<u>Thm 2.22</u> Any <u>ring</u>-finite <u>field</u> extension L of a field K is <u>module-finite</u> (= finite-dimensional K-vector space).
($\Rightarrow L$ is an algebraic extension of K).

<u>Pf</u> Let $L = K[a_1, \dots, a_n]$.

Use induction:

<u>$n=1$:</u> $L = K[a_1]$

If a_1 is algebraic, we're done.
If it isn't, then $1, a_1, a_1^2, \dots \in L$ are linearly independent over K.
$\Rightarrow$ The ring homomorphism

$$\begin{aligned} K[X] &\longrightarrow K[a_1] = L \\ X &\longmapsto a_1 \end{aligned}$$

is an isomorphism.
But $K[X]$ isn't a field!

<u>$n-1 \to n$:</u> Note that $L = K(a_1)[a_2, \dots, a_n]$.
$\Rightarrow$ By the induction hypothesis, the field extension $L = K(a_1)[a_2, \dots, a_n]$ of $K(a_1)$ is module-finite.

If a_1 is algebraic over K, then
$K(a_1) = K[a_1]$ is a module-fin. ext. of K.
Since L is a module-fin. ext. of $K(a_1)$,
L is a module-finite ext. of K.

If a_1 isn't algebraic over K:

$$K(a_1) = \text{field of fractions of } K[a_1]$$
$$\cong \quad \text{—— " ——} \quad \text{of } K[X]$$
$$= K(X).$$

The elements $a_2, \dots, a_n \in L$ are algebraic over $K(a_1) \cong K(X)$.
By Lemma 2.16, we can (for $i = 2, \dots, n$) write $a_i = \frac{p_i}{q_i}$ with $p_i \in L$ integral over $K[a_1] \cong K[X]$ and $0 \neq q_i \in K[a_1] \cong K[X]$.
Now, proceed as in the proof that the extension $\mathbb{C}(X)$ of $\mathbb{C}$ isn't ring-finite (cf. section 2.5):
The ring $K[a_1] \cong K[X]$ contains ∞ many maximal ideals ($\cong$ monic irreducible polynomials).

$\Rightarrow$ There exists $r \in K[a_1] \cong K[X]$ relatively prime to $q_2, \dots, q_n$.

Since $\frac{1}{r} \in L = K[a_1, \dots, a_n] = K(a_1)[a_2, \dots, a_n]$, we can write

$$\frac{1}{r} = \sum_j c_j \, a_2^{e_{2,j}} \cdots a_n^{e_{n,j}} \quad \text{with } c_j \in K[a_1], \ e_{ij} \geq 0.$$

$$\frac{1}{r} = \sum_j c_j \left(\frac{p_2}{q_2}\right)^{e_{2,j}} \cdots \left(\frac{p_n}{q_n}\right)^{e_{n,j}}$$

Multiply by large enough powers of $q_2, \dots, q_n$ to clear out denominators on the RHS.

$\Rightarrow$ Since $c_j \in K[a_1]$ and $p_2, \dots, p_n$ integral over $K[a_1]$, and since the integral closure of $K[a_1]$ in L is a ring, the RHS is then integral.

But $\text{LHS} = \dfrac{q_2^{\cdots} \cdots q_n^{\cdots}}{r} \in K(a_1) \setminus K[a_1]$

$$\cong$$

$$K(X) \setminus K[X]$$

isn't integral over $K[a_1] \cong K[X]$ by Thm 2.15. $\square$

2.7. Proof of Hilbert's Nullstellensatz

It only remains to prove the weak Nullstellensatz:

<u>Thm 2.23 (= Cor 2.13)</u> Assume K is algebraically closed. For any ideal $J \subsetneq K[X_1,\dots,X_n]$, we have $V(J) \neq \emptyset$.

<u>Pf</u> We can assume w.l.o.g. that J is a maximal ideal of $K[X_1,\dots,X_n]$.

$\Rightarrow L = K[X_1,\dots,X_n]/J$ is a field.

Consider L a field extension K. It is generated by the images of $X_1,\dots,X_n$ in L.

$\Rightarrow$ ring-finite field ext.

