Model Theory of Valued Difference Fields

Maurice Boffa Lecture
Mons, Belgium
27 May 2004

Thomas Scanlon
University of California, Berkeley
(scanlon@math.berkeley.edu)

Alternate Title: Arithmetic Tamed

To logicians, arithmetic is horribly complicated.

Theorem 1 (Gödel) *The theory of* $(\mathbb{Z}, +, \times, 0, 1)$ *is undecidable. Moreover, there are sets defined by arbitrarily complicated formulae (in the sense of quantifier complexity, say) which cannot be expressed in terms of simpler formulae.*

On the contary, geometry is very regular.

Theorem 2 (Tarski) *Euclidean geometry, understood as the theory of the real field, is decidable. Moreover, this theory admits elimination of quantifiers in the language of ordered rings.*

$\mathbb{Q}_p$: geometry from arithmetic

The p-adic valuation on $\mathbb{Z}$ (defined on the next slide) is derived from the theory of congruences modulo powers of p and, therefore, has an arithmetic flavor, but the theory of the ring of p-adic integers shares the geometric character of the theory of $\mathbb{R}$.

p-adic valuations

Let p be a prime number. Recall that on $\mathbb{Z}$ one defines the p-adic valuation by $v_p(0) = \infty$ and for nonzero n, $v_p(n) = m$ if $n \equiv 0 \pmod{p^m}$ while $n \not\equiv 0 \pmod{p^{m+1}}$.

The p-adic valuation is extended to $\mathbb{Q}$ via $v_p(\frac{a}{b}) := v_p(a) - v_p(b)$.

Define a metric on $\mathbb{Q}$ by

$$d_p(x, y) := p^{-v_p(x-y)}$$

The ring of p-adic integers, $\mathbb{Z}_p$, (respectively, the field of p-adic numbers, $\mathbb{Q}_p$) is the completion of $\mathbb{Z}$ (respectively, $\mathbb{Q}$) with respect to the p-adic distance.

Decidability of the p-adics

Theorem 3 (Ax, Kochen; Eršov) *The theory of* $(\mathbb{Z}_p, +, \times, 0, 1)$ *is decidable.*

Theorem 4 (Macintyre) *For* $x \in \mathbb{Z}_p$ *and* $n \in \mathbb{Z}_+$ *define* $P_n(x) \leftrightarrow (\exists y \in \mathbb{Z}_p) y^n = x$.

The structure $(\mathbb{Z}_p, +, \times, 0, 1, \{P_n\}_{n \in \mathbb{Z}_+})$ *admits elimination of quantifiers.*

Valued fields, more generally

Definition 1 A valued field is a field K given together with an ordered abelian group $(\Gamma, +, 0, <)$ and a surjective function $v : K \to \Gamma \cup \{\infty\}$ (where ∞ is a new symbol defined to have $\infty > \Gamma$ and $\infty + \gamma = \infty = \gamma + \infty$ for any $\gamma \in \Gamma$) for which

- $v(x) = \infty \Leftrightarrow x = 0$
- $v(xy) = v(x) + v(y)$ for $x, y \in K$
- $v(x + y) \geq \max\{v(x), v(y)\}$

Definition 2 The *ring of integers* of a valued field (K, v) is the ring $\mathcal{O}_{K,v} = \mathcal{O} := \{x \in K \mid v(x) \geq 0\}$. The set $\mathfrak{m} := \{x \in \mathcal{O} \mid v(x) > 0\}$ is a maximal ideal. The field $k(v) := \mathcal{O}/\mathfrak{m}$ is called the *residue field* and the map $\pi : \mathcal{O} \to k(v)$ the *reduction map.*

Henselian fields

As the first-order trace of the completeness of $\mathbb{R}$ is the intermediate value theorem for polynomials, the first-order content of the completeness of $\mathbb{Q}_p$ is Hensel's Lemma.

Definition 3 We say that the valued field (K, v) is *henselian* if for any polynomial $P(x) \in \mathcal{O}_K[x]$ and point $a \in \mathcal{O}$ with $v(P(a)) > 0 = v(P'(a))$ there is some $b \in K$ with $P(b) = 0$ and $v(a - b) > 0$.

