Logic IV: Model Theory of Pseudo-Finite Fields

Lecturer
Prof. Dr. Martin Hils

Notes
Josia Pietsch

Version
git: bb88db0-*
compiled: September 25, 2025 23:21

Contents

These are my notes on the lecture Logic VI: Model Theory of Pseudo-Finite Fields, taught by Prof. Dr. Martin Hils in Winter 2024 at the University Münster.

Warning. *This is not an official script. The official lecture notes can be found here.*

If you find errors or want to improve something, please send me a message: `lecturenotes@jrpie.de`.

These notes follow the way the material was presented in the lecture rather closely. Additions (e.g. from exercise sheets) and slight modifications have been marked with †.

Note. *There is a version optimized for printing using less color.*

[Lecture 01, 2024-10-08]

0.1 Prerequisites

- General material from model theory: Logic 2 is more then enough. Can be found in [TZ12]): Compactness, saturation, type spaces, quantifier elimination, decidability.

  Some model theory of ACF.

- Solid knowledge of field theory, (infinite) Galois theory
- Basic algebraic geometry concerning algebraic varieties over a field and the corresponding commutative algebra (see [Lan73] or, for a more advanced treatment, [FJ23]).

Main bibliographical sources for the course:

- Original paper by James Ax: The elementary theory of finite fields [Ax68].
- Lecture notes by Zoé Chatzidakis: "Notes on the model theory of finite and pseudofinite fields". [Cha18] or [Cha05]?
- Chatzidakis, van den Dries and Macintyre: Definable sets over finite fields [CDM92]

Introduction, Motivation and Overview

The model theory of finite and pseudofinite fields is central toe model theory and applications. Ax's paper is seminal and extremely influential.

We work in the language of rings, $\mathcal{L}_{\text{ring}} = \{0, 1, +, -, \cdot\}$. We consider fields as first order structures in $\mathcal{L}_{\text{ring}}$.

Fact 0.1 (Some Tame Theories of Fields). (a) The theory ACF of algebraically closed fields has QE, is decidable and its completions are given by ACF_p where p is prime or 0 specifying the characteristic.

It also follows that ACF_p is strongly minimal with algebraic closure acl given by field theoretic closure.

(b) RCF, the theory of **real closed fields** $\mathrm{Th}(\mathbb{R})$, is complete and decidable (Tarski). F is **real closed** iff

- -1 is not a sum of squares (**formally real**)[a]
- $\forall a \in F.\ \exists b \in F.\ (a = b^2 \vee -a = b^2)$.
- Every polynomial $p(X) \in F[X]$ of odd degree has a root in F.

If $F \models \mathsf{RCF}$ then $x \leqslant y := \exists z.\ y - x = z^2$ defines a field ordering and RCF has QE in the definitional expansion to $\mathcal{L}_{\text{oRing}} := \mathcal{L}_{\text{ring}} \cup \{\leqslant\}$.

(c) Ax-Kochen, Macintyre: Similarly $\text{Th}(\mathbb{Q}_p)$ admits an explicit (recursive) axiomatization (p-adically closed fields) and quantifier elimination in a definitional expansion.

(d) Using Ax-Kochen / Ershov (AKE) one may also give axiomatizations to theories like $\text{Th}(\mathbb{C}((t)))$, $\text{Th}(\mathbb{R}((t)))$.

[a] clearly this implies characteristic 0

Fact 0.2 (Julia Robinson)**.** In the field $\mathbb{Q}$, the ring of integers $\mathbb{Z}$ is $\mathcal{L}_{\text{ring}}$-definable, hence also $\mathbb{N}$ (by Legendre's four squares theorem), so $\mathbb{Q}$ is undecidable by Gödel.

Question 0.2.1. What about other theories of field?

Especially field important in number theory.

Clearly $\text{Th}(\mathbb{F}_q)$ is decidable ($\mathbb{F}_q$ is finite, just check). But what about uniform decidability?

Notation 0.2.2. We set $T_f := \bigcap_{\substack{q=p^n \\ p \text{ prime}}} \text{Th}(\mathbb{F}_q)$ (finite fields)

We set $\mathsf{Psf} := \{\varphi \mid \forall q \gg 0.\ \mathcal{F}_q \models \varphi\} = \limsup_{q\to\infty} \text{Th}(\mathbb{F}_q)$ (pseudo finite fields), i.e. the theory of the infinite models of T_f.

In order to understand T_f, we need to study Psf. This was done by Ax.

Theorem 0.3 (Ax, 1968 - main theorem of his paper)**.** A field F is pseudo-finite iff the following hold:

1 F is perfect.

2 $\text{Gal}(F) = \text{Gal}(F^{\text{alg}}/F) \cong \hat{\mathbb{Z}}$, i.e. the absolute Galois group of F is isomorphic to $\varprojlim \mathbb{Z}/n\mathbb{Z}$.

3 F is **PAC** (**pseudo algebraically closed**), i.e. every absolutely irreducible algebraic variety V defined over F has an F-rational point.

We will call this theory Psf′ until we have proven the theorem.

Comment 0.4. (a) (1), (2) and (3) are first order expressible.

(b) Modulo (1), (2) is equivalent to $\forall n \geqslant 1$. F has a unique algebraic extension of degree n.

(c) In (3) it is enough to talk about algebraic curves, i.e. $\dim(V) = 1$.

The notions appearing in the theorem will be explained in the course of the lecture.

Remark 0.5. Theorem 0.3 need two essential ingredients from algebraic geometry and number theory:

1 The **Lang-Weil estimates** (a consequence of the "Rieman hypothesis for curves over finite fields"[a]),

2 Chebotarev's density theorem.

We will not prove these two in the lecture and treat them as black boxes.

[a] this is a theorem

1 Preliminaries

1.1 Field theory and infinite Galois theory

Notation 1.0.3. Let $\mathbb{P} := \{p : p \text{ prime}\}$ and $Q := \{p^n : p \in \mathbb{P}, n \in \mathbb{N}_{>0}\}$.

Fact 1.1. (1) If F is a finite field, then $q := |F| \in Q$ and F is perfect.[a]

(2) For every $q \in Q$ there is (up to isomorphism) a unique field of cardinality q, denoted by $\mathbb{F}_q$.

(3) If $q = p^n$ and $q' = p'^{n'}$ then $\mathbb{F}_q \subseteq \mathbb{F}_{q'}$ iff $p = p'$ and $n | n'$.

(4) If F is a finite field, then for every $n \geqslant 1$ there is a unique field extension F_n/F with $[F_n : F] = n$. By uniqueness it follows that this is a Galois extension.

(5) The multiplicative group $(F^\times, \cdot)$ of a finite field F is cyclic, i.e. $\cong \mathbb{Z}/(|F| - 1)\mathbb{Z}$.

(6) If F is a finite field and F_n/F as in (4) then $\mathrm{Gal}\left(F_n/F\right) \cong \mathbb{Z}/n\mathbb{Z}$. Moreover if $F = \mathbb{F}_q$ then $\mathrm{Frob}_q \in \mathrm{Gal}(F_n/F)$ is a generator of it, where $\mathrm{Frob}_q(x) = x^q$.

[a] Recall that a field is **perfect** iff either it has characteristic 0 or it has characteristic p and the Frobenius endomorphism, $x \mapsto x^p$, is an automorphism. Equivalently, every algebraic extension is separable.

Proof (sketch). (1) $\mathrm{char}(F) = p \in \mathbb{P}$, so F is a finite-dimensional $\mathbb{F}_p$-vector space, so $|F| = p^n$. $\mathrm{Frob}_p \colon F \to F$ is injective, hence surjective.

(2) Let $q = p^n \in Q$. In $\mathbb{F}_p^{\mathrm{alg}}$ take the set of zeros of $X^q - X$ (the fixed points under Frob_q). This is a subfield with q elements, every root of $X^q - X$

being simple (-1 is the derrivative).

(3) Follows from (2).

(4) By (3) and (2)

(5) A polynomial of degree m has at most m roots.

(6) If $F = \mathbb{F}_q$, then $F_n = \mathbb{F}_{q^n}$. Then $|F_q| = \{x \in \mathbb{F}_{q^n} | \operatorname{Frob}_q(x) = x\}$. So $\operatorname{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$ is generated Frob_q by Galois correspondence.

Copy from official notes

□

Fact 1.2. For every $p \in \mathbb{P}$, we have $\mathbb{F}_p^{\text{alg}} = \bigcup_{n>0} \mathbb{F}_{p^n}$, so $\mathbb{F}_p^{\text{alg}}$ is an increasing union of finite fields.

[Lecture 02, 2024-10-11]

1.2 Infinite Galois Theory

Recall: If L/K is a field extension, consider $\operatorname{Aut}(L/K) = \{\sigma \in \operatorname{Aut}(L) | \sigma|_K = \operatorname{id}_K\}$. If L/K is **Galois**[1] we write $\operatorname{Gal}(L/K)$ or $G(L/K)$ for $\operatorname{Aut}(L/K)$ and call it the **Galois group** of L over K.

Definition 1.2.4. The **absolute Galois group** of K, denoted by $\operatorname{Gal}(K)$ is defined as $\operatorname{Gal}(K^{\text{sep}}/K) = \operatorname{Aut}(K^{\text{alg}}/K)$, where K^{sep} is a separable closure of K.

Fact 1.3 (Main Theorem of Finite Galois Theory)**.** Let L/K be a finite field extension, i.e. $n = [L : K] = \dim_K(L) < \infty$.

Then

(1) $|\operatorname{Aut}(L/K)| \leqslant n$ with equality iff L/K is Galois.

Assume now that L/K is Galois. Then

(2) the maps

$$\begin{aligned} \{\text{subgroups of } \operatorname{Gal}(L/K)\} &\underset{\mathcal{G}}{\overset{\mathcal{F}}{\rightleftarrows}} \{K \subseteq M \subseteq L \text{ intermediate fields}\} \\ H &\longmapsto L^H \\ \operatorname{Aut}(L/M) &\longmapsfrom M \end{aligned}$$

are inverses of each other and define inclusion reversing bijections.

(3) If H is a subgroup of $\operatorname{Gal}(L/K)$, then it is a normal subgroup iff the

[1] i.e. algebraic, normal and separable

corresponding field extension $\mathcal{F}(H)/K$ is normal (thus Galois).

(4) If $K \subseteq M \subseteq L$ with M/K Galois, then the respective map $\mathcal{G}(L/K) \twoheadrightarrow \mathcal{G}(M/K)$ is a surjective group homomorphism inducing an isomorphism

$$G(L/K)\big/_{G(L/M)} \cong G(M/K).$$

Infinite Galois theory is an extension of this. Here L/K is Galois, but $[L : K]$ not necessarily finite.

In order to obtain a Galois correspondence as in (2) we need to endow the Galois group with a topology, the so-called **Krull topology**.

Definition 1.3.5. A **topological group** is a group G endowed with a *Hausdorff*[a] topology, such that

$$\begin{aligned} G &\longrightarrow G \\ g &\longmapsto g^{-1} \end{aligned}$$

and

$$\begin{aligned} G \times G &\longrightarrow G \\ (g, h) &\longmapsto gh \end{aligned}$$

are continuous.

[a] Some authors don't require that. However in this course topological groups will always be Hausdorff.

Remark 1.3.6. In a topological group G, for any $g \in G$, the maps

$$\begin{aligned} \rho_G \colon G &\longrightarrow G \\ x &\longmapsto xg \end{aligned}$$

and

$$\begin{aligned} \lambda_G \colon G &\longrightarrow G \\ x &\longmapsto gx \end{aligned}$$

are homeomorphisms.

In particular, the topology on G is determined the neighborhoods of $1 \in G$.

Fact 1.4 (Elementary Facts about Topological Groups)**.** Let G be a group.

(1) If $H \leqslant G$ then $\overline{H}$ is also a subgroup of G, where $\overline{H}$ is the closure of

H.

If H is normal (resp. abelian), so is $\overline{H}$.

(2) Every open subgroup of G is also closed (i.e. clopen), as all the cosets are open.

(3) Any closed subgroup *of finite index* in G is open (i.e. clopen).

(4) If G is compact, a closed subgroup H is open iff $(G : H) < \infty$.

(5) Let $U \subseteq G$ be a dense subset. Let $\varnothing \neq V \overset{\text{open}}{\subseteq} G$. Then $U \cdot V = \{uv \mid u \in U, v \in V\} = G$.

Proof. (1) Exercise.

(2) If $H \leqslant G$ is open, so are all cosets of H, thus also $G \backslash H$ (as a union of cosets).

(3) Similar as (2).

(4) clear

(5) Let $g \in G$. If V is open, so is V^{-1} and also $g \cdot V^{-1}$. Since U is dense, we find $u \in U \cap g \cdot V^{-1}$ and v as desired.

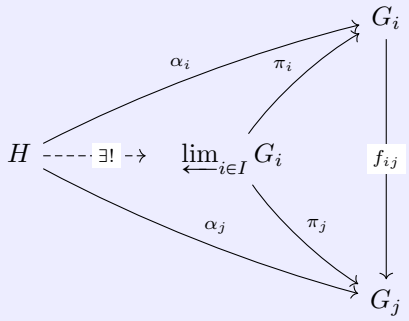
□

Definition† **1.4.7** (Projective limits)**.** Consider a category $\mathcal{C}$. Let $\varnothing \neq I$ be a partially ordered set which is **directed**, i.e. $\forall i, j \in I.\ \exists k \in I.\ k \leqslant i, j$.

For any $i \in I$ let $G_i \in \mathrm{Ob}(\mathcal{C})$. For any $i \leqslant j$ let $f_{ij} \colon G_i \to G_j$ be a morphism, such that these are compatible, i.e. $f_{ik} = f_{jh} \circ f_{ij}$.

$(G_i)_{i \in I}, (f_{ij})_{i,j}$ is a **projective system** in $\mathcal{C}$ (the f_{ij} are part of the datum but often omitted in notation).

The **projective limit** of $(G_i)_{i \in I}$, denoted by $\varprojlim G_i$, is the terminal object in the category of cones over $(G_i)_{i \in I}$, i.e. an object $G \in \mathrm{Ob}(\mathcal{C})$ together with morphisms $\pi_i \colon G \to G_i$ compatible with the f_{ij} such that for every $H \in \mathrm{Ob}(\mathcal{C})$ and $\alpha_i \colon H \to G_i$ compatible with the f_{ij}, there exists a unique morphism $\alpha \colon H \to G$ making the diagram commute:



This is of course unique up to unique isomorphism (if it exists).

Proposition 1.5. In the category of topological groups, the projective limit is the closed subgroup of $\prod_{i\in I} G_i$ given by $\{(a_i)_{si\in I} | \forall i \leqslant j.\ f_{ij}(a_i) = a_j\}$.

The structural maps $f_i \colon \varprojlim_{j\in I} G_i \to G_i$ are the restrictions of the projective map $\pi_i \colon \prod_{j\in I} G_j \to G_i$.

In particular, if all G_i are compact then so is $\varprojlim_{i\in I} G_i$.

Proof. We need to show:

(1) The group constructed above is indeed a topological group and the structural maps are continuous.

(2) It is indeed the projective limit.

This is left as an easy exercise. □

Definition 1.5.8. A **profinite group** is a topological group, which is isomorphic to some projective limit $\varprojlim_{i\in I}$ with all G_i finite (i.e. discrete).

Proposition 1.6. For a topological group G, the following are equivalent:

(a) G is profinite,

(b) G is compact and **totally disconnected**[a].

[a] $\forall x \neq y \in X.\ \exists Z \overset{\text{clopen}}{\subseteq} X.\ x \in Z \wedge y \notin Z$

Proof. (a) $\implies$ (b): Compactness follows from Proposition 1.5. Totally disconnected follows from the definition of the product topology: Let $x \neq y \in \varprojlim_i G_i$.

Then there exists a coordinate, where they differ, i.e. $x_i \neq y_i$. Consider $f_i^{-1}(x_i)$, this is clopen.

(b) $\implies$ (a): This is the harder direction. We'll only sketch the proof. One shows that for every $1 \neq g \in G$, there is an open subgroup $N \leqslant G$ such that $g \notin H$.

Then there is a normal such subgroup as $(G : H) < \infty$, so $\bigcap_{g \in G} H^g = \bigcap_{i=1}^{N} H_{g_i}$ is open.

Then G/N is finite and discrete and $G \hookrightarrow \varprojlim_{N \text{ open normal}} {}^{G}\!/_{N}$ is injective by the above, continuous with dense image, so an isomorphism, so a homeomorphism. □

Lemma 1.7. Let $(G_i)_{i \in I}$,$(f_{ij})_{i,j}$ be a projective system. Suppose that the projective limit of this exists. Let $I_0 \subseteq I$ be **coinitial**, i.e. $\forall i \in I.\ \exists i_0 \in I_0.\ i_0 \leqslant i$, then $\varprojlim_{i \in I_0} G_i \cong \varprojlim_{i \in I} G_i$ are canonically isomorphic.

Proof. Clear. □

Proposition 1.8. Let L/K be Galois and let $\{K \subseteq L_i \subseteq L | i \in I\}$ be the set of all finite Galois subextensions ordered by reversed inclusions.

Then $\mathrm{Gal}(L/K) \cong \varprojlim_{i \in I} G(L_i/K)$ as groups.

Proof. It is injective as any $a \in L$ is in some finite Galois subextension L'/K. Surjectivity is clear, as we can glue field automorphisms (being a field automorphism can be checked locally). □

Definition 1.8.9. For L/K Galois the **Galois group**, $G(L/K)$, is the profinite topological group given by $\varprojlim_{i \in I} G(L_i/K)$.

The topology is called the **Krull topology**.

Remark 1.8.10. By construction, a basis of clopen sets of $G(L/K)$ is given by

$$\{\sigma \cdot G(L/L') | \sigma \in G(L/K), L'/K \text{ finite Galois}\}.$$

Lemma 1.9. Let $L/M/K$ be a tower of field extensions with L/K and M/K Galois.

Then

$$\operatorname{res}\colon G(L/K) \longrightarrow G(M/K)$$

is surjective. More generally, for any intermediate field $K \subseteq M' \subseteq L$, any K-embedding of M' into L extends to an automorphism $\sigma \in G(L/K)$.

Proof. Easy application of Zorn's lemma. □

Proposition 1.10. Let L/K be Galois.

(1) If $K \subseteq M \subseteq L$ then L/M is Galois and $G(L/M)$ is a closed subgroup of $G(L/K)$ and $L^{G(L/M)} = M$.

(2) If H is a subgroup of $G(L/K)$, then $G(L/L^H) = \overline{H}$.

Proof. (1) One has $G(L/M) = \bigcap_{\substack{K \subseteq M' \subseteq M \\ M' \text{ finite}}} \overbrace{G(L/M')}^{\text{clopen}}$. So $G(L/M)$ is closed.

Clearly $M \subseteq L^{G(L/M)}$. For the other inclusion let $a \in L \backslash M$. Since L/M is algebraic, there is a finite Galois extension M_1/M containing a. By the finite Galois correspondence, there is $\sigma_1 \in G(M_1/M)$ such that $\sigma_1(a) \neq a$. By Lemma 1.9 there exists $\sigma \in G(L/M)$ such that $\sigma|_{M_1} = \sigma_1$, so $\sigma(a) \neq a$, i.e. $a \notin L^{G(L/M)}$.

(2) Clearly $H \subseteq \tilde{H} := G(L/L^H)$. As $\tilde{H}$ is closed by (1), we get $\overline{H} \subseteq \tilde{H}$.

Suppose there is $\sigma \in \tilde{H} \backslash \overline{H}$. Then there is some finite Galois extension L'/K with $K \subseteq L' \subseteq L$, such that $\sigma \cdot \operatorname{Gal}(L/L') \cap H = \varnothing$. Let $\operatorname{res}\colon G(L/K)^{-1} \twoheadrightarrow G(L'/K)$. (This is surjective by Lemma 1.9.) Then $\operatorname{res}(\sigma) \notin \operatorname{res}(H)$. So by finite Galois theory, $\operatorname{res}(\sigma)$ moves some element of $(L')^{\operatorname{res}(H)} \subseteq L^H$ ↯.

□

Corollary 1.11 (Infinite Galois Correspondence)**.** Let L/K be Galois and $G := G(L/K)$. Then the maps

$$\begin{aligned} \{\text{closed subgroups of } G\} &\underset{G}{\overset{F}{\rightleftarrows}} \{K \subseteq M \subseteq L\} \\ H &\longmapsto L^H \\ \operatorname{Fix}(M) &\longmapsfrom M \end{aligned}$$

are inverse to each other and define inclusion reversing bijections.

Moreover

(a) a closed subgroup $H \leqslant G$ is open iff L^H/K is finite and then $(G : H) = [L^H : K]$,

(b) for $\sigma \in G$ and $H = G(L/M)$, $\sigma H \sigma^{-1}$ corresponds to σM, i.e. $L^{\sigma H \sigma^{-1}} = \sigma(L^H)$ and $G(L/\sigma(M)) = \sigma G(L/M)\sigma^{-1}$,

(c) for $K \subseteq M \subseteq L$, then M/K is Galois (i.e. normal) iff $G(L/M) \trianglelefteq G$ and then $G(M/K) \cong {}^{G(L/K)}\!/_{G(L/M)}$ as topological groups.

[Lecture 03, 2024-10-15]

Example 1.12. Let $\mathbb{F}_q$ be a finite field. Then, by Fact 1.1 one has $\mathrm{Gal}(\mathbb{F}_q) \cong^{\chi} \varprojlim_I \mathbb{Z}/n\mathbb{Z} =: \hat{\mathbb{Z}}$, where the index set is $I := \mathbb{N}_{\geqslant 1}$ ordered by $n \preceq m :\iff m \mid n$ and $f_{n,m} \colon \mathbb{Z}/n\mathbb{Z} \xrightarrow{\text{can:}z \pmod n \mapsto z \pmod m} \mathbb{Z}/m\mathbb{Z}$.

As $(\mathbb{F}_q^{\mathrm{alg}})^{\langle \mathrm{Frob}_q \rangle = \mathbb{F}_q}$, so $\overline{\langle \mathrm{Frob}_q \rangle} = \mathrm{Gal}(\mathbb{F}_q)$ by Proposition 1.10 (2). So Frob_q, which under χ corresponds to $(1, 1, \ldots) \in \varprojlim {}^{\mathbb{Z}}\!/_{n\mathbb{Z}}$, is a **topological generator** of $\mathrm{Gal}(\mathbb{F}_q)$.

The finite extensions of $\mathbb{F}_q$ are of the form $\mathbb{F}_{q^n}$, $n \geqslant 1$. By the Galois Correspondence (1.11) the open subgroups of $\mathrm{Gal}(\mathbb{F}_q)$ are given by $H_n := \overline{\langle \mathrm{Frob}_q^n \rangle}$ as $(\mathbb{F}_q^{\mathrm{alg}})^{\langle \mathrm{Frob}_q^n \rangle} = \mathbb{F}_{q^n}$.

Under χ, H_n corresponds to $\overline{\langle n \rangle}$, where $n = (n, n, \ldots)$.

Lemma 1.13. Let $\pi_n \colon \hat{\mathbb{Z}} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$ be the structural map. Then $\ker(\pi_n) = \overline{\langle n \rangle} = n\hat{\mathbb{Z}}$.

Proof. One could to this by hand. For fun we use the Galois correspondence (see Example 1.12). The open subgroups of $\hat{\mathbb{Z}}$ admits for every $n \geqslant 1$ a unique open subgroup of index n.

This is equal to $\ker(\pi_n)$ and by Example 1.12 to $\overline{\langle n \rangle}$ (we have $\langle \overline{n} \rangle \subseteq \underbrace{n\hat{\mathbb{Z}}}_{\text{closed}} \leqslant \ker(\pi_n)$). □

Lemma 1.14. (1) $\hat{\mathbb{Z}} = \{(a_n)_{n \geqslant 1} \in \prod_{n \geqslant 1} {}^{\mathbb{Z}}\!/_{n\mathbb{Z}} | m \mid n \implies a_m \equiv a_n \mod m\}$.

(2) For $p \in \mathbb{P}$ let $\mathbb{Z}_p := \varprojlim_{n \geqslant 0} {}^{\mathbb{Z}}\!/_{p^n\mathbb{Z}}$. Then $\hat{\mathbb{Z}} \cong \prod_{p \in \mathbb{P}} \mathbb{Z}_p$ as topological groups.

Proof. (1) by definition.

(2) For $m \in \mathbb{N}_{>0}$, $m = \prod p_i^{h_i}$, we have $\mathbb{Z}/m \cong \prod \mathbb{Z}/p_i^{h_i}$ (Chinese remainder theorem). Now go to the limit.

□

Corollary 1.15. $|\hat{\mathbb{Z}}| = 2^{\aleph_0}$, in particular $\mathbb{Z} \subsetneq \hat{\mathbb{Z}}$.

Proof. $\hat{\mathbb{Z}} \subseteq \prod_{n \in \mathbb{N}_{>0}} \mathbb{Z}/n\mathbb{Z}$, i.e. $|\hat{\mathbb{Z}}| \leqslant 2^{\aleph_0}$. By Lemma 1.14 (2) we get an epimorphism $\hat{\mathbb{Z}} \twoheadrightarrow \prod_{p \in \mathbb{P}} \mathbb{Z}/p\mathbb{Z}$, thus $|\hat{\mathbb{Z}}| \geqslant 2^{\aleph_0}$. □

Definition 1.15.11. (1) Let G be a topological group. A subset $S \subseteq G$ is **topologically generating** iff $\langle S \rangle = G$.

(2) A profinite group is called **procyclic** iff it is topologically generated by a single element. (For example $\hat{\mathbb{Z}} = \overline{\langle 1 \rangle}$, $\mathrm{Gal}(\mathbb{F}_q) = \overline{\langle \mathbb{F}_q \rangle}$).

Lemma 1.16. $\hat{\mathbb{Z}}$ is free procyclic with topological generator 1, i.e. (it is procyclic and) it is the initial object in the category of pointed profinite groups.[a] In partucular $(\hat{\mathbb{Z}}, 1)$ is uniquely determined up to unique isomorphism by this property.

[a] i.e. for every pointed topological group (G, g) there exists a unique isomorphism $(\hat{\mathbb{Z}}, 1) \to (G, g)$.

Proof. Let $G = \varprojlim G_i$ with G_i finite and let $g = (g_i)_{i \in I} \in G \leqslant \prod G_i$

Let $n_i := \mathrm{ord}(g_i) \in \mathbb{N}$. We get a group homomorphism $\mathbb{Z}/n_i\mathbb{Z} \to G_i$, $\overline{1} \mapsto g_i$, so a continuous group homomorpism

$$\varphi_i \colon \hat{\mathbb{Z}} \to \hat{\mathbb{Z}}/n_i\hat{\mathbb{Z}} \cong \mathbb{Z}/n_i\mathbb{Z} \twoheadrightarrow G_i.$$

These commute with $f_{ij} \colon G_i \to G_j$, so by the universal property we get a unique isomorphism $\varphi \colon \hat{\mathbb{Z}} \to G$ as claimed. □

Remark 1.17. If H is a closed subgroup of the profinite group G, then $H = \bigcap_{\substack{H \leqslant \tilde{H} \leqslant G \\ \tilde{H} \text{ open}}} \tilde{H}$.

Proof. Let H_1 denote the right hand side. Suppose $H \subsetneq H_1$. Choose $h_1 \in H_1 \backslash H$. Then there is an open neighborhood $\Omega \ni h_1$, such that $\Omega \cap H = \varnothing$. We may assume that $\Omega = h_1 N$, where N is an open normal subgroup (since these form a neighborhood basis of 1).

Let $\tilde{H} := H \cdot N$. This contains 1 and $h_1 \notin \tilde{H}$, as $h_1 N \cap H = \varnothing$ ↯. □

Definition 1.17.12. The set $\mathbb{N}_*$ of **supernatural numbers** is defined as the set of formal products $\prod_{p\in\mathbb{P}} p^{n(p)}$, where $n(p) \in \mathbb{N} \cup \{\infty\}$.

Lemma 1.18. There is a one-to-one correspondence between $\mathbb{N}_*$ and the set of closed subgroups of $\hat{\mathbb{Z}}$ given by

$$\prod p^{n(p)} \longmapsto \prod_{p\in\mathbb{P}} H_p(n(p))$$

where

$$H_{p^{n(p)}} := \begin{cases} p^{n(p)}\mathbb{Z}_p & \text{if } n(p) \in \mathbb{N} \\ (0) & \text{if } n(p) = \infty, \end{cases}$$

i.e. $H_{p^{n(p)}} = \bigcap_{n\leqslant n(p)} p^n\mathbb{Z}_p$.

Proof. This follows from Remark 1.17 together with the fact that the open subgroups of $\hat{\mathbb{Z}}$ are of the form $n\hat{\mathbb{Z}} = \prod_{p\in P_0} p^{n(p)}\mathbb{Z}_p \times \prod_{q\in\mathbb{P}\setminus P_0} \mathbb{Z}_q$, where $n = \prod_{p\in P_0} p^{n(p)}$. □

Proposition 1.19. (1) For a profinite group G the following are equivalent:

(a) G is procyclic.

(b) There exists a continuous epimorphism $\varphi\colon \hat{\mathbb{Z}} \twoheadrightarrow G$.

(c) For every open and normal subgroup $N \trianglelefteqslant G$, the quotient G/N is cyclic.

(2) Assume that G is procyclic and moreover that for every $n \geqslant 1$ there is a (necessarily unique) open normal subgroup N_n of index n. Then every continous epimorphism $\varphi\colon \hat{\mathbb{Z}} \twoheadrightarrow G$ is an isomorphism.

Proof. (1) $(a) \iff (b)$ is clear from the above. Also $(b) \implies (c)$ is clear: Indeed let $N \trianglelefteqslant G$ be open, and $\varphi\colon \hat{\mathbb{Z}} \twoheadrightarrow G$. Then $\varphi^{-1}(N) \trianglelefteqslant \hat{\mathbb{Z}}$ is open, so of the form $n\hat{\mathbb{Z}}$ for some $n \geqslant 1$. Hence

$$G/N \cong \hat{\mathbb{Z}}/\varphi^{-1}(N) = \hat{\mathbb{Z}}/n\hat{\mathbb{Z}} \cong \mathbb{Z}/n\mathbb{Z}.$$

Let us now assume that G satisfies (c). In particular $G \cong \varprojlim G_i$ with G_i finite cyclic (so abelain), so G is abelian.

For every open subgroup $H \leqslant G$ (automatically normal) denote by $S_H \subseteq G$ the set

$$S_H := \{g \in G | gH \text{ generates } G/H\}.$$

Since G/H is cyclic, we have $S_H \neq \varnothing$. Moreover if $H \leqslant H'$, then $S_H \subseteq S_{H'}$. If H, H' are both open, so is $H \cap H'$ and thus $S_{H\cap H'} \subseteq S_H \cap S_{H'}$. Note that S_H is a finite union of cosets of H, so S_H is clopen, in particular closed.

So $\{S_H | H \leqslant G \text{ open}\}$ has the finite intersection property. By compactness of G, we have $\bigcap_{\substack{H\leqslant G\\ \text{open}}} S_H \neq \varnothing$. By construction any $g \in \bigcap S_H$ is a topological generator.

(2) Note that such a G has a unique open subgroup H_n of index n, since $\hat{\mathbb{Z}}$ has. Let $\varphi : \hat{\mathbb{Z}} \twoheadrightarrow G$ be a continuous epimorphism.

Claim 1. *φ is injective.*

This of course suffices by the usual argument for compact Hausdorff space.

Subproof. For all $n \geqslant 1$ the map

$$\varphi_n = \pi_n \circ \varphi \colon \hat{\mathbb{Z}} \twoheadrightarrow^{\varphi} G \twoheadrightarrow^{\pi}_{1} G/H_n \cong \mathbb{Z}/n\mathbb{Z}.$$

factors through $\hat{\mathbb{Z}}/n\hat{\mathbb{Z}}$ as $\psi_n \colon \hat{\mathbb{Z}}/\hat{n}\mathbb{Z} \cong \mathbb{Z}/n\mathbb{Z} \twoheadrightarrow \mathbb{Z}/n\mathbb{Z}$, so ψ_n is an isomorphism for all $n \geqslant 1$. It follows easily that φ is injective. ■

□

Definition 1.19.13. Let F be a perfect field. Fix an algebraic closure F^{alg} of F.

Then F is called **quasifinite** iff it has a unique extension F_n of degree n in F^{alg} for every $n \geqslant 1$.

Proposition 1.20. For a perfect field F the following are equivalent:

(1) $\text{Gal}(F) \cong \hat{\mathbb{Z}}$,

(2) F is quasifinite.

Proof. (1) $\implies$ (2) is clear by infinite Galois theory.

(2) $\implies$ (1):

Exercise: maybe one can shorten the proof

Assume that F is quasifinite. Let $G := \text{Gal}(F)$.

For ever $n \in \mathbb{N}_{\geqslant 1}$, G has a unique open subgroup N_n of index n, wich in addition is normal and $F_n = (F^{\text{alg}})^{N_n}$ is a Galois extension of F.

Let $G_n := \text{Gal}(F_n/F) = G/N_n$.

Claim 1. *G_n is cyclic.*

One the claim is proved, we are done by Proposition 1.19.

Subproof. We use inductoin on $n \geqslant 1$. $n = 1$ is clear. $n = p \in \mathbb{P}$ is clear as well.

Now let $n \geqslant 2$ be non-prime and assume that the statement holds for all $n' < n$. Pet $p \in \mathbb{P}$ be such that $p \mid n$. Let $g \in G_n$ be an element of order p. Then $F' := F_n^{\langle g \rangle}$ is a finite extension of F of degree $n' = \frac{n}{p}$. So $F' = F_{n'}$. By the induction hypothesis, we have $G_{n'} \cong {}^{G_n}\!/_{\langle g \rangle} \cong {}^{\mathbb{Z}}\!/_{n'\mathbb{Z}}$. Thus there is $h \in G_n$ such that $\langle g, h \rangle = G_n$. The subgroup $\langle g \rangle \cap \langle h \rangle$ has p elements or 1 element. If it has p elements it is equal to $\langle g \rangle$, so $g \in \langle h \rangle$, i.e. $G_n = \langle g, h \rangle = \langle h \rangle$ is cyclic. Otherwise $\langle g \rangle \cap \langle h \rangle = \{1\}$. Both $\langle g \rangle$ and $\langle h \rangle$ are normal, so $[g, h] \in \langle g \rangle \cap \langle h \rangle$ is trivial. So $G_n \cong \underbrace{\langle g \rangle}_{\mathbb{Z}/p\mathbb{Z}} \times \underbrace{\langle h \rangle}_{\cong \mathbb{Z}/n'\mathbb{Z}}$. Note that $p \nmid n'$ as otherwise there would be two different subgroups of order p, i.e. there would be two different extensions of F of degree $\frac{n}{p} = n'$. ■

□

1.3 Model Theory (of ACF)

[Lecture 04, 2024-10-18]

We'll use freely fundamental results from model theory (see [TZ12][2])

Theorem 1.21. Let T be a theory such that all finite $T_0 \subseteq T$ have a model. Then T has a model.

Proof. Use Gödel's completeness and the fact that proofs are finite. □

Theorem 1.22 (Łoś's Theorem)**.** Let $(M_i)_{i \in I}$ be a family of $\mathcal{L}$-sentences and $\mathcal{U}$ an ultrafilter on I.

Let $M := \prod_{i \to \mathcal{U}} M_i := \prod_{i \in I} M_i /_{\sim_{\mathcal{U}}}$.

Let $\varphi(x_1, \ldots, x_n)$ be an $\mathcal{L}$-formula, $a_1, \ldots, a^n \in M$, say $a^j = (a_i^j)_{i \in I} / \sim_U$.

Then we have

$$M \models \varphi[\overline{a}] \iff \{i \in I | M_i \models \varphi[\overline{a_i}]\} \in \mathcal{U}.$$

This gives rise to an alternative, *semantic* proof of the Compactness Theorem (1.21), see [Poi00, Theorem 4.5].

Recall:

[2] A good reference, but somewhat too compact for learning the material for the first time. [Poi00] is a better introduction.

- If $\mathcal{L}$ is a first order language, M an $\mathcal{L}$-structure, $A \subseteq M$ a subset, $\mathcal{L}_A := \mathcal{L} \sqcup \{c_a | a \in A\}$, $M_A := (M, c_A^{M_A} := a)$.

  A set $\pi(x_1, \ldots, x_n)$ of $\mathcal{L}_A$-formulae in $x_1, \ldots, x_n$ is a **partial n-type** over A iff for all $\varphi_1, \ldots, \varphi_N \in \pi$

  $$M_A \models \exists \overline{x} \bigwedge \varphi_i(\overline{x})$$

  (π is finitely satisfiable).

  Note: By compactness, we find $N \succeq M$ and $\overline{b} \in N^n$ a realization of π, written $N \models \pi(\overline{b})$ or $\overline{b} \models \pi$, i.e. $N \models \varphi[\overline{b}]$ for all $\varphi \in \pi$.

- π is called **complete** if it is maximal finitely satisfiable ($\iff$ for every $\mathcal{L}_A$-formula $\varphi(\overline{x})$ either $\psi \in \pi$ or $\neg\psi \in \pi$.)

- $S_n(A) = S_n^M(A) :=$ the space of all complete n-types over A endowed with the **Stone topology**, with basic open (in fact clopen) sets of the form

  $$\langle \varphi \rangle := \{p \in S_n(A) | \varphi \in p\}$$

  where φ is an $\mathcal{L}_A$-formula. This is compact (by the Compactness Theorem (1.21)) and totally disconnected.

- Let $\kappa \geqslant |\mathcal{L}|$ be an infinite cardinal.

  Definition 1.22.14. An $\mathcal{L}$-structure M is **κ-saturated** if for every $A \subseteq M$, $|A| < \kappa$ every $p(x) \in S_1(A)$ is realized in M ($\implies$ every $p(\overline{x}) \in S_n(A)$ is realized in M).

  Notation 1.22.15. We write $\mathrm{tp}^M(\overline{a}/B) := \mathrm{tp}(\overline{a}/B) := \{\varphi(\overline{x}) \in \mathcal{L}_B | M \models \varphi[\overline{a}]\}$, the **type** of $\overline{a}$ over B.

  Here $B \subseteq M$, $\overline{a} \in M^n$ or even $\overline{a} \in M^I$, I infinite.

- Let $A \subseteq M, A' \subseteq M'$ and $f \colon A \to A'$ a bijection. Then f is called **partial elementary** iff it preserves all formulae, i.e. for every $\pi(x_1, \ldots, x_n)$ and all $a_1, \ldots, a_n \in A$ we have

  $$M \models \varphi[a_1, \ldots, a_n] \iff M' \models \varphi[f(a_1), \ldots, f(a_n)]$$

  iff $\mathrm{tp}^M(\overline{a}) = \mathrm{tp}^{M'}(f(\overline{a}))$ for all $\overline{a} \in A^n$

  iff $\mathrm{tp}^M(A) = \mathrm{tp}^{M'}(f(A))$ (where A is enumerated).

- M is **κ-strongly homogeneous** iff every partial elementary selfmap f of M with $|\operatorname{dom}(f)| < \kappa$ extends to some $\sigma \in \mathrm{Aut}(M)$.

  Fact 1.23. Given an $\mathcal{L}$-structure M and an infinite cardinal κ, there is $N \succeq M$ such that N is κ-saturated and κ-strongly homogeneous.

Remark 1.23.16. Much later in the course, we will call **monster model** of a complete theory T a κ-saturated, κ-strongly homogeneous model of T, where $\kappa \gg 0$. (Sometimes a class-sized model is used.)

Recall: An $\mathcal{L}$-theory T has **quantifier elimination** (**QE**) iff for any $\mathcal{L}$-formula $\varphi(x_1, \ldots, x_n)$, $n \geqslant 1$[3], there is a quantifier-free $\mathcal{L}$-formula $\psi(\overline{x})$ such that $T \models \forall \overline{x}.(\varphi \leftrightarrow \psi)$.

Theorem 1.24 (Criterion for QE)**.** For an $\mathcal{L}$-theory T the following are equivalent:

- T has QE.
- T is **substructure complete**, i.e. whenever $M, N \models T$ and A is a common substructure[a] of M and N, then $M_A \equiv N_A$.
- Let $\kappa := |T| = \max(|\mathcal{L}|, \aleph_0)$. Whenever $M, N \models T$, $|M| \leqslant \kappa$, N κ^+-saturated and $f\colon A \hookrightarrow N$ is an embedding of a substructure $A \leqslant M$, there exists $\tilde{f}\colon M \hookrightarrow N$ extending f.

[a] structures are non-empty!

Remark 1.24.17. There are several variants of (3), sometimes more adapted to a concrete situation.

Corollary 1.25. Let Δ be a set of $\mathcal{L}$-formulas and T and $\mathcal{L}$-theory. Suppose that every partial map between models of T that respects the formulas in Δ , i.e.

$$M \models \varphi[a_1, \ldots, a_n] \iff M' \models \varphi[f(a_1), \ldots, f(a_n)]$$

for all $\varphi \in \Delta$, is already elementary.

Then there is a boolean combination of formulas in Δ such that $T \models \forall \overline{x}(\varphi \leftrightarrow \psi)$.

Proof. Name toe formulas in Δ by new relation symbols, i.e. if $\delta(x_1, \ldots, x_n) \in \Delta$, introduce new $R_\delta(x_1, \ldots, x_n)$ and add an axiom $\forall \overline{x.(\delta_8 \overline{x})} \leftrightarrow R_\delta(\overline{x})$. Quantifier-free formulas in the expansion are boolean combinations of formulas in Δ. Now apply Theorem 1.24. □

[3] see [Poi00, section 5.3] for a discussion on the necessity of $n \neq 0$

1.3.1 Some Model Theory of ACF

We work in $\mathcal{L}_{\text{ring}} = \{0, 1, +, -, \cdot\}$. ACF is the $\mathcal{L}_{\text{ring}}$-theory of the algebraically closed fields.

Theorem 1.26. (1) ACF has QE.

(2) The completions are given by ACF_p, where $p \in \mathbb{P} \cup \{0\}$.

(3) Any ACF_p is **strongly minimal**, i.e. if $K \models \mathsf{ACF}$, every definable subset of K is finite or cofinite.

(4) If $A \subseteq K \models \mathsf{ACF}$, then $\operatorname{acl}(A) = (Q(\langle A \rangle)^{\text{alg}}$, where $\langle A \rangle$ denotes the ring generated by A, Q the field of fractions and $\cdot^{\text{alg}}$ the algebraic closure from algebra.

