The Definability of Valuations in Global Fields

An Introduction to Rumely's *Undecidability and Definability for the Theory of Global Fields*

REID DALE
University of California, Berkeley
reiddale@math.berkeley.edu
December 11, 2014

Introduction

This document is meant to be serve as a self-contained introduction to the *definability* portion of Rumely's classic paper [6] on the definability and undecidability of the first-order theory of global fields. For the sake of brevity and the clarity of the argument we restrict ourselves to showing the definability of *nonarchimedean* valuations in the case of *number fields*. The way we go about doing this actually shows more: by showing that we can define all such valuations from a *uniform* family of first-order formulas we will be able to explicitly show that not only are all of the valuation rings of a given number field definable, but also that the ring of integers itself is definable. The key technical tools used in the paper come from local and global class field theory: density theorems for idele class groups, Hasse's local-to-global principle for norms, and the local and global norm residue symbols. The references we use for background number-theoretic facts are Neukirch's classic *Algebraic Number Theory* [5] and Lang's *Algebraic Number Theory* [3]. There is essentially no new content in this paper; I hope only that I've succeeded in producing a friendly introduction to some key themes in the intersection of model theory and algebraic number theory.

Before we begin, we set some notational conventions. I will use symbols such as v and w to refer to valuations (archimedean or nonarchimedean), Gothic letters $\mathfrak{p}, \mathfrak{P}$ to refer to primes in the spectrum of some ring of integers $\mathcal{O}_K$. $\mathcal{O}_v$ will be the valuation ring of v in K, with maximal ideal $\mathfrak{m}_v$ and residue field $\kappa(v) := \mathcal{O}_v/\mathfrak{m}_v$. Typically ℓ and p will be prime integers, and ζ_ℓ will denote a primitive ℓ^{th} root of unity. The idele group of a number field is denoted $\mathbb{I}_K$, and for a given cycle $\mathfrak{c}$ we let $Cl_\mathfrak{c} = J(\mathfrak{c})/K_\mathfrak{c}$ be the corresponding generalized class group. When I speak of a *tuple* $(x_1, \cdots, x_n)$ I will often just write it as $\overline{x}$.

Interpretations of Fields

We assume that the reader is familiar with the most basic concepts of model theory, namely: first-order languages and (unnested) atomic formulas, (parameter) definable sets and definable functions. If required, these definitions may all be found in Chapter 1 of [2]. Beyond these elementary notions, the most important model-theoretic concept for our purposes here is that of an *interpretation* of one structure inside another:

Definition 1. ([2] 4.3) An interpretation Γ of a ρ-structure $\mathcal{B}$ in a τ-structure $\mathcal{A}$ is given by the following data:

- A τ-formula $\partial_\Gamma(x_0, \cdots, x_{n-1})$
- For each unnested atomic ρ-formula $\phi(y_0, \cdot, y_{m-1})$ a τ-formula $\phi_\Gamma((x_{0i})_{0\leq i<n}, \cdots, (x_{(m-1),i})_{0\leq i<n})$ (a "translation" of ρ-formulas into τ-formulas)
- A surjection $\pi : \partial_\Gamma(\mathcal{A}) \to \mathcal{B}$ such that for all $\overline{a}, \overline{b} \in \partial_\Gamma(\mathcal{A})$
  1. $\pi(\overline{a}) = \pi(\overline{b})$ if and only if $\psi_\Gamma(\overline{a}, \overline{b})$ where ψ is the formula $y_0 = y_1$.
  2. For each unnested atomic formula $\phi \in \mathcal{L}_\rho$, $\pi^{-1}(\phi(\mathcal{B})) = \phi_\Gamma(\mathcal{A})$.

The main point of interpretations is that if a structure $\mathcal{A}$ interprets another structure $\mathcal{B}$, then the first-order theory of $\mathcal{B}$ is in some sense already "witnessed" by $\mathcal{A}$. This is made precise by a special case of the so-called *reduction theorem* (which is not too difficult to prove!)

Fact 1. *([2] 4.3.1) Let $\mathcal{B}$ be interpreted in $\mathcal{A}$ as above. Then for every $\phi \in \mathcal{L}_\rho$ there is a $\phi_\Gamma \in \mathcal{L}_\tau$ such that*

$$\mathcal{B} \models \phi(\pi(\overline{a})) \leftrightarrow \mathcal{A} \models \phi_\Gamma(\overline{a})$$

The key use of interpretations for our purposes is the fact that if K is perfect, *any* finite extension $L|K$ can be interpreted (with pararameters) over K.

Theorem 1. *Let K be a perfect field. Then any finite extension $L|K$ is interpretable over K over a finite set of parameters, namely, the parameters of the minimal polynomial of any element θ such that $L = K(\theta)|K$.*

Proof. Let $L|K$ be a finite extension of number fields of degree n. By the primitive element theorem, there is some $\theta \in L$ such that $L = K(\theta)$. Let $f(x) = minpoly(\theta) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Consider K in the natural way as an $\mathcal{L}_{rings} \cup \{a_i\}_{0\leq i<n}$-structure. We aim to construct an interpretation Γ the $\mathcal{L}_{rings}$ structure $(L, +, \times, 0, 1)$ in the $\mathcal{L}_{rings} \cup \{a_i\}_{0\leq i<n}$-structure $(K, +, \times, 0, 1, a_0, \cdots, a_{n-1})$. Since L is an n-dimensional K-vector space with basis $\{1, \theta, \cdots, \theta^{n-1}\}$, we set

- Let $\partial_\Gamma(x_0, \cdots, x_{n-1}) :=$ "$\bigwedge_{0\leq i<n} x_i = x_i$", which has $\partial_\Gamma(K^n) = K^n$.
- Set $\pi : K^n \to L$ by mapping $(c_0, \cdots, c_{n-1}) \mapsto \sum_{0\leq i<n} c_i\theta^i$ which is surjective since $\{1, \theta, \cdots, \theta^{n-1}\}$ is a basis of L over K.
- Set $\psi_\Gamma(\overline{x}, \overline{z}) :=$ "$\bigwedge_{0\leq i<n} x_i = z_i$", so that $\pi(\overline{c}) = \pi(\overline{d})$ if and only if $\psi_\Gamma(\overline{c}, \overline{d})$ since $\{1, \theta, \cdots, \theta^{n-1}\}$ is a basis of L over K.

The slightly harder part of this problem is to endow K^n with an $\mathcal{L}_{rings} \cup \{a_i\}_{0\leq i<n}$-definable field structure $(K, \oplus, \otimes, 0, 1)$ such that $(K^n, \oplus, \otimes, 0, 1) \cong (L, +, \times, 0, 1)$. If we manage to do this, it is routine to check that this gives an interpretation of L in K (over the given choice of parameters) since the only unnested atomic formulas in $\mathcal{L}_{rings}$ are of the form $y_0 + y_1 = y_2$, $y_0 \cdot y_1 = y_2$, and $y = c$ for some constant c.

