Definability in fields
Lecture 2:
Defining valuations

Thomas Scanlon

University of California, Berkeley

6 February 2007
Model Theory and Computable Model Theory
Gainesville, Florida

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Theorem (J. Robinson)

$\mathrm{Th}(\mathbb{Q})$ *is undecidable.*

Defining $\mathbb{Z}$ in $\mathbb{Q}$

Theorem (J. Robinson)

Th($\mathbb{Q}$) *is undecidable. In fact,* $\mathbb{Z} \subseteq \mathbb{Q}$ *is definable in* $(\mathbb{Q}, +, \times, 0, 1)$.

Explicit definition of $\mathbb{Z}$ in $\mathbb{Q}$

Let

$$\phi(u,v,w) := (\exists x,y,z) 2 + uvw^2 + vz^2 = x^2 + uy^2$$

Explicit definition of $\mathbb{Z}$ in $\mathbb{Q}$

Let

$$\phi(u, v, w) := (\exists x, y, z) 2 + uvw^2 + vz^2 = x^2 + uy^2$$

Then $\mathbb{Z}$ is defined by the formula

$$(\forall a, b)[\phi(a, b, 0) \& (\forall n)(\phi(a, b, n) \to \phi(a, b, n+1))] \to \phi(a, b, W)$$

Explicit definition of $\mathbb{Z}$ in $\mathbb{Q}$

Let

$$\phi(u,v,w) := (\exists x,y,z) 2 + uvw^2 + vz^2 = x^2 + uy^2$$

Then $\mathbb{Z}$ is defined by the formula

$$(\forall a,b)[\phi(a,b,0) \& (\forall n)(\phi(a,b,n) \rightarrow \phi(a,b,n+1))] \rightarrow \phi(a,b,W)$$

That is, $W \in \mathbb{Z}$ if and only if W belongs to every inductive set of the form $\phi(a,b,\mathbb{Q})$.

Explicit definition of $\mathbb{Z}$ in $\mathbb{Q}$

Let

$$\phi(u,v,w) := (\exists x,y,z) 2 + uvw^2 + vz^2 = x^2 + uy^2$$

Then $\mathbb{Z}$ is defined by the formula

$$(\forall a,b)[\phi(a,b,0)\&(\forall n)(\phi(a,b,n) \rightarrow \phi(a,b,n+1))] \rightarrow \phi(a,b,W)$$

That is, $W \in \mathbb{Z}$ if and only if W belongs to every inductive set of the form $\phi(a,b,\mathbb{Q})$.
As $\mathbb{Q} \models \phi(a,b,w) \leftrightarrow \phi(a,b,-w)$, the left-to-right implication is clear.

Converse verification

The proof presented in Definability and decision problems in arithmetic, *JSL* **14**, (1949), 98–114 proceeds through a number of clever computations based on some standard theorems in number theory on the representability of rational numbers by quadratic forms.

Converse verification

The proof presented in Definability and decision problems in arithmetic, *JSL* **14**, (1949), 98–114 proceeds through a number of clever computations based on some standard theorems in number theory on the representability of rational numbers by quadratic forms.

For instance, one finds

Lemma

If $p \equiv 3 \pmod 4$ is a prime number and a and b are relatively prime integers, then there are rational numbers x, y and z with $2 + p\frac{a^2}{b^2} + pz^2 = x^2 + y^2$ if and only if b is odd and prime to p.

Hasse-Minkowski Theorem

Theorem

Let $a_1, \ldots, a_n, r \in \mathbb{Q}$. Then there is a rational solution to the equation $\sum a_i X_i^2 = r$ if and only if there is a real solution and for each prime p there is a p-adic solution.

Hasse-Minkowski Theorem

Theorem

Let $a_1, \ldots, a_n, r \in \mathbb{Q}$. Then there is a rational solution to the equation $\sum a_i X_i^2 = r$ if and only if there is a real solution and for each prime p there is a p-adic solution.