Proof. (1) We use Theorem 1.24 (3). Let $K, L \models \mathsf{ACF}$, K countable, L $\aleph_1$-saturated. Let $A \leqslant K$ be a substructure (i.e. a subring), $f\colon A \hookrightarrow L$ an embedding. We need to show that f extends to $\tilde{f}\colon K \hookrightarrow L$.

Step 1: f (uniquely) extends to $f_1\colon Q(A) \hookrightarrow L$. So wlog. A is a subfield.

Step 2: f extends (not necessarily uniquely) to $f_1\colon A^{\text{alg}} \hookrightarrow L$, so wlog. A is algebraically closed.

Step 3: If $A^{\text{alg}} \subsetneq K$, let $b \in K \backslash A$. Then b is transcendental over A, so $K(b) \cong K(X)$.

Choose $b' \in L \backslash f(A)$ (this is non-empty, as L is $\aleph_1$-saturated). Then b' is transcendental over $f[A]$, so $b \mapsto b'$ extends f.

Iterate these steps to get $\tilde{f}\colon K \hookrightarrow L$.

(2) Follows from (1) by substructure completeness, as $\mathbb{F}_p$ and $\mathbb{Z}$ are prime substructures for ACF_p resp. ACF_0.

(3) Let $\varphi(x)$ be a quantifier free $\mathcal{L}_{\text{ring}}$-formula. Let $K \models \mathsf{ACF}$. We need to show that $\varphi[K]$ is finite or cofinite.

φ is a boolean combination of atomic formulas and atomic formulas are equivalent to $p(X) = 0$, $p(X) \in K[X]$.

If $\deg(P) \geqslant 1$, $P(X) = 0$ defines a finite set of at most $\deg(P)$ many elements. If P is constant and non zero, the set defined is empty. If $P \equiv 0$, the set defined is K.

The set of sets which are finite or cofinite is stable under boolean combinations.

(4) "$\supseteq$" is clear.

For the other direction note that $(Q(\langle A \rangle))^{\text{alg}} \preceq K$, as $(Q(\langle A \rangle))^{\text{alg}} \models \mathsf{ACF}$, so it is acl-closed.

□

Corollary 1.27. [a]

Let $K \models \mathsf{ACF}_p$.

(1) If $\overline{a} \in K^n$, $k \subseteq K$, then $\mathrm{MR}(\overline{a}/k) := \mathrm{MR}(\mathrm{tp}(\overline{a}/k)) = \text{acl-dim}(\overline{a}/k) \overset{(1.26)(3)}{=} \mathrm{trdeg}(k(\overline{a})/k)$,

(2) **Additivity for MR**: $\mathrm{MR}(\overline{a}\overline{b}/c) = \mathrm{MR}(\overline{b}/c) + \mathrm{MR}(\overline{a}/c\overline{b})$.

(3) If $\mathcal{U} \succeq K$ is $|K|^+$-saturated, then for an $\mathcal{L}_{\mathrm{ring}}$-formula $\varphi(\overline{x})$ we get

$$\mathrm{MR}(\varphi) = \max\{\mathrm{trdeg}(K(\overline{a})/K) | \overline{a} \in \varphi[\mathcal{U}]\}.$$

(4) ACF_p **eliminates** $\exists^\infty$: For every $\mathcal{L}_{\mathrm{ring}}$-formula $\varphi(x, \overline{y})$, there is $n_\varphi \in \mathbb{N}$ such that in any $K \models \mathsf{ACF}_p$ for all $\overline{b} \in K^{|\overline{y}|}$:

$$\varphi(K, \overline{b}) \text{ is infinite} \iff |\varphi(K, \overline{b})| \geqslant n_\varphi$$

Thus $\exists^\infty x.\ \varphi(x, \overline{y}) :\iff \exists^{\geqslant n_\varphi} x.\ \varphi(x, \overline{y})$ [b] is first order expressible, as a formula in $\overline{y}$.

(5) MR is **definable in families**: Given an $\mathcal{L}_{\mathrm{ring}}$-formula $\varphi(\overline{x}, \overline{y})$ for every $h \in \mathbb{N}$ there is a formula $\chi_{\varphi,h}(\overline{y})$ such that for all $\overline{b} \in K^{|\overline{y}|}$, $K \models \mathsf{ACF}_p$,

$$\mathrm{MR}(\varphi(\overline{x}, \overline{b})) = h \iff K \models \chi_{\varphi,h}(\overline{b}).$$

[a] valid in all strongly minimal theories

[b] $\exists^{\geqslant n} x.\varphi(x)$ is a shorthand for

$$\exists x_1, \ldots, x_n.\ \bigwedge x_i \neq x_j \wedge \bigwedge \varphi(x_i).$$

Proof. (5) $\mathrm{MR}(\varphi(\overline{x}, \overline{b})) \geqslant k$ iff

$$\bigvee_{I \subseteq \{1,\ldots,n\}} \exists^\infty x_{i_1} \ldots \exists^\infty x_{i_k} \exists x_{I^c} \varphi(\overline{x}, \overline{b}).$$

□

Remark 1.28. Morley degree is also definable in ACF_p (we will do this later, it is more complicated). However this is not true in any strongly minimal theory!

Recall: $\mathrm{Spec}(k[X_1, \ldots, X_n]) = \{\varphi \leqslant k[\overline{X}] \text{ prime ideal}\}$.

QE in ACF yields:

Fact 1.29. The map $S_n(k) \to \operatorname{Spec}(k[X_1, \dots, X_n])$, $\operatorname{tp}(\overline{a}/k) \mapsto \{f(\overline{x}) \in k[\overline{x}] | f(\overline{a}) = 0\}$ is a bijection with inverse given by

$$\mathfrak{p} \mapsto \operatorname{tp}(X_1 \mod \mathfrak{p}, \dots, X_n \mod \mathfrak{p}/k),$$

where $k[\overline{X}]/\mathfrak{p} \subseteq L \models \mathsf{ACF}$.

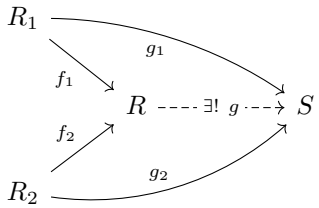
1.4 Some Commutative Algebra and Elementary Algebraic Geometry

[Lecture 05, 2024-10-22]

Tensor product of commutative k-algebras Let $k$be a field. A **commutative k-algebra** is a commutative ring R with a ring homomorphism $i\colon k \to R$.

Remark 1.29.18. The commutative k-algebras form a category, where a morphisms are ring homomorphisms compatible with the maps $i_j\colon k \to R_j$.

Fact 1.30. The category of commutative k-algebras has coproducts: Given two k-algebras R_1,R_2 there is a k-algebra R and morphisms $f_i\colon R_i \to R$ for $i = 1, 2$ satisfying the following universal property:



For any k-algebra homomorphism $g_i\colon R_i \to S$, $i = 1, 2$, there is a unique homomorphism $g\colon R \to S$ such that $g \circ f_i = g_i$, $i = 1, 2$.

R is determined by the universal property up to unique isomorphism. It is denoted by $R_1 \otimes_k R_2$.

Proof. R_j is a k-vector space via i_j, $j = 1, 2$. Let $R := R_1 \otimes_k R_2$ be the tensor product as k-vector spaces.

Recall that if $\mathfrak{B}_j$ is a k-basis of R_j, then a k-basis of R is given by $(b^1 \otimes b^2)_{\substack{b_1 \in \mathfrak{B}_1 \\ b^2 \in \mathfrak{B}_2}}$.

Now assume $1 \in \mathfrak{B}_j$ (if $R_j = (0)$, set $R := (0)$).

The multiplication on R is defined as follows:

Given $b^1, c^1 \in \mathfrak{B}_1$, $b^2, c^2 in \mathfrak{B}_2$ let

$$b^1 c^1 = \sum_{b_i^1 \in \mathfrak{B}_1} \alpha_i b_i^1$$

$$b^2 c^2 = \sum_{b_j^2 \in \mathfrak{B}_2} \beta_j b_j^2$$

for some $\alpha_i, \beta_j \in k$. Set

$$(b^1 \otimes b^2) \cdot (c^1 \otimes c^2) := \sum_{i,j} \alpha_i \beta_j (b_i^1 \otimes b_j^2).$$

Extend this map bilinearly to $\cdot \colon R \times R \to R$. Define $k \to R, 1 \mapsto (1 \otimes 1)$. One verifies:

(i) $\cdot$ is commutative,

(ii) $\cdot$ is distributive,

(iii) $\cdot$ is associative,

(iv) together with $f_j \colon R_j \to R$, $f_1(b_i^1) := b_i^1 \otimes 1$, $f_2(b_i^2) := 1 \otimes b_i^2$ (extended k-linearly) R is a commutative k-algebra, the f_j are morphisms and (R, f_1, f_2) has the universal property of the coproduct.

(Exercise) □

Corollary 1.31. If R_1, R_2 are k-algebras and $\sigma_j \in \mathrm{Aut}_k(R_j)$, $j = 1, 2$, then there exists a unique $\sigma \in \mathrm{Aut}_($ $R_1 \otimes_k R_2)$ such that $f_j \circ \sigma_j = \sigma \circ f_j$.

Proof. Use the universal property. □

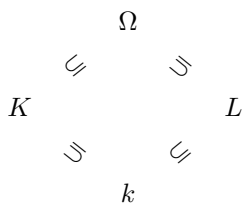
Example* 1.31.19.

(1) Let $R_1 = k[X_1, \ldots, X_n]$, R_2 arbitrary. Then $R_1 \otimes_k R_2 \cong_k R_2[X_1, \ldots, X_n]$.

(2) $\mathbb{C} \otimes_R \mathbb{C} \cong \mathbb{C}[X]/(X^2 + 1) \cong \mathbb{C}[X]/X - \mathbf{i} \times \mathbb{C}[X]/X + \mathbf{i} \cong \mathbb{C} \times \mathbb{C}$, so the tensor product of integral domains need not be an integral domain.

In the notes, this is example 1.32, but there also exists lemma 1.32

Linear disjointness in fields Consider field extensions



Definition 1.31.20. K is **linearly disjoint (l.d.) from L over k** iff any k-linearly independent family $(x_1, \dots, x_n)$ from K is L-linearly independent.

Notation 1.31.21. $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$

improve typesetting

Lemma 1.32. (1) Let $\mathfrak{B}$ be a k-basis of K. Then $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$ iff $\mathfrak{B}$ is linearly independent over L.

(2) Let $R \subseteq K$ and $S \subseteq L$ be subrings such that $Q(R) = K$, $Q(S) = L$. Then $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$ iff for any k-linearly independent family $(r_1, \dots, r_n)$ from R there are no $(s_1, \dots, s_n) \in S^n \backslash \{0\}$ such that $\sum_{i=1}^n s_i r_i = 0$.

Proof. Easy exercise. □

Fact 1.33. For $K \supseteq k \subseteq L \subseteq M$ all contained in Ω, one has

(1) $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} M$ iff $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$ and $KL \overset{\text{l.d.}}{\underset{L}{\downarrow}} M$, where KL denotes the field compositum.[a]

(2) $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$ iff $L \overset{\text{l.d.}}{\underset{k}{\downarrow}} K$.

[a] $KL \coloneqq K(L) = L(K)$

Proof. (1) $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} M \implies K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$ is clear and $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} M \implies KL \overset{\text{l.d.}}{\underset{L}{\downarrow}} M$ follows from Lemma 1.32 as $KL = Q(L[K])$ and $L[K]$ has an L-basis of elements from K.

" $\Longleftarrow$ " is clear from the definitions.

(2) Assume $L \overset{\text{l.d.}}{\underset{k}{\downarrow}} K$. Let $y_1, \dots, y_n \in L$ be k-linearly independent and $x_1, \dots, x_n \in K$ not all 0 such that $\sum x_i y_i = 0$ $(*)$. We may assume that $x_1, \dots, x_r$ are K-linearly independent and

$$x_i = \sum_{\mu=1}^{r} \alpha_{i,\mu} x_\mu$$

for $i = r+1, \dots, n$, $\alpha_{i,\mu} \in k$. In particular $r \geqslant 1$. From $(*)$ we obtain

$$\sum_{\mu=1}^{r} x_\mu y_\mu + \sum_{i=r+1}^{n} \left(\sum_{\mu=1}^{r} \alpha_{i,\mu} x_\mu \right) y_i = 0$$

$$\implies \sum_{\mu=1}^{r} \underbrace{\left(y_\mu + \sum_{i=r+1}^{n} \alpha_{i,\mu} y_i \right)}_{\neq 0} x_\mu = 0,$$

so $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$.

□

Fact 1.34. The following are equivalent:

(1) $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$,

(2) $K[L] \cong_k K \otimes_k L$,

(3) $KL \cong_k Q(K \otimes_k L)$.

Proof (sketch). (1) $\implies$ (2) From the universal property, we get a morphism of k-algebras $K \otimes_k L \xrightarrow{\pi} K[L]$ which is surjective. If $\sum \alpha_{ij} (x_i \otimes y_j) \in \ker(\pi)$, then in $K[L]$ we get

$$\sum_j \left(\sum_i \alpha_{ij} x_i \right) y_j = 0,$$

so by $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$ we get

$$\sum \alpha_{ij} x_i = 0$$

for all j, so $\alpha_{ij} = 0$ for all i, j. (Here (x_i) and (y_j) are k-bases.)

The other directions are easy. □

Fact 1.35. (1) Let $k \subseteq K$, $L \subseteq k^{\text{alg}}$ with K/k and L/k finite. Then

$$K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L \iff [KL : k] = [L : k] \cdot [K : k].$$

If K/k is Galois, this is equivalent to $K \cap L = k$.

(2) Let K/k be algebraic and $L = k(X_1, \dots, X_n)$. Then in any common overfield $\Omega \supseteq K, L \supseteq k$ one has $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$.

(3) Assume K/k is such that $k^{\text{alg}} \cap K = k$, i.e. k is relatively algebraically closed in K, and let L/k be separable algebraic. Then

$K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L$.

Proof. We leave (1) and (2) as exercises.

(3) We may assume that L/k is finite, so by the primitive element theorem there is $\alpha \in L$ such that $L = k(\alpha) \cong k[X]/P(X)$ where $P(X) := \mathrm{MiPo}(\alpha/k)$. Then $P(X)$ is irreducible over K, so

$$[KL : K] = [K(\alpha) : K] = [k(\alpha) : k] = [L : k].$$

Indeed, let $Q(X) := \mathrm{MiPo}(\alpha/K) \in K[X]$. Then the coefficients of Q lie in $K \cap k^{\mathrm{alg}} = k$, so $Q = P$. □

Notation 1.35.22. For $k \subseteq K$, $L \subseteq \Omega$ we write $K \overset{\text{alg}}{\underset{k}{\downarrow}} L$ if K and L are algebraically independent over k, i.e. iff for any $K_0 \subseteq K$ finitely generated over k on has $\mathrm{trdeg}(K_0/k) = \mathrm{trdeg}(K_0L/L)$.

As algebraic closure defines a pregeometry (matroid) in every field (by Steinitz exchange), we easily obtain: add definition

Fact 1.36. For $k \subseteq K \subseteq \Omega$, $k \subseteq L \subseteq M \subseteq \Omega$ we have

(1) $K \overset{\text{alg}}{\underset{k}{\downarrow}} L \iff L \overset{\text{alg}}{\underset{k}{\downarrow}} K$,

(2) $K \overset{\text{alg}}{\underset{k}{\downarrow}} M \iff K \overset{\text{alg}}{\underset{k}{\downarrow}} L \wedge KL \overset{\text{alg}}{\underset{L}{\downarrow}} M$,

(3) $K \overset{\text{alg}}{\underset{k}{\downarrow}} M \leqslant K^{\mathrm{alg}} \overset{\text{alg}}{\underset{k^{\mathrm{alg}}}{\downarrow}} M^{\mathrm{alg}}$.

Fact 1.37. For $k \subseteq K, L \subseteq \Omega$ we have

(1) $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} L \implies K \overset{\text{alg}}{\underset{k}{\downarrow}} L$.

(2) The converse does not always hold, e.g. $\mathbb{C} \overset{\text{l.d.}}{\underset{\mathbb{R}}{\not\downarrow}} \mathbb{C}$ but $\mathbb{C} \overset{\text{alg}}{\underset{\mathbb{R}}{\downarrow}} \mathbb{C}$.

Proof. (1) Suppose $K \overset{\text{alg}}{\underset{k}{\not\downarrow}} L$. Choose $x_1, \ldots, x_n \in k$ algebraically independent over k such that $x_n \in L(x_1, \ldots, x_{n-1})^{\mathrm{alg}}$. Then $k(x_1, \ldots, x_n) \overset{\text{l.d.}}{\underset{k(x_1,\ldots,x_{n-1})}{\not\downarrow}} L(x_1, \ldots, x_{n-1})$ as $1, x_n, x_n^2, \ldots$ are linearly independent over $k(x_1, \ldots, x_{n-1})$ but not over $L(x_1, \ldots, x_{n-1})$. This contradicts Fact 1.33.

□

Remark 1.38. k is relatively algebraically closed in $k(X_1, \dots, X_n)$ (induction on n).

Regular field extensions A context whose things behave very nicely in algebra and algebraic geometry:

Definition 1.38.23. A field extension K/k is called **regular** if $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} k^{\text{alg}}$ (in $\Omega = K^{\text{alg}}$).

Remark 1.38.24. K/k is regular iff for every $k \subseteq K_0 \subseteq K$ with K_0/k finitely generated one has that K_0/k is regular.

Proposition 1.39. Let K/k be regular. Then the restriction map $\text{res}\colon \text{Gal}(K) \twoheadrightarrow \text{Gal}(k)$ is surjective.

Proof. We have $K^{\text{alg}} \supseteq Kk^{\text{alg}} = K[k^{\text{alg}}] \overset{(1.34)}{\cong} K \otimes_k k^{\text{alg}}$. By Corollary 1.31 $\sigma \in \text{Gal}(k)$ comes from $\tilde{\sigma} \in \text{Aut}_k(K[k^{\text{alg}}])$ such that $\tilde{\sigma}|_K = \text{id}_K$. So $\tilde{\sigma}$ lifts to $\tilde{\tilde{\sigma}} \in \text{Gal}(K)$ with $res\left(\tilde{\tilde{\sigma}}\right) = \sigma$. □

Definition 1.39.25. A field extension K/k is called **separable** if $\text{char}(K) = 0$ or $\text{char}(K) = p > 0$ and $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} k^{\frac{1}{p}}$, where

$$k^{\frac{1}{p}} = \{x \in k^{\text{alg}} | x^p \in k\} = \text{Frob}_p^{-1}(k) \subseteq k^{\text{alg}}.$$

(Note that $K \overset{\text{l.d.}}{\underset{k}{\downarrow}} k^{\frac{1}{p}} \iff K \overset{\text{l.d.}}{\underset{k}{\downarrow}} k^{\frac{1}{p^\infty}}$, where $k^{\frac{1}{p^\infty}} := \bigcup k^{\frac{1}{p^n}}$.)

Proposition 1.40. For a field extension K/k the following are equivalent:

(1) K/k is regular,

(2) $K \otimes_k k^{\text{alg}}$ is an integral domain (thus a field),

(3) k is relatively algebraically closed in K and K/k is separable.

Proof. Later (or [Lan73]) □

Proposition 1.41 (Mac Lane)**.** For a field extension K/k the following are equivalent

(1) K/k is separable,

(2) every finitely generated subextension $k \subseteq K_0 \subseteq K$ is separable (i.e. K_0/k is separable),

(3) every finitely generated subextension K_0/k is **separably generated** over k, i.e. there is a transcendence basis $x_1, \ldots, x_n$ of K_0/k such that $K_0/k(x_1, \ldots, x_n)$ is separable algebraic.

Proposition 1.42. (1) If L/k is regular and $L \supseteq K \supseteq k$, then K/k is regular.

(2) If L/K is regular and K/k is regular, then L/k is regular.

(3) If $k = k^{\mathrm{alg}}$, then every K/k is regular.

Proof. Clear from the definitions and elementary reasoning. □

Corollary 1.43. If k is perfect, then K/k is regular iff $K \cap k^{\mathrm{alg}} = k$.

[Lecture 06, 2024-10-25]

Theorem 1.44. Let K/k be regular and L/k arbitrary such that $K \overset{\mathrm{alg}}{\underset{k}{\downarrow}} L$. Then

(1) $K \overset{\mathrm{l.d.}}{\underset{k}{\downarrow}} L$ and

(2) KL/L is regular.

Proof. (1) later (or see [Lan73] or do it as an exercise).

(2)

$$\begin{aligned} K \overset{\mathrm{alg}}{\underset{k}{\downarrow}} L &\implies K \overset{\mathrm{alg}}{\underset{k}{\downarrow}} L^{\mathrm{alg}} \\ &\overset{(1)}{\implies} K \overset{\mathrm{l.d.}}{\underset{k}{\downarrow}} L^{\mathrm{alg}} \\ &\overset{(1.33)}{\implies} KL/L \text{ regular} \end{aligned}$$

□

Corollary 1.45. Let K/k be regular and L/k regular such that $K \overset{\mathrm{alg}}{\underset{k}{\downarrow}} L$. Then KL/k is regular.

Proof. By Theorem 1.44 (2) and Proposition 1.42 (2). □

Algebraic sets and varieties Fix $K \subseteq \Omega \models \mathsf{ACF}$ with $\mathrm{trdeg}(\Omega/K)$ infinite. By QE in ACF all types over $A = K(\overline{a})$ for $\overline{a} \in \Omega$ finite are realized in Ω. Consider affine n-space $\Omega = \mathbb{A}^n(\Omega)$

Definition 1.45.26.

- For $S \subseteq K[X_1, \ldots, X_n]$ let
$$V(S) := V_\Omega(S) := \{\overline{a} \in \Omega^n | \forall f \in S.\ f(\overline{a}) = 0\},$$
called the **algebraic set defined by S**.
- For $Y \subseteq \Omega^n$ set
$$I(Y) := I_K(Y) := \{f \in K[\overline{X}] | \forall \overline{a} \in Y.\ f(\overline{a}) = 0\},$$
called the **ideal (over K) associated to Y**.

Remark 1.45.27. If $I = \langle S \rangle = \langle f_1, \ldots, f_l \rangle \leqslant K[X_1, \ldots, X_n]$ is the ideal generated by S, then $V(S) = V(I) = V(\{f_1, \ldots, f_l\})$.

Proposition 1.46.
(1) Let $I \leqslant K[\overline{X}]$ be an ideal. Then $I(V(I)) \supseteq I$ and $I(V(I))$ is a **radical ideal**, i.e. it coincides with $\sqrt{I(V(I))}$, where $\sqrt{J} := \{f \in K | \exists n \in \mathbb{N}_+.\ f^n \in J\}$. Furthermore $V(I(V(I))) = V(I)$
(2) Let $Y \subseteq \Omega^n$. Then $V(I(Y)) \supseteq Y$ and $I(V(I(Y))) = I(Y)$.
(3) If $V, W \subseteq \Omega$ are K-algebraic sets and $I = I(V)$, $J = I(W)$, then $V \supseteq W$ iff $I \subseteq J$, in particular $I = J$ iff $V = W$.

Proof. Easy. □

For $k \subseteq \Omega$ and an algebraic subsets $W \subseteq \Omega^n$, a **k-rational point** is some $\overline{a} \in W$ such that $a_1, \ldots, a_n \in k$. Let $W(k)$ denote the set of k-rational points of W.

Theorem 1.47 (Hilbert's Nullstellensatz)**.** Let $I \leqslant K[X_1, \ldots, X_n]$ be an ideal and $V := V(I)$.

(1) *Weak form*: Assume that $K \models \mathsf{ACF}$.
   (a) If I is proper, there is $\overline{a} \in V(K)$.
   (b) If $I = \mathfrak{m}$ is maximal, then $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$ for some $a_1, \ldots, a_n \in K$.
(2) *Strong form*: If $f \in K[\overline{X}]$ is 0 on $V(K^{\mathrm{alg}})$, then there exists $n \geqslant 1$ such that $f^n \in I$. In particular
$$I(V(I)) = \sqrt{I}.$$

Proof. (1) $(b) \implies (a)$ is clear, as every ideal is contained in a maximal one.

(b): Consider $K[\overline{X}]/\mathfrak{m} \hookrightarrow \Omega$. The image of $\overline{X} \pmod{\mathfrak{m}}$ is a solution in Ω. As $K \preceq \Omega$ and $\mathfrak{m} = \langle f_1, \dots, f_l \rangle$ for finitely many $f_i \in K[\overline{x}]$ (since $K[\overline{X}]$ is Noetherian by Hilbert's basis theorem), $K \models \exists \overline{x}. \bigwedge f_i(\overline{x}) = 0$. Thus there is $\overline{a} \in K^n$ as claimed.

(2) Let f be as in the statement, i.e. $f|_{V(K^{\mathrm{alg}})} = 0$ and let Y be a new variable. Consider

$$J \coloneqq \langle I, 1 - Y \cdot f \rangle \subseteq K[\overline{X}, Y]$$

and $W \coloneqq V(J)$. By assumption $W(K^{\mathrm{alg}}) = \varnothing$, so by (1) we have $J = K[\overline{X}, Y]$. Thus there are $g_1, \dots, g_l, g \in K[\overline{X}, Y]$ such that

$$1 = \sum_{i=1}^{l} g_i f_i + g \cdot (1 - Yf)$$

Work in $K(\overline{X})$ via the map

$$\begin{aligned} K[\overline{X}, Y] &\longrightarrow K(\overline{X}) \\ X_i &\longmapsto X_i \\ Y &\longmapsto \frac{1}{f}. \end{aligned}$$

We get $1 = \sum_{i=1}^{l} \frac{h_i}{f^{n_i}} f_i$ for $n_i \geqslant 0$ and some $h_i \in K[\overline{X}]$. Setting $n \coloneqq \max_i n_i$ we obtain $f^n = \sum_{i=1}^{l} (h_i f^{n-n_i}) f_i \in I$.

□

Corollary 1.48. $I(\cdot)$ defines a $\subseteq$-reversing bijection

$$\{K\text{-algebraic subsets of } \Omega^n\} \leftrightarrow \{\text{radical ideals of } K[\overline{X}]\}$$

with inverse $V(\cdot)$

Corollary 1.49. Two K-algebraic subsets of Ω are equal iff they have the same K^{alg}-rational points. In particular, we get a bijection between the set of radical ideals of $K[\overline{X}]$ and K-algebraic subsets of $(K^{\mathrm{alg}})^n$.

Corollary 1.50. There is no infinite strictly descending chain of algebraic subsets of Ω^n.

Proof. $K[\overline{X}]$ is Noetherian. □

Theorem 1.51. The K-algebraic subsets are the closed subsets of a Noetherian topology on Ω^n. Similarly, the sets $V(K)$ for a V a K-algebraic subset of Ω^n form the closed subsets of a Noetherian topology on K^n

It is called the **Zariski topology** (over K).

Proof. Let $I, J \leqslant K[\overline{X}]$ be radical ideals, $V := V(I)$, $W := V(J)$. Clearly $V \cap W = V(\langle I, J\rangle)$. More generally

$$\bigcap_{i\in A} V(I_i) = V(\langle I_i | i \in A\rangle)$$

which moreover is equal to a finite subintersection $\bigcap_{i\in A_0} V(I_i)$ by Noetherianness.

Claim 1. $V \cup W = V(I \cdot J)$.

Subproof. "$\subseteq$ " is trivial. "$\supseteq$": if $\overline{a} \in V(I \cdot J)\backslash V$, then there exists $f \in I(V)$ such that $f(\overline{a}) \neq 0$. Let $g \in I(W)$ be arbitrary. Then $f \cdot g \in I \cdot J$, so

$$0 = (f \cdot g)(\overline{a}) = \underbrace{f(\overline{a})}_{\neq 0} \cdot g(\overline{a})$$
$$\implies g(\overline{a}) = 0 \implies \overline{a} \in W.$$

■

□

Definition 1.51.28. A K-algebraic set V is an (affine) **K-variety** if it is irreducible in the Zariski topology (over K), i.e. iff there are no proper K-algebraic subsets $W, Z \subsetneq V$ such that $W \cup Z = V$.

Fact 1.52. For a K-algebraic subset $V \subseteq \Omega^n$ the following are equivalent

(1) V is a K-variety,

(2) $V(K^{\mathrm{alg}})$ is irreducible in the Zariski topology over K,

(3) $I(V) \leqslant K[\overline{X}]$ is a prime ideal.

Proof. (1) $\implies$ (2) is clear.

(2) $\implies$ (3): Let $f, g \in I(V)$ with $f, g \notin I(V)$. Then $V(\langle I(V), f\rangle) =: V_1$, $V(\langle I(V), g\rangle) =: V_2$ satisfy $V_i \subsetneq V$ and $V_1 \cup V_2 = V$, similarly on K^{alg}-rational points, so $V(K^{\mathrm{alg}})$ is not irreducible.

(3) $\implies$ (1):

Suppose (1) fails. Let $V = V_1 \cup V_2$ and take $f \in I(V_1)\backslash I(V)$, $g \in I(V_2)\backslash I(V)$. Then $fg \in I(V)$ $\lightning$. □

Theorem 1.53. If $V \subseteq \Omega^n$ is a K-algebraic set, then there are K-varieties $V_1, \dots, V_r$ such that $V = \bigcup_{i=1}^r V_i$. Moreover if $V_i \nsubseteq V_j$ for any $i \neq j$, then this decomposition is unique up to permutation and the V_i are called the **K-irreducible components**.

Proof. This holds in all Noetherian topological spaces. □

Remark 1.54. If $V = V(I) = \bigcup_{i=1}^r V_i$ is the irreducible decomposition of the K-algebraic set V into K-varieties, then $\mathfrak{p}_i := I(V_i) \leqslant K[\overline{X}]$ are the minimal prime ideals over I (and thus $\sqrt{I} = \bigcap_{i=1}^r \mathfrak{p}_i$).

Definition 1.54.29. Let $K = K^{\text{alg}} \subseteq \Omega$ and let $V \subseteq \Omega^n$ be a K-algebraic set. For a subfield $k \subseteq K$ we say V is **defined over k** if there are $f_1, \dots, f_r \in k[\overline{X}]$ generating $I(V)$.

Note. *V is defined over k iff $I(V)$ has a basis as a K-vector space from $I(V) \cap k[\overline{X}]$.*

Theorem 1.55 (Weil)**.** Let K be algebraically closed and let V be a K-algebraic subset of Ω^n,. Then there is a smallest field of definition $k_0 \subseteq K$ for V, i.e.

(i) V is defined over k_0

(ii) whenever V is defined over k for some $k \subseteq K$, then $k_0 \subseteq k$.

Proof. For $\mu \in \mathbb{N}^n$ set $X^\mu := \prod_{i=1}^n X_i^{\mu_i}$. Then $(X^\mu)_{\mu \in \mathbb{N}}$ forms a K-basis of $K[\overline{X}]$.

Let $\mathfrak{B} := (b_\mu = X^\mu \pmod{I(V)})_{\mu \in \mathfrak{B}}$ be a K-basis of $K[\overline{X}]/I(V)$. For $\nu \in \mathbb{N}^n$ we may write

$$X^\nu = \sum_{\mu \in \mathfrak{B}} a_{\nu,\mu}^\mu \mod I(V)$$

for unique $a_{\nu,\mu} \in K$.

Claim 1. *$k_0 := \mathbb{F}(a_{\nu,\mu})_{\nu,\mu \in \mathbb{N}}$ works, where $\mathbb{F}$ is the prime subfield of K.*

Subproof. (i) The $f_\nu := X^\nu - \sum_{\mu \in B} a_{\nu,\mu} X^\mu$ for $\nu \in \mathbb{N}^n$ generate $I(V)$ by construction.

(ii) Exercise in linear algebra, see [Lan73, Chapter II].

■

□

Remark 1.56. $k_0/\mathbb{F}$ is finitely generated, as if $f_1, \dots, f_l \in k[\overline{X}]$ with $I(V) = \langle f_1, \dots, f_l \rangle$, then $k_0 \subseteq \mathbb{F}(\text{coefficients of } f_1, \dots, f_l) =: k$ and $k/k_0/\mathbb{F}$ with $k/\mathbb{F}$ finitely generated.

(Exercise: A subextension of a finitely generated extension is finitely generated.)

Coordinate rings, rational function field, generic points

Notation 1.56.30. For $k \subseteq \Omega$ and $\overline{a} \in \Omega^n$ we set

- $I(\overline{a}/k) := \{f(\overline{x}) \in k[\overline{X}] : f(\overline{a}) = 0\}$ (a prime ideal by Fact 1.29).
- $\mathrm{loc}(\overline{a}/k) := V(I(\overline{a}/k))$ is a k-variety, the **locus of $\overline{a}$ over k**.
- If V is a k-algebraic set, $k[V] := {}^{k[\overline{X}]}\!/_{I(V)}$ is called the **coordinate ring of V**.
- If V is a k-variety, $k(V) := Q(k[V])$ is called the **field of rational functions on V**.
- If V is a k-variety, $\dim(V) := \mathrm{trdeg}(k(V)/k)$.
- If V is a k-algebraic set with decomposition $V = \bigcup_{i=1}^{r} V_i$ into irreducible k-varieties, $\dim(V) := \max(\dim(V_i))$.

Fact 1.57. Let $\mathfrak{p} \subseteq b[\overline{X}]$ be a prime ideal. Then all maximal chains $\mathfrak{p} = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_l \leqslant k[\overline{X}]$ with $\mathfrak{p}_i$ prime ideals have the same length l, which is equal to $\mathrm{trdeg}(Q(k[\overline{X}]/\mathfrak{p})/k)$.

In particular, a proper k-algebraic subset of a k-algebraic variety V has strictly smaller dimension than V.

Theorem 1.58. Let $V \subseteq \Omega^n$ be a k-variety. Then

$$\dim(V) = \max_{\overline{a} \in V(\Omega)} \{\mathrm{trdeg}(k(\overline{a})/k)\}$$

and for every $\overline{a} \in V(\Omega)$ one has $\mathrm{trdeg}(k(\overline{a})/k) = \dim(V)$ iff the map $X_i \mapsto a_i$, $i = 1, \dots, n$, induces a k-isomorphism $k(V) \cong k(\overline{a})$.

Proof. Recall that $\mathrm{trdeg}(\Omega/k) = \infty$. A morphism $k(V) \overset{\iota}{\hookrightarrow} \Omega$ exists by the

assumption on transcendence degree, as Ω is algebraically closed.

Let $\overline{a}' \in V$. Then $\mathrm{loc}(\overline{a}'/k) \subseteq V$, as $I(\overline{a}'/k) \supseteq I(V)$.

The easy proof is left as an exercise. □

Terminology 1.58.31. $\overline{a} \in V$ with $\mathrm{loc}(\overline{a}/k) = V$ is called **generic in V over k** or a **generic point of V over k**.

Question 1.58.32. Let $\mathfrak{p} \subseteq k[\overline{X}]$ be a prime ideal. When does $I := \mathfrak{p}K[\overline{X}]$ for $k \subseteq K = K^{\mathrm{alg}} \subseteq \Omega$, define a prime ideal?

Let $V := V(\mathfrak{p})$, so $k[V] = k[\overline{X}]/\mathfrak{p}$, $k(V) = Q(k[V])$.

Proposition 1.59. $I = \mathfrak{p}K[\overline{X}]$ for $k \subseteq K = K^{\mathrm{alg}}$ is a prime ideal iff $k(V)/k$ is regular. In particular if V is a K-algebraic set which is defined over k and k-irreducible, then V is K-irreducible iff $k(V)/k$ is regular.

[Lecture 07, 2024-10-29]

Definition 1.59.33. Let V be a k-variety, i.e. a k-irreducible algebraic set. Then V is called **absolutely irreducible** iff it is k^{alg} irreducible.

Remark 1.60. By Proposition 1.59, a k-variety is absolutely irreducible iff for every $K \supseteq k$, V is K-irreducible. This explains the terminology.

2 The Theory Psf′

Definition 2.0.34. A field F is called **pseudofinite** iff it satisfies the following conditions:

(P1) F is perfect.

(P2) For every $n \geqslant 1$, F has a unique algebraic extension F_n of degree n (inside a fixed algebraic closure).[a]

(P3) Every absolutely irreducible variety defined over F has an F-rational point.

[a] Equivalenty - under (P1) - $\mathrm{Gal}(F) \cong \hat{\mathbb{Z}}$, by Proposition 1.20

Definition 2.0.35. A field satisfying (P3) is called **pseudo algebraically closed** (**PAC**).

Theorem 2.1. There is an $\mathcal{L}_{\text{ring}}$-theory, called Psf′, which axiomatizes the class of all pseudofinite fields.

Proof. (See Comment 0.4)

(P1) is first order expressible: For every $p \in \mathbb{P}$ we add an axiom of the form

$$\chi_p :\equiv \underbrace{1 + 1 + \ldots + 1}_{p \text{ times}} = 0 \to \forall x.\ \exists y.\ y^p = x$$

Modulo (P1), (P2) is equivalent to a field F having exactly one extension F_n of degree n, in some fixed algebraic closure, and F_n/F is separable, so $F_n = F(\alpha)$ for some α. For every $n \geqslant 1$ we add an $\mathcal{L}_{\text{ring}}$-sentence ψ expressing the following:

There are $y_0, \ldots, y_{n-1} \in k$ such that

(i) $P(X) = X^n + y_{n-1}X^{n-1} + \ldots + y_1 X + y_0$ is irreducible in $k[X]$.

(ii) Whenever $Q(X) = X^n + z_{n-1}X^{n-1} + \ldots + z_1 X + z_0$ is irreducible in $k[X]$, there are $q_1, \ldots, q_n \in L := k[X]/P(X)$ such that $Q(X) = (X - q_1) \cdot \ldots \cdot (X - q_n)$.

To see this, one uses an $\mathcal{L}_{\text{ring}}$-formula $Irr_n(Y_0, \ldots, Y_{n-1})$ such that $k \models Irr_n(b_0, \ldots, b_{n-1})$ iff $X^n + b_{n-1}X^{n-1} + \ldots + b_0$ is irreducible in $k[X]$ and the fact that, uniformly in the coefficients of an irreducible polynomial $P(X) \in k[X]$ of degree n, the field $L := k[X]/P$ is interpretable in k. The interpretation uses the base set K^n, $O_L := (0, \ldots, 0)$, $1_L := (0, \ldots, 0, 1)$, componentwise addition and multiplication given by a K-bilinear map using the coefficients of $P(X)$ as parameters. The details are left as an exercise.

By the primitive element theorem, in perfect fields every finite extension is generated by a single element.

So modulo (P1) we axiomatize (P2).

The fact that (P3) is axiomatizable follows from the following fact and corollary. □

Fact 2.2 (Grete Hermann 1926; non-standard proof by van-den-Dries & Schmidt 1984)**.** Let $n, d \geqslant 1$ and $\overline{X} = (X_1, \ldots, X_n)$.

(A) There is a constant $A = A(n, d)$ such that for every field K, polynomials $f_1, \ldots, f_m, g \in K[\overline{X}]_{\leqslant d}$ if $g \in \langle f_1, \ldots, f_m \rangle$, then there are $h_1, \ldots, h_m \in K[\overline{X}]_{\leqslant A}$ such that $g = \sum_{i=1}^m h_i f_i$.

Here $K[\overline{X}]_{\leqslant d}$ denotes the finite-dimensional K-linear subspace of $K[\overline{X}]$ given by the polynomials of total degree $\leqslant d$.

(B) There is $B = B(n, d)$ such that for every field K and $f_1, \ldots, f_m, g \in$

$K_{\leqslant d}$ if there exists $k \in \mathbb{N}$ such that $g^k \in \langle f_1, \ldots, f_m \rangle$ then $g^B \in \langle f_1, \ldots, f_m \rangle$.

(C) There is a constant $C = C(n,d)$ such that for all ideals $I, J \leqslant K[\overline{X}]$ generated by elements from $K[\overline{X}]_{\leqslant d}$, the ideals $I \cap J$ and $J : I := \{f \in K[\overline{X}] | fI \subseteq J\}$ are generated by elements from $K[\overline{X}]_{\leqslant C}$.

(D) There is a constant $D = D(n,d)$ such that for every field K and ideal $I \leqslant K[\overline{X}]$ generated by elements from $K[\overline{X}]_{\leqslant d}$ which is no prime, there are $g, h \in K[\overline{X}]_{\leqslant D}$, $g, h \notin I$ such that $g \cdot h \in I$.

(E) There is a constant $E = E(n,d)$ such that for every field K and $I \leqslant K[\overline{X}]$ generated by elements from $K[\overline{X}]_{\leqslant d}$ there are at most E minimal prime ideals over I, and they are all generated by elements from $K[\overline{X}]_{\leqslant E}$.

For $n, d \in \mathbb{N}$ there are $N_n(d)$ monomials in $\overline{X} = (X_1, \ldots, X_n)$ of total degree $\leqslant d$. Choosing these monomials as a basis of the K-vector space $K[\overline{X}]_{\leqslant d}$, every $f \in K[\overline{X}]_{\leqslant d}$ corresponds to an $N_n(d)$-tuple $\overline{b} \in K^{N_n(d)}$ via

$$f = \sum_{i=1}^{N_n(d)} b_i m_i,$$

where $(m_i)_i$ is an enumeration of these monomials. Every ideal $I \leqslant K[\overline{X}]$ generated by elements of $K[\overline{X}]_{\leqslant d}$ may be generated by $N_n(d)$ many elements from $K[\overline{X}]_{\leqslant d}$, so we get the following:

Corollary 2.3. (1) Given $n, d \geqslant 1$, there is a quantifier-free $\mathcal{L}_{\text{ring}}$-formula

$$\varphi_{n,d}(X_1, \ldots, X_n, (y_{ij})_{1 \leqslant i,j \leqslant N(d)})$$

expressing

$$\bigwedge_{i=1}^{N_n(d)} f_i(\overline{X}) = 0,$$

where $f_i := \sum_{j=1}^{N_n(d)} y_{ij} m_j$.

So for every K-algebraic set $V = V(I)$ with $I \leqslant K[\overline{X}]$ generated by elements of $K[\overline{X}]_{\leqslant d}$ there is $\overline{b} \in k^{N_n(d) \times N_n(d)}$ such that $I = \langle f_1, \ldots, f_{N_n(d)} \rangle$, where $(f_1, \ldots, f_{N_n(d)})$ correspond to $\overline{b}$, and so $V(L) = \varphi_{n,d}[L, \overline{b}]$ for any $L \supseteq K$.

