III Transcendental field extensions.

Def 81: (transcendence basis)
Let $K|F$ be a field extension

a) An element $x \in K$ is called *transcendental* over F if x is *not* algebraic over F.

b) A finite set $S = \{x_1, \dots, x_n\}$ of K is called *algebraically independent* over F if

$$\forall f \in F[X_1, \dots, X_n] \setminus \{0\}: f(x_1, \dots, x_n) \neq 0.$$

c) A subset S of K is called algebraically independent over F if

$$\forall T \subseteq S, |T| < \infty: \; T \text{ alg. indep. over } F.$$

d) A subset S of K is called transcendence basis of $K|F$ if

(TB1) S is algebraically independent over F

and (TB2) $K|F(S)$ is algebraic.

Remark 82: In Def 81 c) the set S is algebraically independent over F iff

$\forall b \in S$: $F(S)|F(S \setminus \{b\})$ is not algebraic.

Example 83: a) Suppose $K|F$ is algebraic. Then $S = \emptyset$ is a transcendence basis of $K|F$

b) $K = \overline{\mathbb{Q}}(X)$, $F = \mathbb{Q}$

Claim: $\{X\}$ is a transcendence basis of $K|F$.

Pf: Put $L := \overline{\mathbb{Q}(X)}^K$.

Then $X \in L$ and $\overline{\mathbb{Q}} \subseteq L$ as every elt. of $\overline{\mathbb{Q}}$ is alg. over $\mathbb{Q}$, so also over $\mathbb{Q}(X)$.

Thus $K = L$. □

c) $\{X\}$ is a transcendence basis of $K = \mathbb{Q}(X)|\mathbb{Q}$

Question: Are there elts. $b, c \in K$, $b \neq c$, such that $\{b, c\}$ is algebraically independent?

Answer: No

Proof: We write a for X, so $K = \mathbb{Q}(a)$ and $\{a\}$ is a transcendence basis of $K|\mathbb{Q}$.

b has the form $b = \frac{f(X)}{g(X)} \notin \mathbb{Q}$ with polynomials

$$f(X) = a_0 + a_1 X + \dots + a_N X^N$$
$$g(X) = b_0 + b_1 X + \dots + b_N X^N$$

$\in \mathbb{Q}[X]$, s.t. $a_N \neq 0$ or $b_N \neq 0$

Thus a satisfies

$$0 = b\,g(a) - f(a)$$
$$= \sum_{j=0}^{N} (b\,b_j - a_j)\, a^j$$

Note that $b\,b_N - a_N \neq 0$, or a is algebraic over $\mathbb{Q}(b)$.

Thus $K = \mathbb{Q}(a) = \mathbb{Q}(b)[a] \,|\, \mathbb{Q}(b)$ is algebraic

Thus c is alg. over $\mathbb{Q}(b)$.

Thus $\{b, c\}$ is not alg. ind. $\square$

Example: For $b = \frac{1}{X}$, $c = \frac{1}{X+1}$.

$\{b, c\}$ is alg. dependent over $\mathbb{Q}$

as $h(T,S) = T - S - TS \in \mathbb{Q}[T,S]$ satisfies

$$h(b,c) = 0.$$

Theorem 84: Let $K|F$ be a field extension. Then

a) $K|F$ has a transcendence basis

b) The transcendence bases of $K|F$ share the cardinality.

as $h(T,S) = T - S - TS \in \mathbb{Q}[T,S]$
satisfies

$$h(b,c) = 0.$$

Theorem 84: Let $K|F$ be a field extension. Then

a) $K|F$ has a transcendence basis

b) The transcendence bases of $K|F$ share the cardinality.

Proof: a) Just take an inclusion maximal alg. independent $/F$ subset of K.

b) We only prove it for the case that $K|F$ is finitely generated. Then it has a finite transcendence basis $\{x_1, \dots, x_m\}$. Take one with minimal m.

Let $\{w_1, \dots, w_n\}$ be algebraically independent over F.
We want to show $n \le m$.

Case 1: $m = 0$. $\Rightarrow$ K / F alg.
$\Rightarrow n = 0 \le m$.

Case 2: $m \ge 1$. $w_1, x_1, \dots, x_m$ is alg. dep.
$\Rightarrow \exists\, f(W, X_1, \dots, X_m) \in F[W, X_1, \dots, X_m]$ irreducible : $f(w_1, x_1, \dots, x_m) = 0$.

