Bounded statements in the theory of algebraically closed fields with distinguished automorphisms

By Dan Haran* and Moshe Jarden at Tel Aviv

Introduction and notation

Let $R$ be a countable integral domain and $\mathcal{L}(R)$ the first order language of the theory of rings augmented by constant symbols for the elements of $R$. For a positive integer $e$ we add $e$ unitary operation symbols $\Sigma_1, \ldots, \Sigma_e$, and denote the new language by $\mathcal{L}_e(R)$. One can form a countable set of axioms in $\mathcal{L}_e(R)$ such that a structure

$$(F, \sigma) = \langle F, +, \cdot, \sigma_1, \ldots, \sigma_e, \tilde{a}_R \rangle$$

is its model if and only if $\langle F, +, \cdot \rangle$ is an algebraically closed field containing the homomorphic image $\tilde{R} = \{ \tilde{a} | a \in R \}$ of $R$ and $\sigma_1, \ldots, \sigma_e$ are automorphisms of $F$ fixing the elements $\tilde{a}$ of $\tilde{R}$. We denote by $\mathcal{M}(R)$ the class of these structures. If $R = K$ is a field, which is the case of our prime interest, and $(F, \sigma) \in \mathcal{M}(K)$, then $F$ is an extension of $K$.

In addition to $\mathcal{L}_e(R)$ we shall consider formulae and sentences in other languages, whose interpretation is linked with the models of $\mathcal{M}(R)$:

1. The language $\mathcal{L}(R)$ may be used to speak about the fixed field $F(\sigma)$ of $(F, \sigma) \in \mathcal{M}(R)$. This has been done in [7] and [2].

But $F(\sigma)$ is definable in $(F, \sigma)$, in the language $\mathcal{L}_e(R)$, hence we may assign to every sentence $\theta$ in $\mathcal{L}(R)$ its relativization $\theta'$ to $F(\sigma)$. We denote

$$T' = \{ \theta' \in \mathcal{L}_e(R) | \theta \text{ is a sentence in } \mathcal{L}(R) \}.$$

2. Let $m \geq 1$ and let $(F, \sigma) \in \mathcal{M}(R)$. We put $M = F(\sigma)$ and define

$$M^{(m)} = \{ a \in F | [M(a) : M] \leq m \}.$$
A bounded formula $\varphi$ is a formula in $\mathcal{L}_e(R)$, on whose quantifiers appear as superscripts positive integers, so-called bounds. Thus in the prenex normal form $\varphi$ is written as

$$(Q_1^{m_1}X_1) \cdots (Q_n^{m_n}X_n) [\psi(X_1, \ldots, X_n, Y_1, \ldots, Y_k)],$$

where $Q_i$'s are $\exists$ or $\forall$ and $\psi$ is a quantifier free formula in $\mathcal{L}_e(R)$. As to its meaning: for $(F, \sigma) \in \mathcal{M}(R)$ and $\beta_1, \ldots, \beta_k \in F$ we write $(F, \sigma) \models \varphi(\beta_1, \ldots, \beta_k)$ iff for $M = F(\sigma)$

$$(Q_1 x_1 \in M^{(m_1)}) \cdots (Q_n x_n \in M^{(m_n)}) [F, \sigma] \models \psi(x, \beta).$$

(These formulas are definable in the language $\mathcal{L}_e(R)$, as we show later.)

3. In the next section we discuss two types of so-called Galois formulae and sentences and show how to identify them as bounded formulae and bounded sentences of $\mathcal{L}_e(K)$, where $K$ is a field.

We denote by $T(R)$ the theory of all bounded sentences of $\mathcal{L}_e(K)$ true in all models of $\mathcal{M}(R)$.

Let $K$ be a field. Let $\bar{K}$ (resp. $K_0$) be the algebraic (resp. separable) closure of $K$. The absolute Galois group $G(K) = \text{Aut}(\bar{K}/K) = \mathcal{G}(K,K)$ endowed with the Krull topology has a unique (normalized) Haar measure $\mu = \mu_K$; this may be extended to its direct product $G(K)^\mathfrak{c}$. For $A, B \subseteq G(K)^\mathfrak{c}$ we shall write $A \approx B$ if $\mu(A - B) = \mu(B - A) = 0$.

For a sentence $\theta$ in $\mathcal{L}_e(K)$ we define

$$A(\theta) = A_K(\theta) = \{\sigma = (\sigma_1, \ldots, \sigma_\mathfrak{c}) \in G(K)^\mathfrak{c} | (\bar{K}, \sigma) \models \theta\}.$$  

We denote by $\bar{T}(K)$ the theory of all sentences $\theta$ for which $A(\theta) \approx G(K)^\mathfrak{c}$ (i.e., $\mu(A(\theta)) = 1$). Then two sentences $\theta_1$, $\theta_2$ are equivalent modulo $\bar{T}(K)$ if and only if $A(\theta_1) \approx A(\theta_2)$.

Our aim in this note is to compare bounded sentences with a certain type of Galois sentences, a modification of the Galois sentences introduced in [2]. Instead of conjugacy domains of subgroups of the Galois groups we use here the conjugacy domains of $c$-tuples of elements of the Galois groups. We show that for an arbitrary field $K$, every Galois sentence is equivalent to a bounded sentence of $\mathcal{L}_e(K)$. The converse of this statement is our main result: Every bounded sentence of $\mathcal{L}_e(K)$ is equivalent modulo $T(K)$ to a Galois sentence.

Having this result we consider a countable Hilbertian field $K$ with elimination theory and use Chebotarev fields instead of the Frobenius fields of [2]. Then we proceed, in principle, with the Galois stratification procedure and achieve in this way a primitive recursive procedure for the theory of all bounded sentences in $\bar{T}(K)$.