We define the field structure as follows:

- We let $0 \in K^n$ be the tuple $(0, \cdots, 0)$. This is definable in K by the formula $zero(\overline{x}) =$ "$\bigwedge_{0 \le i < n} x_i = 0$".
- We let $1 \in K^n$ be the tuple $(1, 0, \cdots, 0)$. This is definable in K by the formula $one(\overline{x}) =$ "$x_0 = 1 \wedge \bigwedge_{1 \le i < n} x_i = 0$".
- The graph of addition $\oplus : K^n \to K^n$ is given by the formula

$$Add(\overline{x}, \overline{y}, \overline{z}) = \text{“} \bigwedge_{0 \le i < n} x_i + y_i = z_i \text{”}$$

so that $\oplus : K^n \to K^n$ is the obvious vector space addition.
- Multiplication is the hardest part. To define the graph of multiplication, first recall that the multiplication-by-θ map $T_\theta : L \to L$ is represented by the matrix

$$T_\theta = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -a_0 & -a_1 & -a_2 & \cdots & -a_{n-1} \end{pmatrix}$$

with respect to the basis $\{1, \theta, \cdots, \theta^{n-1}\}$ (this fact is from [5] in the proof of Prop I.2.6). But then

$$(\forall m \in \omega)\, (T_\theta)^m = T_{\theta^m} \; ; \; (\forall x \in K)\, xT_{\theta^m} = T_{x\theta^m} \; ; \; T_{\theta^0} = T_1 = I$$

For $\gamma = c_0 + c_1\theta + \cdots c_{n-1}\theta^{n-1}$ we may therefore represent the multiplication-by-γ map in the basis $\{1, \theta, \cdots, \theta^{d-1}\}$ as the sum $T_\gamma = \sum_{i=0}^{n-1} c_i T_{\theta^i}$. But this allows us to define multiplication on K^n by the following equation

$$(c_0, \cdots, c_{n-1}) \otimes (d_0, \cdots, d_{n-1}) := (\sum_{i=0}^{n-1} c_i T_{\theta^i})(d_0, \cdots, d_{n-1})^T$$

which is definable over the parameters $\{a_0, \cdots, a_{n-1}\}$ since matrix multiplication and addition are clearly definable functions in $\mathcal{L}_{rings}$. From here it is easy to write down an explicit formula $Mult(\overline{x}, \overline{y}, \overline{z})$ for the graph of $\otimes : K^n \to K^n$.

By construction of $\oplus$ and $\otimes$, π is in fact a field isomorphism and so $(L, +, \times, 0, 1)$ is interpretable in $(K, +, \times, 0, 1, a_0, \cdots, a_{n-1})$. □

It is worth remarking that something similar can be achieved even in the *imperfect* case, which must be dealt with if one wishes to consider the case of global function fields.

Definability of Nonarchimedean Valuations

Now that we've set up some model-theoretic background we can proceed to the real substance of Rumely's work. We begin by saying what we mean when we say that a valuation ν is arithmetically *definable* in K:

Definition 2. Given a discrete valuation $\nu : K^\times \to \mathbb{Z}$, an *arithmetic definition* of ν is a formula $\phi(x,y,\overline{z}) \in \mathcal{L}_{rings}$ such that for some choice of parameters $\overline{c} \in K^n$ and *all* $a,b \in K$

$$\nu(a) \geq \nu(b) \leftrightarrow \phi(a,b,\overline{c}).$$

In other words, ν is definable if the set $\{(a,b) \in K^2 \mid \nu(a) \geq \nu(b)\}$ is a parameter-definable subset of K. □

Right away we can reduce this problem to a slightly easier one:

Proposition 1. *A valuation ν is arithmetically definable in K if and only if the valuation ring $\mathcal{O}_\nu \subseteq K$ is parameter-definable.*

Proof. Suppose that ν is arithmetically definable, and let $\phi(x,y,\overline{c})$ be a formula defining it. Then $\mathcal{O}_\nu = \{x \in K \mid \nu(x) \geq 0\} = \phi(K,1,\overline{c})$ and so the formula $\phi(x,1,\overline{c})$ defines $\mathcal{O}_\nu$.

On the other hand, suppose $\mathcal{O}_\nu$ is parameter-definable by a formula $\psi(x,\overline{c})$. Consider the formula $\chi(x,y,\overline{c})$ given by

$$x = 0 \vee (y \neq 0 \wedge \forall z\,(zy = x \to \psi(z,\overline{c})))$$

which says that either $x = 0$ or that $\psi\,(z,\overline{c})$ holds for $z = \frac{x}{y}$. But then if $a,b \in K$ then $K \vDash \chi(a,b,\overline{c})$ just in case either $a = 0$ (in which case $\nu(a) \geq \nu(b)$) *or* $b \neq 0$ and $K \vDash \psi\left(\frac{a}{b},\overline{c}\right)$, in which case $\nu(\frac{a}{b}) \geq 0$ which is equivalent to saying that $\nu(a) \geq \nu(b)$. Hence

$$\{(a,b) \in K^2 \mid \nu(a) \geq \nu(b)\} \subseteq \chi(K^2,\overline{c}).$$

On the other hand, if $\nu(a) \geq \nu(b)$ then either $a = 0$ or $b \neq 0$ and $\frac{a}{b} \in \mathcal{O}_\nu$, so that

$$\chi(K^2,\overline{c}) \subseteq \{(a,b) \in K^2 \mid \nu(a) \geq \nu(b)\}$$

meaning that

$$K \vDash \chi(a,b,\overline{c}) \leftrightarrow \nu(a) \geq \nu(b)$$

and the result is proven. □

It will be useful to perform a further reduction:

Proposition 2. *Let $\ell \in \omega$ with $\ell \geq 2$ and ν a discrete valuation. Suppose that the set $\{x \in K \mid \nu(x) \equiv 0 \mod \ell\}$ is arithmetically definable. Then $\mathcal{O}_\nu$ is arithmetically definable.*

Proof. Let $\psi(x,\overline{c})$ be a definition of $\{x \in K \mid \nu(x) \equiv 0 \mod \ell\}$ and let π be a uniformizer for ν. We claim that the formula

$$\chi(x,\pi,\overline{c}) := \exists y \left(1 + \pi x^\ell = y \wedge \psi(y,\overline{c})\right)$$

is an arithmetic definition of $\mathcal{O}_\nu$. We break into two cases:

- If $\nu(x) \geq 0$ then $\nu(\pi x^\ell) = 1 + \ell\nu(x)$ and so the strong triangle inequality tells us that

$$\nu(1+\pi x^\ell) = \min\left(\nu(1), \nu(\pi x^\ell)\right) = \min(0, 1+\ell\nu(x)) = 0$$

But then $\nu(1+\pi x^\ell) \equiv 0 \mod \ell$ and so $K \vDash \chi(x, \pi, \bar{c})$.
- If $\nu(x) < 0$ then

$$\nu(1+\pi x^\ell) = \min(0, 1+\ell\nu(x)) = 1 + \ell\nu(x)$$

since $\ell > 1$ and $\nu(x) < 0$. But then $\nu(1+\pi x^\ell) \equiv 1 \mod \ell$ and so $K \nvDash \chi(x, \pi, \bar{c})$.