$\{w_i\}$ alg. indep. $\Rightarrow \exists_{1 \le j \le m} : \deg_{X_j} f \ge 1$.

W.l.o.g. $j = 1$. Thus f has the form

$$f(W, \underline{X}) = \sum_{j=0}^{N} g_j(W, X_2, \dots, X_m) X_1^j$$

with $g_N \neq 0$ and $N \ge 1$.

Claim: $g_N(w_1, x_2, \dots, x_m) \neq 0$.

Proof: Otherwise $\exists\, h \in F[W, X_2, \dots, X_m]$ irreducible : $h(w_1, x_2, \dots, x_m) = 0$ and $\deg_W h \ge 1$.

(The latter, because $\{x_2, \dots, x_m\}$ is alg. indep.)

Put $L := F(x_1, \dots, x_m)$.
Then $f(W, x), h(W, x)$ are two irred. polynomials in $L[W]$ having w_1 as a root.
Thus $\exists\, \varphi, \psi \in F[X_1, \dots, X_m]$, $\psi \neq 0$, $\gcd = 1$:

$$f(W, x) = \frac{\varphi(x)}{\psi(x)} \cdot h(W, x_2, \dots, x_m)$$

$$\Rightarrow \psi(x) f(W, x) = \varphi(x) h(W, x_2, \dots, x_m)$$

$$\Rightarrow \psi(\underline{X}) f(W, \underline{X}) = \varphi(\underline{X}) h(W, X_2, \dots, X_m)$$

$L[W] \simeq F[W, \underline{X}]$

Then $\Psi \mid h$ in $F[W, \underline{X}]$,
as $\gcd(\Psi, \varphi) = 1$,
and by $\deg_W h \geq 1$ and $\deg_W \Psi = 0$
and h irred in $F[W, \underline{X}]$, we get

$\Psi \in F^\times$.

Similarly $\varphi \in F^\times$.

So $\exists \lambda \in F^\times$: $f = \lambda h$
But $\deg_{X_1} f \geq 1 > 0 = \deg_{X_1} h$. $\lightning$

□

Claim $\Rightarrow$ x_1 alg. / $F(w_1, x_2, \dots, x_m)$

Thus $\{w_1, x_2, \dots, x_m\}$ is a transcendence basis of $K|F$.

Induction step: Suppose after relabeling $x_1, \dots, x_m$, for an $m \geq r \geq 1$, we have that

$\{w_1, \dots, w_r, x_{r+1}, \dots, x_m\}$
is a transcendence basis of $K|F$.
Then $\exists f \in F[W_1, \dots, W_r, W, X_{r+1}, \dots, X_m]$
irred
$f(w_1, \dots, w_{r+1}, x_{r+1}, \dots, x_m) = 0$

$\{w_1, \dots, w_{r+1}\}$ is alg. indep.

$\Rightarrow \exists_{r+1 \leq j \leq m}$ $\deg_{X_j} f \geq 1$.

Now follow the proof of the base case, to see that

x_j is alg. over $F(w_1, \dots, w_{r+1}, x_{r+1}, \dots, \hat{x}_j, \dots, x_m)$

Thus $\{w_1, \dots, w_{r+1}, x_{r+1}, \dots, \hat{x}_j, \dots, x_m\}$
is a transcendence basis of $K|F$.

This finishes the proof of Case 2.

□

Rk 85: The proof for $K|F$ with no finite transcendence basis is an exercise.

Def 86: The cardinality of a transcendence basis of $K|F$ is called transcendence degree.

Example 87: a) $\deg_{tr}(\mathbb{Q}(\mathbb{X})|\mathbb{Q}) = 1$

b) $\deg_{tr}(\mathbb{C}|\mathbb{Q}) > |\mathbb{N}|$.

c) Let F be a field
$\deg_{tr,F}(F(X_1,\dots,X_m)) = m$.

d) Let $K|F$ be algebraic.
Then
$\deg_{tr}(K(X_1,\dots,X_m)|F) = m$.

III 2. Noether normalization

Recall from III 1. For a finitely generated field extension $K|F$ we found elements $x_1,\dots,x_m$ s.t.

$K|F(x_1,\dots,x_m)$ is alg. and
$F(x_1,\dots,x_m) \cong F(X_1,\dots,X_m)$
$\parallel$
$Q(F[X_1,\dots,X_m])$.

Question 88: Can we generalize this result to a finitely generated ring extension over F?
Answer: Yes!