As $\mathrm{Th}(\mathbb{R})$ and $\mathrm{Th}(\mathbb{Q}_p)$ are decidable, one can check solvability of these equations locally. In fact, there is a very simple procedure to reduce the problem to checking solvability in $\mathbb{R}$ and finitely many p-adic fields (with the finite set of p depending on the coëfficients.

Why should we open the Hasse-Minkowski black box?

It follows from Robinson's theorem that every arithmetic subset of $\mathbb{Q}$ is definable in $(\mathbb{Q}, +, \times)$.

Why should we open the Hasse-Minkowski black box?

It follows from Robinson's theorem that every arithmetic subset of $\mathbb{Q}$ is definable in $(\mathbb{Q}, +, \times)$. In particular, for any prime p, the local ring $\mathbb{Z}_{(p)} := \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$ is definable, and even uniformly so.

Why should we open the Hasse-Minkowski black box?

It follows from Robinson's theorem that every arithmetic subset of $\mathbb{Q}$ is definable in $(\mathbb{Q}, +, \times)$. In particular, for any prime p, the local ring $\mathbb{Z}_{(p)} := \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$ is definable, and even uniformly so. We can recover $\mathbb{Z}$ as $\mathbb{Z} = \bigcap \mathbb{Z}_{(p)}$.

Why should we open the Hasse-Minkowski black box?

It follows from Robinson's theorem that every arithmetic subset of $\mathbb{Q}$ is definable in $(\mathbb{Q}, +, \times)$. In particular, for any prime p, the local ring $\mathbb{Z}_{(p)} := \{\frac{a}{b} \mid a, b \in \mathbb{Z}, p \nmid b\}$ is definable, and even uniformly so. We can recover $\mathbb{Z}$ as $\mathbb{Z} = \bigcap \mathbb{Z}_{(p)}$.

By using the Hasse local-global principle directly, one can uniformly define these valuation rings without first proving the definability of $\mathbb{Z}$.

A reminder about valuations

Recall that a valuation v on a field K is a function $v : K \longrightarrow \Gamma \cup \{\infty\}$ from K to an ordered abelian group (extended by "∞") for which

- $v(x) = \infty \leftrightarrow x = 0$
- $v(xy) = v(x) + v(y)$ and
- $v(x + y) \geq \min\{v(x), v(y)\}$

A reminder about valuation rings

If (K, v) is a valued field, then the ring $\mathscr{O}_{K,v} := \{x \in K \mid v(x) \geq 0\}$ is called the valuation ring of v.

A reminder about valuation rings

If (K, v) is a valued field, then the ring $\mathscr{O}_{K,v} := \{x \in K \mid v(x) \geq 0\}$ is called the valuation ring of v.

A valuation ring without qualification is simply a commutative integral domain R having a unique maximal ideal $\mathfrak{m}$ whose field of fractions may be expressed as $R \cup (\mathfrak{m} \smallsetminus \{0\})^{-1}$.

A reminder about valuation rings

If (K, v) is a valued field, then the ring $\mathcal{O}_{K,v} := \{x \in K \mid v(x) \geq 0\}$ is called the valuation ring of v.

A valuation ring without qualification is simply a commutative integral domain R having a unique maximal ideal $\mathfrak{m}$ whose field of fractions may be expressed as $R \cup (\mathfrak{m} \smallsetminus \{0\})^{-1}$.

If R is a valuation ring with field of fractions K, then there is a valuation v on K defined by $v(x) \geq v(y) \leftrightarrow \frac{x}{y} \in R$ for which $R = \mathcal{O}_{K,v}$.

A reminder about valuation rings

If (K, v) is a valued field, then the ring $\mathscr{O}_{K,v} := \{x \in K \mid v(x) \geq 0\}$ is called the valuation ring of v.

A valuation ring without qualification is simply a commutative integral domain R having a unique maximal ideal $\mathfrak{m}$ whose field of fractions may be expressed as $R \cup (\mathfrak{m} \smallsetminus \{0\})^{-1}$.

If R is a valuation ring with field of fractions K, then there is a valuation v on K defined by $v(x) \geq v(y) \leftrightarrow \frac{x}{y} \in R$ for which $R = \mathscr{O}_{K,v}$. Thus, to define a valuation is equivalent to defining its associated valuation ring.

