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

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

- For $\ell \neq 2, p$, $C \bmod \ell$ 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 $\left|\#C(\mathbb{F}_q) - q - 1\right| \leq 2g\cdot\sqrt{q}$

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

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. $\leftarrow \ell = 2$.

$\boxed{\ell = p}$ $\boxed{w^2 = 2 - 2pz^4}$. Since $p \equiv 1 \bmod 8$, $w^2 \equiv 2 \bmod p$ has a solution so $C(\mathbb{F}_p) \neq \emptyset$. Since this $w_0 \neq 0$, easy to see that $C \bmod p$ is nonsingular at $(w_0, 0)$, hence we get $C(\mathbb{Z}_p) \neq \emptyset$

by Hensel's lemma.

Sketch of a tricky elementary proof (Aitken, Lemmermeyer)

$\boxed{\ell \neq 2, p}$ We'll look for a non-zero solution in $\mathbb{F}_\ell$ to $W^2 = 2X^4 - 2pZ^4$. If we have (W, X, Z) satisfying this:

- if $X \neq 0$, then $w = W/X^2$, $z = Z/X$ we get

$$\underset{W^2/X^4}{\underset{\shortparallel}{w^2}} = \underset{2-2pZ^4/X^4}{\underset{\shortparallel}{2 - 2pz^4}}$$

- if $X = 0$, then $W^2 = -2pZ^4$, so $\left(\frac{-2p}{\ell}\right) = 1$, and so $C(\mathbb{F}_\ell) \ni [0, 0, \pm\sqrt{-2p}, 1]$

Now we prove more generally: for $\ell \neq 2$, $a, b \in \mathbb{F}_\ell^\times$, $aX^4 + bY^4 = Z^2$ has a non-zero $\mathbb{F}_\ell$-solution.

The conic $aX_0^2 + bX_1^2 = X_2^2$ has an $\mathbb{F}_\ell$-point (any conic$/\mathbb{F}_\ell$ does), so we can parametrize its solutions by $(x_0(t), x_1(t), x_2(t))$ for $x_i(t) \in \mathbb{F}_\ell[t]$.

(Check) Each $x_i(t)$ is non-zero, degree ≤ 2, at least two of them have degree 2, and no two are associates.

[Explicitly: choose $x_0, x_1 \in \mathbb{F}_\ell$: $ax_0^2 + bx_1^2 = 1$, then

$$a \cdot (bx_0t^2 - 2bx_1t - ax_0)^2 + b(-bx_1t^2 - 2ax_0t + ax_1)^2 = (bt^2 + a)^2]$$

- Since $x_0(t)$ and $x_1(t)$ are not associates, $\exists\, t_0 \in \mathbb{F}_\ell$ s.t. $\left(\frac{x_0(t_0)}{\ell}\right) \neq \left(\frac{x_1(t_0)}{\ell}\right)$: indeed, if not, then $x_0(t_0)^{\frac{\ell-1}{2}} - x_1(t_0)^{\frac{\ell-1}{2}}$ would vanish on all of

$\mathbb{F}_\ell$. But then we have a degree $\leq \ell-1$ poly vanishing on all of $\mathbb{F}_\ell$, so it must be the zero poly, which implies $x_0(t)$ and $x_1(t)$ are associates.

- Choose $t_0 \in \mathbb{F}_\ell$ such that $\left(\frac{x_0(t_0)}{\ell}\right) \neq -\left(\frac{x_1(t_0)}{\ell}\right)$ (apply previous claim to $x_1(t)\cdot(\text{non-}\square)$).

Thus, $x_0(t_0)\cdot x_1(t_0) = c^2$ some $c \in \mathbb{F}_\ell$, and $x_0(t_0)$ & $x_1(t_0)$ are not both 0

Case 1: $x_0(t_0) \neq 0$: Then we check that $(x_0(t_0), c, x_0(t_0)x_2(t_0))$ is a solution to $aX^4+bY^4=Z^2$

Check: $a\, x_0(t_0)^4 + b\, \cancel{c^4} \overset{?}{=} x_0(t_0)^2 x_2(t_0)^2$

$x_0(t_0)^2 x_1(t_0)^2$

Cancel $x_0(t_0)^2$: $a\, x_0(t_0)^2 + b\, x_1(t_0)^2 = x_2(t_0)^2$. we know

Case 2: $x_1(t_0) \neq 0$. Take $(c, x_1(t_0), x_1(t_0)x_2(t_0))$. ∎

Thus $C(\mathbb{F}_\ell) \neq \emptyset$ $\forall\, \ell \neq 2, p$, so $C(\mathbb{Q}_\ell) \neq \emptyset$ $\forall\, \ell \neq 2, p$; and we've checked $\ell = 2$ & $\ell = p$ separately. Done. ∎

More review of affine varieties

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

Recall we have $\bar{k}[\mathbb{A}^n] = \bar{k}[x_1, \ldots, x_n] \twoheadrightarrow \underset{\text{int. domain}}{\bar{k}[X]} = \dfrac{\bar{k}[x_1, \ldots, x_n]}{\underset{\text{prime ideal}}{I(X)}}$

and $\bar{k}(X) := \operatorname{Frac} \bar{k}[X]$.

