Diophantine Definability and Decidability in the Extensions of Degree 2 of Totally Real Fields

Alexandra Shlapentokh

East Carolina University

Model Theory and Computable Model Theory
University of Florida, February 2007

Table of Contents

Hilbert's Question about Polynomial Equations

Is there an algorithm which can determine whether or not an arbitrary polynomial equation in several variables has solutions in integers?

This problem became known as Hilbert's Tenth Problem

The Answer

This question was answered negatively (with the final piece in place in 1970) in the work of Martin Davis, Hilary Putnam, Julia Robinson and Yuri Matijasevich. Actually a much stronger result was proved. It was shown that the recursively enumerable subsets of $\mathbb{Z}$ are the same as the Diophantine subsets of $\mathbb{Z}$.

Diophantine Sets

Diophantine Sets

A subset $A \subset \mathbb{Z}$ is called Diophantine over $\mathbb{Z}$ if there exists a polynomial $p(T, X_1, \ldots, X_k)$ with rational integer coefficients such that for any element $t \in \mathbb{Z}$ we have that

$$(\exists x_1, \ldots, x_k \in \mathbb{Z} : p(t, x_1, \ldots, x_k) = 0) \Longleftrightarrow t \in A.$$

In this case we call $p(T, X_1, \ldots, X_k)$ a Diophantine definition of A over $\mathbb{Z}$.

Corollary

There are undecidable Diophantine subsets of $\mathbb{Z}$.

A General Question

A Question about an Arbitrary Recursive Ring R

Is there an algorithm, which if given an arbitrary polynomial equation in several variables with coefficients in R, can determine whether this equation has solutions in R?

Arguably, the most important open problems in the area concern the Diophantine status of the ring of integers of an arbitrary number field and the Diophantine status of $\mathbb{Q}$.

One vs. Finitely Many

Replacing Finitely Many by One

- We can let Diophantine definitions consist of several equations without changing the nature of the relation.
- Any finite system of equations over $\mathbb{Z}$ can be effectively replaced by a single polynomial equation over $\mathbb{Z}$ with the identical $\mathbb{Z}$-solution set.
- The statements above remain valid if we replace $\mathbb{Z}$ by any recursive integral domain R whose fraction field is not algebraically closed.

Using Diophantine Definitions to Solve the Problem

Lemma

Let R be a recursive ring of characteristic 0 such that $\mathbb{Z}$ has a Diophantine definition $p(T, \bar{X})$ over R. Then HTP is not decidable over R.

Proof.

Let $h(T_1, \ldots, T_l)$ be a polynomial with rational integer coefficients and consider the following system of equations.

$$\left\{\begin{array}{c} h(T_1, \ldots, T_l) = 0 \\ p(T_1, \bar{X}_1) = 0 \\ \ldots \\ p(T_l, \bar{X}_l) = 0 \end{array}\right. \tag{1}$$

It is easy to see that $h(T_1, \ldots, T_l) = 0$ has solutions in $\mathbb{Z}$ iff (1) has solutions in R. Thus if HTP is decidable over R, it is decidable over $\mathbb{Z}$. $\square$

The Rings of Integers of Number Fields.

Theorem

$\mathbb{Z}$ has a Diophantine definition over the rings of integers of the following fields:

- *Extensions of degree 4, totally real number fields (i.e. finite extensions of $\mathbb{Q}$ all of whose embeddings into $\mathbb{C}$ are real) and their extensions of degree 2. (Denef, 1980 & Denef, Lipshits, 1978) Note that these fields include all Abelian extensions.*
- *Number fields with exactly one pair of non-real embeddings (Pheidas, S. 1988)*
- *Any number field K such that there exists an elliptic curve E of positive rank defined over $\mathbb{Q}$ with $[E(K) : E(\mathbb{Q})] < \infty$. (Poonen, S. 2003)*
- *Any number field K such that there exists an elliptic curve of rank 1 over K and an Abelian variety over $\mathbb{Q}$ keeping its rank over K. (Cornelissen, Pheidas, Zahidi, 2005)*

HTP over $\mathbb{Q}$

To show that HTP is undecidable over $\mathbb{Q}$ it would be enough construct a Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$ or more generally a Diophantine model of $\mathbb{Z}$ over $\mathbb{Q}$.

Definition

Let R_1, R_2 be recursive rings. Then a Diophantine model of R_1 over R_2 is an injective recursive map $\phi : R_1 \longrightarrow R_2$ such that ϕ maps Diophantine sets to Diophantine sets.

