First-Order and Existential Definability and Decidability in Positive Characteristic

Alexandra Shlapentokh

East Carolina University

July 2012

Outline

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.

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 $\mathbb{Q}$.

Does Hilbert's Question Make Sense over Uncountable Rings?

Yes, it does make sense to consider uncountable rings

as long as we consider polynomial equations with coefficients restricted to a countable recursive subring. We can still consider solutions in the bigger ring. In other words, given a polynomial equation with coefficients in a fixed finitely generated ring, we will consider existence of an algorithm which can take the coefficients as inputs and determine whether solutions exist in the bigger, possibly uncountable ring.

Outline

Fields of Positive Characteristic

Definition

Let p be a prime number and let k be a field such that for any element x of the field $px = 0$. In this case we say that the field has characterisitic p.

Example

For any prime number p it is the case that $\mathbb{Z}/p$ is a field of characteristic p. Any field of characteristic p contains $\mathbb{Z}/p$ as a subfield.

Fields of Positive Characteristic

Definition

Let p be a prime number and let k be a field such that for any element x of the field $px = 0$. In this case we say that the field has characterisitic p.

Example

For any prime number p it is the case that $\mathbb{Z}/p$ is a field of characteristic p. Any field of characteristic p contains $\mathbb{Z}/p$ as a subfield.

Transcendence Degree of a Field

Definition (Algebraic Independence)

Let K/k be a field extension, and let $y_1, \ldots, y_n \in K$. In this case, if for any polynomial $P(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ we have that $P(y_1, \ldots, y_n) = 0 \iff P(X_1, \ldots, X_n) \equiv 0$ as an element of $k[X_1, \ldots, X_n]$, and $n \in \mathbb{Z}_{\geq 2}$, we say that $y_1, \ldots, y_n$ are algebraically independent over k. If $n = 1$, then we say that y_1 is transcendental over k.

Definition (Transcendence Degree)

If K/k is a field extension, then the transcendence degree of K/k is the size of the largest subset of elements of K algebraically independent over k.

Transcendence Degree of a Field

Definition (Algebraic Independence)

Let K/k be a field extension, and let $y_1, \ldots, y_n \in K$. In this case, if for any polynomial $P(X_1, \ldots, X_n) \in k[X_1, \ldots, X_n]$ we have that $P(y_1, \ldots, y_n) = 0 \iff P(X_1, \ldots, X_n) \equiv 0$ as an element of $k[X_1, \ldots, X_n]$, and $n \in \mathbb{Z}_{\geq 2}$, we say that $y_1, \ldots, y_n$ are algebraically independent over k. If $n = 1$, then we say that y_1 is transcendental over k.

Definition (Transcendence Degree)

If K/k is a field extension, then the transcendence degree of K/k is the size of the largest subset of elements of K algebraically independent over k.

Rational and Algebraic Function Fields of Positive Characteristic

Definition (Rational Function Field of Positive Characteristic)

Let k be any field of positive characteristic. Let t be transcendental over k. In this case $k(t)$ is a rational function field of positive characteristic over the field of constants k.

Definition (Algebraic Function Field of Positive Characteristic)

Let $k(t)$ be as above and let $K/k(t)$ be a finite extension. In this case K is a (algebraic) function field of positive characteristic. The field of constants of K is the algebraic closure of k in K.

Rational and Algebraic Function Fields of Positive Characteristic

Definition (Rational Function Field of Positive Characteristic)

Let k be any field of positive characteristic. Let t be transcendental over k. In this case $k(t)$ is a rational function field of positive characteristic over the field of constants k.

Definition (Algebraic Function Field of Positive Characteristic)

Let $k(t)$ be as above and let $K/k(t)$ be a finite extension. In this case K is a (algebraic) function field of positive characteristic. The field of constants of K is the algebraic closure of k in K.

Transcendence Degree of Function Fields

Remark

A function field is of transcendence degree 1 over its field of constants. One can also consider the transcendence degree of a function field over $\mathbb{Z}/p$. This degree can be any positive integer or infinity.

Outline

HTP over Rational Function Fields of Positive Characteristic

Theorem

HTP is unsolvable over the following fields:

- *rational function fields over finite fields of characteristic greater than 2 (Pheidas, 1991);*
- *rational function fields over a constant field k, where k is a proper subfield of the algebraic closure of a finite field (Kim and Roush, 1992).*
- *rational function field of a finite transcendence degree greater or equal to two over the algebraic closure of a finite field of odd characteristic (Kim and Roush, 1992).*
- *rational function fields over finite fields of characteristic 2 (Videla, 1994).*

HTP over Rational Function Fields of Positive Characteristic

Theorem

HTP is unsolvable over the following fields:

- *rational function fields over finite fields of characteristic greater than 2 (Pheidas, 1991);*
- *rational function fields over a constant field k, where k is a proper subfield of the algebraic closure of a finite field (Kim and Roush, 1992).*
- *rational function field of a finite transcendence degree greater or equal to two over the algebraic closure of a finite field of odd characteristic (Kim and Roush, 1992).*
- *rational function fields over finite fields of characteristic 2 (Videla, 1994).*

HTP over Rational Function Fields of Positive Characteristic

Theorem

HTP is unsolvable over the following fields:

- *rational function fields over finite fields of characteristic greater than 2 (Pheidas, 1991);*
- *rational function fields over a constant field k, where k is a proper subfield of the algebraic closure of a finite field (Kim and Roush, 1992).*
- *rational function field of a finite transcendence degree greater or equal to two over the algebraic closure of a finite field of odd characteristic (Kim and Roush, 1992).*
- *rational function fields over finite fields of characteristic 2 (Videla, 1994).*

HTP over Rational Function Fields of Positive Characteristic

Theorem

HTP is unsolvable over the following fields:

- *rational function fields over finite fields of characteristic greater than 2 (Pheidas, 1991);*
- *rational function fields over a constant field k, where k is a proper subfield of the algebraic closure of a finite field (Kim and Roush, 1992).*
- *rational function field of a finite transcendence degree greater or equal to two over the algebraic closure of a finite field of odd characteristic (Kim and Roush, 1992).*
- *rational function fields over finite fields of characteristic 2 (Videla, 1994).*

HTP over Algebraic Function Fields of Positive Characteristic of Transcendence Degree 1

Theorem

HTP is unsolvable over the following fields:

- *algebraic function fields over finite fields of characteristic greater than 2 (S. 1996);*
- *algebraic function fields over fields of constants k algebraic over $\mathbb{Z}/p$ and having an extension of degree $p > 2$ (S. 2000);*
- *fields as above for $p = 2$ (Eisenträger 2003)*

HTP over Algebraic Function Fields of Positive Characteristic of Transcendence Degree 1

Theorem

HTP is unsolvable over the following fields:

- *algebraic function fields over finite fields of characteristic greater than 2 (S. 1996);*
- *algebraic function fields over fields of constants k algebraic over $\mathbb{Z}/p$ and having an extension of degree $p > 2$ (S. 2000);*
- *fields as above for $p = 2$ (Eisenträger 2003)*

HTP over Algebraic Function Fields of Positive Characteristic of Transcendence Degree 1

Theorem

HTP is unsolvable over the following fields:

- *algebraic function fields over finite fields of characteristic greater than 2 (S. 1996);*
- *algebraic function fields over fields of constants k algebraic over $\mathbb{Z}/p$ and having an extension of degree $p > 2$ (S. 2000);*
- *fields as above for $p = 2$ (Eisenträger 2003)*

HTP over Algebraic Function Fields of Positive Characteristic of Higher Transcendence Degree

Theorem

HTP is unsolvable over the following fields.