Theorem 89 (Noether normalization)
Let F be a field and $\mathcal{B}|F$ be an integral domain finitely generated over F.
Then $\exists_{m\in\mathbb{N}_0}\, \exists x_1,\dots,x_m \in \mathcal{B}$: $\mathcal{B}|F[x_1,\dots,x_m]$ is integral
and $\{x_1,\dots,x_m\}$ is alg. indep. $/F$.

Rk 90: Note the difficulty is the following question.
Let $\{x_1, \dots, x_m\}$ be max alg. indep. set in B.
Is $B \mid F[x_1, \dots, x_m]$ integral?
(We know that
$Q(B) \mid F(x_1, \dots, x_m)$ is algebraic.)

Example 91: F a field.

$$B := F[X, \tfrac{1}{X}] \subseteq F(X).$$

Take $x := X$.
Then $B \mid F[x]$ is not integral,
but $Q(B) \mid Q(F[x])$ is algebraic.
$\quad\;\; F(x) \qquad F(x)$

Let's find $\{x_1\}$ alg. ind. $/F$ such that $B \mid F[x_1]$ is integral.

Take $h(S,T) \in F[S,T] \setminus \{0\}$ s.t.
$h(x, \frac{1}{x}) = 0$.

$h(S,T) = ST - 1$.
So $(x, \frac{1}{x})$ satisfies $ST - 1 = 0$

Put $\tilde{T} := T - S^{\ell}$. Then
$(x, \frac{1}{x} - x)$ satisfies $S(\tilde{T} + S^{\ell}) - 1 = 0$

i.e. $S^{\ell+1} + S\tilde{T} - 1 = 0$.
E.g. for $\ell = 1$:

$$x^2 + (\tfrac{1}{x} - x)x - 1 = 0$$

Thus x is integral over $F[\frac{1}{x} - x]$

$\{\frac{1}{x} - x\}$ is alg. indep. as
$$\overline{F}^{F(X)} = F.$$

Thus $\{\frac{1}{x} - x\}$ is a desired set.
Rk 92: Let's call this Noether basis (not standard)

Proof of Thm 89:

B is generated as a E-algebra by finitely many elements, say

$$B = F[e_1, \dots, e_m]$$

Case 1: $\{e_1, \dots, e_m\}$ is alg. indep. Then we are done.

Case 2: Suppose $\{e_1, \dots, e_m\}$ is not alg. indep.

$\Rightarrow f \in F[X_1, \dots, X_m] \setminus \{0\}$:

$$f(e_1, \dots, e_m) = 0.$$

Put $z_1 := e_1$ and $z_i := e_i - e_1^{\ell_i}$
$i \in \{2, \dots, m\}$, $\ell_i \in \mathbb{N}$.

- We want to choose $\ell_2, \dots, \ell_m$ s.t.

$$f(z_1, z_2 + z_1^{\ell_2}, z_3 + z_1^{\ell_3}, \dots, z_m + z_1^{\ell_m})$$

$$= \lambda z_1^N + (\text{lower degree terms in } z_1),$$

$\lambda \in F^\times$. If we were successful, then

z_1 is integral over $F[z_2, \dots, z_m]$.

Then we continue with an induction.

- So we need to find suitable $\ell_2, \dots, \ell_m \in \mathbb{N}$.

Put $d := 1 + \deg f$.

We have

$$f(X_1, \dots, X_m) = \sum_{\underline{i} \in I} a_{\underline{i}} \underline{X}^{\underline{i}}$$

Put $J := \{\underline{j} \in \mathbb{N}_0^m \mid a_{\underline{j}} \neq 0\}$

Note: For $\underline{j} \in J$ we have

$$j_1 + \dots + j_m < d.$$

Put $l_1 := 1$, $l_2 := d$, $l_3 := d^2$, ..., $l_m := d^{m-1}$.

Then for $\underline{i}, \underline{j} \in \mathcal{I}$ we have

$$\underline{i} \cdot \underline{l} = \underline{j} \cdot \underline{l} \iff \underline{i} = \underline{j},$$

by using the d-adic expansion of positive integers.