Corollary

If a ring R has a Diophantine model of $\mathbb{Z}$, then HTP is undecidable over R.

Mazur's Archimedean Conjecture

The Conjecture on the Topology of Rational Points

Let V be any variety over $\mathbb{Q}$. Then the topological closure of $V(\mathbb{Q})$ in $V(\mathbb{R})$ possesses at most a finite number of connected components.

Corollary

There is no Diophantine definition of any infinite discrete in archimedean topology set over $\mathbb{Q}$. In particular there is no Diophantine definition of $\mathbb{Z}$ over $\mathbb{Q}$.

Mazur's Non-Archimedean Conjecture

The Non-Archimedean Conjecture

Let V be any variety defined over a number field K. Let $\mathcal{S}$ be a finite set of places of K, and consider $K_{\mathcal{S}} = \prod_{v \in \mathcal{S}} K_v$ viewed as locally compact topological ring. Let $V(K_{\mathcal{S}})$ denote the topological space of $K_{\mathcal{S}}$-rational points. For every point $p \in V(K_{\mathcal{S}})$ define $W(p) \subset V$ to be the subvariety defined over K that is the intersection of Zariski closures of the subsets $V(K) \cap U$, where U ranges through all open neighborhoods of p in $V(K_{\mathcal{S}})$. As p ranges through the points of $V(K_{\mathcal{S}})$, are there only a finite number of distinct subvarieties $W(p)$?

Corollary

No infinite $\mathfrak{p}$-adically discrete set has a Diophantine definition over a number field K for any K-prime $\mathfrak{p}$. Consequently there is no Diophantine definition of $\mathbb{Z}$ over any number field, including $\mathbb{Q}$.

A Theorem of Cornelissen and Zahidi

Theorem

If Mazur's conjecture on topology of rational points holds, then there is no Diophantine model of $\mathbb{Z}$ *over* $\mathbb{Q}$.

The Rings between the Ring of Integers and a Number Field

A Ring in the Middle of $\mathbb{Q}$

Let $\mathcal{V}$ be a set of primes of $\mathbb{Q}$. Let $O_{\mathbb{Q},\mathcal{V}}$ be the following subring of $\mathbb{Q}$.

$$\{\frac{m}{n} : m, n \in \mathbb{Z}, n \neq 0, n \text{ is divisible by primes of } \mathcal{V} \text{ only } \}$$

If $\mathcal{V} = \emptyset$, then $O_{\mathbb{Q},\mathcal{V}} = \mathbb{Z}$. If $\mathcal{V}$ contains all the primes of $\mathbb{Q}$, then $O_{\mathbb{Q},\mathcal{V}} = \mathbb{Q}$. If $\mathcal{V}$ is finite, we call the ring small. If $\mathcal{V}$ is infinite, we call the ring big or large.

A Ring in the Middle of a Number Field K.

Let $\mathcal{V}$ be a set of primes of a number field K. Then define

$$O_{K,\mathcal{V}} = \{x \in K : \mathrm{ord}_{\mathfrak{p}}\, x \geq 0\ \forall \mathfrak{p} \notin \mathcal{V}\}.$$

As above, if $\mathcal{V}$ is finite, call the ring small and call the ring big or large otherwise.

Definability over Small Subrings of Number Fields

Theorem

Let K be a number field. Let $\mathfrak{p}$ be a non-archimedean prime of K. Then the set of elements of K integral at $\mathfrak{p}$ is Diophantine over K. (Julia Robinson and others)

Theorem

Let K be a number field. Let $\mathcal{S}$ be any set of non-archimedean primes of K. Then the set of non-zero elements of $O_{K,\mathcal{S}}$ is Diophantine over $O_{K,\mathcal{S}}$. (Denef, Lipshitz)

Corollary

- *$\mathbb{Z}$ has a Diophantine definition over the small subrings of $\mathbb{Q}$.*
- *HTP is undecidable over the small subrings of $\mathbb{Q}$.*

Corollary

For any number field K, if $\mathbb{Z}$ has a Diophantine definition over O_K, then $\mathbb{Z}$ has a Diophantine definition over any small subring of K

Definability of $\mathbb{Z}$ over Large Subrings of Number Fields

Theorem

Let K be a number field satisfying one of the following conditions:

