$\mathbb{A}^n_k \qquad k[x_1, \dots, x_n]$

$$\begin{array}{ccc} I: \ X & \longrightarrow & I(X) \\ \cap\!| & & \cap\!| \\ \mathbb{A}^n_k & & k[x_1 \dots x_n] \end{array}$$

I is a map from $I: \mathcal{P}(\mathbb{A}^n_k) \longrightarrow \mathcal{P}(k[x_1 \dots x_n])$

$S \subseteq k[x_1 \dots x_n] \rightsquigarrow V(S) \subseteq \mathbb{A}^n_k$

$V: \mathcal{P}(k[x_1, \dots, x_n]) \longrightarrow \mathcal{P}(\mathbb{A}^n_k)$

$S \longrightarrow V(S)$

1) V, I reverse inclusions

2) $Y \subseteq \mathbb{A}^n \Rightarrow V(I(Y)) \supseteq Y$

$\alpha \subseteq k[x_1 \dots x_n] \Rightarrow I(V(\alpha)) \supseteq \alpha$

3) $V(I(Y)) = \overline{Y}$ Zariski closure of Y

What is $I(V(\alpha))$? or $I(V(S))$?

$\forall X \subseteq \mathbb{A}^n \quad \therefore I(X)$ is a radical ideal

$\forall \alpha \subseteq k[x_1 \dots x_n] \quad \alpha \subseteq I(V(\alpha))$ radical ideal

$$\boxed{\sqrt{\alpha} \subseteq \sqrt{I(V(\alpha))} = I(V(\alpha))}$$

Theorem of zeros of D. Hilbert - Nullstellensatz

Assume that K is an algebraically closed field $\Longrightarrow$

for any $\alpha \subseteq K[x_1, \dots x_n]$, $\boxed{I(V(\alpha)) = \sqrt{\alpha}.}$

This is the "strong" form of the Nullstellensatz.

1) The assumption "K algebraically closed" is necessary.

2) We will give a proof using the Normalization Lemma of Emmy Noether!

1) K is algebraically closed $\Longleftrightarrow$ every polynomial of positive degree in $K[x]$ has a zero in K

K is not alg. closed $\Longrightarrow \exists\ F \in K[x]$, $\deg F = d \geq 1$, s.t. $V(F) \subseteq A^1_K$ is empty $\therefore V(F) = \emptyset$

$I(V(F)) = I(\emptyset) = K[x]$

$\langle F \rangle$ Factorize F in irreducible factors:

$F = F_1^{m_1} \cdots F_r^{m_r} \Longrightarrow \exists$ an irreducible polynom. F s.t.

$V(F) = \emptyset \Longrightarrow \langle F \rangle$ is a maximal ideal

$\Longrightarrow \sqrt{\langle F \rangle} = \langle F \rangle$ because $\langle F \rangle \subseteq \sqrt{\langle F \rangle}$

$\alpha \ni 1 \Longleftrightarrow \sqrt{\alpha} \ni 1$

$\alpha = \langle F \rangle$ $\qquad \boxed{\sqrt{\alpha} = \langle F \rangle \subsetneq I(V(\alpha)) = K[x]}$

K field $\quad K \subseteq E \quad E$ field, K subfield of E

Ex. $K = \mathbb{Q}$, $E = \mathbb{R}$; $K = \mathbb{R}$, $E = \mathbb{C}$ ...; ...

K, $E = \overline{K}$

consider a family of elements of E $\{z_i\}_{i \in I}$

Def. The family $\{z_i\}_{i\in I}$ is algebraically free over K, or the elements z_i are algebraically independent over K, if in the polynomial ring $K[X_i]_{i\in I}$ there are no non-zero polynomials vanishing in the family $\{z_i\}_{i\in I}$

If $F \in K[X_i]_{i\in I}$ s.t. $F(z_i) = 0 \Longrightarrow F = 0$

$\{z_i\}_{i\in I}$ $\quad E$ can be interpreted as a K-vector space

linearly indep. : there is no non-zero polynom. F of degree 1 homogeneous in $K[X_i]_{i\in I}$ s.t. $F(z_i)_{i\in I} = 0$

$\{z_i\}$ algebraically indep. $\Longrightarrow$ linearly indep.