Together this means that $\chi(K, \pi, \bar{c}) = \mathcal{O}_\nu$, and so $\mathcal{O}_\nu$ is arithmetically definable. □

Given a discrete valuation ν on K we will construct an arithmetic definition of $\{x \in K \mid \nu(x) \equiv 0 \mod \ell\}$ for some prime $\ell \in \omega$. To do so, we *first* show that we can construct definitions for all valuations under mild field-theoretic conditions on K by reducing the problem to one of expressing a given $x \in K$ as the norm of some element y in some cyclic extension of the form $K(\sqrt[\ell]{a})$. We recall the following fact from Galois Theory:

Fact 2. *([4] VI.6.2). Let K be a field, $\ell \neq char(K)$ be prime, and suppose that K contains all ℓ^{th} roots of unity. Then*

- *If $L|K$ is a cyclic field extension with $[L:K] = \ell$ then there is some $\alpha \in K$ such that $L = K(\sqrt[\ell]{\alpha})$.*
- *If $a \in K$ and α is a root of $x^\ell - a$, $K(\alpha)$ is a cyclic extension of K of degree either 1 or ℓ.*

□

By the above fact, for well chosen ℓ all cyclic extensions of local fields $L_w|K_\nu$ with $[L_w : K_\nu] = \ell$ can be written as $L_w = K_\nu(\sqrt[\ell]{\alpha})$ for some $\alpha \in K_\nu$. The following lemma shows that under mild field-theoretic hypotheses the *ramification* behavior of ν in the extension $K(\sqrt[\ell]{\alpha})|K$ is tightly *controlled* by the (mod ℓ)-arithmetic of $\nu(\alpha)$.

Lemma 1. *Suppose that K is a number field that has all $2\ell^{th}$ roots of unity and suppose that ν is a discrete valuation on K such that $char(\kappa(\nu)) \neq \ell$. Let $L_w = K_\nu(\sqrt[\ell]{\alpha})$ for some $\alpha \in K_\nu^\times$. Recall that since K_ν is a complete valued field, w is uniquely specified.*

1. *If $\nu(\alpha) \not\equiv 0 \mod \ell$ then $L_w|K_\nu$ is totally ramified of degree ℓ and the image of the norm map is given by*

$$N_{L_w|K_\nu}(L_w^\times) = \left\langle \alpha, (K_\nu)^\times \right\rangle.$$

2. *If $\nu(\alpha) \equiv 0 \mod \ell$ but $\alpha \notin (K_\nu)^\ell$ then $L_w|K_\nu$ is unramified, $[L_w : K_\nu] = \ell$, and*

$$N_{L_w|K_\nu}(L_w^\times) = \{x \in K_\nu^\times \mid \nu(x) \equiv 0 \mod \ell\}$$

3. *If $\alpha \in (K_\nu)^\ell$ then $L_w = K_\nu$ and, trivially, $N_{L_w|K_\nu}(L_w^\times) = K_\nu^\times$.*

Proof. Recall the formula $[L_w : K_\nu] = e(w|\nu)f(w|\nu)$. Since ℓ is prime and $L_w = K_\nu(\sqrt[\ell]{\alpha})$ we have that either $[L_w : K_\nu] = \ell$, in which exactly one of $e(w|\nu)$ or $f(w|\nu)$ is ℓ (and the other is 1), *or* $[L_w : K_\nu] = 1$ and $e(w|\nu) = f(w|\nu) = 1$. These possibilities correspond to the above three cases:

1. If $\nu(\alpha) \not\equiv 0 \mod \ell$ then $\sqrt[\ell]{\alpha} \notin K$ for otherwise $\nu(\alpha) = \ell\nu(\sqrt[\ell]{\alpha})$, forcing $\nu(\alpha) \equiv 0 \mod \ell$. This simultaneously shows that $[L_w : K_{nu}] = \ell$ *and* $e(w|\nu) \neq 1$ and so, by the remarks above, $e(w|\nu) = \ell$. But then $L_w|K_\nu$ is totally ramified.
   Now note that if $a \in K_\nu^\times$ then $N_{L_w|K_\nu}(a) = a^\ell$ and that

   $$N_{L_w|K_\nu}(\sqrt[\ell]{\alpha}) = \prod_{0 \leq i \leq \ell-1} \zeta_\ell^i \sqrt[\ell]{\alpha} = \alpha$$

   since $L_w|K_\nu$ is Galois and the Galois conjugates of $\sqrt[\ell]{\alpha}$ are precisely of the form $\zeta_\ell^i \sqrt[\ell]{\alpha}$. This shows that the subgroup $\left\langle \alpha, K_\nu^\times)^\ell \right\rangle \subseteq N_{L_w|K_\nu}(L_w^\times)$. We wish to show the reverse inclusion. Indeed, note that since $\nu(\alpha)$ and ℓ are relatively prime, $\nu : \left\langle \alpha, K_\nu^\times)^\ell \right\rangle \to \mathbb{Z}$ is surjective, and so if $\beta \in N_{L_w|K_\nu}(L_w^\times)$ then there is $\gamma \in \left\langle \alpha, K_\nu^\times)^\ell \right\rangle$ such that $\nu(\beta) = -\nu(\gamma)$, so that

   $$\beta\gamma \in N_{L_w|K_\nu}(\mathcal{O}_w^\times) \subseteq \mathcal{O}_\nu^\times.$$

   If we can show that $\beta\gamma = u^\ell$ for some $u \in \mathcal{O}_\nu^\times \subseteq K_\nu^\times$ then we will have that

   $$\beta = \gamma^{-1}u^\ell \in \left\langle \alpha, (K_\nu^\times)^\ell \right\rangle,$$

   proving the claim. To do so it suffices to show that $N_{L_w|K_\nu}(\mathcal{O}_w^\times) = (\mathcal{O}_\nu^\times)^\ell$. We use the following fact:

   Fact 3. *([3] IX.3, Lemma 4) Let $L_w|K_\nu$ be a cyclic extension of local fields of characteristic 0 of degree n. Then $[K_\nu^\times : N_{L_w|K_\nu}(L_w^\times)] = [L_w : K_\nu]$ and $[\mathcal{O}_{K_\nu}^\times : N_{L_w|K_\nu}(\mathcal{O}_{L_w}^\times)] = e(w|\nu)$.* □

