0.2. Diophantine Approximation

"How well can you approximate a given real number α by rational numbers?"

Thm A rational number $\frac{p}{q}$ (with $\gcd(p,q)=1$) satisfies $|p-q\alpha| < |p'-q'\alpha|$ for all $\frac{p'}{q'} \neq \frac{p}{q}$ with $|q'| \leq |q|$ if and only if $\frac{p}{q}$ is the result of a truncation of the continued fraction expansion of α. (A convergent.)

Rmk Replacing the inequality $|p-q\alpha| < |p'-q'\alpha|$ by $\left|\frac{p}{q}-\alpha\right| < \left|\frac{p'}{q'}-\alpha\right|$, you get slightly more such numbers $\frac{p}{q}$ (still arise from the continued fraction expansion of α).

Question How quickly do the "best" approximations $\frac{p}{q}$ with $|q| \leq N$ converge to α as $N \to \infty$?

Dirichlet's Approximation Theorem

For any $\alpha \in \mathbb{R}$ and $N \geq 1$, there is some $\frac{p}{q} \in \mathbb{Q}$ with $|q| \leq N$ and $|p - q\alpha| < \frac{1}{N}$.

Pf HW. □

Roth's Theorem

For any algebraic number $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and any $\varepsilon > 0$, there is a constant $C > 0$ such that

$$|p - q\alpha| > \frac{C}{|q|^{1+\varepsilon}} \quad \text{for any } \frac{p}{q} \in \mathbb{Q}.$$

Rmk False for $\alpha \in \mathbb{Q}$.

Rmk False for $\varepsilon = 0$ by Dirichlet's Approx Thm.

Rmk False for some transcendental numbers $\alpha \in \mathbb{R}$.

False $\alpha = \sum_{i=1}^{\infty} 2^{-a_i}$ with

$a_1 < a_2 < \cdots \longrightarrow \infty$ very quickly.

Thue's Theorem

Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be a squarefree homogeneous degree n polynomial. Consider its n roots in $\mathbb{P}^1(\mathbb{C})$. Assume one of the following:

a) f has root in $\mathbb{P}^1(\mathbb{C}) \setminus \mathbb{P}^1(\mathbb{R})$.

b) $n \geq 3$.

Then, for any $r \in \mathbb{Q}^\times$, there are only finitely many solutions $(x,y) \in \mathbb{Z}^2$ to the Thue equation

$$f(x,y) = r.$$

Ex $f(x,y) = x^2 + y^2$ satisfies a)

$x^2 + y^2 = r$ has only fin. many sol. $(x,y) \in \mathbb{Z}^2$.

($\exists$ fin. many $z = x + iy \in \mathbb{Z}[i]$ with $N(z) = r$)

Ex $f(x,y) = x^2 - 3y^2$ doesn't satisfy a) or b)

$x^2 - 3y^2 = 1$ has ∞ many sol. $(x,y) \in \mathbb{Z}^2$

(corr. to $z \in x + \sqrt{3}y \in \mathbb{Z}[\sqrt{3}]$ with $N(z) = 1$, so at least any $z \in \mathbb{Z}[\sqrt{3}]^{\times 2}$).

PL using Roth's Theorem assuming f has $n \geq 3$ roots in $\mathbb{P}^1(\mathbb{R}) \setminus \mathbb{P}^1(\mathbb{Q})$

W.l.o.g. the X^n-coeff. in $f(X,Y)$ is 1.

Write $f(X,Y) = (X - \alpha_1 Y) \cdots (X - \alpha_n Y)$ with distinct $\alpha_1, \ldots, \alpha_n \in \mathbb{R} \setminus \mathbb{Q}$.

$$|X - \alpha_i Y| + |X - \alpha_j Y| \geq |\alpha_i - \alpha_j| \cdot |Y| \quad \forall i,j$$

$$\Rightarrow |X - \alpha_i Y| \text{ or } |X - \alpha_j Y| \geq \frac{|\alpha_i - \alpha_j|}{2} \cdot |Y| \quad \forall i,j$$

$$\Rightarrow |X - \alpha_k Y| \geq D \cdot |Y| \text{ with } D = \frac{1}{2} \min_{i \neq j} |\alpha_i - \alpha_j|$$

for all but at most one index k.

