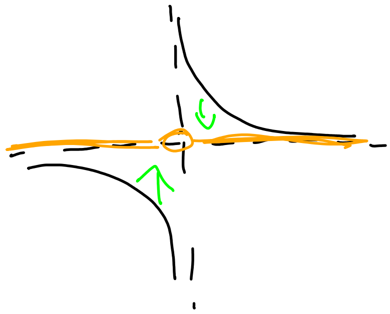
Warmup

$\mathbb{R}\setminus\{0\} \subseteq \mathbb{R}$ isn't an algebraic subset



$\{(x,y)\in\mathbb{R}^2 \mid xy=1\}$ is an algebraic subset of $\mathbb{R}^2$ and the projection onto the x-axis is $\mathbb{R}\setminus\{0\}$.

Rmk For any ideal J of $K[x_1,\dots,x_n]$, we have $I(V(J)) \supseteq \sqrt{J}$.

Thm 2.11 (Hilbert's Nullstellensatz)

Assume that K is algebraically closed. Then, $I(V(J)) = \sqrt{J}$ for any ideal J of $K[x_1,\dots,x_n]$.

Exe If $n=1$, $J=(f)$ with

$f = c(x-a_1)^{e_1}\cdots(x-a_r)^{e_r}$, then

$V(J) = \{a_1,\dots,a_r\}$,

$I(V(J)) = ((x-a_1)\cdots(x-a_r)) = \sqrt{(f)}$.

Rmk The Thm is wrong if K is not algebraically closed.

Pf Let $f \in K[x]$ be any irreducible pol. of degree ≥ 2.

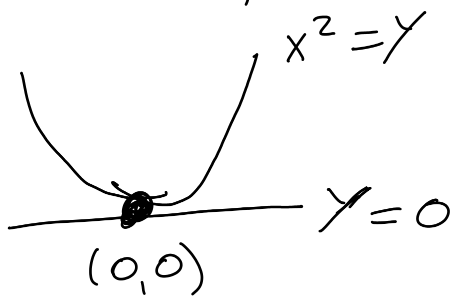
$\Rightarrow f$ has no roots in K: $V(f) = \emptyset$

$\Rightarrow I(V(f)) = K[x]$.

But $\sqrt{(f)} = (f) \neq K[x]$. $\square$

Ex $n = 2$, $J = (x^2, Y) = (x^2 - Y, Y)$

$V(J) = \{(0,0)\}$.



$I(V(J)) = \{f \in K[x,y] \mid f(0,0) = 0\} = (X, Y)$
$= \sqrt{J}$.

Cor 2.12 If K is algebraically closed, we get bijections

$$\{\text{radical ideal } J \subseteq K[x_1, \dots, X_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{alg. subset of } K^n\}$$

which are each other's inverse.

Cor 2.13 (Weak Nullstellensatz)

If $J \subsetneq K[x_1, \dots, x_n]$, then $V(J) \neq \emptyset$.

Pf using Hilbert's Nsts

If $V(J) = \emptyset$, then

$$\sqrt{J} = I(V(J)) = I(\emptyset) = K[x_1, \dots, x_n].$$

$$\Rightarrow \underbrace{1}_{\text{constant polynomial}} \in \sqrt{J} \Rightarrow \underbrace{1^n}_{=1} \in J \text{ for some } n \geq 1$$

$$\Rightarrow J = K[x_1, \dots, x_n]. \qquad \square$$

Thm 2.14 (Nichtnullstellensatz)

We have $I(K^n) = 0$.

Pf using Hilbert's Nsts

$$I(K^n) = I(V(0)) = \sqrt{0} = 0. \qquad \square$$

Rmk Thm 2.14 holds for any infinite (not necessarily algebraically closed) field K.

Pf Use induction over n.

$n=0$: clear.

$n=1$: nonzero polynomials have only finitely many roots, and therefore have a non-root in K.

$n-1 \to n$: Let $0 \neq f \in K[X_1, \dots, X_n]$.

Write $f(X_1, \dots, X_n) = \sum_{i=0}^{d} g_i(X_1, \dots, X_{n-1}) \cdot X_n^i$

with $g_i \in K[X_1, \dots, X_{n-1}]$, $g_d \neq 0$.

By induction, there exist $(a_1, \dots, a_{n-1}) \in K^{n-1}$ such that $g_d(a_1, \dots, a_{n-1}) \neq 0$.

$\Rightarrow 0 \neq f(a_1, \dots, a_{n-1}, X_n) \in K[X_n]$ (it has degree d).

By the $n=1$ case, there exists $a_n \in K$ such that $f(a_1, \dots, a_{n-1}, a_n) \neq 0$. $\square$

Rmk The weak Nsts implies Hilbert's (strong) Nsts.

Pf "$I(V(J)) \supseteq \sqrt{J}$" done earlier

"$I(V(J)) \subseteq \sqrt{J}$"

Let $f \in I(V(J))$.

$\Rightarrow \forall P \in V(J): f(P) = 0$.

$\Rightarrow \{P \in V(J) \mid f(P) \neq 0\}^{\subseteq K^n} = \emptyset$.