Take $\underline{I} \in \mathcal{I}$, s.t. $\underbrace{\underline{i} \cdot \underline{l}}_{=:N}$ is maximal

Then $f(b_{1,1}, \dots, b_m) = \Delta x_1^N + \text{lower terms}$

for some $\Delta \in F^\times$. $\square$

One application is Hilbert's Nullstellensatz:

Thm 93 (HNS) Let F be an alg. closed field and $\mathfrak{A} \subsetneq F[X_1, \dots, X_m]$ be an ideal. Then $\exists\, \underline{x} = (x_1, \dots, x_m) \in F^m$: $\forall_{f \in \mathfrak{A}}$: $f(\underline{x}) = 0$.

Proof: Take $\mathfrak{M} \in \operatorname{Specm}(F[\underline{X}])$, s.t. $\mathfrak{M} \supseteq \mathfrak{A}$.

$K := F[\underline{X}]/\mathfrak{M}$ | F is a field extension, s.t. K is a f.g. F-algebra.

Noether normalization $\Rightarrow$

$\exists_{\ell \in \mathbb{N}_0}\, \exists\, k_1, \dots, k_\ell \in K$: $K \mid F[k_1, \dots, k_\ell]$ is integral and $F[k_1, \dots, k_\ell] \cong F[T_1, \dots, T_\ell]$.

Lem 70 $\Rightarrow$ $F[k_1, \dots, k_\ell]$ is a field

$\Rightarrow \ell = 0$.

F alg. closed $\overset{\ell=0}{\Rightarrow}$ $K = F$

Thus $\exists a_1, \dots, a_m \in F$:
$X_i \equiv_{\mathfrak{M}} a_i$, $i = 1, \dots, m$.

Thus $\mathfrak{M} = (X_1 - a_1, \dots, X_m - a_m)_{F[\underline{X}]}$.

Thus $\forall f \in \mathfrak{A}: f(\underline{a}) = 0$

□

HNS has several equivalent formulations

The next 4 Theorems are equivalent to HNS.

Thm 94 (HNS2)
Let F be a field and A be a f.g. F algebra and $\varphi: F \to L$ be a field embedding into an alg. closed field.
Then φ can be extended to A.

Thm 95 (HNS3) Let F be a field A be a f.g. F-algebra Suppose A is a field. Then $A|F$ is algebraic.

Thm 96: (HNS4)
Let F be a field, $\mathfrak{A} \subseteq F[X_1, \dots, X_n]$ be an ideal and f an element of $F[X_1, \dots, X_n]$, s.t.

$$\forall \underline{x} \in V(\mathfrak{A}) : f(\underline{x}) = 0.$$

Then $\exists k \in \mathbb{N}: f^k \in \mathfrak{A}$.

Recall: $V(\mathfrak{A}) := \{\underline{x} \in \overline{F}^m \mid \forall g \in \mathfrak{A}: g(\underline{x}) = 0\}$, the algebraic set of $\mathfrak{A}$.

We prove 94, 95 and 96 in showing that they are equivalent to 93.

Proof: HNS ⇒ HNS 2:

We have $A \hookrightarrow \bar{F} \otimes_F A =: \bar{A}$
$a \longmapsto 1 \otimes_F a$,
as $\bar{F}$ is an F v.s.
Extend φ to $\bar{F}$, by $\bar{F}|F$ being algebraic, see Proof of Lem 14 and use Zorn.

Thus w.l.o.g. $F = \bar{F}$.
Take a ring homomorphism
$\pi : F[X_1, \dots, X_m] \twoheadrightarrow A = F[a_1, \dots, a_m]$
· $\pi|_F = id_F$
· $\pi(X_i) = a_i$.

and put $\mathfrak{M} := \ker(\pi)$.
Then $1 \notin \mathfrak{M}$ and, by HNS, $V(\mathfrak{M}) \neq \emptyset$. Take $x \in V(\mathfrak{M})$

Define $\varphi_A : A \longrightarrow L$ via
$\varphi_A(\pi(f)) := \varphi(f(x))$

· well-def: $\pi(f) = \pi(g) \Rightarrow f - g \in \mathfrak{M}$
$\Rightarrow (f-g)(x) = 0 \Rightarrow \varphi(f(x)) = \varphi(g(x))$.

· $\varphi_A|_F = \varphi$ ✓
· φ_A is a ring hom. ✓

HNS 2 ⇒ HNS 3: Take $\varphi_A : A \to L$ from HNS 2, for $\varphi = id_F$ and $L = \bar{F}$.
A is a field ⇒ φ_A is injective
⇒ $A|F$ is algebraic.