- *a field $K = k(u,v) \otimes_{\mathbb{Z}/p} F$, where $p > 2$, k is algebraic over $\mathbb{Z}/p$ and has an extension of degree p, u is transcendental over k, v is algebraic over $k(u)$, and $k(u,v)$ and F linearly disjoint over $\mathbb{Z}/p$ (S. 2000);*
- *K as above for $p = 2$ (Eisenträger 2003)*
- *any field K finitely generated over $\mathbb{Z}/p$ (S. 2002)*
- *a field $K = E \otimes_{\mathbb{Z}/p} F$, where E is finitely generated over a field k algebraic over $\mathbb{Z}/p$ and with an extension of degree p, and E and F are linearly disjoint over $\mathbb{Z}/p$ (S. 2003)*
- *an algebraic function field K of finite transcendence degree greater or equal to two over the algebraic closure of a finite field of odd characteristic (Eisenträger, 2012)*

HTP over Algebraic Function Fields of Positive Characteristic of Higher Transcendence Degree

Theorem

HTP is unsolvable over the following fields.

- *a field $K = k(u, v) \otimes_{\mathbb{Z}/p} F$, where $p > 2$, k is algebraic over $\mathbb{Z}/p$ and has an extension of degree p, u is transcendental over k, v is algebraic over $k(u)$, and $k(u, v)$ and F linearly disjoint over $\mathbb{Z}/p$ (S. 2000);*
- *K as above for $p = 2$ (Eisenträger 2003)*
- *any field K finitely generated over $\mathbb{Z}/p$ (S. 2002)*
- *a field $K = E \otimes_{\mathbb{Z}/p} F$, where E is finitely generated over a field k algebraic over $\mathbb{Z}/p$ and with an extension of degree p, and E and F are linearly disjoint over $\mathbb{Z}/p$ (S. 2003)*
- *an algebraic function field K of finite transcendence degree greater or equal to two over the algebraic closure of a finite field of odd characteristic (Eisenträger, 2012)*

HTP over Algebraic Function Fields of Positive Characteristic of Higher Transcendence Degree

Theorem

HTP is unsolvable over the following fields.

- *a field $K = k(u, v) \otimes_{\mathbb{Z}/p} F$, where $p > 2$, k is algebraic over $\mathbb{Z}/p$ and has an extension of degree p, u is transcendental over k, v is algebraic over $k(u)$, and $k(u, v)$ and F linearly disjoint over $\mathbb{Z}/p$ (S. 2000);*
- *K as above for $p = 2$ (Eisenträger 2003)*
- *any field K finitely generated over $\mathbb{Z}/p$ (S. 2002)*
- *a field $K = E \otimes_{\mathbb{Z}/p} F$, where E is finitely generated over a field k algebraic over $\mathbb{Z}/p$ and with an extension of degree p, and E and F are linearly disjoint over $\mathbb{Z}/p$ (S. 2003)*
- *an algebraic function field K of finite transcendence degree greater or equal to two over the algebraic closure of a finite field of odd characteristic (Eisenträger, 2012)*

HTP over Algebraic Function Fields of Positive Characteristic of Higher Transcendence Degree

Theorem

HTP is unsolvable over the following fields.

- *a field $K = k(u, v) \otimes_{\mathbb{Z}/p} F$, where $p > 2$, k is algebraic over $\mathbb{Z}/p$ and has an extension of degree p, u is transcendental over k, v is algebraic over $k(u)$, and $k(u, v)$ and F linearly disjoint over $\mathbb{Z}/p$ (S. 2000);*
- *K as above for $p = 2$ (Eisenträger 2003)*
- *any field K finitely generated over $\mathbb{Z}/p$ (S. 2002)*
- *a field $K = E \otimes_{\mathbb{Z}/p} F$, where E is finitely generated over a field k algebraic over $\mathbb{Z}/p$ and with an extension of degree p, and E and F are linearly disjoint over $\mathbb{Z}/p$ (S. 2003)*
- *an algebraic function field K of finite transcendence degree greater or equal to two over the algebraic closure of a finite field of odd characteristic (Eisenträger, 2012)*

HTP over Algebraic Function Fields of Positive Characteristic of Higher Transcendence Degree

Theorem

HTP is unsolvable over the following fields.

- *a field $K = k(u, v) \otimes_{\mathbb{Z}/p} F$, where $p > 2$, k is algebraic over $\mathbb{Z}/p$ and has an extension of degree p, u is transcendental over k, v is algebraic over $k(u)$, and $k(u, v)$ and F linearly disjoint over $\mathbb{Z}/p$ (S. 2000);*
- *K as above for $p = 2$ (Eisenträger 2003)*
- *any field K finitely generated over $\mathbb{Z}/p$ (S. 2002)*
- *a field $K = E \otimes_{\mathbb{Z}/p} F$, where E is finitely generated over a field k algebraic over $\mathbb{Z}/p$ and with an extension of degree p, and E and F are linearly disjoint over $\mathbb{Z}/p$ (S. 2003)*
- *an algebraic function field K of finite transcendence degree greater or equal to two over the algebraic closure of a finite field of odd characteristic (Eisenträger, 2012)*

Outline

Completing the Extension of Kim and Rousch

Theorem (K. Eisentraeger and S, work in progress)

Let K be any function field of positive characteristic not containing the algebraic closure of a finite field. In this case HTP is undecidable over K.

Completing the Proof of the First-Order Undecidability

Theorem (Eisentraeger, S. , work in progress)

If K is any function field of positive characteristic, then the first-order theory of K in the language of rings is undecidable.

The Main Unsolved Question

A Problem

Let C_p be the algebraic closure of $\mathbb{Z}/p$ for some rational prime p. Show that HTP over a function field (or even a rational function field) over C_p is undecidable.

