The elementary theory of all pseudofinite fields

Modelltheorie pseudoendlicher Strukturen

21st April 2021 - Simone Ramello

Outline

1. Pseudofinite fields ← bottom-up perspective
2. Bounds on ideals in polynomial rings
3. The theory *Psf*
4. Examples of pseudofinite fields
5. A lemma for next time

Slogan: pseudofinite fields are the asymptotic version of finite fields (this will be more precise in talk #4).

I. Pseudofinite fields

A pseudofinite field is a field k such that

1. k is perfect ($\mathrm{char}\, k = 0$ or $\mathrm{char}\, k = p > 0 \wedge \forall x \exists y\, (x = y^p)$)
2. $\mathrm{Gal}(k^{alg}/k) \cong \hat{\mathbb{Z}}$ ($\Leftrightarrow$ k perfect and k has exactly one separable extension of degree n $\forall n$)
3. every absolutely irreducible variety defined over k has a k-rational point.

$k \subseteq \Omega$, $X = V(f_1, \dots f_m) \subseteq \Omega^n$, $f_1, \dots f_m \in k[x_1, \dots x_n]$

ABS. IRR. $(f_1, \dots f_m) \subseteq \Omega[x_1, \dots x_n]$ is prime

If $X_1, \dots X_n$ are variables and $I = (i_1, \dots i_n) \in \mathbb{N}^n$, then

$$X^I = X_1^{i_1} \cdots X_n^{i_n}, \qquad |I| = i_1 + \dots + i_n.$$

If $f(X) \in k[X]$, $f = \sum_I a_I X^I$, then $\deg(f) = \sup_I |I|$.

Call $k[X]_{\leq d} = \{ f \in k[X] \mid \deg f \leq d \}$, $d > 0$ integer.

* $\forall d$, $k[X]_{\leq d}$ definable in k using $N(d) := \dim_k k[X]_{\leq d}$ variables; let $[f] \in k^{N(d)}$ associated to $f \in k[X]_{\leq d}$,
* multiplication $k[X]_{\leq d} \times k[X]_{\leq d} \longrightarrow k[X]_{\leq 2d}$ is also definable in k.

II. Bounds on ideals in polynomial rings

THEOREM (BLACKBOX)

for any $n, d > 0$ integers, there exist constants

$$A = A(n,d) \qquad D = D(n,d)$$

such that for all fields k and polynomials $f_1 \dots f_m, g \in k[x]_{\leq d}$,

* if $g \in (f_1, \dots f_m)$, there are $h_1, \dots h_m \in k[x]_{\leq A}$ such that

$$g = h_1 f_1 + \dots + h_m f_m,$$

* if $(f_1, \dots f_m) \subseteq k[x]$ is not prime, then there are $h_1, h_2 \in k[x]_{\leq D}$ such that $h_1 h_2 \in (f_1, \dots f_m)$ but $h_1, h_2 \notin (f_1, \dots f_m)$.

III. The theory *Psf*

GOAL: the class of pseudofinite fields is an elementary class.

1. k is perfect $\rightsquigarrow$ $\varphi_p = (\underbrace{1+\cdots+1}_{p\text{-times}} = 0 \rightarrow \forall x \exists y\ (x = y^p))$

3. every absolutely irreducible variety defined over k has a k-rational point.

PAC

$\rightsquigarrow$ ψ_m such that $k \models \psi_m([f_1], \cdots [f_m])$ if and only if $(f_1, \ldots f_m) \subseteq \mathbb{Z}[X]$ is prime

Step 1: $f_1, \dots f_m \in k[X]_{\le d}$, then

$I = (f_1, \dots f_m) \subseteq k[X]$ is prime iff for all $g, h \in k[X]_{\le D}$

either $gh \notin I$ or one of $g, h \in I$

iff for all $g, h \in k[X]_{\le D}$,

either for all $h_1, \dots h_m \in k[X]_{\le A}$, $gh \neq h_1 f_1 + \dots + h_m f_m$, or there exist $h_1, \dots h_m \in k[X]_{\le A}$ such that $g = h_1 f_1 + \dots + h_m f_m$ or $h = h_1 f_1 + \dots + h_m f_m$.

first-order property of $[f_1] \dots [f_m]$

$\varphi_{m,d}(y)$, $|y| = m \cdot N(d)$

Step 2: by quantifier elimination of the theory of algebraically closed fields, there is a quantifier free formula $\Psi_m(y)$ such that

$$\Omega \models \varphi_m([f_1], \dots [f_m]) \quad \text{iff} \quad \Omega \models \Psi_m([f_1], \dots [f_m])$$

$$\text{iff} \quad k \models \Psi_m([f_1], \dots [f_m]).$$

So $k \models \Psi_{m,d}([f_1], \dots [f_m])$ iff $(f_1, \dots f_m) \subseteq \Omega[X]$ is a prime ideal

iff $V(f_1, \dots f_m)$ is abs. irreducible.