In the second section we extend the transfer principle of [6] to bounded sentences. We consider the ring of integers $R$ of a global field $K$ and a bounded sentence $\theta$ of $\mathcal{L}_1(R)$. For every prime ideal $P \neq 0$ of $R$ we denote $F_P = R/P$ and let $\Phi_P$ be the Frobenius automorphism $\Phi_P(x) = x^{NP}$. It is shown that the Dirichlet density of

$$\#\{P | (F_P, \Phi_P) \models \theta\}$$

is equal to the Haar measure of the set $A_K(\theta)$.
It can be shown that the bounded sentences of $\mathcal{L}_Q^c(\Sigma)$ do not exhaust all the sentences of $\mathcal{L}_Q^c(\Sigma)$; there exist sentences in $\mathcal{L}_Q^c(\Sigma)$ which are not equivalent modulo $\mathcal{F}(\Sigma)$ to a bounded sentence. One may therefore ask about the decidability of the theory of all sentences in $\mathcal{L}_Q^c(\Sigma)$ which are true in $(\Sigma, F)$ for almost all $\sigma \in G(\Sigma)$. This is yet an open problem.

1. Galois stratifications

Let $R$ be a ring. We show some immediate connections between formulae in $\mathcal{L}_Q^c(R)$, $\mathcal{L}_Q^c(R)$ and bounded formulae.

**Lemma 1.1.** A bounded formula $\varphi = \varphi(Y_1, \ldots, Y_k)$ in $\mathcal{L}_Q^c(R)$ is equivalent modulo $T(R)$ to a formula $\tilde{\varphi} = \tilde{\varphi}(Y_1, \ldots, Y_k)$ of $\mathcal{L}_Q^c(R)$, i.e., for $(F, \sigma) \in \mathcal{F}(R)$ and $\beta_1, \ldots, \beta_k \in F$

$$(F, \sigma) \models \varphi(\beta_1, \ldots, \beta_k) \iff (F, \sigma) \models \tilde{\varphi}(\beta_1, \ldots, \beta_k).$$

*Proof.* Assume that $\varphi$ is $(\exists X) \left[ \psi(X, Y_1, \ldots, Y_k) \right]$, where $\psi(X, Y)$ is a formula of $\mathcal{L}_Q^c(R)$. Define $\tilde{\varphi}$ to be

$$(\exists X)(\exists X_1) \cdots (\exists X_m) \left[ \psi(X, Y_1, \ldots, Y_k) \land \left( \bigwedge_{j=1}^{m} \bigwedge_{i=1}^{e} \Sigma_i X_i = X_j \right) \right. \land \left. (X^m + X_1 X^{m-1} + \cdots + X_m = 0) \right].$$

Then $\tilde{\varphi}$ is obviously the desired formula. Thus the Lemma follows by induction on the structure of $\varphi$ (also observe that

$$(\forall^n X) \left[ \psi(X, Y) \right] \equiv \neg (\exists X) \left[ \neg \psi(X, Y) \right].$$

**Lemma 1.2.** To every formula $\varphi = \varphi(Y_1, \ldots, Y_k)$ in $\mathcal{L}_Q^c(R)$ there exists a bounded formula $\varphi = \varphi'(Y_1, \ldots, Y_k)$, equivalent to $\varphi$ in the following sense: for a couple $(F, \sigma) \in \mathcal{F}(R)$ and $\beta_1, \ldots, \beta_k \in F(\sigma)$ we have

$$(F, \sigma) \models \varphi'(\beta) \iff F(\sigma) \models \varphi(\beta).$$

*Proof.* By induction on the structure of $\varphi$. If $\varphi$ is atomic, put

$${\varphi}' = \varphi; \quad (\varphi_1 \lor \varphi_2)' = \varphi_1' \lor \varphi_2'; \quad (\neg \varphi)' = \neg {\varphi}';$$

and finally $(\exists X) \varphi)' = (\exists X) {\varphi}'.

Let $T' = \{ \theta' \in T(R) \mid \theta \text{ is a sentence in } \mathcal{L}_Q^c(R) \}$. The converse to Lemma 1.2 is not valid, as we shall see later.

We now turn to the main subject of this section: Galois stratification and sentences were originally introduced in [4] to solve diophantine problems modulo every prime; in [2] they appear — in the context of a decision procedure for Frobenius fields — in a form which is very similar to the one which we describe below.

We need some preliminary definitions: Let $K$ be a field. A non-empty constructible set $A$ over $K$ in the $n$-dimensional affine space $\mathcal{A}^n$ is a basic set, if $A = V - V(g)$, where $V$ is a $K$-irreducible closed set and $g \in K[x_1, \ldots, x_n]$. If $x = (x_1, \ldots, x_n)$ is a generic point of $V$ over $K$, we call it also a generic point of $A$; $K[A] = K[x, g(x)^{-1}]$, resp. $K(A) = K(x)$ are the co-ordinate ring, resp. the field of functions of $A$. A basic set $A$ is *normal*, if $K[A]$ is integrally closed.
Let \( C \subseteq \mathbb{A}^n \), \( A \subseteq \mathbb{A}^n \) be basic normal sets, and let \( \varphi : C \rightarrow A \) be an epimorphism defined over \( K \), defined by an \( m \)-tuple \((f_1, \ldots, f_m)\) of polynomials in \( K[X_1, \ldots, X_n] \). Now, if \( x \) is a generic point of \( C \), \( y = (f_1(x), \ldots, f_m(x)) \) is a generic point of \( A \) and \( \varphi \) induces a \( K \)-embedding \( K[A] \rightarrow K[C] \), which we regard for simplicity as a ring inclusion. If \( K[C] = K[A][u] \), with \( u \) integral over \( K[A] \), such that \( \text{disc}_{K[C]/K[A]}(u) \in K[A]^* \), we say that \( \varphi : C \rightarrow A \) is a basic set cover with a primitive element \( u \). [Note: \( K[C] \) is then the integral closure of \( K(A) \) in \( K(C) \), cf. [10], p. 264.] If \( K(C)/K(A) \) is a Galois extension, we call the cover \( C \) a Galois cover, and denote \( \mathcal{G}(C/A) = \mathcal{G}(K(C)/K(A)) \).

