$C(\mathbb{R}) \neq \emptyset$

Next time: we'll start by very quickly defining nonsingularity for general varieties, and then we'll prove the theorem. (see Gaurav's talk video)

PSet post tomorrow am.

7/8 ① Some algebraic geometry review

② proof of our Hasse principle counterexample

Recall $C \hookrightarrow \mathbb{P}^3$ is the projective curve (over $\mathbb{Q}$) given by the vanishing locus of the homogeneous polys

$$F_1(X_0, \dots, X_3) = X_0X_3 - X_1^2$$

$$F_2(X_0, \dots, X_3) = X_2^2 - 2X_0^2 + 2pX_3^2$$

We saw $C \setminus \{[0,0,\pm\sqrt{-2p},1]\} \xleftarrow{\sim} C^0$

C^0 = the affine curve $w^2 = 2 - 2pz^4$.

I said C is a nonsingular curve. We haven't defined either of these notions!

So we digress to some AG background.

We'll restrict this to the affine case for now, but to define dimension and nonsingularity of a projective variety, you look at its intersections with the standard affine cover of $\mathbb{P}^n$:

$\mathbb{P}^n = \bigcup_{i=0}^{n} U_i$, where

$U_i = \{[a_0, \dots, a_n] \in \mathbb{P}^n \mid a_i \neq 0\} \xrightarrow{\sim} \mathbb{A}^n$

$[a_0, \dots, a_n] \longmapsto \left(\frac{a_0}{a_i}, \dots, \widehat{\left(\frac{a_i}{a_i}\right)}, \dots, \frac{a_n}{a_i}\right)$

omit!

$k \subset \bar{k}$

Recall:

(1) An affine variety $X \subset \mathbb{A}^n$ is, for some set $S \subset \bar{k}[x_1, \dots, x_n]$, $X = V(S) = \{P \in \mathbb{A}^n \mid f(P) = 0 \ \forall f \in S\}$

$I(X)$

(1') The ideal of X is $I(X) = \{g \in \bar{k}[x_1, \dots, x_n] \mid g(P) = 0 \ \forall P \in X\}$.

(1'') The affine coordinate ring of X is $\bar{k}[X] = \bar{k}[x_1, \dots, x_n]/I(X)$.

(1''') $\bar{k}[X] \longrightarrow \{\text{functions } X \to \bar{k}\}$

$\bar{g} \longmapsto [P \xrightarrow{X} g(P)]$

$\bar{k}[x_1, \dots, x_n] \supset g + I(X)$

well-defined (ind. of the element in $g + I(X)$) because $I(X)$ vanishes on X.

(2) X is irreducible if $I(X) \subset \bar{k}[x_1, \dots, x_n]$ is a prime ideal. Equivalently $k[X]$ is an integral domain.

Eg: $f(x,y) \in \bar{k}[x,y]$ irreducible (as polynomial). We'll see $I(V(f)) = (f)$. This ideal is prime in the UFD $\bar{k}[x,y]$. (special case of Hilbert's Nullstellensatz.)

Assume here on X = irreducible affine variety

(3) The field of rational functions on X is $\mathrm{Frac}(\bar{k}[X]) = \bar{k}(X)$.

(eg. $X = \mathbb{A}^n$. $\bar{k}[X] = \bar{k}[x_1, \dots, x_n]$
$\bar{k}(X) = \bar{k}(x_1, \dots, x_n)$

(4) $\dim(X) = \mathrm{trdeg}_{\bar{k}}(\bar{k}(X))$.

(so $\dim(\mathbb{A}^n) = n$.)

(5) X is defined over $k \subset \bar{k}$ if $I(X)$ can be generated (over $\bar{k}$) by elements of $k[x_1, \dots, x_n]$

Example Plane curves. Let $f(x,y) \in \bar{k}[x,y]$ be irreducible and non-constant. Then $I(V(f)) = (f)$.

Why: ($\supseteq$ is clear). Suppose $g \in I(V(f))$ and $f \nmid g$ (in the UFD $\bar{k}[x,y]$). By Gauss's Lemma, f and g are coprime in $\bar{k}(x)[y]$ (field, PID), so $\exists\, u, v \in \bar{k}(x)[y]$ such that $uf + vg = 1$.

Rescale this by suitable $w \in \bar{k}[x] \setminus 0$ to get $(uw)f + (vw)g = w$. Thus $w \in I(V(f))$. (uw, vw in $\bar{k}[x][y]$) But $w \in \bar{k}[x] \setminus 0$, so it has finitely many roots in $\bar{k}$.