Global fields

Recall that a global field is a field K which is either a number field, that is, a finite algebraic extension of the field of rational numbers, or is a function field of a curve over a finite field, that is, a finite extension of a field of the form $\mathbb{F}_p(t)$ for some prime p.

Rumely's definition of valuation rings

Theorem (Rumely)

There is a formula $\psi(x, y)$ in the language of rings for which for any global field K and any parameter $b \in K$, the set $\psi(K, b) := \{a \in K \mid K \models \psi(a, b)\}$ is a valuation ring. Moreover, for any valuation ring $R \subseteq K$, there is a parameter $r \in K$ for which $R = \psi(K, r)$.

Two consequences of Rumely's theorem

- The formula $V(x) := (\forall b)\psi(x,b)$ defines the ring of algebraic integers $\mathscr{O}_K$ in the field field K and the relative algebraic closure of $\mathbb{F}_p$ in a global field of characteristic $p > 0$.
- The sentence "$V(K)$ is a field" is true of all global fields of positive characteristic and is false of all number fields.

Two consequences of Rumely's theorem

- The formula $V(x) := (\forall b)\psi(x,b)$ defines the ring of algebraic integers $\mathscr{O}_K$ in the field field K and the relative algebraic closure of $\mathbb{F}_p$ in a global field of characteristic $p > 0$.
- The sentence "$V(K)$ is a field" is true of all global fields of positive characteristic and is false of all number fields.

Norm groups

Recall that if L/K is a Galois extension of fields, then there is a group homomorphism $N_{L/K} : L^\times \to K^\times$ defined by

$$N_{L/K}(x) := \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

Norm groups

Recall that if L/K is a Galois extension of fields, then there is a group homomorphism $N_{L/K} : L^\times \to K^\times$ defined by

$$N_{L/K}(x) := \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(x)$$

Given a presentation of L as $K[x]/(P)$ for some irreducible polynomial $P \in K[x]$, the norm group of the extension, $N_{L/K}(L^\times) \leq K^\times$, is definable.

Hasse norm theorem

Theorem (Hasse)

Let L/K be a Galois extension of global fields. Then $a \in K^{\times}$ is a norm ($a \in N_{L/K}(L^{\times})$) if and only if a is a norm for every completion $\widehat{L}$ of L.

Hasse norm theorem

Theorem (Hasse)

Let L/K be a Galois extension of global fields. Then $a \in K^\times$ is a norm ($a \in N_{L/K}(L^\times)$) if and only if a is a norm for every completion $\widehat{L}$ of L.

As a special case of Hasse's theorem, take $L = K(\sqrt{A})$. Then $N_{L/K}(x_0 + x_1\sqrt{A}) = x_0^2 - Ax_1^2$ and this instance of Hasse's theorem follows from Minkowski's theorem on quadratic forms.

Defining the valuations

To be honest, the Hasse norm theorem is only one of several big theorems in number theory required for Rumely's definition and the definition is achieved only in pieces.

- If v is a discrete valuation on K, $t \in K$, $v(t) = 1$, and $\ell > 1$ is a natural number, then $v(x) \geq 0 \Leftrightarrow v(tx^\ell + 1) \equiv 0 \pmod{\ell}$.
- Using the Hasse principle, Rumely produces a formula correctly defines the condition $v(x) \equiv 0 \pmod{\ell}$ subject to a unit condition at another valuation. To correctly define v, these other conditions need to be quantified out.

Defining the valuations

To be honest, the Hasse norm theorem is only one of several big theorems in number theory required for Rumely's definition and the definition is achieved only in pieces.

- If v is a discrete valuation on K, $t \in K$, $v(t) = 1$, and $\ell > 1$ is a natural number, then $v(x) \geq 0 \Leftrightarrow v(tx^\ell + 1) \equiv 0 \pmod{\ell}$.
- Using the Hasse principle, Rumely produces a formula correctly defines the condition $v(x) \equiv 0 \pmod{\ell}$ subject to a unit condition at another valuation. To correctly define v, these other conditions need to be quantified out.