   By using Hensel's lemma it is not hard to show that $[\mathcal{O}_{K_\nu}^\times : (\mathcal{O}_{K_\nu}^\times)^\ell] = \ell = [\mathcal{O}_{K_\nu}^\times : N_{L_w|K_\nu}(\mathcal{O}_{L_w}^\times)]$ and so as $(\mathcal{O}_{K_\nu}^\times)^\ell \subseteq N_{L_w|K_\nu}(\mathcal{O}_{L_w}^\times)$, in fact we have

   $$(\mathcal{O}_{K_\nu}^\times)^\ell = N_{L_w|K_\nu}(\mathcal{O}_{L_w}^\times)$$

   as desired.
2. If $\nu(\alpha) \equiv 0 \mod \ell$ but $\alpha \notin (K_\nu)^\times$ then by writing $\alpha = \pi^\ell \tilde{\alpha}$ with π a uniformizer we have that $L_w = (K(\sqrt[\ell]{\tilde{\alpha}}))$ with $\nu(\tilde{\alpha}) = 0$, so without loss of generality we may assume that $\nu(\alpha) = 0$. But then

   $$\alpha \notin (K_\nu)^\ell \cap (\mathcal{O}_K^\times) = (\mathcal{O}_K^\times)^\ell$$

   and so $\kappa(w) = \kappa(\nu)(\sqrt[\ell]{\alpha + \mathfrak{m}_\nu}) \neq \kappa(\nu)$, implying that

   $$[\kappa(w) : \kappa(\nu)] = \ell = f(w|\nu)$$

   by primality of ℓ. But then by the fundamental identity this implies that $L_w|K_\nu$ is unramified and that $[L_w : K_\nu] = \ell$. Moreover,

   $$N_{L_w|K_\nu}(L_w^\times) = \{x \in K_\nu^\times \mid \nu(x) \equiv 0 \mod \ell\}$$

since $[\mathcal{O}_v^\times : N_{L_w|K_v}(\mathcal{O}_w^\times)] = e(w|v) = 1$ and since $[K_v^\times : N_{L_w|K_v}(L_w^\times)] = \ell = [K_v^\times : (K_v^\times)^\ell]$ and since $(K_v^\times)^\ell \subseteq N_{L_w|K_v}(L_w^\times)$.

3. If $\alpha \in (K_v^\times)^\ell$ then $L_w = K_v$ and the result is clear.

□

For a prime $\ell \in \omega$ and global field K such that $\mu_{2\ell} \subseteq K$, consider the set

$$\Lambda^{K;\ell} = \{\alpha \in K \mid \neg\exists x \left(x^\ell - \alpha = 0\right)\},$$

the set of $\alpha \in K$ such that the extension $K(\sqrt[\ell]{\alpha})|K$ is nontrivial and hence of degree exactly ℓ. Consider the function $N_\ell : \Lambda_{K;\ell} \times K^\ell \to K$ given by setting

$$N_\ell(\alpha, \beta_0, \cdots \beta_{\ell-1}) = N_{K(\sqrt[\ell]{\alpha})|K}\left(\beta_0 + \beta_1\sqrt[\ell]{\alpha} + \cdots + \beta_i\sqrt[\ell]{\alpha}^i + \cdots + \beta_{\ell-1}\sqrt[\ell]{\alpha}^{(\ell-1)}\right)$$

Claim 1. *$N_\ell : \Lambda_{K;\ell} \times K^\ell \to K$ is a polynomial map with integer coefficients.*

Proof. We know that for all $\alpha \in \Lambda_{K;\ell}$ that $\{1, \sqrt[\ell]{\alpha}, \sqrt[\ell]{\alpha}^2, \cdots, \sqrt[\ell]{\alpha}^{(\ell-1)}\}$ is a basis of $K(\sqrt[\ell]{\alpha})|K$. Under this basis, the multiplication-by-$\sqrt[\ell]{\alpha}$ map is given by the matrix

$$T_{\sqrt[\ell]{\alpha}} = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \cdots & \cdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ -\alpha & 0 & 0 & \cdots & 0 \end{pmatrix}$$

(As in [5] in the proof of Prop I.2.6). Moreover,

$$(\forall m \in \omega)\, (T_{\sqrt[\ell]{\alpha}})^m = T_{\sqrt[\ell]{\alpha}^m}\ ;\ (\forall x \in K)\, xT_{\sqrt[\ell]{\alpha}^m} = T_{x\sqrt[\ell]{\alpha}^m}\ ;\ T_{\sqrt[\ell]{\alpha}^0} = T_1 = I$$

and so

$$N_\ell(\alpha, \beta_0, \cdots, \beta_{\ell-1}) = N_{K(\sqrt[\ell]{\alpha})|K}\left(\beta_0 + \beta_1\sqrt[\ell]{\alpha} + \cdots + \beta_i\sqrt[\ell]{\alpha}^i + \cdots + \beta_{\ell-1}\sqrt[\ell]{\alpha}^{(\ell-1)}\right)$$

$$= \det(T_{\sum \beta_i \sqrt[\ell]{\alpha}}) = \det(\sum_{i=0}^{\ell-1} \beta_i (T_{\sqrt[\ell]{\alpha}})^i)$$

which is clearly an integer-coefficient polynomial in the variables $\alpha, \beta_0, \cdots, \beta_\ell$. □

The utility of this claim is that the function N_ℓ *uniformly* parametrizes the norms $N_{K(\sqrt[\ell]{\alpha})|K}$ in a *first-order* manner. Using this parametrization we can construct a formula ψ_ℓ that encodes ramification information for extensions of the form $K_v(\sqrt[\ell]{\alpha})|K_v$. For a fixed prime ℓ consider the first-order-formula $\psi_\ell(u; x, y)$ given by

$$\psi_\ell(u; x, y) := \text{“}u \neq 0 \wedge \exists\overline{z_1}\exists\overline{z_2}\exists\overline{z_3}\exists t\, (t = N_\ell(y, \overline{z_1}) \wedge xt = N_\ell(xy, \overline{z_2}) \wedge u = N_\ell(t, \overline{z_3}))\text{”}$$

which, in plain English, says that $u \in N_{K(\sqrt[\ell]{t})|K}(K(\sqrt[\ell]{t})^\times)$ for some t such that $t \in N_{K(\sqrt[\ell]{y})|K}(K(\sqrt[\ell]{y})^\times)$ and such that $xt \in N_{K(\sqrt[\ell]{xy})|K}(K(\sqrt[\ell]{xy})^\times)$.