Assume that \( \varphi : C \rightarrow A \) is a Galois cover over \( K \). Let \((F, \sigma = (\sigma_1, \ldots, \sigma_n)) \in \mathcal{M}(K) \) and put \( M = F(\sigma_1, \ldots, \sigma_n) \). A point \( a \in A(M) \) defines a \( K \)-homomorphism \( \rho_0 : K[A] \rightarrow M \), which may be extended to \( \rho : K[C] \rightarrow \bar{M} \) (= the alg. closure of \( M \)). Then \( \rho K[C]/\rho K[A] \) is an extension of rings, its corresponding extension of quotient fields \( K(c)/K(a) \) is a finite Galois extension. Now \( \rho \) induces an isomorphism between \( \mathcal{G}(K(c)/K(a)) \) and the decomposition group of \( \varphi \) (cf. [8], Chpt. IX. Prop. 15). Its inverse, composed with the restriction to \( K(c) \) defines a continuous homomorphism

\[
\rho^* : G(M) \rightarrow \mathcal{G}(C/A)
\]

defined explicitly by the formula

\[
\rho^* (\rho \tau) = \rho (\rho \tau), \quad \tau \in G(M).
\]

We lift \( \rho^* \) in the obvious way to a map

\[
\rho^* : G(M)^c \rightarrow \mathcal{G}(C/A)^c.
\]

The extension \( \rho \) of \( \rho_0 \) is not unique; however, the set

(2) \[ \text{Ar}_{A,F,\sigma}(a) = \{ \rho^* \sigma \rho_1 : K[C] \rightarrow \bar{M} \text{ extends } \rho_0 \} = \{ (\rho^* \sigma) \tau : \tau \in \mathcal{G}(C/A) \} \]

is uniquely determined by \( a \). We call it the Artin symbol of \( a \) with respect to \((F, \sigma)\). The conjugation on \( \mathcal{G}(C/A)^c \) (by elements \( \tau \in \mathcal{G}(C/A) \)): \( (t_1, \ldots, t_n)^\tau = (\tau^{-1} t_1, \ldots, \tau^{-1} t_n, \tau) \)

defines an equivalence relation on \( \mathcal{G}(C/A)^c \); the Artin symbol is a conjugacy class.

A Galois stratification of the \( n \)-dimensional \((n \geq 0)\) affine space \( \mathbb{A}^n \) over \( K \) is a structure

(3) \[ \mathcal{A} = \langle \mathbb{A}^n, C_i \rightarrow A_i, \text{Con}(A_i) \rangle_{i \in I}, \]

where \( \mathbb{A}^n = \bigcup_{i \in I} A_i \) is a finite disjoint union of \( K \)-normal basic sets, and for every \( i \in I \)

\[ C_i \rightarrow A_i \]

is a Galois cover and \( \text{Con}(A_i) \subseteq \mathcal{G}(C_i/A_i)^c \) is a conjugacy domain (i.e., a subset closed under conjugation by elements of \( \mathcal{G}(C_i/A_i) \)).

We define an atomic Galois formula to be

(4) \[ \text{Ar}(X_1, \ldots, X_n) \subseteq \text{Con}(\mathcal{A}), \]

and for \( a = (a_1, \ldots, a_n) \in \mathbb{A}^n(M) \) we write

\[ (F, \sigma) \models \text{Ar}(a) \subseteq \text{Con}(\mathcal{A}) \]

if for the unique \( i \in I \), such that \( a \in A_i \),

\[ \text{Ar}_{A_i,F,\sigma}(a) \subseteq \text{Con}(A_i). \]

1) As in [2], Section 3 we suppress the reference to the cover \( C \) in the Artin symbol.
Using disjunctions, negations and quantification one may form general Galois sentences from these formulae.

Remark. Galois formulae may be seen as formulae of an appropriate first order language. In fact, this is the language, which has for every \( n \geq 0 \) and every Galois stratification \( \mathcal{A} \) of \( A^n \) over \( K \) one \( n \)-ary relational symbol (4), — and no other relational symbols (including equality) apart from these.

A structure \((F, \sigma) \in \mathcal{M}(K)\) may then be viewed as a relational structure for this language in the following way: its domain is \( M=F(\sigma) \), and the relation corresponding to the symbol (4) is defined above.

For a detailed treatment of Galois stratifications the reader is referred to [2], Section 3. Here we only comment on some minor changes.

First, one may with no loss assume that all the stratifications involved in a Galois sentence \( \theta \) are associated with the same affine space \( A^n \). Then using the concept of refinement (see [2], paragraph preceding Lemma 3.3) and of complementary stratification ([2], Lemma 3.5) one converts \( \theta \) to an equivalent (modulo \( T(K) \)) sentence \( \theta' \) in the following prenex normal form:

\[
(Q_{1}, X_{1}) \cdots (Q_{n}X_{n})[\forall (X_{1}, \ldots , X_{n}) \subseteq \text{Con}(\mathcal{A})],
\]

where \( Q_{1}, \ldots , Q_{n} \) are quantifiers and \( \mathcal{A} \) is a Galois stratification.

Next, note that in [2] we define \( \text{Con}(A) \) and \( \text{Ar}_{A,F,\sigma} (=\text{Ar}_{A,M} \text{ in [2]}) \) as conjugacy domains of subgroups of \( \mathcal{G}(C/A) \), while here we take the \( e \)-tuples of the generators of these subgroups. This is somewhat a stronger concept, however all of Section 3 (except Cor. 3.9) goes through, if the couple \( \langle M, \sigma \rangle \) has the Čebotarev property (which parallels to being a Frobenius field in [2]):

(\* ) Let \( C \rightarrow A \) be a Galois cover over \( M \), such that \( M(A)/M \) is a regular extension. Let \( N \) be the algebraic closure of \( M \) in \( M(C) \), and let \( \tau=(\tau_{1}, \ldots , \tau_{e}) \in \mathcal{G}(C/A)_{e} \). If \( \text{Res}_{N}\tau=\text{Res}_{M}\sigma \), then there exists an \( M \)-epimorphism \( \rho: M[C] \rightarrow M \), such that \( \rho M[A]=M \), and \( \rho^{\ast}(\sigma) = \tau \).