$\underset{\text{Thm 2.22}}{\Rightarrow}$ module-finite $\Rightarrow$ algebraic

$\Rightarrow L = K$. In other words, the map

$$\begin{aligned} K &\longrightarrow L = K[X_1,\dots,X_n]/J \\ c &\longmapsto c \bmod J \end{aligned}$$

is an isomorphism. Let $a_i \in K$ be the preimage of $(X_i \bmod J) \in L$.

$$\Rightarrow \quad X_i - a_i \in J \qquad \forall i = 1, \dots, n$$

$$\Rightarrow J' := (X_1 - a_1, \dots, X_n - a_n) \subseteq J$$

But J' is a maximal ideal of $K[X_1, \dots, X_n]$ because

$$K[X_1, \dots, X_n]/J' \cong K$$
$$X_i \longleftrightarrow a_i$$

$$\Rightarrow \quad J = J' \Rightarrow V(J) = V(J') = \{(a_1, \dots, a_n)\}.$$

$J' \subseteq J$ are max. id.

$\square$

The kernel of the ring homomorphism

$$K[X_1, \dots, X_n] \longrightarrow K$$
$$X_i \longmapsto a_i$$

is the set of polynomials $f(X_1, \dots, X_n)$ such that $f(a_1, \dots, a_n) = 0$, which is the ideal $J' = (X_1 - a_1, \dots, X_n - a_n)$.

From now on, we'll always assume that the field K is algebraically closed.

(unless stated otherwise ...)

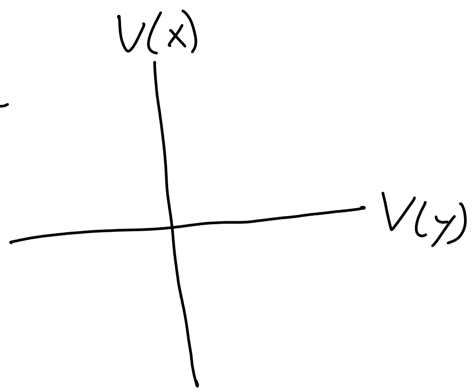
2.8. Irreducibility

Def An algebraic set $\emptyset \neq X \subseteq K^n$ is *irreducible* if you can't write $X = X_1 \cup X_2$ with any algebraic sets $X_1, X_2 \subsetneq X$. Otherwise, it's *reducible*.

Ex Any one-point set $X = \{p\}$ is irreducible.

Ex $V(XY) \subseteq K^2$ is reducible

$$\begin{array}{c} V(XY) \\ \shortparallel \\ V(X) \cup V(y) \end{array}$$



Ex $K \subseteq K^1$ is irreducible.

Ex $V(X), V(y) \subseteq K^2$ are irreducible.

Thm 2.24 An algebraic subset $X \subseteq K^n$ is irreducible if and only if $I(X)$ is a prime ideal of $K[X_1,\dots,X_n]$.

Pf Recall that $X \neq \emptyset \underset{\text{Weak Nullstellensatz}}{\Longleftrightarrow} V(I) \neq K[X_1,\dots,X_n]$.

"$\Rightarrow$" Assume $I(X) \overset{\neq K[X_1,\dots,X_n]}{}$ is not a prime ideal.

$\rightsquigarrow$ Let $f,g \notin I(X)$, but $fg \in I(X)$.

$$f,g \notin I(X) \;\Rightarrow\; V(f), V(g) \not\supseteq X \;\Rightarrow\; X \cap V(f),\, X \cap V(g) \subsetneq X$$

$$fg \in I(X) \;\Rightarrow\; V(f) \cup V(g) = V(fg) \supseteq X \;\Rightarrow\; X = \underbrace{(X \cap V(f))}_{} \cup \underbrace{(X \cap V(g))}_{\text{algebraic subsets of } X}$$

"$\Leftarrow$" Assume $X = X_1 \cup X_2$, $X_1, X_2 \subsetneq X$ algebraic subsets.

$$\Downarrow$$

$$I(X_1), I(X_2) \supsetneq I(X)$$

Let $f_i \in I(X_i) \setminus I(X)$. $\Rightarrow f_i(P) = 0 \;\forall P \in X_i$

Since $X = X_1 \cup X_2$, this implies $(f_1 f_2)(P) \;\forall P \in X$

$\Rightarrow f_1 f_2 \in I(X) \Rightarrow I(X)$ not prime. $\square$

Cor 2.25 $V(J) \subseteq K^n$ is irreducible if J is a prime ideal.

Pf Recall that $I(V(J)) = \sqrt{J}$ by Hilbert's Nullstellensatz.

But $\sqrt{J} = J$ for any prime ideal:

If $f^n \in J$, then $f \in J$. $\square$

Rmk $(X^2) \subseteq K[X]$ is not a prime ideal, but $V(x^2) = V(x) = \{0\}$ is irreducible.