Defining the valuations

To be honest, the Hasse norm theorem is only one of several big theorems in number theory required for Rumely's definition and the definition is achieved only in pieces.

- If v is a discrete valuation on K, $t \in K$, $v(t) = 1$, and $\ell > 1$ is a natural number, then $v(x) \geq 0 \Leftrightarrow v(tx^\ell + 1) \equiv 0 \pmod{\ell}$.
- Using the Hasse principle, Rumely produces a formula correctly defines the condition $v(x) \equiv 0 \pmod{\ell}$ subject to a unit condition at another valuation. To correctly define v, these other conditions need to be quantified out.

Defining $\mathbb{N}$ in number rings

Theorem (J. Robinson)

If $\mathcal{O}_K$ is the ring of integers in a number field, then $\mathbb{N}$ is a definable subset of $\mathcal{O}_K$.

Defining $\mathbb{N}$ in number rings

Theorem (J. Robinson)

If $\mathscr{O}_K$ is the ring of integers in a number field, then $\mathbb{N}$ is a definable subset of $\mathscr{O}_K$.

The proof makes use of a theorem on the coding of finite sets in $\mathscr{O}_K$ using divisibility.

Defining $\mathbb{N}$ in number rings

Theorem (J. Robinson)

If $\mathscr{O}_K$ is the ring of integers in a number field, then $\mathbb{N}$ is a definable subset of $\mathscr{O}_K$.

The proof makes use of a theorem on the coding of finite sets in $\mathscr{O}_K$ using divisibility. With a uniform definition of the places, one obtains a uniform coding of finite sets.

Coding finite sets

Theorem (Rumely)

Finite sets are uniformly definable in global fields. There is a formula $\vartheta(t, s)$ in the language of rings so that for every global field K and parameter $b \in K$ the set $\vartheta(K, b)$ is finite and for every finite set $B \subseteq K$ there is some code $b \in K$ with $B = \vartheta(K, b)$.

Uniform definition of $\mathbb{N}$

Corollary

The set of natural numbers is uniformly definable in the class of number fields.

Uniform definition of $\mathbb{N}$

Corollary

The set of natural numbers is uniformly definable in the class of number fields.

Proof.

$n \in K$ is a natural number if and only if there is a finite set $A \subseteq K$ for which

- $n \in A$
- $0 \in A$
- $(\forall a \in A)[a = 0 \vee a - 1 \in A]$

□

Uniform definition of $\mathbb{F}[x]$

Using similar tricks we find uniform definitions for:

- $\{a^n \mid n \in \mathbb{N}\}$ (taking a as a parameter)
- $R[a]$ (taking a as a parameter where $R = \mathbb{Z}$ in characteristic zero and R is the relative algebraic closure of $\mathbb{F}_p$ in characteristic $p > 0$)

Uniform definition of $\mathbb{F}[x]$

Using similar tricks we find uniform definitions for:

- $\{a^n \mid n \in \mathbb{N}\}$ (taking a as a parameter)
- $R[a]$ (taking a as a parameter where $R = \mathbb{Z}$ in characteristic zero and R is the relative algebraic closure of $\mathbb{F}_p$ in characteristic $p > 0$)

Uniform definition of $\mathbb{F}[x]$

Using similar tricks we find uniform definitions for:

- $\{a^n \mid n \in \mathbb{N}\}$ (taking a as a parameter)
- $R[a]$ (taking a as a parameter where $R = \mathbb{Z}$ in characteristic zero and R is the relative algebraic closure of $\mathbb{F}_p$ in characteristic $p > 0$)

Uniform definition of $\mathbb{F}[x]$

Using similar tricks we find uniform definitions for:

- $\{a^n \mid n \in \mathbb{N}\}$ (taking a as a parameter)
- $R[a]$ (taking a as a parameter where $R = \mathbb{Z}$ in characteristic zero and R is the relative algebraic closure of $\mathbb{F}_p$ in characteristic $p > 0$)

From a theorem of R. Robinson, it follows that $(\mathbb{N}, +, \times)$ is uniformly interpretable either as $\mathbb{N}$ itself or as the set of powers of a transcendental element.