Defn: Let $f \in \bar{k}(X)$, and let $P \in X$. f is defined at P if $\exists\ g, h \in \bar{k}[X]$: $f = g/h$ and $h(P) \neq 0$.

$\boxed{2}$ g and h are not unique! $\left(\bar{k}[X] \to \operatorname{Fun}(X, \bar{k})\right)$

Eg: $X = V(x_1x_4 - x_2x_3) \subset \mathbb{A}^4$, so $\bar{k}[X] = \dfrac{\bar{k}[x_1, \ldots, x_4]}{(x_1x_4 - x_2x_3)}$ ← $I(X)$!

Note $\dfrac{\bar{x}_1}{\bar{x}_2} = \dfrac{\bar{x}_3}{\bar{x}_4}$ in $\bar{k}(X)$ (by def this means $\bar{x}_1\bar{x}_4 = \bar{x}_2\bar{x}_3$ ie $x_1x_4 - x_2x_3 \in I(X)$)

So $f = \dfrac{\bar{x}_1}{\bar{x}_2}$ is defined at all $P \neq (a, 0, c, 0)$ $a, c \in \bar{k}$.

Defn: For $P \in X$, the local ring of X at P $\mathcal{O}_{X,P}$ is $\mathcal{O}_{X,P} = \{ f \in \bar{k}(X) \mid f \text{ is defined at } P \}$.

Have a $\bar{k}$-algebra hom $\mathcal{O}_{X,P} \twoheadrightarrow \bar{k}$ (surjective)
(evaluation) $f = g/h \longmapsto g(P)/h(P)$

Its kernel $m_{X,P} = \{ f \in \mathcal{O}_{X,P} \mid f(P) = 0 \}$ is a maximal ideal; and it is the only maximal ideal in $\mathcal{O}_{X,P}$: if $f = g/h$ with $g(P) \neq 0$ $h(P) \neq 0$ (ie $f \notin m_{X,P}$), then $h/g \in \mathcal{O}_{X,P}$, so $f \in \mathcal{O}_{X,P}^{\times}$.

Thus $\mathcal{O}_{X,P} \setminus m_{X,P} = \mathcal{O}_{X,P}^{\times}$ so $m_{X,P}$ is the only max'l ideal.

Thus $\mathcal{O}_{X,P}$ is an integral domain and a local ring.
(and $\mathrm{Frac}(\mathcal{O}_{X,P}) = \bar{k}(X)$).

Again we are focusing on the affine case because in general we reduce to this case:

If $X \subset \mathbb{P}^n$ is a projective variety ($= V(F_1, \dots, F_r) \subset \mathbb{P}^n$ for some homogeneous $F_i \in \bar{k}[X_0, \dots, X_n]$), then $\forall\, i = 0, \dots, n$,

$$X \cap U_i \subset U_i \cong \mathbb{A}^n \qquad (U_i = \{X_i \neq 0\} \subset \mathbb{P}^n)$$

is an affine variety, possibly empty. We say X is irreducible if $I(X) \subset \bar{k}[X_0, \dots, X_n]$ is prime, and in this case $I(X \cap U_i) \subset \bar{k}[\mathbb{A}^n]$ is prime.

Define the function field of X to be

$$\bar{k}(X) = \bar{k}(X \cap U_i) \text{ for any } i: X \cap U_i \neq \emptyset$$

and for $P \in X \cap U_i$, we set $\mathcal{O}_{X,P} = \mathcal{O}_{X \cap U_i, P}$

(*) There are canonical isos

$$\begin{array}{ccc} \bar{k}(X \cap U_i) & \cong & \bar{k}(X \cap U_j) \\ \cup & & \cup \\ \mathcal{O}_{X \cap U_i, P} & \cong & \mathcal{O}_{X \cap U_j, P} \end{array}$$

when $P \in X \cap U_i \cap U_j$

Do problem 1 of pset 3 to see what's going on.
post tomorrow. (Prove the general).

Two fundamental results from commutative algebra

<u>Defn:</u> A ring R is <u>Noetherian</u> if every ideal of R is finitely-generated.