(2) For $\varphi_{n,d}$ as in (1) there is a quantifier free $\mathcal{L}_{\text{ring}}$-formula $\chi_{n,d}(\overline{y})$ such that for every field K and

$$\overline{b} \in K^{N_n(d) \times N_n(d)}$$

the ideal $\langle f_1, \dots, f_{N_n(d)} \rangle K^{\mathrm{alg}}[\overline{X}]$ is prime[a] iff $K \models \chi_{n,d}(\overline{b})$.

[a] so in particular $\varphi_{n,d}(\overline{X}, \overline{b})$ defines an absolutely irreducible variety

Proof. (1) is clear.

ad (2): By Fact 2.2 (A) and (D) there is an $\mathcal{L}_{\mathrm{ring}}$-formula $\tilde{\chi_{n,d}}(\overline{y})$ such that in any field K for $\overline{b} \in K^{N_n(d) \times N_n(d)}$ the corresponding ideal $\langle f_1, \dots, f_{N_n(d)} \rangle \leqslant K[X]$ is prime iff $K \models \tilde{\chi_{n,d}}(\overline{b})$.

Since ACF eliminates quantifiers, there is $\chi_{n,d}(y)$ quantifier free such that

$$\mathsf{ACF} \models \forall \overline{y} \left(\overline{\chi_{n,d}}(\overline{y}) \leftrightarrow \chi_{n,d}(\overline{y}) \right).$$

Then $\chi_{n,d}(\overline{y})$ is as desired, as for $\overline{b} \in K^{N_n(d) \times N_n(d)}$ one has

$$\begin{aligned} & K \models \chi_{n,d}(\overline{b}) \\ \text{iff } & K^{\mathrm{alg}} \models \chi_{n,d}(\overline{b}) \\ \text{iff } & \langle f_1, \dots, f_{N_n(d)} \rangle K^{\mathrm{alg}}[\overline{X}] \leqslant K^{\mathrm{alg}}[\overline{X}] \text{ is prime.} \end{aligned}$$

□

From Corollary 2.3 it follows that being PAC is $\mathcal{L}_{\mathrm{ring}}$-axiomatizable (by infinitely many $\mathcal{L}_{\mathrm{ring}}$-sentences) finishing the proof of Theorem 2.1.

Remark 2.3.36. We will not give a proof for Fact 2.2 but we will later give and alternative (effective) approach to show that being an absolutely irreducible variety is definable in parameters which his the only thing we used in the proof of Theorem 2.1.

Recall that if $M \subseteq N$ are $\mathcal{L}$-structures, then M is **existentially closed** (**e.c.**)in N iff for every quantifier free $\mathcal{L}(M)$-formula $\varphi(\overline{x})$ we have

$$N \models \exists \overline{x}.\ \varphi(\overline{x}) \implies M \models \exists \overline{x}.\ \varphi(\overline{x}).$$

$M \models T$ is existentially closed, iff it is existentially closed in every superstructure $N \models T$.

Proposition 2.4. For a field K the following are equivalent:

(1) K is PAC.

(2) For every absolutely irreducible K-variety V, $V(K)$ is Zariski dense in V, i.e. not contained in any proper algebraic subset $W \subsetneq V$.

(3) Let L/K be regular. Then K is e.c. in L.

Proof. (1) $\implies$ (2): Let V be an absolutely irreducible K-variety. Towards a contradiction assume that $V(K)$ is not Zariski dense in V. Then, working in K^{alg}, there is $f(\overline{X}) \in K^{\mathrm{alg}}[\overline{X}]$ vanishing on $V(K)$ but not on $V(K^{\mathrm{alg}})$. Multiplying f by all its conjugates and raising it to to some power p^N in case $\mathrm{char}(K) = p > 0$, we may assume $f(\overline{X}) \in K[\overline{X}]$, where $\overline{X} = (X_1, \ldots, X_n)$ and $V \subseteq \mathbb{A}^n$. Define a K-variety $U \subseteq \mathfrak{A}^{n+1}$ by the ideal $\langle I(V), 1 - X_{n+1} f \rangle \subseteq \mathfrak{B}$. U is absolutely irreducible and has the same function field as V. By construction $U(K) = \varnothing$, contradicting (1).

(2) $\implies$ (3): Let L/K be regular. We want to show that K is e.c. in L. For this we may assume that L/K is finitely generated, say $L = K(a_1, \ldots, a_n)$. Let $\varphi(\overline{x})$ be a quantifier-free $\mathcal{L}_{\mathrm{ring}}(K)$-formula such that $L \models \exists \overline{x}.\ \varphi(\overline{x})$.

We may assume that

$$\varphi(\overline{x}) \equiv \bigwedge_{i=1}^{m} f_i(\overline{x}) = 0 \wedge j(\overline{x}) \neq 0$$

for polynomials $f_1, \ldots, f_m, g \in K[\overline{X}]$. Indeed, if $\varphi \equiv \varphi_1 \vee \ldots \vee \varphi_n$, then $L \models \exists \overline{x}.\ \varphi_i$ for some i.

Using the same trick as before, adding a new variable, we see that $\exists \overline{x}.\ \varphi(\overline{x})$ is equivalent to

$$\exists \overline{X}, X_{n+1}.\ \bigwedge_{i=1}^{m} f_i(\overline{X}) = 0 \wedge X_{n+1} g(\overline{X}) = 1.$$

Thus we may assume $\varphi(\overline{x}) \equiv \bigwedge_{i=1}^{m} f_i(\overline{x}) = 0$.

Let $\overline{b} \in L^n$ such that $L \models \varphi[\overline{b}]$. Set $V := \mathrm{loc}(\overline{b}/K)$. Then $K(\overline{b}) = K(V)$ is a regular extension of K (as $K \subseteq K(\overline{b}) \subseteq L$) and so V is an absolutely irreducible variety. By construction $V \subseteq V(\langle f_1, \ldots, f_n \rangle)$. By (2) $V(K) \neq \varnothing$ and any $\overline{c} \in V(K)$ satisfies $\varphi(\overline{x})$.

(3) $\implies$ (1): Let V be an absolutely irreducible K-variety, $V \subseteq \mathbb{A}^n$. Then $K(V)/K$ is regular, so by (3) K is e.c. in $K(V)$. Let $\overline{a}$ be a generic point of V over K, so $K(V) = K(\overline{a})$, and let $f_1, \ldots, f_m \in K[\overline{X}]$ be such that $I(V) = \langle f_1, \ldots, f_n \rangle$. Then

$$K(V) = K(\overline{a}) \models \exists \overline{x}.\ \bigwedge_{i=1}^{m} f_i(\overline{x}) = 0,$$

so $K \models \exists \overline{x}.\ \bigwedge_{i=1}^{m} f_i(\overline{x}) = 0$, i.e. $V(K) \neq \varnothing$. □

[Lecture 08, 2024-11-05]

Corollary 2.5. Let L/K be regular and $F \supseteq K$ a PAC field which is $|L|^+$-saturated.

Then there exists $f\colon L \underset{K}{\hookrightarrow} F$ respecting K, i.e. $f|_K = \mathrm{id}_K$.

Proof. By saturation of F it suffices to show that any finitely generated ${}^{L_0}\!/_K$ such that $L_0 \subseteq L$ K-embeds into F.

Let $L_0 = K(\overline{a})$. Set $V := \mathrm{loc}(\overline{a}/K)$. This is absolutely irreducible as L_0/K is regular.

By Proposition 2.4 $V(F)$ is Zariski dense in V.

$\mathrm{qftp}_{\mathcal{L}_{\mathrm{ring}}}(\overline{a}/K)$ is finitely satisfiable in F as

$$\mathrm{qftp}(\overline{a}/K) = \{\overline{x} \in V, x \notin W \text{ for all } K\text{-algebraic sets } W \subsetneq V\}.$$

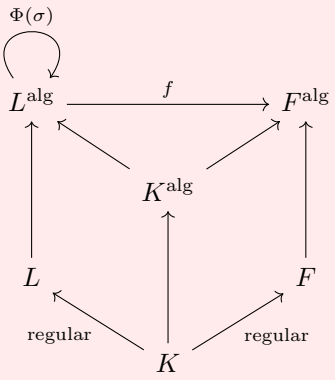
So by $|K|^+$-saturation of F, we find $\overline{b} \in F$ such that $\mathrm{loc}(\overline{b}/K) = V$, i.e. $\mathrm{qftp}(\overline{a}/K) = \mathrm{qftp}(\overline{b}/K)$, so $K(\overline{a}) = L_0 \hookrightarrow F, \overline{a} \mapsto \overline{b}$. □

To prove a quantifier reduction in Psf', we need a strengthening of Corollary 2.5 in certain cases, namely that ${}^{F}\!/_{f(L)}$ is regular (in specific cases).

Proposition 2.6 (Embedding Lemma)**.** Let $L^{\mathrm{alg}} \supseteq K^{\mathrm{alg}} \subseteq F^{\mathrm{alg}}$ with $L \supseteq K \subseteq F$ such that ${}^{L}\!/_K$ and ${}^{F}\!/_K$ are regular and K, F, L are perfect (equivalently, these fields are perfect, $K^{\mathrm{alg}} \cap L = K$ and $K^{\mathrm{alg}} \cap F = K$, see Corollary 1.43). Now assume that $F \models \mathsf{Psf}'$ and that F is $|L|^+$-saturated. Let $\Phi := \mathrm{Gal}(F) \twoheadrightarrow \mathrm{Gal}(L)$ be a continuous epimorphism wich respects K, i.e. $\forall \sigma \in \mathrm{Gal}(F).\ \sigma|_{K^{\mathrm{alg}}} = \Phi(\sigma)|_{K^{\mathrm{alg}}}$.[a] Then there is a K^{alg}-embedding $f\colon L^{\mathrm{alg}} \hookrightarrow F^{\mathrm{alg}}$ (with $f(L) \subseteq F$) such that

(i) f induces Φ, i.e. $\forall \sigma \in \mathrm{Gal}(F), a \in L^{\mathrm{alg}}.\ \sigma(f(a)) = f(\Phi(\sigma)(a))$ and

(ii) ${}^{F}\!/_{f(L)}$ is regular.



[a]It suffices to have this for topological generators.

Proof. Note: By regularity of L/K and F/K the restriction maps $\mathrm{Gal}(L) \twoheadrightarrow \mathrm{Gal}(K)$, $\mathrm{Gal}(F) \twoheadrightarrow \mathrm{Gal}(K)$ are surjective (see Proposition 1.39).

Let $\Omega \coloneqq Q(L \otimes_K F)^{\mathrm{alg}} = Q(L^{\mathrm{alg}} \otimes_{K^{\mathrm{alg}}} F^{\mathrm{alg}})^{\mathrm{alg}}$.

Working in Ω we thus have $L \overset{\text{l.d.}}{\underset{K}{\downarrow}} F$. Thus $\mathrm{Gal}(L^{\mathrm{alg}}F^{\mathrm{alg}}/LF) = \mathrm{Gal}(L) \times_{\mathrm{Gal}(K)} \mathrm{Gal}(F)$ [4] by the properties of $\otimes$ (Exercise).

Let $H \leqslant \mathrm{Gal}(L^{\mathrm{alg}}F^{\mathrm{alg}}/LF)$ be the closed subgroup given by the graph of Φ, i.e. $H = \{(\Phi(\sigma), \sigma) | \sigma \in \mathrm{Gal}(F)\}$. If σ_0 is a topological generator of $\mathrm{Gal}(F) \cong \hat{\mathbb{Z}}$, then $\tau_0 = (\Phi(\sigma_0), \sigma_0)$ is a topological generator of H, $\sigma_0 \mapsto \tau_0$ gives an isomorphism, and $\Phi(\sigma_0)$ is a topological generator of the (procyclic) group $\mathrm{Gal}(L)$.

Let $\tau \in \mathrm{Gal}(LF)$ be such that $\tau|_{L^{\mathrm{alg}}F^{\mathrm{alg}}} = \tau_0$ and set $M \coloneqq ((LF)^{\mathrm{alg}})^{\tau}$ be the fixed field of τ, so also the fixed field under $\overline{\langle \tau \rangle} \cong \hat{\mathbb{Z}}$.

By construction $\tau|_{L^{\mathrm{alg}}} = \Phi(\sigma_0)$ and $\tau|_{F^{\mathrm{alg}}} = \sigma_0$. So $M \cap L^{\mathrm{alg}} = L$ and $M \cap F^{\mathrm{alg}} = F$, so M/L and M/F are regular. Let F_n/F be the unique extension of degree n. Then as $M \overset{\text{l.d.}}{\underset{F}{\downarrow}} F^{\mathrm{alg}}$ (by regularity), $M_n \coloneqq MF_n$ is the unique extension of M of degree n (note that M is quasifinite) and $\mathrm{Gal}(M) \cong \mathrm{Gal}(F)$, since

$$\begin{array}{ccc} \mathrm{Gal}(M) & \xrightarrow[\text{res}]{} & \mathrm{Gal}(F) \\ \| \wr & & \| \wr \\ \hat{\mathbb{Z}} & \longrightarrow & \hat{\mathbb{Z}} \end{array}$$

is surjective, hence an isomorphism.[5]

Indeed $M^{\mathrm{alg}} = MF^{\mathrm{alg}} = M[F^{\mathrm{alg}}]$. Choose $M_0 \preceq M$ satisfying

[4]This denotes the **fiber product**, $\{(\sigma, \tau) \in \mathrm{Gal}(L) \times \mathrm{Gal}(F) | \sigma|_{K^{\mathrm{alg}}} = \tau|_{K^{\mathrm{alg}}}\}$.
[5]see Proposition 1.19 (2)

(a) $|M_0| \leqslant |L| + \aleph_0$,

(b) $L \subseteq M_0$ and there is $F_0 \preceq F$ such that $F_0 \subseteq M_0$ and $K \subseteq F_0$.

(c) $F^{\mathrm{alg}}[M_0] \supseteq L^{\mathrm{alg}}$.

As $F \subseteq F(M_0) \subseteq M$ and M/F is regular, Arguing as in the proof of Corollary 2.5 we find an F_0-embedding $f\colon M_0 \hookrightarrow F$. As $M_0 \overset{\text{l.d.}}{\underset{F_0}{\downarrow}} F_0^{\mathrm{alg}}$ (exercise; follows in various ways), f extends to an F_0^{alg}-embedding

$$\tilde{f}\colon M_0[F_0^{\mathrm{alg}}] \hookrightarrow F^{\mathrm{alg}}.$$

Note that $M_0[F_0^{\mathrm{alg}}]$ is algebraically closed, as $M_{0,n} = M_0 F_{0,n}$ for all n, $M_0[F_0^{\mathrm{alg}}]$ contains L, so it contains L^{alg}.

Claim 1. *$\tilde{f}|_{L^{alg}}\colon L^{alg} \hookrightarrow F^{alg}$ is as desired.*

Subproof. Indeed let $a \in L^{\mathrm{alg}}$, so $a = \sum_i m_i b_i$ for some $m_i \in M_0$, $b_i \in F_0^{\mathrm{alg}}$.

We compute

$$\begin{aligned} \Phi(\sigma_0)(a) &= \tau(a) \\ &= \sum \tau(m_i)\tau(b_i) \\ &\overset{\substack{\tau|_M = \mathrm{id}_M \\ \tau|_{F^{\mathrm{alg}}} = \sigma_0}}{=} \sum m_i \sigma_0(b_i). \end{aligned}$$

Since $\tilde{f}|_{F_0^{\mathrm{alg}}} = \mathrm{id}_{F_0^{\mathrm{alg}}}$, we get $\tilde{f}(\Phi(\sigma_0)(a)) = \sigma \tilde{f}(m_i)\sigma_0(b_i)$.

Also

$$\begin{aligned} \sigma_0(\tilde{f}(a)) &= \sigma_0(\sigma_i \tilde{f}(m_i) b_i) \\ &\overset{\tilde{f}(m_i) \in F}{=} \sum \tilde{f}(m_i)\sigma(b_i). \end{aligned}$$

So (i) holds for all $\sigma \in \mathrm{Gal}(F)$ (since we have shown it for the topological generator σ_0).

ad (ii): $\tilde{f}(L)$ is perfect. So we need to show $\tilde{f}(L)^{\mathrm{alg}} \cap F = \tilde{f}(L)$. Let $a \in L^{\mathrm{alg}}$ such that $\tilde{f}(a) \in F$. Then

$$\begin{aligned} & \sigma_0(\tilde{f}(a)) = \tilde{f}(a) \\ \iff\ & \tilde{f}(\Phi(\sigma)(a)) = \tilde{f}(a) \\ \overset{\tilde{f} \text{ injective}}{\iff}\ & \Phi(\sigma_0)(a) = a \\ \iff\ & a \in L. \end{aligned}$$

■

□

Lemma 2.7. Let $L_1, L_2 \supseteq K$ be arbitrary field extensions such that $L_1 \equiv_K L_2$. Then $l_1 \cap K^{\mathrm{alg}} \equiv_K L_2 \cap K^{\mathrm{alg}}$.

Proof. Note that if $L_2^* \succeq L_2$, then $L^{\mathrm{alg}} \cap L_2^* = K^{\mathrm{alg}} \cap L_2$ as $L_2^{\mathrm{alg}} \cap L_2^* = L_2$.

So we may assume that L_2 is $|L_1|^+$-saturated. Then there is an elementary K-embedding of L_1 into L_2 by universality of saturated models. Then f restricts to an isomorphism as claimed, since $f(L_1) \preceq L_2$

□

Proposition 2.8. Let K be a (perfect)[a] field, $K \subseteq F_1, F_2$, $F_i \models \mathsf{Psf}'$, F_i/K regular. Then $F_1 \equiv_K F_2$.

[a] This also follows from the other assumptions.

Proof. We may assume that F_2 is $|F_1|^+$-saturated. It is enough to find a K-embedding $f\colon F_1 \hookrightarrow F_2$ such that $F_2/f(F_1)$ is regular. Then id_K sits in a back-and-forth system given by partial isomorphisms between relatively algebraically closed subfields.

Let $\sigma_1 \in \mathrm{Gal}(F_1)$ be a topological generator of $\mathrm{Gal}(F_1)$ and $\sigma_0 := \sigma_1|_{K^{\mathrm{alg}}}$ a topological generator of $\mathrm{Gal}(K)$.

Claim 1. *There exists a topological generator σ_2 of $\mathrm{Gal}(F_2) \cong \hat{\mathbb{Z}}$ such that $\sigma_2|_{K^{alg}} = \sigma_0$.*

Subproof. Assume that $\varphi\colon \hat{\mathbb{Z}} \twoheadrightarrow H$ is a continuous epimorphism and $h \in H$ is a topological generator.

We need to show that there exists a topological generator σ_2 of $\hat{\mathbb{Z}}$ in $\varphi^{-1}(h)$.

As H is procyclic, we have $H = \varprojlim_{i\in\mathbb{N}} H_i$ such that $H_i \cong \mathbb{Z}/n_i\mathbb{Z}$ and $H_{i+1} \twoheadrightarrow H_i$ so $n_i | n_{i+1}$.

Let $\varphi_i := \pi_i \circ \varphi\colon \hat{\mathbb{Z}} \to H_i \cong \mathbb{Z}/n_i\mathbb{Z} = \langle h_i \rangle$, where $h_i = \pi(h)$.

φ_i factors through $\psi_i\colon \hat{\mathbb{Z}}/n_i\hat{\mathbb{Z}} = \mathbb{Z}/n_i\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}/n_i\mathbb{Z}$, so ψ_i is the multiplication by some $k_i \in \left(\mathbb{Z}/n_i\mathbb{Z}\right)^*$

Let $k \in \hat{\mathbb{Z}}^\times := \varprojlim \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ such that $\pi_{n_i}(k) = h_i$ for all i and $k \in \hat{\mathbb{Z}}^* \subseteq \hat{\mathbb{Z}}$ is a topological generator.

Then $\varphi(k) = h$.

$\Phi\colon \mathrm{Gal}(F_1) \xrightarrow{\cong} \mathrm{Gal}(F_2), \sigma_1 \mapsto \sigma_2$ respects K^{alg}. By the Embedding Lemma (2.6) we find f as claimed. ■

□

Setting $K = F$ in Proposition 2.8 yields:

Corollary 2.9. Let $F \subseteq F'$ be pseudofinite fields. Then $F \preceq F' \iff F^{\mathrm{alg}} \cap F' = F$.

Theorem 2.10. Let $F_1, F_2 \models \mathsf{Psf}'$ with a common subfield K. Then the following are equivalent:

(1) $F_1 \equiv_K F_2$,

(2) $F_1 \cap K^{\mathrm{alg}} \cong_K F_2 \cap K^{\mathrm{alg}}$.

Proof. (1) $\implies$ (2) by Lemma 2.7.

(2) $\implies$ (1): By Proposition 2.8 $f\colon F_1 \cap K^{\mathrm{alg}} \cong F_2 \cap K^{\mathrm{alg}}$ is elementary, so in particular id_K is elementary, so $F_1 \equiv_K F_2$. □

[Lecture 09, 2024-11-08]

Theorem 2.11. The completions of Psf' are given by adding sentences of the form

$$\exists t.\ f(t) = 0$$

and

$$\forall t.\ f(t) \neq 0$$

for $f(T) \in \mathbb{Z}[T]$.

Proof. These sentences determine the characteristic, as for $p \in \mathbb{P}$ the constant polynomial $p \in \mathbb{Z}[T]$ is contained.

Thus applying the Lemma 2.12 to $K = \mathbb{F}_p$ or $K = \mathbb{Q}$ will yield the result. □

Lemma 2.12. Let K be a perfect field and $L_1, L_2 \supseteq K$. Suppose that for every $f(T) \in K[T]$ we have $L_1 \models \exists t.\ f(t) = 0 \iff L_2 \models \exists t.\ f(t)$.

Then $K^{\mathrm{alg}} \cap L_1 \cong_K K^{\mathrm{alg}} \cap L_2$.

Proof. By compactness of the Krull topology on $\mathrm{Gal}(K)$, it suffices to show the following:

Claim 1. *Let $N \supseteq K$ be a finite normal ($\iff$ Galois) extension. Then $L_1 \cap N \cong_K L_2 \cap N$.*

Subproof. Let $L_1 \cap N = K(\alpha)$ and $f(T) := \mathrm{MiPo}(\alpha/K)$. Then $L_1 \models \exists t.\ f(t) = 0$, hence $L_2 \models \exists t.\ f(t) = 0$.

So $L_1 \cap N \xhookrightarrow[K]{\varphi} L_2 \cap N$.

In particular $[L_1 \cap N : K] \leqslant [L_2 \cap N : K]$. By symmetry we have equality, i.e. φ is an automorphism. ■

□

Theorem 2.13 (Quantifier reduction in Psf')**.** Let $\varphi(\overline{x})$ be an $\mathcal{L}_{\mathrm{ring}}$-formula. Then there is an $\mathcal{L}_{\mathrm{ring}}$-formula $\psi(\overline{x})$, a boolean combination of formulas of the form

$$\exists t.\ f(t, \overline{x}) = 0,$$

where $f(T, \overline{X}) \in \mathbb{Z}[T, \overline{X}]$, such that $\mathsf{Psf}' \models \forall \overline{x}.\ (\varphi(\overline{x}) \iff \psi(\overline{x}))$.

Proof. By Corollary 1.25 it suffices to show that all partial maps between models of Psf' that preserves all formulas of the type $\ulcorner \exists t.\ f(t, \overline{x}) = 0 \urcorner$ are actually partial elementary maps.

So we need to show: If $F, F' \models \mathsf{Psf}'$, $\overline{a} \in F^n$, $\overline{b} \in (F')^n$ such that for all $f(T, X_1, \ldots, X_n) \in \mathbb{Z}[T, \overline{X}]$

$$F \models \exists t.\ f(t, \overline{a}) = 0 \iff F' \models \exists t.\ f(t, \overline{b}), \tag{1}$$

then $\mathrm{tp}(\overline{a}) = \mathrm{tp}(\overline{b})$.

By Theorem 2.10 this is equivalent to the map $\overline{a} \mapsto \overline{b}$ extending to an isomorphism

$$Q(\langle \overline{a} \rangle)^{\mathrm{alg}} \cap F \leftrightarrow Q(\langle \overline{b} \rangle)^{\mathrm{alg}} \cap F'.$$

Let $\mathbb{F} \subseteq F, F'$ be the prime subfield. (It coincides, as the constant polynomials are included, hence the characteristic is determined.)

Applying (1) to polynomials not depending on T yields that $I(\overline{a}/\mathbb{F}) = I(\overline{b}/\mathbb{F})$, so $\mathbb{F}(\overline{a}) \overset{h\colon \overline{a} \mapsto \overline{b}}{\cong} \mathbb{F}(\overline{b})$.

By the proof of Quantifier Reduction in Psf (2.13) applied to $f(T, \overline{a})$ separable over $\mathbb{F}(\overline{a})$ we see that h extends to $h^{\mathrm{sep}} : \mathbb{F}(\overline{a})^{\mathrm{sep}} \cap F \cong \mathbb{F}(\overline{b})^{\mathrm{sep}} \cap F'$.

Since F and F' are perfect, $F(\overline{a})^{\mathrm{alg}} \cap F = (F(\overline{a})^{\mathrm{sep}} \cap F)^{\mathrm{perf}}$.

So we get h^{alg} extending h. □

Remark 2.13.37. We will later see that Psf' is not model-complete.

Notation 2.13.38. Let $\mathcal{L}_c := \mathcal{L}_{\text{ring}} \sqcup \{c_{i,n} | n \geqslant 2, 0 \leqslant i < n\}$.

Let Psf'_c be the $\mathcal{L}_c$-theory Psf' to which we add for $n \geqslant 2$ the sentence

$$\psi_n :\equiv \text{“}X^n + c_{n-1,n}X^{n-1} + \ldots + c_{0,n} \text{ is irreducible”}.$$

Remark 2.13.39. As any $F \models \mathsf{Psf}'$ is quasifinite, it admits an expansion to a model of Psf'_c.

Theorem 2.14. Psf'_c is model-complete.

Proof. Let $F_1, F_2 \models \mathsf{Psf}'_c$, $F_1 \subseteq F_2$.

Let $K_n \big/ F_1$ be the unique extension of F_1 of degree n, $n \geqslant 2$. As $F_1 \models \psi_n$, we get $K_n \cong F_1[X] \Big/ \left(X^n + c_{n-1,n}^{F_1} X^{n-1} + \ldots + c_{0,n}^{F_1}\right) F_1[X]$ and as $X^n + \sum_{i=0}^n c_{i,n} X^i$ is irreducible in $F_2[X]$, as $F_2 \models \psi_n$, we get $K_n \cap F_2 = F_1$, so $F_1^{\text{alg}} \cap F_2 = F_1$.

By Corollary 2.9 we obtain $F_1 \preceq F_2$ (in $\mathcal{L}_{\text{ring}}$, so also in $\mathcal{L}_c$). □

Theorem 2.15. Let $F \models \mathsf{Psf}'$, and let $D \subseteq F^n$ be F-definable. Then there is an algebraic set $W \subseteq F^{n+m}$ for some $m \geqslant 0$ such that

(i) $\pi(W) = D$,

(ii) $\forall d \in D.\ \pi^{-1}(d) \cap W$ is finite.

Example 2.16. Let D be the set of squares. Set $W := \{(x, y) | y^2 = x\}$.

Proof. Observe: Assume that $D \subseteq F^{k+l}$, $k + l = n$ and $W \subseteq F^{k+l+m}$ is an algebraic set as in the statement. Let $e \in F^k$, $D_e := \{d \in F^l | (e, d) \in D\}$ and $W_e \subseteq F^{l+m}$ defined similarly. Then W_e is an algebraic set satisfying the statement for D_e.

Hence we may assume that D is $\varnothing$-definable.

By Remark 2.13.39, F expands to a model of Psf'_c.

Theorem 2.14 implies that if $D = \varphi[F]$, we may assume that $\varphi(\overline{x})$ is an existential $\mathcal{L}_c$-formula and as $f(\overline{x}) \neq 0 \iff \exists y.\ f(\overline{x}) - y = 0$ we may assume

$$\varphi(\overline{x}) \equiv \exists \overline{y} \theta(\overline{x}, \overline{y})$$

with $\theta(\overline{x}, y)$ positive quantifier-free, i.e. defining an algebraic set $W \subseteq F^{m+n}$ such that $\pi(W) = D$.

Claim 1. *W may be chosen so that $\pi \colon W \twoheadrightarrow D$ has finite fibers. ((ii) from the theorem)*

Subproof. By Quantifier Reduction in Psf (2.13) D may be defined by an $\mathcal{L}_{\text{ring}}$-formula, which is a Boolean combination of the form

$$\exists t.\ f(t, \overline{x}) = 0,$$

$f(T, \overline{X}) \in \mathbb{Z}[T, \overline{X}]$, i.e. by a positive Boolean combination of formulas of the form $\exists t.\ f(t, \overline{x}) = 0$ or $\forall t.\ f(t, \overline{x}) \neq 0$.

Call a definable set $S \subseteq F^n$ *special* iff it is as in the statement of the theorem, i.e. iff there is an algebraic set $W \subseteq F^{n+m}$ such that $\pi(W) = S$ and all fibers are finite.

Equivalently, there is $\varphi(\overline{x}) \equiv \exists \overline{y} \theta(\overline{x}, \overline{y})$, where θ is a conjunction of polynomial equations and there is $N \in \mathbb{N}$ such that $F \models \forall \overline{x}.\ \exists^{\leqslant N} \overline{y}.\ \theta(\overline{x}, \overline{y})$ with $\varphi(F) = D$.

(1) The collection of special sets is closed under positive boolean combinations, i.e. if $D_1, D_2 \in S$ then $D_1 \cap D_2, D_1 \cup D_2 \in S$.

Indeed: Let $D := D_1 \cap D_2$. Let $\varphi_i(\overline{x}) \equiv \exists \overline{y_i}.\ \theta(\overline{x}, \overline{y_i})$ witnessing $D_i \in S$.

Set $\varphi(\overline{x}) :\equiv \exists \overline{y_1} \exists \overline{y_2}.\ (\theta_1(\overline{x}, \overline{y}_1) \wedge \theta(\overline{x}, \overline{y}_2)$. This witnesses $D \in S$.

On the other hand let $D := D_1 \cap D_2$. Take φ_i as before. We may assume $|\overline{y_1}| = m = |\overline{y_2}|$. Set

$$\varphi(\overline{x}) :\equiv \exists \overline{y}.\ \bigwedge_{\substack{1 \leqslant j \leqslant N_1 \\ 1 \leqslant k \leqslant N_2}} f_{j,1}(\overline{x}, \overline{y}) \cdot f_{k,2}(\overline{x}, \overline{y}) = 0.$$

(2) For $f(T, \overline{X}) \in \mathbb{Z}[T, \overline{X}]$, the set defined by

$$\exists t.\ f(t, \overline{x}) = 0$$

is a positive Boolean combination of special sets (so special by (1)).

Indeed let $f(T, \overline{X}) = \sum_{i=1}^{N} c_i(\overline{X}) T^i$, $d_i(\overline{X}) \in \mathbb{Z}[\overline{X}]$. Then $\exists t.\ f(t, \overline{x}) = 0$ is equivalent to

$$\underbrace{\bigwedge_{i=1}^{N} d_i(\overline{X}) = 0}_{\text{special}} \vee \underbrace{\left[\exists y \exists t.\ \prod (d_i(\overline{x}) \cdot y - 1) = 0 \wedge f(t, \overline{x}) = 0\right]}_{\text{special}}.$$

(3) $\forall t.\ f(t,\overline{x}) \neq 0$ is equivalent to a positive boolean combination of special sets.

Indeed, $\forall t.\ f(t,\overline{x}) \neq 0$ is equivalent to (working in Psf'_c) the disjunction of $\exists y.\ (d_0(\overline{x}\cdot y) - 1 = 0 \wedge_{i=1}^{N} d_i(\overline{x}) = 0$ (special, saying $f(T,\overline{x})$ is constant nonzero).

$$\exists y.\ \prod_{i=1}^{N}(d_i(\overline{x})\cdot y - 1) = 0 \wedge \text{“the unique extension } F_{N!} \text{ does not contain a zero of } f(T,\overline{x})\text{ ”}$$

where $F_{N!}$ denotes the unique extension of F of degree $N!$.

Note: $F_{N!} = F[\alpha]$ for some α a root of $T^{N!} + \sum_{i=0}^{N!-1} c_{i,N!}T^i = \mathrm{MiPo}(\alpha/F)$. Work in the F basis $1, \alpha, \ldots, \alpha^{N!-1}$ of $F_{N!}$.

Assume for simplicity $\deg(f(T,\overline{X})) = N$, so $f(T,\overline{x}) = \underbrace{d_N(\overline{x})}_{\neq\varnothing}\prod_{i=1}^{N}(T - a_i)$, $a_i \in F_{N!}$.

$a_i = \sum_{j=0}^{N!-1} b_{ij}\alpha^j$, $b_{ij} \in F$. We quantify existentially over z_i, $i = 1,\ldots,N$ saying

$$\exists z_i.\ \prod_{j=1}^{N!-1}(b_{ij}z_- 1) = 0,$$

the formula quantifying also over b_{ij} is special.

■

□

3 The Relationship between Psf' and T_f / Psf, Decidability

[Lecture 10, 2024-11-15]

The connection to finite fields relies on the following fundamental result:

Theorem 3.1 (Lang-Weil Estimates)**.** Given n, r, d, there is a constant $C = C(n,r,d)$ such that for every finite field $\mathbb{F}_q$ and every absolutely irreducible variety $V \subseteq \mathbb{A}^n$ defined over $\mathbb{F}_q$ of dimension r and degree $\leqslant d$ one has

$$|\#V(\mathbb{F}_q) - q^r| \leqslant Cq^{r-\frac{1}{2}}.$$

Remark 3.1.40. Here if V is defined by $f_1(\overline{x}) = \ldots = f_m(\overline{x}) = 0$, we may

work with the naive definition

$$\deg(V) := \prod_{i=1}^{m} \deg(f_i),$$

so the Lang-Weil Estimates (3.1) really hold in a definable family of absolutely irreducible algebraic varieties.

We will later mainly need the following special case (see for example [FJ23]), a consequence of the Riemann hypothesis for function fields:

Theorem 3.2 (Lang-Weil for plane curves)**.** Let $f(X,Y) \in \mathbb{F}_q[X,Y]$ be an absolutely irreducible polynomial of degree d and let Γ be the plane curve defined by $f(X,Y) = 0$.

Then

$$q + 1 - (d-1)(d-2)\sqrt{q} - d \leqslant \#\Gamma(\mathbb{F}_q) \leqslant q + 1 + (d-1)(d-2)\sqrt{q},$$

so in particular

$$|\#\Gamma(\mathbb{F}_q) - q| \leqslant (d-1)(d-2)\sqrt{q} + (d-1).$$

Corollary 3.3. Let $V \subseteq \mathbb{A}^n$ be an absolutely irreducible variety of dimension r and $\deg(V) \leqslant d$ defined over $\mathbb{F}_q$. Assume that $q > C(n,d,r)^2$. Then $V(\mathbb{F}_q) \neq \varnothing$.

Proof. Indeed, if $q > C^2$, then $q^r > c \cdot q^{r-\frac{1}{2}}$, so the result follows from the Lang-Weil Estimates (3.1). □

Corollary 3.4. Let $\mathcal{U}$ be a non-principal ultrafilter on the set Q of prime powers. Then $\prod_{\mathcal{U}} \mathbb{F}_q$ is pseudofinite.

Proof. We know already that $\prod_{\mathcal{U}} \mathbb{F}_q =: K$ is quasifinite. Every absolutely irreducible variety $V \subseteq \mathbb{A}^n$ is in a definable family of constant dimension and bounded degree, and for this family $(V_b)_b$, there is C such that whenever $q > C^2$, then $V_b(\mathbb{F}_q) \neq \varnothing$ (see Corollary 3.3). Thus

$$K \models \forall z.\ \exists x.\ x \in V_z$$

for the corresponding family V_z showing that K is PAC, thus K is pseudofinite. □

Corollary 3.5. Every infinite subfield K of $\mathbb{F}_p^{\mathrm{alg}}$ is PAC. In particular if $\mathrm{Gal}(K) \cong \hat{\mathbb{Z}}$, then K is pseudofinite.

Proof. Every absolutely irreducible variety V defined over K is defined using finitely many parameters, so it is defined over $\mathbb{F}_q \subseteq K$. By Corollary 3.3 for any $N \gg 0$ with $\mathbb{F}_{q^N} \subseteq K$ we get $V(\mathbb{F}_{q^N}) \neq \varnothing$, so in particular $V(K) \neq \varnothing$. □

Example 3.6. Let $n = \prod_{p\in\mathbb{P}} p^{\nu_p}$ be an infinite supernatural number with all exponents $\nu_p < \infty$ and let $p_0 \in \mathbb{P}$. Then

$$\mathbb{F}_{p_0^n} := \bigcup_{\substack{n'|n \\ n'\in\mathbb{N}}} \mathbb{F}_{p_0^{n'}} = \left(\mathbb{F}_{p_0}^{\mathrm{alg}}\right)^H,$$

where $H = \prod_{p\in\mathbb{P}} p^{\nu_p}\mathbb{Z}_p \cong \hat{\mathbb{Z}}$, is an infinite field with absolute Galois group $H \cong \hat{\mathbb{Z}}$, so it is pseudofinite by Corollary 3.5.

Notation 3.6.41. For a field K with prime subfield $\mathbb{F}$, we denote by $\mathrm{Abs}(K)$ the field $K \cap \mathbb{F}^{\mathrm{alg}}$, the **subfield of absolute numbers**.

Lemma 3.7. If K is pseudofinite, then $\mathrm{Abs}(K)$ is perfect with procyclic absolute Galois group.

Proof. As $K/\mathrm{Abs}(K)$ is regular, $\mathrm{Gal}(K) \twoheadrightarrow \mathrm{Gal}(\mathrm{Abs}(K)$ is surjective (Proposition 1.39), so $\mathrm{Gal}(\mathrm{Abs}(K))$ is procyclic. □

Goal. *We want to show that whenever $K_0 \subseteq \mathbb{F}^{alg}$ has a procyclic Galois group, there is a non-principal ultrafilter on Q, $\mathcal{U}$, such that* $\mathrm{Abs}(\prod_{\mathcal{U}} \mathbb{F}_q) \cong K_0$.

In characteristic 0, this requires a deep ingredient from number theory (the Čebotarev density theorem, Theorem 3.20 in Lecture 11). In positive characteristic, this is elementary:

Proposition 3.8. Let p be prime and $K_0 \subseteq \mathbb{F}_p^{\mathrm{alg}}$ an arbitrary subfield. Then there are a sequence $(F_n)_n$ of finite fields of characteristic p and an ultrafilter $\mathcal{U}$ on $\mathbb{N}$ such that $K := \prod_{\mathcal{U}} F_n$ is pseudofinite with $\mathrm{Abs}(K) = K_0$.

Proof. **1st case** K_0 is infinite:

Let $(k_n)_{n\in\mathbb{N}}$ be a strictly increasing sequence of integers such that $K_0 = \bigcup \mathbb{F}_{p^{k_n}}$ and $k_n | k_{n+1}$ for all n, i.e. K_0 is the increasing union of the $\mathbb{F}_{p^{k_n}}$

For $F_n := \mathbb{F}_{p^{k_n}}$ and a non-principal ultrafilter $\mathcal{U}$ on $\mathbb{N}$, one gets $\mathrm{Abs}(\prod_{\mathcal{U}} F_n) = K_0$.

Indeed, a polynomial $f(T) \in \mathbb{F}_p[T]$ has a root in K_0 iff it has a root in all but finitely many F_n iff it has a root in $\prod_{\mathcal{U}} F_n$. We get $\mathrm{Abs}\left(\prod_{\mathcal{U}} F_n\right) \cong K_0$ by Lemma 2.12.

2nd case $K_0 = \mathbb{F}_{p^m}$ is finite:

Let $(l_n)_{n \geqslant 0}$ be an enumeration of $\mathbb{P}$ and let $F_n := \mathbb{F}_{p^{m \cdot l_n}}$.

As before let $\mathcal{U}$ be a non-principal ultrafilter on $\mathbb{N}$. As in the first case, one verifies $\mathrm{Abs}\left(\prod_{\mathcal{U}} F_n\right) \cong K_0$, again using Lemma 2.12. □

Theorem 3.9. For any $K_0 \subseteq \mathbb{Q}^{\mathrm{alg}}$ with $\mathrm{Gal}(K_0)$ procyclic there exists a non-principal ultrafilter $\mathcal{U}$ on $\mathbb{P}$ such that $\mathrm{Abs}(\prod_{\mathcal{U}} \mathbb{F}_p) \cong K_0$.

We will prove this in Lecture 12. This will be more work.

Recall that

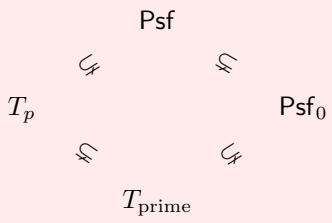
$$T_f := \{\varphi \ \mathcal{L}_{\mathrm{ring}}\text{-sentence} \mid \forall q \in Q.\ \mathbb{F}_q \models \varphi\},$$
$$\mathsf{Psf} := \{\varphi \ \mathcal{L}_{\mathrm{ring}}\text{-sentence} \mid \forall q \gg 0.\ \mathbb{F}_q \models \varphi\}.$$

Note that Psf is the theory of all infinite models of T_f.

Let $T_{\mathbf{prime}} := \{\varphi | \forall p \in \mathbb{P}.\ \mathbb{F}_p \models \varphi\}$.

Corollary 3.10. (1) $\mathsf{Psf} = \mathsf{Psf}'$. Moreover the completions of Psf are determined by the isomorphism type of $\mathrm{Abs}(F)$ and any $K_0 \subseteq \mathbb{F}^{\mathrm{alg}}$ (for $\mathbb{F} = \mathbb{F}_p$ or $\mathbb{F} = \mathbb{Q}$) with $\mathrm{Gal}(K_0)$ procyclic occurs as $\mathrm{Abs}(F)$ for some $F \models \mathsf{Psf}$.

(2) We have the following strict inclusions of theories:



Proof. (1) One direction follows from Proposition 3.8 and Theorem 3.9, the other direction from Corollary 3.4. The characterization of the completions is Theorem 2.11.

(2) We have $T_{\text{prime}} \overset{(3.9)}{\subseteq} \mathsf{Psf}_0$. The other inclusions are clear by the above. As for $T_f \subsetneq T_{\text{prime}}$ note that for every $p \in \mathbb{P}$, T_{prime} contains a sentence of the form

$$\varphi_p \equiv \underbrace{1 + \ldots + 1}_{p \text{ times}} = 0 \to \neg\exists x_1, \ldots, x_{p+1}. \bigwedge_{1 \leqslant i < j \leqslant p+1} x_i \neq x_j,$$

which is not in T_f.