But $\prod_{i=1}^{n} (X - \alpha_i Y) = f(X,Y) = r$, so

$$\frac{c}{|Y|^{1.5}} \leq |X - \alpha_\ell Y| \leq \frac{|r|}{(D \cdot |Y|)^{n-1}}$$

for the remaining index ℓ.

$$\Rightarrow |Y|^{n-2.5} < \frac{|r|}{c \cdot D^{n-1}} \Rightarrow |Y| \text{ is bounded}$$

$\Rightarrow |X|$ is bounded. $\square$

1. Varieties (Review of Algebraic Geometry)

1.1. Affine varieties

Let k be a field.

Def For an ideal $I \subseteq k[x_1, \dots, x_n]$, we associate the set of zeros

$$V(I) = \{(x_1, \dots, x_n) \in \overline{k}^n \mid f(x_1, \dots, x_n) = 0 \ \forall f \in I\}.$$

Def An *affine variety* defined over k is a set $X \subseteq \overline{k}^n$ of the form $X = V(I)$ with $I \subseteq k[x_1, \dots, x_n]$.

We write $X \subseteq \mathbb{A}^n_k$.

Def For $X \subseteq \mathbb{A}^n_k$, we write

$$X(k) = X \cap k^n.$$

$$X(\overline{k}) = X$$

Ex $k = \mathbb{R}$, $n = 1$, $I = (x^2 + 1)$

$\Rightarrow V(I) = \{\pm i\} \subseteq \mathbb{A}^1_{\mathbb{R}}$ is an affine variety over $\mathbb{R}$

$I' = (1) \Rightarrow V(I') = \emptyset$

$V(I) \neq V(I')$, but $V(I)(\mathbb{R}) = V(I')(\mathbb{R})$ ($= \emptyset$)

But $\{\pm i\}$ isn't an affine variety over $\mathbb{R}$, but is an affine variety over $\mathbb{C}$.

Def An affine variety $X \neq \emptyset$ over K is *irreducible* if we can't write $X = X_1 \cup X_2$ with affine varieties $X_1, X_2 \subsetneq X$ over K.

Rmks "irreducible over K" $\not\Longleftrightarrow$ "irreducible over $\overline{K}$"

E.g. $V(x^2+1) = \{\pm i\}$ is irreducible over $\mathbb{R}$ (because x^2+1 is)

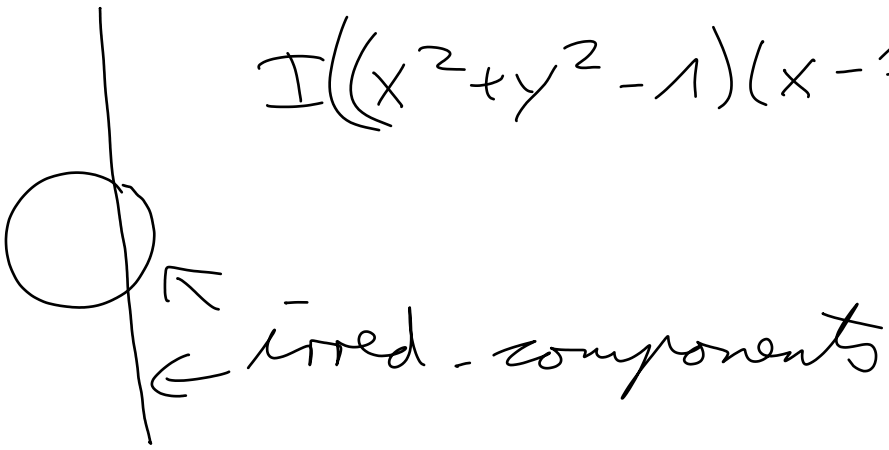
but not irreducible over $\mathbb{C}$

Def Irreducible over $\overline{K}$ is called *geometrically irreducible*.