(Equivalently, every increasing chain of ideals $I_1 \subset I_2 \subset \cdots$ terminates).

Hilbert Basis Theorem Suppose R is Noetherian. Then $R[x]$ is Noetherian.

<u>Cor:</u> $k[x_1, \ldots, x_n]$ is Noetherian (k a field)

<u>Cor:</u> In our previous setting ($X \subset \mathbb{A}^n$ irr. aff. var., $P \in X$), $\mathcal{O}_{X,P}$ is Noetherian.

<u>Pf:</u> Let $I \subset \mathcal{O}_{X,P}$. The quotient $\bar{k}[X] \twoheadleftarrow \bar{k}[x_1, \ldots, x_n]$ is Noetherian, so $I \cap \bar{k}[X]$ is finitely-generated, so $I \cap \bar{k}[X] = (f_1, \ldots, f_r)$. Claim: $I = \sum_{j=1}^{r} \mathcal{O}_{X,P} \cdot f_j$

<u>Reason:</u> for $f \in I$, $f = g/h$ with $g, h \in \bar{k}[X]$, $h(P) \neq 0$, and so $f \cdot h \in I \cap \bar{k}[X]$, hence $f \cdot h = \sum a_j \cdot f_j$ for some $a_j \in \bar{k}[X]$, so $f = \sum_{j=1}^{r} \frac{a_j}{h} \cdot f_j$ ($a_j/h \in \mathcal{O}_{X,P}$). ∎

Hilbert Nullstellensatz

Version 1 Suppose $K \supset \bar{k}$ is a field, and for some n there is a surjective $\bar{k}$-algebra homomorphism

$$\bar{k}[x_1, \ldots, x_n] \twoheadrightarrow K.$$

Then $K = \bar{k}$.

(False if we replace $\bar{k}$ with a non-algebraically closed).

eg $\mathbb{R}[x] \twoheadrightarrow \mathbb{C}$

$x \longmapsto i$

$\boxed{\text{Version 2}}$ For any proper ideal $I \subsetneq \bar{k}[x_1,\dots,x_n]$,

$V(I) \neq \emptyset$. (false w/ k not alg. closed).

$\boxed{\text{Version 3}}$ For any ideal $I \subseteq \bar{k}[x_1,\dots,x_n]$,

$$I(V(I)) = \underbrace{\sqrt{I}}_{\text{(radical of } I)} := \{ f \in \bar{k}[x_1,\dots,x_n] \mid f^d \in I \text{ for some } d > 0 \}$$

Note V3 $\Rightarrow$ what we proved last time, that for $f(x,y) \in \bar{k}[x,y]$ irreducible, then $I(V(f)) = (f)$

It also implies in our $\overset{X}{V}(x_1x_4 - x_2x_3) \subset \mathbb{A}^4$ eg

$$I(X) = I(V(x_1x_4 - x_2x_3)) = \sqrt{(x_1x_4 - x_2x_3)} = (x_1x_4 - x_2x_3)$$

<u>Cor</u>: Let $X \subset \mathbb{A}^n$ be an irreducible affine variety. Then $\bigcap_{P \in X} \mathcal{O}_{X,P} \overset{\text{inside } \bar{k}(X)}{=} \bar{k}[X]$.

<u>Pf</u>: Suppose $f \in \bigcap_{P \in X} \mathcal{O}_{X,P} \subset \bar{k}(X)$. Consider

$J_f = \{ h \in \bar{k}[x_1,\dots,x_n] \mid \bar{h} \cdot f \in \bar{k}[X] \}$, an ideal (containing $I(X)$) of $\bar{k}[x_1,\dots,x_n]$. (meaning the image in $\bar{k}[X]$) Then $V(J_f) = \emptyset$: for any $P \in X$, $\exists\, g, h \in \bar{k}[X]$: $f = g/h$ and $h(P) \neq 0$. $g = hf \in \bar{k}[X]$. Thus ($h \in J_f$), so $P \notin V(J_f)$. By V2 of the Nullstellensatz, $J_f = \bar{k}[x_1,\dots,x_n] \ni 1$, so $1 \cdot f \in \bar{k}[X]$.

(meaning any lift of h to $\bar{k}[x_1,\dots,x_n]$)

$\boxed{\text{Back to curves}}$ Let $C \subset \mathbb{A}^n$ be an irreducible curve, and let $P \in C$. What does $\mathcal{O}_{C,P}$ look like?

$\boxed{\text{Prop:}}$ Suppose $P \in C$ is a nonsingular point. Then $\mathcal{O}_{C,P}$ is a discrete valuation ring (DVR).

