangle) = \emptyset$, so by (ii)

$$\langle I, fT - 1 \rangle = K[X_1, \ldots, X_n, T].$$

and (i) follows.

Proof of claim

Suppose that $V(\langle I, fT-1\rangle) \neq \emptyset$. So there is a point

$$(x_1, \ldots, x_n, t) \in V(\langle I, fT-1\rangle),$$

thus

$$f(x_1, \ldots, x_n)\, t - 1 = 0.$$

Recall that $f \in I(V(I))$, so $f(x_1, \ldots, x_n) = 0$. Hence

$$-1 = 0,$$

which is absurd. So $V(\langle I, fT-1\rangle) = \emptyset$ and the claim follows.

(iii) $\Rightarrow$ (ii): By Zorn's lemma, $\forall$ ideal $I \subsetneq K[X_1, \dots, X_n]$

$\exists$ a maximal ideal $\mathfrak{m}$ s.t. $I \subseteq \mathfrak{m}$. Thus

$$K[X_1, \dots, X_n]/\mathfrak{m} = K[\xi_1, \dots, \xi_n] =: E$$

By (iii) we know that $[E : K] < \infty$.

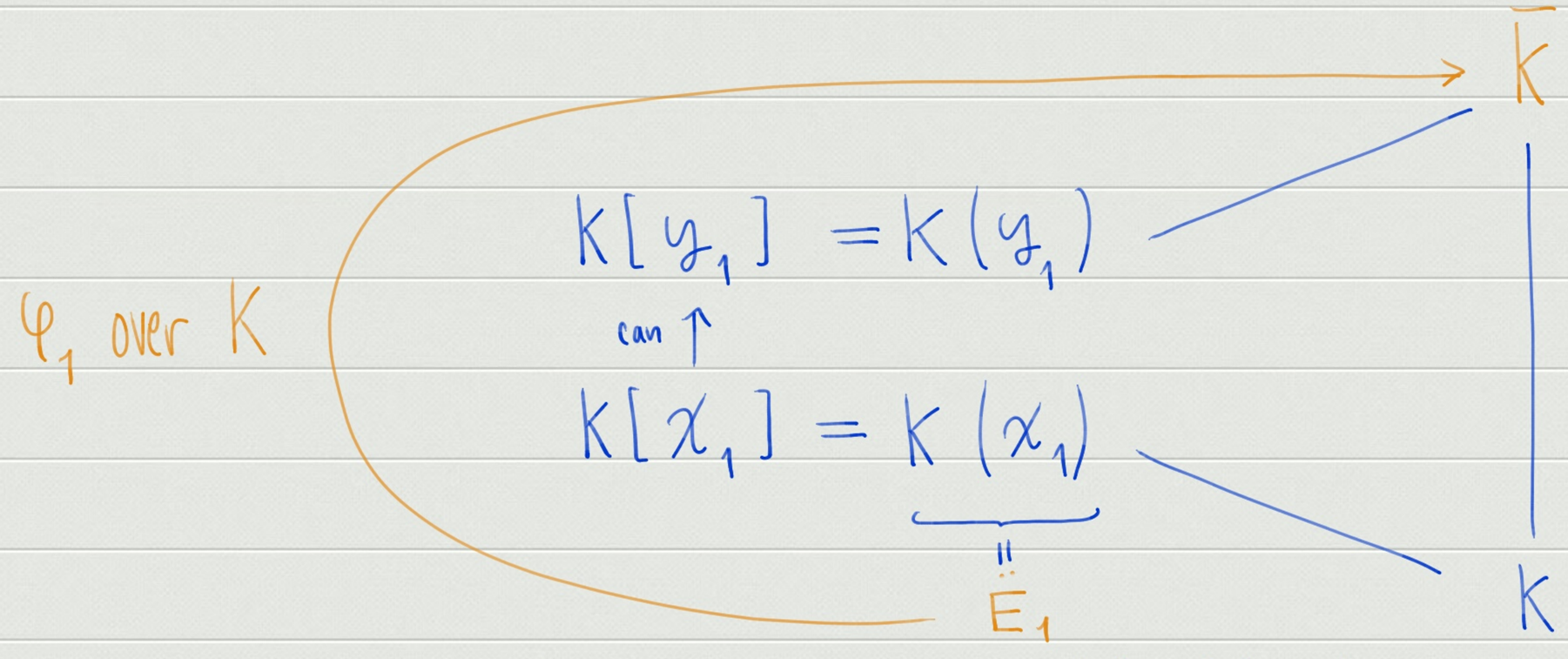
Claim There is an embedding $E \xrightarrow{\varphi} \bar{K}$ over K and

$$P := (\varphi(\xi_1), \dots, \varphi(\xi_n)) \in V(\mathfrak{m}) \subseteq V(I).$$