Biïnterpretability with $\mathbb{Z}$

With coding of finite sets and $\mathbb{N}$ at our disposal, we can encode finite sequences uniformly. From this it follows that global fields understand their own natural recursive presentation.

Biïnterpretability with $\mathbb{Z}$

With coding of finite sets and $\mathbb{N}$ at our disposal, we can encode finite sequences uniformly. From this it follows that global fields understand their own natural recursive presentation.

Theorem (Rumely)

Global fields are uniformly biïnterpretable with $\mathbb{N}$.

Biïnterpretability with $\mathbb{Z}$

With coding of finite sets and $\mathbb{N}$ at our disposal, we can encode finite sequences uniformly. From this it follows that global fields understand their own natural recursive presentation.

Theorem (Rumely)

Global fields are uniformly biïnterpretable with $\mathbb{N}$.

Proof.

□

Biïnterpretability with $\mathbb{Z}$

With coding of finite sets and $\mathbb{N}$ at our disposal, we can encode finite sequences uniformly. From this it follows that global fields understand their own natural recursive presentation.

Theorem (Rumely)

Global fields are uniformly biïnterpretable with $\mathbb{N}$*.*

Proof.

For the sake of illustration, suppose that $K = \mathbb{Q}(\alpha)$ where the minimal polynomial of α over $\mathbb{Q}$ is $P(X)$ and has degree d. □

Biïnterpretability with $\mathbb{Z}$

With coding of finite sets and $\mathbb{N}$ at our disposal, we can encode finite sequences uniformly. From this it follows that global fields understand their own natural recursive presentation.

Theorem (Rumely)

Global fields are uniformly biïnterpretable with $\mathbb{N}$.

Proof.

For the sake of illustration, suppose that $K = \mathbb{Q}(\alpha)$ where the minimal polynomial of α over $\mathbb{Q}$ is $P(X)$ and has degree d. Then K is naturally presented as $\mathbb{Q}^d$ (itself presented as a certain subset S of $\mathbb{N}^{4d}$) with coördinatewise addition and multiplication expressed in terms of P. □

Biïnterpretability with $\mathbb{Z}$

With coding of finite sets and $\mathbb{N}$ at our disposal, we can encode finite sequences uniformly. From this it follows that global fields understand their own natural recursive presentation.

Theorem (Rumely)

Global fields are uniformly biïnterpretable with $\mathbb{N}$.

Proof.

For the sake of illustration, suppose that $K = \mathbb{Q}(\alpha)$ where the minimal polynomial of α over $\mathbb{Q}$ is $P(X)$ and has degree d.
Then K is naturally presented as $\mathbb{Q}^d$ (itself presented as a certain subset S of $\mathbb{N}^{4d}$) with coördinatewise addition and multiplication expressed in terms of P.
Using coding of finite sequences and α as a parameter, the identification of K with S becomes definable. □

Finitely generated fields

We will extend this analysis to finitely generated fields in two ways.

- K is a finitely generated field of characteristic zero, then its constant field, $k := \{a \in K \mid [\mathbb{Q}(a) : \mathbb{Q}] < \infty\}$, is a number field. We will lift what we know about k to K.
- K itself may be understood as a function field over k. We aim to define the valuations on K trivial on k in order to internally present K as a field of functions.

Finitely generated fields

We will extend this analysis to finitely generated fields in two ways.

- K is a finitely generated field of characteristic zero, then its constant field, $k := \{a \in K \mid [\mathbb{Q}(a) : \mathbb{Q}] < \infty\}$, is a number field. We will lift what we know about k to K.
- K itself may be understood as a function field over k. We aim to define the valuations on K trivial on k in order to internally present K as a field of functions.

Finitely generated fields

We will extend this analysis to finitely generated fields in two ways.

- K is a finitely generated field of characteristic zero, then its constant field, $k := \{a \in K \mid [\mathbb{Q}(a) : \mathbb{Q}] < \infty\}$, is a number field. We will lift what we know about k to K.
- K itself may be understood as a function field over k. We aim to define the valuations on K trivial on k in order to internally present K as a field of functions.