WRAP-UP:

$m \cdot N(d)$ quantifiers

$$\theta_{n,d} = \forall m \, \forall [f_1] \cdots \forall [f_m] \left(\Psi_{m,d}([f_1], \ldots [f_m]) \rightarrow \exists z_1 \ldots z_n \left(\bigwedge_{i=1}^{m} f_i(z_1 \ldots z_n) = 0 \right) \right).$$

$m \leq N(d)$, hence

$$\bigwedge_{j=1}^{N(d)} \forall [f_1] \cdots [f_j] \left(\Psi_{j,d}(\ldots \right.$$

2. $\mathrm{Gal}(k^{alg}/k) \cong \hat{\mathbb{Z}}$

$\hat{\mathbb{Z}} := \varprojlim_{m \mid n} \mathbb{Z}/n\mathbb{Z} \quad \{\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}\}$

$= \{(a_n)_{n \geq 2} \in \prod_{n \geq 2} \mathbb{Z}/n\mathbb{Z} \mid \text{if } m \mid n, \; a_m \equiv a_n \bmod m\}$

* (k perfect)

$\mathrm{Gal}(k^{alg}/k) \cong \hat{\mathbb{Z}}$ iff k has exactly one extension of degree n for all $n \in \mathbb{N}$.

(A) k has at least one extension of degree n

(B) k has at most one extension of degree n

(A) "at least"

$\rho_n(y)$, $|y| = n$, saying "$x^n + y_1 x^{n-1} + \ldots + y_n$ is irreducible"

$$\forall u_1, \ldots u_n \bigwedge_{i=1}^{n} \Big[(x^{n-i} + u_1 x^{n-i-1} + \ldots + u_{n-i})(x^i + u_{n-i+1} x^{i-1} + \ldots + u_n) \neq x^n + y_1 x^{n-1} + \ldots + y_n \Big]$$

$$\rightsquigarrow \quad \xi_n = \exists y_1 \ldots y_n \, \rho_n(y_1 \ldots y_n)$$

(B) AT MOST

We want to say that if $\rho_n(y)$ and $\rho_n(7)$ hold, then if $\alpha^n + y_1\alpha^{n-1} + \ldots + y_n = 0$,

$k(\alpha)$ contains all roots of $x^n + 7_1 x^{n-1} + \ldots + 7_n$.

We do that by defining $(k(\alpha), +, \times, 0, 1, k)$ in k.

Let: $M = k^n$, $P_k = \{(\lambda, 0, \ldots 0) \mid \lambda \in k\}$,

$0^* = (0, \ldots 0)$, $1^* = (1, 0, \ldots 0)$

$+^*$ is just pointwise sum

Fix a basis of $k(\alpha)$, $\{1, \alpha, \alpha^2, \ldots \alpha^{n-1}\}$.

Then for this basis, multiplication by α is a linear transformation with associated matrix

$$M_\alpha := \begin{bmatrix} 0 & 0 & \cdots & 0 & -y_n \\ 1 & 0 & & 0 & -y_{n-1} \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -y_1 \end{bmatrix}.$$

$$\alpha^n = -\sum_{i=1}^{n} y_i \alpha^{n-i}$$

Similarly, multiplication by α^j has matrix M_α^j.

$$(u_1, \dots u_n) \, x^* \, (v_1, \dots v_n) = (u_1 I_n + u_2 M_\alpha + \dots + u_n M_\alpha^{n-1}) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}.$$

* this definition is uniform.

Since $(k(\alpha), +, \times, 1, 0, P_k)$ is definable in k, there is a formula $\theta(y)$ such that, if $x^n + y_1 x^{n-1} + \ldots + y_{n-1}x + y_n$ is irreducible and α is a root, then

$$k \models \theta(y) \text{ iff } k(\alpha) \models \forall z_1, \ldots z_n \left(\rho_n(z_1, \ldots z_n) \wedge P_k(z_1) \wedge \ldots \wedge P_k(z_n) \rightarrow \exists u_1, \ldots u_n \left(x^n + z_1 x^{n-1} + \ldots + z_n = (x-u_1)\ldots(x-u_n)\right)\right)$$

$\rightsquigarrow$ η_n such that

$k \models \eta_n$ iff k has at most one extension of deg. n.

Axiomatization

$\forall p$, φ_p $\rightsquigarrow$ $\underbrace{1+1+1+\cdots+1}_{p\text{-times}} = 0 \rightarrow \forall x \exists y \ (x = y^p)$

$\forall n$, $\xi_n \wedge \eta_n$ $\rightsquigarrow$ k has at most & at least one extension of degree n.

$\forall n, d$, $\theta_{n,d}$ $\rightsquigarrow$ for every choice of polynomials of degree at most d in n variables, if the ideal they generate in $\Omega[X]$ is prime, they have a common root.

