Geometric proof of Ax-Kochen's theorem on p-adic forms

Jan Denef

October 4, 2010

The Ax-Kochen Theorem

Ax-Kochen Theorem (1965)

$\forall d \in \mathbb{N}$, $\forall$ *primes* $p \gg 0$, *any homogeneous polynomial over* $\mathbb{Z}_p$ *of degree* d *with* $> d^2$ *variables has a nontrivial zero in* $\mathbb{Z}_p$.

- $\mathbb{Z}_p$ is the ring of p-adic itegers.
- Was conjectured by E.Artin for all p.
- Not true for all p: Terjanian 1966.
- Is true for $\mathbb{Z}_p$ replaced by $\mathbb{F}_p[[t]]$, for all p, where $\mathbb{F}_p$ is the finite field with p elements. Proof (Chevalley, Tsen, Lang) (1950) does not adapt to $\mathbb{Z}_p$.

Ax-Kochen's proof

The Ax-Kochen Theorem is a direct consequence of:

Ax-Kochen-Ersov Transfer Principle (1965)

Let φ be a statement about rings formulated in predicate logic. Then for all primes $p \gg 0$ we have:
φ is true in $\mathbb{Z}_p$ if and only if φ is true in $\mathbb{F}_p[[t]]$.

- The proofs of Ax-Kochen and Ersov of this principle are entirely based on model theory (mathematical logic).
- Another proof by P.Cohen (1969) is based on quantifier elimination (more elementary, but very much in the spirit of mathematical logic).

First geometric proof

- Uses that it is true for $\mathbb{F}_p[[t]]$.
- Proves a very special case of Ax-Kochen-Ersov Transfer Principle, which we call Transfer of Surjectivity.
- Still similar to Ax-Kochen proof, but no logic.
- Is based on a Theorem of Abramovich and Karu on Weak Toroidalization of Morphisms.
- Instead of toroidalization one can use Cutkosky's Theorem on Local Monomialization of Morphisms, but toroidalization yields a simpler proof and additional results.
- Also yields a geometric proof of the Ax-Kochen-Ersov Transfer Principle, altough here one needs a little bit of mathematical logic (even for the statement of the transfer principle).

Second geometric proof

- No transfer, no $\mathbb{F}_p[[t]]$, no logic.
- By proving in geometric way a conjecture of Colliot-Thélène using toroidalization.
- Colliot-Thélène proved that his conjecture implies the Ax-Kochen Theorem.

Colliot-Thélène's Conjecture

Let $f : X \to Y$ be a surjective morphism of smooth projective geometrically irreducible varieties over $\mathbb{Q}$. Assume that

- *the generic fibre of f is geometrically irreducible,*
- *the generic fibre of f has 'nice' degenerations.*

Then f induces a surjection on the p-adic points, for all $p \gg 0$.

The universal hypersurface

Consider the universal homogeneous polynomial of degree d in n variables $x_1, \ldots, x_n$

$$\sum_{e_1+\cdots+e_n=d} c_{e_1,\ldots,e_n} \, x_1^{e_1} \ldots x_n^{e_n} \, ,$$

where the coefficients $c_{e_1,\ldots,e_n}$ are indeterminates.
This defines a hypersurface

$$H \subset \mathbb{P}^n \times \mathbb{P}^M,$$

where $M := \sharp(\text{monomials of degree } d)-1$. Consider the projection

$$\pi : H \to \mathbb{P}^M.$$

Reformulation of Ax-Kochen Theorem

For all primes $p \gg 0$, the map $\pi : H(\mathbb{Z}_p) \to \mathbb{P}^M(\mathbb{Z}_p)$ is surjective.

Transfer of Surjectivity

Thus the Ax-Kochen Theorem is a direct consequence of the following special case of the Ax-Kochen-Ersov Transfer Principle:

Theorem: Transfer of Surjectivity

Let $f : X \to Y$ be a morphism of varieties over $\mathbb{Z}$ (i.e. integral separable schemes of finite type over $\mathbb{Z}$). For all primes $p \gg 0$ we have:

$$f : X(\mathbb{Z}_p) \to Y(\mathbb{Z}_p)$$

is surjective if and only if

$$f : X(\mathbb{F}_p[[t]]) \to Y(\mathbb{F}_p[[t]])$$

is surjective.

Notation and conventions

- p denotes always a prime number.
- Let R be a noetherian integral domain.
- Denote by Frac(R) the field of fractions of R.
- A variety over R is an integral separated scheme of finite type over R.
- Let X and Y be varieties over R.
- Let $f : X \to Y$ be an R-morphism of varieties over R.
- For any R-algebra A, let $X(A)$ be the set of A-rational points on X.