Outline

Function Fields

Definition (Algebraic and Integral Functions)

Algebraic functions are roots of polynomials with coefficients in a field of rational functions, in our case $k(t)$. If γ is an algebraic function, then it is an integral function if it satisfies a *monic* irreducible over $k(t)$ polynomial with coefficients in the polynomial ring $k[t]$.

Example

$\sqrt{t^2+1}$ is a root of a monic irreducible polynomial $X^2-(t^2+1)=0$. Thus, $\sqrt{t^2+1}$ is an integral function. At the same time $\sqrt{\frac{t+1}{t-1}}$ is a root of the polynomial $(t+1)X^2-(t-1)$, which is irreducible over $\mathbb{Z}/p(t)$ and has polynomial coefficients but is not monic. To make $(t+1)X^2-(t-1)$ monic we have to allow rational function coefficients, and therefore $\sqrt{\frac{t+1}{t-1}}$ is not an integral function.

Function Fields

Definition (Algebraic and Integral Functions)

Algebraic functions are roots of polynomials with coefficients in a field of rational functions, in our case $k(t)$. If γ is an algebraic function, then it is an integral function if it satisfies a *monic* irreducible over $k(t)$ polynomial with coefficients in the polynomial ring $k[t]$.

Example

$\sqrt{t^2+1}$ is a root of a monic irreducible polynomial $X^2 - (t^2+1) = 0$. Thus, $\sqrt{t^2+1}$ is an integral function. At the same time $\sqrt{\frac{t+1}{t-1}}$ is a root of the polynomial $(t+1)X^2 - (t-1)$, which is irreducible over $\mathbb{Z}/p(t)$ and has polynomial coefficients but is not monic. To make $(t+1)X^2 - (t-1)$ monic we have to allow rational function coefficients, and therefore $\sqrt{\frac{t+1}{t-1}}$ is not an integral function.

Integral Functions and Primes of Function Fields

Definition

If K is a function field over a field of constants k (and a finite extension of $k(t)$), then the set of all functions integral over $k[t]$ form a ring O_K which we call the ring of integral functions of K. We will also consider the integral closure in K of $k[\frac{1}{t}]$ and denote that ring by $O_{K,\infty}$.

Definition

A prime of a function field K is a prime ideal of O_K or a prime ideal of $O_{K,\infty}$. The prime ideals of $O_{K,\infty}$ are referred to as *infinite primes*. If $\mathfrak{p}$ is a prime coming from a prime ideal of O_K, then $O_K/\mathfrak{p}$ is a finite extension of k and $[O_K/\mathfrak{p} : k]$ is called the degree of the prime. For infinite primes we replace O_K by $O_{K,\infty}$.

Integral Functions and Primes of Function Fields

Definition

If K is a function field over a field of constants k (and a finite extension of $k(t)$), then the set of all functions integral over $k[t]$ form a ring O_K which we call the ring of integral functions of K. We will also consider the integral closure in K of $k[\frac{1}{t}]$ and denote that ring by $O_{K,\infty}$.

Definition

A prime of a function field K is a prime ideal of O_K or a prime ideal of $O_{K,\infty}$. The prime ideals of $O_{K,\infty}$ are referred to as *infinite primes*. If $\mathfrak{p}$ is a prime coming from a prime ideal of O_K, then $O_K/\mathfrak{p}$ is a finite extension of k and $[O_K/\mathfrak{p} : k]$ is called the degree of the prime. For infinite primes we replace O_K by $O_{K,\infty}$.

Order at a Prime over Global Function Fields

Order at a Prime from O_K over a Function Field

If K is a global function field, $x \neq 0$ and $x \in O_K$, then for any prime $\mathfrak{p}$ of K originating in O_K there exists a non-negative integer m such that $x \in \mathfrak{p}^m$ but $x \notin \mathfrak{p}^{m+1}$. We call m the order of x at $\mathfrak{p}$ and write $m = \operatorname{ord}_{\mathfrak{p}} x$. If $y \in K$ and $y \neq 0$, we write $y = \frac{x_1}{x_2}$, where $x_1, x_2 \in O_K$ with $x_1 x_2 \neq 0$, and define $\operatorname{ord}_{\mathfrak{p}} y = \operatorname{ord}_{\mathfrak{p}} x_1 - \operatorname{ord}_{\mathfrak{p}} x_2$. This definition is not dependent on the choice of x_1 and x_2 which are of course not unique. We define $\operatorname{ord}_{\mathfrak{p}} 0 = \infty$ for any prime $\mathfrak{p}$ of O_K.

Order at a Prime from $O_{K,\infty}$ over a Function Field

The order at the primes which are ideals of $O_{K,\infty}$ are defined in the analogous manner with $O_{K,\infty}$ substituting for O_K.

Order at a Prime over Global Function Fields

Order at a Prime from O_K over a Function Field

If K is a global function field, $x \neq 0$ and $x \in O_K$, then for any prime $\mathfrak{p}$ of K originating in O_K there exists a non-negative integer m such that $x \in \mathfrak{p}^m$ but $x \notin \mathfrak{p}^{m+1}$. We call m the order of x at $\mathfrak{p}$ and write $m = \operatorname{ord}_{\mathfrak{p}} x$. If $y \in K$ and $y \neq 0$, we write $y = \frac{x_1}{x_2}$, where $x_1, x_2 \in O_K$ with $x_1 x_2 \neq 0$, and define $\operatorname{ord}_{\mathfrak{p}} y = \operatorname{ord}_{\mathfrak{p}} x_1 - \operatorname{ord}_{\mathfrak{p}} x_2$. This definition is not dependent on the choice of x_1 and x_2 which are of course not unique. We define $\operatorname{ord}_{\mathfrak{p}} 0 = \infty$ for any prime $\mathfrak{p}$ of O_K.

Order at a Prime from $O_{K,\infty}$ over a Function Field

The order at the primes which are ideals of $O_{K,\infty}$ are defined in the analogous manner with $O_{K,\infty}$ substituting for O_K.