- *K is a totally real filed.*
- *K is an extension of degree 2 of a totally real field.*
- *There exists or an elliptic curve E defined over $\mathbb{Q}$ such that $[E(K) : E(\mathbb{Q})] < \infty$.*

Let $\varepsilon > 0$ be given. Then there exists a set $\mathcal{S}$ of non-archimedean primes of K such that

- *The natural density of $\mathcal{S}$ is greater $1 - \dfrac{1}{[K : \mathbb{Q}]} - \varepsilon$.*
- *$\mathbb{Z}$ is a Diophantine subset of $O_{K,\mathcal{S}}$.*
- *HTP is undecidable over $O_{K,\mathcal{S}}$.*

(S. 2002, 2003, 2006)

Note that this result says nothing about subrings of $\mathbb{Q}$.

Ring Version of Mazur's Conjectures

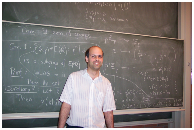
The Archimedean Conjecture

Let K be a number field and let $\mathcal{W}$ be a set of non-archimedean primes of K. Let V be any affine algebraic set defined over K. Let $\overline{V(O_{K,\mathcal{W}})}$ be the topological closure of $V(O_{K,\mathcal{W}})$ in $\mathbb{R}$ if $K \subset \mathbb{R}$ or in $\mathbb{C}$, otherwise. Then how many connected components does $\overline{V(O_{K,\mathcal{W}})}$ have?

The Non-archimedean Conjecture

Let K be a number field and let $\mathcal{W}$ be a set of non-archimedean primes of K. Let $\mathfrak{p}$ be a K-prime. Then is there an infinite $\mathfrak{p}$-adically discrete subset of $O_{K,\mathcal{W}}$ with a Diophantine definition over $O_{K,\mathcal{W}}$?

Ring Version of Mazur's Archimedean Conjecture over $\mathbb{Q}$: Poonen's Theorem, 2003



Theorem

There exist recursive sets of rational primes $\mathcal{T}_1$ and $\mathcal{T}_2$, both of natural density zero and with an empty intersection, such that for any set $\mathcal{S}$ of rational primes containing $\mathcal{T}_1$ and avoiding $\mathcal{T}_2$, the following hold:

- *There exists an affine curve E defined over $\mathbb{Q}$ such that the topological closure of $E(O_{\mathbb{Q},\mathcal{S}})$ in $E(\mathbb{R})$ is an infinite discrete set. Thus the ring version of Mazur's archimedean conjecture does not hold for $O_{\mathbb{Q},\mathcal{S}}$.*
- *$\mathbb{Z}$ has a Diophantine model over $O_{\mathbb{Q},\mathcal{S}}$.*
- *Hilbert's Tenth Problem is undecidable over $O_{\mathbb{Q},\mathcal{S}}$.*

Ring Version of Mazur's Conjectures over Number Fields, Part I

Totally Real Number Fields and Their Extensions of Degree 2.

Let K be a totally real number field (including $\mathbb{Q}$) or an extension of degree 2 of a totally real number field.

- For any $\varepsilon > 0$ and any archimedean topology of K there exists a set $\mathcal{W}$ of natural density greater than $1 - \varepsilon$ such that some infinite discrete in the archimedean topology subset of $O_{K,\mathcal{W}}$ is Diophantine over $O_{K,\mathcal{W}}$. (S. 2003, 2006)
- For any $\varepsilon > 0$ and any prime $\mathfrak{p}$ of K there exists a set $\mathcal{W}$ of natural density greater than $1 - \varepsilon$ such that some infinite discrete in the $\mathfrak{p}$-adic topology subset of $O_{K,\mathcal{W}}$ is Diophantine over $O_{K,\mathcal{W}}$. (Poonen, S. 2005, S. 2006)

Fields with One Pair of Non-real Embeddings

Let K be a number field with one pair of non-real embeddings into its algebraic closure. Then for some set $\mathcal{W}$ of natural density $1/2$, the ring $O_{K,\mathcal{W}}$ has an infinite Diophantine subset discrete in an archimedean topology of the field. (S. 2003)

Ring Version of Mazur's Conjectures over Number Fields, Part II

Fields with Elliptic Curves of Rank 1

Let K be a number field with a rank one elliptic curve.