**Theorem 1.3.** (i) If \( M \) is a PAC field and \( G(M) \) admits a set of \( e \) free generators \( \sigma_{1}, \ldots , \sigma_{e} \), then the couple \( \langle M, \sigma \rangle \) has the Čebotarev property.

(ii) Let \( K \) be a countable Hilbertian field. Then for almost all \( \sigma \in G(K)^{e} \) the couple \( \langle K(\sigma), \sigma \rangle \) has the Čebotarev property.

**Proof.** See [2], Cor. 1.4 (and the Remark following it) and Cor. 1.6.

**Lemma 1.4.** Every Galois formula \( \theta(Y_{1}, \ldots , Y_{k}) \) is equivalent to a bounded formula \( \hat{\theta}(Y_{1}, \ldots , Y_{k}) \) of \( \mathcal{L}_{2}(K) \) in the following sense: for every \( (F, \sigma) \in \mathcal{M}(K) \) and \( \beta_{1}, \ldots , \beta_{k} \in F(\sigma) \)

\[
(F, \sigma) \models \theta(\beta_{1}, \ldots , \beta_{k}) \iff (F, \sigma) \models \hat{\theta}(\beta_{1}, \ldots , \beta_{k}).
\]

**Proof.** It suffices to prove the Lemma for an atomic formula. Indeed, in the general case replace the atomic components of \( \theta \) by appropriate equivalent bounded formulae, and the quantifiers \( \exists, \forall \) by \( \exists^{1}, \forall^{1} \); the resulting formula clearly satisfies the requirements of this Lemma.
Let therefore $\mathcal{A} = \langle A_k, C_i \rightarrow A_i, \text{Con}(A_i) \rangle_{i \in I}$ be the underlying stratification for the atomic formula $\theta(Y_1, \ldots, Y_k)$. For every $j \in I$ and $z = (\tau_1, \ldots, \tau_e) \in \text{Con}(A_j)$ let $\mathcal{A}_{j, z} = \langle A_k, C_i \rightarrow A_i, \text{Con}_{j, z}(A_i) \rangle_{i \in I}$ be a Galois stratification of $A_k$, where

$$\text{Con}_{j, z}(A_i) = \begin{cases} \{ x \mid x \in \mathcal{G}(C_j/A_j) \} & j = i, \\ \emptyset & j \neq i. \end{cases}$$

Also let $\theta_{j, z}$ be the corresponding Galois formula; then, from definitions, $\theta$ is equivalent modulo $T(K)$ to $\bigvee_{j \in I} \bigvee_{z \in \text{Con}(A_j)} \theta_{j, z}$. Hence it suffices to prove the Lemma for a formula $\theta = \theta_{j, z}(Y_1, \ldots, Y_k)$.

In that case $C_j = V(f_1, \ldots, f_m; g) - V(g)$, where $f_1, \ldots, f_m, g \in K[X_1, \ldots, X_m]$, is a normal subset of an affine space $A^m$; there are also $h_1, \ldots, h_k \in K[X_1, \ldots, X_m]$, such that $\phi_j(x) = (h_1(x), \ldots, h_k(x))$ for every $x \in C_j$. Let $x$ be a generic point of $C_j$ over $K$; then $K[C_j] = K[x, g(x)^{-1}]$ and there is a primitive element $z \in K(C_j)$ for the cover $C_j \rightarrow A_j$. Let $p_0, p_1, \ldots, p_e \in K[X_1, \ldots, X_m, U]$ be such that

$$z = p_0(x, g(x)^{-1}), \quad \tau_i z = p_i(x, g(x)^{-1}), \quad i = 1, \ldots, e.$$ 

Finally define $\hat{\theta}$ to be

$$(\exists^d X_1 \cdots \exists^d X_m) (\exists^d U) \left[ \bigwedge_{i=1}^m f_i(X) = 0 \land g(X) U = 1 \land \bigwedge_{i=1}^k h_i(X) = Y_i \right. \land \left. \bigwedge_{i=1}^e \Sigma t p_0(X, U) = p_i(X, U) \right],$$

where $d = [K(C) : K(A)]$.

For $(F, \sigma) \in \mathcal{M}(K)$ and $\beta_1, \ldots, \beta_k \in M = F(\sigma)$ we have $(F, \sigma) \models \hat{\theta}(\beta)$ iff there is a $K$-homomorphism $\rho: K[C_j] \rightarrow F$, such that $\text{Res}_{K[A_j], \rho}$ defines $\beta$ (in particular $\rho K[A_j] \subseteq M$) and $\sigma_i(\rho z) = \rho(\tau_i z)$ for $i = 1, \ldots, e$. This is equivalent to $Ar_{A_j, F, \sigma}(\beta) \subseteq \text{Con}_{j, z}(A_j)$. Thus $\hat{\theta}$ is equivalent to $\theta$.

Lemma 1.4 tells us, that our Galois formulae may be identified as formulae in the language $\mathcal{L}_e(K)$.

**Theorem 1.5.** Every bounded sentence $\omega$ of $\mathcal{L}_e(K)$ is equivalent modulo $T(K)$ to a Galois sentence $\theta$ (i.e., for every $(F, \sigma) \in \mathcal{M}(K)$ we have $(F, \sigma) \models \omega \iff (F, \sigma) \models \theta$).

To prove this theorem we use a new concept which generalizes Galois stratifications:

Let $C \xrightarrow{\phi} B \xrightarrow{\psi} A$ be a pair of $K$-morphisms of $K$-normal basis sets. We call it a **restricted Galois cover**, if $C \xrightarrow{\psi \circ \phi} A$ is a Galois cover.