□

We now want to reduce questions about higher-dimensional (absolutely irreducible) varieties to curves.

First some terminology: A **K-hyperplane** in $\mathbb{A}^n$ is a subset determined by an equation $a_1X_1 + \ldots + a_nX_n = b$, $a_i, b \in K$, $a_i \neq 0$ for some i. For the purpose of this course, we will restrict to hyperplanes not containing $0 \in K^n$ and may thus normalize the equation to

$$H_{\overline{a}} : \sum_{i=1}^{n} a_i X_i = 1$$

All hyperplanes (over K) not containing 0 are of this form and $H_{\overline{a}} = H_{\overline{a}'}$ iff $\overline{a} = \overline{a}'$, so they are parameterized by $\mathbb{A}^n$ as well.

A **geometric hyperplane** over $K_0 \subseteq K$ is an $H_{\overline{a}}$ such that $\operatorname{trdeg}(\overline{a}/K_0) = n$, i.e. $\overline{a}$ is generic in $\mathbb{A}^n$ over K_0.

Theorem 3.11 (Bertini's Theorem)**.** Let $V \subseteq \mathbb{A}^n$ be an irreducible K-variety, $K = K^{\text{alg}}$ and $\dim(V) \geqslant 2$.

Then there exists a proper K-subvariety $W \subseteq \mathbb{A}^n$ such that for all $\overline{a} \in K^n \backslash W(K)$ the algebraic set $H_{\overline{a}} \cap V$ is irreducible of dimension $\dim(V) - 1$.

In Lecture 11, we will give a model-theoretic proof of Bertini's Theorem (3.11) due to Poizat, showing that the intersection with a generic hyperplane H yields $V \cap H$ irreducible of $\dim(V \cap H) = \dim(V) - 1$. As being irreducible is definable in ACF, this will suffice.

Corollary 3.12. Let K be an infinite field and V an absolutely irreducible K-variety of dimension $\dim(V) = r \geqslant 2$. Then V contains an absolutely irreducible K-curve.

Proof. Let $K \subseteq L$ and $f(X_1, \ldots, X_n) \in L[X_1, \ldots, X_n] \backslash \{0\}$.

It suffices to show that there is $\overline{a} \in K^n$ such that $f(\overline{a}) \neq 0$ as the special set W in Bertini's Theorem (3.11) is contained in a hypersurface (given by $f(\overline{X}) = 0$).

We prove this by induction on n. The case $n = 0, 1$ is clear.

$n \rightsquigarrow n+1$: Let $f(X_1, \dots, X_n, Y) = \sum_{i=1}^{N} c_i(\overline{X}) Y^i$ with $c_N(\overline{X}) \neq 0$. By the induction hypothesis there is $\overline{a} \in K^n$ such that $c_N(\overline{a}) \neq 0$, so $0 \neq f(\overline{a}, Y) \in L[Y]$. By the case $n = 1$ we find $b \in K$ such that $f(\overline{a}, b) \neq 0$. □

Corollary 3.13. A field K is PAC iff for every absolutely irreducible $f(X, Y) \in K[X, Y]$ the curve $\Gamma \subseteq \mathbb{A}^2$ defined by f contains infinitely many K-rational points.

Remark 3.13.42. One may even prove that it suffices to ask for *one* K-rational point for every absolutely irreducible plane curve (Frey-Geyer, see e.g. [FJ23])

Proof of Corollary 3.13. Any field K satisfying the assumption is infinite, so by Corollary 3.12 in an absolutely irreducible K-variety V of dimension $\geqslant 2$ we find an absolutely irreducible K-curve $\Gamma \subseteq V$. To prove $V(K) \neq \varnothing$ it thus suffices to prove $\Gamma(K) \neq \varnothing$.

Let $K(\Gamma)$ be the function field of Γ, a finitely generated regular extension of K of transcendence degree 1. In particular, $K(\Gamma)/K$ is separable and thus separably generated (see Proposition 1.40, Proposition 1.41) and we find a transcendence basis t of $K(\Gamma)/K$ such that $K(\Gamma)/K(t)$ is separable. By the primitive element theorem, there is s separable algebraic over $K(t)$ such that $K(\Gamma) = K(t, s)$.

Let $F(X) := \mathrm{MiPo}(s/K(t))$. Let $f(X, Y) \in K[X, Y]$ be irreducible such that $F(X) = \frac{f(X,t)}{g(t)}$ for some $g(t) \in K[t]$.

By construction, if Γ' denotes the plane curve defined by $f(X, Y) = 0$, we get $K(\Gamma) \cong_K K(\Gamma')$, so in particular $f(X, Y)$ is absolutely irreducible (as $K(\Gamma')/K$ is regular) and Γ and Γ' are birational, so they admit isomophic non-empty Zariski open subsets $\Omega \overset{o}{\subseteq} \Gamma$ and $\Omega' \overset{o}{\subseteq} \Gamma'$. But then $\Gamma \backslash \Omega$ and $\Gamma' \backslash \Omega'$ are 0-dimensional (so only have finitely many K^{alg}-points), then if $\Gamma'(K)$ is infinite, $\Gamma(K) \neq \varnothing$.

□

Remark 3.14. This shows that we only need the special case of the Lang-Weil Estimates (3.1) given in Theorem 3.2 to prove that $\mathsf{Psf} = \mathsf{Psf}'$, as Psf' may be axiomatized using absolutely irreducible polynomials in 2 variables. These obviously form a quantifier free family, when restricted to polynomials of degree $\leqslant d$.

[Lecture 11, 2024-11-19]

Proof of Theorem 3.11. Let $K \preceq U \models \mathsf{ACF}$ and let $V \subseteq \mathbb{A}^n$ be an absolutely irreducible K-variety of dimension $r \geqslant 2$.

Since irreducibility is definable in families (by Corollary 2.3), it suffices to show that for $\overline{\beta} \in U^n$ with $\operatorname{trdeg}(\overline{\beta}/K) = n$, i.e. $\overline{\beta}$ generic in $\mathbb{A}^n$ over K, the variety $V \cap H_{\overline{\beta}}$ is absolutely irreducible of dimension $r-1$, where

$$H_{\overline{\beta}} : \sum_{i=1}^{n} \beta_i X_i = 1.$$

Let $\overline{\alpha} = (\alpha_1, \ldots, \alpha_n)$ be generic in V over K, i.e. $\overline{\alpha} \in V(U)$ such that $\operatorname{MR}\left(\overline{\alpha}/K\right) = r$.

Let $\overline{\beta} \in U^n$ be generic in $H_{\overline{\alpha}}$ over $K(\overline{\alpha})$, i.e. $\sum_{i=1}^{n} \beta_i \alpha_i = 1$ and $\operatorname{MR}(\overline{\beta}/K\overline{\alpha}) = n-1$.

Thus

$$\operatorname{MR}(\overline{\alpha}\overline{\beta}/K) = r + (n-1).$$

Claim 3.11.1. $\operatorname{MR}(\overline{\beta}/K) = n$.

Subproof. Otherwise $\operatorname{MR}(\overline{\beta}/K) = n-1$ and thus $\operatorname{MR}(\overline{\alpha}/K\overline{\beta}) = r$, so $V \subseteq H_{\overline{\beta}}$ since $\overline{\alpha} \in H_{\overline{\beta}}$ and $\overline{\alpha}$ is generic in V over $K(\overline{\beta})$.

As $\dim V = r \geqslant 2$, we find $\overline{\alpha}' \in V(K)$ such that $\overline{\alpha}'$ is not of the form $\lambda \cdot \overline{\alpha}$ for some $\lambda \in U$. Thus

$$\overline{\alpha} \cdot \overline{y} = 1$$
$$\overline{\alpha}' \cdot \overline{y} = 1$$

defines an affine linear subvariety of $\mathbb{A}^N$ of dimension $n-2$, defined over $K(\overline{\alpha})$, which contains $\overline{\beta}$. So $\operatorname{MR}(\overline{\beta}/K\overline{\alpha}) \leqslant n-2$ ↯. ■

Let $V \cap H_{\overline{\beta}} = Z_1 \cup \ldots \cup Z_m$ be the decomposition into (absolutely) irreducible components over $K(\overline{\beta})^{\mathrm{alg}}$. By Krull's Hauptidealsatz, $H_{\overline{\beta}}$ beging given by one equation, and as $V \nsubseteq H_{\overline{\beta}}$ by what we have just seen, $\dim Z_i = r-1$ for $i = 1, \ldots, m$.

Claim 3.11.2. *We have $m = 1$, i.e. $V \cap H_{\overline{\beta}}$ is absolutely irreducible.*

Subproof. Let $\overline{\alpha}, \overline{\alpha}' \in V \cap H_{\overline{\beta}}(U)$ be independent generic over $K(\overline{\beta})$, i.e.

$$\operatorname{MR}\left(\overline{\alpha}/K\overline{\beta}\right) = \operatorname{MR}\left(\overline{\alpha}'/K\overline{\beta}\right) = r-1$$

and $\operatorname{MR}(\overline{\alpha}\overline{\alpha}'/K\overline{\beta}) = 2r-2$. By Claim 3.11.1, we get

$$\operatorname{MR}(\overline{\alpha}\overline{\alpha}'\overline{\beta}/K) = n + 2r - 2. \tag{+}$$

It suffices to show that $\mathrm{tp}(\overline{\alpha}\overline{\alpha}'\overline{\beta}/K)$ is uniquely determined by this construction, i.e. by the conditions

(i) $\mathrm{MR}(\overline{\beta}/K) = n$,

(ii) $\overline{\alpha}, \overline{\alpha}' \in V \cap H_{\overline{\beta}}$ independent generic over $K(\overline{\beta})$.

Indeed the equivalence relation on $V \cap H_{\overline{\beta}}$ given by

$$x \sim x' :\Longleftrightarrow \bigwedge_{i=1}^{m} \big(x \in Z_i \leftrightarrow x' \in Z_i\big)$$

is $K_{\overline{\beta}}$-definable (as it is $K(\overline{\beta})^{\mathrm{alg}}$-definable and $\mathrm{Aut}\big(K(\overline{\beta})^{\mathrm{alg}}/K(\overline{\beta})\big)$-invariant).

If $m \geqslant 2$, we would find $\overline{\alpha}_1, \overline{\alpha}_2, \overline{\alpha}'_1, \overline{\alpha}'_2$ such that $\overline{\alpha}_1 \sim \overline{\alpha}'_1$ but $\overline{\alpha}_2 \not\sim \overline{\alpha}'_2$, thus $\mathrm{tp}(\overline{\alpha}_1\overline{\alpha}'_1\overline{\beta}/K) \neq \mathrm{tp}(\overline{\alpha}_2\overline{\alpha}'_2\overline{\beta}/K)$.

We have

$$\mathrm{MR}(\overline{\beta}/K\overline{\alpha}\overline{\alpha}') \leqslant n-2 \qquad (\text{as } \overline{\beta} \in H_{\overline{\alpha}} \cap H_{\overline{\alpha}'})$$

$$\mathrm{MR}(\overline{\alpha}\overline{\alpha}'/K) \leqslant 2r \qquad (\text{as } \overline{\alpha}, \overline{\alpha}' \in V)$$

$$\mathrm{MR}(\overline{\alpha}\overline{\alpha}'/K) + \mathrm{MR}(\overline{\beta}/K\overline{\alpha}\overline{\alpha}') = 2r + n - 2 \qquad (+)$$

It follows that $\mathrm{MR}(\overline{\beta}/K\overline{\alpha}\overline{\alpha}') = n-2$ and $\mathrm{MR}(\overline{\alpha}\overline{\alpha}'/K) = 2r$. So $\mathrm{tp}(\overline{\alpha}\overline{\alpha}'/K)$ is uniquely determined (it is the generic of the irreducible variety of $V \times V$ over K) and $\mathrm{tp}(\overline{\beta}/K\overline{\alpha}\overline{\alpha}')$ is uniquely determined (it is the generic of the absolutely irreducible affine-linear variety $H_{\overline{\alpha}} \cap H_{\overline{\alpha}'}$). ■

□

Before we give the proof of Theorem 3.9, we will settle the decidability of the various theories at work:

Theorem 3.15. The theories Psf, Psf_0, Psf_p ($p \in \mathbb{P}$), T_f and T_{prime} are all decidable.

Proof. Decidability of Psf yields decidability of

$$\mathsf{Psf}_p = \mathsf{Psf} \cup \{\underbrace{1 + \ldots + 1}_{p \text{ many}} = 0\}.$$

We will first show decidability of Psf_0. Note that Psf is recursively axiomatizable by the axioms for quasifinite fields together with axioms $\varphi_{n,d}$ for $d, n \in \mathbb{N}$ stipulating the existence of at least n rartional points for every absolutely irreducible plane curve of degree $\leqslant d$ Let Γ denote this set of axioms.

Then

$$\Gamma_0 := \Gamma \cup \{\underbrace{\neg \overbrace{1 + \ldots + 1}^{p \text{ many}} = 0}_{=:\chi_p} \,|\, p \in \mathbb{P}\}$$

is a recursive axiomatization of Psf_0.

Decision Procedure for Psf_0

Input The input is an $\mathcal{L}_{\text{ring}}$-sentence φ.

Step 1 Systematically enumerate all proofs using Γ as axioms until a sentence of the form $\varphi \leftrightarrow \psi$ is proved, where ψ is a boolean combination of formulas of the form $\exists t.\ f(t) = 0$, $f(X) \in \mathbb{Z}[X] \backslash \{0\}$. By Theorem 2.11 this step terminates.

Step 2 Let $(f_i)_{i=1,\ldots,N}$ be the polynomials that appear in the atomic subformulas of ψ and set $F := \prod_{i=1}^{N} f_i$. Effectively construct the splitting field $L/\mathbb{Q}$ of F, a finite Galois extension of $\mathbb{Q}$ (using Euclid's algorithm, the fact that $\overline{\mathbb{Q}}$ is a computable field, etc).

Compute $G := \mathrm{Gal}(L/\mathbb{Q})$ and list all cyclic subgroups $H_i \leqslant G$, $i = 1, \ldots, k$.

Step 3 For $i = 1, ..., k$, compute $L_i := L^{H_i}$ and decide whether $L_i \models \psi$. (Note that an atomic sentence of the form $\exists t.\ f(t) = 0$ may be effectively decided in L_i.)

Output $\varphi \in \mathsf{Psf}_0$ iff $L_i \models \psi$ for $i = 1, \ldots, k$.

Indeed for $K \models \mathsf{Psf}_0$ one has $K \models \varphi$ iff $K \models \psi$ iff $K \cap L \models \psi$. Any $K \cap L$ is among the $(L_i)_{i=1,\ldots,k}$, since $K \cap L = \mathrm{Abs}(K) \cap L$ and $\mathrm{Gal}(\mathrm{Abs}(K))$ is procyclic. Moreover given $H_i \leqslant G$ cyclic, choose a generator $\sigma_i \in G$ with $\langle \sigma_i \rangle = H_i$, then lift σ_i to $\tilde{\sigma}_i \in \mathrm{Gal}(\mathbb{Q})$. Then $K_i := \left(\mathbb{Q}^{\mathrm{alg}}\right)^{\tilde{\sigma}_i}$ has procyclic absolute Galois group, thus is of the form $\mathrm{Abs}(F_i)$ for $F_i \models \mathsf{Psf}_0$ by Theorem 3.9. This shows that $L_i \models \psi$ is necessary for all $i = 1, \ldots, k$ so that $\psi \in \mathsf{Psf}_0$.

Decision Procedure for Psf

Input An $\mathcal{L}_{\text{ring}}$-sentence φ.

Step 1 If $\varphi \notin \mathsf{Psf}_0$, then $\varphi \notin \mathsf{Psf}$, stop.

Step 2 Effectively compute ψ such that $\mathsf{Psf} \vdash \varphi \leftrightarrow \psi$, where ψ is a boolean combination of formulas of the form $\exists t.\ f(t) = 0$, $f(X) \in \mathbb{Z}[X] \backslash \{0\}$ as before.

Find a formal proof of ψ from Γ_0 (which exists, since $\psi \in \mathsf{Psf}_0$) and write down the primes $p_1, \ldots, p_m$ for which the axioms χ_{p_i} appears in the proof.

(For any $p \in \mathbb{P}$ not in the list, $\mathsf{Psf}_p \vdash \varphi$.)

Step 3 Effectively construct a finite field $\mathbb{F}_{p_i}^{n_i}$ for any $i = 1, \ldots, m$, such that all $f(X) \pmod{p_i}$ appearing in ψ completely split over $\mathbb{F}_{p_i^{n_i}}$.

Then check whether $\mathbb{F}_{p_i^{m_i}} \models \psi$ for any $m_i | n_i$, i.e. for any subfield of $\mathbb{F}_{p_i^{n_i}}$.

If this is the case for all subfields and all $p_1, \ldots, p_m$, then $\psi \in \mathsf{Psf}$ and thus $\varphi \in \mathsf{Psf}$. Otherwise $\varphi \notin \mathsf{Psf}$.

Decision Procedure for T_f

Input An $\mathcal{L}_{\text{ring}}$-sentence φ.

Step 1 If $\varphi \notin \mathsf{Psf}$, then $\varphi \notin T_f$ (by Corollary 3.10).

Otherwise $\varphi \in \mathsf{Psf}$ and we can effectively find a proof of φ from Γ.

Step 2 Let $d, n \in \mathbb{N}$ be such that all axioms of the form $\varphi_{d',n'}$ used in the proof of $\Gamma \vdash \varphi$ are such that $d' \leqslant d$ and $n' \leqslant n$.

(Note that by the Lang-Weil Estimates for Plane Curves (3.2), there is a computable function $(d, n) \mapsto B(d, n)$ such that for all $q > B(d, n)$ one has $\mathbb{F}_q \models \varphi_{d',n'}$ for all $d' \leqslant d, n' \leqslant n$.)

Step 3 For all $q \leqslant B(d, n)$, check whether $\mathbb{F}_q \models \varphi$. If this is the case for all $q \leqslant B(d, n)$, then $\varphi \in T_f$. Otherwise $\varphi \notin T_f$.

Decision Procedure for T_{prime}

Input An $\mathcal{L}_{\text{ring}}$-sentence φ.

Step 1 Decide whether $\varphi \in \mathsf{Psf}_0$. If not, then $\varphi \notin T_{\text{prime}}$ by Corollary 3.10.

Step 2 Find a proof of φ from Γ_0. Let $p_1, \ldots, p_m$ be the primes such that χ_{p_i} is used in the proof. Find $d, n \in \mathbb{N}$ such that $d \geqslant d', n \geqslant n'$ for all the $\varphi_{d',n'}$ used in the proof.

Step 3 For all primes $p \leqslant \max(B(d,n), p_1, \ldots, p_m)$ check whether $\mathbb{F}_q \models \varphi$. If this is the case, $\varphi \in T_{\text{prime}}$. Otherwise $\varphi \notin T_{\text{prime}}$. □

Remark 3.15.43. [a] One may actually show that the decision procedures from Theorem 3.15 may all be taken to be primitive recursive (see [FJ23]). Our approach does not show this immediately.

[a] This is 3.15 in the handwritten notes

[Lecture 12, 2024-11-22]

We will be back in M2 next week.

We will now prove Theorem 3.9, using a deep result from number theory.[6]

Notation 3.15.44. For a **number field** K, i.e., a field extension $K/\mathbb{Q}$ of finite degree, we call $\mathcal{O}_K := \mathrm{Int}_K(\mathbb{Z})$ the **ring of integers of** K. (Int_K the integral closure in K),

Fact 3.16. $\mathcal{O}_K$ is a Dedekind domain, i.e. every non-zero ideal $I \trianglelefteq \mathcal{O}_K$ uniquely factors into primes $I = \mathfrak{p}_1^{e_1} \cdot \ldots \cdot \mathfrak{p}_m^{e_m}$ $\mathfrak{p}_i \trianglelefteq \mathcal{O}_k$ maximal, $e_i \in \mathbb{N}$.

If L/K are number fields, $\mathfrak{q} \in \mathrm{Spec}(\mathcal{O}_L)\backslash\{0\}$, then $\mathfrak{q} \cap \mathcal{O}_K =: \mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)\backslash\{0\}$ $\mathfrak{p}\mathcal{O}_L \trianglelefteq \mathcal{O}_L$ decomposes as $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}^e \cdot \mathfrak{q}_2^{e_2} \cdot \ldots \cdot \mathfrak{q}_m^{e_m}$, $e > 0$.

One writes $\mathfrak{q}|\mathfrak{p}$ and says "$\mathfrak{q}$ **divides** $\mathfrak{p}$".

Definition 3.16.45. $\mathfrak{q}$ is **unramified** in L/K if $e = 1$.

Fact 3.17. If L/K is Galois with $G = \mathrm{Gal}\left(L/K\right)$ and if $\mathfrak{q}_i|\mathfrak{p}$, $i = 1, \ldots, m$ are the divisors of $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)$ in $\mathrm{Spec}(\mathcal{O}_L)$, then $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$ is a G-orbit ($\sigma \cdot \mathfrak{q} := \sigma(\mathfrak{q})$) and $e_1 = \ldots = e_m$ in $\mathfrak{q} = \prod \mathfrak{q}_i^{e_i}$.

If L/K is Galois and $\mathfrak{p} \in \mathrm{Spec}(\mathcal{O}_K)\backslash\{0\}$, we say $\mathfrak{p}$ is **unramified** in L/K if all $\mathfrak{q}|\mathfrak{p}$ are unramified (equivalently one $\mathfrak{q}_i|\mathfrak{p}$ is unramified) in L/K.

Fact 3.18. Let $K/\mathbb{Q}$ be finite Galois. Then only finitely many prime numbers ramify in $K/\mathbb{Q}$.

Let L/K be finite Galois, $\mathfrak{p} \trianglelefteq \mathcal{O}_K =: k$, $\mathfrak{q} \trianglelefteq \mathcal{O}_L =: l$ such that $\mathfrak{q}|\mathfrak{p}$. Let $D(\mathfrak{q}) := \{\sigma \in \mathrm{Gal}\left(L/K\right) | \sigma(\mathfrak{q}) = \mathfrak{q}\}$ denote the **decomposition group** of $\mathfrak{q}$. Then

[6] I you don't know number theory, today's lecture won't make much sense. Feel free to skip it.

$\mathcal{O}_{L/\mathfrak{q}} \supseteq \mathcal{O}_{K/\mathfrak{p}}$ is an extension of finite fields and every $\sigma \in D(\mathfrak{q})$ induces $\overline{\sigma} \in \mathrm{Gal}(l/k)$.

Fact 3.19. If L/K is finite Galois, $\mathfrak{p} \trianglelefteq \mathcal{O}_K$ unramified in L/K. Then for any prime divisor $\mathfrak{q} \in \mathrm{Spec}\,(\mathcal{O}_L)$ of $\mathfrak{p}$, we get $D(\mathfrak{q}) \cong \mathrm{Spec}\left(l/k\right)$, $\sigma \mapsto \sigma$, where $l = \mathcal{O}_{L/\mathfrak{q}} \supseteq k = \mathcal{O}_{K/\mathfrak{p}}$.

In this situation $k = \mathbb{F}_{p^n} \subseteq l = \mathbb{F}_{p^{m \cdot n}}$ and then Frob_{p^n} generates $\mathrm{Gal}(l/k)$.

Definition 3.19.46. In the setting of Fact 3.19, the **Artin symbol**, $\left(\frac{L|K}{\mathfrak{q}}\right)$, is the unique element σ in $D(\mathfrak{q}) \leqslant \mathrm{Gal}\left(L/K\right)$ such that for any $a \in \mathcal{O}_L$ one has $\sigma(a) \equiv a^{(p^n)} \pmod{\mathfrak{q}}$. In other words $\left(\frac{L|K}{\mathfrak{q}}\right)$ corresponds to Frob_{p^n} under the isomorphism from Fact 3.19.

One writes $\left(\frac{L|K}{\mathfrak{p}}\right)$ (also called **Artin symbol**) for the conjugacy class of $\left(\frac{L|K}{\mathfrak{q}}\right)$ for $\mathfrak{q}|\mathfrak{p}$. Note that this is well-defined since

$$\left(\frac{L|K}{\sigma(\mathfrak{q})}\right) = \sigma \left(\frac{L|K}{\mathfrak{q}}\right) \sigma^{-1}$$

and

$$D(\sigma(\mathfrak{q})) = \sigma D(\mathfrak{q}) \sigma^{-1}.$$

Definition 3.19.47. Let $S \subseteq \mathbb{P}$. The **natural density of S** is defined as

$$d(S) := \lim_{x \to \infty} \frac{\#S \cap [0, x]}{\#\mathbb{P} \cap [0, x]}$$

(if this limit exists).

Theorem 3.20 (Čhebotarev Density Theorem)**.** Let $K/\mathbb{Q}$ be finite Galois and $G = \mathrm{Gal}\left(K/\mathbb{Q}\right)$. Let $C \subseteq G$ be a conjugacy class in G. Let $S_K := \{p \in \mathbb{P} | p \text{ is unramified in } K/\mathbb{Q} \text{ and } \left(\frac{K|\mathbb{Q}}{\mathfrak{p}}\right) = C\}$.

Then $d(S_K) = \frac{\#C}{\#G}$. In particular, S_K is infinite.

Remark 3.20.48. If $K \subseteq L$ and $L/\mathbb{Q}$, $K/\mathbb{Q}$ are Galois, then $S_L \subseteq S_K$.

Theorem 3.21. Let $\sigma_0 \in \mathrm{Gal}(\mathbb{Q})$. Then there is a non-principal ultrafilter $\mathcal{U}$ on $\mathbb{P}$ such that if $(L, \tilde{\sigma_1}) := \prod_{\mathcal{U}} \left(\mathbb{F}_p^{\mathrm{alg}}, \mathrm{Frob}_p\right)$ (working in $\mathcal{L}_{\mathrm{ring}} \cup \{\sigma\}$) then $\sigma_1 := \tilde{\sigma_1}|_{\mathbb{Q}^{\mathrm{alg}}}$ is conjugate to σ_0.

Proof. For $K/\mathbb{Q}$ finite Galois, let $\sigma_0^{(K)} := \sigma_0|_K \in \mathrm{Gal}\left(K/\mathbb{Q}\right)$. Let $C^{(K)}$ be the conjugacy class of $\sigma_0^{(K)}$ in $\mathrm{Gal}\left(K/\mathbb{Q}\right)$. Let S_K as in Theorem 3.20 (for $C^{(K)}$).

By Theorem 3.20, S_K is infinite. Write $\mathbb{Q}^{\mathrm{alg}} = \bigcup_{n\in\mathbb{N}} K_N$, $K_0 = \mathbb{Q} \subseteq K_1 \subseteq K_2 \subseteq \ldots$ such that every $K_n/\mathbb{Q}$ is finite Galois.

Clearly $S_{K_{n+1}} \subseteq S_{K_n}$ for all n (see Remark 3.20.48)

Let $\mathcal{U}$ be an ultrafilter containing all S_{K_n} and all cofinite sets (in particular, $\mathcal{U}$ is non-principal).

Claim 1. $(L, \tilde{\sigma_1}) := \prod_{\mathcal{U}} \left(\mathbb{F}_p^{alg}, \mathrm{Frob}_q\right)$ *works!*

Subproof. It suffices to show that $\sigma_0^{(K_n)}$ and $\sigma_1^{(K_n)} := \tilde{\sigma_1}|_{K_n}$ are conjugate (in $\mathrm{Gal}\left(K_n/\mathbb{Q}\right)$) for all n.

As $S_{K_n} \in \mathcal{U}$ by construction, we get $(L, \tilde{\sigma_1}) \twoheadleftarrow \prod_{p\in S_{K_n}} (\mathbb{F}_q^{\mathrm{alg}}, \mathrm{Frob}_p)$. For $p \in S_{K_n}$ choose $\mathfrak{q}_p | p$ a prime in $\mathcal{O}_{K_n}$.

We have

$$\mathcal{O}_{K_n} \overset{\Delta}{\hookrightarrow} \prod_{p\in S_{K_n}} \mathcal{O}_{K_n} \twoheadrightarrow \prod_{p\in S_{K_n}} \mathcal{O}_{K_n}/\mathfrak{q}_p \leqslant \prod_{p\in S_{K_n}} \mathbb{F}_p^{\mathrm{alg}} \twoheadrightarrow L$$

where the composition is injective. Fix diagram

Let $\{\tau_1, \ldots, \tau_m\}$ be the conjugacy class of $\sigma_0^{(K_n)}$. $S_{K_n} = S_1 \sqcup \ldots \sqcup S_m$, where $p \in S_i \iff \left(\frac{K_n|\mathbb{Q}}{\mathfrak{q}_p}\right) = \tau_i$.

Since $\mathcal{U}$ is an ultrafilter, there exists $i_0 \leqslant m$, such that $S_{i_0} \in \mathcal{U}$, so $\sigma_1^{(K_n)} = \tau_{i_0}$ proving the claim. ■

□

Proof of Theorem 3.9. , Let $K_0 \subseteq \mathbb{Q}^{\mathrm{alg}}$ with $\mathrm{Gal}(K_0)$ procyclic. Choose a topological generator σ_0 of $\mathrm{Gal}(K_0) \leqslant \mathrm{Gal}(\mathbb{Q})$. $\mathrm{Fix}(\sigma_0) = \left(\mathbb{Q}^{\mathrm{alg}}\right)^{\sigma_0} = K_0$.

If $\sigma_1 = \tau\sigma_0\tau^{-1}$, then $\mathrm{Fix}(\sigma_1) = \tau(K_0) \cong K_0$.

By Theorem 3.21, there is $\mathcal{U}$ on $\mathbb{P}$ such that if $(L, \tilde{\sigma_1}) = \prod_{\mathcal{U}}(\mathbb{F}_p^{\text{alg}}, \text{Frob}_p)$, then $\sigma_1 := \tilde{\sigma_1}|_{\mathbb{Q}^{\text{alg}}}$ is conjugate to σ_0.

$$\begin{aligned} K_0 &= \text{Fix}(\sigma_0) \cong \text{Fix}(\sigma_1) \\ &= \underbrace{\text{Fix}(\tilde{\sigma_1})}_{\prod_{\mathcal{U}} \mathbb{F}_p} \cap \mathbb{Q}^{\text{alg}} \\ &= \text{Abs}(\prod_{\mathcal{U}} \mathbb{F}_p). \end{aligned}$$

□

4 The Measure of Chatzidakis-van den Dries-Macintyre and Applications

Recall the Lang-Weil Estimates (3.1):

For all n, N there exists $C(n, N)$ such that for every finite field $\mathbb{F}_q$ and absolutely irreducible $\mathbb{F}_q$ variety $V \subseteq \mathbb{A}^n$ defined with polynomials of degree $\leqslant N$, we have

$$|\#V(\mathbb{F}_q) - q^{\dim(V)}| \leqslant Cq^{\dim(V)-\frac{1}{2}}.$$

Theorem 4.1 (Main Theorem of [CDM92])**.** Let $\varphi(\overline{x}, \overline{y})$ be a n $\mathcal{L}_{\text{ring}}$-formula, $|\overline{x}| = n$, $|\overline{y}| = m$. Then there is a finite set $D \subseteq \{0, \ldots, n\} \times \mathbb{Q}_{>0}$ of pairs (d, μ) ("dimension" and " multiplicity") and a constant $C = C(\varphi) \in \mathbb{N}$ such that for every finite field $\mathbb{F}_q$ and parameter $\overline{b} \in \mathbb{F}_q^m$ if $\varphi(\mathbb{F}_q^n, \overline{b}) \neq \varnothing$, then

$$|\#\varphi(\mathbb{F}_q^n, \overline{b}) - \mu q^d| \leqslant Cq^{d-\frac{1}{2}}. \tag{$*$}$$

for some $(d, \mu) \in D$.

Moreover, for every $(d, \mu) \in D$, there is a formula $\varphi_{d,\mu}(\overline{y})$ such that for every $\mathbb{F}_q$ and $\overline{b} \in \mathbb{F}_q^m$ such that $\mathbb{F}_q \models \varphi_{d,\mu}(\overline{b})$ iff $(*)$ holds for (d, μ).

Remark 4.2. (1) If $\varphi(\overline{x}, \overline{y})$ expresses that $\overline{x} \in V_{\overline{y}}$ for an absolutely irreducible variety $V_{\overline{y}}$ of dimension d, then $D = \{(d, 1)\}$ and C comes from the Lang-Weil Estimates (3.1).

(2) Let $\varphi(x, y) :\equiv \exists z.\ z^2 = x + y$ (or $\varphi(x) :\equiv \exists z.\ z^2 = x$). Then $D = \{(1, \frac{1}{2}), \underbrace{(1, 1)}_{\text{for characteristic 2}}\}$. $C = 1$ works. Moreover $\varphi_{1,1}(y) \equiv 1 + 1 = 0 \vee \exists^{\leqslant 5} x.\ x = x$. $\varphi_{1,\frac{1}{2}} \equiv 1 + 1 \neq 0 \vee \exists^{\leqslant 4} x.\ x = x$.

(3) For $q \gg 0$, the $\varphi_{d,\mu}(\mathbb{F}_q)$ partition $\{\overline{b} \in \mathbb{F}_q^m | \varphi(\mathbb{F}_q, \overline{b}) \neq \varnothing\}$. easy exercise

(4) Given $\varphi(x, y)$, there exist $B > 0$ and $r > 0$ such that for all $\mathbb{F}_q$ and

$\bar{b} \in \mathbb{F}_q^m$,

$$\#\varphi(\mathbb{F}_q, \bar{b}) \leqslant B \vee \#\varphi(\mathbb{F}_q, \bar{b}) > rq.$$

[Lecture 13, 2024-11-26]

Remark 4.3. Let φ, D, C, $\varphi_{d,\mu}$ as in Theorem 4.1.

Then for $q \gg 0$ and $\bar{b} \in \mathbb{F}_q^m$ with $\mathbb{F}_q \models \varphi_{0,\mu}(\bar{b})$, one has

$$|\varphi(\mathbb{F}_q, \bar{b})| = \mu.$$

Proposition 4.4 (Some Applications)**.** (i) There is no $\mathcal{L}_{\text{ring}}$-formula $\varphi(x)$ such that for infinitely many $q \in Q$, $\varphi(\mathbb{F}_{q^2}) = \mathbb{F}_q$.[a]

(ii) There is no $\mathcal{L}_{\text{ring}}$-formula $\varphi(x)$ which defines the set of generators of $\mathbb{F}_q^\times$ (a cyclic group) for all $q \in Q$ (even for all powers of a fixed prime).

[a] Note that individually they are definable. However, the proposition says that they are not *uniformly* definable.

Proof. (i) Let $B > 0$ and $r > 0$ as in Remark 4.2 (iv). For $q \in Q$ such that $q > B$ and $q > \frac{1}{r}$ ($\iff rq^2 > q$) one has $\#\mathbb{F}_q = q \neq \#\varphi(\mathbb{F}_{q^2})$.

(ii) $(\mathbb{F}_q^\times, \cdot) \cong \mathbb{Z}_{q-1}$, so the set of generators has cardinality $\varphi(q-1)$[7]

Observe

(a) $p \in \mathbb{P} \implies \varphi(p^n = (p-1)p^{n-1}$, as $(a,p) = 1 \iff (a, p^n) = 1$ for $n \geqslant 1$.

(b) $\varphi(mn) = \varphi(m)\varphi(n)$ if $(m,n) = 1$ by the Chinese remainder theorem.

As $\varphi(q^n) \geqslant \sqrt{p^n}$ for all p and $n > 0$ we get from (a) and (b) that $\varphi(n) \geqslant \sqrt{\frac{n}{2}}$ for all $n \in \mathbb{N}$.

In particular $\{q \in Q | \varphi(q-1) \leqslant B\}$ is finite.

Given $r > 0$ we will show that there is $p^M = q \in Q$ such that $\varphi(p^M - 1) < r(p^M - 1) \leqslant rp^M$. By (a) and (b) we have for any $n \geqslant 1$

$$\frac{\varphi(n)}{n} = \prod_{\substack{l \text{ prime} \\ l|n}} \left(1 - \frac{1}{l}\right). \tag{+}$$

Choose distinct primes $l_1, \ldots, l_m$ and set $M := \prod_{i=1}^m (l_i - 1)$.

For $p \in \mathbb{P}$ by the little Fermat we get

$$p^M = k^{l_i - 1} \equiv 1 \pmod{l_i}$$

[7] Euler's totient function

for $i = 1, \ldots, m$, so $l_i | \left(p^M - 1\right)$ for all i.

Thus by (+),

$$\frac{\varphi(p^M - 1)}{p^M - 1} \leqslant \prod_{i=1}^{m} \left(1 - \frac{1}{l_i}\right).$$

The right hand side can be made $< r$, use for example the prime number theorem.

□

Corollary 4.5. Let $\varphi(x, y)$, D, $C = C(\varphi)$, $\varphi_{d,\mu}(y)$, $(d, \mu) \in D$ be as in Theorem 4.1.

For every $F \models \mathsf{Psf}$, the set F^m is then partitioned by $\varphi_{d,\mu}(F)$, $(d, \mu) \in D \cup \{\varnothing\}$, where $\varphi_{\varnothing}(y) :\equiv \neg\exists x.\ \varphi(x, y)$.

Proof. Indeed $T_f \cup \{\exists^{\infty} x.\ x = x\} \models$ the φ_I, $I \in D \cup \{\varnothing\}$ partition F^m (by Remark 4.2 (3)). □

Definition 4.5.49. Given an $\mathcal{L}_{\text{ring}}$-formula $\varphi(x, y)$, $F \models \mathsf{Psf}$, $\bar{b} \in F^m$ we define the **dimension** of $\varphi(x, \bar{b})$ as the unique $d \in \{0, \ldots, n\}$ and the **multiplicity** of $\varphi(x, \bar{b})$ as the unique $\mu \in \mathbb{Q}_{>0}$ such that $F \models \varphi_{d,\mu}(\bar{b})$, $(d, \mu) \in D$

(if $\varphi(F, \bar{b}) \neq \varnothing$).

If $\varphi(F, \bar{b}) = \varnothing$, set $\varphi(x, \bar{b})$ is said to be of dimension and multiplicity 0.

Lemma 4.6. If $F \models \mathsf{Psf}$, $F \models \forall x.\ (\varphi(x, b) \leftrightarrow \psi(x, c))$, then $\dim(\varphi(x, b)) = \dim(\psi(x, c))$ and $\mu(\varphi(x, b)) = \mu(\psi(x, c))$.

Thus for $S \subseteq F^n$ definable with parameters, $(\dim(S), \mu(S))$ is well-defined.

Proof. This holds for $q \gg 0$ (depending on the data), so it holds in Psf. □

Proposition 4.7. Let $F \models \mathsf{Psf}$ and $S \subseteq F^{n_1}$, $T \subseteq F^{n_2}$ be definable sets (with parameters).

Then:

(1) If V is an absolutely irreducible variety defined over F of algebraic dimension d, then $\dim(V(F)) = d$ and $\mu(V(F)) = 1$ (including $\dim_{\text{alg}}(V) = 0$, where V is just a point, which lies in F).

(2) If S and T are disjoint and $n = n_1 = n_2$, then

(a) $\dim(S \cup T) = \max(\dim(S), \dim(T))$.

(b) $\mu(S \cup T) = \begin{cases} \mu(S) + \mu(T) & \text{if } \dim(S) = \dim(T), \\ \max(\mu(S), \mu(T)) & \text{otherwise.} \end{cases}$

(3) Assume that $f\colon S \twoheadrightarrow T$ is a definable surjection such that for all $c \in T$, $\dim(f^{-1}(c)) = d$ for some fixed d.

(4) Assume that $f\colon S \twoheadrightarrow T$ is as before assume that in addition $\mu(f^{-1}(c)) = \mu$ for all $c \in T$ and some fixed $\mu \in Q_{>0}$.

Then $\mu(S) = \mu \cdot \mu(T)$.

Proof. Both S and T (and V or f in (1), (3)) are defined in some $F_0 \preceq F$ with F_0 countable.

So we may assume that F is countable.

By Corollary 3.10 we find an ultrafilter $\mathcal{U}$ on Q such that $F \equiv \prod_{\mathcal{U}} \mathbb{F}_q$.

Since Q is countable, $\mathcal{U}$ is ω-incomplete. Thus $\prod_{\mathcal{U}} \mathbb{F}_q$ is $\aleph_1$-saturated.

So by universality of saturated models, we get $\iota\colon F \xrightarrow{\preceq} \prod_{\mathcal{U}} \mathbb{F}_q$. Thus we may assume $F = \prod_{\mathcal{U}} \mathbb{F}_q$.

(1) Follows from the corresponding result for large finite fields:

If $V = V_{\bar{b}}$ and $\bar{b} = \bar{b}_{q/\sim}$, then for almost all $q \in Q$, $V_{\bar{b}_q}$ is absolutely irreducible of $\dim_{\text{alg}}(V_{\bar{b}_q}) = \dim(V_{\bar{b}})$, so we finish by the Lang-Weil Estimates (3.1).

(2) As before, being disjoint is true almost everywhere. ...

(3) Exercise.

□

Corollary 4.8. Let S be a *non-empty* definable set in some $F \models \mathsf{Psf}$. Then the following defines a finitely additive[a] probability measure (with values in $[0,1] \cap \mathbb{Q}$) on definable subsets of S:

For $T \subseteq S$ definable, set

$$m_S(T) := \begin{cases} \frac{\mu(T)}{\mu(S)} & \text{if } \dim(S) = \dim(T), \\ 0 & \text{otherwise.} \end{cases}$$

[a] not σ-additive!

Proof. Proposition 4.7 (2). □

Corollary 4.9. Let $F \models \mathsf{Psf}$ and $S \subseteq F^n$ be definable. Consider S as a subset of $(F^{\mathrm{alg}})^n$. Let V be the F-algebraic set $\subseteq \mathbb{A}^n$ such that $V(F^{\mathrm{alg}}) = \overline{S}^{\mathrm{Zar}}$, where $\left(\cdot^{\mathrm{Zar}}\right)$ is the closure wrt. the Zariski topology on $\left(F^{\mathrm{alg}}\right)^n$.

Then $\dim(S) = \dim(V(F)) = \dim_{\mathrm{alg}}(V)$. In particular, if $A \subseteq F$, then $\mathrm{acl}_{\mathsf{Psf}}(A) = Q(\langle A \rangle)^{\mathrm{alg}} \cap F$.