More general Ax-Kochen-Eršov theorems

Theorem 5 (Ax, Kochen; Eršov) *If (K, v) and (L, w) are two henselian fields of characteristic zero, then $(K, v) \equiv (L, w)$ if and only if*

- $\mathrm{char}(k(v)) = 0$ *or* $\mathrm{char}(k(v)) = p$ *and $v(p)$ is the least positive element of the value group of K (as is $w(p)$ in L's value group) and*
- *the residue fields of K and L have the same theories as do the value groups.*

As a consequence of this theorem and a theorem of Ax on the decidability of the theory of finite fields, the theory of the p-adics is decidable uniformly in p.

Relative Frobenii from arithmetic

If K is a field of characteristic p, then the map $F : K \to K$ (called the [p-power] Frobenius [on K]) defined by $x \mapsto x^p$ is a homomorphism of rings.

On a field of characteristic zero, no such polynomial map is a homomorphism, but the Frobenius leaves its mark nevertheless.

Definition 4 Let K be a field of characteristic zero and p a prime number. We say that the field endomorphism $\sigma : K \to K$ is an *(arithmetic) relative Frobenius* if $\sigma(\zeta) = \zeta^p$ for every root of unity $\zeta \in K^\times$ of order prime to p.

Relative Frobenii geometrized

Definition 5 If (K, v) is a valued field of characteristic zero with residue characteristic $(\mathrm{char}(k(v)))$ p, then a (geometric) relative Frobenius on K is a field endomorphism $\sigma : K \to K$ for which $v(\sigma(x)) = v(x)$ for all $x \in K$ and $\sigma(x) \equiv x^p \pmod{\mathfrak{m}}$ for all $x \in \mathcal{O}$.

Every geometric Frobenius is actually an arithmetic Frobenius. (Almost) conversely, if $K \subseteq \mathbb{Q}^{\mathrm{alg}}$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$ is an arithmetic relative Frobenius, then there is a valuation v on K for which σ is a geometric relative Frobenius.

Comparing geometric and arithmetic Frobenii

Let (K, v) be a valued field of residue characteristic p.

Lemma 6 *If $\zeta \in K^\times$ is a root of unity, then $v(\zeta) = 0$.*

Lemma 7 *If $\zeta, \xi \in K^\times$ are two distinct roots of unity of order prime to p, then $v(\zeta - \xi) = 0$.*

Proposition 6 *If $\sigma : K \to K$ is a geometric Frobenius, then it is also an arithmetic Frobenius.*

Proof: Let $\mu := \{\zeta \in \mathcal{O}^\times \mid \zeta^n = 1 \text{ for some } n \text{ prime to } p\}$.

$$\begin{array}{ccc} \mu & \xrightarrow{x \mapsto \frac{\sigma x}{x^p}} & \mu \\ {\scriptstyle\pi}\downarrow & & \downarrow{\scriptstyle\pi} \\ (\mathbb{F}_p^{\mathrm{alg}})^\times & \xrightarrow{x \mapsto 1} & (\mathbb{F}_p^{\mathrm{alg}})^\times \end{array}$$

Witt vectors

Given a prime p there is a functor W from the category of $\mathbb{F}_p$-algebras to the category of commutative rings with the following properties:

- If k is a perfect field, then $W[k]$ is a valuation ring with maximal ideal generated by p.
- In general, $W[k]/pW[k]$ is naturally identified with k. In fact, if $\psi : k \to k'$ is a map of rings, then the map $W(\psi) : W[k] \to W[k']$ may be identified with ψ modulo p. In particular, for k a perfect field, $W(F) : W[k] \to W[k]$ is a relative Frobenius.

Witt vectors, continued

- For any $n \in \mathbb{Z}_+$, there is a natural identification (as sets) of $W[k]/p^n W[k]$ with k^n. The ring operations on $W[k]/p^n W[k]$ correspond to polynomial functions on k^n.
- $W[k]$ is p-adically complete.

$W[\mathbb{F}_p] = \mathbb{Z}_p$ and $W[\mathbb{F}_p^{\mathrm{alg}}]$ is the completion of the maximal unramified extension of $\mathbb{Z}_p$.

Teichmüller characters

Let k be a perfect field of characteristic p. One may define a multiplicative section of the reduction map $\tau : k \to W[k]$ by the formula

$$\tau(x) = \lim_{n \to \infty, \pi(a) = \sqrt[p^n]{x}} a^{p^n}$$

Theorem 7 (van den Dries) *Let (K, v) be the field of fractions of $W[\mathbb{F}_p^{\mathrm{alg}}]$. Let T be a unary predicate on K whose interpretation is defined by*
$K \models T(x) \Leftrightarrow x = 0$ or $x^n = 1$ for some nonzero integer n. Then the theory of $(K, +, \times, v, T)$ is decidable.