Recall: A DVR R is a Noetherian local integral domain such that the maximal ideal m_R is principal and non-zero, so field $\neq$ DVR.

Ex: • p prime: $\mathbb{Z}_p$, $\mathbb{Z}_{(p)} = (\mathbb{Z}-p\mathbb{Z})^{-1}\mathbb{Z}$

$$= \left\{ \frac{a}{b} \in \mathbb{Q} \;\middle|\; a \in \mathbb{Z}, b \in \mathbb{Z} \setminus p\mathbb{Z} \right\}$$

• For any $\bar{k}$, and $a \in \bar{k}$, $\bar{k}[t]_{(t-a)} = \left\{ \frac{g(t)}{h(t)} \in \bar{k}(t) \;\middle|\; g(t) \in \bar{k}[t],\ (t-a) \nmid h(t) \right\}$

This is $\mathcal{O}_{\mathbb{A}^1, a}$

Lemma: Let R be a DVR. Set $m_R = (t)$ — t is called a uniformizer of R.

Then $\forall\, x \in R$, $\exists!$ $n \in \mathbb{Z}_{\geq 0}$ and $u \in R^\times$: $x = t^n \cdot u$.

Moreover, R is a PID.

Pf: Existence. Let $x \in R$. If $x \in R^\times$, take $n=0, u=x$ ✓.

So wma $x \in R \setminus R^\times = m_R$, hence $x = t \cdot x_1$ for some $x_1 \in R$. If $x_1 \in R^\times$, take $n=1$, $u = x_1$. ✓ If not, $x_1 \in m_R$, so $x_1 = t \cdot x_2$ $(x_2 \in R)$. And so on: eventually, we come to some $x_{n_0} \in R^\times$ — then take $n = n_0$, $u = x_{n_0}$ — or this goes on forever & we get an infinite chain $(x) \subset (x_1) \subset (x_2) \subset \cdots$ This terminates b/c R is Noetherian: for some m, $(x_m) = (x_{m+1}) = \cdots$

So $x_m = t x_{m+1}$ and $x_{m+1} = v \cdot x_m$ for some $v \in R^\times$.

so $x_m = tv\, x_m$, so $tv = 1$, a contradiction. ✓

Uniqueness: If $x = u_1 t^{n_1} = u_2 t^{n_2}$, wma $n_1 \geq n_2$, and then $t^{n_1 - n_2} = u_1^{-1} u_2 \in R^\times$, so $n_1 - n_2 = 0$ and thus $u_1 = u_2$ as well.

R is a PID because for $(0) \subsetneq I \subset R$, we set $n_I = \min\{n \in \mathbb{Z}_{\geq 0} \mid t^n \in I\}$. Then $I = (t^{n_I})$. ∎

Finally, given a DVR, we can define the valuation

$v_R : \operatorname{Frac}(R)^\times \longrightarrow \mathbb{Z}$ by

$v_R : R \setminus 0 \longrightarrow \mathbb{Z}_{\geq 0}$ is $v_R(x) =$ the $n \in \mathbb{Z}_{\geq 0}$: $x = t^n \cdot u,\ u \in R^\times$.

On $\operatorname{Frac}(R)^\times$, $v_R(a/b) = v_R(a) - v_R(b)$ for $a, b \in R$.

This satisfies
- group hom
- $v_R(x+y) \geq \min\{v_R(x), v_R(y)\}$

Ex: $v_p : \mathbb{Q}^\times \longrightarrow \mathbb{Z}$

$p^n \cdot \frac{a}{b} \longmapsto n$

$(ab, p) = 1$

$v_{(t-a)} : \overline{k}(t)^\times \longrightarrow \mathbb{Z}$, $a \in \overline{k}$

$(t-a)^n \cdot \frac{g(t)}{h(t)}$

$(gh, t-a) = 1$

Shangjie talk

also have

$v_\infty : \overline{k}(t)^\times \longrightarrow \mathbb{Z}$

on $\overline{k}[t]$, this is $v_\infty(f) = -\deg(f)$

$\overline{k}[1/t] \subset \overline{k}(t)$ and $\overline{k}[1/t]_{(1/t)}$ is a DVR, and this is the associated valuation.

this corresponds to $\infty \in \mathbb{P}^1$,

so we have a bijection

$$\boxed{\mathbb{P}^1 \longleftrightarrow \text{surj. discrete valuations on } \overline{k}(t)}.$$

Now we prove the Prop: $P \in C \subset \mathbb{A}^n$ a nonsingular point on the curve C $\Rightarrow$ $\mathcal{O}_{C,P}$ is a DVR. (next time)

(We've just seen some examples of this.)