Primes of a Rational Function Field

In the case $K = k(t)$ all but one prime correspond to irreducible polynomials in t and the remaining (infinite) prime corresponds to the degree of polynomials. For example, consider $x = \frac{t^2+1}{t-1}$ over k where -1 is not a square. Let $\mathfrak{p}_1$ correspond t^2+1, $\mathfrak{p}_2$ correspond to $t-1$, $\mathfrak{p}_\infty$ correspond to degree. In this case,

$$\text{ord}_{\mathfrak{p}_1} x = 1,$$

$$\text{ord}_{\mathfrak{p}_2} x = -1,$$

$$\text{ord}_{\mathfrak{p}_\infty} x = \text{ord}_{\mathfrak{p}_\infty}(t^2+1) - \text{ord}_{\mathfrak{p}_\infty}(t-1) = -2 - (-1) = -1.$$

Properties of Order

If $x, y \in K$, and $\mathfrak{q}$ is a prime of K, then

$$\operatorname{ord}_{\mathfrak{q}}(xy) = \operatorname{ord}_{\mathfrak{q}}(x) + \operatorname{ord}_{\mathfrak{q}}(y).$$

In particular,

$$\operatorname{ord}_{\mathfrak{q}}(x^r) = r \operatorname{ord}_{\mathfrak{q}}(x).$$

Further, $\operatorname{ord}_{\mathfrak{q}}(x+y) \geq \min(\operatorname{ord}_{\mathfrak{q}} x, \operatorname{ord}_{\mathfrak{q}} y)$ and if $\operatorname{ord}_{\mathfrak{q}} x < \operatorname{ord}_{\mathfrak{q}} y$, then $\operatorname{ord}_{\mathfrak{q}}(x+y) = \operatorname{ord}_{\mathfrak{q}}(x)$

Diophantine Sets or Existentially Definable Sets

Let R be a commutative integral domain. A subset $A \subset R^m$ is called Diophantine over R if there exists a polynomial $p(T_1, \ldots T_m, X_1, \ldots, X_k)$ with coefficients in R such that for any element $(t_1, \ldots, t_m) \in R^m$ we have that

$$\exists x_1, \ldots, x_k \in R : p(t_1, \ldots, t_m, x_1, \ldots, x_k) = 0$$

$$\Updownarrow$$

$$(t_1, \ldots, t_m) \in A.$$

In this case we call $p(T_1, \ldots, T_m, X_1, \ldots, X_k)$ a Diophantine definition of A over R.

Integrality at Finitely Many Primes When the Field of Constants is Finite

Proposition (Robert Rumely, 1980)

If K is a function field over a finite field of constants, $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_m\}$ is a finite collection of primes of K, then the set $\{x \in K : \text{ord}_{\mathfrak{p}_i} x \geq 0, i = 1, \ldots, m\}$ is existentially definable over K.

Outline

p-divisibility

Definition

Let $x, y \in \mathbb{Z}_{\neq 0}$ and let p be a rational prime. In this case we will say that $x\big|_p y$ if $y = xp^s$, where $s \in \mathbb{Z}_{\geq 0}$.

Proposition (Pheidas 1987)

If p is a rational prime, then multiplication is existentially definable in the system $(\mathbb{Z}_{>0}, +, |_p)$.

p-divisibility

Definition

Let $x, y \in \mathbb{Z}_{\neq 0}$ and let p be a rational prime. In this case we will say that $x|_p y$ if $y = xp^s$, where $s \in \mathbb{Z}_{\geq 0}$.

Proposition (Pheidas 1987)

If p is a rational prime, then multiplication is existentially definable in the system $(\mathbb{Z}_{>0}, +, |_p)$.

Simulating Integers with Multiplication

What does this mean?

The exist linear polynomials

$$L_i(T_1, T_2, T_3, X_1, \ldots, X_m),$$

$$M_i(T_1, T_2, T_3, X_1, \ldots, X_m),$$

$$N_i(T_1, T_2, T_3, X_1, \ldots, X_m),$$

with coefficients in $\mathbb{Z}$ and with $i = 1 \ldots, n$ such that for any positive integers a_1, a_2, a_3 the system

$$\begin{cases} L_i(a_1, a_2, a_3, X_1, \ldots, X_m)|_p M_i(a_1, a_2, a_3, X_1, \ldots, X_m), \\ N_i(a_1, a_2, a_3, X_1, \ldots, X_m) = 0, \\ i = 1, \ldots, n \end{cases}$$

has solutions in positive integers if and only if $a_3 = a_2 a_1$.

An Undecidability Consequence

Corollary

There is no algorithm to decide whether an arbitrary system of the form

$$\begin{cases} L_i(X_1,\ldots,X_r)|_p M_i(X_1,\ldots,X_r), \\ N_i(X_1,\ldots,X_r) = 0, \\ i = 1,\ldots,\ell \end{cases}$$

where

$$L_i(X_1,\ldots,X_r),$$

$$M_i X_1,\ldots,X_r),$$

$$N_i(X_1,\ldots,X_r),$$

are linear polynomials with coeffcients in $\mathbb{Z}$*, has solutions in positive integers.*

Conmnecting to Diophantine Undecidability over Function Fields

Proposition

Let K be a countable function field over a field of constants k of positive characteristic p. Let $\mathfrak{q}$ be a prime of K. Suppose the following subsets of K are Diophantine over K:

$$INT = \{x \in K : \mathrm{ord}_{\mathfrak{q}}\, x \geq 0\};$$

$$p(K) = \{(x, y) \in K^2 : y = x^{p^s}, s \in \mathbb{Z}_{\geq 0}\}.$$

Then HTP is unsolvable over K.

Constructing a Model of $(\mathbb{Z}_{\geq 0}, +, |_p)$

Proof.

Send $n \longrightarrow A_n = \{x \in K : \text{ord}_{\mathfrak{q}}\, x = n\}$. Observe the following:

- For any $x \in K$ we have that $\exists n : x \in A_n \Leftrightarrow \text{ord}_{\mathfrak{q}}\, x \geq 0$
- $x, y \in A_n \Leftrightarrow \text{ord}_{\mathfrak{q}} \frac{x}{y} = 0$
- $x \in A_n, y \in A_m, z \in A_{n+m} \Leftrightarrow \text{ord}_{\mathfrak{q}} \frac{xy}{z} = 0$
- $x \in A_n, y \in A_m, n|_p m \Leftrightarrow \exists s \in \mathbb{Z}_{\geq 0}, \exists z \in A_n : y = z^{p^s}$

□

Integrality at a Prime for the Transcendence One Degree Case

Theorem (S. 2000)

If K is a function field of positive characteristic and transcendence degree one not containing the algebraic closure of a finite field, then for any prime $\mathfrak{q}$ of K the set

$$INT = \{x \in K : \operatorname{ord}_{\mathfrak{q}} x \geq 0\}$$

is existentially definable over K.