Thus for any $(a,b) \in V(f)$, there are only finitely many possibilities for a. The same argument (now using $\bar{k}(y)[x]$...) shows there are only finitely many possibilities for b. So under the $f \nmid g$ assumption, $V(f)$ is finite! This is a contradiction [either x or y appears in $f(x,y)$ — suppose it is x, so $f(x,y) = c_0(y) + c_1(y)x + \cdots + c_r(y)x^r$ for some $c_i(y) \in \bar{k}[y]$ and for some $i_0 \geq 1$ $c_{i_0}(y) \neq 0$. $c_{i_0}(y)$ has finitely many roots $S_{i_0} \subset \bar{k}$, and so for any $t \in \bar{k} \setminus S_{i_0}$, $f(x,t)$ is a non-constant polynomial in x, so it has a root. $\bigcup_{t \in \bar{k} \setminus S_{i_0}} \{\text{roots of } f(x,t)\}$ is infinite]. ∎

Remark: Nullstellensatz $I(V(\text{an ideal } J)) = \sqrt{J} = \{f : \text{some } f^n \in J\}$

Thus, taking $X = V(f)$, we've just shown $\bar{k}[X] = \bar{k}[x,y]/I(X) = \bar{k}[x,y]/(f)$, an integral domain. Let's check that $\operatorname{trdeg}_{\bar{k}} \bar{k}(X) = 1$ (i.e., X is a curve)

Again, at least one of x or y appears in f. Suppose it is x. Notation: For $g \in \bar{k}[x,y]$, write $\bar{g}$ for its image in $\bar{k}[X] = \bar{k}[x,y]/(f)$.

Then $\bar{y} \in \bar{k}(X)$ is transcendental over $\bar{k}$ (else $\bar{y} \in \bar{k}$, i.e. $y \in \bar{k} + (f)$, so in $\bar{k}[x,y]$ $y = \underset{\bar{k}}{c} + \underset{\bar{k}[x,y]}{f} \cdot g$. Since x appears in f, this is impossible).

Thus $\bar{k}(\bar{y})$ has trdeg 1, and $\bar{x}$ is algebraic over $\bar{k}(\bar{y})$ (from the equation $f(x,y) = 0$).

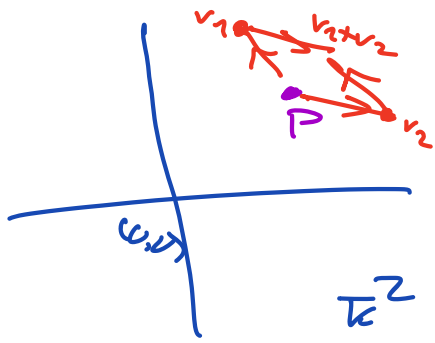
Thus $\operatorname{trdeg}_{\bar{k}} \bar{k}(X) = 1$. ∎

(7) Tangent spaces and nonsingular points on affine varieties

Let $X \subset \mathbb{A}^n$ be an irreducible affine variety.

Fix $P = (p_1, \dots, p_n) \in X \subset \mathbb{A}^n$.

First, $T_P \mathbb{A}^n = \bar{k}^n$ as a vector space with origin P.



For each $F \in I(X) \subset \bar{k}[x_1, \dots, x_n]$, we get a linear function on $T_P \mathbb{A}^n$, given by

$$dF|_P = \sum_{i=1}^{n} \frac{\partial F}{\partial x_i}(P) \cdot (x_i - p_i), \text{ where}$$

$$x_i : T_P \mathbb{A}^n \longrightarrow \bar{k}$$
$$(b_1, \dots, b_n) \longmapsto b_i .$$

Defn: $T_P X = \{ v \in T_P \mathbb{A}^n \mid dF|_P(v) = 0 \ \forall F \in I(X) \}$.

(this recovers our original defn when X is a curve in $\mathbb{A}^2$).

Concretely, if $I(X) = (f_1, \dots, f_r)$, and $J(P)$ is the matrix

$$J(P) = \begin{bmatrix} \frac{\partial f_1}{\partial x_1}(P) & \frac{\partial f_1}{\partial x_2}(P) & \cdots & \frac{\partial f_1}{\partial x_n}(P) \\ \vdots & & & \vdots \\ \frac{\partial f_r}{\partial x_1}(P) & - & - & \frac{\partial f_r}{\partial x_n}(P) \end{bmatrix}$$

$T_P X \cong \ker J(P)$

Defn: X is nonsingular at $P \in X$ if

$$\dim(X) = \dim_k T_P(X) \quad (\leq \text{ always holds but } T_P X \text{ can be larger; eg: } y^2 = x^3 \text{ at } (0,0).)$$

This recovers the defn for plane curves where we said $V(f)$ was nonsing at $P=(a,b)$ if $\left(\frac{\partial f}{\partial x}(P) \quad \frac{\partial f}{\partial y}(P)\right) \neq (0 \quad 0)$.

