A Universal First-Order Formula for the Ring of Integers inside a Number Field
Presentation by Jennifer Park

1 Motivation

Hilbert's Tenth Problem over R; H10R: Is there an algorithm to decide, given a polynomial equation $f(x_1, \cdots, x_n) = 0$ with $f(x_1, \cdots, x_n) \in R[x_1, \cdots, x_n]$, whether or not it has a solution with $x_1, \cdots, x_n \in R$.

$H10(\mathbb{Q})$ (and $H10K$ for K a number field) are open.

A possible approach to produce a negative result for these question: Suppose that we can find a polynomial $p \in K[t, y_1, \cdots, y_m]$ such that $\mathcal{O}_K = \{a \in K \mid \exists \bar{b} \in K^m \, p(a, \bar{b}) = 0\}$.

Claim: If such a p exists, and if $H10\mathcal{O}_K$ is known to have a negative answer then H10K also has a negative answer.

Proof. Suppose for contradiction that there is an algorithm for H10K and let $f \in \mathcal{O}_K[x_1, \cdots, x_n]$. Consider the system of equations $f(x_1, \cdots, x_n) = 0, p(x_1, y_{11}, \cdots, y_{1m}) = 0, ..., p(x_n, y_{n1}, \cdots, y_{nm}) - 0$. Then by taking a degree two extension of K, $K(\sqrt{c})$, for two polynomials f, g we can express $f = 0 \wedge g = 0$ as $Nm(f + \sqrt{c}g) = 0$, which is again a polynomial. Then do induction. □

Definition 1. $A \subseteq R$ is Diophantine if $\exists n \in \mathbb{Z}_{>0}$ and $p \in R[t, y_1, \cdots, y_n]$ such that $A = \{a \in R \mid \exists \bar{b} \in R^n \, f(a, \bar{b}) = 0\}$

Theorem 1. *(Robinson, 1949) There is a polynomial $q \in \mathbb{Q}[t, x_1, x_2, y_1, \cdots, y_7, z_1, \cdots, z_6]$ such that $\mathbb{Z} = \{t \in \mathbb{Q} \mid \forall a_1, a_2 \exists b_1, \cdots, b_7 \forall c_1, \cdots, c_6 \in \mathbb{Q} \; g(t, a_1, a_2, b_1, \cdots, b_7, c_1, \cdots, c_6) = 0\}$*

Theorem 2. *(Poonen, 2009) There is a polynomial $h \in K[t, x_1, x_2, y_1, \cdots, y_7]$ satisfying $\mathcal{O}_K = \{t \in K \mid \forall a_1, a_2 \exists b_1, \cdots, b_7 \in K \; h(t, a_1, a_2, b_1, \cdots, b_7) = 0\}$.*

Theorem 3. *(Koenigsman) There is a polynomial $f \in \mathbb{Q}[t, x_1, \cdots, x_{418}]$ satisfying $\mathbb{Z} = \{t \in \mathbb{Q} \mid \forall a_1, \cdots, a_{418} \in \mathbb{Q} \; h(t, a_1, \cdots, a_{418}) = 0\}$. $\mathbb{Q} \setminus \mathbb{Z}$ is Diophantine.*

Theorem 4. *Park, 2012 $K \setminus \mathcal{O}_K$ is Diophantine.*

2 $\mathbb{Q} \setminus \mathbb{Z}$ is Diophantine

The idea is to use the following Diophantine sets as building blocks: for $a, b \in \mathbb{Q}^\times$

$$S_{a,b} := \{2x_1 \in \mathbb{Q} \, : \, \exists x_2, x_3, x_4 \in \mathbb{Q} \; x_1^2 - ax_2^2 - bx_3^2 + abx_4^2 = 1\}$$

The trace of norm one elements of a, b: $T_{a,b} = S_{a,b} + S_{a,b}$, which is diophantine as it is $\{x_1 + x_2 \mid \exists x_1, x_2 \in S_{a,b}\}$.