Let $(F, \sigma) \in \mathcal{M}(K)$, $M = F(\sigma)$. Denote

$$B(M, \psi) = \{ b \in B(F) \mid \psi(b) \in A(M) \}.$$
A point \( b \in B(M, \psi) \) defines a \( K \)-map \( \rho_0 : K[B] \to F \) such that \( \rho_0 K[A] \subseteq M \). Since \( K[C] \) is integral over \( K[B] \), \( \rho_0 \) can be extended to \( \rho : K[C] \to F \), which induces a group homomorphism

\[
\rho^* : G(M)^e \to \mathcal{G}(C/A)^e
\]

(as explained earlier for Galois covers). One easily verifies that

\[
\{ \rho^* \sigma | \rho_1 : K[C] \to F \text{ extends } \rho_0 \} = \{ (\rho^* \sigma|^t) | t \in \mathcal{G}(C/B) \}
\]

and we call this restricted conjugacy class (= an equivalence class with respect to the relation of conjugation by elements of \( \mathcal{G}(C/B) \)) of \( \mathcal{G}(C/A)^e \) the Artin symbol of \( b \), denoted by \( \text{Ar}_{B, F, \sigma}(b) \).

Let \( B^i \xrightarrow{\psi^i} A_i, j = 1, \ldots, n \) be \( K \)-isomorphisms of \( K \)-constructible sets; denote \( B = B^1 \times \cdots \times B^n, A = A^1 \times \cdots \times A^n \) and define \( \psi : B \to A \) by

\[
\psi(b_1, \ldots, b_n) = (\psi^1(b_1), \ldots, \psi^n(b_n))
\]

A restricted Galois stratification of the set \( B \) is a structure

\[
\mathcal{A} = \langle B, C_i \xrightarrow{\psi_i} B_i \xrightarrow{\psi_i} A_i, \text{Con} (B_i) \rangle_{i \in I},
\]

where \( B = \bigcup_{i \in I} B_i \) is a finite disjoint union of \( K \)-normal basic sets, and for every \( i \in I \)

\[
C_i \xrightarrow{\psi_i} B_i \xrightarrow{\psi_i} A_i
\]

is a restricted Galois cover with \( \psi_i = \text{Res}_{B_i} \psi_i \), and \( \text{Con} (B_i) \) is a restricted conjugacy domain (= a union of restricted conjugacy classes) of \( \mathcal{G}(C_i/A_i)^e \) with respect to \( B_i \). (It follows that \( A = \bigcup_{i \in I} A_i \).)

An atomic restricted Galois formula over \( B \) is an expression

\[
[F, \sigma] \in \mathcal{M}(K) \text{ and } \psi = (b_1, \ldots, b_n) \in B(M, \psi), \text{ where } M = F(\sigma), \text{ we write}
\]

\[
(F, \sigma) \models [\text{Ar} (b) \subseteq \text{Con} (\mathcal{A})] \iff \text{Ar}_{B, F, \sigma}(b) \subseteq \text{Con} (B_i)
\]

for the unique \( i \in I \) such that \( b \in B_i \).

From these formulae one forms general restricted Galois formulae over \( B \) by negations, disjunctions, conjunctions and quantifications. However, it is important to notice that there are \( n \) distinct types of variables, according to their location in atomic formulae, and a variable of type \( i \) (\( 1 \leq i \leq n \)) may appear in atomic components at \( i \)-th place only (i.e. instead of \( X_i \) in (8)). The interpretation of such formulae in \( (F, \sigma) \in \mathcal{M}(K) \) is obvious: a variable of type \( i \) is quantified in \( B(F(\sigma), \psi^i) \).

Before going on we want to comment on the process of refinement of restricted Galois stratifications (see also [2], a remark preceding Lemma 3.3). Assume that for some \( i \in I \) in (7) \( B_i = \bigcup_{k \in I'} B_k \) and that there are restricted Galois covers

\[
C_k \xrightarrow{\psi_k} B_k \xrightarrow{\psi_k} A_k, \quad k \in I',
\]

where \( \psi_k = \text{Res}_{B_k} \psi_i \). For every \( k \in I' \) the inclusion \( B_k \subseteq B_i \) defines a \( K \)-homomorphism \( \mu_{0, k} : K[B_i] \to K[B_k] \), which may be extended to \( \mu_k : K[C_i] \to K(B_k) \). Assume that \( \mu_k K[C_i] \subseteq K[C_k] \). Then \( \mu_k \) induces a group homomorphism \( \mu_k^* : \mathcal{G}(C_i/A_i)^e \to \mathcal{G}(C_k/A_k)^e \).
This may depend on our choice of the extension $\mu_k$, however

$$\text{Con}(B'_k) = \bigcup_{i \in \mathcal{C}_{i}(\mathcal{H}_k)} [\mu_k^{e-1} \text{Con}(B_i')]$$

depends on $\mu_{0,k}$ only. Now if $(F, \sigma) \in \mathcal{H}(K)$, $M = F(\sigma)$ and $b \in B'_k(M, \psi)$, then

$$\text{Ar}_{B_k, F, \sigma}(b) \subseteq \text{Con}(B_i) \iff \text{Ar}_{B_k, F, \sigma}(b) \subseteq \text{Con}(B'_k).$$

Therefore the refinement $\mathcal{B}'$ of $\mathcal{B}$ obtained by replacing $\langle C_i \to B_i \to A_i, \text{Con}(B_i) \rangle$ in (7) by $\langle C'_i \to B'_i \to A'_i, \text{Con}(B'_i) \rangle_{i \in I}$, is equivalent to $\mathcal{B}$ in the sense indicated above.