Integrality at a Prime for the Higher Transcendence Degree Case

Theorem (Eisentraeger, S., work in progress)

If K is a function field of positive characteristic and not containing the algebraic closure of a finite field, then for some prime $\mathfrak{q}$ of K there exists a set $I \subset K$ such that

- *I is Diophantine over K.*
- *If $x \in I$, then $\text{ord}_{\mathfrak{q}}\, x \geq 0$.*
- *If $x \in \mathbb{Z}/p(t)$, and $\text{ord}_{\mathfrak{q}}\, x \geq 0$, then $x \in I$.*

Integrality at a Prime for the Higher Transcendence Degree Case

Theorem (Eisentraeger, S., work in progress)

If K is a function field of positive characteristic and not containing the algebraic closure of a finite field, then for some prime $\mathfrak{q}$ of K there exists a set $I \subset K$ such that

- *I is Diophantine over K.*
- *If $x \in I$, then $\text{ord}_{\mathfrak{q}}\, x \geq 0$.*
- *If $x \in \mathbb{Z}/p(t)$, and $\text{ord}_{\mathfrak{q}}\, x \geq 0$, then $x \in I$.*

Integrality at a Prime for the Higher Transcendence Degree Case

Theorem (Eisentraeger, S., work in progress)

If K is a function field of positive characteristic and not containing the algebraic closure of a finite field, then for some prime $\mathfrak{q}$ of K there exists a set $I \subset K$ such that

- *I is Diophantine over K.*
- *If $x \in I$, then $\operatorname{ord}_{\mathfrak{q}} x \geq 0$.*
- *If $x \in \mathbb{Z}/p(t)$, and $\operatorname{ord}_{\mathfrak{q}} x \geq 0$, then $x \in I$.*

Outline

p-th Powers Are Definable Everywhere

Theorem (The New Result on p-th Powers)

Let K be any function field of positive characteristic p. In this case the set

$$p(K) = \{(x, x^{p^n}) : x \in K, n \in \mathbb{Z}_{\geq 0}\}$$

is definable over K. (Joint work with Kirsten Eisentraeger)

The General Plan

Notation

- Let k be a field of characteristic $p > 0$,
- let t be transcendental over k,
- let K be a finite separable extension of $k(t)$.

The Three Step Program

1. Define p-th powers of t.
2. Define p-th powers of a set of functions with simple zeros and poles.
3. Define p-th powers of arbitrary functions.

The General Plan

Notation

- Let k be a field of characteristic $p > 0$,
- let t be transcendental over k,
- let K be a finite separable extension of $k(t)$.

The Three Step Program

1. Define p-th powers of t.
2. Define p-th powers of a set of functions with simple zeros and poles.
3. Define p-th powers of arbitrary functions.

The General Plan

Notation

- Let k be a field of characteristic $p > 0$,
- let t be transcendental over k,
- let K be a finite separable extension of $k(t)$.

The Three Step Program

1. Define p-th powers of t.
2. Define p-th powers of a set of functions with simple zeros and poles.
3. Define p-th powers of arbitrary functions.

The General Plan

Notation

- Let k be a field of characteristic $p > 0$,
- let t be transcendental over k,
- let K be a finite separable extension of $k(t)$.

The Three Step Program

1. Define p-th powers of t.
2. Define p-th powers of a set of functions with simple zeros and poles.
3. Define p-th powers of arbitrary functions.

The General Plan

Notation

- Let k be a field of characteristic $p > 0$,
- let t be transcendental over k,
- let K be a finite separable extension of $k(t)$.

The Three Step Program

1. Define p-th powers of t.
2. Define p-th powers of a set of functions with simple zeros and poles.
3. Define p-th powers of arbitrary functions.

The General Plan

Notation

- Let k be a field of characteristic $p > 0$,
- let t be transcendental over k,
- let K be a finite separable extension of $k(t)$.

The Three Step Program

1. Define p-th powers of t.
2. Define p-th powers of a set of functions with simple zeros and poles.
3. Define p-th powers of arbitrary functions.

p-th Powers of t over Rational Function Field of Characteristic Greater Than 2

Lemma (Pheidas)

Let k be a finite field of characteristic $p > 2$. Let t be transcendental over k. Then the equations below are satisfied with $u, v, w \in k(t)$ if and only if for some $s \in \mathbb{Z}_{\geq 0}$ we have that $w = t^{p^s}$.

$$\begin{cases} w - t = v^p - v \\ \frac{1}{w} - \frac{1}{t} = u^p - u \end{cases} \tag{1}$$

Satisfiability is easy

For any $x \in K$ and any $s \in \mathbb{Z}_{\geq 0}$

$$x^{p^s} - x = (x^{p^{(s-1)}} + x^{p^{(s-2)}} + \ldots + x)^p - (x^{p^{(s-1)}} + x^{p^{(s-2)}} + \ldots + x) \tag{2}$$

p-th Powers of t over Rational Function Field of Characteristic Greater Than 2

Lemma (Pheidas)

Let k be a finite field of characteristic $p > 2$. Let t be transcendental over k. Then the equations below are satisfied with $u, v, w \in k(t)$ if and only if for some $s \in \mathbb{Z}_{\geq 0}$ we have that $w = t^{p^s}$.

$$\begin{cases} w - t = v^p - v \\ \frac{1}{w} - \frac{1}{t} = u^p - u \end{cases} \tag{1}$$

Satisfiability is easy

For any $x \in K$ and any $s \in \mathbb{Z}_{\geq 0}$

$$x^{p^s} - x = (x^{p^{(s-1)}} + x^{p^{(s-2)}} + \ldots + x)^p - (x^{p^{(s-1)}} + x^{p^{(s-2)}} + \ldots + x) \tag{2}$$

Conctructing p-th powers of t

We proceed in two steps. First we show that if w satisfies equations below, then it is equal to t or it is a p-th power.

$$\begin{cases} w - t = v^p - v \\ \frac{1}{w} - \frac{1}{t} = u^p - u \end{cases} \tag{3}$$

Second, we show that if $w = w_1^p$ we can rewrite the equations above:

$$\begin{cases} w_1 - t = (v^p - w_1^p) + (w_1 - v) = v_1^p - v_1 \\ \frac{1}{w_1} - \frac{1}{t} = u^p - \frac{1}{w_1^p} + \frac{1}{w_1} - u = u_1^p - u_1 \end{cases} \tag{4}$$

Conctructing p-th powers of t

We proceed in two steps. First we show that if w satisfies equations below, then it is equal to t or it is a p-th power.

$$\begin{cases} w - t = v^p - v \\ \frac{1}{w} - \frac{1}{t} = u^p - u \end{cases} \tag{3}$$

Second, we show that if $w = w_1^p$ we can rewrite the equations above:

$$\begin{cases} w_1 - t = (v^p - w_1^p) + (w_1 - v) = v_1^p - v_1 \\ \frac{1}{w_1} - \frac{1}{t} = u^p - \frac{1}{w_1^p} + \frac{1}{w_1} - u = u_1^p - u_1 \end{cases} \tag{4}$$

Conctructing p-th powers of t

We proceed in two steps. First we show that if w satisfies equations below, then it is equal to t or it is a p-th power.

$$\begin{cases} w - t = v^p - v \\ \frac{1}{w} - \frac{1}{t} = u^p - u \end{cases} \tag{3}$$

Second, we show that if $w = w_1^p$ we can rewrite the equations above:

$$\begin{cases} w_1 - t = (v^p - w_1^p) + (w_1 - v) = v_1^p - v_1 \\ \frac{1}{w_1} - \frac{1}{t} = u^p - \frac{1}{w_1^p} + \frac{1}{w_1} - u = u_1^p - u_1 \end{cases} \tag{4}$$

The Denominators of $v^p - v$ and $w - t$ in a rational field.