Ex $V(x) \subseteq K^2$ is irreducible because (x) is a prime ideal of $K[X,Y]$ because $K[X,Y]/(X) \cong K[Y]$ is an integral domain

$$X \mapsto 0$$

Lemma/Reminder 2.26 If R is a unique factorization domain (such as $\mathbb{Z}$, $K[X_1, \dots, X_n]$), then (f) is a prime ideal if and only if $f \in R$ is irreducible.

__Exe__ $V(X^2+Y^2-1) \subseteq \mathbb{C}^2$ is irreducible because $X^2+Y^2-1 \in \mathbb{C}[X,Y]$ is.

__Pf__ Assume $X^2+Y^2-1 = f(X,Y)\cdot g(X,Y)$ for some nonconstant polynomials $f(X,Y), g(X,Y) \in \mathbb{C}[X,Y]$. Since X^2+Y^2-1 has degree 2 in X, either a) both $f(X,Y)$ and $g(X,Y)$ have degree 1 in X, or

b) one of them (say $f(X,Y)$) has degree 0 in X, the other has degree 2 in X.

Case b) is impossible: If $f(X,Y) = f(Y)$ depends only on Y, take some root $b \in \mathbb{C}$ of $f(Y)$. Then, $a^2+b^2-1 = f(b)\cdot g(a,b) = 0 \quad \forall a \in \mathbb{C}$.

(false)

Hence, $f(X,Y)$ and $g(X,Y)$ have degree 1 in X.

Similarly, — " — Y.

$\Rightarrow f(X,Y) = pX + qY + r$ for some $p,q \in \mathbb{C}^\times$, $r \in \mathbb{C}$.

$\Rightarrow a^2+b^2-1 = 0$ for all $a,b \in \mathbb{C}$ on the line given by $pa+qb+r=0$.

$\Rightarrow$ Take $a = -\dfrac{qb+r}{p}$.

so the unit circle contains a line (over $\mathbb{C}$)

$$\Rightarrow 0 = p^2(a^2+b^2-1)$$
$$= (qb+r)^2 + p^2b^2 - p^2$$
$$= (q^2+p^2)b^2 + 2qrb + r^2 - p^2 \quad \forall b \in \mathbb{C}$$

$$\Rightarrow q^2+p^2 = 0 \text{ and } 2qr = 0 \text{ and } r^2-p^2 = 0$$

$$2qr = 0 \xRightarrow{q \neq 0} r = 0 \Rightarrow p = 0 \quad \lightning$$

$$r^2 - p^2 = 0 \Rightarrow p = 0$$

$\square$

Warning / Correction

X^2+Y^2-1 is <u>not</u> irreducible over the field $\mathbb{F}_2$:

$$X^2+Y^2-1 \equiv (X+Y+1)^2 \mod 2.$$

Thm 2.27 Let $X \subseteq K^n$ be algebraic. Then:

a) $X = X_1 \cup \dots \cup X_m$ for some irreducible sets $X_1, \dots, X_m \subseteq X$ with $X_i \not\subseteq X_j$ for all $i \neq j$.

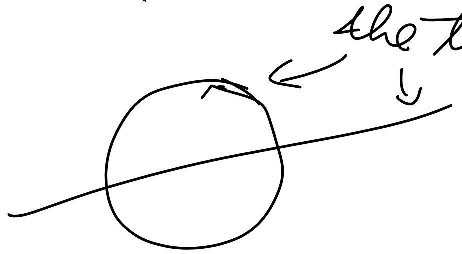
b) This decomposition is unique. The sets $X_1, \dots, X_m$ are called the *irreducible components* of X.

c) Any irreducible subset $Y \subseteq X$ is contained in some X_i.

Ex $V(X), V(Y)$ are the irreducible components of $V(XY)$.

Ex If X is a finite set, its irreducible components are its one-point subsets.

Ex



Pf a) By Hilbert's Basis Theorem (Thm 2.7, Lemma 2.6), there is no chain of ideals $I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq \cdots$

Hence, there is no chain

$$Y_1 \supsetneq Y_2 \supsetneq Y_3 \supsetneq \cdots$$

$\Rightarrow$ If some X can't be decomposed into (finitely many) irreducible components, there is an inclusion-minimal such set X.

$\Rightarrow$ X isn't irreducible

$\rightsquigarrow$ Write $X = A \cup B$ with $A, B \subsetneq X$ algebraic.

$\Rightarrow$ Both A and B can be written as unions of finitely many irreducible subsets.

$\Rightarrow$ X can!