- For some set $\mathcal{W}$ of K-primes of natural density 1 there exists an infinite subset of the ring $O_{K,\mathcal{W}}$ which is discrete in every topology (archimidean and non-archimedean) of K.
- For some set $\mathcal{W}$ of K-primes of natural density 1, the ring $O_{K,\mathcal{W}}$ has a Diophantine model of $\mathbb{Z}$ and thus HTP is undecidable over $O_{K,\mathcal{W}}$.

(Poonen, S. 2005)

Close to Algebraic Closure

If the fields are "close" enough to the algebraic closure of $\mathbb{Q}$ one starts to get decidability results not just for HTP but also for the first order theory. (See results by Rumely, Van den Dries, Macintyre, Jarden, Razon, Prestel, Green, Pop, Roquette, Moret-Bailly, and others.) So if we are looking for undecidability we should stay "far" away from the algebraic closure.

Denef's Theorem for Infinite Extensions of $\mathbb{Q}$, 1980

Theorem

Let K be a totally real field (possibly of infinite degree) such that for some elliptic curve E defined over $\mathbb{Q}$, the rank of E over $\mathbb{Q}$ is positive and the same as over K. Then the ring of integers of K has a Diophantine definition of $\mathbb{Z}$.

More Terminology

Integral Closure

Let $R_1 \subset R_2$ be integral domains. Then the integral closure of R_1 in R_2 is the set of elements of R_2 satisfying monic irreducible polynomials with coefficients in R_1.

Big and Small Rings in Infinite Extensions

Let K_∞ be an infinite algebraic extension of $\mathbb{Q}$. Let K be any number field contained in K_∞. Let $\mathcal{W}_K$ be a set of primes of K and let R be the integral closure of $O_{K,\mathcal{W}_K}$ in K_∞. Then we call R big or large if $\mathcal{W}_K$ is infinite, and we call R small otherwise. We denote R by $O_{K_\infty,\mathcal{W}_{K_\infty}}$.

Some Results on Definability in Big and Small Rings in Totally Real Infinite Extensions

Theorem

Every totally real subfield of a cyclotomic extension with finitely many ramified primes contains a small subring, not equal to the ring of integers, where $\mathbb{Z}$ is existentially definable and HTP is unsolvable. (S. 1994)

Theorem

Every totally real subfield K_∞ of a cyclotomic extension with finitely many ramified primes contains a big subring R where $\mathbb{Z}$ is existentially definable and HTP is unsolvable. Further for any $\varepsilon > 0$ it can be arranged that R is the integral closure of a ring $O_{K,\mathcal{W}_K}$, where K is a number field contained in K_∞ and the natural density of $\mathcal{W}_K$ is greater than $1 - \varepsilon$. (S. 2004)

New results

Theorem

Let K_∞ be a totally real subfield of a cyclotomic extension with finitely many ramified rational primes and a finite ramification degree for 2. Let G_∞/K_∞ be any extension of degree 2. Let $K \neq \mathbb{Q}$ be a totally real number field contained in G_∞. Then for some large subring $O_{K,\mathcal{R}_K}$ of K we have that $\mathbb{Z}$ is existentially definable its integral closure $O_{G_\infty,\mathcal{R}_{G_\infty}}$ in G_∞.

Theorem

Let K_∞ be a totally real subfield of a cyclotomic extension with finitely many ramified rational primes. Let G_∞/K_∞ be any extension of degree 2. Let K be a number field contained in G_∞. Then for any small subring $O_{K,\mathcal{S}_K}$ of K, not equal to the ring of integers of K, we have that $\mathbb{Z}$ is existentially definable in its integral closure $O_{G_\infty,\mathcal{S}_{G_\infty}}$ in G_∞.

A Corollary

Theorem

Let A_∞ be an abelian (possibly infinite) extension of $\mathbb{Q}$ with finitely many ramified primes. Then the following statements are true.

- *If the ramification degree of 2 is finite, then for any number field A contained in A_∞ and not equal to $\mathbb{Q}$, there exists an infinite set of A-primes $\mathcal{W}_A$ such that $\mathbb{Z}$ is existentially definable in the integral closure of $O_{A,\mathcal{W}_A}$ in A_∞. Thus, HTP is undecidable over the integral closure of $O_{A,\mathcal{W}_A}$ in A_∞ and both archimedean and non-archimedean ring versions of Mazur's conjectures are false for this ring.*
- *For any number field $A \subset A_\infty$ and any finite non-empty set $\mathcal{S}_A$ of its primes, we have that $\mathbb{Z}$ is existentially definable in the integral closure of $O_{A,\mathcal{S}_A}$ in A_∞. Thus HTP is undecidable over the integral closure of $O_{A,\mathcal{S}_A}$ in A_∞.*