We have a bijection

$$\{P \in V(J) \mid f(P) \neq 0\} \longleftrightarrow \{(P,t) \in \underbrace{V(J) \times K}_{\subseteq K^{n+1}} \mid f(P) \cdot t = 1\}$$

$$= V(J') \subseteq K^{n+1}$$

where $J' \subseteq K[X_1, \dots, X_n, T]$ is the ideal generated by the elements of J and by the polynomial $f(X_1, \dots, X_n) \cdot T - 1$.

$LHS = \emptyset \Rightarrow RHS = V(J') = \emptyset$

$\Rightarrow J' = K[X_1, \dots, X_n, T]$.

weak Nsts

$\Rightarrow 1 \in J'$

$\Rightarrow$ We can write

$$1 = \sum_{i=0}^{d} p_i(x_1, \dots, x_n) \cdot T^i + (f(x_1, \dots, x_n) \cdot T - 1) \cdot q(x_1, \dots, x_n, T)$$

with $p_i \in J$, $q \in K[x_1, \dots, x_n, T]$.

$$1 = \sum_{i=0}^{d} p_i \cdot T^i + (f \cdot T - 1) q$$

Plug in $T = \frac{1}{f}$:

$$1 = \sum_{i=0}^{d} p_i \cdot \frac{1}{f^i}. \quad (\text{in } K(x_1, \dots, x_n)).$$

$$\Rightarrow f^d = \underbrace{\sum_{i=0}^{d} \underbrace{\underbrace{p_i}_{\in J} \cdot \underbrace{f^{d-i}}_{\in K[x_1, \dots, x_n]}}_{\in J}} \in J$$

$\Rightarrow f \in \sqrt{J}$. $\square$

2.5. Ring and field extensions

<u>Def</u> Let R be a ring. A <u>ring extension</u> of R is a ring S containing R as a subring.

<u>Rmk</u> A ring extension of R is also an R-module.

<u>Def</u> Let K be a field. A <u>field extension</u> of K is a field L containing K as a subfield.

<u>Rmk</u> A field ext. of K is also a ring ext. of K and a K-vector space ($=K$-module).

<u>Def</u> Let S be a ring extension of R. The ring extension generated by a subset A of S is the smallest (= inclusion-minimal) subring $R[A]$ of S containing R and A.

<u>Rmk</u> $R[A]$ is the set of sums of products of the form $r \cdot a_1 \cdots a_m$ with $r \in R$ and $a_1, \dots, a_m \in A$.

Rmk Take $A = \{a_1, \dots, a_n\}$.

$R[A]$ is the image of the R-algebra homomorphism

$$\begin{aligned} R[X_1, \dots, X_n] &\longrightarrow S. \\ r \in R &\longmapsto r \\ X_i &\longmapsto a_i \end{aligned}$$

Def Let L be a field extension of K. The field extension generated by a subset A of L is the smallest subfield $K(A)$ of L containing K and A.

Rmk $K(A)$ is the quotient field of the ring extension $K[A]$ generated by A.

Ex $R[X_1, \dots, X_n]$ is a ring extension of R generated by $X_1, \dots, X_n$.

Ex $K(X_1, \dots, X_n)$ is a field extension of K generated by $X_1, \dots, X_n$.

Rmk We now have three notions of being finitely generated:

- fin. generated as a module: $\exists a_1, \dots, a_n$: every el. can be written as a sum of terms ra_i with $r \in R$.
  ((module-) finite)

- fin. generated as a ring extension: $\exists a_1, \dots, a_n$ every el. can be written as a sum of products $r a_1^{e_1} \cdots a_n^{e_n}$ with $r \in R$, $e_i \geq 0$.
  (ring-finite)

- fin. generated as a field extension: $\exists a_1, \dots, a_n$: every el. can be written as the quotient of two such sums
  (field-finite)

Rmk module-finite

$$\Downarrow$$

ring-finite

$$\Downarrow$$

field-finite

However:

Rmk module-finite

$$\not\Uparrow$$

ring-finite

Pf $\mathbb{C}[X]$ is a finitely generated ring ext. of $\mathbb{C}$,

but not a finitely generated $\mathbb{C}$-module

($=\mathbb{C}$-vector space).

Basis: $1, X, X^2, \dots$ $\square$

Rmk ring-finite

$$\not\Uparrow$$

field-finite

Pf $\mathbb{C}(X)$ is a finitely generated field ext. of $\mathbb{C}$,

but not a fin. generated ring ext. of $\mathbb{C}$.

Assume $\mathbb{C}(X) = \mathbb{C}[a_1, \dots, a_n]$.

Write $a_i(X) = \dfrac{p_i(X)}{q_i(X)}$ with $p_i, q_i \in \mathbb{C}[X]$,

$q_i \neq 0$.

Let $t \in \mathbb{C}$ be not a root of $q_1(X) \cdots q_n(X)$.

By assumption, we can write

$$\mathbb{C}(X) \ni \frac{1}{X-t} = \sum_j c_j \left(\frac{p_1(X)}{q_1(X)} \right)^{e_{1,j}} \cdots \left(\frac{p_n(X)}{q_n(X)} \right)^{e_{n,j}}$$

with $c_j \in K$, $e_{i,j} \geq 0$.

Multiply by $X-t$ and sufficiently large powers of $q_1(X), \ldots, q_n(X)$.

Plug in $X = t$.

$\Rightarrow$ LHS $\neq 0$, RHS $= 0$ $\lightning$ $\square$