Lemma 2. *Let ν be a nontrivial discrete valuation and suppose that $\ell \neq char(\kappa(\nu))$ and that K contains $\mu_{2\ell}$. Suppose further that $b \in \mathcal{O}_\nu^\times \setminus (\mathcal{O}_\nu^\times)^\ell$ and $\nu(a) = 1$. If $K \vDash \psi_\ell(u; a, b)$, then $\nu(u) \equiv 0 \mod \ell$.*

Proof. Suppose $K \vDash \psi_\ell(u; a, b)$. By Lemma 1 above we immediately have that $K_\nu(\sqrt[\ell]{b})|K_\nu$ is unramified of degree ℓ and that $K_\nu(\sqrt[\ell]{ab})|K_\nu$ is totally ramified of degree ℓ and by construction it is clear that the same claims hold for the extensions $K(\sqrt[\ell]{b})|K$ and $K(\sqrt[\ell]{ab})|K$ respectively. The equations occuring in $\psi_\ell(u; a, b)$ occuring of the form $t = N_\ell(b, \overline{z_1})$ and $at = N_\ell(ab, \overline{z_2})$ imply that

$$t = \tau_1 a^{m_1 \ell} \wedge at = \tau_2 (ab)^{m_2}$$

for some $\tau_i \in \mathcal{O}_\nu^\times \cap K^\times$, $m_i \in \mathbb{Z}$, and $t \in K$ by Lemma 1 since $N_{K_\nu(\sqrt[\ell]{a})|K_\nu}(K_\nu(\sqrt[\ell]{a}^\times) = \{x \in K_\nu^\times \mid \nu(x) \equiv 0 \mod \ell\}$, since $N_{K_\nu(\sqrt[\ell]{ab})|K_\nu}(K_\nu(\sqrt[\ell]{a}^\times) = \langle ab, (K_\nu)^\times \rangle$, and since $\nu(ab) = 1 = \nu(a)$ means that a and ab are uniformizers for K_ν. We then have

$$\tau_1 a^{m_1 \ell + 1} = at = \tau_2^\ell (ab)^{m_2}$$

so that, dividing by a, we can write $t = (\tau_2 a^{m_1} b^{m_1})^\ell b$. But then $\frac{\sqrt[\ell]{t}}{\sqrt[\ell]{b}} = \tau_2 a^{m_1} b^{m_1} \in K$ so that $K_\nu(\sqrt[\ell]{t}) = K_\nu(\sqrt[\ell]{b})$ is unramified of degree ℓ. This means that we may write $u = \tau t^{m\ell}$ for some $\tau \in \mathcal{O}_\nu^\times \cap K$ and $m \in \mathbb{Z}$ so that $\nu(u) = m\ell$ so $\nu(u) \equiv 0 \mod \ell$. ☐

As such, picking *any* $a, b \in K$ satisfying the above hypotheses for a fixed discrete valuation ν yields a subset $\psi_\ell(K, a, b) \subseteq \{x \in K \mid \nu(x) \equiv 0 \mod \ell\}$, but *a priori* the reverse inclusion may not hold. Our next goal is to use facts from class field theory to show that we can choose $a, b \in K$ so that the formula $\psi_\ell(u; a, b)$ (in *one* free variable) *almost* satisfies the desired property.

Up until now we haven't needed to use the correspondence between nontrivial discrete valuations ν on K and nonzero primes $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$, but to make the connection to class field theory explicit we will henceforth identify a discrete valuation ν with the unique prime $\mathfrak{p}_\nu \in \mathrm{Spec}(\mathcal{O}_K)$ such that $(\mathcal{O}_K)_{\mathfrak{p}_\nu} = \mathcal{O}_\nu$.

Lemma 3. *Let ν be a nontrivial discrete valuation, that $\ell \neq char(\kappa(\nu))$, that K contains $\mu_{2\ell}$, and that $\nu(\ell) = 0$. Let $\mathfrak{p} = \mathfrak{p}_\nu$ be the prime associated to ν. Then there exists $a, b \in K$ and $\mathfrak{q} \neq \mathfrak{p} \in Spec(\mathcal{O}_K)$ with associated valuation $\nu_\mathfrak{q}$ such that*

$$\psi_\ell(K; a, b) = \{x \in K \mid \nu(x) \equiv 0 \mod \ell \wedge \nu_\mathfrak{q}(x) \equiv 0 \mod \ell\}$$

Proof. We first *construct* candidates for $a, b \in K$ and $\mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_K)$ and then show that they yield the desired conclusion.

Construction. We first construct a and along the way we will also construct $\mathfrak{q}$. Consider the set $R_{\ell,K} = \{\mathfrak{r} \in \mathrm{Spec}(\mathcal{O}_K) \setminus \{0\} \mid \mathfrak{r}|\ell\}$ the set of divisors of ℓ. I first claim that there is an $m \in \mathbb{Z}$ such that if $c \equiv 1 \mod \mathfrak{r}^m$ then $c \in (K_{\nu_\mathfrak{r}}^\times)^\ell$. Let $\mathfrak{r} \in R_{\ell,K}$, let $m = 2\nu_\mathfrak{r}(\ell)$, and consider the polynomial

$f(x) = x^\ell - c$ which has derivative ℓ. If $c \equiv 1 \mod \mathfrak{r}^m$ then

$$f(1) = 1 - a \equiv 0 \mod \mathfrak{r}^m \equiv 0 \mod \mathfrak{r}^{2\nu_\mathfrak{r}(\ell)} \equiv 0 \mod (\ell)^2\mathfrak{r} \equiv 0 \mod (f'(1))^2\mathfrak{r}$$

so by Hensel's lemma we have that there is *some* $d \in K$ such that $f(d) = d^\ell - c = 0$, so that $c \in (K_{\nu_\mathfrak{r}}^\times)^\ell$. Since $R_{\ell,K} = \{\mathfrak{r}_i\}_{i\in I}$ is finite, if for all $i \in I$ we take $m_i = 2\nu_{\mathfrak{r}_i}(\ell) \in \mathbb{Z}$ then taking $m := \sup(\{m_i\})$ gives us the desired number. Given this m, define a cycle

$$\mathfrak{c} := \prod_{\nu|\infty} \nu \times \prod_{\mathfrak{r}\in R_{\ell,K}} \nu_\mathfrak{r}^m$$

and consider the *generalized class group* associated to the cycle $\mathfrak{c}$, $Cl_\mathfrak{c} = J(\mathfrak{c})/K_\mathfrak{c}$. Consider the class of $[\mathfrak{p}_\nu] \in C_\mathfrak{c}$. We use the following analogue of Dirichlet's Theorem on Arithmetic Progressions for generalized class groups:

Fact 4. *([5] Theorem VII.13.2) Let H be a subgroup of $J(\mathfrak{c})$ such that $P_\mathfrak{c} \subseteq H$. Then for every class $[\mathfrak{p}] \in J(\mathfrak{c})/H$, the density of primes in $[\mathfrak{p}]$ is $\dfrac{1}{[J(\mathfrak{c}) : H]} > 0$.* □

Given this fact, we may choose a prime $\mathfrak{q} \neq \mathfrak{p} \in [\mathfrak{p}]^{-1}$. By construction, $\mathfrak{p}\mathfrak{q} = (a)$ for some $a \in K$ satisfying $a \equiv 1 \mod \mathfrak{r}^m$ for all $\mathfrak{r} \in R_{\ell,K}$ and such that $a > 0$ in all archimedean valuations.