More generally we have

$$\dim(S) = \max\{\mathrm{trdeg}\left(F(\overline{a})/F\right) | \overline{a} \in S(F'), F' \geq F\} \qquad (*)$$

Proof. V is F-definable, since it is $\mathrm{Gal}(F)$-invariant.

By Theorem 2.15, there is an F-algebraic $W(F) \subseteq F^{n+l}$ such that $\pi(W(F)) = S$, with finite fibers, say bounded in cardinality by $N \in \mathbb{N}$.

Shrinking W if necessary, we may assume that $W(F)$ is Zariski dense in $W(F^{\mathrm{alg}})$ (replace W by W^* , where $\underbrace{\overline{W(F)}^{\mathrm{Zar}}}_{\text{in } F^{\mathrm{alg}}} = W^*(F^{\mathrm{alg}})$, with $W^* \subseteq W$).

Then the absolutely irreducible components $W_1, \ldots, W_k$ are alle defined over F.

By Proposition 4.7 (3), we get $\dim(S) = \dim(W(F))$. By Proposition 4.7 and induction on dimension we get

$$\dim(W(F)) = \dim_{\mathrm{alg}}(W)$$

and

$$\mu(W(F)) = \#\,\mathrm{argmax}_i\, \mu(W_i).$$

$$\pi \colon W(F) \twoheadrightarrow S$$

is definable and surjective and S is Zarisiki-dense in $V(F^{\mathrm{alg}})$, so $\dim_{\mathrm{alg}}(V) \leqslant \dim_{\mathrm{alg}}(W)$

Claim 1. $\dim_{alg}(W) = \dim_{alg}(V)$.

Subproof. By the above it suffices to show $\dim_{\mathrm{alg}}(W_i) \leqslant \dim_{\mathrm{alg}}(V)$ for all i.

Let $\overline{a} \in F'^{n+l}$, $F' \geq F$, such that $\mathrm{loc}\left(\overline{a}/F\right) = W_i$ (this exists since $W_i(F)$ is Zariski dense in $W_i(F^{\mathrm{alg}})$).

Let $\overline{a} = \overline{a}_1\overline{a}_2$, with $\overline{a}_1 \in F'^m$, $\overline{a}_2 \in F'^l$.

Then $\pi(\overline{a}) = \overline{a}_1$ and by assumption

$$F' \models \exists^{\leqslant N} \overline{x}_2.\ (\overline{a}_1, \overline{x}_2) \in W_i \qquad (**)$$

If $d = \operatorname{trdeg}\left(\overline{a}_2/F\overline{a}_1\right) > 0$, then $Z := \operatorname{loc}(\overline{a}_2/F(\overline{a}_1)^{\mathrm{alg}} \cap F')$ is absolutely irreducible, (because $F(\overline{a}_1)^{\mathrm{alg}} \cap F(\overline{a}_2)/F(\overline{a}_1)^{\mathrm{alg}} \cap F'$ is regular) of $\dim_{\mathrm{alg}} > 0$. So it contains infinitely many F'-rational points (by PAC), contradicting (**) as $Z \subseteq \pi^{-1}(\overline{a}_1) \cap W_i$. ■

□

[Lecture 14, 2024-11-29]

- Given any field K and $X \subseteq K^n$, three is a smallest algebraic set $W(K^{\mathrm{alg}}) \subseteq \left(K^{\mathrm{alg}}\right)^n$ such that $X \subseteq W(K^{\mathrm{alg}})$, namely $\overline{X}^{\mathrm{Zar}}$ (the Zariski closure taken in K^{alg}).

  Clearly, as W is $\mathrm{Aut}\left(K^{\mathrm{alg}}/K\right)$-invariant, it is definable over K.

- If V is a K-algebraic set, we will construct a K-algebraic set $V^* \subseteq V$ with the following two properties:

  (i) Every absolutely irreducible K-variety $\tilde{V} \subseteq V$ satisfies $\tilde{V} \subseteq V^*$.

  (ii) The absolutely irreducible components of V^* are all definable over K.

We will see that in case $X = V(K)$ and K is PAC (e.g. if $K \models \mathsf{Psf}$), then $V^*(K^{\mathrm{alg}}) = \overline{X}^{\mathrm{Zar}}$, i.e. the two constructions coincide in this case.

4.1 The Decomposition-Intersection Procedure

To a K-algebraic set $V \subseteq \mathbb{A}^n$ one associates a K-algebraic set $V' \subseteq V$ as follows: Let $V = V_1 \cup \ldots \cup V_l$ be the decomposition into absolutely irreducible components of V.

- Then $\underbrace{\mathrm{Aut}\left(K^{\mathrm{alg}}/K\right)}_{G} \curvearrowright \{V_1, \ldots, V_l\}$ via $\sigma \circ V_i(K^{\mathrm{alg}}) = (\sigma V_i)(K^{\mathrm{alg}})$.

- For $i = 1, \ldots, l$ let $W_i := \bigcap_{\sigma \in G} \sigma(V_i)$, a K-algebraic set for all i.

  Note that $V_i(K^{\mathrm{alg}}) \cap K^n = W_i(K^{\mathrm{alg}}) \cap K^n = W_i(K^n)$.

- Set $V' := \bigcup_{i=1}^{l} W_i$, a K-algebraic set with $V' \subseteq V$ by construction. Moreover

  (i)' Every absolutely irreducible K-variety $\tilde{V} \subseteq V$ satisfies V'.

  (iii)' $V'(K) = V(K)$.

- Iterating this, construct a decreasing sequence $\left(V^{(m)}\right)_{m \geqslant 0}$ of K-algebraic sets $V^{(0)} := V$, $V^{(m+1)} := \left(V^{(m)}\right)'$.

  Since the topology is Noetherian, the sequence stabilizes at some r, i.e. $V^{(r)} = V^{(r+1)}$. $V^* := V^{(r)}$ is called the **K-absolute kernel of V**.

Lemma 4.10. Let V be a K-algebraic set and V^* be its K-absolute kernel. Then V^* is a K-algebraic subset of V and one has that

(i) every absolutely irreducible K-variety $\tilde{V} \subseteq V$ satisfies $\tilde{V} \subseteq V^*$,

(ii) all absolutely irreducible components of V^* are definable over K and

(iii) $V^*(K) = V(K)$.

Proof. (i) and (iii) hold by induction (on m, it holds for $V^{(m)}$).

ad (i): The construction of V' shows that if not all absolutely irreducible components of V are definable over K, then $V' \subsetneq V$.

Indeed, let $V_1, \ldots, V_l$ be the absolute irreducible components of V with V_i not definable over K. Then by construction, $\bigcap_{\sigma \in G} \sigma V_i = W_i \supsetneq V_i$. Thus $V_i \nsubseteq W_j$ for any j, as ($V_i \nsubseteq V_j$ for all $i \neq i$). □

Proposition 4.11. Let K be PAC and let $V \subseteq \mathbb{A}^n$ be a K-algebraic set. Let V^* be the K-absolute kernel of V.

Then $V^*(K^{\mathrm{alg}}) = \overline{V(K)}^{\mathrm{Zar}}$ in $\left(K^{\mathrm{alg}}\right)^n$.

In other words, V^* is the smallest K-algebraic set containing $V(K)$.

Proof. By Lemma 4.10 (iii), $V^*(K^{\mathrm{alg}}) \supseteq \overline{Z(K)}^{\mathrm{Zar}}$.

By Lemma 4.10 (ii), the absolutely irreducible components $V_1^*, \ldots, V_k^*$ are all defined over K, so as K is PAC, $V_i^*(K)$ is Zariski dense in V_i for $i = 1, \ldots, k$. Thus $\overline{V(K)}^{\mathrm{Zar}} \supseteq V_i^*(K^{\mathrm{alg}})$ for $i = 1, \ldots, k$, so $V^*(K^{\mathrm{alg}}) \subseteq \overline{V(K)}^{\mathrm{Zar}}$. □

Definition 4.11.50. For a K-algebraic set $V \subseteq \mathbb{A}^n$ with absolutely irreducible components $V_1, \ldots, V_l$ we define $\alpha(V) \in \{-\infty, 0, \ldots., n-1\}$ as follows:

- $\alpha(V) := -\infty$ iff all V_i are definable over K,
- otherwise $\alpha(V) := \max\{\dim(V_i) | V_i \text{ not definable over } K\} \in \{0, \ldots, n-1\}$.

Lemma 4.12. If $V \subseteq \mathbb{A}^n$ is a K-algebraic set and $r \geqslant 0$ is minimal such that $V^{(r+1)} = V^{(r)}$ (i.e. $V^{(r)} = V^*$ is the K-absolute kernel of V), then $r \leqslant n$.

Proof. We have

(a) $\alpha(V) = -\infty$ iff $V = V'$ iff $V = V^*$ iff $r = 0$.

(b) If $\alpha(V) \geqslant d$ then $\alpha(V') < \alpha(V)$:

Indeed, Let $V_1, \dots, V_l$ be the absolutely irreducible components of V. $\alpha = \alpha(V) \geqslant 0$. Reordering the sequence we may assume

- $V_1, \dots, V_e$ are definable over K with $\dim(V_i) \geqslant \alpha$.

  We have $W_i = V_i$.

- $V_{e+1}, \dots, V_f$ are not definable over K and satisfy $\dim(V_i) = \alpha$ for $i = e+1, \dots, f$,

  in this case $W_i \subseteq V_i$, so $\dim(W_i) < \alpha$,

- $V_{f+1}, \dots, V_l$ have dimension $< \alpha$.

The irreducible components of V' are $V_1, \dots, V_e$ and some $U_1, \dots, U_N$ with $\bigcup_{i=1}^{N} U_i = \bigcup_{i=e+1}^{l} W_i$ so $\dim(U_i) < \alpha$ for all i.

□

Lemma 4.13. Let $f_1, \dots, f_r \in K[X_1, \dots, X_n]$ and let $V = V(\{f_1, \dots, f_r\})$ be the associated K-algebraic subset of $\mathbb{A}^n$.

Let $V_1, \dots, V_l$ be the absolutely irreducible components of V.

Let K'/K be finite Galois such that all V_i are definable over K'. Let $b_1, \dots, b_N$ be a K-basis of K' and let $g_{i_1}, \dots, g_{i_{r(i)}} \in K'[X]$ such that $V_i = V(\{g_{i_1}, \dots, g_{i_{r(i)}}\})$.

Let $g_{i,j,\nu} \in K[\overline{X}]$, $\nu = 1, \dots, N$ such that $g_{i,j} = \sum_{\nu=1}^{N} b_\nu g_{i,j,\nu}$. Then $W_i = V(\{g_{i,j,\nu} | 1 \leqslant j \leqslant r(i), 1 \leqslant \nu \leqslant N\})$ and thus

$$V' = V\left(\left\{ \prod_{1 \leqslant i \leqslant l} g_{i,j(i),\nu(i)} \;\middle|\; \begin{matrix} j\colon \{1,\dots,l\} \to \mathbb{N}, j(i) \leqslant r(i), \\ \nu\colon \{1,\dots,l\} \to \{1,\dots,N\} \end{matrix} \right\}\right)$$

Proof. Note that every $\sigma \in G = \mathrm{Gal}\left(K'/K\right)$ induces a (multiplicative) character $\sigma\colon {K'}^\times \to {K'}^\times$.

By the linear independence of pairwise distinct characters, the matrix

$$(\sigma_i(b_j))_{\substack{1 \leqslant i \leqslant n \\ 1 \leqslant j \leqslant N}} \in (K')^{n \times n}$$

is regular, where the σ_i enumerate G. Indeed, any linear dependence of the row vectors $(\sigma_i(b_1), \dots, \sigma_i(b_N))$ would yield a linear dependence of the characters, as the b_i form a K-basis of K' and σ_i is K-linear for all i.

Applying this to the equation

$$g_{ij} = \sum_{\nu=1}^{N} b\nu g_{i,j,\nu} = 0$$

and its G-conjugates, we infer $W_i = \bigcap_{j=1}^{N} \sigma_j(V_i) = V\left(\left\{g_{i,j,\nu} |^{1 \leqslant j \leqslant r(i)}_{1 \leqslant \nu \leqslant N}\right\}\right)$. □

Remark 4.14. Instead of working with K'/K finite Galois, we may use any K'/K finite separable such that each V_i is defined over K'.

Proof. Exercise. □

Goal. *We want to understand how the complexity of V' depends on the complexity of V, in a uniform way, thus also the complexity of V^* (by Lemma 4.12).*

Definition 4.14.51.

- $\mathcal{L}_{\mathbf{root}} := \mathcal{L}_{\text{ring}} \cup \{\rho_d | d \geqslant 2\}$, where ρ_d is a d-ary function.
- A **field with root functions** is an $\mathcal{L}_{\text{root}}$-structure such that K is a field and for every $d \geqslant 2$ and the following universal axiom is satisfied:

$$\forall x_1, \ldots, x_d, t.\ (t^d + x_1 t^{d-1} + \ldots + x_{d-1} t + x_0 = 0 \implies \rho(\overline{x})^d + x_1 \rho(\overline{x})^{d-1} + \ldots + x_0 = 0).$$

Observe.

- *In any field with root functions, if a monic polynomial has a root, the root function applied to its coefficients is a root.*
- *Every field can be expanded to a field with root functions (but this is of course not unique).*

Lemma 4.15. For every $d > 0$, there is a *quantifier-free* $\mathcal{L}_{\text{root}}$-formula $\text{Irr}_d(x_1, \ldots, x_d)$, such that for every field K with root functions

$$K \models \text{Irr}_d(\overline{x}) \text{ iff } t^d + x_1 t^{d-1} + \ldots + x_d \in K[t]$$

is irreducible.

Proof. It suffices to show that for K, L fields with root functions A a common $\mathcal{L}_{\text{root}}$-substructure, and $a_1, \ldots, a_d \in A$, we have that

$$t^d + a_1 t^{d-1} + \ldots + a_d =: p_{\overline{a}}(t)$$

is irreducible in $K[t]$ iff it is irreducible in $L[t]$.

(This uses that Irr_d is given by a first-order $\mathcal{L}_{\text{ring}}$-formula.)

Let $F := Q(A)$. Then since A is closed under root functions, F is relatively algebraically closed in K and L. Now use the following fact from algebra:

Fact* 4.15.52. If F is relatively algebraically closed in K, then any $f(t) \in F[t]$ irreducible stays irreducibly in $K[t]$.

Subproof. Otherwise $f(t) = g(t) \cdot h(t)$, but then some coefficients of g and h are in $(K \backslash F) \cap F^{\mathrm{alg}}$. ■

□

[Lecture 15, 2024-12-03]

Lemma 4.16. Let K be a field with root functions and let $A \subseteq K$ be a subset. Then the $\mathcal{L}_{\mathrm{root}}$-substructure generated by A is $\mathrm{Int}_K(\langle A \rangle_{\mathcal{L}_{\mathrm{ring}}})$, the integral closure in K of the subring generated by A.

In particular, the field of fractions of $\langle A \rangle_{\mathcal{L}_{\mathrm{root}}}$ equals $Q\left(\langle A \rangle_{\mathcal{L}_{\mathrm{ring}}}\right)^{\mathrm{alg}} \cap K$.

Proof. This follows from the definitions, once one notes that if α is integral over R and β is integral over $R[\alpha]$, then β is integral over R (for an integral domain R). □

Notation 4.16.53. If K is a field with root functions an $A \subseteq K$, we write $\langle A \rangle$ for $\langle A \rangle_{\mathcal{L}_{\mathrm{ring}}}$ and $\langle A \rangle_{\mathrm{root}}$ for $\langle A \rangle_{\mathcal{L}_{\mathrm{root}}} = \mathrm{Int}_K(\langle A \rangle)$

Situation 4.17. Let K be a field, $X = (X_1, \ldots, X_n)$ and $Z = (Z_1, \ldots, Z_m)$. Fix $f = (f_1, \ldots, f_r)$ where $f_i \in \mathbb{Z}[X, Z]$ for $i = 1, \ldots, r$. We are interested in the family of algebraic subsets of $\mathbb{A}^n$ given by

$$V_{\overline{a}} := V\{(f_1(X, \overline{a}), \ldots, f_r(X, \overline{a})\}$$

for $\overline{a} \in K^m$.

We write $V_{K,\overline{a}}$ to emphasize that we consider $V_{\overline{a}}$ as a K-algebraic set.

By $V'_{K,\overline{a}}$ and $V^*_{K,\overline{a}}$ we denote the K-algebraic sets obtained by the intersection-decomposition procedure, with K as the defining field.

Now let k be an arbitrary field, $\overline{a} \in K^m$ and $K_0 := Q\left(\langle \overline{a} \rangle\right)^{\mathrm{alg}} \cap K$. Let $K_1 = K_0(\alpha)$ be a finite separable extension such that all absolutely irreducible components $V_1, \ldots, V_k$ of $V_{\overline{a}}$ are defined over K_1. We may and will assume that $\alpha \in \mathrm{Int}_{K_0^{\mathrm{alg}}}(\langle \overline{a} \rangle)$, i.e. $\mathrm{MiPo}\left(\alpha / K_0\right) =: q(T) \in \langle \overline{a} \rangle[T]$. Assume $\deg(q) = N$. For $i = 1, \ldots, k$ choose $g_{i,1}, \ldots, g_{i,r(i)} \in K_1[X]$ such that

$$V_i = V\left(\{g_{i,1}, \ldots, g_{i,r(i)}\}\right)$$

and let $g_{i,j,\nu} \in K_0[X]$ such that

$$g_{i,j} = \sum_{\nu=0}^{N} \alpha^{\nu-1} g_{i,j,\nu}. \tag{$*$}$$

This is possible as $\left(b_\nu := \alpha^{\nu-1}\right)_{\nu=1}^{N}$ is a K_0-basis of K_1.

$$[K[\alpha] : K] = N, \tag{$**$}$$

as K_0 is relatively algebraically closed in K. Thus ($*$) is also the unique decomposition of $g_{i,j}$ in $K(\alpha)/K$.

Chasing denominators we may assume

$$g_{i,j} \in \mathrm{Int}_{K_0}\left(\langle \overline{a} \rangle\right)[X]. \tag{$***$}$$

We now look at the decomposition of V into $V_1, \ldots, V_k$ syntactically:

Definition 4.17.54. Let K be a field with root function and let f be as in Situation 4.17.

(1) A **potential decomposition for f** is a tuple

$$\mathcal{D} = (q(Z,T), g_1(X,Z), \ldots, g_k(X,Z)),$$

such that

D1 $q(Z,T)$ is an $\mathcal{L}_{\mathrm{root}}$-term (over $\varnothing$) that is polynomial and monic in T, i.e. it is of the form $q(Z,T) = T^N + c_1(X)T^{n-1} + \ldots + c_{N-1}(X)T + c_N(X)$ for some $\mathcal{L}_{\mathrm{root}}$-terms $c_i(Z)$ in Z.

D2 Each g_i is a tuple $(g_{i,j,\nu}(X,Z))_{\substack{1 \leqslant j \leqslant r(i) \\ 1 \leqslant \nu \leqslant N}}$ of $\mathcal{L}_{\mathrm{root}}$-terms that are polynomial in X.

(2) Let $\mathcal{D}$ be a potential decomposition for f as in (1) and $\overline{a} \in K^m$. Then $\mathcal{D}$ is an **actual decomposition of f at $\overline{a}$ over K** if the following conditions hold:

D3 $q(\overline{a}, T) \in K[T]$ is separable and irreducible in $K[T]$ (it is automatically monic by D1).

D4 If $\alpha \in K^{\mathrm{alg}}$ is a zero of $q(\overline{a}, T)$ and

$$g_{i,j}(X) := \sum_{\nu=1}^{N} g_{i,j,\nu}(X, \overline{a})\alpha^{\nu-1} \in K(\alpha)[X]$$

and

$$V_I := V(\{g_{i,1}, \ldots, g_{i,r(i)}\} \subseteq \left(K^{\mathrm{alg}}\right)^n$$

then $V_1, \dots, V_k$ are the absolutely irreducible components of $V_{\overline{a}}$ and pairwise distinct.

Lemma 4.18. (1) Let f be as in the Situation 4.17 and let $\mathcal{D} = (q, g_1, \dots, g_k)$ be a potential decomposition of f.

Then there is a quantifier free $\mathcal{L}_{\text{root}}$-formula $\text{Dec}_{\mathcal{D},f}(Z)$ such that for every field K with root functions and every $\overline{a} \in K^m$ one has that $\mathcal{D}$ is an actual decomposition for f at $\overline{a}$ over K iff

$$K \models \text{Dec}_{\mathcal{D},f}(\overline{a}).$$

(2) For every field K with root function and every $\overline{a} \in K^m$ there is an actual decomposition of f at $\overline{a}$ over K.

(3) If $\mathcal{D} = (q, g_1, \dots, g_k)$ is an actual decomposition of f at $\overline{a}$ over K then

$$V'_{K,\overline{a}} = V\left(\left\{\prod_{i=1}^{k} g_{i,j(i),\nu(i)}|^{j\colon \{1,\dots,k\}\to\mathbb{N}, j(i)\leqslant r(i)}_{\nu\colon \{1,\dots,k\}} \to \{1,\dots,N\}\right\}\right)$$

(4) There are finitely many potential decompositions $\mathcal{D}_1, \dots, \mathcal{D}_J$ of f, such that for every field with root function K and every $\overline{a} \in K^m$, there is $j \leqslant J$ such that $\mathcal{D}_j$ is an actual decomposition for f at $\overline{a}$ over K.

Proof. (1) Note that by Corollary 2.3 in any definable family of algebraic sets, the set of parameters giving rise to an absolutely irreducible variety is quantifier free $\mathcal{L}_{\text{ring}}$-definable. Working in $\mathcal{L}_{\text{root}}$ we get the result.

(2) By Lemma 4.16 and the discussion after Situation 4.17, in particular $(**)$ and $(***)$, $V_{K,\overline{a}}$ may be decomposed into absolutely irreducible components over $K_1 = K_0(\alpha)$, where $K_0 = Q(\langle \overline{a} \rangle_{\mathcal{L}_{\text{root}}})$ is relatively algebraically closed in K (Lemma 4.16) and α is separable algebraic over K_0 with

$$q(T) = \text{MiPo}\left(\alpha/K_0\right) \in \langle \overline{a} \rangle_{\mathcal{L}_{\text{root}}}[T]$$

(so $q(T)$ is also irreducible in $K[T]$).

(3) This holds by Lemma 4.13.

(4) This holds by compactness using (1) and (2).

□

Theorem 4.19. In Situation 4.17 there are finitely many quantifier free $\mathcal{L}_{\mathrm{root}}$-formulas, $\chi_1(z), \ldots, \chi_I(z)$, a function $M\colon \{1, \ldots, I\} \to \mathbb{N}$ and for every $1 \leqslant i \leqslant I$ and $1 \leqslant j \leqslant M(i)$ a finite tuple $h_{i,j}$ of $\mathcal{L}_{\mathrm{root}}$-terms of in (X, Z) that are polynomial in X such that in every field with root functions K the following hold:

(a) The sets $C_i := \chi_i(K)$, $i = 1, \ldots, I$, define a partition of K^m (where $C_i = \varnothing$ is not excluded).

(b) For any $\overline{a} \in C_i$, the absolutely irreducible components $V^*_{K,\overline{a}}$ are exactly the $M(i)$ distinct K-algebraic sets[a]

$$V(h_{i,j}(X, \overline{a})), j = 1, \ldots, M(i).$$

Here, $M(i) = 0$ means that $V^*_{K,\overline{a}} = \varnothing$.

[a] This is a slight abuse of notation, as the h_{ij} are tuples.

Proof. By Lemma 4.12 if $r \geqslant 0$ is minimal such that $V^{(r)}_{K,\overline{a}} = V^*_{K,\overline{a}}$, then $r \leqslant n$.

We thus conclude by iterating Lemma 4.18 (4), (1) and (2) at most n times.

Note that the different potential decompositions just cover but not necessarily partition K^n, but it s easy to make the cases disjoint (in a quantifier-free manner) setting $\chi_{x_{i+1}} :\equiv \chi'_{i+1} \wedge \left(\bigwedge_{j=1}^{i} \neg\chi'_j\right)$. □

Corollary 4.20 (Existence of Bounds for the Decomposition-Intersection Procedure)**.** For any $n, e \in \mathbb{N}$, there exist $D = D(n, e)$ and $M = M(n, e)$ such that for every field K and $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$, of degree $\leqslant e$ the following hold for the algebraic set $V := V(\{f_1, \ldots, f_r\}) \subseteq \left(K^{\mathrm{alg}}\right)^n$:

(i) V^*_K has at most M absolutely irreducible components.

(ii) Each absolutely irreducible component of V^*_K is of the form

$$V(\{h_1, \ldots, h_k\}),$$

for $h_R \in K[X]_{\leqslant D}$.

Proof. Every field may be expanded to a field with root functions, so we can apply Theorem 4.19.

Note that the $\dim_K\left(K[X_1, \ldots, X_n]_{\leqslant e}\right) \in \mathbb{N}$ is independent of K, so that in the above, r and R are automatically bounded in terms of (n, e) resp. (n, d). □

Proposition 4.21. There are constants $C = C(n, e) > 0$ and $M = M(n, e)$

such that for every finite field $\mathbb{F}_q$ and $\mathbb{F}_q$-algebraic subset $V \subseteq (\mathbb{F}_q^{\mathrm{alg}})^n$, defined by polynomials from $\mathbb{F}_q[X_1, \ldots, X_n]_{\leqslant e}$ such that $V(\mathbb{F}_q) \neq \varnothing$, we get

$$|\#V(\mathbb{F}_q) - \mu q^d| \leqslant C q^{d-\frac{1}{2}}$$

for some $d \in \{0, \ldots, \dim_{\mathrm{alg}}(V)\}$, $\mu \in \{1, \ldots, M\}$.

Proof. We prove this by induction on the algebraic dimension of V. Assume $V(\mathbb{F}_q) \neq \varnothing$ and let $V^* := V^*_{\mathbb{F}_q}$ with absolutely irreducible components $V_1, \ldots, V_s$ of V^* (all defined over $\mathbb{F}_q$).

By Existence of Bounds for the Decomposition-Intersection Procedure (4.20) (i) $s \leqslant M = M(n, e)$ (and $s \geqslant 1$ as $V^*(\mathbb{F}_q) \neq \varnothing$).

Permuting the V_i, we may assume that $d := \dim_{\mathrm{alg}}(V^*) = \dim_{\mathrm{alg}}(V_1) = \ldots = \dim_{\mathrm{alg}}(V_\mu)$ and $\dim_{\mathrm{alg}}(V_i) < d$ for $i > \mu$.

For this (d, μ) there is $c > 0$ such that

$$|\#V(\mathbb{F}_q) - \mu q^d| \leqslant c \cdot q^{d-\frac{1}{2}}.$$

Indeed by the Existence of Bounds for the Decomposition-Intersection Procedure (4.20) (ii) each V_i is defined by polynomials in $\mathbb{F}_q[X]_{\leqslant D}$ and we have

$$V(\mathbb{F}_q) = V^*(\mathbb{F}_q) = \bigcup_{i=1}^{s} V_i(\mathbb{F}_q)$$

By the Lang-Weil Estimates (3.1), there is $C_1 = C_1(n, D) > 0$, thus $C_1(n, e)$, such that

$$|\#V_j(\mathbb{F}_q) - q^d| \leqslant C_1 q^{d-\frac{1}{2}} \text{ for } 1 \leqslant j \leqslant \mu \tag{+}$$

and a constant $C_2(n, e)$such that

$$|\#V_j(\mathbb{F}_q)| \leqslant C_2 q^{d-1} \text{ for } j = \mu + 1, \ldots, s. \tag{++}$$

Moreover, for any $1 \leqslant j < j' \leqslant s$ we get

$$\dim_{\mathrm{alg}}(V_j \cap V_{j'}) < d \leqslant \dim_{\mathrm{alg}}(V) \tag{+++}$$

as $V_j \neq V_{j'}$ and both are absolutely irreducible of dimension d.

As $V_j \cap V_{j'}$ is defined by polynomials of degree $\leqslant D^2$, by induction there is $C_3 = C_3(n, e) > 0$ such that

$$|\#V_j(\mathbb{F}_q) \cap V_{j'}(\mathbb{F}_q)| \leqslant C_3 q^{d-1}.$$

The estimate follows from (+), (++) and (+ + +). □

Proposition 4.22. Let $f_1, \dots, f_r \in \mathbb{Z}[X_1, \dots, X_n, Z_1, \dots, Z_m]$ be polynomials of degree $\leqslant e$ in $\overline{X}$ (i.e. considered as a polynomial in $\mathbb{Z}[\overline{Z}]$) and let $C = C(n,e) > 0$ an $M = M(n,e) \in \mathbb{N}_{>0}$ be as in Proposition 4.21.

For $\mathbb{F}_q$ and $\overline{a} \in \mathbb{F}_q^m$ we consider

$$V_{\overline{a}} = V\left(\{f_1(\overline{X}, \overline{a}), \dots, f_r(\overline{X}, \overline{a})\}\right).$$

Set $f = (f_1 \dots, f_r)$. Let $(d, \mu) \in \{0, \dots, n\} \times \{1, \dots, M\}$. Then there is an $\mathcal{L}_{\text{ring}}$-formula $\chi_{f,d,\mu}(\overline{Z})$ (also depending on C, but this is suppressed in the notation) such that for every $\mathbb{F}_q$ and $\overline{a} \in \mathbb{F}_q^m$, we have

$$|\#V_{\overline{a}}(\mathbb{F}_q) - \mu q^d| \leqslant C q^{d-\frac{1}{2}} \text{ iff } \mathbb{F}_q \models \chi_{f,d,\mu}(\overline{a}).$$

Proof.

Claim 1. *For any $d \in \{0, \dots, n\}$ and $\mu \in \{1, \dots, M\}$, there is an $\mathcal{L}_{ring}$-formula $\tilde{\chi}_{f,d,\mu}(\overline{Z})$ such that for every field K and parameter $\overline{a} \in K^m$ the following are equivalent:*

(i) $\dim_{alg}(V^*_{K,\overline{a}}) = d$ *and* $V^*_{K,\overline{a}}$ *has precisely μ absolute irreducible components of dimension d.*

(ii) $K \models \tilde{\chi}_{f,d,\mu}(\overline{a})$.

Subproof. By the bounds in the decomposition-intersection procedure and the definability of absolute irreducibility and of dimension in families. ■

Depending on the choice of C, we there is a constant $H \in \mathbb{N}$ such that for all $q \geqslant H, q \in Q$, all $\overline{a} \in \mathbb{F}_q^m$ with $V_{\overline{a}}(\mathbb{F}_q) \neq \varnothing$ there is exactly one $(d, \mu) \in \{0, \dots, n\} \times \{1, \dots, M\}$ sucht that

$$|\#V_{\overline{a}}(\mathbb{F}_q) - \mu q^d| \leqslant C \cdot q^{d-\frac{1}{2}}. \tag{$*$}$$

By the proof of Proposition 4.21, $(*)$ holds for such $q \geqslant H$ precisely when $\mathbb{F}_q \models \tilde{\chi}(\overline{a})$.

Note that we may choose H such that for all $q \geqslant H$ if $V_{\overline{a}}(\mathbb{F}_q) = \varnothing$ for some $\overline{a} \in \mathbb{F}_q^m$, then $(*)$ holds for no (d, μ).

Let $\chi_{f,d,\mu}(\overline{Z}) :\equiv \left[\exists^{\geqslant H} x.\ x = x \wedge \tilde{\chi}_{f,d,\mu}(\overline{Z})\right] \vee [$ list all the cases for the finitely many $q < H$ counting in $\mathbb{F}_q^n$ which is of cardinality $\leqslant H^n$ $]$

□

Lemma 4.23. Let $\varphi(\overline{X}, \overline{Z})$ be a quantifier free $\mathcal{L}_{\text{ring}}$-formula, $|\overline{X}| = n$, $|\overline{Z}| = m$. Then there are $C(\varphi) > 0$ and $M(\varphi) \in \mathbb{N}_{>0}$ such that for every

finite $\mathbb{F}_q$ and $\overline{a} \in \mathbb{F}_q^m$ such that $\varnothing \neq \varphi(\mathbb{F}_q, \overline{a}) \subseteq \mathbb{F}_q^n$, there is $(d, \mu) \in \{0, \dots, n\} \times \{1, \dots, M\}$ such that

$$|\#\varphi(\mathbb{F}_q, \overline{a}) - \mu q^d| \leqslant C q^{d-\frac{1}{2}}. \tag{$\star$}$$

Moreover for every $(d, \mu) \in \{0, \dots, n\} \times \{1, \dots, M\}$, there is an $\mathcal{L}_{\text{ring}}$-formula $\chi_{\varphi,d,\mu}(\overline{Z})$ such that for all $\mathbb{F}_q$ and $\overline{a} \in \mathbb{F}_q^m$ ($\star$) holds for $\varphi(\mathbb{F}_q, \overline{a})$ and (d, μ) iff $\mathbb{F}_q \models \chi_{\varphi,d,\mu}(\overline{a})$.

Proof. Using elementary equivalences, one sees that there are polynomials $g_1, \dots, g_n \in \mathbb{Z}[\overline{X}, \overline{Z}]$ and polynomials $f_{i,j} \in \mathbb{Z}[\overline{X}, \overline{Z}]$, $i = 1, \dots, N$, $J = 1, \dots, r(i)$ such that in the theory of fields, $\varphi(\overline{X}, \overline{Z})$ is equivalent to

$$\bigvee_{i=1}^{N} \underbrace{\left(\bigwedge_{j=1}^{r(i)} f_{i,j}(\overline{X}, \overline{Z}) = 0 \wedge g_i(\overline{X}, \overline{Z}) \neq \varnothing \right)}_{\varphi_i(\overline{X}, \overline{Z})}$$

such that the $\varphi_i(\overline{X}, \overline{Z})$ define pairwise disjoint sets in every field. Exercise

Let $\overline{X'} = (X_1', \dots, X_N')$ be a tuple of new variables and let

$$\varphi'(\overline{X}, \overline{X'}, \overline{Z}) :\equiv \bigwedge_{i=1}^{N} \left(\bigvee_{j=1}^{r(i)} f_{i,j}(\overline{X}, \overline{Z}) = 0 \wedge g_i(\overline{X}, \overline{Z}) \cdot X_i' - 1 = 0 \wedge \bigwedge_{i' \neq i} X_{i'}' = 0 \right).$$

Then $\varphi'(\overline{X}, \overline{X}', \overline{a})$ defines an algebraic set for every $\overline{a} \in K^m$ for every field, which is an algebraic subset of $\mathbb{A}^{n+N}$ of bounded degree $\leqslant (e+1)^N$. By construction, it is of dimension $\leqslant n$, so by Proposition 4.21 we find, whenever $\varphi'(\mathbb{F}_q, \overline{a}) \neq \varnothing$ for $\overline{a} \in \mathbb{F}_q^m$, some $(d, \mu) \in \{0, \dots, n\} \times \{1, \dots, M\}$, where $M = M(\varphi) = M(N + n, (e+1)^N)$ with

$$|\#\varphi'(\mathbb{F}_q, \overline{a}) - \mu q^d| \leqslant C q^{d-\frac{1}{2}}, \tag{$*$}$$

where $C(\varphi) := C(n + n, (e+1)^N)$.

By construction (and as the $\varphi_i(\overline{X}, \overline{Z})$ were pairwise inconsistent), the projection $\mathbb{F}_q^{N+n} \to \mathbb{F}_q^n$ defines a bijection between $\varphi'(\mathbb{F}_q, \overline{a})$ and $\varphi(\mathbb{F}_q, \overline{a})$, so ($*$) holds for φ in place of φ'.

In the same way, applying Proposition 4.22 to φ', we find $\chi_{\varphi,d,\mu}(\overline{Z}) :\equiv \chi_{\varphi',d,\mu}(\overline{Z})$. □

Remark 4.23.55. The main theorem, Theorem 4.1, is thus established for quantifier-free φ.

For the proof of Theorem 4.1, in the general case we need to refine the argument in the proof of Theorem 2.15, showing that every definable set $D \subseteq F^n$ is of the form $\pi(W(F))$, where $W \subseteq \mathbb{A}^{n+l}$ is an F-algebraic set and $\pi\colon W(F) \twoheadrightarrow D$ has finite fibers.

In particular, we need the following lemma:

Lemma 4.24. In the theory Psf_c[a] every $\mathcal{L}_c$-formula $\varphi(\overline{X})$ is equivalent to a conjunction of formulas of the form

$$\exists T.\ g(\overline{X}, \overline{c}, T) = 0$$

where $g \in \mathbb{Z}[\overline{X}, \overline{C}, T]$, and $\overline{C} = (C_{i,j})_{\substack{i \geqslant 2 \\ 1 \leqslant j \leqslant i}}$.

[a] Psf with constant symbols $(c_{ij})_{\substack{i \geqslant 2 \\ 1 \leqslant j \leqslant i}} =: \overline{c}$

Remark 4.25. The equivalence in Lemma 4.24 holds for $q \gg 0$ in $(\mathbb{F}_q, c_{i,j})$, where for every $i \geqslant 2$, $T^i + c_{i,1}T^{i-1} + \ldots + c_{i,i-1}T + c_{i,i}$ is irreducible in $\mathbb{F}[T]$.

Proof. Indeed Psf_c is axiomatized by $T_f \cup \{\exists^{\geqslant n} x.\ x = x | n \in \mathbb{N}\} \cup \{T^i + c_{i,1}T^{i-1} + \ldots + c_{i,i} \text{ is irreducible} | i \geqslant 2\}$. We conclude by compactness. □

Proof of Lemma 4.24. By Quantifier Reduction in Psf (2.13) we know that every $\mathcal{L}_{\text{ring}}$-formula $\varphi(\overline{X})$ is equivalent to a boolean combination of formulas of the form

$$\exists t.\ f(t, \overline{X}) = 0, \quad f(T, \overline{X}) \in \mathbb{Z}[T, \overline{X}].$$

It thus suffices to show that in Psf_c every formula of the for $\neg\exists t.\ f(t, \overline{X}) = 0$, i.e. $\forall t.\ \neg f(t, \overline{X}) = 0$ is a conjunction of formulas of the form

$$\exists t.\ g(t, \overline{c}, \overline{X}) = 0.$$

Subproof. Let $f(T, \overline{X}) = \sum_{i=0}^{N} d_i(\overline{X})T^i$, where $d_i(\overline{X}) \in \mathbb{Z}[\overline{X}]$. Working in Psf_c (see the proof of Theorem 2.15, $\forall t.\ \neg f(t, \overline{X}) = 0$ is equivalent to the disjunction of the following two formulas:

- $\exists y.\ (d_0(\overline{X}) \cdot y - 1 = 0) \wedge \bigwedge_{i=1}^{N} d_i(\overline{X}) = 0$,
- $\exists y.\ \prod_{i=1}^{N}(d_i(\overline{X}) \cdot y - 1) = 0 \wedge$ "In the unique extension $F_{N!}$ of $F \models \mathsf{Psf}_c$ of degree $N!$, no root of $f(T, \overline{X})$ lies in F".

  Using the constants $c_{N!,j}$ for $j = 1, \ldots, N!$, the latter formula may indeed be expressed as a conjunction of formulas of the required form using the constants.

The details are left as an exercise.

Work in the basis $1, \alpha := \overline{X}, \alpha^2, \ldots, \alpha^{N!-1}$ of $F_{N!} := {}^{F[T]}\!/_{F^{N!}}$ and look at the coefficients of the roots.

■

Note that $\exists t_1.\ g_1(\overline{X}, \overline{c}, t_1) = 0 \vee \exists t_2.\ g_2(\overline{X}, \overline{c}, t_2) = 0$ is equivalent to

$$\exists t.\ g_1(\overline{X}, \overline{c}, t) \cdot g_2(\overline{X}, \overline{c}, t) = 0,$$

so we are indeed left with a conjunction of such conditions.

□

Lemma 4.26. Let $F \models \mathsf{Psf}$ and let $D \subseteq F^n$ be definable in $\mathcal{L}_{\text{ring}}(F)$. Then there are $(m, e) \in \mathbb{N}^2$ such that D is a finite union of sets of the form $\pi(W(F))$ with W an F-algebraic subset of $(F^{\text{alg}})^{n+m}$ such that for every $d \in (F^{\text{alg}})^n$, $\pi^{-1}(d) \cap W(F^{\text{alg}})$ is of cardinality $\leqslant e$.

Proof. By Lemma 4.24 we have $D = \varphi(F, \overline{a})$, where

$$\varphi(\overline{X}, \overline{Z}) \equiv \bigwedge_i \exists t.\ g_i(\overline{X}, \overline{c}, \overline{Z}) = 0,$$

working in Psf_c. In particular, D is defined by a conjunction of conditions

$$\exists t.\ g(\overline{X}, t) = 0, g \in F[\overline{X}, T].$$

Maybe for certain $\overline{a} \in F^n$, $g(\overline{a}, T) = 0$. We write $f(\overline{X}, T) = \sum_{i=0}^N d_i(\overline{X}) T^i$ as before.

Then

$$\exists t.\ f(t, \overline{X}) = 0 \iff \left(\bigwedge_{i=0}^N d_i(\overline{X}) = 0\right) \vee \left(\exists t.\ \exists u.\ \left(f(t, \overline{X}) = 0 \wedge \prod_{i=0}^N \left(d_i(\overline{X}) \cdot u - 1\right) = 0\right)\right).$$

(Note that there are at most N options for t and at most $N + 1$ options for u.)

Put the conjunction of the right-hand sides in disjunctive normal form and get the result with e computable from the data. □

[Lecture 17, 2024-12-06]

Lemma 4.27. Let $\varphi(\overline{X}, \overline{Z})$ be an $\mathcal{L}_{\text{ring}}$-formula of the form

$$\exists \overline{Y} \psi(\overline{X}, \overline{Z}, \overline{Y}),$$

where $|\overline{X}| = n$, $|\overline{Y}| = k$, $|\overline{Z}| = m$ and $\psi(\overline{X}, \overline{Z}, \overline{Y})$ is of the form

$$\bigwedge_j h_j(\overline{X}, \overline{Z}, \overline{Y}) = 0$$

for $h_i \in \mathbb{Z}[\overline{X}, \overline{Z}, \overline{Y}]$ and such that there is $e \in \mathbb{N}$ so that for every field K and $\overline{a} \frown \overline{b} \in K^{n+m}$ the set $\psi(\overline{a}, \overline{b}, K)$ is finite of cardinality $\leqslant e$.

Then the statement of Theorem 4.1 holds for $\varphi(\overline{X}, \overline{Z})$.