Now, if $B'_i \subseteq B_i$ is a $K$-basic set, we can find — by subtracting hypersurfaces from the sets under consideration — two $K$-normal basic open subset $B'_i \subseteq B_i$ and $C'_i \subseteq C_i$, such that $A'' = \psi(B'_i)$ is also a $K$-normal basic set and $C'_i \xrightarrow{\text{Res } \psi_i} B'_i \xrightarrow{\text{Res } \psi_i} A''$ is a restricted Galois cover. Moreover, if $L \supseteq K(C'_i) \supseteq K(A''_i)$ is a finite Galois tower of field extension, we can find — again, replacing $C'_i$, $B'_i$, $A''_i$ by their open subsets — a restricted Galois cover $D''_i \xrightarrow{\psi''_i} B'_i \xrightarrow{\text{Res } \psi_i} A''_i$, such that $K(D''_i) = L$ and $K[D''_i] \subseteq K[C'_i]$.

Thus, using the stratification Lemma (see [2], Lemma 2.13) we may replace a given restricted Galois stratification over $B$ by a refinement (7), where the sets $B_i$ of $\mathcal{B}$, which are obtained by partition of the corresponding sets in the original stratification, may be chosen to have certain additional desirable properties and the fields of functions $K(C'_i)$ of their covers $C'_i$ may contain certain given extensions of $K(A''_i)$. The new formula (3) obtained in this way is equivalent to the formula associated with the original stratification, for all structures in $\mathcal{M}(K)$.

As an application consider two restricted Galois stratifications $\mathcal{B}'$, $\mathcal{B}''$ of a set $B$. Using their refinements we may assume with no loss that they have the same restricted Galois covers $\{C_i \to B_i \to A_i\}_{i \in I}$ and hence differ only in the restricted conjugacy domains: $\text{Con}'(B_i)$ for $\mathcal{B}'$ and $\text{Con}''(B_i)$ for $\mathcal{B}''$, $i \in I$. It is then clear, that the formula

$$[\text{Ar}(X) \subseteq \text{Con}(B')] \lor [\text{Ar}(X) \subseteq \text{Con}(B'')]$$

is equivalent modulo $T(K)$ to a formula (8) associated with (7), where

$$\text{Con}(B'_i) = \text{Con}'(B_i) \cup \text{Con}''(B_i), \quad i \in I.$$

Moreover, the formula $\neg [\text{Ar}(X) \subseteq \text{Con}(\mathcal{B})]$, associated with (7), is equivalent modulo $T(K)$ to an atomic formula $[\text{Ar}(X) \subseteq \text{Con}(\mathcal{B}')])$, where $\mathcal{B}'$ is the complementary stratification (cf. [2], Lemma 3.5):

$$\mathcal{B}' = \langle B, C_i \xrightarrow{\psi_i} B_i \xrightarrow{\psi_i} A_i, \text{Con}''(B_i) \rangle_{i \in I}$$

with $\text{Con}'(B_i) = \mathcal{B}(C_i/A_i)^c - \text{Con}(B_i), i \in I$.

Thus a restricted Galois sentence over $B$ is equivalent modulo the theory of all restricted Galois sentences over $B$, which are true in all structures in $\mathcal{H}(K)$, to a sentence of the form

$$\langle Q_1 X_1 \cdots (Q_n X_n) [\text{Ar}(X_1, \ldots, X_n) \subseteq \text{Con}(B)],$$

after a possible permutation of the components $B^1, \ldots, B^n$ of the set $B$. 

Remark 1.6. If \( \psi = \text{id} \), (10) is equivalent to a Galois sentence. Indeed, for every \( 1 \leq j \leq n \), \( B^j \) is in some affine space \( A^{m_j} \), hence \( B \subseteq A \equiv A^{m_1} \times \cdots \times A^{m_n} \). We may represent \( A - B \) as a disjoint union \( \bigcup_{i \in I} B_i \) of \( K \)-normal sets and for \( i \in I \) define \( A_i = B_i, \phi_i = \text{id} \), \( \text{Con} (B_i) = \emptyset \). One may in an obvious way identify \( A \) with \( A^m \), where \( m = m_1 + \cdots + m_n \).

Then the Galois sentence

\[
(Q_1 Y_{11}) \cdots (Q_1 Y_{1m_1}) \cdots (Q_n Y_{nm_n}) \left[ \text{Ar} (Y_{11}, \ldots, Y_{1m_1}, \ldots, Y_{n1}, \ldots, Y_{nm_n}) \subseteq \text{Con} (\mathcal{B}) \right],
\]

where

\[
\mathcal{B}^r = \left( A^m, A_i \xrightarrow{\psi_i} B_i, \text{Con} (B_i) \right)_{i \in \hat{I}, r \in I},
\]

is obviously equivalent to (10).

Lemma 1.7. Every restricted Galois sentence \( \theta \) is equivalent to a Galois sentence \( \hat{\theta} \) in the following sense: \( (F, \sigma) \models \hat{\theta} \Leftrightarrow (F, \sigma) \models \theta \), for every \( (F, \sigma) \in \mathcal{M} (K) \).

Proof. With no loss we may assume that \( \theta \) is (10) and \( \mathcal{B} \) given by (7).

Let \( 1 \leq r \leq n \) and put \( \hat{B} = B^r \times \cdots \times B^{r-1} \times A^r \times B^{r+1} \times \cdots \times B^n \). Define epimorphisms \( \hat{\psi} : \hat{B} \to A \) by \( \hat{\psi} = \psi^1 \times \cdots \times \psi^{r-1} \times \text{id} \times \psi^{r+1} \times \cdots \times \psi^n \) and \( \hat{\phi} : B \to \hat{B} \) by

\[
\hat{\phi} = \text{id} \times \cdots \times \text{id} \times \psi^r \times \text{id} \times \cdots \times \text{id}.
\]

(Thus \( \hat{\psi} \circ \hat{\phi} = \psi \).)