What Needed to Be Done for Big Rings

Let K_∞ be a totally real subfield of a cyclotomic extension with finitely many ramified rational primes and a finite ramification for 2. Let K be a number field contained in K_∞. Let G be an extension of degree 2 of K. Let E_1, E_2 be two cyclic extensions of K. Let $\mathcal{W}_K$ be a set of K-primes inert in the extension E_1E_2G/K. Let $G_\infty = GK_\infty$. Then show that there exists a positive integer n and a polynomial $F(t, \bar{x}) \in K[t, \bar{x}]$ satisfying the following conditions. For any $t \in O_{G_\infty, \mathcal{W}_{G_\infty}}$, if there exists $\bar{x} \in (O_{K_\infty, \mathcal{W}_{K_\infty}})^n$ such that $F(t, \bar{x}) = 0$, then $t \in O_{K_\infty, \mathcal{W}_{K_\infty}}$. Further, if $t \in O_{G_\infty, \mathcal{W}_{G_\infty}} \cap K$, there exist $\bar{x} \in (O_{K, \mathcal{W}_K})^n$ such that $F(t, \bar{x}) = 0$.

What Needed to Be Done for Small Rings

Let K_∞ be a totally real subfield of a cyclotomic extension with finitely many ramified rational primes. Let K be a number field contained in K_∞. Let G be an extension of degree 2 of K. Let $G_\infty = GK_\infty$. Let $\mathcal{S}_K$ be a non-empty set of K-primes. Then show that there exists a positive integer n and a polynomial $F(t, \bar{x}) \in K[t, \bar{x}]$ satisfying the following conditions. For any $t \in O_{G_\infty, \mathcal{S}_{G_\infty}}$, if there exists $\bar{x} \in (O_{K_\infty, \mathcal{S}_{K_\infty}})^n$ such that $F(t, \bar{x}) = 0$, then $t \in O_{K_\infty, \mathcal{S}_{K_\infty}}$. Further, if $t \in O_{G_\infty, \mathcal{S}_{G_\infty}} \cap K$, there exist $\bar{x} \in (O_{K, \mathcal{S}_K})^n$ such that $F(t, \bar{x}) = 0$.

The Weak Vertical Method

The Main Idea

If an *element above* is equivalent to an *element below* modulo sufficiently *large element below*, then the *element above* is really *below*.

The Weak Vertical Method for Integers and Extensions of Degree 2

Proposition

Assume the following.

- K_∞ is an algebraic extension of $\mathbb{Q}$.
- G_∞ is an extension of degree 2 of K_∞.
- $x \in O_{G_\infty}$
- $\alpha \in O_{G_\infty}, G_\infty = K_\infty(\alpha), \alpha^2 = a \in K_\infty$.
- $x = y_1 + y_2\alpha, y_1, y_2 \in K_\infty$.
- $z, w \in O_{K_\infty}$.
- $x \equiv z \mod w$ in O_{G_∞}
- For any embedding $\sigma : G_\infty \longrightarrow \tilde{\mathbb{Q}}$ (the algebraic closure of $\mathbb{Q}$) we have that $|\sigma(2\alpha y_2)| < |\sigma(w)|$.

Then $x \in K_\infty$.

Proof

Let M be a number field such that $M \subset K_\infty$ and $a = \alpha^2, y_1, y_2, z, w \in M$. Then

$$\mathbf{N}_{M/\mathbb{Q}}(w) > \mathbf{N}_{M/\mathbb{Q}}(2\alpha y_2).$$

Let

$$\bar{x} = y_1 - \alpha y_2$$

be the conjugate of x over K_∞ and note that

$$\bar{x} \equiv z \mod w \text{ in } O_{G_\infty}$$

also. Therefore

$$2\alpha y_2 = x - \bar{x} \equiv 0 \mod w.$$

(Observe that since $x, \bar{x} \in O_{G_\infty}$ we also have $2\alpha_1 y_2$ in O_{G_∞}.) Hence, either

$$y_2 = 0 \text{ or } \mathbf{N}_{M/\mathbb{Q}}(w) \leq \mathbf{N}_{M/\mathbb{Q}}(2\alpha y_2).$$

The second option leads to a contradiction.