Proof. By Proposition 4.22, there is a constant $A(\psi)(= A(\varphi)) = A > 0$ and $M = M(\varphi) \in \mathbb{N}_{>0}$ such that for every $\mathbb{F}_q$ and $\overline{a} \in \mathbb{F}_q^m$ with $\mathbb{F}_q \models \exists x, y.\ \psi(x, \overline{a}, y)$ one has

$$|\#\{(\overline{x}, \overline{y}) \in \mathbb{F}_q^{n+k} : \mathbb{F}_q \models \psi(\overline{x}, \overline{a}, \overline{y})\} - \mu q^d| \leqslant A q^{d-\frac{1}{2}} \tag{2}$$

for some $d \in \{0, \ldots, n+k\}$, $\mu \in \{1, \ldots, M\}$.

Assume $q \gg 0$ and assume that (2) holds for $\mathbb{F}_q$, $\overline{a} \in \mathbb{F}_q^m$, d, μ. We define

$$\begin{aligned} D &:= \varphi(\mathbb{F}_q, \overline{a}) \subseteq \mathbb{F}_q^n \\ D_j &:= \{\overline{x} \in \mathbb{F}_q^n | \exists^{=j} \overline{y}.\ \mathbb{F}_q \models \psi(\overline{x}, \overline{a}, \overline{y})\}, \quad j = 1, \ldots, e \\ E &:= \{(\overline{x}, \overline{y}) \in \mathbb{F}_q^{n+k} | \mathbb{F}_q \models \psi(\overline{x}, \overline{a}, \overline{y})\}. \end{aligned}$$

In other words, $D = \pi(E) = D_1 \cup \ldots \cup D_e$, where

$$D_j = \{d \in D | \#\left(\pi^{-1}(d) \cap E\right) = j\}.$$

In terms of counting solutions, we get

(i) $\#D = \#D_1 + \ldots + \#D_e$, $\#E = \#D_1 + 2\#D_2 + \ldots + e\#D_e$. By (2), $|\#E - \mu q^d| \leqslant A q^{d-\frac{1}{2}}$. Note that since $q \gg 0$, necessarily $d \leqslant n$.

Problem. *D_j is not quantifier-free definable.*

We may however employ a little trick: For $j = 1, \ldots, e$, let $\overline{Y}^j := (Y_1^j, \ldots, Y_k^j)$ be new variables. For $j(1) \neq j(2)$ we write $\overline{Y}^{j(1)} \neq \overline{Y}^{j(2)}$ if they differ in at least one coordinate.

For $1 \leqslant j \leqslant e$ we consider the following quantifier-free auxiliary formulas:

$$\psi_j(\overline{X}, \overline{Z}, \overline{Y}^1, \ldots, \overline{Y}^j) :\equiv \bigwedge_{i=1}^{j} \psi(\overline{X}, \overline{Z}, \overline{Y}^i) \wedge \bigwedge_{1 \leqslant i(1) < i(2) \leqslant j} \overline{Y}^{i(1)} \neq \overline{Y}^{i(2)}.$$

Set $H_j := \{(\overline{x}, \overline{y}^1, \ldots, \overline{y}^j\} \in \mathbb{F}_q^{n+jk} : \mathbb{F}_q \models \psi_j(\overline{x}, \overline{a}, \overline{y}^1, \ldots, \overline{y}^j)\}$.

Note that every $d \in D$ gives rise to $j!$ elements in H_j. More generally $0 \leqslant t \leqslant e - j$ every $d \in D_{j+t}$ gives rise to $\frac{(j+t)!}{t!}$ many points in H_j.

Summing up, we get for $1 \leqslant j \leqslant e$:

$$\#H_j = j!\#D_j + (j+1)!\#D_{j+1} + \ldots + \frac{e!}{(e-j)!}\#D_e.$$

This is a system of e $\mathbb{Q}$-linear equations in the $\#D_j$, which has full rank. Multiplying with the inverse, we may compute $(\#D_j)_j$ in terms of $(\#H_i)_i$ and get using (i):

(ii) $\#D = r_1\#H_1 + \ldots + r_e\#H_e$ for $r_1, \ldots, r_e \in \mathbb{Q}$ depending only e.

As $\#H_j \leqslant \text{constant} \cdot \#E$ using Lemma 4.23 [8] we find $A_j(\varphi) > 0$ and $M_j(\varphi) \in \mathbb{N}$ such that

(iii) $|\#H_j - \mu_j q^d| \leqslant A_j q^{d-\frac{1}{2}}$ for some $\mu_j \in \{0, \ldots, M_j\}$. [9]

(ii) and (iii) yield:

(iv) $|\#D - (r_1\mu_1 + \ldots + r_e\mu_e)q^d| \leqslant Cq^{d-\frac{1}{2}}$, where $C := C(\varphi) := |r_1|A_1 + \ldots + |r_e|A_e$.

As $\#D \geqslant \frac{\#E}{e}$ and as $q \gg 0$, we get $\#D \geqslant \frac{\mu}{e}q^d - \frac{A}{e}q^{d-\frac{1}{2}}$ (using (2)) so $r_1\mu_1 + \ldots + r_e\mu_e \geqslant \frac{\mu}{e} > 0$.

There are only finitely many $(d, \nu) \in \{0, \ldots, n\} \times \mathbb{Q}_{>0}$ we obtain this way.

Definability of the cases follows for $q \gg 0$ follows from definability of the cases in Lemma 4.23, as the cases are disjoint for $q \gg 0$. For the remaining finitely many small $\mathbb{F}_q$, we do it by hand. □

We can now proof the the general case:

Proof of Theorem 4.1. We reduce the statement to the special case of Lemma 4.27.

Let $\varphi(\overline{X}, \overline{Z})$ be an arbitrary $\mathcal{L}_{\text{ring}}$-formula.

By Lemma 4.24 and Remark 4.25 there is an $\mathcal{L}_c$-formula $\varphi'(\overline{X}, \overline{Z})$, which is a conjunction of $\mathcal{L}_c$-formulas of the form

$$\exists T.\ g(\overline{X}, \overline{c}, \overline{Z}, T) = 0,$$

where $g(\overline{X}, \overline{Z}, \overline{C}, T) \in \mathbb{Z}[\overline{X}, \overline{Z}, \overline{C}, T]$, $\overline{C} = (C_{i,j})_{\substack{i \geqslant 2 \\ 1 \leqslant j \leqslant i}}$ such that for every $q \gg 0$ in every enriched finite field $(\mathbb{F}, \overline{c})$ φ and φ' are equivalent.

We may assume that the variables $c_{i,j}$ appearing in the different polynomials g are all the same. Let $\overline{Z}'$ be a tuple of new variables of the appropriate length.

For the 1st part of Theorem 4.1, it suffices to show the result for $\psi' \equiv \bigwedge_{i=1}^{l} \exists T.\ G_i(\overline{X}, \overline{Z}, \overline{Z}', T) = 0$. Here, $\overline{Z}, \overline{Z}'$ are the parameter variables. We'll write $\psi'(\overline{X}, \overline{Z})$ and incorporate $\overline{Z}'$ in $\overline{Z}$ in our notation.

Given $G_i(\overline{X}, \overline{Z}, T) = \sum_{j=0}^{N_i} g_{i,j}(\overline{X}, \overline{Z})T^j$, we disjointly decompose the condition $\exists T.\ G_i(\overline{X}, \overline{Z}, T) = 0$ into

$$\left(\bigwedge_{j=0}^{N_i} g_{i,j}(\overline{X}, \overline{Z}) = 0\right) \vee \left(\exists T.\ G_i(\overline{X}, \overline{Z}, T) = 0 \wedge \exists U.\ \prod_{j=0}^{N_i} \left(g_{i,j}(\overline{X}, \overline{Z}) \cdot U - 1\right) = 0\right).$$

[8] The statement for quantifier-free formulas, note that the ψ_j are quantifier free.
[9] We might need to neglect some H_j, so $\mu_j = 0$ is allowed here.

Using these decompositions and bringing the their conjunction into DNF, we get a finite disjoint disjunction of formulas as in Lemma 4.27.

Indeed, they look like

$$\bigwedge f_I(\overline{X},\overline{Z}) = 0 \wedge \exists T_1,\ldots,T_n \left(\bigwedge_{j=1}^{N} h_j(\overline{X},\overline{Z},T_i) = 0 \right).$$

Setting

$$\tilde{\psi}(\overline{X},\overline{Z},T_1,\ldots,T_N) :\equiv \bigwedge f_I(\overline{X},\overline{Z}) = 0 \wedge \bigwedge_{j=1}^{N} h_j(\overline{X},\overline{Z},T_j) = 0,$$

there is $e \in \mathbb{N}$ such that $\tilde{\psi}(\overline{X},\overline{Z},F)$ has $\leqslant e$ elements for any field F and $(\overline{x},\overline{z}) \in F^{n+m}$.

The first part of Theorem 4.1 now follows from Lemma 4.27, as the set of formulas for which the statement holds is obviously stable under disjoint disjunctions.

Definablilty of the cases The initial replacement of $\overline{c}$ by $\overline{Z}'$ might prose a problem. However, the equivalent of φ and ψ' holds for $q \gg 0$ and all finite tuples $\overline{b}$ satisfying a definable $\mathcal{L}_{\text{ring}}$-condition.

Indeed, whenever $T^n + b_{n,1}T^{n-1} + \ldots + b_{n,n-1}T + b_{n,n} \in \mathbb{F}_q[T]$ is irreducible it is fine. □

5 Simplicity and the Independence Theorem in Psf

We will see that (in char $\neq 2$[10]) in every $F \models \mathsf{Psf}$, the formula $\varphi(X,Y) :\equiv \exists z.\ z^2 = x + y$ has the **independence property**, IP, i.e. for every $n \in \mathbb{N}$ there are $a_0,\ldots,a_{n-1}$ and $(b_I)_{I\subseteq n}$ in F such that for all i, I

$$F \models \varphi(a_i, b_I) \text{ iff } i \in I.$$

In particular, φ is unstable, so every completion of Psf is unstable.

Notation 5.0.56. Recall that for field $K \subseteq L, L' \subseteq U$ we set $L \underset{K}{\downarrow}^{\text{alg}} L'$ iff L and L' are algebraically independent over K, i.e. for every finite tuple $\overline{a}$ from L, $\text{trdeg}\left(K(\overline{a})/K\right) = \text{trdeg}\left(L'(\overline{a})/L'\right)$.

[10] In char = 2 there is another formula.

Definition 5.0.57. Let T be an arbitrary complete theory of fields and U a monster model of T. For $A, B, C \subseteq U$ we write $A \underset{B}{\downarrow}^{\mathbf{alg}} C$ if $Q(\langle AB\rangle) \underset{Q(\langle B\rangle)}{\downarrow}^{\text{alg}} Q(\langle BC\rangle)$.

Lemma 5.1. Let T be a complete theory of fields. Let $U \models T$ be a monster model of T and let $A, B, C, D, \ldots$ be small subsets of U. Then we have:

(1) **Aut-invariance**: if $ABC \equiv A'B'C'$ then $A \underset{B}{\downarrow}^{\text{alg}} C \iff A' \underset{B'}{\downarrow}^{\text{alg}} C'$.

(2) **Symmetry**: $A \underset{B}{\downarrow}^{\text{alg}} C \iff C \underset{B}{\downarrow}^{\text{alg}} A$.

(3) **Full Transitivity**: $A \underset{B}{\downarrow}^{\text{alg}} CD \iff [A \underset{B}{\downarrow}^{\text{alg}} C$ and $A \underset{BC}{\downarrow}^{\text{alg}} D$.

(4) **Finite Character**:

$$A \underset{B}{\downarrow}^{\text{alg}} C \iff [\forall A_0 \overset{\text{finite}}{\subseteq} A : A_0 \underset{B}{\downarrow}^{\text{alg}} C].$$

(5) **Local Character**: If A_0 is finite, then for every C, there is $C_0 \subseteq C$ with $|C_0| \leqslant |T|$ (actually, we even have C_0 finite [a]) such that $A_0 \underset{C_0}{\downarrow}^{\text{alg}} C$.

(6) **Extension**: Given A, B, C, there is $A' \equiv_B A$ such that $A' \underset{B}{\downarrow} C$.

[a] But this is not part of the definition of local character.

Remark 5.2. Usually for an independence notion $\downarrow$, **local character** means that there is $C_0 \subseteq C$ of cardinality $\leqslant |T|$ such that

$$A_0 \underset{C_0}{\downarrow} C$$

Proof of Lemma 5.1. This holds for every Aut-invariant pregeometry. The fact that alg defines a pregeometry is Steinitz' Exchange Lemma, which yields symmetry. □

Next week we will use the theorem of Kim-Pillay and the Indepencence Theorem to characterize non-forking in Psf and prove its simplicity.

[Lecture 18, 2024-12-10]

Definition 5.2.58. Let T be a complete $\mathcal{L}$-theory with monster model U.

- An $\mathcal{L}$-formula $\varphi(\overline{x},\overline{y})$ has the **tree property**, **TP**, with respect to k, where $k \geqslant 2$ is an integer, iff there is a tree of parameters $(b_\eta)_{\eta\in\omega^{<\omega}}$, with $b_\eta \in U^{|\overline{y}|}$, such that
  (i) For every $\eta \in \omega^{<\omega}$, the set of formulas
  $$\{\varphi(\overline{x}, b_{\eta^\frown i}) | i \in \omega\}$$
  is **k-inconsistent**, i.e. every k-element subset is inconsistent.
  (ii) For every branch $\beta \in \omega^\omega$, the set of formulas
  $$\{\varphi(\overline{x}, b_{\beta|_n}) | n \in \omega\}$$
  is consistent.
- $\varphi(\overline{x},\overline{y})$ has **TP** iff it has TP with respect to some $k \geqslant 2$.
- T is **simple** iff no formula $\varphi(\overline{x},\overline{y})$ has TP, i.e. iff T is **NTP**.
- $\varphi(\overline{x},\overline{y})$ has the **strict order property**, **SOP**, iff there is a sequence $(b_i)_{i\in\omega}$ in $U^{|\overline{y}|}$ such that
  $$\varphi(U, b_0) \subsetneq \varphi(U, b_1) \subsetneq \varphi(U, b_2) \subsetneq \dots$$
- T has **SOP** iff there is a formula that has SOP. Otherwise T has **NSOP**.
- $\varphi(\overline{x},\overline{y})$ has the **order property**, **OP**, iff there are $(a_i)_{i\in\omega}$ in $U^{|\overline{x}|}$ and $(b_i)_{i\in\omega}$ in $U^{|\overline{y}|}$ such that for all $i, j \in \omega$ one has
  $$U \models \varphi(a_i, b_j) \text{ iff } i < j.$$
- T is **stable** iff no formula has OP.
- $\varphi(\overline{x},\overline{y})$ has the **independence property IP** iff there are $(a_i)_{i\in\omega}$ from $U^{|\overline{x}|}$ and $(b_J)_{J\subseteq\omega}$ from $U^{|\overline{y}|}$ such that for all $i \in \omega$ and $J \subseteq \omega$ one has
  $$U \models \varphi(a_i, b_J) \text{ iff } i \in J.$$
- T is **NIP** (**dependent**) iff no formula has IP.

Remark 5.3 (Shelah)**.** T is unstable iff it has IP or SOP. In particular (see below), T is stable iff T is NIP and NTP.

Proposition 5.4. Let T be a complete $\mathcal{L}$-theory with monster model U and let $\varphi(\overline{x},\overline{y})$ be an $\mathcal{L}$-formula. We have:

(i) φ has SOP $\implies$ φ has OP.

(ii) φ has IP $\implies$ φ has OP.

In particular, every stable theory is NIP.

(iii) φ has TP $\implies$ φ has OP.

In particular, every stable theory is NTP.

(iv) T is NTP $\implies$ T NSOP.

Proof of Proposition 5.4. (i) clear.

(ii) If $(a_i)_{i\in\omega}$, $(b_J)_{J\subseteq\omega}$ witness that φ has IP, then $(a_i)_{i\in\omega}$, $(\tilde{b}_j)_{j\in\omega}$ with $\tilde{b}_j := b_{\{0,\dots,j-1\}}$ witness that φ has OP.

(iv) Assume that $\varphi(\overline{x},\overline{y})$ has SOP. By compactness we find $(b_q)_{q\in\mathbb{Q}}$ in $U^{|\overline{y}|}$ such that for $q, q' \in \mathbb{Q}$ we have

$$\varphi(U, b_q) \supsetneq \varphi(U, b_{q'}) \iff q > q'.$$

It is easy to see that the $\mathcal{L}$-formula

$$\psi(\overline{x}, \overline{y}\overline{y}') :\equiv \varphi(\overline{x},\overline{y}) \wedge \neg\varphi(\overline{x},\overline{y}')$$

has TP with respect to 2.[11]

□

For a formula $\varphi(\overline{x},\overline{y})$ and $A \subseteq U$, we set

$$S_\varphi(A) := \left\{ \begin{array}{c} \text{maximal consistent sets of formulas} \\ \text{of the form } \varphi(\overline{x},\overline{a}) \text{ or } \neg\varphi(\overline{x},\overline{a}) \text{ for } \overline{a} \in A^{|\overline{y}|} \end{array} \right\},$$

the set of **complete φ-types over A**.

For the proof of (iii), we need the following:

Fact 5.5. The following are equivalent:

- $\varphi(\overline{x},\overline{y})$ has OP.
- For every infinite cardinal κ there is $A \subseteq U$ with $|A| = \kappa$ such that $|S_\varphi(A)| > \kappa$.
- There is $A \subseteq U$ such that $|S_\varphi(A)| > |A| \geqslant \aleph_0$.

[11] Use that every open interval in $\mathbb{Q}$ contains countably many pairwise disjoint open intervals to construct a tree of parameters as required by TP.

Continuation of proof of Proposition 5.4. (iii) By Fact 5.5, it suffices to show that if $\varphi(\overline{x},\overline{y})$ has TP, then $|S_\varphi(A)| > |A|$ for some infinite $A \subseteq U$.

Let κ be an infinite cardinal such that $\kappa^{\aleph_0} > \max\{2^{\aleph_0}, \kappa\}$.

Such a cardinal exists. Indeed any $\kappa > 2^{\aleph_0}$ of cofinality $\aleph_0$ will do, as then $\mathrm{cof}(\kappa^{\aleph_0}) > \aleph_0$ by Kőnig's Theorem, so $\kappa^{\aleph_0} > \kappa$.

Using that $\varphi(\overline{x},\overline{y})$ has TP with respect to $k \geqslant 2$, by compactness we find $(b_\eta)_{\eta\in\kappa^{<\omega}}$ in $U^{|\overline{y}|}$ such that

(1) $\{\varphi(\overline{x}, b_{\eta^\frown i}) | i \in \kappa\}$ is k-inconsistent for every $\eta \in \kappa^{<\omega}$.

(2) $\pi_\beta := \{\varphi(\overline{x}, b_{\beta|_i)|i\in\omega}\}$ is consistent for every $\beta \in \kappa^\omega$.

Given $\beta \in \kappa^\omega$ by Zorn's Lemma we find $F_\beta \subseteq \kappa^{<\omega}$ such that the following hold:

(a) $\beta \in F_\beta$

(b) $\bigcup_{\gamma\in F_\beta} \pi_\gamma$ is consistent.

(c) Whenever $\underbrace{\delta}_{\in K^\omega} \notin F_\beta$, then the set of formulas

$$\pi_\delta \cup \bigcup_{\gamma\in F_\beta} \pi_\gamma$$

is inconsistent.

Let $T_\beta := \{\gamma|_n | n \in \omega, \gamma \in F_\beta\}$. Then T_β is a tree. Suppose there is $\eta \in T_\beta$ and pairwise distinct $i_1, \ldots, i_k \in \kappa$ such that $\eta^\frown i_j \in T_\beta$ for $j = 1, \ldots, k$. Then there are $\gamma_1, \ldots, \gamma_k \in F_\beta$ such that $\eta^\frown i_j$ is an initial segment of γ_j for $j = 1, \ldots, k$.

So the consistency statement (b) contradicts the inconsistency of $\{\varphi(\overline{x}, b_{\eta^\frown i_j}) | j = 1, \ldots, k\}$ (which is a consequence of (1)).

It follows that T_β may be embedded into the three $k^{<\omega}$ and so its set of branches embeds into the set κ^ω.

In particular, $|F_\beta| \leqslant |k^\omega| = 2^{\aleph_0}$. As $\kappa^{\aleph_0} > 2^{\aleph_0}$ by assumption, there is $F \subseteq \kappa^\omega$ with $|F| = \kappa^{\aleph_0}$ and such that $F_\beta \neq F_{\beta'}$ for all $\beta \neq \beta'$ from F.

Let $A := \{(b_\eta)_i | \eta \in \kappa^{<\omega}, 1 \leqslant i \leqslant |\overline{y}|\}$ be the set of elements appearing as a coordinate of some b_η.

For $\beta \in F$ let $\rho_\beta \in S_\varphi(A)$ such that $\rho_\beta \supseteq \bigcup_{\gamma\in F_\beta} \pi_\gamma$. If $\beta \neq \beta'$ are from F, wlog. there is $\delta \in F_\beta \backslash F_{\beta'}$. Then $\pi_\delta \subseteq \rho_\beta$ and $\rho_{\beta'} \cup \pi_\delta$ is inconsistent. In particular $\rho_\beta \neq \rho_{\beta'}$. So $|S_\varphi(A)| \geqslant \kappa^{\aleph_0} > \kappa = |A|$.

□

Proposition 5.6. Any completion of Psf has NSOP. More precisely, given any $\mathcal{L}_{\text{ring}}$-formula $\varphi(\overline{x}, \overline{y})$, there is a bound $N_\varphi \in \mathbb{N}$ such that in no $F \models T_f$ there are tuples $b_0, \ldots, b_{N_\varphi} \in F^{|\overline{y}|}$ such that

$$\varphi(F, b_0) \supsetneq \varphi(F, b_1), \supsetneq \ldots \supsetneq \varphi(F, b_{N_\varphi}).$$

Proof. If no such bound exists, by compactness we find $F \models T_f$ and $(b_i)_{i \in \mathbb{N}}$ such that

$$\varphi(F, b_i) \supsetneq \varphi(F, b_{i+1})$$

for all i. In particular, F is necessarily infinite, i.e. $F \models \mathsf{Psf}$. It thus suffices to show the first statement.

Assume $F \models \mathsf{Psf}$ and $(b_i)_{i \in \mathbb{N}}$ and $\varphi(\overline{x}, \overline{y})$ witness SOP. Let $Q \subseteq \{0, \ldots, |\overline{x}|\} \times \mathbb{Q}_{>0}$ be the finite set associated to $\varphi(\overline{x}, \overline{y})$ in Theorem 4.1. In particular $(\dim(\varphi(\overline{x}, b_i)), \mu(\varphi(\overline{x}, b_i))) \in Q$ for all $i \in \mathbb{N}$. We may thus assume that there is (d, μ) such that $(\dim(\varphi(\overline{x}, b_i)), \mu(\varphi(\overline{x}, b_i))) = (d, \mu)$ for all $i \in \mathbb{N}$.

We argue by induction on $d \geqslant 0$.

Case $d = 0$ Then $\mu(\varphi(\overline{x}, b_i)) = \#\varphi(F, b_i) = \mu$ for all i (by Remark 4.3) contradicting $\varphi(F, b_0) \supsetneq \varphi(F, b_1)$.

Case $d > 0$ Let $S_i := \varphi(F, b_i)$, so $S_0 \supsetneq S_1 \supsetneq S_2 \supsetneq \ldots$. Set $T_i := S_0 \backslash S_i$, so $S_0 = S_i \cup T_i$.

Since $(\dim(S_i), \mu(S_i)) = (d, \mu) = (\dim(S_0), \mu(S_0))$,

Proposition 4.7 (2) yields $\dim(T_i) < d$.

As $T_1 \subsetneq T_2 \subsetneq T_3 \subsetneq \ldots$ we are done by induction and compactness. □

We will use the following:

Fact 5.7. Assume that T is a complete theory such that every formula $\varphi(x, \overline{y})$ is NTP with respect to 2.[a] Then T is NTP.

[a] $|x| = 1$

Theorem 5.8. Any completion of Psf is NTP.

Proof. Using Fact 5.7, Theorem 5.8 follows from Proposition 5.9. □

Proposition 5.9. For every $\mathcal{L}_{\text{ring}}$-formula $\varphi(\overline{x}, \overline{y})$, there exists a bound $N_\varphi \in \mathbb{N}$ such that for every $F \models \mathsf{Psf}$, every definable set $S \subseteq F^{|\overline{x}|}$ every set of indices I if

- $S_i = \varphi(F, b_i)$ is a subset of S,
- $\dim(S_i) = d = \dim(S)$ for all i and
- if $i \neq j$ are from I, then $\dim(S_i \cap S_j) < d$,

then $|I| \leqslant N_\varphi$.

Proof. Suppose no such N_φ exists. Using compactness, it follows that there is $F \models \mathsf{Psf}$, $S \subseteq F^{|\overline{x}|}$ definable and $b_i \in F^{|\overline{y}|}$ for $i \in I = \mathbb{N}$, such that $F, S, S_i := \varphi(F, b_i)$ adhere to the assumptions.

Let D be the finite subset of $\{0, \ldots, |\overline{x}|\} \times \mathbb{Q}_{>0}$ associated with φ and $\mu_0 := \min\{\mu | (d, \mu) \in D\}$. We have $m_S(S_i \cap S_j) = 0$ for all $i \neq j$ and

$$m_S(S_i) = \frac{\mu(S_i)}{\mu(S)} \geqslant \frac{\mu_0}{\mu(S)},$$

so for every $I_0 \overset{\text{finite}}{\subseteq} \mathbb{N}$ we get $m_S\left(\bigcup_{i \in I_0} S_i\right) = \sum_{i \in I_0} m_S(S_i) \geqslant \frac{|I_0|\mu_0}{\mu(S)}$, so $|I_0| \leqslant \frac{\mu(S)}{\mu_0}$. But $I_0 \overset{\text{finite}}{\subseteq} \mathbb{N}$ was arbitrary $\lightning$ □

[Lecture 19, 2024-12-16]

Definition 5.9.59. Let T be a complete $\mathcal{L}$-theory with monster model U. Let $A \subseteq U$ be small, $\varphi(\overline{x}, \overline{y})$ and $\mathcal{L}$-formula and $b \in U^{|\overline{y}|}$.

- For $k \geqslant 2$ one says that $\varphi(\overline{x}, b)$ **k-divides over A** if there is a sequence $(b_i)_{i \in \mathbb{N}}$ in $U^{|\overline{y}|}$ of realizations of $\mathrm{tp}(b/A)$ such that $\{\varphi(\overline{x}, b_i) | i \in \mathbb{N}\}$ is k-inconsistent.
- $\varphi(\overline{x}, b)$ **divides over A** iff it k-divides over A for some $k \geqslant 2$.
- A partial type $\pi(\overline{x})$ **divides over A** iff it implies a formula which divides over A.[a]
- A partial type $\pi(\overline{x})$ **forks over A** iff it implies a disjunction

$$\bigvee_{1 \leqslant j \leqslant n} \varphi_j(\overline{x}, b_j)$$

such that each $\varphi(\overline{x}, b_j)$ divides over A.

[a] Observe that $\varphi(\overline{x}, b)$ divides over A iff $\{\varphi(\overline{x}, b)\}$ divides over A.

Notation 5.9.60. We write

$$A \underset{B}{\downarrow}^{f} C$$

if for every finite tuple a from A $\mathrm{tp}(a/BC)$ does not fork over B.

The following theorems will not be proved in this lecture:

Theorem 5.10 (Kim)**.** If T is simple, $\downarrow^f$ satisfies the following properties: Aut-invariance, Symmetry, Full Transitivity, Finite Character, Local Character, Extension.[a].

[a] cf. Lemma 5.1

Theorem 5.11 (Kim-Pillay)**.** If T is simple, $\downarrow^f$ satisfies the **Independence Theorem over a Model**: For every $M \models T$ and $M \subseteq A, B \subseteq U$ with $A \underset{M}{\downarrow^f} B$ if $p(x) \in S(A)$ and $q(x) \in S(B)$ are types that do not fork over M such that $p|_M = q|_M$, there is $r(x) \in S(AB)$ with $r|_A = p$ and $r|_B = q$ such that r does not fork over M.

Theorem 5.12 ("Theorem of Kim-Pillay")**.** Let T be complete and let $\downarrow$ be a ternary relation on small subsets of the monster model $U \models T$ satisfying Aut-invariance, Symmetry, Full Transitivity, Finite Character, Local Character, Extension and the Independence Theorem over a Model. Then T is simple and $\downarrow = \downarrow^f$.

Proposition 5.13. In any completion T of Psf, $\downarrow^{\mathrm{alg}}$ satisfies the Independence Theorem over a Model.

Corollary 5.14. Any completion of Psf is simple, with non-forking equal to $\downarrow^{\mathrm{alg}}$.

Proof of Proposition 5.13. We will convert the problem into an amalgamation problem for algebraically closed fields with automorphisms.

Let $F \models \mathsf{Psf}$ and $F \subseteq A, B \subseteq U$ with $U \succeq F$, $A \underset{F}{\downarrow^{\mathrm{alg}}} B$. Assume that $p(\overline{x}) \in S(A)$ and $q(\overline{x}) \in S(B)$ are types such that $p|_F = q|_F$ and for any $c \models p$ and $d \models q$ one has

$$c \underset{F}{\downarrow^{\mathrm{alg}}} A \text{ and } d \underset{F}{\downarrow^{\mathrm{alg}}} B.$$

Replacing A (and B) by its relative algebraic closure in U, we may assume that A and B are relatively algebraically closed in U. Moreover, replacing c by $F(c)^{\mathrm{alg}} \cap U \cong_F F(d)^{\mathrm{alg}} \cap U$, we may assume that $p|_F = q|_F$ is the type of an enumeration of a relatively algebraically closed subset C of U.

Let $X_{AB} := (AB)^{\mathrm{alg}} \cap U$. For $C \models p$ in U, let $X_{AC} := (AC)^{\mathrm{alg}} \cap U$. For $C' \models q$, let $X_{BC'} := (BC')^{\mathrm{alg}} \cap U$

Note that $C \cong_F C'$, $C \underset{F}{\downarrow}^{\mathrm{alg}} A$ and $C' \underset{F}{\downarrow}^{\mathrm{alg}} A$.

$\mathrm{Gal}(X_{AB})$, $\mathrm{Gal}(X_{AC})$, $\mathrm{Gal}(X_{BC'})$, $\mathrm{Gal}(A)$, $\mathrm{Gal}(B)$, $\mathrm{Gal}(C) \cong \mathrm{Gal}(C')$ and $\mathrm{Gal}(F)$ are all procyclic, with surjective restriction maps whenever this makes sense. As $\mathrm{Gal}(F) \cong \hat{\mathbb{Z}}$, it follows that all restriction maps are isomorphisms and all Galois groups are $\cong \hat{\mathbb{Z}}$.

Identifying C with C', we find inclusions between various relatively algebraically closed subsets of U, such that all maps commute:

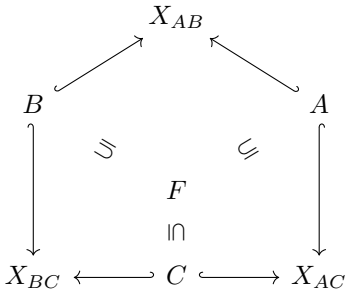


Figure 1

Note that the whole diagram is not a subdiagram of the subsets of U (yet).

We find generators of the various Galois groups

$$\begin{aligned}
\sigma_{AB} &\in \mathrm{Gal}(X_{AB}),\\
\sigma_{AC} &\in \mathrm{Gal}(X_{AC}),\\
\sigma_{BC} &\in \mathrm{Gal}(X_B C),\\
\sigma_A = \mathrm{res}(\sigma_{AB}) &= \mathrm{res}(\sigma_{AC}) \in \mathrm{Gal}(A),\\
\sigma_B = \mathrm{res}(\sigma_{AB}) &= \mathrm{res}(\sigma_{BC}) \in \mathrm{Gal}(B),\\
\sigma_C = \mathrm{res}(\sigma_{AC}) &= \mathrm{res}(\sigma_{BC})\\
\sigma_F = \mathrm{res}(\sigma_{AB}) = \mathrm{res}(\sigma_{AC}) &= \mathrm{res}(\sigma_{BC}) \in \mathrm{Gal}(F).
\end{aligned}$$

Now let $F^{\mathrm{alg}} \subseteq A^{\mathrm{alg}}$, B^{alg}, C^{alg} etc. together with compatible coherent restrictions of the automorphisms, yielding

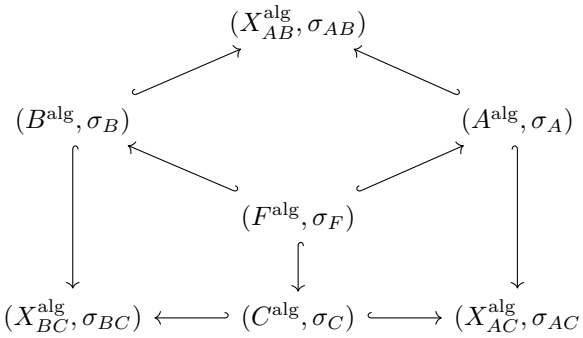


Figure 2

We need to do a little detour now.

Definition 5.14.61. Let T be an arbitrary complete theory and $U \models T$ a monster model.

- Let $A \subseteq B \subseteq U$. A partial type $\pi(\overline{x})$ over B is called **finitely satisfiable** in A if for any $\varphi_1, \ldots, \varphi_n \in \pi$, there is $a \in A^{|\overline{x}|}$ such that

$$U \models \bigwedge_{i=1}^{n} \varphi_i(a).$$

- If $M \preceq U$ and $M \subseteq B \subseteq U$ and $p(\overline{x}) \in S(M)$, then an extension $q(\overline{x}) \in S(B)$ of $p(\overline{x})$ is called a **coheir** of p if q is finitely satisfiable in M.

Lemma 5.15. (1) Let $\pi(\overline{x})$ be a partial type over B which is finitely satisfiable in $A \subseteq B$. Then there is $q(\overline{x}) \in S(B)$ extending π such that q is finitely satisfiable in A.

(2) If $M \preceq U$ and $M \subseteq B \subseteq U$, then any $p(\overline{x}) \in S(M)$ admits a coheir in $S(B)$.

Proof. (2) follows from (1) by setting $\pi(\overline{x}) := p(\overline{x})$, $A = M$ ad $p(\overline{x})$ is finitely satisfiable in M.

ad (1): By Zorn's Lemma, we may assume that $\pi(\overline{x})$ may not be properly extended to a partial type over B which is finitely satisfiable in A. If π was not complete over B, there would exist an $\mathcal{L}_B$-formula $\varphi(\overline{x})$ such that both $\pi(\overline{x}) \cup \{\varphi(\overline{x})\}$ and $\pi(\overline{x}) \cup \{\neg\varphi(\overline{x})\}$ are consistent. One of these partial types is then finitely satisfiable in A, contradicting maximality of π.

Indeed if $\pi(\overline{x}) \cup \{\varphi(\overline{x})\}$ is not finitely satisfiable in A, there are $\varphi_1, \ldots, \varphi_n \in \pi$ such that $\bigwedge_{i=1}^{n} \varphi_i(\overline{x}) \wedge \varphi(\overline{x})$ has no solution in A. Similarly, there are $\varphi'_1, \ldots, \varphi'_{n'} \in \pi$ such that $\bigwedge \varphi'_i(\overline{x}) \wedge \neg\varphi(\overline{x})$ has no solution in A.

But then $\bigwedge \varphi_i(\overline{x}) \wedge \bigwedge \varphi'_i(\overline{x})$ has no solution in π, contradicting that π is finitely satisfiable in A. □

Recall that for $K \models \mathsf{ACF}$ and a field extension L/K a type $p(\overline{x}) \in S_n(K)$ admits a unique extension to $q(\overline{x}) \in S_n(L)$ such that for $a \models q$ one has

$$a \underset{K}{\downarrow}^{\text{alg}} L \iff \operatorname{trdeg}(a/L) = \operatorname{trdeg}(a/K) \iff \operatorname{loc}(a/L) = \operatorname{loc}(a/K) \iff L(a) \cong Q(K(a) \otimes_K L).$$

Proposition 5.16. Let $K \preceq U \models F$, $K \subseteq L \subseteq U$ and let $p(\overline{x}) = \operatorname{tp}(a/K)$. Then p admits a unique coheir $q(\overline{x}) \in S(L)$ given by the unique extension to L of the same transcendence degree.

Proof. A coheir exists by Lemma 5.15. Suppose for a contradiction that $\operatorname{tp}\left(a'/L\right)$ is finitely satisfiable in K and $\operatorname{trdeg}\left(a'/L\right) < \operatorname{trdeg}\left(a'/K\right)$. Then there is $b \in L^n$ which is algebraically independent over K but algebraically dependent over $K(a')$.

There is an $\mathcal{L}_{\text{ring}}$-formula $\varphi(\overline{x}, \overline{y})$ such that $\varphi(\overline{x}, b) \in \operatorname{tp}\left(a'/L\right)$ and whenever $U \models \varphi(c, d)$, then $\operatorname{trdeg}\left(d/c\right) < n$.

By finite satisfiablilty, there is e from K such that $U \models \varphi(e, b)$, so $\operatorname{trdeg}\left(b/K\right) \leqslant \operatorname{trdeg}\left(b/e\right) < n$ ↯. □

Definition 5.16.62. Let $\mathcal{P}(3)^- := \mathcal{P}(3)\backslash\{3\}$ be the set of proper subsets of 3.

- A **3-amalgamation problem** (**3-AP**) in ACF_σ is given by a system of quantifier free $\mathcal{L}_{\text{ring}} \cup \{\sigma\}$-types $\{p_w(x_w)\}_{w \in \mathcal{P}(3)^-}$ over $\varnothing$ such that the following conditions hold:
  - (i) For any w, $K_w \models p_w$ enumerates an algebraically closed set such that σ is an automorphism.
  - (ii) If $w \subseteq w'$, then x_w subtuple of $x_{w'}$ and $p_{w'}|_{x_w} = p_w$.
  - (iii) For any $w = \{i, j\}$ with $i \neq j$ and any $K_w \models p_w$ one has $K_w = (K_i K_j)^{\text{alg}}$ and $K_i \underset{K_\varnothing}{\downarrow}^{\text{alg}} K_j$, where K_i, K_j, $K_\varnothing$ denote the subtuples of K_w corresponding to the subsets of variables

$X_{\{i\}}$, $X_{\{j\}}$ and $X_\varnothing$.

- A **solution** of $\{p_w(x_w)\}_{w\in\mathcal{P}(3)^-}$ is given by a type $p_3(x_3)$ such that (i) and (ii) hold for $\{p_w(x_w)\}_{w\in\mathcal{P}(3)}$ and in addition the following holds:

  (iii)' If $K_{\{0,1,2\}} \models p_3$, then $K_{\{0,1,2\}} = (K_0K_1K_2)^{\mathrm{alg}}$ and $K_0 \underset{K_0}{\downarrow}^{\mathrm{alg}} K_1K_2$.[a]

[a] Note: It follows that $K_1 \underset{K_\varnothing}{\downarrow}^{\mathrm{alg}} K_0K_2$ and $K_2 \underset{K_\varnothing}{\downarrow}^{\mathrm{alg}} K_0K_1$.

[Lecture 20, 2024-12-17]

Proposition 5.17. Every 3-AP in ACF_σ admits a solution.

Proof. Let $\{P_w\}_{w\in\mathcal{P}(3)^-}$ be a 3-AP in ACF_σ. Let $(K_w,\sigma_w) \models p_w$ $(w\in\mathcal{P}(3)^-)$. These realizations all live in some $U \models \mathsf{ACF}$ (sufficiently saturated).

We mas assume that $K_{\{0\}} \subseteq K_{\{0,1\}}$ and $K_{\{0\}} \subseteq K_{\{0,2\}}$ such that $K_{\{0,1\}} \underset{K_\varnothing}{\downarrow}^{\mathrm{alg}} K_{\{0,2\}}$.

Then for the compositum, we have $K_{\{0,1\}}K_{\{0,2\}} = \mathrm{Frac}(K_{\{0,1\}} \otimes K_{\{0,2\}})$ and $\sigma_{\{0,1\}}\cup\sigma_{\{0,2\}}$ induces an automorphism $\tilde{\sigma}$ of the compositum $K_{\{0,1\}}K_{\{0,2\}}$. Note that, as fields, we may assume $K_{\{1,2\}} \subseteq (K_{\{0,1\}}K_{\{0,2\}})^{\mathrm{alg}} =: K_{\{0,1,2\}}$. In order to find $\sigma_{\{0,1,2\}} \in \mathrm{Aut}(K_{\{0,1,2\}}$ extending both $\tilde{\sigma}$ and $\sigma_{1,2}$, it suffices to show

$$\text{If } a\in K_{\{1,2\}}, \text{ then } \mathrm{tp}_{\mathsf{ACF}}\left(a/K_{\{1\}}K_{\{2\}}\right) \vdash \mathrm{tp}\left(a/K_{\{0,1\}}K_{\{0,2\}}\right). \tag{3}$$

or equivalently, using elimination of imaginaries in ACF (or just Galois theory),

$$\mathrm{dcl}_{\mathsf{ACF}}(K_{\{0,1\}K_{\{0,2\}}}) \cap (K_{\{1\}}K_{\{2\}})^{\mathrm{alg}} = \mathrm{dcl}_{\mathsf{ACF}}(K_{\{1\}}K_{\{2\}}). \tag{4}$$

To settle (4), assume that

$$a \in K_{\{1,2\}} \cap \mathrm{dcl}_{\mathsf{ACF}}\left(\underbrace{(K_{\{0\}}K_{\{1\}})^{\mathrm{alg}}}_{K_{\{0,1\}}}\underbrace{(K_{\{0\}}K_{\{1\}})^{\mathrm{alg}}}_{K_{\{0,2\}}}\right)$$

There is a $\varnothing$-definable function F and tuples $d_{\{0,i\}}$ from $K_{\{0,i\}}$ for $i=1,2$ such that

$$F(d_{\{0,1\}},d_{\{0,2\}}) = a.$$

We may choose tuples $c_i \in K_{\{i\}}$ for $i=0,1,2$ and $\mathcal{L}_{\mathrm{ring}}$-formulas $\varphi_i(X_0,X_i,Z_{0,i})$ with

$$U \models \varphi_i(c_0,c_i,d_{\{0,i\}})$$

for $i=1,2$ such that whenever $\models \varphi_i(c_0',c_i',d_{\{0,i\}}'$, then $d_{\{0,i\}}' \in \mathrm{acl}_{\mathsf{ACF}}(c_0',c_i')$.