Multiplicative residues

Let X be a variety over R.
Let A be a local R-algebra without zero divisors, and $\mathfrak{m}$ its maximal ideal.

Definition

Let $z, z' \in \mathrm{Frac}(A)$. The elements z, z' have same multiplicative residue if

$$z' \in z(1 + \mathfrak{m}).$$

Let $a, a' \in X(A)$ and $x_1, \ldots, x_r$ rational functions on X. The points a, a' have same residues with respect to $x_1, \ldots, x_r$, if for $i = 1, \ldots, r$

1. $a \mod \mathfrak{m} = a' \mod \mathfrak{m}$,
2. *$x_i(a)$ is defined as element of $\mathrm{Frac}(A)$ if and only if $x_i(a')$ is defined,*
3. *$x_i(a)$, $x_i(a')$ have same multiplicative residue, if both are defined.*

Residues: more terminology

Instead of working with rational functions $x_1, \ldots, x_r$, we can also work with subvarieties:

Definition

Let $a, a' \in X(A)$ and $D_1, \ldots, D_r \subset X$ closed subsets of X. The points a, a' have same residues with respect to $D_1, \ldots, D_r$, if for $i = 1, \ldots, r$

1. $a \mod \mathfrak{m} = a' \mod \mathfrak{m}$,
2. *If locally at $a \mod \mathfrak{m}$, the ideal of D_i is principal, say generated by g_i, then $g_i(a)$, $g_i(a')$ have same multiplicative residue.*

Residues of $\mathbb{Z}_p$ and $\mathbb{F}_p[[t]]$

- The multiplicative residue of $z \in \mathbb{Z}_p$ is completely determined by
  1. $\operatorname{ord}_p z \in \mathbb{Z}$,
  2. $\overline{\mathrm{ac}}(z) := z\, p^{-\operatorname{ord}_p z} \mod p \in \mathbb{F}_p$.
- The multiplicative residue of $z' \in \mathbb{F}_p[[t]]$ is completely determined by
  1. $\operatorname{ord}_t z' \in \mathbb{Z}$,
  2. $\overline{\mathrm{ac}}(z') := z'\, t^{-\operatorname{ord}_t z'} \mod t \in \mathbb{F}_p$.
- These are determined by the same kind of data, hence we can identify multiplicative residues of elements in $\mathbb{Z}_p$ with these of $\mathbb{F}_p[[t]]$.
- Thus our definition of a and a' having *same residues with respect to* $x_1, \ldots, x_r$, also makes sense if $a \in X(\mathbb{Z}_p)$ and $a' \in X(\mathbb{F}_p[[t]])$.
  We are assuming here that $R = \mathbb{Z}$.

Tameness Theorem

Let $f : X \to Y$ be an morphism of varieties over R, and assume R has characteristic zero.

Tameness Theorem

Given rational functions $x_1, \ldots, x_r$ on X, there exist rational functions $y_1, \ldots, y_s$ on Y, and $\Delta \in R \setminus \{0\}$, such that for any $R[\Delta^{-1}]$-algebra A which is a henselian valuation ring we have the following.
Any $b \in Y(A)$ having same residues w.r.t. $y_1, \ldots, y_s$ as an image $f(a')$, with $a' \in X(A)$, is itself an image of an $a \in X(A)$ with same residues as a' w.r.t. $x_1, \ldots, x_r$.

Logarithmic Hensel Lemma

Let $f : X \to Y$ be a morphism of varieties over R, and $D \subset X$, $E \subset Y$ closed subsets with $f^{-1}(E) \subset D$. Denote the irreducible components of D and E by $D_1, \ldots, D_r$ and $E_1, \ldots, E_s$. Let A be any henselian integral local R-algebra with maximal ideal $\mathfrak{m}$.

Logarithmic Hensel Lemma

Let $a \in X(A) \setminus D(A)$, and set $\bar{a} := a \mod \mathfrak{m}$. Assume that

1. *X smooth/R at $\bar{a}$, and D strict normal crossings divisor/R at $\bar{a}$,*
2. *Y smooth/R at $f(\bar{a})$, and E strict normal crossings divisor/R at $f(\bar{a})$,*
3. *f log-smooth at $\bar{a}$ with respect to D, E.*

Then, any $b \in Y(A)$ having same residues w.r.t. $E_1, \ldots, E_s$ as an image $f(a')$, with $a' \in X(A)$, is itself an image of an $a \in X(A)$ with same residues as a' w.r.t. $D_1, \ldots, D_r$.

