Lectures on Large Stable Fields IV
Stable and Superstable Fields

Dave Marker

Mathematics, Statistics, and Computer Science
University of Illinois at Chicago

February 15, 2021

www.math.uic.edu/∼marker/mc-S21

Last time

Theorem

If $(K, +, \cdot, \ldots)$ is a stable field, then the additive group and the multiplicative group are connected.

Lemma (Surjectivity Principle)

If $(G, \cdot, \ldots)$ is a connected superstable groups and $\sigma : G \to G$ is a definable finite-to-one homomorphism then σ is surjective.

Corollary

Let $(K, +, \cdot, \ldots)$ be a superstable field.

1. *The multiplicative homomorphism $x \mapsto x^n$ is surjective.*
2. *Superstable fields are perfect.*
3. *If $char(K) = p > 0$, then the additive homomorphism $x \mapsto x^p - x$ is surjective*

Cyclic Galois extensions

Theorem (Kummer extensions)

Suppose that L/K is a cyclic Galois extension of degree n, where n is relatively prime to the characteristic of K and K contains all n^{th} roots of unity. The minimal polynomial of L/K is $X^n - a$ for some $a \in K$.

Theorem (Artin–Schreier extensions)

Suppose that $char(K) = p > 0$ and L/K is a Galois extension of degree p. The minimal polynomial of L/K is $X^p - X - a$ for some $a \in K$.

Superstable fields

Lemma

Suppose an infinite superstable field K contains all m^{th} roots of unity for $m \leq n$. Then K has no Galois extensions of order n.

Suppose L/K is Galois of degree n and $p|n$ is prime.

By the Fundamental Theorem of Galois Theory, there is $K \subseteq F \subset L$ such that L/F is a Galois extension of degree p.
Let $L = F(\alpha)$. The field F is interpretable in K and hence it is also superstable.

If $p \neq \mathrm{char}(K)$, the minimal polynomial of α is $X^p - a$. But $x \mapsto x^p$ is surjective, so $X^p - a$ is not irreducible.

If $p = \mathrm{char}(K)$, the minimal polynomial of α is $X^p + X - a$. But $x \mapsto x^p - x$ is surjective, so $X^p - X - a$ is not irreducible.

Corollary

If K is an infinite superstable field, then K contains all n^{th} roots of unity.

We prove this by induction on n.

Suppose K contains all m^{th} roots of unity for $m < n$.
By the previous lemma K has no proper Galois extensions of order less than n.

Let ξ be a primitive n^{th}-root of unity.
Then $K(\xi)/K$ is a Galois extension of degree at most $n-1$, a contradiction.

Theorem (Cherlin–Shelah)

Every infinite superstable field is algebraically closed.

Let $(K, +, \cdot, \dots)$ be a superstable field.
By the previous lemmas, K has contains all roots of unity and hence has no proper separable extensions.

But $x \mapsto x^p$ is surjective so K is perfect and every algebraic extension is separable.

Bounded Fields

Definition

A field K is *bounded* if there are only finitely many isomorphism types of separable algebraic extensions of degree n for all n.

Examples:

- separably closed fields
- real closed fields
- finite fields
- pseudofinite fields where there is a unique extension of degree n for all n.

Theorem (Poizat)

An infinite bounded stable field is separably closed.

Bounded Stable Fields

Lemma

Suppose K is an infinite bounded stable field.

1. *If $char(K)$ doesn't divide n, then $x \mapsto x^n$ is surjective.*
2. *If $char(K) = p > 0$, then $x \mapsto x^p - x$ is surjective.*

Lemma $\Rightarrow$ Theorem

Follow Macintyre's argument. Note that if F/K is a finite separable extension F is bounded and stable.

Suppose K is infinite and stable, n is relatively prime to $\mathrm{char}(K)$ and $x \mapsto x^n$ is not surjective.

Since $K^\times$ is connected $(K^\times)^n$ is an infinite index subgroup.
We will show that if L/K is a finite separable extension there are only finitely many cosets of $K^\times/(K^\times)^n$ that have n^{th}-roots in L.

Thus there are infinitely many isomorphism types of separable extensions of K of degree at most n and K is not bounded.

Let L/K be a finite separable extension.
Let $\sigma_1, \ldots, \sigma_m$ be the embeddings of L into $K^{\rm alg}$ fixing K.

Let $X = \{a \in L^\times : a^n \in K\}$
Define $\sim$ on X by

$$a \sim b \Leftrightarrow \bigwedge_{i=1}^{m} \frac{\sigma_i(a)}{a} = \frac{\sigma_i(b)}{b}.$$

Since $a^n \in K$, $\sigma_i(a)^n = a^n$.
Thus each $\frac{\sigma_i(a)}{a}$ is an $n^{\rm th}$ root of unity.
It follows that there are only finitely many $\sim$ classes.