Teichmüller characters via valued difference rings

The Teichmüller map is definable in $(W[\mathbb{F}_p^{alg}], +, \times, v, \sigma)$ (where σ is the relative Frobenius) by the condition

$$b = \tau(a) \quad \Leftrightarrow \quad \pi(b) = a \text{ and } \sigma(b) = b^p$$

Related maps defined on other (than the multiplicative group) algebric groups are definable in this structure.

For instance, if E is an elliptic curve over $\mathbb{Q}_p$ for which we have a good integral model, then there is a natural reduction map $\pi : E(K) \to \overline{E}(k(v))$ from the group of K-points on E to the $k(v)$-points on the reduced elliptic curve. A section of π is definable in $(K, +, \times, v, \sigma)$ and the image of this section contains (most of) the torsion subgroup of $E(K)$.

The theory of the relative Frobenius

Theorem 8 (Bélair, Macintyre, Scanlon) *The theory of the Witt vectors of the algebraic closure of the field of p elements given together with the relative Frobenius is decidable and eliminates quantifiers in a natural language, namely in the expansion of the language of valued difference fields by divisibility predicates on the value group.*

p-adic analytic functions

If $\sum_{n=0}^{\infty} a_n x^n \in \mathbb{Z}_p[[x]]$ is any power series over $\mathbb{Z}_p$, then for any $\xi \in p\mathbb{Z}_p$, the sum $\sum_{n=0}^{\infty} a_n \xi^n$ converges. More generally (and one can see that this is more general via the change of variables $x \mapsto px$), if $\sum_{n=0}^{\infty} a_n x^n \in \mathbb{Z}_p[[x]]$ is a power series with p-adic coefficients for which $v(a_n) \to \infty$, then for any $\eta \in \mathbb{Z}_p$, the series $\sum_{n=0}^{\infty} a_n \eta^n$ converges.

The usual Taylor series expansion of the exponential function $\sum_{n=0}^{\infty} \frac{1}{n!} x^n$ has a nontrivial p-adic radius of convergence.

The power series

$$\sum_{n=0}^{\infty} \frac{p^n}{n!} x^n$$

defines an analytic function on $W[\mathbb{F}_p^{\mathrm{alg}}]$ (for $p > 2$) and as in the case of the real numbers this function is a homomorphism from the additive group to the multiplicative group.

Analytic structure on valued fields

Let (K, v) be a complete valued field (with value group a subgroup of $\mathbb{Q}$). A power series $\sum a_\alpha x^\alpha \in K[[x_1, \ldots, x_n]]$ defines an analytic function function $f : \mathcal{O}^n \to K$ if for every $\xi \in \mathcal{O}^m$ the sum $\sum a_\alpha \xi^m$ converges.

By K_{an} we mean K considered as a structure in the language of valued fields augmented by a function symbol for each analytic function over K (to be interpreted by its corresponding function on $\mathcal{O}^n$ and by the zero map off its natural domain).

Analytic quantifier elimination

The theory of $(\mathbb{Q}_p)_{an}$ does not eliminate quantifiers, even if we expand the language to ensure quantifier elimination for the algebraic reduct. However, we have the following theorem.

Theorem 9 (Denef, van den Dries) $(\mathbb{Z}_p)_{an}$ *admits elimination of quantifiers in the expansion of the language of analytic rings enriched by the Macintyre power predicates and a restricted division function* $\mathcal{Q}$ *defined by*

$$\mathcal{Q}(x,y) = \begin{cases} \frac{x}{y} \text{ if } v(x) \geq v(y) \neq \infty \\ 0 \text{ otherwise} \end{cases}$$

Analytic difference structure

Question 10 What is the theory of $(W[\mathbb{F}_p^{\text{alg}}]_{an}, \sigma)$?

A detailed answer to this question will come tomorrow, but another question must be addressed first.

Question 11 Is there mathematical content in the mixing of analytic functions and the relative Frobenius?