HNS 3 ⇒ HNS: exercise

HNS ⇒ HNS 4: (Rabinowitsch trick)
Let $\tilde{\mathfrak{M}} \subseteq F[X, Y]$ be the ideal generated by $\mathfrak{M}$ and $1 - Y \cdot f$.

Claim: $\widetilde{\mathfrak{a}} = F[\underline{X}, Y]$.

Pf: Assume $\widetilde{\mathfrak{a}} \neq 1$.
By HNS and Homework 4.3.(i), the ideal $\widetilde{\mathfrak{a}}$ has a zero in F^{m+1}, say $(\underline{x}, y)$

$\Rightarrow \quad \underline{x} \in V(\mathfrak{a})$ and $1 - y f(\underline{x}) = 0$ ↯

as $f(\underline{x}) = 0$. □

Claim $\Rightarrow \exists_{\ell \in \mathbb{N}_0} \exists\, g_i \in F[\underline{X}, Y]$, $i = 0, \dots, e$: $\exists\, h_i \in \mathfrak{a}$, $i = 1, \dots, e$:

$$1 = g_0(\underline{X}, Y) \cdot (1 - Y f(\underline{X})) + \sum_{i=1}^{e} g_i(\underline{X}, Y) h_i(\underline{X})$$

Substitute $\frac{1}{f}$ for Y (if $f \neq 0$) and multiply with f^k for k big enough.

$\Rightarrow f^k \in \mathfrak{a}$.

HNS4 $\Rightarrow$ HNS: exercise

□ (equiv.)

Note that even without the exercises we have proven HNS 2, 3, 4.

Example 97: $\mathbb{C}^2 \supseteq W$ an affine line

$W = \{(x, y) \in \mathbb{C}^2 \mid ax + by = c\}$
$(a, b, c \in \mathbb{C})$

Suppose $g \in \mathbb{C}[X, Y]$ satisfies $g|_W \equiv 0$.

Then $(c - aX - bY) \mid g$.

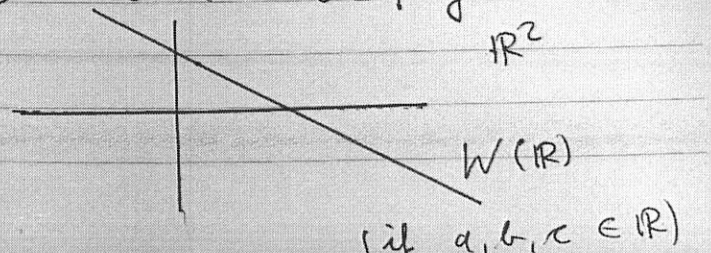
Proof: $\mathfrak{a} := (c - aX - bY)$ ideal in $\mathbb{C}[X, Y]$

HNS 4 $\Rightarrow \exists_{k \in \mathbb{N}}$: $g^k \in \mathfrak{a}$.

$c - aX - bY$ is irred and $\mathbb{C}[X, Y]$ UFD

$\Rightarrow$ $c - aX - bY$ prime element.

$\Rightarrow$ $c - aX - bY \mid g$ □



(if $a, b, c \in \mathbb{R}$)

Define $\varphi_A : A \longrightarrow L$ via
$\varphi_A(\pi(f)) := \varphi(f(x))$.

· well-def: $\pi(f) = \pi(g) \Rightarrow f - g \in \mathfrak{M}$
$\Rightarrow (f-g)(x) = 0 \Rightarrow \varphi(f(x)) = \varphi(g(x))$.

· $\varphi_A|_F = \varphi$. ✓
· φ_A is a ring hom. ✓

HNS2 $\Rightarrow$ HNS3: Take $\varphi_A : A \to L$ from HNS2, for $\varphi = id_F$ and $L = F$.
A is a field $\Rightarrow$ φ_A is injective
$\Rightarrow$ $A|F$ is algebraic.

HNS3 $\Rightarrow$ HNS: exercise

HNS $\Rightarrow$ HNS4: (Rabinowitsch trick)
Let $\tilde{\mathfrak{M}} \subseteq F[\underline{X}, Y]$ be the ideal generated by $\mathfrak{M}$ and $1 - Y \cdot f$.

Claim: $\widetilde{\mathfrak{A}} = F[\underline{X}, Y]$.