We now aim to construct b using class field theory. Keep in mind that our choice of b should make it apparent that $\psi(K, a, b) \subseteq \mathcal{O}_\mathfrak{p} \cap \mathcal{O}_\mathfrak{q}$, for one direction of the proof. Our choice of $\mathfrak{p}$ and $\mathfrak{q}$ yields that they are the *only* ramified primes in the extension $K(\sqrt[\ell]{a})|K$. Since ℓ is prime, this means that $\mathfrak{p}\mathcal{O}_{K(\sqrt[\ell]{a})} = \mathfrak{P}^\ell$ and $\mathfrak{q}\mathcal{O}_{K(\sqrt[\ell]{a})} = \mathfrak{Q}^\ell$ for primes $\mathfrak{P}, \mathfrak{Q} \in \mathrm{Spec}(\mathcal{O}_{K(\sqrt[\ell]{a})})$.

Then by the fundamental identity and the theorems on local norm indices we have that

$$[\mathcal{O}_{K_\mathfrak{p}} : N_{K(\sqrt[\ell]{a})_\mathfrak{P}|K_\mathfrak{p}}(\mathcal{O}^\times_{K(\sqrt[\ell]{a})_\mathfrak{P}})] = \ell = [\mathcal{O}_{K_\mathfrak{q}} : N_{K(\sqrt[\ell]{a})_\mathfrak{Q}|K_\mathfrak{q}}(\mathcal{O}^\times_{(K(\sqrt[\ell]{a}))_\mathfrak{Q}})] > 1.$$

and so, in particular, there is a unit $\tau_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}} \setminus N_{K(\sqrt[\ell]{a})_\mathfrak{P}|K_\mathfrak{p}}(\mathcal{O}^\times_{K(\sqrt[\ell]{a})_\mathfrak{P}})$. At this stage we invoke pertinent facts from both local and global class field theory

Fact 5. *([5])*

1. *(Local Norm Residue Symbol [V.1.3]) Let $L_w|K_\nu$ be a finite Galois extension of local fields. Then there is a canonical surjective morphism*

$$(-, L_w|K_\nu) : K_\nu^\times \to Gal(L_w|K_\nu)^{ab}$$

   with $\ker((-, L_w|K_\nu)) = N_{L_w|K_\nu}(L_w^\times)$.
2. *(Global Norm Residue Symbol [VI.5.5]) Let $L|K$ be a finite Galois extension of number fields. Then there is a canonical surjective morphism*

$$(-, L|K) : \mathbb{I}_K/K^\times \to Gal(L|K)^{ab}$$

   with kernel $\ker((-, L|K)) = N_{L|K}(\mathbb{I}_L/L^\times)$.

3. *(Local-Global Compatibility [VI.5.6]) If $L|K$ is a finite abelian extension of number fields and ν is a valuation (archimedean or nonarchimedean) then the following diagram commutes*

$$\begin{array}{ccc} K_\nu^\times & \xrightarrow{(-,L_w|K_\nu)} & Gal(L_w|K_\nu) \\ \Big\downarrow{\scriptstyle \theta} & & \Big\downarrow{\scriptstyle \iota} \\ \mathbb{I}_K/K^\times & \xrightarrow[(-,L|K)]{} & Gal(L/K) \end{array}$$

where $\theta : K_\nu^\times$ maps $\theta_\nu(a) = [(\cdots, 1, \cdots, 1, a, 1, \cdots, 1, \cdots)] \in \mathbb{I}_K/K^\times$ where a is the ν^{th} coordinate of the idele $(\cdots, 1, \cdots, 1, a, 1, \cdots, 1, \cdots)$ and ι is the embedding guaranteed to exist by decomposition theory.

4. *(Product Formula [VI.5.7]) If $L|K$ is a finite abelian extension of number fields and $\alpha = (\alpha_\nu)_\nu \in \mathbb{I}_K$ then*

$$(\alpha, L|K) = \prod_{\nu \in \mathcal{M}_K} (\alpha_\nu, L_w|K_\nu)$$

where L_w is the unique extension of local fields of K_ν with $w|\nu$. Moreover, for a principal idele $\alpha = (a)_\nu$ we have that

$$\prod_{\nu \in \mathcal{M}_K} (a, L_w|K_\nu) = 1$$

□

Recall our choice of $\tau_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}} \setminus N_{K(\sqrt[\ell]{a})_\mathfrak{P}|K_\mathfrak{p}}(\mathcal{O}^\times_{K(\sqrt[\ell]{a})_\mathfrak{P}})$. The by the theorem above on local norm residues,

$$(\tau_\mathfrak{p}, K(\sqrt[\ell]{a}))_\mathfrak{P}|K_\mathfrak{p}) = \sigma \neq \mathrm{id}_L \in Gal(L/K)$$

since $\tau_\mathfrak{p}$ was chose to *not* be a norm. Since $K(\sqrt[\ell]{a})_\mathfrak{P}|K_\mathfrak{p}$ is *cyclic of prime order*, the local norm residue map $(-, K(\sqrt[\ell]{a})_\mathfrak{Q}|K_\mathfrak{q}) : \mathcal{O}^\times_{K_\mathfrak{q}} \to Gal(L_w|K_\nu) = Gal(L/K)$ is surjective! As such, there is a non-norm $\tau_\mathfrak{q} \in \mathcal{O}^\times_{K_\mathfrak{q}}$ with $(\tau_\mathfrak{q}, K(\sqrt[\ell]{a})_\mathfrak{Q}|K_\mathfrak{q}) = \sigma^{-1}$.

We now produce a first approximation for our desired b. Let $\tilde{b} \in K$ be such that $\tilde{b} \equiv \tau_\mathfrak{p} \mod \mathfrak{p}$, $\tilde{b} \equiv \tau_\mathfrak{q} \mod \mathfrak{q}$, $\tilde{b} \equiv 1 \mod \mathfrak{r}^m$ for all $\mathfrak{r} \in R_{\ell,K}$, and such that $\tilde{b}$ is positive in all real valuations. Since this is a *finite* list of valuations, the

Fact 6. *(Approximation Theorem, [5] II.3.4) Let $|-|_1, \cdots, |-|_n$ be pairwise inequivalent valuations of the field K and let $z_1, \cdots, z_n \in K$ be given. Then for every $\epsilon > 0$ there is a $y \in K$ such that*

$$(\forall 1 \leq i \leq n) \ \ |y - z_i|_i < \epsilon \quad \square$$

guarantees the existence of such a $\tilde{b}$ by considering, for every prime $\mathfrak{s}$ appearing above, the induced absolute value $|-|_\mathfrak{s}$ given by $|x|_\mathfrak{s} = |N(\mathfrak{s})|^{-\nu_\mathfrak{s}(x)}$ and by letting each archimedean prime being associated to its natural absolute value.