But if $a \sim b$, then $\sigma_i(a/b) = a/b$ for all i.
But a/b is separable over K and this is only possible if $a/b \in K$ and $a^n = b^n (\bmod\ (K^*)^n)$.
Thus only finitely many classes of $K^\times/(K^\times)^n$ have $n^{\rm th}$-roots in L.

Let K be an infinite, stable, bounded field of characteristic $p > 0$.
Let $\wp : K \to K$ by $x \mapsto x^p - x$.
If $\wp$ is not surjective then, since the additive group is connected, $\wp(K)$ has infinite index in K

Let L/K be a finite separable extension. An analogous argument to the one above shows that the set of cosets $b\wp(K)$ such that $b \in \wp(L)$ is finite.

Valuations on Stable Fields

Theorem (Poizat)

If K is an infinite stable field and v is a non-trivial henselian valuation on K, then K is separably closed.

Recall: If $(K, \mathcal{O})$ is a valued field with valuation v and residue field $\boldsymbol{k}$, then $(K, \mathcal{O})$ is *henselian* if any of the following equivalent conditions hold.

1. if $p(X) \in K[X]$, $\overline{p}$ is the image of p under reduction and there is $a \in \boldsymbol{k}$ such that $\overline{p}(a) = 0$ and $\overline{p}'(a) \neq 0$, then p has a zero in K.
2. If L/K is separable algebraic, there is unique extension of $\mathcal{O}$ to a valuation ring on K.
3. If L/K is algebraic, there is unique extension of $\mathcal{O}$ to a valuation ring on K.

Examples: $\mathbb{Q}_p$, $k((X))$, Hahn series, separably closed valued fields...

Any separably closed field K except the algebraic closure of the prime field has a non-trivial henselian valuation.

Let k be the prime subfield of K and let $t \in K$ be transcendental over k. We can define a non-trivial valuation v_0 on $k(t)$. Then we can extend v_0 to v a non-trivial valuation on K and this valuation must be henselian.

Recall: Shelah's conjectured that an infinite NIP field is either algebraically closed, real closed or admits a non-trivial henselian valuation.

Poizat's result shows that Shelah's Conjecture implies that an infinite stable field is separably closed.

It suffices to show that if K is a stable field admitting a nontrivial henselian valuation then $x \mapsto x^n$ is surjective for all n relatively prime to $\mathrm{char}(K)$ and if $\mathrm{char}(K) = p > 0$, then $x \mapsto x^p - x$ is surjective.

Then the usual arguments will show that K is separably closed–note if L/K is a finite Galois extension, then the valuation of K extends to a henselian valuation on L.

Let $\boldsymbol{k}$ be the residue field of K.
Work in $(K, v) \prec (K_1, v_1)$ where $a \in K_1$ realizes the unique generic type of K.

Replacing a by a^{-1} if necessary we may assume $v(a) \geq 0$.
Let $b \in K$ with $v(b) > 0$. Then ba is generic and $v(ba) > 0$. So, without loss of generality, we may assume $v(a) > 0$.

We have a generic with $v(a) > 0$.

claim 1 If $\mathrm{char}(\boldsymbol{k})$ does not divide n, then $x \mapsto x^n$ is surjective.

$1 + a$ is also generic. Let $p(X) = X^n - 1 - a$.
Reduce to $\boldsymbol{k}$ and consider $\overline{p}(X) = X^n - 1$.
Then 1 is a simple zero of $\overline{p}$ in $\boldsymbol{k}$.
Since K is henselian there is a zero in K.

Thus the generic $1 + a$ is in $(K^\times)^n$ so $(K^\times)^n$ is generic and, hence, of finite index in $K^\times$.

But $K^\times$ is connected. Thus $K = K^n$.

claim 2 If $\mathrm{char}(K) = p > 0$, then K is closed under $x \mapsto x^p - x$ is surjective.

We have a generic with $v(a) > 0$.

Let $p(X) = X^p - X - a$. Then $\overline{p}(X) = X^p - X$ and 1 is a simple zero in $\boldsymbol{k}$. Thus the image of $x \mapsto x^p$ is generic and, since $(K, +, \dots)$ is connected, must be all of K.

claim 3 If $\mathrm{char}(K) = 0$ and $\mathrm{char}(k) = p > 0$, then $x \mapsto x^p$ is surjective.

We have a generic with $v(a) > 0$.
By claim 1, there is b such that $b^{p-1} = \frac{1}{p}$.
We will show that $b^p + a \in K^p$. Then K^p is generic and $K = K^p$.

Let $f(Y) = (Y+b)^p - b^p - a$. It suffices to find a y such that $f(y) = 0$.

$$\begin{aligned} f(Y) &= Y^p + pbY^{p-1} + \binom{p}{2} b^2 Y^{p-2} + \cdots + pb^{p-1}Y - a \\ &= Y^p + \sum_{i=1}^{p-2} \binom{p}{i} b^i Y^{p-i} + Y - a. \end{aligned}$$

Note that p divides $\binom{p}{i}$, $i = 1, \dots p-1$ and $v(b) = -\frac{v(p)}{p-1}$ so $v(\binom{p}{i} b^i) \geq v(p) - \frac{v(p)i}{p-1} > 0$ for $1 \leq i < p-1$.