Psf

IV. Examples of pseudofinite fields

1. ultraproducts of finite fields

LANG-WEIL BOUND

for integers $n, d > 0$ there is a constant $C(n,d) > 0$ such that for all finite fields $\mathbb{F}_q$ and varieties X defined by polynomials in $\mathbb{F}_q[x_1, \dots x_n] \leq d$, ($X$ absolutely irreducible)

$$|\#X(\mathbb{F}_q) - q^{\dim X}| \leq C \cdot q^{\dim X - \frac{1}{2}}.$$

2. infinite algebraic extensions of finite fields with the "right" Galois group

In particular, if $q > C^2$, then

$$\#\overline{X}(\mathbb{F}_q) \geq q^{\dim \overline{X}} - Cq^{\dim \overline{X} - 1/2} > 0.$$

TAKE-AWAY: $\forall n,d$ For q big enough, $\mathbb{F}_q \models \theta_{n,d}$.

Consequence: if Q is the set of prime powers and $\mathcal{U}$ is an ultrafilter on Q, then $\prod_{q \in Q} \mathbb{F}_q / \mathcal{U}$ is pseudo-finite.

non-principal

Consequence: if Q is the set of prime powers and $\mathcal{U}$ is an ultrafilter on Q, then $\prod_{q \in Q} \mathbb{F}_q / \mathcal{U}$ is pseudo-finite.

1. every $\mathbb{F}_q$ is perfect $\rightsquigarrow$ this holds in the ultraproduct
2. $\xi_n \wedge \eta_n$ hold in every $\mathbb{F}_q$ $\rightsquigarrow$ they hold in the ultraproduct
3. $\forall n,d$ there is $q \gg 0$ such that $\mathbb{F}_q \models \theta_{n,d}$ $\rightsquigarrow$ the $\theta_{n,d}$ hold in the ultra-product

Consequence #2: Say k is quasi-finite if it is perfect and its Galois group is $\hat{\mathbb{Z}}$. Denote by k_n its unique extension of degree n.

A Steinitz number is a formal product

$$S = \prod_{p \text{ prime}} p^{s(p)}, \quad s(p) \in \mathbb{N} \cup \{\infty\}.$$

- $\mathbb{N} \subseteq \{\text{Steinitz numbers}\} =: S$.

There is a bijection

$$\{\text{algebraic extensions of } k\} \longrightarrow S$$
$$k' \longmapsto s,$$
$$s(p) = \sup\{m \in \mathbb{N} \mid k_{p^m} \subseteq k'\}.$$

If $k = \mathbb{F}_q$, the inverse is

$$s \longmapsto k_s = \bigcup_{n \in \mathbb{N},\, n \mid s} \mathbb{F}_{q^n},$$

where $s \mid s'$ iff $\forall p$ primes, $s(p) \leq s'(p)$.

Fact: k_S is quasi-finite iff $S(p) \neq \infty$ $\forall p$.

Consequence #2: if $k = \mathbb{F}_q$ and $s \in S$ is such that $s(p) \neq \infty$ $\forall p$ and $s(0) \neq 0$ for infinitely many p, then k_S is pseudofinite.

If $\overline{X}$ is defined over k_S, then there is an $m >> 0$ such that $\overline{X}$ is defined over $\mathbb{F}_{q^m}$ and, by Lang-Weil, $\overline{X}(\mathbb{F}_{q^m}) \neq \emptyset$. Hence, $\overline{X}(k_S) \neq \emptyset$.

V. A lemma for next time

Suppose k is perfect PAC,

1. if a is a tuple from $k' \supseteq k$ and $k(a)$ is regular over k, then there is a k-morphism
$$k[a] \longrightarrow k,$$

2. if k is $\aleph_1$-saturated and $A \subseteq k'$ is countable for some $k' \supseteq k$ such that $k(A)/k$ is regular, then there is a k-morphism $k[A] \longrightarrow k$.

1. Consider $I(a/k) = \{ f \in k[X] \mid f(a) = 0 \}$ and, since $k(a) \simeq \frac{k[X]}{I(a/k)}$ is regular, then

$$\overline{X} = V(I(a/k))$$ is a variety

hence there is $b \in \overline{X}(k)$.

The map $a \mapsto b$ extends to $k[a] \longrightarrow k$.

2. slogan: 1 + saturation.

More precisely, enumerate A as $\langle a_i \mid i \in \omega \rangle$ and consider $X = \langle X_i \mid i \in \omega \rangle$. For all finite $a \subseteq A$, let

$$I(a/k) = (f^a_1, \dots f^a_{r_a})$$

and let $p(X) = \bigcup_{\substack{a \subseteq A \\ \text{finite}}} \{f^a_1, \dots f^a_{r_a}\}$. By 1, this is finitely consistent and so, by $\aleph_1$-saturation, there is a realization $B \subseteq k$.

The map $A \mapsto B$ is the required k-morphism between $k[A] \to k$.

thank you!

REFERENCES:

(Learnweb)

Ax68 : "The elementary theory of finite fields"

Cha05: "Notes on the model theory of finite and pseudofinite fields"

+

Brawley, Schnibben : "Infinite algebraic extensions of finite fields"