Definition of log-smoothness

Assume the notation and assumptions 1/ and 2/ of previous slide.

- Choose uniformizing parameters $x_1, \dots, x_n$ over R on a nbh of $\bar{a}$ in X so that locally at $\bar{a}$ the locus of $\prod_i x_i$ is D.
- Choose uniformizing parameters $y_1, \dots, y_m$ over R on a nbh of $f(\bar{a})$ in Y so that locally at $f(\bar{a})$ the locus of $\prod_j y_j$ is E.
- Uniformizing parameters over R on a nbh U, are regular functions on U that induce an etale morphism to affine space over R.

Definition

f is called log-smooth at $\bar{a}$ with respect to D, E, if the logarithmic jacobian

$$\left(\frac{\partial \log y_j}{\partial \log x_i}(\bar{a})\right)_{i,j}$$

has rank $=$ relative dimension of Y/R at $f(\bar{a})$.

Proof of Logarithmic Hensel

Assume the notation of the two previous slides.

- If $x_i(a) \notin \mathfrak{m}$, for all i, then $y_j(a) \notin \mathfrak{m}$, since $f^{-1}(E) \subset D$. Hence the logarithmic jacobian equals the ordinary jacobian. Thus Hensel's Lemma applies.
- In the general case, we change coordinates

$$x_i = x_i(a)(1 + x_i'), \;\; y_j = y_j(f(a))(1 + y_j').$$

Since this does not change the logarithmic jacobian we are reduced to the previous case. However, the details are more subtle.

Toroidal morphisms

Definition

Let k be a field of characteristic zero. Let $f : X \to Y$ be a dominating morphism of nonsingular k-varieties, and $D \subset X$, $E \subset Y$ strict normal crossings divisors. We call f toroidal with respect to D and E if $f^{-1}(E) \subset D$, and if, after replacing k by an algebraic closure of k, for each closed point a of X there exist formal uniformizing parameters $x_1, \dots, x_n$ for X at a, and $y_1, \dots, y_m$ for Y at $f(a)$ such that

1. *locally at a, D is the locus of $\prod_i x_i = 0$,*
2. *locally at $f(a)$, E is the locus of $\prod_j y_j = 0$,*
3. *the morphism f gives the y_j as monomials in the x_i.*

Uniformizing parameters x_i for X at a are elements of $\widehat{\mathcal{O}}_{X,a}$ such that the $x_i - c_i$ form a system of regular parameters for $\widehat{\mathcal{O}}_{X,a}$, for suitable $c_i \in k$.

Corollary of Logarithmic Hensel

Let $f : X \to Y$ be a dominating morphism of smooth varieties over R, and assume R has characteristic zero. Let $D \subset X$, $E \subset Y$ be closed subsets with $f^{-1}(E) \subset D$. Denote the irreducible components of D and E by $D_1, \ldots, D_r$ and $E_1, \ldots, E_s$. Assume that D, E are simple normal crossings divisors over R. Because a toroidal morphism is log-smooth, we have:

Corollary

If $f \otimes \mathrm{Frac}(R)$ is toroidal w.r.t. D, E, then there exists $\Delta \in R \setminus \{0\}$, such that for any henselian integral local $R[\Delta^{-1}]$-algebra A we have: Any $b \in Y(A)$ having same residues w.r.t. $E_1, \ldots, E_s$ as an image $f(a')$, with $a' \in X(A)$, is itself an image of an $a \in X(A)$ with same residues as a' w.r.t. $D_1, \ldots, D_r$.

The Tameness Theorem is a direct consequence of this corollary and weak toroidalization, using induction on the dimension of $X \otimes_R \mathrm{Frac}(R)$.

Toroidalization of Morphisms

Theorem: Weak Toroidalization (Abramovich-Karu 2000, $+\ \epsilon$)

Let k be a field of characteristic zero. Let $f : X \to Y$ be a dominating morphism of k-varieties, and let $Z \subset X$ be a proper closed subset. Then there exist nonsingular k-varieties X', Y' and a commutative diagram

$$\begin{array}{ccccc} D & \subset & X' & \stackrel{m_X}{\to} & X \\ & & \downarrow f' & & \downarrow f \\ E & \subset & Y' & \stackrel{m_Y}{\to} & Y \end{array}$$

with m_X, m_Y modifications, D, E strict normal crossings divisors, so that

1. *f' is a toroidal morphism with respect to D, E,*
2. *$m_X^{-1}(Z)$ is a divisor on X', and is contained in D,*
3. *the restricted morphism $X' \setminus D \to m_X(X' \setminus D)$ is an isomorphism.*

Transfer of Residues

The following lemma is an easy application of Hironaka's Embedded Resolution of Singularities.