Note that in the generalized class group $J(\mathfrak{cpq})/P_\mathfrak{cpq}$ the class every element in the class $[(\tilde{b})]$ is principal (since the equivalence relation defining this generalized class group is a *refinement* of the one defining the class group Cl_K since we have the natural surjection $J(\mathfrak{cpq})/P_\mathfrak{cpq} \to Cl_K$). Then by the density theorem for primes in living in a given class in the generalized class group, there exists a *principal* prime $\mathfrak{t} = (t) \in [(\tilde{b})]$ (which is emphatically *not* $\mathfrak{p}$ or $\mathfrak{q}$). Then $[\mathfrak{t}][(\tilde{b})^{-1}] \in J(\mathfrak{c}\mathfrak{p}\mathfrak{q})/P_{\mathfrak{c}\mathfrak{p}\mathfrak{q}}$ is trivial and so the principal ideal $\mathfrak{t}(\tilde{b}^{-1})$ has a generator $g \equiv 1 \mod \mathfrak{c}\mathfrak{p}\mathfrak{q}$. Then setting $b := g\tilde{b}$ yields a generator of $\mathfrak{t}$ such that

- $b \equiv 1 \mod \mathfrak{r}^m$ for all $\mathfrak{r} \in R_{\ell,K}$
- $b \equiv \tau_{\mathfrak{p}} \mod \mathfrak{p}$, $b \equiv \tau_{\mathfrak{q}} \mod \mathfrak{q}$
- b is positive for all real valuations on K

which all follow since $g \equiv 1 \mod \mathfrak{c}\mathfrak{p}\mathfrak{q}$ and by choice of $\tilde{b}$.

Verification. We now sketch how to verify that, in fact,

$$\psi_\ell(K; a, b) = \{x \in K \mid \nu(x) \equiv 0 \mod \ell \wedge \nu_{\mathfrak{q}}(x) \equiv 0 \mod \ell\}$$

To show that $\psi_\ell(K; a, b) \subseteq \{x \in K \mid \nu(x) \equiv 0 \mod \ell \wedge \nu_{\mathfrak{q}}(x) \equiv 0 \mod \ell\}$ it turns out that what we really need to do is use the fact that

Fact 7. *([5] VI.4.5) Let $L|K$ be a cyclic extension of algebraic number fields. An $x \in K^\times$ is of the form $x = N_{L|K}(y)$ for some $y \in L^\times$ if and only if $x = N_{L_w|K_v}(y_w)$ for some $y_w \in L_w^\times$ for all completions L_w of L.*

to show that $a \in N_{K(\sqrt[\ell]{b})|K}(K(\sqrt[\ell]{b})^\times)$. It turns out that to apply this fact, the main thing we have to show is that $a \in (K_{\mathfrak{t}}^\times)^\ell$ which can be done using Artin Reciprocity. Indeed, since b is a norm for all $K_{\mathfrak{r}}$ such that $\mathfrak{r} \in R_{\ell,K}$ (by choice of cycle $\mathfrak{c}$ and integer m as well as the lemma characterizing norm groups in the ramified case) we have that $(b, (K(\sqrt[\ell]{a}))_{\mathfrak{R}}|K_{\mathfrak{r}}) = \mathrm{id}_K$. For real valuations ν_{real} we have that $(b, (K(\sqrt[\ell]{a}))_{w_{real}}|K_{\nu_{real}}) = 1$ since $|b|_{\nu_{real}} > 0$. For all $\mathfrak{s} \notin \mathcal{M}_{K,\infty} \cup R_{\ell,K} \cup \{\mathfrak{p}, \mathfrak{q}, \mathfrak{t}\}$ we have that $(K(\sqrt[\ell]{a}))_{\mathfrak{S}}$ is unramified and because $\nu_{\mathfrak{s}}(b) = 0$ as b is a uniformizer for $\nu_{\mathfrak{t}}$. Then the product formula for norm residues tells us that

$$\mathrm{id}_K = (b, (K(\sqrt[\ell]{a}))_{\mathfrak{P}}|K_{\mathfrak{p}})(b, (K(\sqrt[\ell]{a}))_{\mathfrak{Q}}|K_{\mathfrak{q}})((b, (K(\sqrt[\ell]{a}))_{\mathfrak{T}}|K_{\mathfrak{t}})) = ((b, (K(\sqrt[\ell]{a}))_{\mathfrak{T}}|K_{\mathfrak{t}}))$$

since our choice of b forces $(b, (K(\sqrt[\ell]{a}))_{\mathfrak{P}}|K_{\mathfrak{p}}) = (\tau_{\mathfrak{p}}, (K(\sqrt[\ell]{a}))_{\mathfrak{P}}|K_{\mathfrak{p}}) = \sigma$ and similarly that $(b, (K(\sqrt[\ell]{a}))_{\mathfrak{Q}}|K_{\mathfrak{q}}) = \sigma^{-1}$. Then as

$$\ker((-, (K(\sqrt[\ell]{a}))_{\mathfrak{T}}|K_{\mathfrak{t}})) = N_{(K(\sqrt[\ell]{a}))_{\mathfrak{T}}|K_{\mathfrak{t}}}((K(\sqrt[\ell]{a}))_{\mathfrak{T}}^\times)$$

b is a norm of $(K(\sqrt[\ell]{a}))_{\mathfrak{T}}|K_{\mathfrak{t}}$. But by choice of $\mathfrak{t} \neq \mathfrak{p}, \mathfrak{q}$ we have that this extension is unramified; but as b is a uniformizer for $\nu_{\mathfrak{t}}$ we must have that $(K(\sqrt[\ell]{a}))_{\mathfrak{T}} = K_{\mathfrak{t}}$ and so $a \in (K_{\mathfrak{t}}^\times)^\ell$. Now, using this Hasse's Norm theorem and our construction of a and b it is not too hard to show that $N_{K(\sqrt[\ell]{b})|K}(K(\sqrt[\ell]{b})^\times)$ and the proof of Lemma 2 it is not too hard to show that

$$\psi_\ell(K; a, b) \subseteq \{x \in K \mid \nu(x) \equiv 0 \mod \ell \wedge \nu_{\mathfrak{q}}(x) \equiv 0 \mod \ell\}$$

Conversely, the verification that *if* $\nu(x) \equiv 0 \mod \ell$ and $\nu_{\mathfrak{q}}(x) \equiv 0 \mod \ell$ *then* $K \vDash \psi_\ell(x; a, b)$ is a fairly straightforward of the local-to-global principle for norms as well as the product formula for the norm residue symbol evaluated at principal ideles. The precise details may be found in ([6], Lemma 3). □

Now that we've shown this hard technical lemma, the definability of $\mathcal{O}_\nu$ is almost immediate.