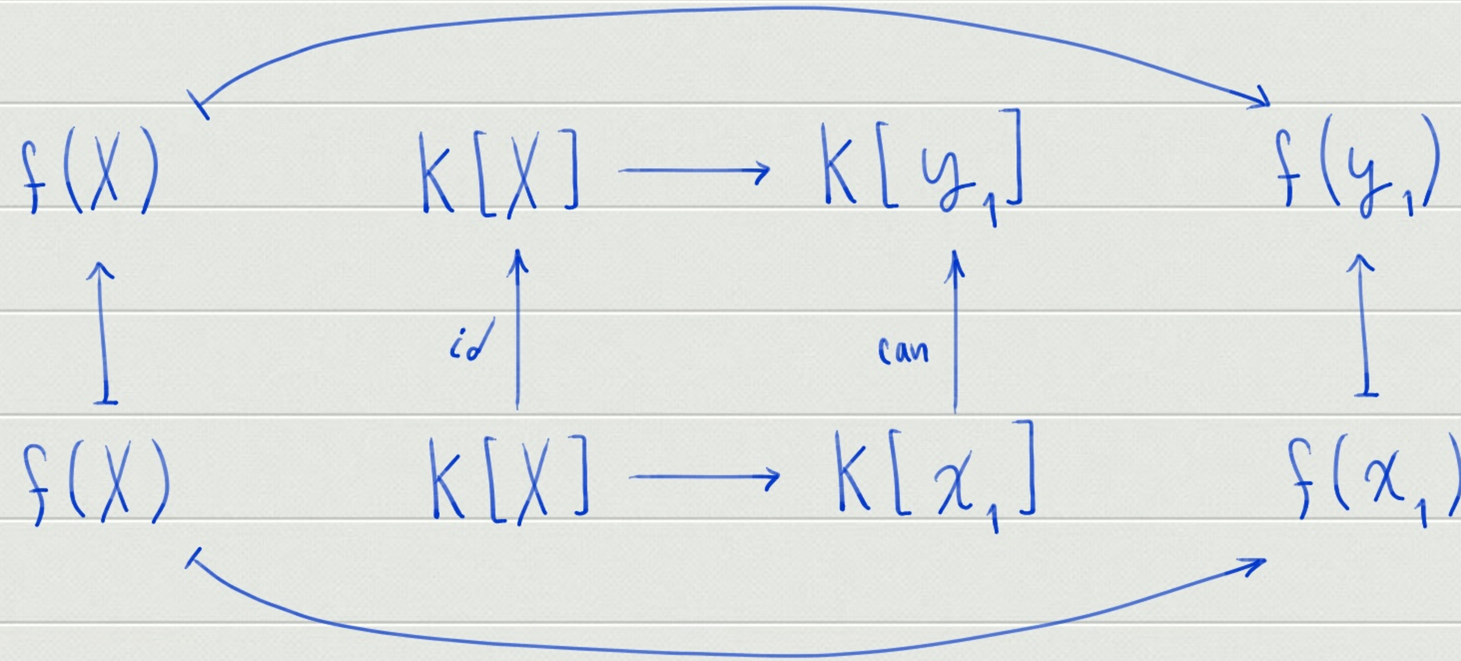
So in particular, $V(I) \neq \emptyset$, i.e. (ii) follows.