Suppose $v = \frac{A}{z_2}$, where A, z_2 are relatively prime polynomials. In this case $v^p - v = \frac{A^p}{z_2^p} - \frac{A}{z_2^p} = \frac{A^p - Az_2^{p-1}}{z_2^p}$. Observe that $(A^p - Az_2^{p-1}, z_2^p) = 1$ as polynomials over k. Indeed, if P is a prime polynomial dividing z_2^p, then P divides z_2 and P is prime to A, and therefore to $A^p - Az_2^{p-1}$. Thus z_2^p is the reduced denominator of $v^p - v$.

We now have $w - t = v^p - v = \frac{a}{z_2^p}$, where z_2, a are relatively prime polynomials. Since t does not have a denominator, we conclude that $w = \frac{Z_1}{z_2^p}$, where z_2, Z_1 are relatively prime polynomials.

The Denominators of $v^p - v$ and $w - t$ in a rational field.

Suppose $v = \frac{A}{z_2}$, where A, z_2 are relatively prime polynomials. In this case $v^p - v = \frac{A^p}{z_2^p} - \frac{A}{z_2^p} = \frac{A^p - Az_2^{p-1}}{z_2^p}$. Observe that $(A^p - Az_2^{p-1}, z_2^p) = 1$ as polynomials over k. Indeed, if P is a prime polynomial dividing z_2^p, then P divides z_2 and P is prime to A, and therefore to $A^p - Az_2^{p-1}$. Thus z_2^p is the reduced denominator of $v^p - v$.

We now have $w - t = v^p - v = \frac{a}{z_2^p}$, where z_2, a are relatively prime polynomials. Since t does not have a denominator, we conclude that $w = \frac{Z_1}{z_2^p}$, where z_2, Z_1 are relatively prime polynomials.

The Denominators of $v^p - v$ and $w - t$ in a rational field.

Suppose $v = \frac{A}{z_2}$, where A, z_2 are relatively prime polynomials. In this case $v^p - v = \frac{A^p}{z_2^p} - \frac{A}{z_2^p} = \frac{A^p - Az_2^{p-1}}{z_2^p}$. Observe that $(A^p - Az_2^{p-1}, z_2^p) = 1$ as polynomials over k. Indeed, if P is a prime polynomial dividing z_2^p, then P divides z_2 and P is prime to A, and therefore to $A^p - Az_2^{p-1}$. Thus z_2^p is the reduced denominator of $v^p - v$.
We now have $w - t = v^p - v = \frac{a}{z_2^p}$, where z_2, a are relatively prime polynomials. Since t does not have a denominator, we conclude that $w = \frac{Z_1}{z_2^p}$, where z_2, Z_1 are relatively prime polynomials.

The numerator of w.

We now consider the second equation $\frac{1}{w} - \frac{1}{t} = u^p - u$ and by a similar argument conclude that $\frac{1}{w} - \frac{1}{t} = \frac{b}{z_1^p}$. Thus,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{tz_2^p - Z_1}{tZ_1} = \frac{b}{z_1^p}.$$

If $(t, Z_1) = 1$ then tZ_1 is the reduced denominator and $tZ_1 = z_1^p$, leading to a contradiction.

So let $Z_1 = t^k \tilde{Z}_1, k \in \mathbb{Z}_{>0}, (\tilde{Z}_1, t) = 1$. In this case,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{z_2^p - t^{k-1}\tilde{Z}_1}{Z_1} = \frac{b}{z_1^p}.$$

If $k > 1$, then $(z_2^p, t^{k-1}\tilde{Z}_1) = 1$ and Z_1 is the reduced denominator forced to be equal to z_1^p. If $k = 1$, then the numerator is equal to $z_2^p - \tilde{Z}_1$ and may be divisible by t, so that $\frac{Z_1}{t} = z_1^p$. In other words, either $w = t\frac{z_1^p}{z_2^p}$ or $w = \frac{z_1^p}{z_2^p}$. In the last case w is a p-th power.

The numerator of w.

We now consider the second equation $\frac{1}{w} - \frac{1}{t} = u^p - u$ and by a similar argument conclude that $\frac{1}{w} - \frac{1}{t} = \frac{b}{z_1^p}$. Thus,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{tz_2^p - Z_1}{tZ_1} = \frac{b}{z_1^p}.$$

If $(t, Z_1) = 1$ then tZ_1 is the reduced denominator and $tZ_1 = z_1^p$, leading to a contradiction.
So let $Z_1 = t^k \tilde{Z}_1, k \in \mathbb{Z}_{>0}, (\tilde{Z}_1, t) = 1$. In this case,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{z_2^p - t^{k-1}\tilde{Z}_1}{Z_1} = \frac{b}{z_1^p}.$$

If $k > 1$, then $(z_2^p, t^{k-1}\tilde{Z}_1) = 1$ and Z_1 is the reduced denominator forced to be equal to z_1^p. If $k = 1$, then the numerator is equal to $z_2^p - \tilde{Z}_1$ and may be divisible by t, so that $\frac{Z_1}{t} = z_1^p$. In other words, either $w = t\frac{z_1^p}{z_2^p}$ or $w = \frac{z_1^p}{z_2^p}$. In the last case w is a p-th power.

The numerator of w.

We now consider the second equation $\frac{1}{w} - \frac{1}{t} = u^p - u$ and by a similar argument conclude that $\frac{1}{w} - \frac{1}{t} = \frac{b}{z_1^p}$. Thus,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{tz_2^p - Z_1}{tZ_1} = \frac{b}{z_1^p}.$$

If $(t, Z_1) = 1$ then tZ_1 is the reduced denominator and $tZ_1 = z_1^p$, leading to a contradiction.