By construction, we get that the following $\mathcal{L}_{\text{ring}}$-formula

$$\exists z_{0,1}, z_{0,2}.\ [\varphi_1(X_0, c_1, z_{0,1}) \wedge \varphi_2(X_0, c_2, z_{0,2}) \wedge F(z_{0,1}, z_{0,2}) = a]$$

lies in $\text{tp}_{\mathsf{ACF}}(c_0/K_{\{1,2\}}) \subseteq \text{tp}_{\mathsf{ACF}}(K_0/K_{\{1,2\}})$.. By (i) and transitivity of $\downarrow^{\text{alg}}$, we get

$$K_{\{0\}} \underset{K_\varnothing}{\downarrow}^{\text{alg}} K_{\{1,2\}}.$$

By Proposition 5.16 we get that $\text{tp}_{\mathsf{ACF}}\left(K_{\{0\}}/K_{\{1,2\}}\right)$ is finitely satisfiable in $K_\varnothing$. So there are $d_i' \in (K_\varnothing K_{\{i\}})^{\text{alg}} = K_{\{i\}}$ such that $F(d_1', d_2') = a$. Hence $a \in \text{dcl}_{\mathsf{ACF}}(K_{\{1\}} K_{\{2\}})$. □

Continuation of proof of Proposition 5.13. The Figure 2 represents a 3-AP in ACF_σ, so it admits a solution $(\tilde{L}, \tilde{\sigma})$ by Proposition 5.17 with compatible $\mathcal{L}_\sigma$-embeddings of $(X_{AB}^{\text{alg}}, \sigma_{AB})$ etc. into $(\tilde{L}, \tilde{\sigma})$ such that A^{alg}, B^{alg}, C^{alg} are independent.

Note that the fields in Figure 1 are the fixed fields of Figure 2.

$L := \text{Fix}(\tilde{L})$ allows for compatible embeddings of X_{AB} etc. into L as relatively algebraically closed subsets. A, B, C are algebraically independent over F in L and L is perfect with Galois group $\hat{\mathbb{Z}}$.[12] By the Lemma 5.18, L regularly embeds into some $F' \models \mathsf{Psf}$, so $F' \geq F$. Identifying A, B, C with their images in F', $\text{tp}\left(C/AB\right)$ is the desired solution. □

Lemma 5.18. Let L be perfect with procyclic Galois group. Then L regularly embeds into a model of Psf.

Proof. □ Homework

Theorem 5.19. Any completion T of Psf has IP. In particular, T is unstable. In char $\neq 2$, more precisely, the formula $\varphi_2(x, y) :\equiv \exists z.\ z^2 = x + y$ has IP.

Remark 5.20. In char $= 2$, one may work in the field $F[\zeta_3]$ (interpretable in F) and show that $\varphi_3(x, y) :\equiv \exists z.\ z^2 - x + y$ as IP in F', so F is IP.

Proof of Theorem 5.19. Let $F \models \mathsf{Psf}$, $\text{char}(F) \neq 2$. Let $\sigma \in \text{Gal}(F)$ be a topological generator, so $(F^{\text{alg}}, \sigma) \models \mathsf{ACF}_\sigma$ and $\text{Fix}(\sigma) = F$.

[12] Procyclic is clear, as $\text{Gal}(L)$ is topologically generated by $\tilde{\sigma}$; as it surjects onto $\text{Gal}(F) = \hat{\mathbb{Z}}$ we conclude.

Claim 5.19.1. *For every $n \in \mathbb{N}$, there is $(K, \sigma) \supseteq (F^{alg}, \sigma)$ with $(K, \sigma) \models \mathsf{ACF}_\sigma$ and $a_1, \ldots, a_n \in \mathrm{Fix}(K)$, $b_I \in \mathrm{Fix}(K)$, $I \subseteq \{1, \ldots, n\}$ such that*

$$\sqrt{a_i + b_I} \in \mathrm{Fix}(K) \text{ iff } i \in I. \tag{5}$$

Note that (5) is well-defined since the other square root is $-\sqrt{a_i + b_I}$ and $-1 \in \mathrm{Fix}(K)$.

Subproof. Let $a_1, \ldots, a_n, b_I$, $I \subseteq \{1, \ldots, n\}$ be algebraically independent over F^{alg}. Let $\overline{e} = (\overline{a}, \overline{b})$, $L := F^{\mathrm{alg}}(\overline{e})$. Let σ be the extension of $\sigma|_{F^{\mathrm{alg}}}$ given by $\sigma(a_i) = a_i$, $\sigma(b_I) = b_I$ for all i, I. $(L, \sigma) \supseteq (F^{\mathrm{alg}}, \sigma)$. Let M/L be given by adjoining

$$c_{i,I} := \sqrt{a_i + b_I}$$

for all i, I. Let $R := F^{\mathrm{alg}}[a_1, \ldots, a_n, b_I, I \subseteq \{1, \ldots, n\}]$. $a_i + b_I$ are irreducible in R and pairwise non associate. So $a_I + b_I \pmod{(L^\times)^2}$ are $\mathbb{F}_2$-linearly independent in $L^\times/(L^\times)^2$ (an $\mathbb{F}_2$-vector space written multiplicatively).

By Kummer theory, $\mathrm{Gal}\left(M/L\right) \cong \left(\mathbb{Z}/2\mathbb{Z}\right)^{n \cdot 2^n}$. On M, let $\tilde{\sigma}$ be the extension of $\sigma|_L$ given by

$$\tilde{\sigma}(c_{i,I}) := \begin{cases} c_{i,I} & \text{if } i \in I \\ -c_{i,I} & \text{if } i \notin I \end{cases}$$

Let $K := M^{\mathrm{alg}}$, and σ the extension of $\tilde{\sigma}$ to K^{alg}. ■

By Lemma 5.18, there is a regular extension $F'/\mathrm{Fix}(K)$, such that $F' \models \mathsf{Psf}$. $F' \geq F$ (since regular), showing that φ_2 has IP in $\mathrm{Th}(F)$. □

6 Some results around dcl in Psf

[Lecture 21,]

A description of dcl in Psf

Definition 6.0.63.

- For $K \models \mathsf{Psf}$ and $P(X, \overline{Y}), Q(X, \overline{Y}) \in \mathbb{Z}[X, \overline{Y}]$, $|\overline{Y}| = d$ we define a function

$$\kappa_{P,Q} \colon K^d \longrightarrow K$$
$$\overline{a} \longmapsto \begin{cases} b & \text{if } \{Q(x, \overline{a}) | x \in K, P(x, \overline{a}) = 0\} = \{b\}, \\ 0 & \text{otherwise.} \end{cases}$$

- We set $\mathcal{L}_\kappa := \mathcal{L}_{\mathrm{ring}} \sqcup \{\kappa_{P,Q} | P, Q \text{ as above}\}$ and $\mathsf{Psf}_K := \mathsf{Psf} \cup \{\text{ definition of } \kappa_{P,Q} \text{ as above}\}$.

Remark 6.0.64. Note that $\mathsf{Psf}_\kappa \supseteq \mathsf{Psf}$ is an expansion by definitions, i.e. every model of Psf uniquely extends to a model of Psf_κ, as the $\kappa_{P,Q}$ are $\mathcal{L}_{\text{ring}}$-definable functions. In particular, there are no new definable sets.

Proposition 6.1 (Hrushovski)**.** Psf_κ eliminates quantifiers and $\mathcal{L}_\kappa$-substructures of models are definably closed.

Proof. We first show

Claim 1. *If* $A = \langle A \rangle_{\mathcal{L}_\kappa} \leqslant \kappa \models \mathsf{Psf}_\kappa$,

then $A = \operatorname{dcl}(A)$.

Subproof. Assume $A = \langle A \rangle_{\mathcal{L}_\kappa}$.

(a) A is a subfield:

Indeed, let $a \in A \backslash \{0\}$. Let $P(X,Y) := X \cdot Y - 1$ and $Q(X,Y) := X$, we get $\kappa_{P,Q}(a) = \frac{1}{a}$.

(b) A is perfect:

Indeed, assume $\operatorname{char}(K) = p > 0$. Let $a \in A$. Let $P(X,Y) := X^p - Y$, $Q(X,Y) := X$. Then $\kappa_{P,Q}(a) = a^{\frac{1}{p}} \in A$.

Now, observe that $A \subseteq \operatorname{dcl}(A) \subseteq \operatorname{acl}(A) = A^{\text{alg}} \cap K$.

Towards a contradiction suppose that there is $b \in \operatorname{dcl}(A) \backslash A$. By Quantifier Reduction in Psf (2.13) every field automorphism of $\sigma \in \operatorname{Aut}_{\text{field}}(\operatorname{acl}(A)/A)$ is elementary, so as $b \in \operatorname{dcl}(A)$, we have $\sigma(b) = b$ for every $\sigma \in \operatorname{Aut}_{\text{field}}(\operatorname{acl}(A)/A)$.

By compactness of the Krull topology of $\operatorname{Aut}_{\text{field}}(\operatorname{acl}(A)/A)$, there is a finite normal (hence Galois by (b)) extension $\tilde{B}/A$ such that $b \in B$ and b is fixed under every $\sigma_{\text{field}}\left(B/A\right)$, where $B := \tilde{B} \cap K = \operatorname{acl}(A) \cap \tilde{B} \subseteq \operatorname{acl}(A)$.

As B/A is finite separable, by the primitive element theorem there is $c \in B$ such that $B = A(c)$. Moreover if $\tilde{P}(X) := \operatorname{MiPo}(c/A)$, then there is a bijective correspondence between the set of roots of $\tilde{P}$ in B (and thus in K) with $\operatorname{Aut}_{\text{field}}(B/A)$ given by $\sigma \mapsto \sigma(c)$.

Let $\overline{a} \in A^d$ and $P(X,\overline{Y}), Q(X,\overline{Y}) \in \mathbb{Z}[X,\overline{Y}]$ such that $\tilde{P}(X) = P(X,\overline{a}) \in A[X]$ and $Q(c,\overline{a}) = b \in A(c) = A[c]$.

Let $\tilde{Q}(X) := Q(X,\overline{a})$.

By definition, $\kappa_{P,Q}(\overline{a}) = b$. Indeed, let $\sigma \in \operatorname{Aut}_{\text{field}}(B/A)$. Then $\tilde{Q}(\sigma(c)) = \sigma(\tilde{Q}(c)) = \sigma(b) = b$. ∎

Remark 6.1.65. We proved that $\mathrm{dcl}(A) = \underbrace{Q\left(\langle A\rangle\right)^{\mathrm{perf}}}_{A'} \cup \bigcup_{P,Q} \kappa_{P,Q}(A')$, i.e. it suffices to apply a $\kappa_{P,Q}$ once.

Claim 2. Psf_κ *eliminates quantifiers.*

Subproof. By Quantifier Reduction in Psf (2.13) it suffices to show that if $f\colon A \cong B$ is an $\mathcal{L}_\kappa$-isomorphism, $A \leqslant K \models \mathsf{Psf}_\kappa$, $B \leqslant L \models \mathsf{Psf}_\kappa$ then f extends to an $\mathcal{L}_{\mathrm{ring}}$-isomorphism

$$\tilde{f}\colon A^{\mathrm{alg}} \cap K \cong B^{\mathrm{alg}} \cap L.$$

We know that this holds iff for every $\tilde{P}(X) \in A[X]$ one has $K \models \exists t.\ \tilde{P}(t) = 0$ iff $L \models \exists t.\ f(\tilde{P})(t) = 0$. $(*)$

Let $\overline{a} \in A^d$ and $P(X, \overline{Y}) \in \mathbb{Z}[X, \overline{Y}]$ such that $\tilde{P}(X) = P(X, \overline{a})$ and $Q(X, \overline{Y}) := 1$. By definition,

$$\kappa_{P,Q}(\overline{a}) = \begin{cases} 1 & \text{if } K \models \exists t.\ \tilde{P}(t) = 0, \\ & \text{otherwise.} \end{cases}$$

As $\kappa_{P,Q}(f(\overline{a}))$ has the same result, since f preserves $\mathcal{L}_\kappa$, we get $(*)$. ■

□

Corollary 6.2. Let $A \subseteq K \models \mathsf{Psf}$. Then $\mathrm{dcl}(A) = \langle A\rangle_{\mathcal{L}_\kappa}$

Geometric Representability of Profinite Groups over Pseudofinite Fields

Definition 6.2.66. Let T be a complete theory of fields and let G be a profinite group.

We say that G is **geometrically represented over** $K_0 \models T$ iff there is $K \succeq K_0$ and $K_0 \subseteq A \subseteq B \subseteq K$ such that $\mathrm{Aut}_{\mathrm{el}}(B/A) \cong G$.

Here, $\mathrm{Aut}_{\mathbf{el}}(B/A)$ is the group of *elementary* permutations of B fixing A pointwise.

Notation 6.2.67. Let k be a prime field[a] and let p be a prime.

- If $\mathrm{char}(k) \neq p$ and $n \in \mathbb{N}$, we denote by μ_{p^n} the group of p^n-th roots of unity in k^{alg}.

  We set $\Omega_p := \mu_{p^\infty} := \bigcup_{n\in\mathbb{N}} \mu_{p^n}$.

- If $\mathrm{char}(k) = p$, i.e. $k = \mathbb{F}_p$, we let $\wp$ be the Artin-Schreier map $x \mapsto x^p - x$ on $k^{\mathrm{alg}} = \mathbb{F}_p^{\mathrm{alg}}$ and we set $\Omega_p \coloneqq \bigcup_{n\in\mathbb{N}} \ker(\wp^n)$.

[a] i.e. $k = \mathbb{F}_p$ or $k = \mathbb{Q}$

Remark 6.3. If K is a field and p a prime, then either $\Omega \subseteq K$ or $K \cap \Omega_p$ is a finite subgroup of Ω_p.

Proposition 6.4 (Beyarslan-Hrushovski)**.** Let q be a prime and $K \models \mathsf{Psf}$ of char $\neq p$ such that $\mu_{p^\infty} \subseteq K$. Then $\hat{\mathbb{Z}}_p \coloneqq \varprojlim_n \mathbb{Z}/p^n$ is geometrically represented over K. In particular, $\mathbb{Z}/p^n$ is geometrically representable over K for all $n \in \mathbb{N}$.

We will prove a generalization of this:

Proposition 6.5. Let $K \models \mathsf{Psf}$ and $\nu \leqslant K^\times$ be a divisible group of roots of unity. Then the **Pontryagin dual**, $\nu^\vee \coloneqq \mathrm{Hom}_{????}(\nu, S^n) \cong \prod_{\substack{p\in\P \\ \zeta_p\in\nu}} \hat{\mathbb{Z}}_p$ is geometrically represented over K.

Proof. For a prime p such that $\zeta_p \in \nu$ we choose a coherent system $(\omega_{p^n})_{n\in\mathbb{N}}$ of of (primitive) p^n-th roots of unity with $\omega_p = \zeta_p$ and

$$\left(\omega_{p^{n+1}}\right)^p = \omega_{p^n}$$

for all $n \in \mathbb{N}$.

Then ν is the direct sum of the μ_{p^∞} with $\zeta_p \in \nu$ and $\mu_{p^\infty} = \bigcup_{n\in\mathbb{N}} \mu_{p^n} = \bigcup_n \langle omegaega_{p^n} \rangle$.

We let $K((t^{\mathbb{Q}}))$ be the field of **Hahn series** with coefficients from K and exponents from $\mathbb{Q}$.[13]

The following is well known:

If $v_t(a) \coloneqq \begin{cases} \infty & \text{if } a = 0, \\ \min(\mathrm{supp}(a)) & \text{if } a \neq 0, \end{cases}$ then $(K((t^{\mathbb{Q}})), v_t)$ is a valued field with residue field K and the value group is $\mathbb{Q}$, which is **maximal**, i.e. does not admit any proper immediate extension. Thus by valuation theory one gets

$$(*)K((t^{\mathbb{Q}}))\text{is a quasifinite field} \tag{6}$$

More precisely

**For every $n \in \mathbb{N}$, $K((t^{\mathbb{Q}}))$ has a unique extension of degree n given by $K_n((t^{\mathbb{Q}})) = K_n K((t^{\mathbb{Q}}))$ where K_n/K (7)

[13] i.e. $K((t^{\mathbb{Q}})) = \{a = \sum_{q\in\mathbb{Q}} a_q t^q | a_q \in K, \mathrm{supp}(a) \text{ is a well-ordered subset of } \mathbb{Q}\}$.

In particular, $\frac{K((t^{\mathbb{Q}}))}{K}$ is a regular extension and res: $\mathrm{Gal}(K((t^{\mathbb{Q}}))) \to \mathrm{Gal}(K) \cong \hat{\mathbb{Z}}$ is an isomorphism.

By there is $\tilde{K} \models \mathsf{Psf}$ into which $K((t^{\mathbb{Q}}))$ regularly embeds and so $K \preceq \tilde{K}$.

Given $p \in \P$ such that $\zeta_p \in \nu$ (so $\mu_{p^\infty} \subseteq \nu$), we define the following field automorphism τ_p on $K((t^{\mathbb{Q}}))$: For $q \in \mathbb{Q}\backslash\{0\}$, $q = p^z \cdot \frac{a}{b}$, $a, b, z \in \mathbb{Z}$, $p \nmid a$, $q \nmid b$,

$$\tau_p\left(t^q\right) := \begin{cases} t^q & \text{if } z \geqslant 0, \\ \omega_{p^{-z}} & \text{if } z < 0. \end{cases}$$

Set $\tau_p(\sum_\gamma a_\gamma t^\gamma) := \sum_\gamma a_\gamma \tau_p(t^\gamma)$. As $K((t^{\mathbb{Q}}))$ is relatively algebraically closed in $\tilde{K}$,

Each τ_p restricts to a field automorphism of $K\left(t^{\frac{1}{n}} | n \geqslant 1\right) \supseteq K(t)$ fixing $K(t)$, so by construction $\tau_p \in \mathrm{Aut}_{\mathrm{el}}(K(t^{\frac{1}{n}} | n \geqslant 1)/K(t))$ for all p such that $\zeta_p \in \nu$.

It is easy to check that the τ_p topologically generate a subgroup H of $\mathrm{Aut}(K(t^{\frac{1}{n}} | n \geqslant 1)/K(t))$ isomorphic to $\prod_{\substack{p \in \P \\ \zeta_p \in \nu}} \hat{\mathbb{Z}}_p$.

Set $B := K(t^{\frac{1}{n}} | n \geqslant 1)$ and $A := B^H \supseteq K(t)$.

Then $H = \mathrm{Aut}_{\mathrm{el}}\left(B/A\right)$, essentially by Galois theory. □

[Lecture 22, 2025-01-10]

We'll now discuss some negative results.

Lemma 6.6. Let K be a field and $L \succeq K$ (so $K^{\mathrm{alg}} \overset{\mathrm{l.d.}}{\downarrow}_K L$). Let K'/K be a normal (algebraic) extension and $L' := K'L$ $(= K' \otimes_K L)$.

Then any $\tau \in \mathrm{Aut}(L/K)$ admits an extension τ' to L' which commutes with any $\sigma \in \mathrm{Aut}(L'/L)$. If $\mathrm{Aut}(L'/L)$ is abelian, any extension τ' will do.

Proof. As $L' = K' \otimes_K L$, let $\tau' := \mathrm{id}_{K'} \otimes \tau$ which commutes with all $\sigma \in \underbrace{\mathrm{Aut}(L'/L)}_{\sigma \otimes \mathrm{id}_L} \cong \mathrm{Aut}(K'/K)$.

Everything follows. □

The following technical lemma just wraps some computation for later use:

Lemma 6.7. Let $(D, +)$ be an abelian group and let $P, T, S_1, \ldots, S_m$ be endomorphisms of $(D, +)$, $\Sigma := \{S_1, \ldots, S_m\}$. Assume $PT = TP$, $PS_i =$

S_iP, $TS_i = S_iT$ for all i.

Set $\ker(\Sigma) \coloneqq \bigcap_{i=1}^{m} \ker(S_i)$ and $\Omega \coloneqq \bigcup_{n\in\mathbb{N}} \ker(P^n)$.

Assume in addition:

(i) P is surjective,

(ii) $T|_\Omega = 0$ and

(iii) $\Omega \cap \ker(\Sigma) \subseteq \ker(P^r)$ for some $r \in \mathbb{N}$.

Then if $a \in \ker(\Sigma)$ and $P(a) \in \ker(T)$, then $a \in \ker(T)$.

Proof. Let $a \in \ker(\Sigma)$ such that $P(a) \in \ker(T)$. Let $P(a) =: b$ and let $C \coloneqq \{x \in D | \exists n, m > 0.\ P^n(x) = P^m(b)\} \ni a$. As $T(b) = 0$ and $S_i(b) = S_i(P(a)) = P(S_i(a)) = P(0) = 0$ for all i, we get

$$S_i(C) \subseteq \Omega \text{ for } i = 1, \dots, m. \tag{8}$$

Indeed if $P^n(c) = P^m(b)$ for $n > 0$, then $P^n(S_i(c)) = S_i(P^n(c)) = S_i(P^m(b)) = P^m(S_i(b)) = P^m(0) = 0$, so $S_i(c) \in \ker(P^n) \subseteq \Omega$.

By the same argument:

$$T(C) \subseteq \Omega. \tag{9}$$

By (ii) we have $TS_i|_C = 0$ for all i, so $S_i(T(C)) = 0$, i.e. $T(C) \subseteq \ker(\Sigma)$.

By (iii) $T(C) \subseteq \ker(P^r)$ for some r. Moreover, by (i) and the definition of C, we get $P(C) = C$.

Thus $PT(C) = TP(C) = T(C)$. By induction we get $P^rT(C) = T(C)$. So $T(C) = 0$, i.e. $a \in \ker(T)$. □

Lemma 6.8. Let K be a field such that $\mathrm{Gal}(K)$ is topologically finitely generated. Then the following holds:

(1) For every $n \in \mathbb{N}$, K has only finitely many separable extensions of degree $\leqslant n$.

(2) If $L \geq K$, then res: $\mathrm{Gal}(L) \to \mathrm{Gal}(K)$ is an isomorphism.

Proof. Let $\mathrm{Gal}(K) = \overline{\langle \sigma_1, \dots, \sigma_n \rangle}$.

(1) It suffices to show that K admits only finitely many Galois extensions of degree $\leqslant n$.[14] This follows as

- there are only finitely many groups of cardinality $\leqslant n$ up to isomorphism and

[14] $n' \coloneqq n!$

- for each of these there are at most n^m many continuous group homomorphisms $\mathrm{Gal}(K) \to G$.

We finish by Galois theory.

(2) If $L \geq K$, L/K is regular, so res: $\mathrm{Gal}(L) \twoheadrightarrow \mathrm{Gal}(K)$ by Proposition 1.39.

But the finite number of separable extension of degree n of L and K are the same, so they all come from K, so res is injective.

In other words $L^{\mathrm{sep}} = K^{\mathrm{sep}}L = K^{\mathrm{sep}} \otimes_K L$.

□

Theorem 6.9. Let Kbe a field such that $\mathrm{Gal}(K)$ is topologically finitely generated.

If $p \neq \mathrm{char}(K)$ assume that K contains a primitive p-th root of unity.

If a finite group G with $p|\#G$ is geometrically represented over K, then $\Omega_p \subseteq K$.

Proof. By assumption, there are $K \preceq L$ and intermediate fields $K \subseteq A \subseteq B \subseteq L$ such that $G = \mathrm{Aut}_{\mathrm{el}}(B/A)$ is finite with $p|\#G$. Let $\tau \in G$ be of order p. Replacing A by B^τ, then B by $A(\alpha_0, \ldots, a_{p-1})$, where $\tau^i(\alpha_0) = \alpha_i$ for $i = 0, \ldots, p-1$ such that $\tau(\alpha_0) \neq \alpha_0$, we may assume $\mathrm{Aut}_{\mathrm{el}}(B/A) = \mathrm{Gal}(B/A) = \langle\tau\rangle \cong \mathbb{Z}/p$ and B/A is Galois.

We may take L $|B|^+$-saturated and strongly $|B|^+$-homogeneous. Let τ_L be an extension of τ to an element of $\mathrm{Aut}(L/A)$. Combining Lemma 6.6 and Lemma 6.8, τ_L extends to some $\tau_{L^{\mathrm{sep}}} \in \mathrm{Aut}\left(L^{\mathrm{sep}}/A\right)$ such that $\tau_{L^{\mathrm{sep}}}$ commutes with every $\sigma \in \mathrm{Gal}(L)$, in particular with topological generators $\sigma_1, \ldots, \sigma_n$ of $\mathrm{Gal}(L)$.

- If $\mathrm{char}(K) = p$, let $(D, +) = (L^{\mathrm{sep}}, +)$. By construction we may assume that $\tau_{L^{\mathrm{sep}}}$ fixes K^{sep}.
- If $\mathrm{char}(K) \neq p$, $(D, +) = (L^{\mathrm{sep}\times}, \cdot)$ (written additively). We also write $\mathrm{End}(D)$ additively.

We consider the following endomorphisms of D :

- $S_i = \sigma_i - \mathrm{id}$ (i.e. $S_i(x) = \frac{\sigma_i(x)}{x}$ in the case of $\mathrm{char}(K) \neq p$)
- $T := T_{L^{\mathrm{sep}}} - \mathrm{id}$.
- If $\mathrm{char}(K) = p$, $P(x) := x^p - x = \wp(x)$.
- If $\mathrm{char}(K) \neq p$, $P(x) := p \cdot x$ ($x \mapsto x^p$ mulitplicatively)

By Artin-Schreier / Kummer theory, we get $B = A(b)$ for some b with $P(b) = a \in A$.

Define Ω as in Lemma 6.7 , i.e. $\Omega = \Omega_p$ (so $\Omega = \mu_{p^\infty}$ or $\bigcup_{n\in\mathbb{N}} \ker(\wp^n)$).

Clearly P commutes with T and the S_i. Let us check the other hypotheses in Lemma 6.7:

(i) P is surjective (✓ as L^{sep} is separably closed),

(ii) $T|_{\Omega_p} = 0$ (✓ since $\tau_{L^{\mathrm{sep}}}$, fixes $K^{\mathrm{sep}} \supseteq \Omega_p$),

(iii) Suppose that $\Omega_p \nsubseteq K$.

Then by Remark 6.3 $K \cap \Omega_p$ is a finite subgroup of Ω_p. Thus for some $r \in \mathbb{N}$, P^r vanishes on $K \cap \Omega_p$).

As $L \geq K$, we have $L \cap \Omega_p = K \cap \Omega_p$ and by Galois theory $L = \ker(\Sigma)$.

Thus P^r vanishes on $\ker(\Sigma) \cap \Omega_p = K \cap \Omega_p$.

By Lemma 6.7 we get $T(b) = 0$, i.e. $\tau_(b) = b$, so $\tau|_B = \mathrm{id}_B$ ↯. □

Recall that in a fixed $\mathrm{char}\, p \in \P \cup \{0\}$, the completions of Psf_p are in bijective correspondence with the conjugacy classes in $\mathrm{Gal}(\mathbb{F}_p)$, where $\mathbb{F}_0 := \mathbb{Q}$.

Indeed, the isomorphism type of $\mathrm{Abs}(K)$ determines (and is determined by) the completion $\mathrm{Th}(K)$ of Psf (cf. **??**).

$\mathrm{Gal}(\mathbb{F}_p)$ is a compact topological group, so it has a unique left-invariant[15] probability measure called the **Haar measure** μ_G.

Let Π be the set of conjugacy classes of $\mathrm{Gal}(\mathbb{F}_p)$ and $\pi\colon \mathrm{Gal}(\mathbb{F}_p) \twoheadrightarrow \Pi$ the canonical projection. $\mu := \pi_* \mu_G$ is the induced measure on Π, i.e. $\mu(U) := \mu_G(\pi^{-1}(U))$.

Identifying Π with the set of completions $\mathcal{C}_p$ of Psf_p, we get a measure μ on $\mathcal{C}_p$.

We will use the following as a black box:

Fact 6.10 (Jarden)**.** For almost all $T \in \mathcal{C}_p$, if $K \models T$, then $\mathrm{Abs}(K) \preceq K$. (Equivalently, for almost all $\sigma \in G$ $(\mathbb{F}_p^{\mathrm{alg}})^\sigma \models \mathsf{Psf}$.)

Corollary 6.11. Let K be field such that $\mathrm{Gal}(K)$ is topologically finitely generated and let p be a prime number, $p \neq \mathrm{char}(K)$. Assume that $K[\zeta_p]$ does not contain μ_{p^∞}. Then no finite group G with $p|\#G$ is geometrically represented in $\mathrm{Th}(K)$.

Proof. Let $K' := K[\zeta_p]$. Then $[K' : K] \leqslant p - 1$. If there is G geometrically represented in $\mathrm{Th}(K)$ such that $p|\#G$, then there is H finitely generated, geometrically represented in $\mathrm{Th}(K')$ with $p|\#H$. Indeed, K' is interpretable in K. The result follows from Theorem 6.9. □

[15] i.e. $\mu(gS) = \mu(S)$ for all $g \in G$ and Borel sets S

Corollary 6.12 (Beyarslan-Hrushovski)**.** For almost all $T \in \mathcal{C}_p$, the following holds:

If $K \models T$ and $\mathrm{Abs}(K) \subseteq A \subseteq K$, then $\mathrm{dcl}(A) = \mathrm{acl}(A)$.

Proof. For each p' prime with $p' \neq \mathrm{char}(K) = p$, the set $\{\sigma \in \mathrm{Gal}(\mathbb{F}_p) | \sigma^{p'-1} \text{ fixes } \mu_{p'^\infty}\}$ has measure 0. Exercise.

Thus $\bigcup_{\substack{p' \neq p \\ p' \in ¶}} \{\sigma \in \mathrm{Gal}(\mathbb{F}_p) | \sigma^{p'-1} \text{ fixes } \mu_{p'^\infty}\}$ has measure 0. Moreover, if p, the set

$$\{\sigma \in \mathrm{Gal}(\mathbb{F}_p) | \sigma \text{ fixes } \Omega_p\}$$

has measure 0.

By Fact 6.10, we may assume that $\mathrm{Abs}(K) \preceq K$, so by Corollary 6.11 and Theorem 6.9 any finite (and thus any profinite) group geometrically represented in T is trivial for a set of $T \in \mathcal{C}_p$ of measure 1. For these T the statement holds. □

[Lecture 23, 2025-01-14]

Remark 6.13. While dcl = acl over $\mathrm{Abs}(K)$ is a restricted form of Skolemization, the completions of Psf are never Skolemized.

Indeed if $K \models \mathsf{Psf}$, we have seen that there is $\tilde{K} \succeq K$ and $K \subseteq K((t^{\mathbb{Q}}))^{\text{rel. alg. closed}} \subseteq \tilde{K}$. We know that $\mathrm{dcl}_{\mathsf{Psf}}(K((t^{\mathbb{Q}})) = \mathrm{acl}(K((t^{\mathbb{Q}})) = K((t^{\mathbb{Q}}))$. $K((t^{\mathbb{Q}}))$ is a Henselian valued field, which is separably closed, thus it is not PAC by a result of Freyer-Prestel (see [FJ23]).

6.1 Further Results on Geometric Model Theory in Psf

6.1.1 Global Definable Types in Psf_0

Recall that if T is a complete $\mathcal{L}$-theory and $M \models T$ a type $p \in S_n(M)$ is **definable** iff for every $\mathcal{L}$-formula $\varphi(\overline{x}, \overline{y})$, $|\overline{x}| = n$, there is an $\mathcal{L}(M)$-formula $d_p\varphi(\overline{y})$, such that for all $\overline{b} \in M^{|\overline{y}|}$, $\varphi(\overline{x}, \overline{b}) \in p$ iff $M \models d_p(\overline{b})$.

Remark 6.14. If $p \in S_n(\mathcal{M})$ is definable and $\mathcal{M} \subseteq \mathcal{C} \subseteq \mathcal{U}$ with $\mathcal{U} \succeq \mathcal{M}$ a monster model, then for $\overline{b} \in \mathcal{C}^{|\overline{y}|}$ and $\varphi(\overline{x}, \overline{y})$ $\mathcal{L}$-formula, we let $\varphi(\overline{x}, \overline{b}) \in p|_{\mathcal{C}}$ iff $\mathcal{U} \models d_p\varphi(\overline{b})$.

This defines a complete type over $\mathcal{C}$ and $p|_{\mathcal{U}}$ is called a **global** definable type.

Example 6.15. (1) If $\overline{a} \in M^n$, $\mathrm{tp}(\overline{a}/\mathcal{M})$ is definable. ("realized types are definable"): This is trivial, take $d_p\varphi(\overline{y}) = \varphi(\overline{a}, \overline{y})$.

(2) Let $T = \mathsf{DLO}$, $\mathcal{M} \models T$, then $p_\infty(x)$ given by $\{m < x | m \in \mathcal{M}\}$ is a definable type.

The same holds for any o-minimal theory, e.g. RCF.

(3) Let T be the theory of the random graph[a]. $\mathcal{M} \models T$. $p \in S_1(M)$ determined by $\{R(x,m)|m \in \mathcal{M}\} \cup \{x \neq m | m \in \mathcal{M}\}$ is definable.

(4) Let T be strongly minimal $\mathcal{M} \models T$, then $p_{\text{gen}}(x) \in S_1(\mathcal{M})$ determined by $\{x \neq m | m \in \mathcal{M}\}$ is a non-realized, definable type.

Note that (2) and (3) are unstable, whereas (4) is stable.

[a] Fraisse limit of all finite graphs

Fact 6.16 (Shelah)**.** Let T be a complete $\mathcal{L}$-theory. The following are equivalent:

(1) T is stable, i.e. κ-stable for some $\kappa \geqslant |\mathcal{L}|$, i.e. $\forall A \subseteq \mathcal{U}.\ |A| \leqslant \kappa \implies |S_1(A)| \leqslant \kappa$.

(2) No $\mathcal{L}$-formula $\varphi(\overline{x}, \overline{y})$ has OP.

(3) Every type over a model is definable.

Question 6.16.68. Do there exist non-realized global definable types in Psf?

Theorem 6.17 (Hils - Hrushovski)**.** If $K \models \mathsf{Psf}_0$, there exist non-realized definable types in $S_n(K)$ for all n, even of transcendence degree n over K.

To prove this, we need some input from the model theory of valued fields. Those will only be stated here.

In the proof of Proposition 6.5, we have seen the following:

Lemma 6.18. If $K \models \mathsf{Psf}$ and $(K((t^{\mathbb{Q}})), v_t)$ the Hahn series field, there is $\tilde{K} \succeq K$ such that $K \subseteq K((t^{\mathbb{Q}})) \subseteq \tilde{K}$ with $K((t^{\mathbb{Q}}))$ relatively algebraically closed in $\tilde{K}$.

Notation and Classical Facts from the Model Theory of Valued Fields
Recall that a **valuation** on a field L is a (surjective) map $v\colon L \twoheadrightarrow \Gamma_L \cup \{\infty\}$, where $(\Gamma_L, +, \leqslant)$is an ordered abelian group such that

(i) $v(x) = \infty$ iff $x = 0$,

(ii) $v(x \cdot y) = v(x) + v(y)$

(iii) $v(x + y) \geqslant \min(v(x), v(y))$,

where we use the convention $\infty > \Gamma_L$, and $\gamma + \infty = \infty + \gamma = \infty + \infty = \infty$ for all $\gamma \in \Gamma_L$.

- $\mathcal{O}_L := \{x \in L | v(x) \geqslant 0\}$ is called the **valuation ring** of L. Its unique maximal ideal is given by $\mathfrak{m}_L := \{x \in L | v(x) > 0\}$.
- $k_L := \frac{\mathcal{O}_L}{\mathfrak{m}_L}$ is called the **residue field** and $\mathrm{res} : \mathcal{O}_L \twoheadrightarrow k_L$ is the canonical map, called the **residue map**.
- Γ_L is called the **value group**.
- (L, v) is called **henselian** iff for every $P(X) \in \mathcal{O}_L[X]$ and every $a \in \mathcal{O}_L$ with $v(P(a)) > 0 = v(P'(a))$, then there is $b \in \mathcal{O}_L$ such that $P(b) = 0$ and $\mathrm{res}(b) = \mathrm{res}(a)$.
- A **section** (or **cross section**) of the valuation is a group homomorphism $s \colon (\Gamma_L, +) \to (L^\times, \cdot)$ such that $v \circ s = \mathrm{id}_{\Gamma_L}$.
- Assume $\mathrm{char}(L) = \mathrm{char}(k_L)$. A **lift** of the residue field is a field embedding $i \colon k_L \to L$, $(i(k_L) \subseteq \mathcal{O}_L)$ such that $\mathrm{res} \circ i = \mathrm{id}_{k_L}$.

If $(L, \Gamma_L, k_L, v, s, i)$ is a valued field (of equal characteristic) with lift and section, we treat it as a first order structure in a 3-sorted language with

- a sort VF for the valued field, endowed with $\mathcal{L}_{\mathrm{ring}}$,
- a sort RF for the residue field, endowed with (another copy of) $\mathcal{L}'_{\mathrm{ring}}$,
- a sort Γ for the value group (with ∞), endowed with $\mathcal{L}_{\mathrm{oag}} \cup \{\infty\} = \{0, \leqslant, +, \infty\}$,
- connecting functions $v \colon \mathrm{VF} \to \Gamma$, $\pi \colon \mathrm{VF} \to \mathrm{RF}$ (residue map on $\mathcal{O}$, extended by 0), $i \colon \mathrm{RF} \to \mathrm{VF}$, $s \colon \Gamma \to \mathrm{VF}(\infty \mapsto 0)$.

Fact 6.19. Let $\mathbb{L} := (L, \Gamma_L, k_L, v, s, i, \pi)$ be a henselian valued field of equal characteristic 0 with lift and section. Then $\mathrm{Th}(\mathbb{L})$ eliminates VF-quantifiers.

A proof may be found in [van14].

Syntactically (with a little bit of algebra) we get:

Corollary 6.20. With the notation from Fact 6.19 we have

(a) The residue field k_L is stably embedded with induced structure of a prime field.

(b) Γ_L is stabily embedded with induced structure of an OAG.

(c) $k_L \perp \Gamma_L$, i.e. every definable subset $D \subseteq k_L^n \times \Gamma_L^m$ is a finite union of rectangles $D_1 \times D_2$, where $D_1 \overset{\text{definable}}{\subseteq} k_L^n$, $D_2 \overset{\text{definable}}{\subseteq} \Gamma_L^m$.

Proof of Theorem 6.17. We will show the following more precise version, where $K((t^{\mathbb{Q}}))$ is considered as a (henselian, equchar 0) valued field with lift $(a \mapsto at^0)$ and section $(q \mapsto t^q)$:

Proposition 6.21. Let $K \models \mathsf{Psf}_0$, let $\overline{a}$ be a tuple from $K((t^{\mathbb{Q}}))$. Where $K \subseteq K((t^{\mathbb{Q}})) \overset{\text{rel. alg. closed}}{\subseteq} \tilde{K}$, where $\tilde{K} \succeq K$. This exists by **??**. Then $\mathrm{tp}_{\mathrm{Th}(K)}\left(\frac{\overline{a}}{K}\right)$ is definable.

Subproof. By Quantifier Reduction in Psf (2.13), every $\mathcal{L}_{\mathrm{ring}}$-formula $\varphi(\overline{x}, \overline{y})$ is equivalent modulo Psf to a boolean combination of formulas of the form $\exists t.\ f(\overline{X}, \overline{Y}, t) = 0$, where $f \in \mathbb{Z}[\overline{X}, \overline{Y}, T]$.

For $\psi(\overline{X}, \overline{Y}) :\equiv \exists t.\ f(\overline{X}, \overline{Y}, t) = 0$ and $\overline{b} \in K^{|\overline{y}|}$ one has $K((t^{\mathbb{Q}})) \models \psi(\overline{a}, \overline{b})$ iff $\tilde{K} \models \psi(\overline{a}, \overline{b})$, since $K((t^{\mathbb{Q}}))$ is relatively algebraically closed in $\tilde{K}$.

By Corollary 6.20 (a) and since K is in $\varnothing$-definable bijection via i with the residue field, for any $\psi(\overline{x}, \overline{y})$ as above, the set $\{\overline{b} \in K^{|\overline{y}|} | K((t^{\mathbb{Q}})) \models \psi(\overline{a}, \overline{b})\}$ is $\mathcal{L}_{\mathrm{ring}}(K)$-definable by $\chi(\overline{y})$.

Setting $p := \mathrm{tp}_{\mathrm{Th}(K)}(\overline{a}/K)$, we see that $d_p\psi(\overline{y}) :\equiv \chi(\overline{y})$ works.

By quantifier reduction this suffices to show that p is definable. ■

□

Remark 6.22. The same proof shows that $\mathrm{tp}_{\mathcal{L}_{\mathrm{ring}}}(\overline{a}/K)$ is definable for every $\overline{a} \in K((t^{\mathbb{Q}})) \overset{\text{rel. alg. closed}}{\subseteq} \tilde{K}$, $\tilde{K} \succeq K$, where K satisfies

(i) $\mathrm{char}(K) = 0$,

(ii) in $\mathrm{Th}(K)$, the quantifier free type of a relatively algebraically closed subfield determines its type ("quantifier reduction")

(iii) $K((t^{\mathbb{Q}}))$ embeds in a relatively algebraically closed way in $\tilde{K} \succeq K$ over K.

E.g. this holds for K PAC of $\mathrm{char}\,0$, with $\mathrm{Gal}(K)$ topologically finitely generated.

(Actually, it suffices that K has only finitely many Galois extension of every degree n for all $n \in \mathbb{N}$.)

Exercise, generalize the homework to achieve (iii)

7 ACFA, the theory of e.c. difference fields

[Lecture 24, 2025-01-17]

Definition 7.0.69. • A **difference field** is a structure (K, σ), where K is a field and $\sigma \in \mathrm{Aut}(K)$.

- For a difference field (K, σ) and $n \in \mathbb{N}$, the **difference polynomial ring in n variables over K** is defined as

$$K\langle X_1, \ldots, X_n\rangle := K[X_1, \ldots, X_n, \sigma(X_1), \ldots, \sigma(X_n), \sigma^2(X_1), \ldots, \sigma^2(X_n), \ldots] = K[\sigma^j(X_i) | j \in \mathbb{N}, i = 1, \ldots, n],$$

where the $\sigma^j(X_i)$ are ordinary variables.