By the refinement process described above we may assume that there is a partition \( \hat{B} = \bigcup_{k \in \hat{I}} \hat{B}_k \) into \( K \)-normal basic sets \( \hat{B}_k \) such that for every \( i \in I \) there is a unique \( k \in \hat{I} \) with \( \hat{\phi} (B_i) = \hat{B}_k \). For every \( k \in \hat{I} \) pick up an \( i \in I \) such that \( \hat{\phi} (B_i) = \hat{B}_k \); then there is a restricted Galois cover \( \hat{C}_k \xrightarrow{\hat{\psi}_k} \hat{B}_k \xrightarrow{\text{Res} \hat{\psi}} \hat{A}_k \), where \( \hat{C}_k = C_i, \hat{A}_k = A_i = \hat{\psi} (\hat{B}_k) \) and \( \hat{\phi}_k = (\text{Res} \hat{\psi} \hat{\phi}) \circ \phi_i \). By a further refinement we may even assume, that for every \( i' \in I \) with \( \hat{\phi} (B_{i'}) = \hat{B}_k \) we have \( C_{i'} = C_i = \hat{C}_k \), hence this cover is indeed well-defined (i.e. independent of the choice of \( i \in I \)).

Suppose that we have defined for every \( k \in \hat{I} \) a restricted conjugacy domain \( \text{Con} (\hat{B}_k) \) in \( \mathcal{B} (\hat{C}_k/\hat{A}_k)^r \). Then we obtain a restricted Galois stratification of \( \hat{B} \)

\[
(11) \quad \hat{\mathcal{B}} = \left( \hat{B}, \hat{C}_k \xrightarrow{\hat{\psi}_k} \hat{B}_k \xrightarrow{\text{Res} \hat{\psi}} \hat{A}_k, \text{Con} (\hat{B}_k) \right)_{k \in \hat{I}}
\]

and a corresponding sentence

\[
(12) \quad (Q_1 X_1) \cdots (Q_n X_n) \left[ \text{Ar} (X_1, \ldots, X_n) \subseteq \text{Con} (\hat{\mathcal{B}}) \right].
\]

We claim that there is a way to define \( \{ \text{Con} (\hat{B}_k) \}_{k \in \hat{I}} \) such that the following two formulae are equivalent

\[
(13) \quad (Q_r X_r) \left[ \text{Ar} (X_1, \ldots, X_n) \subseteq \text{Con} (\hat{\mathcal{B}}) \right]
\]

\[
(14) \quad (Q_r X_r) \left[ \text{Ar} (X_1, \ldots, X_n) \subseteq \text{Con} (\hat{\mathcal{B}}) \right],
\]

hence also (10) will be equivalent to (12).
However, it suffices to take \( Q_r = \exists \). Indeed, if the claim has been proved in this case, then

\[
(\forall X_i) [\text{Ar}(X) \subseteq \text{Con}(\mathcal{B})] \equiv (\exists X_i) [\text{Ar}(X) \subseteq \text{Con}(\mathcal{B}')] \\
\equiv (\exists X_i) [\text{Ar}(X) \subseteq \text{Con}(\mathcal{B})'] \equiv (\forall X_i) [\text{Ar}(X) \subseteq \text{Con}(\mathcal{B})'],
\]

where \(-^c\) denotes complementary stratifications defined in (5).

Let therefore \( Q_r = \exists \). Define for every \( k \in \hat{I} \)

\[
\text{Con}(\hat{B}_k) = \bigcup_{i=1}^{\hat{I}} \bigcup_{i \in \Phi(k, \hat{B}_k)} \text{Con}(\hat{B}_k)^i.
\]

Let \((F, \sigma) \in \mathcal{M}(K), M = F(\sigma)\) and let \( h_j \in B^i(M, \psi^i), j = 1, \ldots, r-1, r+1, \ldots, n. \) Then it is enough to show that the following two statements are equivalent:

\[
(16) \quad (F, \sigma) \models (\exists X_i) [\text{Ar}(b_1, \ldots, b_{r-1}, X_r, b_{r+1}, \ldots, b_n) \subseteq \text{Con}(\mathcal{B})],
\]

\[
(17) \quad (F, \sigma) \models (\exists X_i) [\text{Ar}(b_1, \ldots, b_{r-1}, X_r, b_{r+1}, \ldots, b_n) \subseteq \text{Con}(\mathcal{B}')].
\]

Now, if (16) holds, there is a \( b_i \in B^i(M, \psi^i) \) such that \( b_i = (b_1, \ldots, b_{r-1}, b_r, b_{r+1}, \ldots, b_n) \in \hat{B}_i \) for some \( i \in \hat{I} \) and \( \text{Ar}_{\hat{B}_i, F, \sigma}(b_i) \subseteq \text{Con}(\hat{B}_i) \). Then \( b_i' = \psi^i(b_i) \in \text{Ar}(M, i, id) \) and

\[ b' = (b_1, \ldots, b_{r-1}, b_r', b_{r+1}, \ldots, b_n) \in \Phi(b_i) = \hat{B}_k \]

for a unique \( k \in \hat{I} \). Since \( \text{Ar}_{\hat{B}_k, F, \sigma}(b') \subseteq \text{Ar}_{\hat{B}_k, F, \sigma}(b_i) \), and since \( \text{Ar}_{\hat{B}_k, F, \sigma}(b') \) is a restricted conjugacy class of \( \mathcal{G}() \) with respect to \( \hat{B}_k \), we have that

\[ \text{Ar}_{\hat{B}_k, F, \sigma}(b') - \bigcup_{i \in \Phi(k, \hat{B}_k)} \text{Ar}_{\hat{B}_k, F, \sigma}(b_i)^i, \]

hence (17) follows.