Examples 1) $\{z\}$ family of one element: z alg. indep.
if $F \in K[X]$ s.t. $F(z)=0 \Rightarrow F=0$.
$K \subseteq E \ni z$ This means that z transcendental element over K

For ex. $\pi \in \mathbb{R}$: transc. over $\mathbb{Q}$

2) π, π^2 both transcendental over $\mathbb{Q}$, but $\{\pi, \pi^2\}$ is not alg. indep. over $\mathbb{Q}$: $\mathbb{Q}[X_1, X_2] \ni F(X_1, X_2)$ s.t. $F(\pi, \pi^2) = 0$? $F = X_1^2 - X_2 \in \mathbb{Q}[X_1, X_2]$, $F(\pi, \pi^2) = 0$

π, π^2 are alg. dependent over $\mathbb{Q}$, but they are linearly independent over $\mathbb{Q}$: λ, μ
$\lambda \pi + \mu \pi^2 = 0 \Longrightarrow \lambda = \mu = 0$

3) $\emptyset$ is a free family over any field.

4) $z_1, \dots, z_n \in E$ $\varphi : K[X_1, \dots, X_n] \longrightarrow E$
$F \longmapsto F(z_1, \dots, z_n)$

φ is a ring homom.: $\operatorname{Ker} \varphi = \{F \mid F(z_1, \dots, z_n) = 0\}$
$z_1, \dots, z_n$ are algebraically indep. $\Longleftrightarrow \operatorname{Ker} \varphi = (0) \Longleftrightarrow$
$K[X_1, \dots, X_n] \cong \varphi(K[X_1, \dots, X_n])$

$\varphi(K[x_1 \dots x_n]) = K[z_1, \dots, z_n] \subseteq E$ subring: the minimal subring of E containing K and $z_1, \dots, z_n$

$z_1, \dots, z_n$ are alg. indep. $\Longleftrightarrow$ $K[z_1, \dots, z_n] \simeq K[x_1 \dots x_n]$

We can construct a theory of bases and dimension for the notion of algebraically indep elements over K which is analogous to the theory for linearly indep. elements.

<u>BASES</u> $K \subseteq E$ Consider $\mathcal{S} = \{$families of elements of E algebraically indep over $K\} \ni \emptyset$

$\Rightarrow \mathcal{S} \neq \emptyset$ $\mathcal{S} \subseteq \mathcal{P}(E)$ non empty

We want to prove that $\mathcal{S}$ has maximal elements w.r. respect to inclusion: we can apply Zorn lemma:

Zorn's Lemma: if S is partially ordered and inductive, then S has maximal elements.

INDUCTIVE: for every chain of elements of S, $a_1 \le a_2 \le \dots \le a_r \le \dots$: $\exists\, a \in S$

$a_r \le a \quad \forall r \ge 1$

$\mathcal{S}$: $\mathcal{Q}_1 \subseteq \mathcal{Q}_2 \subseteq \dots \subseteq \mathcal{Q}_r \subseteq \dots$ chain in $\mathcal{S}$

Look for $\mathcal{Q} \in \mathcal{S}$ s.t. $\mathcal{Q} \supseteq \mathcal{Q}_r$, $\forall r \ge 1$

$\mathcal{Q} = \bigcup_{i \ge 1} \mathcal{Q}_i$: Claim: $\mathcal{Q}$ belongs to $\mathcal{S}$ i.e. the elements of $\mathcal{Q}$ are alg. indep. over K

If $\exists\, F \in K[x_i]_{i \in I}$, $F \ne 0$, $F(z_i) = 0$ for $\{z_i\}_{i \in I} = \mathcal{Q}$: F involves only a finite number of variables $\Rightarrow \exists\, \underline{z_1, \dots, z_n} \in \mathcal{Q}$ alg. depend.

$\Rightarrow \exists\, \mathcal{Q}_i$ in the chain s.t. $z_1, \dots, z_n \in \mathcal{Q}_i$: <u>contradiction</u>

Conclusion: $\mathcal{S}$ has maximal elements.

$\mathcal{S}$ has maximal elements : <u>transcendence bases</u> of E over K

$\mathcal{B} \subseteq E$

<u>Thm.</u> Two transcendence bases of E over K have the same cardinality i.e. are in bijection.

Transcendence degree of E over K: tr. d. E/K

<u>Def.</u> K A K-algebra is a ring A containing K

$K \subseteq A$. More in general, a K-algebra is a ring containing a field isomorphic to K.