Koenigmann showed: $\bigcap_{p \in \mathbb{Q}^\times} (T_{-1,p} + T_{-2,p}) = \bigcap_{p \equiv 3 \mod 8, p \text{ prime}} \mathbb{Z}_{(p)}$

$\bigcap_{p \in \mathbb{Q}^\times} (T_{2,p} + T_{-2,p}) = \bigcap_{p \equiv 5 \mod 8, p \text{ prime}} \mathbb{Z}_{(p)}$

$\bigcap_{p \in \mathbb{Q}^\times} (T_{-1,p} + T_{2,p}) = \bigcap_{p \equiv 7 \mod 8, p \text{ prime}} \mathbb{Z}_{(p)}$

$\bigcap_{p\in\mathbb{Q}^\times}(T_{-p,q}+T_{2p,q}) = \bigcap_{p\equiv 1 \mod 8, p \text{ prime}} \mathbb{Z}_{(p)}$
Using this you can show that $\mathbb{Z}_{(2)}$ is diophantine. Then
$\mathbb{Z} = \mathbb{Z}_2 \cap \bigcap_{p\in\mathbb{Q}^\times} [(T_{-1,p}+T_{-2,p})\cap \cdots \uparrow$
which gives a $\forall\exists$ definition of $\mathbb{Z}$ in $\mathbb{Q}$.
To get an $\forall$ definition:

Proposition 1. *1.* $T_{a,b}+T_{c,d} = \bigcap_{p \text{ prime},(a,b)_p=(c,d)_p=-1} \mathbb{Z}_{(p)}$.

2. *If the Jacobson radical of the ring $T_{a,b}+T_{c,d}$ is Diophantine then $\bigcup_{p \text{ prime},(a,b)_p=(c,d)_p=-1} \mathbb{Z}_{(p)}$ is defined with one universal quantifier.*

3. *Most of the rings appearing above have diophantine Jacobson radical, and*

$$\mathbb{Z} = \mathbb{Z}_{(2)} \cap \bigcap_{p,q\in\mathbb{Q}^\times} \Big(\bigcup_{\ell \text{ prime},(-1,\ell)_p=(-2,\ell)_p=-1} \mathbb{Z}_{(\ell)} \cdots \Big)$$

3 Over Number Fields

Biggest obstruction: how to generalize things like $p\equiv 3 \mod 8$? Look more closely at the Hilbert symbol.

$S_{a,b}(K) := \{2x_1\in K \,:\, \exists x_2,x_3,x_4\in K\ x_1^2-ax_2^2-bx_3^2+abx_4^2=1\}$
If $\sqrt{-1},\sqrt{-2}\in K$ then $\bigcap_{p\in\mathbb{Q}^\times}(T_{-1,p}(K)+T_{-2,p}(K)) = K$.
Question: What number theoretic construction gives

$$T_{a,b}(K)+T_{c,d}(K) = \bigcap_{\mathfrak{p} \text{ prime},(a,b)_\mathfrak{p}=(c,d)_\mathfrak{p}=-1} (\mathcal{O}_K)_\mathfrak{p}$$

What is known is that if $a,b\in K^\times$ then $(a,b)_\mathfrak{p} = ((-1)^{\nu_\mathfrak{p}(a)\nu_\mathfrak{p}(b)} red_\mathfrak{p}(\frac{a^{\nu_\mathfrak{p}(b)}}{b^{\nu_\mathfrak{p} a)}}) \dfrac{q-1}{2}$
for $q=|\mathbb{F}_\mathfrak{p}|$.

Suppose that a is a p-adic unit. Then $(a,p)_\nu=-1$ if and only if $\nu(p)$ is odd and $red_\nu(a)$ in $\mathbb{F}_\nu$ is not a square.

$red_\nu(a)\in\mathbb{F}_\nu^2$ if and only if $a\in(K_\nu^\times)^2$ if and only if $\mathfrak{p}_\nu$ splits in $K(\sqrt{a})/K$.

Artin Homomorphism: Given L/K a finite extension, $L=K(\sqrt{a})$ we have the morphism $\psi: I^s\to Gal(L/K)\cong\{\pm1\}$ that maps $\mathfrak{p}\to(a/\mathfrak{p})$ Legendre symbol $=1$ is a is a square mod $\mathfrak{p}$ and -1 otherwise.

And consider the map $\psi: I^s\to Gal(K(\sqrt{a},\sqrt{b})/K)\cong\{\pm1\}^2$ mapping $\mathfrak{p}\mapsto[(a/\mathfrak{p}),(b/\mathfrak{p})]$ (Legendre symbols).

Using these maps we can show

Proposition 2. $\bigcap_{p\in K^\times} T_{p,a}(K)+T_{p,b}(K) = \bigcap_{\mathfrak{p} \text{ prime},\psi(\mathfrak{p})=(-1,-1)} (\mathcal{O}_K)_\mathfrak{p}$

Given this proposition, much of Koenigsman's previous argument goes through and the result is proved.