So let $Z_1 = t^k \tilde{Z}_1, k \in \mathbb{Z}_{>0}, (\tilde{Z}_1, t) = 1$. In this case,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{z_2^p - t^{k-1}\tilde{Z}_1}{Z_1} = \frac{b}{z_1^p}.$$

If $k > 1$, then $(z_2^p, t^{k-1}\tilde{Z}_1) = 1$ and Z_1 is the reduced denominator forced to be equal to z_1^p. If $k = 1$, then the numerator is equal to $z_2^p - \tilde{Z}_1$ and may be divisible by t, so that $\frac{Z_1}{t} = z_1^p$. In other words, either $w = t\frac{z_1^p}{z_2^p}$ or $w = \frac{z_1^p}{z_2^p}$. In the last case w is a p-th power.

The numerator of w.

We now consider the second equation $\frac{1}{w} - \frac{1}{t} = u^p - u$ and by a similar argument conclude that $\frac{1}{w} - \frac{1}{t} = \frac{b}{z_1^p}$. Thus,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{tz_2^p - Z_1}{tZ_1} = \frac{b}{z_1^p}.$$

If $(t, Z_1) = 1$ then tZ_1 is the reduced denominator and $tZ_1 = z_1^p$, leading to a contradiction.
So let $Z_1 = t^k \tilde{Z}_1, k \in \mathbb{Z}_{>0}, (\tilde{Z}_1, t) = 1$. In this case,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{z_2^p - t^{k-1}\tilde{Z}_1}{Z_1} = \frac{b}{z_1^p}.$$

If $k > 1$, then $(z_2^p, t^{k-1}\tilde{Z}_1) = 1$ and Z_1 is the reduced denominator forced to be equal to z_1^p. If $k = 1$, then the numerator is equal to $z_2^p - \tilde{Z}_1$ and may be divisible by t, so that $\frac{Z_1}{t} = z_1^p$. In other words, either $w = t\frac{z_1^p}{z_2^p}$ or $w = \frac{z_1^p}{z_2^p}$. In the last case w is a p-th power.

The numerator of w.

We now consider the second equation $\frac{1}{w} - \frac{1}{t} = u^p - u$ and by a similar argument conclude that $\frac{1}{w} - \frac{1}{t} = \frac{b}{z_1^p}$. Thus,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{tz_2^p - Z_1}{tZ_1} = \frac{b}{z_1^p}.$$

If $(t, Z_1) = 1$ then tZ_1 is the reduced denominator and $tZ_1 = z_1^p$, leading to a contradiction.
So let $Z_1 = t^k \tilde{Z}_1, k \in \mathbb{Z}_{>0}, (\tilde{Z}_1, t) = 1$. In this case,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{z_2^p - t^{k-1}\tilde{Z}_1}{Z_1} = \frac{b}{z_1^p}.$$

If $k > 1$, then $(z_2^p, t^{k-1}\tilde{Z}_1) = 1$ and Z_1 is the reduced denominator forced to be equal to z_1^p. If $k = 1$, then the numerator is equal to $z_2^p - \tilde{Z}_1$ and may be divisible by t, so that $\frac{Z_1}{t} = z_1^p$. In other words, either $w = t\frac{z_1^p}{z_2^p}$ or $w = \frac{z_1^p}{z_2^p}$. In the last case w is a p-th power.

The numerator of w.

We now consider the second equation $\frac{1}{w} - \frac{1}{t} = u^p - u$ and by a similar argument conclude that $\frac{1}{w} - \frac{1}{t} = \frac{b}{z_1^p}$. Thus,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{tz_2^p - Z_1}{tZ_1} = \frac{b}{z_1^p}.$$

If $(t, Z_1) = 1$ then tZ_1 is the reduced denominator and $tZ_1 = z_1^p$, leading to a contradiction.
So let $Z_1 = t^k \tilde{Z}_1, k \in \mathbb{Z}_{>0}, (\tilde{Z}_1, t) = 1$. In this case,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{z_2^p - t^{k-1}\tilde{Z}_1}{Z_1} = \frac{b}{z_1^p}.$$

If $k > 1$, then $(z_2^p, t^{k-1}\tilde{Z}_1) = 1$ and Z_1 is the reduced denominator forced to be equal to z_1^p. If $k = 1$, then the numerator is equal to $z_2^p - \tilde{Z}_1$ and may be divisible by t, so that $\frac{Z_1}{t} = z_1^p$. In other words, either $w = t\frac{z_1^p}{z_2^p}$ or $w = \frac{z_1^p}{z_2^p}$. In the last case w is a p-th power.

The numerator of w.

We now consider the second equation $\frac{1}{w} - \frac{1}{t} = u^p - u$ and by a similar argument conclude that $\frac{1}{w} - \frac{1}{t} = \frac{b}{z_1^p}$. Thus,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{tz_2^p - Z_1}{tZ_1} = \frac{b}{z_1^p}.$$

If $(t, Z_1) = 1$ then tZ_1 is the reduced denominator and $tZ_1 = z_1^p$, leading to a contradiction.

So let $Z_1 = t^k \tilde{Z}_1, k \in \mathbb{Z}_{>0}, (\tilde{Z}_1, t) = 1$. In this case,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{z_2^p - t^{k-1}\tilde{Z}_1}{Z_1} = \frac{b}{z_1^p}.$$

If $k > 1$, then $(z_2^p, t^{k-1}\tilde{Z}_1) = 1$ and Z_1 is the reduced denominator forced to be equal to z_1^p. If $k = 1$, then the numerator is equal to $z_2^p - \tilde{Z}_1$ and may be divisible by t, so that $\frac{Z_1}{t} = z_1^p$. In other words, either $w = t\frac{z_1^p}{z_2^p}$ or $w = \frac{z_1^p}{z_2^p}$. In the last case w is a p-th power.

The numerator of w.

We now consider the second equation $\frac{1}{w} - \frac{1}{t} = u^p - u$ and by a similar argument conclude that $\frac{1}{w} - \frac{1}{t} = \frac{b}{z_1^p}$. Thus,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{tz_2^p - Z_1}{tZ_1} = \frac{b}{z_1^p}.$$

If $(t, Z_1) = 1$ then tZ_1 is the reduced denominator and $tZ_1 = z_1^p$, leading to a contradiction.
So let $Z_1 = t^k \tilde{Z}_1, k \in \mathbb{Z}_{>0}, (\tilde{Z}_1, t) = 1$. In this case,

$$\frac{z_2^p}{Z_1} - \frac{1}{t} = \frac{z_2^p - t^{k-1}\tilde{Z}_1}{Z_1} = \frac{b}{z_1^p}.$$

If $k > 1$, then $(z_2^p, t^{k-1}\tilde{Z}_1) = 1$ and Z_1 is the reduced denominator forced to be equal to z_1^p. If $k = 1$, then the numerator is equal to $z_2^p - \tilde{Z}_1$ and may be divisible by t, so that $\frac{Z_1}{t} = z_1^p$. In other words, either $w = t\frac{z_1^p}{z_2^p}$ or $w = \frac{z_1^p}{z_2^p}$. In the last case w is a p-th power.