Proof of claim

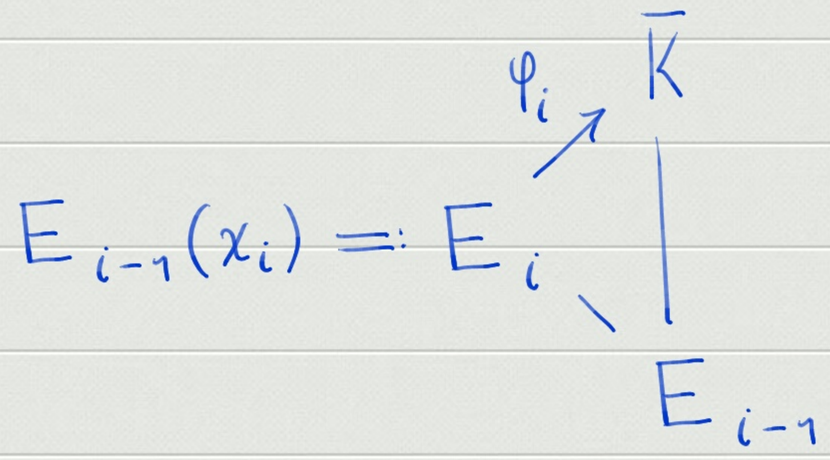
As $[E:K] < \infty$, there is $x_1 \in E$ algebraic over K. WLOG $P_{x_1/K}(X) \in K[X]$ has degree $d_1 > 1$. There is $y_1 \in \overline{K}$ s.t. $P_{x_1/K}(y_1) = 0$



where the vertical arrow is the canonical map defined by the commutativity of



So φ_1 is indeed a K-algebra homomorphism. Thus inductively define $\varphi_2 / E_1, \ldots$ by



As $[E:K] < \infty$, eventually $E_i = E$ and $\varphi_i =: \varphi : E \longrightarrow \overline{K}$ over K. Thus

$$\forall \; g = \sum_I a_I X_1^{\alpha_1} \cdots X_n^{\alpha_n} \in \mathfrak{m} \quad \text{we have}$$

$$g(P) = \sum_I a_I \, \varphi(\xi_1)^{\alpha_1} \cdots \varphi(\xi_n)^{\alpha_n}$$

$$= \varphi\left(\sum_I a_I \, \xi_1^{\alpha_1}, \ldots, \xi_n^{\alpha_n} \right)$$

$$= (\varphi \circ \pi)\left(\sum_I a_I X_1^{\alpha_1} \cdots X_n^{\alpha_n} \right)$$

$$= 0 \; .$$

and the claim follows.

(ii) $\Rightarrow$ (iii) : Suppose we have a field ext'n E / K s.t. $E = K[x_1, \ldots, x_n]$.

The kernel $m := \ker(\psi)$ of the ring homomorphism

$$K[X_1, \ldots, X_n] \xrightarrow{\psi} K[x_1, \ldots, x_n]$$

$$f(X_1, \ldots, X_n) \mapsto f(x_1, \ldots, x_n)$$

is a maximal ideal, so by (ii) there exists a point

$$P = (y_1, \ldots, y_n) \in V(m)$$

We have a ring isomorphism

$$K[y_1, \dots, y_n] \xrightarrow{\kappa} K[x_1, \dots, x_n]$$

$$f(y_1, \dots, y_n) \mapsto f(x_1, \dots, x_n)$$

Indeed,

$$\kappa\left(f(y_1, \dots, y_n)\right) = 0,$$

$$f(x_1, \dots, x_n) = 0,$$

$$f(X_1, \dots, X_n) \in \mathfrak{M},$$

$$f(y_1, \dots, y_n) = 0.$$

But $y_1, \dots, y_n \in \overline{K}$, so $K[y_1, \dots, y_n]$ is a field extn of K of finite degree, so is its isomorphic image $K[x_1, \dots, x_n]$. Thus (iii) follows $\square$

We have thus described a proof of the followin.

Theorem (Hilbert*) For each ideal $I \subseteq K[X_1, \ldots, X_n]$

$$\mathcal{I}(\mathcal{V}(I)) = \mathrm{rad}(I).$$

So we have a bijective, inclusion reversing map

$$\begin{array}{ccc} \mathcal{A}_{/K} & \longrightarrow & \mathcal{I}_{rad,/K} \\ V & \longmapsto & \mathcal{I}(V) \end{array}$$

---

* Hilbert, D., Ueber die vollen Invariantsysteme, Mathematische Annalen, Band 42, pp. 313-337, 1893.