- 1^{st} order formula in language of rings. e.g.:

$$\overbrace{\underbrace{\forall y \exists z \exists w}_{\text{bound variables}} \left(\left(\underbrace{x}_{\text{free variable}} z + 3 = y^2 \right) \vee \neg (z = x + w) \wedge (x = x + 1) \right)}^{\phi(x)}$$

- 1^{st} order sentence $=$ 1^{st} order formula with no free variable
- positive existential formula: only $\exists$, $+$, 0, 1, $=$, $\wedge$, $\vee$, (,), variables
- diophantine formula: $\exists x_1 \ldots \exists x_n$ poly=poly

Let R be a ring (commutative with 1)

- 1^{st} order formula $\phi(x_1, \ldots, x_n) \rightsquigarrow \underbrace{\{\vec{x} \in R^n \ : \ \phi(\vec{x}) \text{ is true }\}}_{\text{definable sets}}$
- positive existential formulas $\rightsquigarrow$ positive existential sets
- diophantine formulas $\rightsquigarrow$ diophantine sets

Claim For any ring R:

$$\{ \text{ positive existential sets } \} = \{ \text{ diophantine sets } \}$$

Proof Sketch for $R = \mathbb{Z}$

- $f = g \rightsquigarrow f - g = 0$
- $f = 0 \vee g = 0 \rightsquigarrow fg = 0$
- $f = 0 \wedge g = 0 \rightsquigarrow f^2 + g^2 = 0$

Definitions:

- 1^{st} order theory of the ring R

  $= \{$ 1^{st} order sentences that are true for R $\}$

- positive existential theory of the ring R

  $= \{$ positive existential sentences that are true for R $\}$

- . . .

Definitions(cont.):

- the theory is decidable $\iff \exists$ an algorithm with:

  Input: 1^{st} order sentence

  Output:

  YES if true

  NO otherwise

H10 for Various Rings

Definitions:

- H10/R asks whether $\exists$ algorithm with:

  Input: $f \in \mathbb{Z}[x_1, \ldots, x_n]$

  Output:

  YES $\exists \vec{a} \in R^n$ such that $f(\vec{a}) = 0$

  NO otherwise

- H10/R with coefficients in S where S is encodable is the same except $f \in S[x_1, \ldots, x_n]$

	Ring R	H10	1^{st} order theory is decidable
local field	$\mathbb{C}$	YES	YES
local field	$\mathbb{R}$	YES	YES
	$\mathbb{F}_q$	YES	YES
local field	finite extensions of $\mathbb{Q}_p$		
	$= p$-adic field	YES	YES
local field	$\mathbb{F}_q((t))$	?	?
	include a symbol for t		
global field	number field	?	NO
global field	$\mathbb{Q}$	?	NO
global field	global function field	NO	NO
global field	$\mathbb{F}_q(t)$	NO	NO
	include a symbol for t		
	$\mathbb{C}(t)$	?	?
	include a symbol for t		
	$\mathbb{C}(t, u)$	NO	NO
	include symbols for t and u		
	$\mathbb{R}(t)$	NO	NO
	include a symbol for t		
	$\mathbb{Z}$	NO	NO
$[K : \mathbb{Q}] < \infty$	$\mathcal{O}_K$	? (NO for some)	NO

H10/$\mathbb{Q}$

Variety/$\mathbb{Q}$ is assumed to be quasi-projective, $\bar{\mathbb{Q}}$-irreducible.

Proposition: H10/$\mathbb{Q}$ has a positive answer $\iff \exists$ algorithm to decide whether a given variety/$\mathbb{Q}$ has a rational point

(most general) $\iff \ldots$ algebraic set/$\mathbb{Q}$ $\ldots$

(most special) $\iff \ldots$ non-singular affine variety/$\mathbb{Q}$ $\ldots$

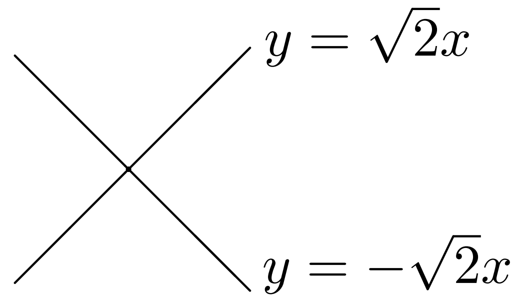
Proof:

- Suppose we have an algorithm for nonsingular affine varieties.
- We need to build an algorithm for algebraic sets.
- Let X be an algebraic set over $\mathbb{Q}$.
- The algorithm will be by induction on $\mathbf{dim} X$.

Step 1:

WLOG X is irreducible $/\mathbb{Q}$, otherwise decompose X into irreducible components $/\mathbb{Q}$

Example: $x^2 - 2y^2 = 0$



Step 2:

- WLOG X is irreducible over $\bar{\mathbb{Q}}$ (X is a variety)
- otherwise $\bar{\mathbb{Q}}$ irreducible components $Y_1, \ldots, Y_r$ are permuted transitively by $\mathbf{Gal}\left(\bar{\mathbb{Q}}/\mathbb{Q}\right)$
- If $p \in X(\mathbb{Q})$ is fixed by $\mathbf{Gal}\left(\bar{\mathbb{Q}}/\mathbb{Q}\right)$, then so if $p \in \bigcap Y_i$
- $\bigcap Y_i$ has lower dimension

Step 3:

- WLOG X is non-singular variety, otherwise $X = X^{\text{sing}} \cup X^{\text{non-sing}}$
- X^{sing} has lower dimension

Step 4:

Any non-singular variety is a finite union of affine varieties, which will be non-singular.

Definition:

- X algebraic set/$\mathbb{Q}$
- $S \subseteq X(\mathbb{Q})$
- Then S is diophantine $\iff \exists$ morphism of algebraic sets $f : Y \longrightarrow X$ such that $S = f(Y(\mathbb{Q}))$

Remark: Suppose $X = \mathbb{A}^n_{\mathbb{Q}}$ and $S \subseteq X(\mathbb{Q}) = \mathbb{Q}^n$

1. S is diophantine/$\mathbb{Q}$
2. $\iff S$ is diophantine/$\mathbb{Q}$ in the old sense
3. $\iff S$ is positive existential

$2 \implies 1$ $S = \{\vec{a} \in \mathbb{Q}^n \quad : \quad \exists \vec{x} \in \mathbb{Q}^m \quad p(\vec{a}, \vec{x}) = 0\}$

$p(\vec{a}, \vec{x})$ defines an algebraic subset $Y \subseteq \mathbb{A}^{n+m}$

$f : \mathbb{A}^{n+m} \longrightarrow \mathbb{A}^n$

$S = f(Y(\mathbb{Q}))$

$1 \implies 3$ OK