Why is w a p-th power in any case?

If w is not a p-th power, then $w = t\frac{z_1^p}{z_2^p}$, where z_1, z_2 are relatively prime polynomials and it satisfies an equation
$w - t = v^p - v = \frac{A}{z_2^p} - \frac{A}{z_2}$. Thus, $z_2 v$ is also a polynomial in t.
Now we rewrite the equation in the following form:

$$tz_1^p - z_2^p t = (z_2 v)^p - (z_2 v)z_2^{p-1}$$

$$tz_1^p - (z_2 v)^p = z_2^p t - (z_2 v)z_2^{p-1}$$

Looking at the right side observe that that any prime polynomial dividing z_2 occurs to the power at least 2 on the right. So if we differentiate the left side with respect to t we should get a polynomial which has all the zeros of z_2. However the derivative of the left side is z_1^p leading us to the conclusion that z_2 is a constant.

Why is w a p-th power in any case?

If w is not a p-th power, then $w = t\frac{z_1^p}{z_2^p}$, where z_1, z_2 are relatively prime polynomials and it satisfies an equation $w - t = v^p - v = \frac{A}{z_2^p} - \frac{A}{z_2}$. Thus, $z_2 v$ is also a polynomial in t. Now we rewrite the equation in the following form:

$$tz_1^p - z_2^p t = (z_2 v)^p - (z_2 v) z_2^{p-1}$$

$$tz_1^p - (z_2 v)^p = z_2^p t - (z_2 v) z_2^{p-1}$$

Looking at the right side observe that that any prime polynomial dividing z_2 occurs to the power at least 2 on the right. So if we differentiate the left side with respect to t we should get a polynomial which has all the zeros of z_2. However the derivative of the left side is z_1^p leading us to the conclusion that z_2 is a constant.

Why is w a p-th power in any case?

If w is not a p-th power, then $w = t\frac{z_1^p}{z_2^p}$, where z_1, z_2 are relatively prime polynomials and it satisfies an equation
$w - t = v^p - v = \frac{A}{z_2^p} - \frac{A}{z_2}$. Thus, $z_2 v$ is also a polynomial in t.
Now we rewrite the equation in the following form:

$$tz_1^p - z_2^p t = (z_2 v)^p - (z_2 v) z_2^{p-1}$$

$$tz_1^p - (z_2 v)^p = z_2^p t - (z_2 v) z_2^{p-1}$$

Looking at the right side observe that that any prime polynomial dividing z_2 occurs to the power at least 2 on the right. So if we differentiate the left side with respect to t we should get a polynomial which has all the zeros of z_2. However the derivative of the left side is z_1^p leading us to the conclusion that z_2 is a constant.

Divisors, and Height

Definition

If K is a function field, then a divisor is a formal product $\prod_{\mathfrak{p}} \mathfrak{p}^{a(\mathfrak{p})}$, where the product is taken over all the primes of K, $a(\mathfrak{p}) \in \mathbb{Z}$ and all but finitely many exponents are zero. If $x \in K$, then the divisor of x is

$$(x) = \prod_{\mathfrak{p}} \mathfrak{p}^{\operatorname{ord}_{\mathfrak{p}} x}$$

The height of x is

$$\sum_{\mathfrak{p}, \operatorname{ord}_{\mathfrak{p}} x > 0} \deg(\mathfrak{p}) \operatorname{ord}_{\mathfrak{p}} x = - \sum_{\mathfrak{p}, \operatorname{ord}_{\mathfrak{p}} x < 0} \deg(\mathfrak{p}) \operatorname{ord}_{\mathfrak{p}} x.$$

Principal Divisors and Class Number

Definition

A divisor is principal if it is a divisor of a field element. A class number (if it is exists) can be defined as the size of the group of divisors with the same degree of "zeros" and "poles" modulo the group of principal divisors. Any divisor with the same degree of "zeros" and "poles" raised to the class number becomes principal.

Remarks on the General Case

The preceding argument works for a rational function field over any field of constants of characteristic greater than 2, but it relies on the following facts:

- the class number of a rational field is one;
- t has a divisor of the form $\frac{p}{q}$ (i.e one pole and one zero, both of degree 1);
- the positive order at a prime goes down by at most one under differentiation.

To overcome these difficulties we usually have to establish that the divisor not just of w is a p-th power of another divisor but also that the divisors of $w + a$ for sufficiently many constants a are p-th powers of other divisors. We also need to use a consequence of Riemann-Roch theorem to show that if w does not have a divisor which is a p-th power of another divisor, then it can be of bounded height only with the bound depending on the genus of the field. If the height of w is bounded, then we can "push" it into the rational subfield where things proceed essentially as above.

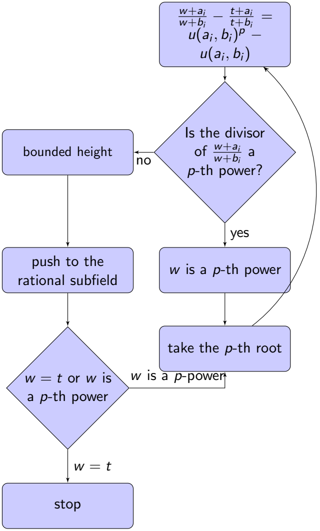
Remarks on the General Case

The preceding argument works for a rational function field over any field of constants of characteristic greater than 2, but it relies on the following facts:

- the class number of a rational field is one;
- t has a divisor of the form $\frac{p}{q}$ (i.e one pole and one zero, both of degree 1);
- the positive order at a prime goes down by at most one under differentiation.

To overcome these difficulties we usually have to establish that the divisor not just of w is a p-th power of another divisor but also that the divisors of $w + a$ for sufficiently many constants a are p-th powers of other divisors. We also need to use a consequence of Riemann-Roch theorem to show that if w does not have a divisor which is a p-th power of another divisor, then it can be of bounded height only with the bound depending on the genus of the field. If the height of w is bounded, then we can "push" it into the rational subfield where things proceed essentially as above.

Flowchart


$\frac{w+a_i}{w+b_i} - \frac{t+a_i}{t+b_i} = u(a_i, b_i)^p - u(a_i, b_i)$
Is the divisor of $\frac{w+a_i}{w+b_i}$ a p-th power?
no
bounded height
yes
push to the rational subfield
w is a p-th power
take the p-th root
$w = t$ or w is a p-th power
w is a p-power
$w = t$
stop