Ingredients of the Weak Vertical Method

- We need a polynomial equation $P(t_1, \dots, t_m, x_1, \dots, x_k)$ with coefficients in G_∞ such that if
$$P(t_1, \dots, t_m, x_1, \dots, x_k) = 0$$
has solutions in the ring under consideration in G_∞, it is the case that $t_1, \dots, t_m \in K_\infty$. (*This is done using norm equations of units.*)
- We need to be able to use $t_1, \dots, t_m$ to construct rational integers in some way. (*We use powers of units to accomplish this task.*)
- We need to be able to bound absolute value of all the conjugates in a "Diophantine manner". (*Here we use sum of squares for real embeddings, and the fact that complex conjugates have the same absolute value for complex embeddings.*) This part also requires bounding order at finitely many primes over infinite extensions. (*We generalize methods used over number fields.*)

Solutions Above and Below with Integral Units

Proposition (Denef, Lipshitz, 1979)

Let M be a totally real number field. Let G be an extension of degree 2 of M generated by $\alpha \in O_G$ such that $\alpha^2 = a \in M$ and G is not totally real. Next let $b \in O_M$ be such that for any embedding $\sigma : M \longrightarrow \tilde{\mathbb{Q}}$ we have that $\sigma(a)\sigma(b) < 0$. Let $\beta \in \tilde{\mathbb{Q}}$ be such that $\beta^2 = b$ and let $H = M(\beta)$. Let $\varepsilon \in O_{GH}$ and assume that

$$\mathbf{N}_{GH/G}(\varepsilon) = 1$$

Then for some positive integer k we have that $\varepsilon^k \in O_H$. Further there are solutions to this norm equation which are not roots of unity.

Proof

Let

$$A_{GH} = \{\varepsilon \in O_{GH} : \mathbf{N}_{GH/G}(\varepsilon) = 1\}.$$

Let

$$A_H = \{\varepsilon \in O_H : \mathbf{N}_{H/M}(\varepsilon) = 1\}.$$

Let $[M : \mathbb{Q}] = n$, $[G : \mathbb{Q}] = 2n$ and $[GH : \mathbb{Q}] = 4n$. Let $s_G > 0$ be the number of pairs non-real embeddings of G into $\tilde{\mathbb{Q}}$. Let r_G be the number of real embeddings of G into $\tilde{\mathbb{Q}}$. (Thus $r_G + 2s_G = 2n$).
Given our assumptions, all of the embeddings of GH into $\tilde{\mathbb{Q}}$ are non-real and there are $2n$ conjugate pairs of these embeddings. The rank of A_{GH} is $(2n-1) - (r_G + s_G - 1) = r_G + 2s_G - r_G - s_G = s_G$. The rank of A_H is $r_G/2 + 2s_G - 1 - (n-1) = s_G$. So the ranks of A_{GH} and A_H are the same. Further, since H and G are linearly disjoint over K, we also have that $A_H \subseteq A_{GH}$ and thus the proposition holds.

Proposition: A Version for Infinite Extensions

Let K_∞ be a totally real field. Let G_∞ be an extension of degree 2 of K_∞ generated by $\alpha \in O_{G_\infty}$ such that $\alpha^2 = a \in K_\infty$. Next let $b \in O_{K_\infty}$ be such that for any embedding $\sigma : K_\infty \longrightarrow \tilde{\mathbb{Q}}$ we have that $\sigma(a)\sigma(b) < 0$. Let $\beta \in \tilde{\mathbb{Q}}$ be such that $\beta^2 = b$ and let $H_\infty = K_\infty(\beta)$. Let $\varepsilon \in O_{G_\infty H_\infty}$ and assume that

$$\mathbf{N}_{G_\infty H_\infty / G_\infty}(\varepsilon) = 1$$

Then for some positive integer k we have that $\varepsilon^k \in O_{H_\infty}$.

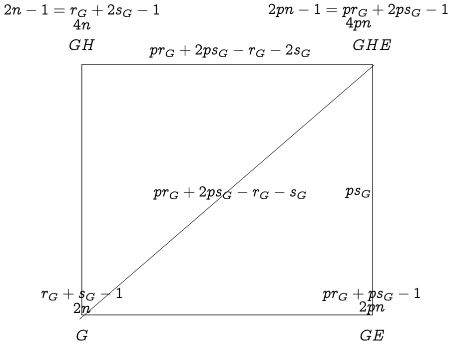
Norm Equations of Units for Larger Rings