Lemma: $f \in k[x,y]$ irreducible, non-constant. Then $\text{Sing} = \{P \in V(f) \mid P \text{ is a singular point of } V(f)\}$ is finite.

Pf: $\text{Sing} = V(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}) \subset \mathbb{A}^2$. We've seen (in the $I(V(f)) = (f)$ proof) that $V(f, \frac{\partial f}{\partial x})$ is finite unless $f \mid \frac{\partial f}{\partial x}$, i.e. unless $\frac{\partial f}{\partial x} = 0$, i.e. unless f is a poly in y and (if $\text{char } k = p$) x^p. (exercise). Likewise $V(f, \frac{\partial f}{\partial y})$ is finite unless f is a poly in x and (if $\text{char } k = p$) y^p.

Thus, $V(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y})$ is finite unless $\text{char } k = p$ and $f(x,y) = g(x^p, y^p) = g(x,y)^p$, contradicting irreducibility of f. So $\text{Sing} = \text{finite}$. ∎

Return to our $C = V(X_0X_3 - X_1^2,\ X_2^2 - 2X_0^2 + 2pX_3^2) \hookrightarrow \mathbb{P}^3$

$\cup$

$C^0 = V(w^2 - 2 + 2pz^4) \hookrightarrow \mathbb{A}^2$

for p a prime, $p \equiv 1 \bmod 8$, $\left(\frac{2}{p}\right)_4 \neq 1$.

Exercise: C is nonsingular

Prop: $C^0(\mathbb{Q}) = C(\mathbb{Q}) = \emptyset$.

Pf: Recall $C \setminus C^0 = \{[0,0,\pm\sqrt{-2p},1]\}$ ← not $\mathbb{Q}$-points!

so $C^0(\mathbb{Q}) = C(\mathbb{Q})$

Suppose $(w,z) \in C^0(\mathbb{Q})$: $w^2 = 2 - 2pz^4$. Write $z = r/t$ for r,t coprime in $\mathbb{Z}$. $w^2 = 2 - 2pr^4/t^4$, so $t^4w^2 = 2(t^4 - pr^4)$. Write $w = a/b$, a,b coprime in $\mathbb{Z}$

so $b^2 \mid t^4a^2$, so $b^2 \mid t^4$, so $b \mid t^2$: $t^2 = b\cdot u$, some $u \in \mathbb{Z}$.

$w = \frac{a}{b} = \frac{au}{t^2}$, so $\frac{t^4a^2}{b^2} = (au)^2 = 2(t^4 - pr^4)$

so au is even, so $w = \frac{2s}{t^2}$ $(s \in \mathbb{Z})$

Thus, $\boxed{2s^2 = t^4 - pr^4.}$

If $q \mid s$ is any odd prime, we get $\left(\frac{p}{q}\right) = 1$, hence $\left(\frac{q}{p}\right) = 1$. We know $\left(\frac{2}{p}\right) = 1$ and $\left(\frac{-1}{p}\right) = 1$, so

$\boxed{\left(\frac{s}{p}\right) = 1}$. Thus $\left(\frac{s^2}{p}\right)_4 = 1$ (s^2 is a 4th power mod p).

so $\left(\frac{2s^2}{p}\right)_4 \neq 1$, contradicting $2s^2 = t^4 - pr^4$. !

$C(\mathbb{R}) \neq \emptyset$, clearly.

- It is not clear that $C(\mathbb{Q}_\ell) \neq \emptyset$ $\forall$ primes ℓ.

- For $\ell \neq 2, p$, C mod ℓ is non-singular; (easy check) it suffices to show $C(\mathbb{F}_\ell) \neq \emptyset$. Not obvious! } by Hensel

General approach: use the "Riemann hypothesis for curves over finite fields":

General Theorem: Let C be a projective nonsingular (irreducible) curve over $\mathbb{F}_q$ "of genus g". (Here $g=1$)

Then $|\#C(\mathbb{F}_q) - q - 1| \leq 2g\sqrt{q}$

Plug in $g=1$: $|\#C(\mathbb{F}_\ell) - \ell - 1| \leq 2\sqrt{\ell}$

to get $C(\mathbb{F}_\ell) \neq \emptyset$, we just need $\ell + 1 > 2\sqrt{\ell}$, ie $(\sqrt{\ell} - 1)^2 > 0$. True for all ℓ!

Conclusion: when "$g=1$," $C(\mathbb{F}_\ell) \neq \emptyset$ for any nonsing. projective curve / $\mathbb{F}_\ell$.

That treats via Hensel all $\ell \neq 2, p$ in our example.

For $\ell = 2$ or p, still give a Hensel's lemma argument but with a little more care.

exercises.