Lemma/Def Any affine variety X over K can be written uniquely as $X = X_1 \cup \dots \cup X_r$ with $X_1, \dots, X_r$ irreducible and $X_i \not\subseteq X_j$ $\forall i, j$.
The $X_1, \dots, X_r$ are called the *irreducible components* of X.

Ese

$I\left((x^2+y^2-1)(x-\tfrac{1}{2})\right)$



← irred. components

Def The closed subsets of $\overline{K}^n$ w.r.t. the Zariski topology over K are the affine varieties $X \subseteq \overline{K}^n$ over K.
We equip any affine variety $X \subseteq \overline{K}^n$ with the subspace topology.

Def To an affine variety $X \subseteq \mathbb{A}^n_K$, we associate the vanishing ideal

$$I(X) = \{ f \in K[X_1, \dots, X_n] \mid f(P) = 0 \ \forall P \in X(\overline{K}) \}.$$

Rmk (Hilbert's Nullstellensatz)
$I(V(J)) = \sqrt{J}$, the radical of J:

$$\sqrt{J} = \{ f \in K[X_1, \dots, X_n] \mid f^n \in J \text{ for some } n \geq 1 \}.$$

Rmk $I(X)$ is a radical ideal:

if $f^n \in I(X)$, then $f \in I(X)$.

1.2. Rings of functions

Def The coordinate ring of an affine variety X over k is

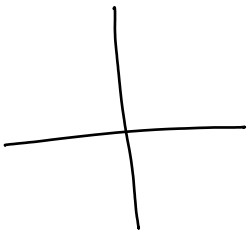
$$\Gamma(X) = \Gamma(X, \mathcal{O}_X) = \mathcal{O}_X(X) := k[x_1, \dots, x_n]/I(X).$$

Its elements are the (regular) functions on X.

Rmk $\mathcal{O}_X(X)$ is reduced: has no nilpotent elements $f \neq 0$.

Rmk $\mathcal{O}_X(X)$ is an integral domain if and only if X is irreducible.

Ex $X = V(x_1 x_2) \subseteq \mathbb{A}^2$ is not irreducible



$$\mathcal{O}_X(X) = k[x_1, x_2]/(x_1 \cdot x_2)$$

is not an integral domain

Def If X is irreducible, its field of rational functions $k(X)$ is the field of fractions of $\mathcal{O}_X(X)$.

Def An element $t \in K(X)$ is **defined at** $P \in X(\bar{k})$ if we can write $t = \frac{f}{g}$ with $f, g \in \mathcal{O}_X(X)$ and $g(P) \neq 0$.

Ex $X = V(xy - z^2) \subseteq \mathbb{A}^3_k$

$\mathcal{O}_X(X) = k[x,y,z]/(xy - z^2)$

The rational functions $\frac{x}{z}$ and $\frac{z}{y}$ on X are the same! ($xy = z^2 \Rightarrow \frac{x}{z} = \frac{z}{y}$).

$t = \frac{x}{z} = \frac{z}{y}$ is defined everywhere on X except at the points with $y = z = 0$.

Def Let $X \subseteq \mathbb{A}^n$ be irreducible.

For an open subset $\emptyset \neq U \subseteq X$, the ring of rational functions on X defined on U is

$$\Gamma(U, \mathcal{O}_X) = \mathcal{O}_X(U) := \{ t \in K(X) \mid t \text{ defined at } P \ \forall P \in U(\bar{k}) \}$$

$$\Gamma(\emptyset, \mathcal{O}_X) = \mathcal{O}_X(\emptyset) = 0$$