Lemma

Let M, G, H, α, β be as before. Let E be a totally real cyclic extension of M of prime degree p. Let $\mathcal{W}_M$ be a set of primes of M not splitting in the extension E/M of degree p. Then there exists $\varepsilon \in O_{HGE}$ such that ε is not a root of unity and is a solution to the system (2). Further, for any $\varepsilon \in O_{GHE,\mathcal{W}_{GHE}}$ (the integral closure of $O_{M,\mathcal{W}_M}$ in GHE) that is a solution to (2), we have that for some positive integer k it is the case that $\varepsilon^k \in O_{HE}$. If we assume that all the roots of unity in GHE are already in GE, we can replace k by 2.

$$\begin{cases} \mathbf{N}_{HGE/GE}(\varepsilon) = 1, \\ \mathbf{N}_{HGE/HG}(\varepsilon) = 1. \end{cases} \tag{2}$$

Proof Outline, Part I: Existence of Integral Solutions



Let

$$A_G = \{x \in O_{GHE} : \mathbf{N}_{GHE/G}(x) = 1\},$$
$$A_{GH} = \{x \in O_{GHE_2} : \mathbf{N}_{GHE/GH}(x) = 1\},$$
$$A_{GE} = \{x \in O_{HGE} : \mathbf{N}_{HGE/GE}(x) = 1\},$$

It is clear that $A_{GH} \cup A_{GE} \subseteq A_G$. By computing the ranks of the integral unit groups involved we show that

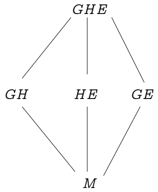
$$\operatorname{rank} A_{GH} + \operatorname{rank} A_{GE} > \operatorname{rank} A_G.$$

Proof Outline, Part II: All Solutions Are Integral

$$\begin{tikzcd} E \arrow[r, dash, "4"] \arrow[d, dash, "p"'] & GHE \arrow[d, dash, "p"] \\ M \arrow[r, dash, "4"'] & GH \end{tikzcd}$$

By assumption all the primes of $\mathcal{W}_M$ are inert in the extension E/M. Given that $[E:M] = p$, where p is an odd prime, $[GH:M] = 4$, and all the extensions are Galois, a counting argument shows that a GH-prime $\mathfrak{p}_{GH}$ above an M-prime $\mathfrak{p}_M \in \mathcal{W}_M$, is inert in the extension GHE/GH. At the same time, any $x \in O_{GHE,\mathcal{W}_{GHE}}$ satisfying $\mathbf{N}_{HGE/HG}(x) = 1$ must have a divisor composed of GHE-primes lying above GH-primes splitting in the extension GHE/GH, and, in particular, any prime in the denominator of x must lie above a GH primes splitting in the extension GHE/GH. But the only primes in the denominators of the divisors of elements of $O_{GHE,\mathcal{W}_{GHE}}$ are primes of $\mathcal{W}_{GHE}$ lying above primes of $\mathcal{W}_{GH}$ inert in the extension GHE/GH. Thus the divisor of x is trivial and it is an integral unit.

Proof Outline, Part III: Roots of Unity



- By Parts I and II, if $\varepsilon \in O_{GHE,\mathcal{W}_{GHE}}$ has the GE and GH norms equal to 1, then $\varepsilon \in O_{GHE}$ (and such integral units exist).
- By Denef-Lipshitz argument, if $\varepsilon \in O_{GHE}$ and has the GE norm equal to 1, then for some $k \in \mathbb{Z}_{>0}$ we have that $\varepsilon^k \in HE$.
- Let $\bar{\varepsilon}$ be the conjugate of ε over HE. Then $\bar{\varepsilon}^k \in HE$ also. Further the GE norm of $\bar{\varepsilon}$ is 1. Hence, $\frac{\varepsilon}{\bar{\varepsilon}} = \xi$ is a root of unity of order at most k and its GE norm equal to 1.
- If we assume that $\xi \in GE$, then its GE norm is ξ^2 and thus k is at most 2.