Lemma: Transfer of Residues

Let X be a variety over $\mathbb{Z}$, and $x_1, \ldots, x_r$ rational functions on X. Assume that $p \gg 0$.

1. *For each $a \in X(\mathbb{Z}_p)$ there exists $a' \in X(\mathbb{F}_p[[t]])$ with same residues as a w.r.t. $x_1, \ldots, x_r$.*
2. *For each $a \in X(\mathbb{F}_p[[t]])$ there exists $a' \in X(\mathbb{Z}_p)$ with same residues as a w.r.t. $x_1, \ldots, x_r$.*

Proof of Transfer of Residues

Given: $a \in X(\mathbb{Z}_p)$
Goal: find $a' \in X(\mathbb{F}[[t]])$ with same residues as a w.r.t. $x_1, \ldots, x_r$.
We consider 3 cases.

- Case 1: the x_i are uniformizing parameters on X, meaning that they induce an etale morphism $\pi : X \to \mathbb{A}^r_{\mathbb{Z}}$.
  Choose $z_i \in \mathbb{F}[[t]]$ having same multiplicative residue as $x_i(a_i)$.
  Hensel's Lemma for π yields $a' \in X(\mathbb{F}[[t]])$ with $x_i(a') = z_i$.
- Case 2: the x_i are monomials in uniformizing parameters on X.
  Choose a' having same residues as a w.r.t. these uniformizers.
- Case 3: the general case.
  Reduce locally to case 2, by applying Embedded Resolution of Singularities to the union of the divisors of the x_i on $X \otimes \mathbb{Q}$.

Proof of Transfer of Surjectivity

Given: $f : X \longrightarrow Y$, $p \gg 0$, $b \in Y(\mathbb{Z}_p)$, surjectivity for $\mathbb{F}_p[[t]]$.

Goal: find $a \in X(\mathbb{Z}_p)$ with $f(a) = b$.

1. By Tameness Theorem, get rational functions $y_1, \ldots, y_s$ on Y $\rightsquigarrow$ any $b \in Y(\mathbb{Z}_p)$ having same residues w.r.t. $y_1, \ldots, y_s$ as an image, is itself an image.
2. By Transfer of Residues get $b' \in Y(\mathbb{F}_p[[t]])$ $\rightsquigarrow$ b and b' have same residues w.r.t. $y_1, \ldots, y_s$.
3. By surjectivity for $\mathbb{F}_p[[t]]$, get $a' \in X(\mathbb{F}_p[[t]])$ $\rightsquigarrow$ $f(a') = b'$.
4. By Transfer of Residues, get $a'' \in X(\mathbb{Z}_p)$
   $\rightsquigarrow$ a' and a'' have same residues w.r.t. $y_1 \circ f, \ldots, y_s \circ f$.
   $\rightsquigarrow$ $f(a')$ and $f(a'')$ have same residues w.r.t. $y_1, \ldots, y_s$.
   $\rightsquigarrow$ b and $f(a'')$ have same residues w.r.t. $y_1, \ldots, y_s$, by 2/ and 3/.
5. Thus $b = f(a)$ for some $a \in X(\mathbb{Z}_p)$, by 1/.

Second geometric proof

Colliot-Thélène's Conjecture

Let $f : X \to Y$ be a surjective morphism of smooth projective geometrically irreducible varieties over $\mathbb{Q}$. Assume that

- *the generic fibre of f is geometrically irreducible,*
- *the generic fibre of f has 'nice' degenerations, i.e. for any discrete valuation on the function field of Y, with valuation ring $A \supset \mathbb{Q}$, there exists a proper flat model $\mathfrak{X}$ over A of the generic fibre of f so that:*
  1. *$\mathfrak{X}$ is integral and regular,*
  2. *the special fibre of $\mathfrak{X}$ has an irreducible component of multiplicity 1 which is geometrically integral.*

Then f induces a surjection on the p-adic points, for all $p \gg 0$.

Colliot-Thélène proved that his conjecture implies the Ax-Kochen Theorem.

A sketch of our proof of the conjecture will be contained in the next version of these slides. This will be posted on my personal web page http://wis.kuleuven.be/algebra/denef.html
I will also add slides sketching proofs of the general Ax-Kochen-Ersov Transfer Principle, and the Basarab Quantifier Elimination Theorem.