$K\langle X_1, \ldots, X_n\rangle$ is endowed with the natural extension $\tilde{\sigma}$ of σ given by $\tilde{\sigma}(\sigma^j(X_i)) := \sigma^{j+1}(X_i)$. In a slight abuse of notation we will write σ instead of $\tilde{\sigma}$.

Remark 7.1. • We will treat difference fields as first order structures in the language $\mathcal{L}_\sigma := \mathcal{L}_{\mathrm{ring}} \cup \{\sigma\}$.

The class of difference fields is elementary, i.e. it may be axiomatized in $\mathcal{L}_\sigma$.

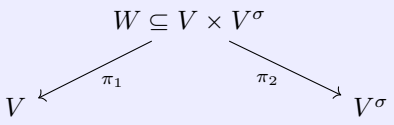
- If $I = (f_1, \ldots, f_m) \leqslant K[X_1, \ldots, X_n]$, then $I^\sigma := (f_1^\sigma, \ldots, f_m^\sigma) \leqslant K[X_1, \ldots, X_n]$ is an ideal, where $\left(\sum a_i X^i\right)^\sigma := \sum \sigma(a_i) X^i$. I is prime iff I^σ is prime.
- If $V = V(f_1, \ldots, f_m) = V(I)$, then $\sigma(V(K)) = \{\sigma(\overline{a}) | \overline{a} \in V(K)\} = V^\sigma(K)$, where $V^\sigma := V(I^\sigma)$.

Definition 7.1.70. The theory ACFA in $\mathcal{L}_\sigma$ is given by the following conditions on an $\mathcal{L}_\sigma$-structure (K, σ):

(i) K is an algebraically closed field.

(ii) $\sigma \in \mathrm{Aut}(K)$.

(iii) For every $d, n \in \mathbb{N}$ and (absolutely) irreducible variety $V \subseteq \mathbb{A}^n$ defined over K with polynomials of degree $\leqslant d$ and every absolutely irreducible $W \subseteq V \times V^\sigma$ defined over K with polynomials of degree $\leqslant d$ such that in



$\pi_1(W) \subseteq V$ and $\pi_2(W) \subseteq V^\sigma$ are Zariski dense, there is $\overline{a} \in K^n$ such that $(\overline{a}, \sigma(\overline{a})) \in W(K)$.

Note. *By Fact 2.2 and the definability of Morley rank in* ACF*, (iii) is indeed a*

first order axiom scheme.

Theorem 7.2. ACFA is the model companion of the theory of difference fields, i.e. every difference field embeds into a model of ACFA and ACFA is model-complete.

Equivalently, the models of ACFA are precisely the e.c. difference fields.

Proof.

Claim 1. *If (K,σ) is an e.c. difference field, then it is a model of* ACFA.

Subproof. Assume that (K,σ) is an e.c. difference field. Then σ extends to an automorphism σ' of K^{alg}, so $(K,\sigma) \subseteq (K^{\mathrm{alg}},\sigma')$ as difference fields. As (K,σ) is e.c., it follows that $K = K^{\mathrm{alg}}$, so (i) and (ii) hold for (K,σ).

We now show (iii). Assume that $V \subseteq \mathbb{A}^n$ is an irreducible variety over K,. $W \subseteq V \times V^\sigma$ an irreducible subvariety such that $\pi_1(W) \subseteq V$ and $\pi_2(W) \subseteq V^\sigma$ are Zariski dense.

Let $L \succeq K$ be an $|K|^+$-saturated elementary extension of K and let $(\overline{\alpha},\overline{\beta}) \in L^{2n}$ be a generic of W over K. As $\pi_1(W)$ is Zariski dense in V (and thus the generic type p_W of W over K projects to the generic type p_V of V over K), $\overline{\alpha} \models p_V$, i.e. $\overline{\alpha}$ is generic in V over K. Similarly, $\overline{\beta}$ is generic in V^σ over K.

Thus $\tilde{\sigma}\colon K(\overline{\alpha}) \to \sigma(K)(\overline{\beta})$ with $\tilde{\sigma}|_K = \sigma$, $\tilde{\sigma}(\alpha_i) := \beta_i$ is a partial automorphism of L. It extends to $\sigma' \in \mathrm{Aut}(L)$ and thus $(K,\sigma) \subseteq (L,\sigma')$. If $W = \mathrm{Var}(f_1,\dots,f_m)$, we thus get

$$(L,\sigma) \models \exists x_1,\dots,x_n \bigwedge_{i=1}^{m} f_i(\overline{x},\sigma(\overline{x})) = 0,$$

so, as (K,σ) is e.c. in (L,σ), we get

$$(K,\sigma) \models \exists \overline{x} \bigwedge_{i=1}^{m} f_i(\overline{x},\sigma(\overline{x})) = 0,$$

showing that (iii) is satisfied. ∎

Claim 2. *If $(K,\sigma) \models$* ACFA*, then (K,σ) is an e.c. difference field.*

Subproof. Assume $(K,\sigma) \models$ ACFA. Let (L,σ) be a difference field extension of (K,σ) and let $\varphi(\overline{x})$ be a quantifier-free $\mathcal{L}_\sigma(K)$-formula such that $(L,\sigma) \models \exists \overline{x}.\ \varphi(\overline{x})$. We need to show that $(K,\sigma) \models \exists \overline{x}.\ \varphi(\overline{x})$.

$\varphi(\overline{x})$ is a finite disjunction of formulas of the form

$$\bigwedge_{i=1}^{m} f_i(\overline{x}) = 0 \wedge \bigwedge_{j=1}^{k} g_j(\overline{x}) \neq 0,$$

where $f_i, g_j \in K\langle \overline{X} \rangle$.

We may assume that these are disjunct and, setting $g(\overline{X}) \coloneqq \prod_{j=1}^{k} g_j(\overline{X})$, we may further assume that $\varphi(\overline{X})$ is of the form

$$g(\overline{X}) \neq 0 \wedge \bigwedge_{i=1}^{m} f_i(\overline{X}) = 0.$$

Since $\exists \overline{x}.\ \varphi(\overline{x})$ is equivalent to

$$\exists \overline{x}, y.\ g(\overline{x}) \cdot y - 1 = 0 \wedge \bigwedge_{i=1}^{m} f_i(\overline{x}) = 0,$$

we may assume that

$$\varphi(\overline{x}) \equiv \bigwedge_{i=1}^{m} f_i(\overline{x}) = 0.$$

Let r be such that $f_1, \ldots, f_m \in K[\overline{X}, \sigma(\overline{X}), \ldots, \sigma^r(\overline{X})]$. Then

$$\begin{aligned} & K \models f_i(\overline{a}, \sigma(\overline{a}), \ldots, \sigma^r(\overline{a})) = 0 \\ \iff & K \models \exists \overline{t}_1, \ldots, \overline{t}_r.\ f_i(\overline{x}, \overline{t}_1, \ldots, \overline{t}_r) = 0 \\ & \wedge \bigwedge_{i=1}^{r-1} \sigma(\overline{t}_i) = \overline{t}_{i+1} \wedge \sigma(\overline{x}) = \overline{t}_1. \end{aligned}$$

Thus we may assume $r = 1$, i.e. $f_i \in K[\overline{X}, \sigma(\overline{X})]$ and

$$\varphi(\overline{X}) \equiv \bigwedge_{i=1}^{m} f_i(\overline{X}, \sigma(\overline{X})) = 0.$$

Let $\tilde{W} \subseteq \mathbb{A}^{2n}$ be the K-variety defined by

$$\tilde{W} \coloneqq \mathrm{Var}(f_1(\overline{X}, \overline{Y}), \ldots, f_m(\overline{X}, \overline{Y})).$$

Choose $\overline{\alpha} \in L^n$ such that $(L, \sigma) \models \varphi[\overline{\alpha}]$. Set

$$\begin{aligned} \overline{\beta} &\coloneqq \sigma(\overline{\alpha}), \\ W &\coloneqq \mathrm{loc}(\overline{\alpha}, \overline{\beta}/K) \subseteq \mathbb{A}^{2n}, \\ V &\coloneqq \mathrm{loc}(\overline{\alpha}/K) \subseteq \mathbb{A}^{n}, \\ V' &\coloneqq \mathrm{loc}(\overline{\beta}/K) \subseteq \mathbb{A}^{n}. \end{aligned}$$

Then $V' = V^\sigma$ and W,V and V^σ are irreducible with generics over K given by $(\overline{\alpha}, \overline{\beta})$, $\overline{\alpha}$ resp. $\overline{\beta}$. Thus $\pi_1 \colon W \to V$ and $\pi_2 \colon W \to V^\sigma$ have Zariski dense image. By (iii) there is $\overline{a} \in K^n$ such that $(\overline{a}, \sigma(\overline{a})) \in W(K) \subseteq \tilde{W}(K)$, so in particular $(K, \sigma) \models \varphi[\overline{a}]$. ■

□

Notation 7.2.71. For $A \subseteq K \models \mathsf{ACFA}$ we set $\mathrm{acl}_\sigma(A) := \mathrm{Frac}\left(\langle \bigcup_{z\in\mathbb{Z}} \sigma^z(A)\rangle\right)^{\mathrm{alg}}$.

Theorem 7.3 (Quantifier reduction)**.** Quantifier Reductionthm:acfa-quantifier-reduction Let $(E,\sigma) \subseteq (K_i,\sigma_i) \models \mathsf{ACFA}$ for $i = 1,2$ with $E = \mathrm{acl}_\sigma(E)$. Then

$$(K_1,\sigma_1) \equiv_E (K_2,\sigma_2).$$

Corollary 7.4. (1) Let $K \models \mathsf{ACFA}$, $A \subseteq K$. Then $\mathrm{qftp}_{\mathcal{L}_\sigma}(\mathrm{acl}_\sigma(A))$ determines $\mathrm{tp}_K(a)$, i.e. if $A_i \subseteq K_i$ for $i = 1,2$, $K_i \models \mathsf{ACFA}$, then $\mathrm{tp}(A_1) = \mathrm{tp}(A_2)$ iff there exists an $\mathcal{L}_\sigma$ isomorphism $f\colon \mathrm{acl}_\sigma(A_1) \simeq \mathrm{acl}_\sigma(A_2)$ sending A_1 to A_2.

(2) The completions of ACFA are determined by $p := \mathrm{char}(K)$ and the conjugacy class of $\sigma|_{\mathbb{F}_p^{\mathrm{alg}}}$ inside $\mathrm{Gal}(\mathbb{F}_p)$ (where $\mathbb{F}_0 := \mathbb{Q}$).

Proof of **??**.

$$\begin{array}{ccc} (K_1,\sigma_1) & & (K_2,\sigma_2) \\ & \supseteq \quad\quad \subsetneq & \\ & (E,\sigma) = \mathrm{acl}_\sigma(E) & \end{array}$$

Working in some large $K \models \mathsf{ACFA}$ containing K_1 and K_2, we may assume $K_1 \overset{\text{l.d.}}{\underset{E}{\downarrow}} K_2$, and thus $K_1K_2 \simeq \mathrm{Frac}\,(K_1 \otimes_E K_2)$. Then $\sigma_1 \otimes \sigma_2$ extends to an automorphism of K_1K_2, which extends to $\tilde{\sigma} \in \mathrm{Aut}(\tilde{K})$, for some $\tilde{K} \subseteq K$ with $(\tilde{K},\tilde{\sigma}) \models \mathsf{ACFA}$, as models of ACFA are e.c. difference fields. By model completeness, $(K_i,\sigma_i) \preceq (\tilde{K},\tilde{\sigma})$, so $K_1 \equiv_E K_2$ in $\mathcal{L}_\sigma$. □

Theorem 7.5. If $(K,\sigma) \models \mathsf{ACFA}$, then $F := \mathrm{Fix}(\sigma) \models \mathsf{Psf}$. Moreover, for every $\tilde{F} \models \mathsf{Psf}$ there is $(K,\sigma) \models \mathsf{ACFA}$ such that $\tilde{F} = \mathrm{Fix}(\sigma)$.

Proof of Theorem 7.5. The second part follows from the first, as $\mathrm{Abs}(\tilde{F}) = \mathrm{Fix}(\sigma)$ for some σ of the Galois group of the prime subfield $\mathbb{F}_p$ of $\tilde{F}$ and $(\mathbb{F}_p^{\mathrm{alg}},\sigma) \subseteq (K,\sigma) \models \mathsf{ACFA}$.

We need to show that if $(K,\sigma) \models \mathsf{ACFA}$, then for $F := \mathrm{Fix}(\sigma)$:

Claim 7.5.1. *F is perfect.*

Claim 7.5.2. $\mathrm{Gal}(F) = \hat{\mathbb{Z}}$.

Claim 7.5.3. *F is PAC.*

Proof of Claim 7.5.1. Clear. □

Proof of Claim 7.5.2. As $\mathrm{Gal}(F) = \overline{\langle\sigma\rangle}$, it suffices to show that F admits an extension of degree n for all $n \geqslant 1$.

Claim 7.5.2.1. *For $n \geqslant 1$ there exists $a_n \in K$ such that $\sigma^n(a_n) = a_n$ and $\sigma^i(a_n) \neq a_n$ for $i < n$.*

Subproof. Let $y_1, \ldots, y_n$ be algebraically independent over K and extend σ to $\sigma' \colon K(\overline{y}) \to K(\overline{y})$ via $\sigma'(y_i) := y_{i+1}$ for $i < n$ and $\sigma'(y_n) := y_1$. As $(K, \sigma) \overset{\text{e.c.}}{\subseteq} (K(\overline{y}), \sigma')$, a_n exists in K. ■

Let $p(X) := \prod_{i=0}^{n-1}(X - \sigma^i(a_n)) \in K[X]$. Then $p^\sigma = p$, so $p(X) \in F[X]$. $F_n := {}^{F[\sigma^i(a_n) | i = 0, \ldots, n-1]}\!/_{F}$ is a Galois extension of degree n: Indeed $\mathrm{Gal}(F_n/F)$ is generated by σ, so σ is a topological generator of $\mathrm{Gal}(F)$ and $\mathrm{id}, \sigma, \ldots, \sigma^{n-1}$ are pairwise distinct in $\mathrm{Gal}(F_n/F)$, so $\mathrm{Gal}(F_n/F) \simeq \frac{\mathbb{Z}}{n\mathbb{Z}}$ □

Proof of Claim 7.5.3. Let $V \subseteq \mathbb{A}^n$ be an absolutely irreducible variety which is definable over F. Set $W := \Delta \cap V \times V$, i.e. $W = \mathrm{Var}(f_1(\overline{X}), \ldots, f_m(\overline{X}), X_1 - Y_1, \ldots, X_n - Y_n)$, where $V = \mathrm{Var}(f_1, \ldots, f_m)$.

As $V = V^\sigma$ and V, V^σ and W are absolutely irreducible with $\pi_1(W) = V$, $\pi_2(W) = V^\sigma$, axiom (iii) of ACFA yields $\overline{a} \in K^n$ such that $(\overline{a}, \sigma(\overline{a})) \in W$, so $\overline{a} = \sigma(\overline{a}) \in V(K)$. In other words $\overline{a} \in V(F)$. □

□

$\mathrm{acl}_{\mathrm{mth}}$ new notation for model theoretic acl?

Proposition 7.6. In models of ACFA, $\mathrm{acl}_{\mathrm{mth}}(A) = \mathrm{acl}_\sigma(A)$.

Proof. $\mathrm{acl}_\sigma(A) \subseteq \mathrm{acl}_{\mathrm{mth}}(A)$ is clear.

Conversely, let $b \in K \setminus \mathrm{acl}_\sigma(A)$, where $A \subseteq K \models \mathsf{ACFA}$. For $n \in \mathbb{N}$ we find $(K_i, \sigma_i) \simeq_{\mathrm{acl}_\sigma(A)} (K, \sigma)$ such that $K_0, K_1, \ldots$ are algebraically independent (so linearly disjoint) over $\mathrm{acl}_\sigma(A)$ and $(K_0, \sigma_0) = (K, \sigma)$. Let $(L, \sigma) := \mathrm{acl}_\sigma\left(\bigcup K_i, \sigma\right)$. Then there exists $(\mathcal{U}, \sigma) \supseteq (L, \sigma)$ with $\mathcal{U} \models \mathsf{ACFA}$. Let b_i be the copy of b in K_i. The b_i are pairwise distinct and have the same type over $\mathrm{acl}_\sigma(A)$ by Corollary 7.4. So $b \notin \mathrm{acl}_{\mathrm{mth}}(A)$. □

Definition 7.6.72. Let $(K, \sigma) \models \mathsf{ACFA}$ and $A, B, C \subseteq K$. We set $A \underset{B}{\overset{\sigma}{\downarrow}} C$ iff

$$\mathrm{acl}_\sigma(AB) \underset{\mathrm{acl}_\sigma(B)}{\overset{\mathrm{alg}}{\downarrow}} \mathrm{acl}_\sigma(BC).$$

Theorem 7.7 (Hrushovski, Shuddhodan-Varshavsky; w/o proof)**.** (1) $\mathsf{ACFA} = \{\varphi \ \ \mathcal{L}_\sigma\text{-sentence} : \forall q \gg 0.\ (\mathbb{F}_q^{\mathrm{alg}}, \mathrm{Frob}_q) \models \varphi\}$. In particular if $\mathcal{U}$ is a non-principal ultrafilter on the set of prime powers, then $\prod_{\mathcal{U}}(\mathbb{F}_q^{\mathrm{alg}}, \mathrm{Frob}_q) \models \mathsf{ACFA}$.

(2) $\mathsf{ACFA}_0 = \{\varphi \ \ \mathcal{L}_\sigma\text{-sentence} : \forall p \gg 0, p \in \mathbb{P}.\ (\mathbb{F}_p^{\mathrm{alg}}, \mathrm{Frob}_p) \models \varphi\}$.

[Lecture 25, 2025-01-21]

Theorem 7.8 (Independence Theorem in ACFA)**.** ACFA satisfies the independence theorem wrt. $\mathop{\smile\!\!\!\!\!\!|}^{\sigma}$ over acl_σ-closed sets.

Proof. This is just Proposition 5.17 namely that every 3-AP in ACF_σ admits a solution, together with the following two results:

(i) quantifier reduction, i.e. the quantifier-free $\mathcal{L}_\sigma$ of an acl_σ-closed set determines its complete type (Corollary 7.4).

(ii) model-theoretic algebraic closure equals acl_σ (Proposition 7.6).

□

Corollary 7.9. Every completion of ACFA is simple (actually **supersimple**[a]) and $\mathop{\smile\!\!\!\!\!\!|}^{f'} = \mathop{\smile\!\!\!\!\!\!|}^{\sigma}$

[a] i.e. every $\mathrm{tp}(\overline{a})$, $\overline{a}$ finite, does not fork over some finite $A_0 \subseteq A$

Proof. This holds by the Independence Theorem in ACFA (7.8) and the Theorem of Kim-Pillay (5.12). □

Corollary 7.10. Every completion of ACFA has IP, so in particular is unstable.

Proof. We have seen that if $(K, \sigma) \models \mathsf{ACFA}$, then $\mathrm{Fix}(\sigma) \models \mathsf{Psf}$ (Theorem 7.5).

By Theorem 5.19 we have that every completion of Psf has IP. □

Recall the following definitions:

Definition 7.10.73. • A complete $\mathcal{L}$-theory **eliminates imaginaries**, **EI** iff for every $\mathcal{M} \models T$ and $a \in \mathcal{M}^{\mathrm{eq}}$ (Shelah's $\mathcal{M}^{\mathrm{eq}}$ construction adding to $\mathcal{M}$ sorts for $M^n/E = S_E\ (M^{\mathrm{eq}})$, where E is $\varnothing$-definable evuialence relation on M^n), there is a real tuple $\overline{b} \in M^n$, such that a and $\overline{b}$ are interdefinable.

- T **uniformly eliminates imaginaries**, **UEI**, iff for every $\varnothing$-definable equivalence relation E on M^n, there is an $\varnothing$-definable function $f\colon M^n \to M^m$, such that $E(\overline{a},\overline{a}')$ iff $f(\overline{a}) = f(\overline{a}')$, $\overline{a},\overline{a}' \in M^n$, i.e. f induces $\overline{f}\colon M^n/_E \hookrightarrow M^m$.

Fact 7.11. For a complete $\mathcal{L}$-theory such that all models have at least 2 elements, the following are equivalent:

(1) T has UEI

(2) T has EI and $|\operatorname{dcl}(\varnothing)| \geqslant 2$.

Proof. □ Easy exercise

Definition 7.11.74.

- T **weakly eliminates imaginaries**, **WEI** iff for every $\mathcal{M} \models T$, $a \in M^{\mathrm{eq}}$, there is $\overline{b} \in M^n$ such that $a \in \operatorname{dcl}^{\mathrm{eq}}(\overline{b})$ and $\overline{b} \in \operatorname{acl}^{\mathrm{eq}}(a)$.
- T **eliminates finite imaginaries**, **FEI**,iff for every $M \models T$ and finite set $F = \{\overline{a}_1, \ldots, \overline{a}_m\} \subseteq M^n$, there is $\overline{b} \in M^k$ such that $\overline{b} = \ulcorner F \urcorner$, i.e. assuming $\mathcal{M}$ is ω-strongly homogeneous (e.g. a monster model) that for all $\sigma \in \operatorname{Aut}(\mathcal{M})$, we have $\sigma(F) = F$ iff $\sigma(\overline{b}) = \overline{b}$.

Fact 7.12. For a complete $\mathcal{L}$-theory T, the following are equivalent:

(1) T has EI,

(2) T has WEI and FEI.

Proof. Left as an exercise. □

Corollary 7.13. Let $\mathcal{L} \supseteq \mathcal{L}_{\mathrm{ring}}$ and T a complete $\mathcal{L}$-theory extending the theory of fields. Assume that T has WEI. Then T has UEI.

Proof. As $0 \neq 1$are $\varnothing$-definable, by Fact 7.12 and Fact 7.11 it suffices to show that T has FEI.

Let $F = \{\overline{a}_1, \ldots, \overline{a}_m\} \subseteq M^n$ for $\mathcal{M} \models T$ (assumed strongly ω-homogeneous). We consider the following polynomial

$$P(Z, Y_1, \ldots, Y_n) := \prod_{i=1}^{m} (Z - \sum_{j=1}^{n} a_{ij} Y_j) \in M[Z, \overline{Y}].$$

Claim 1. *A field automorphism of M (in particular, any $\sigma \in \mathrm{Aut}(\mathcal{M})$) fixes P iff it permutes the $\overline{a}_i$ iff $\sigma(F) = F$.*

Subproof. " $\Longleftarrow$ " is by the definition of P.

" $\Longrightarrow$ " Assume $P^\sigma = P$. Then σ necessarily maps irreducible factors of P to irreducible factors of P (in the UFD $M[Z, \overline{Y}]$). These are given by $Z - \sum_{i=1}^{n} a_{ij} Y_j$ and uniquely determined if normalized in Z.

Thus $\sigma(F) = F$. ■

So the coefficients of $P(Z, \overline{Y})$ are $\overline{b}$ as desired. □

Definition 7.13.75. Let ${}^{L}\!/_{K}$ be a difference field extension and $b \in L$. Then b is **transformally algebraic over** K iff there is $P(X) \in K\langle X\rangle \backslash \{0\}$ such that $P(b) = 0$.

Equivalently, $\mathrm{trdeg}(K\langle b\rangle/K) < \infty$.

The **transformal algebraic closure** is defined as $\mathrm{trfcl}_L(K) := \{b \in L | b \text{ transformally algebraic over } K\}$.

It is easy to see that $\mathrm{trfcl}_L(-)$ defines a pregeometry, as it satisfies Steinitz-exchange. We get notions of **transformal algebraic independence**, **transformal transcendence basis**, **transformal transcendence degree** etc.

Exercise

Lemma 7.14 (Neumann's Lemma)**.** Let G be a group, $G \curvearrowright \Omega$ an action on a set without finite orbits. Then if $X, Y \overset{\text{finite}}{\subseteq} \Omega$, there is $g \in G$ such that $gX \cap Y = \varnothing$.

We will prove this next time.

Theorem 7.15. Every completion of ACFA has UEI.

Proof of Theorem 7.15. By Corollary 7.13 it suffices to show that if $(K, \sigma) \models \mathsf{ACFA}$, then $T := \mathrm{Th}(K, \sigma)$ has WEI.

Equivalently, by compactness, it suffices to show that if $e \in K^{\mathrm{eq}}$ and $E := \mathrm{acl}^{\mathrm{eq}}(e) \cap K$, then $e \in \mathrm{dcl}^{\mathrm{eq}}(E)$.

We may assume that (K, σ) is a monster model of T. Let f be an $\varnothing$-definable function and $\overline{a} \in K^N$ such that $f(\overline{a}) = e$. Let P be the set of realizations of $\mathrm{tp}(\overline{a}/E)$ in K.

Claim 7.15.1. *There is a tuple $\overline{c} \in P$ such that $f(\overline{c}) = e$ and $\overline{a} \underset{E}{\downarrow^{\sigma}} \overline{c}$.*

Subproof. There exists $\overline{b} \in K^N$ such that $\mathrm{tp}(\overline{a}/Ee) = \mathrm{tp}(\overline{b}/Ee)$ (in particular $\overline{b} \in P$) such that

$$E = \mathrm{acl}_\sigma(E\overline{a}) \cap \mathrm{acl}_\sigma(E\overline{b}). \tag{10}$$

Indeed, set $G := \mathrm{Aut}(K/Ee)$. Let $\Omega := K \backslash E$. Then $G \curvearrowright \Omega$ has only infinite orbits by definition of E. Using compactness to achieve (10), it suffices to show (10) for finite subsets $X = Y$ of $\mathrm{acl}_\sigma(E\overline{a}) \backslash E$

By Neumann's Lemma (7.14), we find $\sigma \in G$ such that $\sigma(X) \cap X = \varnothing$.

Choose such a $\overline{b} \equiv_{Ee} \overline{a}$ with (10) of maximal transformal transcendence degree m over $E\overline{a}$ and then such that for some transformal transcendence basis $(b_{i_1}, \ldots, b_{i_m})$ of $\overline{b}$ over $E\overline{a}$, $\mathrm{trdeg}(E\langle \overline{a}, \overline{b}\rangle / E\langle \overline{a}, b_{i_1}, \ldots, b_{i_m}\rangle) =: n$ is as large as possible. (This maximum exists as otherwise m were not maximal by compactness)

Now let $\overline{c}$ be such that $\mathrm{tp}(\overline{c}/E\overline{a}) = \mathrm{tp}(\overline{b}/E\overline{a})$ and

$$\overline{c} \underset{E\overline{a}}{\downarrow^\sigma} \overline{b}. \tag{11}$$

Then as $e = f(\overline{a})$ and $\mathrm{tp}(\overline{b}/Ee) = \mathrm{tp}(\overline{a}/Ee)$, we get $f(\overline{c}) = f(\overline{b}) = f(\overline{a}) = e$ and $\mathrm{acl}_\sigma(E\overline{c}) \cap \mathrm{acl}_\sigma(E\overline{b}) \overset{(11)}{\subseteq} \mathrm{acl}_\sigma(E\overline{a}) \cap \mathrm{acl}_\sigma(E\overline{b}) \overset{(10)}{=} E$.

By maximality of m, we get $\mathrm{trftrdeg}(\overline{c}/E\overline{b}) \leqslant m$. On the other hand, by (11) we get

$$\mathrm{trftrdeg}(\overline{c}/E\overline{b}) \geqslant \mathrm{trftrdeg}(\overline{c}/E\overline{b}\overline{a}) \overset{(11)}{=} \mathrm{trftrdeg}(\overline{c}/E\overline{a}) = \mathrm{trftrdeg}(\overline{b}/E\overline{a}) = m.$$

Thus $\mathrm{trftrdeg}(\overline{c}/E\overline{b}) = m$.

Similarly, if $c_{i_1}, \ldots, c_{i_m}$ is the transformal transcendence basis of $\overline{c}$ over $E\overline{b}$ copied from $b_{i_1}, \ldots, b_{i_m}$, then $\mathrm{trdeg}(E\langle \overline{b}, \overline{c}\rangle / E\langle \overline{b}, \overline{c}_{i_1}, \ldots, \overline{c}_{i_m}\rangle) \leqslant n$ and thus by a similar argument as before, using (11) it is equal to n.

Thus $\overline{c} \underset{E\overline{b}}{\downarrow^\sigma} \overline{a}$. ($c_{i_1}, \ldots, c_{i_m} \underset{E\overline{b}}{\downarrow^\sigma} \overline{a}$, then $\overline{c} \underset{E\overline{b}c_{i_1}, \ldots, c_{i_n}}{\downarrow^\sigma} \overline{a}$). Moreover, by our choice (11), we get that (!)

$$\overline{c} \underset{E}{\downarrow^\sigma} \overline{a}, \overline{b}.$$

Hence $\overline{c} \underset{E}{\downarrow^\sigma} \overline{a}$, proving the claim.

Ad (!): Let $F = \mathrm{acl}_\sigma(F)$ and $\overline{c} \in K^N$. Then there is a smallest $F_0 = \mathrm{acl}_\sigma(F_0)$ such that $\overline{c} \underset{F_0}{\downarrow^\sigma} F$. (This uses that ACF eliminates imaginaries). Set $F := \mathrm{acl}_\sigma(E\overline{a}\overline{b})$. $F_0 \subseteq \mathrm{acl}_\sigma(E\overline{a}) \cap \mathrm{acl}_\sigma(E\overline{b}) \overset{(10)}{=} E$. ∎

We will finish the proof next time.

[Lecture 26, 2025-01-24]

In memory of

ZOÉ CHATZIDAKIS
03. 04. 1955 - 22. 01. 2025

Continuation of proof of Theorem 7.15.

Claim 7.15.1. *f is constant on P.*

Subproof. Suppose not, so there is $\overline{d} \in P$ such that $e = f(\overline{a}) \neq f(\overline{d}) =: e'$. We may assume $\overline{d} \underset{E}{\downarrow}^{\sigma} \overline{a}$: Indeed, let $\overline{c} \in P$ be such that $\overline{c} \underset{E}{\downarrow}^{\sigma} \overline{a}\overline{d}$. If $f(\overline{c}) \neq e$, choose $\overline{c}$ add the new $\overline{d}$. If $f(\overline{c}) = e$, then $f(\overline{c}) \neq e'$. Let $\tau \in \mathrm{Aut}(K/F)$ such that $\tau(\overline{d}) = \overline{a}$. Let $\tau(\overline{c})$ be the new $\overline{d}$.

Using the Independence Theorem in ACFA (7.8) over acl_σ-closed sets (we use it over E),

Claim 7.15.1 and the avoe lead to a contradiction: Let $\overline{a}, \overline{d} \in P$ with $\overline{a} \underset{E}{\downarrow}^{\sigma} \overline{d}$ and $f(\overline{a}) \neq f(\overline{d})$.

Set $A := \mathrm{acl}_\sigma(E\overline{a})$, $D := \mathrm{acl}(E\overline{d}$, so $A \underset{E}{\downarrow}^{\sigma} D$. Let $\overline{c} \in P$ such that $f(\overline{c}) = f(\overline{a})$ and $\overline{c} \underset{E}{\downarrow}^{\sigma} \overline{a}$. (This exists by Claim 7.15.1.)

Let $p(x) := \mathrm{tp}(\overline{c}/A)$, so p does not fork over E. Similarly , let $q(x) := \mathrm{tp}(\overline{c}'/D)$, where $\overline{c}' \underset{E}{\downarrow}^{\sigma} \overline{d}$, $\overline{c}' \in P$ and $f(\overline{c}') = f(\overline{d})$. (This exists by using $\tau \in \mathrm{Aut}(K/E)$, $\tau(\overline{a}) = \overline{d}$ and setting $\overline{c}' := \tau(\overline{c}.)$ q does not fork over E.

By the Independence Theorem in ACFA (7.8) there exists $r(x) \in S(AD), r \supseteq p \cup q$ (and r does not fork over E, but we don't need that). Let $\tilde{c} \models r$. Then $f(\overline{a}) \overset{\tilde{c} \models b}{=} f(\tilde{c}) \overset{\tilde{c} \models q}{=} f(\overline{d})$, but $f(\overline{a}) \neq f(\overline{d})$ ↯ ■

We obtain that $e \in \mathrm{dcl}^{\mathrm{eq}}(E)$, as $\mathrm{Aut}(K/E)$ fixes e. □

Corollary 7.16. If $(K, \sigma) \models \mathsf{ACFA}$, the fixed field $F := \mathrm{Fix}(\sigma)$ is stably embedded in K.[a]

In fact every $\mathcal{L}_\sigma(K)$-definable subset X of F^m is $\mathcal{L}_{\mathrm{ring}}(F)$-definable.

[a] Recall that a predicate P is **stably embedded** in a model M iff for all $n \in \mathbb{N}$ every subset of P^n which is definable in N is definable in N with parameters from P.

Proof. Let $X \subseteq F^m$ be $\mathcal{L}_\sigma(K)$-definable. As $\mathrm{Th}(K,\sigma)$ has EI (there is $c \in K^n$ such that $c = \ulcorner X \urcorner$. $(\tau(X) = X \iff \tau(c) = c$ for all $\tau \in \mathrm{Aut}(K,\sigma))$.

As $\sigma(X) = X$ fixes its element pointwise and $\sigma inn\, \mathrm{Aut}(K,\sigma)$, we get $\sigma(c) = c$, so $c \in F^N$, so X is $\mathcal{L}_\sigma(F)$-definable.

The fact that X is even $\mathcal{L}_{\mathrm{ring}}(F)$-definable follows from the following more precise result. □

Proposition 7.17. Let $(K,\sigma) \models \mathsf{ACFA}$ and $F := \mathrm{Fix}(\sigma)$ ($F \models \mathsf{Psf}$ by Theorem 7.5). Then the induced structure on F is given by $\mathcal{L}_{\sigma\text{-ind}}$, obtained by expanding $\mathcal{L}_{\mathrm{ring}}$ by a $2n$-ary relation C_n for each $n \geqslant 2$ defined as follows:

$$(a_1,\ldots,a_n,b_1,\ldots,b_n) \in C_n$$
$$\iff p_{\overline{a}}(X) := X^n + a_1X^{n-1} + \ldots + a_n \in F[X] \text{ is ir}$$
$$\wedge \text{if} p_{\overline{a}}(\alpha) = 0 \text{ then } \sigma(\alpha) = b_1 + b_2\alpha + \ldots + b_{n-1}\alpha^{n-1}.$$

Exercise: C_n is $\mathcal{L}_{\mathrm{ring}}(F)$-definable, proving the corollary

Proof. Note that if $X^n + a_1X^{n-1} + \ldots + a_n =: p_{\overline{a}}(x)$ is irreducible in $F[X]$ and if $p_{\overline{a}}(\alpha) = 0$, then $F_n := F[\alpha]$ is the unique (Galois) extension of F of degree n, and $\mathrm{Gal}\left(F_n/F\right) = \langle \sigma|_{F_n} \rangle \cong \mathbb{Z}/n\mathbb{Z}$.

In particular, the n roots of $p_{\overline{a}}$ in F_n are given by $\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)$.

If $\sigma(\alpha) = b_1 + b_2\alpha + \ldots + b_n\alpha^{n-1}$ for $\overline{b} \in F^n$, then $\sigma(\sigma^k(\alpha)) = \sigma^k(\sigma(a)) = b_1 + b_2\sigma^k(\alpha) + \ldots + b_n\sigma^k(\alpha)^{n-1}$.

In other words, $\overline{b}$ is independent of the root $\tilde{\alpha}$ of $P_{\overline{a}}(X)$.

Cleary, the C_n are $\varnothing$-definable in (K,σ).

Conversely, we need to show that every finite domain partial elementary selfmap τ of F with respect to $\mathcal{L}_{\sigma\text{-ind}}$ is partial elementary in (K,σ). Any such τ extends to $\tilde{\tau} \in \mathrm{Aut}_{\mathcal{L}_{\sigma\text{-ind}}}(F)$.

If $F_n = F[\alpha]$ and $\mathrm{MiPo}(\alpha/F) = p_{\overline{a}}(X)$, then by the definition of C_n, if $\overline{b} \in F^n$ is the unique n-tuple from F such that $(\overline{a},\overline{b}) \in C_n$, we get $\models C_n(\tilde{\tau}(\overline{a}),\tilde{\tau}(\overline{b}))$. In other words if α' is a root of $p_{\tilde{\tau}(\overline{a})}(X)$, then $\sigma(\alpha') = \tilde{\tau}(b_1) + \ldots + \tilde{\tau}(b_n)\alpha'^{n-1}$. Thus $\alpha \mapsto \alpha'$ defines an extension of $\tilde{\tau}$ to $\tilde{\tau_n}\colon F_n \cong F_n$ commuting with $\sigma|_{F_n}$.

So $\tilde{\tau}$ extends to $\tilde{\tau}_\infty \in \mathrm{Aut}(F^{\mathrm{alg}}, \sigma|_{F^{\mathrm{alg}}})$. By **??**, $\tilde{\tau}_\infty$ is partial elementary in (K,σ). In particular, τ is partial elementary. □

Corollary 7.18. Let T be a completion of ACFA and $T' := \mathrm{Th}_{\mathcal{L}\text{-ind}}(F)$, $F := \mathrm{Fix}(\sigma)$ for $(K,\sigma) \models T$.

Then T' has UEI.

Corollary 7.19. Let $F \models \mathsf{Psf}$, let $(c_{n,i})_{\substack{n\geqslant 2\\ 1\leqslant i\leqslant n}}$ be from F such that $P_{\overline{c}^n}(x)$ is irreducible of degree n for every $n \geqslant 2$, where $\overline{c}^n := (c_{n,1}, \ldots, c_{n,n}$. Then $\mathrm{Th}(F, (c_{n,i})_{\substack{n\geqslant 2\\ i\leqslant n}}$ has EI in $\mathcal{L}_{\mathrm{ring}} \cup \{c_{n,i}\}$.

Proof. We first how that if we choose a topological generator σ of $\mathrm{Gal}(F)$ and then for evey $n \geqslant 2$ $2n$-tuples $(\overline{a}^n, \overline{b}^n) \in F^{2n}$ lying in C_n, then $(F, \overline{a}^n, \overline{b}^n, n \geqslant 2)$ has EI. Indeed this follows from Corollary 7.18 since the $\mathcal{L}_{\sigma\text{-ind}}$-structure of F (lying inside $(F^{\mathrm{alg}}, \sigma) \subseteq (K, \sigma) \models \mathsf{ACFA}$) is definable in $\mathcal{L}_{\mathrm{ring}} \cup \{\overline{a}^n, \overline{b}^n | n \geqslant 2\}$.

Now observe that if $\overline{a}^n = (c_{n,1}, \ldots, c_{n,n}) = \overline{c}^n$, there is $\overline{b}^n \in \langle \overline{a}^n \rangle^{\mathrm{alg}} \cap F = \mathrm{acl}_{\mathsf{Psf}}(\overline{a})$ such that $(\overline{a}^n, \overline{b}^n)$ lie in C_n (for the choice of $\sigma|_{F_n}$).

If follows that very $e \in F^{\mathrm{eq}}$ has a weak code in $(F, (c_{n,i})_{\substack{n\geqslant 2\\ 1\leqslant i\leqslant n}})$, so the theory has WEI, so UEI by Corollary 7.13. □

Remark 7.20.

Proof of Lemma 7.14. We use nested induction. Outer induction on $|X|$. If $|X| = 0$ this is not very difficult. Assume that for X' with $|X'| < |X|$ the statement holds. Assume for contradiction that it fails for X. So there is Y finite such that $gX \cap Y \neq \varnothing$ for all $g \in G$.

Claim 7.14.1. *For any finite set $C \subseteq \Omega$ $|C| \leqslant |X|$ only finitely many translates of X by elements of g contain C. (We count translated versions of X, not the number of elements of G).*

Subproof. By induction on $|X| - |C|$: If $|X| = |C|$, $gX \supseteq C \implies gX = C$.

Now assume $|C| < |X|$ and the claim holds for all C' with $|C| < |C'| \leqslant |X|$.

By the outer induction assumption translating C if necessary, we may assume

$$C \cap Y = \varnothing. \tag{12}$$

By the inner induction assumption for each of the (finitely many) elements $y \in Y$ only finitely many translates of X contain $C \cup \{y\}$, as by (12) $|C \cup \{y\}| > |C|$.

Only finitely many translates of X contain C and intersect Y non-trivially.

On the other hand, by the assumption that X, Y is a counter example, every translate of X meets Y, proving the induction step, thus proving the claim. ■

Now let $C := \varnothing$ in the claim. It follows that X has only finitely many translates. But there is no finite orbit $\lightning$. □

Index

References

[Ax68] James Ax. "The Elementary Theory of Finite Fields". eng. In: *Annals of mathematics* 88.2 (1968), pp. 239–271. ISSN: 0003-486X.

[CDM92] Z. Chatzidakis, L. v.d. Dries, and A. Macintyre. "Definable sets over finite fields." In: *Journal für die reine und angewandte Mathematik* 427 (1992), pp. 107–136. URL: http://eudml.org/doc/153417.

[Cha05] Zoé Chatzidakis. *Notes on the model theory of finite and pseudofinite fields*. 2005. URL: https://www.math.ens.psl.eu/~chatzidakis/papiers/Madrid05.ps.

[Cha18] Zoé Chatzidakis. *Notes on the model theory of finite and pseudofinite fields*. 2018. URL: https://www.math.ens.psl.eu/~chatzidakis/papiers/Singapore.pdf.

[FJ23] Michael D Fried and Moshe Jarden. *Field Arithmetic*. eng. Fourth edition. Vol. 11. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge / A Series of Modern Surveys in Mathematics. Cham: Springer, 2023. ISBN: 3031280199.

[Lan73] Serge Lang. *Introduction to algebraic geometry*. 3rd printing, with corrections. Addison-Wesley, 1973.

[Poi00] Bruno Poizat. *A course in model theory*. eng. Universitext. New York, NY [u.a.]: Springer, 2000. ISBN: 0387986553.

[TZ12] Katrin Tent and Martin Ziegler. *A course in model theory*. eng. Lecture notes in logic 40. Ithaca, NY: ASL [u.a.], 2012. ISBN: 9780521763240.

[van14] Lou van den Dries. "Lectures on the model theory of valued fields". English (US). In: *Model Theory in Algebra, Analysis and Arithmetic*. Ed. by H Dugald Macpherson and Carlo Toffalori. Lecture Notes in Mathematics. Germany: Springer, 2014, pp. 55–157. ISBN: 9783642549359. DOI: 10.1007/978-3-642-54936-6_4.