Over Infinite Extensions

Lemma

Let K_∞ be a totally real field. Let G_∞, H_∞ be two extensions of degree 2 of K_∞ generated by α, β respectively with $\alpha^2 = a, \beta^2 = b \in O_{K_\infty}$ satisfying $\sigma(a)\sigma(b) < 0$ for all embeddings σ of K_∞ into $\tilde{\mathbb{Q}}$. Let E be a totally real cyclic extension of K_∞ of prime degree p generated by $\gamma \in O_{E_\infty}$. Let K be a number field contained in K_∞ such that K_∞/K is a normal extension, $[K(\gamma) : K] = p$, $[K(\alpha) : K] = [K(\beta) : K] = 2$ and for every number field M with $K \subseteq M \subset K_\infty$ we have that $[M : K] \not\equiv 0 \mod p$. Let $\mathcal{W}_K$ be a set of primes of K inert in the extension $K(\gamma)/K$. Then there exists $\varepsilon \in O_{H_\infty G_\infty E_\infty}$ such that ε is not a root of unity and is a solution to the system (3). Further, for any $\varepsilon \in O_{G_\infty H_\infty E_\infty, \mathcal{W}_{G_\infty H_\infty E_\infty}}$ (the integral closure of $O_{K,\mathcal{W}_K}$ in $G_\infty H_\infty E_\infty$) that is a solution to (3), we have that for some positive integer k it is the case that $\varepsilon^k \in O_{H_\infty E_\infty}$. If we assume that all the roots of unity in $G_\infty H_\infty E_\infty$ are already in $G_\infty E_\infty$, we can replace k by 2.

$$\begin{cases} \mathbf{N}_{H_\infty G_\infty E_\infty / G_\infty E_\infty}(\varepsilon) = 1, \\ \mathbf{N}_{H_\infty G_\infty E_\infty / H_\infty G_\infty}(\varepsilon) = 1. \end{cases} \tag{3}$$

Generating Integers and Bounds

Producing Integers the Old-fashioned Way

$$\frac{\varepsilon^n - 1}{\varepsilon - 1} \cong n \mod (\varepsilon - 1) \text{ in } \mathbb{Z}[\varepsilon].$$

Proposition on Bounds

Let M be a totally real number field and let G be an extension of degree two of M generated by $\alpha \in O_G$ with $\alpha^2 \in O_M$. Suppose $x \in M, x = y_1 + y_2\alpha$. Let $z \in M$ and suppose that for all the real embeddings σ of G into $\tilde{\mathbb{Q}}$ we have that $1 \leq \sigma(x) < \sigma(z)$ and all conjugates of z are bigger than 1. Then $|\mathbf{N}_{M/\mathbb{Q}}(y_2\alpha)| < |\mathbf{N}_{M/\mathbb{Q}}(x)\mathbf{N}_{M/\mathbb{Q}}(z)|$.

Generating Integers and Bounds, continued

Proof of the Proposition on Bounds

By assumption, for any real embedding σ, we have that $\sigma(y_1 + y_2\alpha) < \sigma(z)$. Note that $\bar{\sigma} : M \longrightarrow \tilde{\mathbb{Q}}$ sending $y_1 + y_2\alpha$ to $\sigma(y_1 - y_2\alpha)$ is also a real embedding and therefore $|\sigma(y_1 - y_2\alpha)| \leq |\sigma(z)|$. Hence we have that $|\sigma(2\alpha y_2)| = |\sigma(x) - \bar{\sigma}(x)| < 2|\sigma(z)|$. At the same time, if $\tau : M \longrightarrow \tilde{\mathbb{Q}}$ is not a real embedding, then $\tau(y_1 + y_2\alpha)$ and $\tau(y_1 - y_2\alpha)$ are complex conjugates and have the same absolute value. Thus $|2\tau(\alpha y_2)| = |\tau(x) - \bar{\tau}(x)| \leq 2|\tau(x)|$, where $\bar{\tau}(x)$ is the complex conjugate of $\tau(x)$. Thus, assuming ϕ ranges over all embeddings, σ ranges of all real embeddings and τ ranges over all non-real embeddings of G into $\tilde{\mathbb{Q}}$,

$$|\mathbf{N}_{M/\mathbb{Q}}(\alpha y_2)| = \left|\prod_{\phi}\phi(\alpha y_2)\right| = \prod_{\sigma}|\sigma(\alpha y_2)|\prod_{\tau}|\tau(\alpha y_2)|$$

$$< \prod_{\sigma}|\sigma(z)|\prod_{\tau}|\tau(x)| \leq \prod_{\phi}|\phi(zx)| = |\mathbf{N}_{M/\mathbb{Q}}(zx)|$$

A Commercial

Hilbert's Tenth Problem:
Diophantine Classes and Extensions to Global Fields
Series: New Mathematical Monographs (No. 7)
Alexandra Shlapentokh
East Carolina University