Thus $\overline{f}(Y) = Y^p + Y$, 0 is a simple 0 in $\boldsymbol{k}$ and f has a zero in K.

Artin–Schreier extensions of stable fields

Theorem (Scanlon)

If $(K, +, \cdot, \dots)$ is an infinite stable field of characteristic $p > 0$, then $x \mapsto x^p - x$ is surjective.

Without loss of generality we can assume K is $\aleph_1$-saturated. Let

$$k = \bigcap_{n=1}^{\infty} K^{p^n}.$$

Note that $k = k^p$ is perfect.
Let $I = \bigcap_{a \in k^\times} a\wp(K) \subseteq \wp(K)$. We want to show $I \cap k$ is non-trivial.

By Baldwin–Saxl, there are $a_1, \dots, a_n \in k^\times$ such that $I = a_1\wp(K) \cap \dots \cap a_n\wp(K)$.

We work in K^{alg}.
Let

$$G = \left\{ (x_1, \ldots, x_n, t) : \bigwedge_{i=1}^{n} t = a_i(x_i^p - x_i) \right\}$$

If $(\overline{b}, t) \in G$, then $t \in I$.

Note G is an algebraic subgroup of $\mathbb{G}_a^{n+1}$ defined over k and the dimension of G is at least 1.

We need one fact from algebraic group theory.

Lemma

If F is a perfect field and G is an algebraic subgroup of $\mathbb{G}_a^l$ of positive dimension defined over F, then G contains an algebraic subgroup H defined over F and definably isomorphic over F to $\mathbb{A}^1$.

There is $H \subseteq G$ an algebraic group defined over k and $f : \mathbb{A}^1 \to H$ an isomorphism defined over k.

$$G = \left\{ (x_1, \ldots, x_n, t) : \bigwedge_{i=1}^{n} t = a_i(x_i^p - x_j) \right\}$$

We have $H \subseteq G$ and $f : \mathbb{A}^1 \to H$ an isomorphism defined over k. Thus $H(k) = f(k)$ is infinite.

If $(x_1, \ldots, x_n, 0) \in H$, then $x_i^p - x_i = 0$, so $x_i \in \{0, 1, \ldots, p-1\}$. Thus there is some point $(\overline{x}, t) \in H(k)$ with $t \neq 0$, but then $t \in I$.

Thus $I \cap k$ is a non-trivial ideal of k. So $I \supseteq k$. and $\wp(K) \supseteq I \supseteq k$.

Since $\wp(K) \supseteq k$, by compactness $\wp(K) \supseteq K^{p^n}$ for some n.
Let $a \in K$. Then $a^{p^n} \in \wp(K)$ so there is $\alpha \in K$ such that

$$\alpha^p - \alpha = a^{p^n}.$$

Work in K^{alg}. There is a unique β such that $\beta^{p^n} = \alpha$. Then

$$\wp(\beta)^{p^n} = (\beta^p - \beta)^{p^n} = (\beta^p)^{p^n} - \beta^{p^n} = \alpha^p - \alpha = a^{p^n}.$$

Thus $\wp(\beta) = a$.
Since $\beta^{p^n} = \alpha$, $K(\beta)/K$ is purely inseparable. But $\beta^p - \beta = a$, thus $K(\beta)/K$ is separable. Thus we must have $\beta \in K$.

Remarks: • The only place we used stability was in the application of Baldwin–Saxl that uses only NIP so this is also true in NIP fields.

• Kaplan–Scanlon–Wagner also show that infinite simple fields of characteristic $p > 0$ have no proper Artin–Schreier extensions

Corollary

If K is an infinite NIP field of characteristic $p > 0$ and L/K is a finite Galois extension, then p does not divide $[L : K]$.

Otherwise, we can find $K \subseteq F \subset L$ with L/F separable of degree p. But F is also NIP and, hence, closed under Artin–Schreier extensions.

Corollary

If K is an infinite NIP field of characteristic $p > 0$, then $K \supseteq \mathbb{F}_p^{\mathrm{alg}}$

Let $k = K \cap \mathbb{F}_p^{\mathrm{alg}}$.
Since K is closed under Artin–Schrier extensions $\mathbb{F}_{p^{p^n}} \subset k$ for all n.
Thus k is infinite and perfect. Using the Lang–Weil estimates it's easy to see that k is PAC. We then apply the following result.

Theorem (Duret)

If K is NIP and $L \subset K$ is a PAC subfield algebraically closed in K, then L is separably closed.

Thus k is separably closed and, since perfect, algebraically closed.