Buium's p-jet functions

From the relative Frobenius $\sigma : W[k] \to W[k]$ on $W[k]$ one can define a new operator $\delta : W[k] \to W[k]$ by

$$\delta(x) \quad := \quad \frac{\sigma(x) - x^p}{p}$$

A p-jet function (on $W[k]^n$) is a function $f : W[k]^n \to K$ of the form $f(x_1, \ldots, x_n) =$
$g(x_1, \ldots, x_n; \delta(x_1), \ldots, \delta(x_n); \ldots; \delta^m(x_1), \ldots, \delta^m(x_n))$ for some m and analytic function g.

Examples of p-jet functions

- Recall that the Legendre symbol $(\frac{a}{p})$ is defined on $\mathbb{Z} \setminus p\mathbb{Z}$ by $(\frac{a}{p}) = 1$ if a is a square modulo p and $(\frac{a}{p}) = -1$ otherwise. For p an odd prime, one can exptress the Legendre symbol as $(\frac{a}{p}) = a^{\frac{p-1}{2}}(1 + \sum_{n=1}^{\infty}(-1)^{n-1}\frac{(2n-2)!p^n}{2^{2n-1}(n-1)!n!}(\delta_p a)^n a^{-pn})$.
- Recall that via the j-invariant, the affine line may be regarded as the moduli space for elliptic curves. Buium constructs a p-jet function $f : W[k] \to W[k]$ having the property that if E, E' are isogenous elliptic curves over $W[k]$ then $f(j(E)) = f(j(E'))$, but the fibres of f are "small."
- For any elliptic curve E over $W[k]$, Buium constructs a p-jet function $\mu : E(W[k]) \to W[k]$ which is a surjective homomorphism.

Completeness and Quantifier elimination for analytic difference fields

Theorem 12 *The theory of* $(W[\mathbb{F}_p^{\mathrm{alg}}]_{an}, W(F))$ *eliminates quantifiers in the expansion of the language by* $\mathcal{Q}$ *and divisibility predicates on the value group.*

Nash theorems

Theorem 13 (Nash, Greenberg) *Let* (K, v) *be a complete discretely valued field with an algebraically closed residue field and* $f_1, \ldots, f_\ell \in \mathcal{O}[x_1, \ldots, x_m]$ *a finite sequence of polynomials over* $\mathcal{O}$*. Let* $X = V((f_1, \ldots, f_\ell))(\mathcal{O}) = \{a \in \mathcal{O}^m \mid f_1(a) = \cdots = f_\ell(a) = 0\}$*. For any natural number* M*, if we identify* $\mathcal{O}/\mathfrak{m}^{M+1}$ *with* $k(v)^{M+1}$ *in the usual way, then* $X \mod \mathfrak{m}^{M+1}$ *is a constructible set.*

The quantifier elimination theorems imply that when K is the field of fractions of $W[k]$ for $k = k^{\mathrm{alg}}$, then the same result is true for X any definable (in $(W[k]_{an}, W(F))$) set.

Buium's Fermat adèles

Buium has introduced a uniform (in p) version of his p-jet functions. The key operations in the formation of his ring of *Fermat adèles* are

- closure under uniform p-adic completion,
- closure under the p-jet operator $x \mapsto \delta_p(x) = \frac{W(F)(x)-x^p}{p}$, and
- closure under taking of principal parts.

Model theoretic approach to Fermat adèles

- Van den Dries' uniform analytic Ax-Kochen-Eršov theorem (and its refinement by Lipshitz and Z. Robinson) give(s) a method to express the uniform p-adic completions.
- The (uniform) theory of analytic difference rings allows us to understand $W(F)$ uniformly in p. Work of Hrushovski (to be discussed by Chatzidakis here), gives a uniform theory of the function $x \mapsto x^p$ on $W[k]$. To understand δ uniformly, we need both. For now, it is unknown what that joint theory is (and *a fortiori*, the theory of $W[k]_{an}$ with $W[k]$ and the p-power map is unknown).
- I do not have a good proposal for incorporating the principal part operator. Is it really necessary? For instance, the Legendre symbol is a Fermat adèle simply in terms of the first two operations.

Conclusion

Arithmetic itself, as codified in the theory of the integers, is logically beyond reach, but a great many of the most powerful tools used to study number theory have tractible theories.

Moreover, rather than merely codifying the empirical observation that work in complete fields, *etc.*, can be easier than direct analysis of number theoretic problems, the formal logical presentation of these theories exposes hitherto unseen uniformities.