Theorem 2. *Let K be a number field. Then all nontrivial discrete valuations ν are arithmetically definable.*

Proof. We first prove the result under the hypotheses above. Let ℓ be a prime number. Suppose that ν is a nonarchimedean valuation on K such that $\nu(\ell) = 0$, that K contains the $2\ell^{\text{th}}$ roots of unity, and that $\text{char}(\kappa(\nu)) \neq \ell$. By the proof of Lemma 3 (namely, the density theorem for primes in classes in generalized class groups) we may pick *two* distinct primes $\mathfrak{q}_1, \mathfrak{q}_2$ and elements $a_1, b_1, a_2, b_2 \in K$ such that $\psi_\ell(K; a_i, b_i) = \{x \in K^\times \mid \nu(x) \equiv 0 \mod \ell \wedge \nu_{\mathfrak{q}_i}(x) \equiv 0 \mod \ell\}$. But clearly *any* $y \in K^\times$ such that $\nu(y) \equiv 0 \mod \ell$ can be written as the product $y = z_1 z_2$ with $z_i \in \{x \in K^\times \mid \nu(x) \equiv 0 \mod \ell \wedge \nu_{\mathfrak{q}_i}(x) \equiv 0 \mod \ell\}$ and any such product has $\nu(z_1 z_2) \equiv 0 \mod \ell$. Set

$$\phi_\ell(x; a_1, b_1, a_2, b_2) := (\exists z_1, z_2) x = z_1 z_2 \wedge \psi_\ell(z_1; a_1, b_1) \wedge \psi_\ell(z_2; a_2, b_2).$$

Then

$$\phi_\ell(K; a_1, b_1, a_2, b_2) = \{x \in K^\times \mid \nu(x) \equiv 0 \mod \ell\}.$$

By Proposition 2, this implies that in fact ν is arithmetically definable!

To eliminate the special assumptions about K we show that we use an easy fact from commutative algebra:

Fact 8. *(Going-Up Theorem, [1] 5.11) Let $A \subseteq B$ be an integral extension of commutative rings and let $\mathfrak{p} \in Spec(A)$. Then there exists a $\mathfrak{q} \in B$ such that $\mathfrak{q} \cap A = \mathfrak{p}$.*

Using this fact we can prove the following

Claim 2. *Suppose that $L|K$ is a finite extension of number fields. Suppose that all discrete valuations w on L are arithmetically definable. Then all discrete valuations ν on K are definable.*

Proof of **claim**: Let ν be a discrete valuation on K. Then by the going up theorem, there is some $w|\nu$ on L. By assumption, w is arithmetically definable, say by some formula $\Phi_w(x; y; \bar{c})$. Take an element θ such that $L = K(\theta)$ and let $\{a_0, \cdots a_{n-1}\} \subseteq K$ (where $n = [L : K]$) be the coefficients of the minimal polynomial of θ. By Theorem 1, there exists an interpretation Γ of $(L, +, \times, 0, 1)$ in $(K, +, \times, 0, 1, a_0, \cdots, a_{n-1})$. Let $\Psi_\Gamma(\bar{x}, \bar{y}\overline{\pi^{-1}(c)})$ be a formula defining w. By construction, the first-order formula $\Psi_\Gamma(x_0, 0, \cdots, 0; y_0, 0, \cdots, 0; \overline{\pi^{-1}(c)})$ is satisfied exactly by those $x_0 \in K$ such that

$$w(x_0 + 0 \cdot \theta + \cdots + 0 \cdot \theta^{n-1}) \geq w(y_0 + 0 \cdot \theta + \cdots + 0 \cdot \theta^{n-1})$$

But as $w|\nu$, this is precisely the set

$$\{(x_0, y_0) \in K \mid w(x_0) \geq w(y_0)\} = \{(x_0, y_0) \in K \mid \nu(x_0) \geq \nu(y_0)\}$$

and so ν is arithmetically definable in K, as desired. □

Now note that for all discrete valuations ν on K, one of the following must occur: $\nu(2) = 0$, $\nu(3) = 0$ and either $\text{char}(\kappa(\nu)) \neq 2$, $\text{char}(\kappa(\nu)) \neq 3$. Consider the field $K(\zeta_{12})|K$. Then for *any* discrete valuation ν on K, any extension $w|\nu$ must have that

$$\{x \in (K(\zeta_{12}))^\times \mid w(x) \equiv 0 \mod \ell\} = \phi_{\ell_w}((K(\zeta_{12}); a_w, b_w)$$

for some $\ell_w \in \{2,3\}$ and $a_w, b_w \in (K(\zeta_{12}))^\times$. But then w is arithmetically definable over $K(\zeta_{12})$ and so by the claim above ν is arithmetically definable over K.

Conclusion and Further Results

In his original paper [6], proves the following stronger result:

Theorem 3. *([6] Theorems 1,6) Let K be a global field.*

- *If K is a number field, then every discrete valuation is arithmetically definable, as are the closed unit balls of all archimedean valuations.*
- *If K is a function field, then every discrete valuation is arithmetically definable.*

The function field analogue is proven using similar methods to the ones outlined above, and the proof of the archimedean case for number fields has a very topological flavor and relies upon deep theorems on quadratic forms.

By tweaking the first-order formulas ϕ_ℓ (defined in our proof of Theorem 2 above), Rumely is able to construct first order formulas $\Phi_\ell(x;\bar{z})$ such that for *all* global fields K and $\bar{c} \in K$, $\Phi(K;\bar{c})$ is either $\mathcal{O}_\nu$ for some discrete valuation ν or is all of K. This uses the characterization of valuation rings of K as subrings $R \subseteq K$ such that if $c \neq 0 \in K$, then either c or $c^{-1} \in R$. Moreover, Rumely shows there is a finite list $\{\ell_1, \cdots, \ell_n\}$ of primes such that *every* discrete ν on K there is some tuple $\overline{c_\nu} \in K$ with $\Phi_{\ell_i}(K;\overline{c_\nu}) = \mathcal{O}_\nu$ for some i. Using this and the fact that *universal* quantification is the same as taking a large intersection and that $\mathcal{O}_K = \bigcap_{\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)\setminus\{0\}} \mathcal{O}_\mathfrak{p}$ Rumely shows the following:

Theorem 4. *([6] Corollary 3) There is a first-order formula $Int(x)$ such such that, for all number fields K, $Int(K) = \mathcal{O}_K$.*

These results point to and culminate in Rumely's proof that

Theorem 5. *([6] Theorem 4) The first-order theory of global fields is **essentially** undecidable; that is, any consistent extension of the common first-order theory of global fields is undecidable.*

References

1. M. Atiyah and I. MacDonald. *Introduction To Commutative Algebra*. Addison Wesley, 1st edition, 1969.
2. W. Hodges. *A Shorter Model Theory*. Cambridge University Press, 1st edition, 1997.
3. S. Lang. *Algebraic Number Theory*. Springer, 2nd edition, 1994.
4. S. Lang. *Algebra*. Springer, 3rd edition, 2002.
5. J. Neukirch. *Algebraic Number Theory*. Springer, 1st edition, 1999.
6. R. S. Rumely. Undecidability and Definability for the Theory of Global Fields. *Transactions of the American Mathematical Society*, 262(1):195–217, November 1980.