Pf: Assume $\widetilde{\mathfrak{A}} \neq 1$.
By HNS and homework 4.3.(i), the ideal $\widetilde{\mathfrak{A}}$ has a zero in F^{m+1}; say $(\underline{x}, y)$

$\Rightarrow$ $\underline{x} \in V(\mathfrak{A})$ and $1 - y f(\underline{x}) = 0$ ↯

as $f(\underline{x}) = 0$. □

Claim $\Rightarrow \exists_{\ell \in \mathbb{N}_0} \exists\, g_i \in F[\underline{X}, Y]$, $i = 0, \dots, \ell$: $\exists\, h_i \in \mathfrak{A}$, $i = 1, \dots, \ell$:

$$1 = g_0(\underline{X}, Y) \cdot (1 - Y f(\underline{X})) + \sum_{i=1}^{\ell} g_i(\underline{X}, Y) h_i(\underline{X})$$

Substitute $\frac{1}{f}$ for Y (if $f \neq 0$) and multiply with f^k for k big enough.

$\Rightarrow f^k \in \mathfrak{A}$.

HNS4 $\Rightarrow$ HNS: exercise

□ (equiv.)

Note that even without the exercises we have proven HNS 2, 3, 4.

Example 97: $\mathbb{C}^2 \supseteq W$ an affine line

$W = \{(x, y) \in \mathbb{C}^2 \mid ax + by = c\}$
$(a, b, c \in \mathbb{C})$

Suppose $g \in \mathbb{C}[X, Y]$ satisfies $g|_W \equiv 0$.

Then $(c - aX - bY) \mid g$.

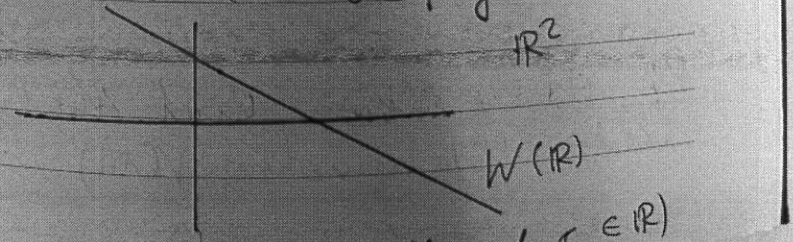
Proof: $\mathfrak{A} := (c - aX - bY)_{\mathbb{C}[X,Y]}$ ideal in $\mathbb{C}[X, Y]$

HNS 4 $\Rightarrow \exists_{k \in \mathbb{N}}$: $g^k \in \mathfrak{A}$.

$c - aX - bY$ is irred and $\mathbb{C}[X, Y]$ UFD

$\Rightarrow$ $c - aX - bY$ prime element.

$\Rightarrow$ $c - aX - bY \mid g$ □



Example 98 Consider $\mathfrak{a}$ the ideal in $\overline{\mathbb{Q}}[X,Y]$ generated by the polynomial X^2+Y^2+1.

$$\mathfrak{a} = \{ f(X,Y)\cdot(X^2+Y^2+1) \mid f \in \overline{\mathbb{Q}}[X,Y] \}$$

$$V(\mathfrak{a}) = \{(x,y)\in\overline{\mathbb{Q}}^2 \mid x^2+y^2=-1\}$$
$$= \{(ix,iy) \mid x,y\in\overline{\mathbb{Q}},\ x^2+y^2=1\}$$
$$\ni (0,i)$$

But $V(\mathfrak{a})\cap\mathbb{Q}^2=\emptyset$, i.e. $V(\mathfrak{a})$ has no "$\mathbb{Q}$-points".

Def: Let R be a ring and $\mathfrak{a}$ an ideal in R.

$$\sqrt{\mathfrak{a}} := \{ r\in R \mid \exists_{m\in\mathbb{N}}\ r^m\in\mathfrak{a}\}$$
"radical of $\mathfrak{a}$"

Rk HNS4 claims that the biggest ideal in $F[\underline{X}]$ vanishing $V(\mathfrak{a})$ is $\sqrt{\mathfrak{a}}$.

IV Algebraic spaces

IV 1. Notations and first properties for algebraic sets

In this chapter we fix a field extension $L=L/k$ and a positive integer n.

Remark 99: This includes $k=L$ and L/k non-algebraic.

Notation 100: Let $S\subseteq k[\underline{X}_1,\dots,\underline{X}_n]$. We write $V(S)$ for the set of its zeros in L^n. (This depends on L and n!)

$$V(S) := \{ \underline{x}\in L^n \mid \forall_{f\in S}\ f(\underline{x})=0\}$$

A subset of L^n of this form is called a k-algebraic set.