$K \subseteq E$, $z_1, \dots, z_n \in E$ $A = K[z_1, \dots, z_n]$ is the minimal subring of E containing K and $z_1 \dots, z_n$: is a K-algebra: the K-algebra generated by $z_1 \dots, z_n$

$K \subseteq A$: A is a finitely generated K-algebra if $\exists\, z_1 \dots z_n \in A$ $A = K[z_1, \dots, z_n]$

Proposition
$K, z_1 \dots z_n$

$K \subseteq E = K(z_1, \dots, z_n)$ minimal field containing
$= Q(K[z_1 \dots z_n])$
E is generated as a field by $z_1 \dots z_n$

Then there is a transcendence basis of E over K contained in $\{z_1 \dots z_n\}$.

Pf. $S = \{$subsets of $\{z_1 \dots z_n\}$ formed by alg. indep. elements over $K\} \neq \emptyset$

S is a finite set $\Rightarrow$ it has maximal elements
We can assume that $z_1, \dots, z_r$ are alg. indep over K and a maximal element in $S \Rightarrow \forall z_{r+1}, \dots, z_n$
$z_1 \dots z_r, z_i$ are alg. depend.
$\exists F \in K[X_1 \dots X_{r+1}]$ s.t. $F(z_1 \dots z_r, z_i) = 0$, $F \neq 0$
$K(z_1 \dots z_r)[X] \Rightarrow z_i$ is algebraic

over $K(z_1 \dots z_r) \Rightarrow K(z_1 \dots z_r, z_i)$ is an algebraic extension. Repeat $\Rightarrow K(z_1 \dots z_n) = E$ is an algebraic extension of $K(z_1 \dots z_r)$
$\Rightarrow \{z_1 \dots z_r\}$ is maximal in the set of all alg. indep. subsets of $E \Rightarrow$ a transc. basis.

The transcendence degree of $E = K(z_1 \ldots z_n)$ is finite and $\leq n$: $\operatorname{tr.d.} K(z_1 \ldots z_n)/K \leq n$.

Algebra over a ring : $A \subseteq B$ rings, A subring of B

We say that B is an A-algebra.

More in general: an A-algebra is a ring containing a subring isomorphic to A

For ex. $\varphi : A \longrightarrow B$ ring homom., φ injective

$\Rightarrow \varphi(A) \subseteq B$, $\varphi(A) \simeq A \Longrightarrow B$ is an A-algebra

$A \subseteq B$ $\quad b \in B$

<u>Def.</u> b is integral over A if b is a root of a <u>monic</u> polynomial of $A[x]$: $\exists\, a_1, \ldots, a_n \in A$ st.

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

$$(x^n + a_1 x + \cdots + a_n)(b) = 0$$

If b is integral over $A \Rightarrow b$ is algebraic over A. The converse is not always true.

If A is a field, b is algebraic over A $\Longrightarrow$ b is integral over A

$$(a_0 x^n + a_1 x^{n-1} + \text{———} + a_n)(b) = 0$$ polyn. of degree n

$a_0 \neq 0$

a_0^{-1} exists in A if A is a field

$\Rightarrow$ $a_0^{-1}(a_0 x^n + \text{———} + a_n)$ is monic and vanishes at b

<u>Ex.</u> $\underset{A}{\overset{\shortparallel}{\mathbb{Z}}} \subseteq \underset{B}{\overset{\shortparallel}{\mathbb{Q}}}$ $b \in \mathbb{Q}$: when is b integral over $\mathbb{Z}$?

when is b algebraic over $\mathbb{Z}$?

$b = \frac{m}{n}$ $(nx - m)(b) = 0$

b is integral over $\mathbb{Z}$ $\Longrightarrow$ $b \in \mathbb{Z}$

Normalization Lemma.

A K-algebra : finitely generated integral domain $\quad A = K[y_1, \dots, y_n]$

$Q(A) = K(y_1, \dots, y_n) \qquad \operatorname{tr.d.} Q(A)/K = r \quad (\leq n)$

Then ~~there~~ exist $z_1, \dots, z_r \in A$, algebraically independent over K, s.t. A is integral over $K[z_1, \dots, z_r]$ i.e. each element ~~of~~ of A is integral over $K[z_1, \dots, z_r]$.