If (17) is true, there is a \( b_i' \in \text{Ar}(M, i, id) \) such that \( b_i' = (b_1, \ldots, b_{r-1}, b_r', b_{r+1}, \ldots, b_n) \in \hat{B}_k \) for some \( k \in \hat{I} \) and \( \text{Ar}_{\hat{B}_k, F, \sigma}(b') \subseteq \text{Con}(\hat{B}_k) \). Thus the \( K\)-map \( \rho: K[\hat{B}_k] \to K[b'] \) may be extended to \( \rho': K[G] \to K[b'] \) and \( \rho \circ \sigma \in \text{Con}(\hat{B}_i) \) for some \( i \in \hat{I} \) with \( \Phi(b_i) = \hat{B}_k \) and some \( i \in \Phi(k, \hat{B}_k) \). Without restriction \( \tau = id \), otherwise replace \( \rho \) by \( \rho \circ \tau \). Now \( \text{Res}_{K[i, \hat{B}_i]} \rho \) defines a point \( b \in B_i \) with \( \text{Ar}_{\hat{B}_i, F, \sigma}(b) \subseteq \text{Con}(\hat{B}_i) \). Since \( \hat{B}(b) = b' \), we have

\[ b = (b_1, \ldots, b_{r-1}, b_r, b_{r+1}, \ldots, b_n) \]

where \( \psi^i(b_r) = b_r' \in \text{Ar}(M, \psi^i) \), hence \( b_i' \in B^i(M, \psi^i) \). Thus (16) follows.

This ends the proof of this Lemma, by induction and by Remark 1.6. \( \square \)

Let \( m \) be a positive integer and let \( \psi: \mathcal{A}^m \to \mathcal{A}^m \) be defined by \( \psi(z) = (s_1(z), \ldots, s_m(z)) \), where \( s_1, \ldots, s_m \) are the elementary symmetric polynomials in \( m \) variables. Then for every \( z = (z_1, \ldots, z_m) \in \mathcal{A}^m \) the extension \( K(z)/K(\psi(z)) \) is normal, its automorphisms permute \( z_1, \ldots, z_m \) and \( [K(\psi(z), z_1): K(\psi(z))] \leq m. \) This extension need not be separable; however, it is easy to find a \( \mathcal{K}\)-constructible set \( B \subseteq \mathcal{A}^m \), large enough for our purposes, such that \( K(z)/K(\psi(z)) \) is Galois for every \( z \in B \). For example

\[ B = \bigcup_{r=0}^m \left[ \text{V}(Z_{r+1}, \ldots, Z_m) - \text{V} \left( \prod_{a=1}^r (Z_a - Z_{a+b}) \right) \right]. \]

The image \( A = \psi(B) \) of \( B \) is a \( \mathcal{K}\)-constructible subset of \( \mathcal{A}^m \).
Thus we obtain (in a notation suited for a later application) the following

**Lemma 1.8.** Let $m_j$ be a positive integer. There are $K$-constructible sets $B^j, A^j \subseteq \mathcal{A}^{(m_j)}$ and a $K$-epimorphism $B^j \xrightarrow{\psi^j} A^j$ such that for every $z = (z_1, \ldots, z_{m_j}) \in B^j$ and every $K \subseteq M$:

(a) $K(z)/K(\psi^j(z))$ is a Galois extension and $[K(\psi^j(z), z_1): K(\psi^j(z))] \leq m_j$;

(b) every $\tau \in \mathcal{G}(K(z)/K(\psi^j(z))$ permutes $z_1, \ldots, z_{m_j}$;

(c) if $z \in B^j(M, \psi^j)$, then $z_1 \in M^{(m_1)}$;

(d) if $z_1 \in M^{(m_1)}$, there is some $(z_1, \ldots, z_{m_j}) \in B^j(M, \psi^j)$ with $z_1 = z_1'$, (E.g., let $z_1 = z_1', \ldots, z_r$ be all the distinct conjugates of $z_1'$ over $M$ and $z_{r+1} = \cdots = z_{m_j} = 0$.)

**Proof of Theorem 1.5.** By adding new, suitably quantified variables we may assume that the bounded sentence $\omega$ is constructed by disjunctions, conjunctions, negations and bounded quantifications from formulae of the form

(i) $f(X_1, \ldots, X_n) = 0$

where $f \in K[X_1, \ldots, X_n]$, and

(ii) $\Sigma_i X_j = X_j$.

Indeed, e.g. instead of $\Sigma_2 Y_1 = Y_2$ we write $(\exists^m Y_1) [\Sigma_1 X_1 = Y_1 \land \Sigma_2 Y_1 = Y_2]$, where $m$ is the bound on the quantifier of $X_1$. Instead of $\Sigma_i \psi_i(X_1, \ldots, X_n)$ we insert

$$(\exists^{m_1} Y_1) (\exists^{m_2} Y_2) [Y_1 - f_1(X) = 0 \land Y_2 - f_2(X) = 0 \land (\Sigma_i Y_1 = Y_2)],$$

where the bound $m_1$ (resp. $m_2$) is determined from the bounds on quantifiers of $X_1, \ldots, X_n$ and the polynomial $f_1$ (resp. $f_2$). (Note that for $\alpha_1 \in M^{(m_1)}, \alpha_2 \in M^{(m_2)}$ we have $\alpha_1 + \alpha_2, c\alpha_1, \alpha_2 \in M^{(m_1+m_2)}$ for every $c \in M$; thus by induction on the structure of $f_i$ one can find $m_1 \in \mathbb{N}$ such that for $K \subseteq M$

$$\alpha_j \in M^{(m_j)}, \quad j = 1, \ldots, n \Rightarrow f_1(\alpha_1, \ldots, \alpha_n) \in M^{(m_j)}).$$

Therefore $\omega$ may be written in the prenex normal form as

$$(Q_1^{m_1} X_1) \cdots (Q_n^{m_n} X_n) \bigvee_{\lambda \in \Lambda} [(X_1, \ldots, X_n) \in D_\lambda \land \omega_\lambda(X_1, \ldots, X_n)]$$

where $Q_1, \ldots, Q_n$ are $\exists$ or $\forall$ and $D_\lambda \subseteq \mathcal{A}^n$ for each $\lambda \in \Lambda$ is a $K$-constructible set and $\omega_\lambda$ is a conjunction of formulae of type (ii) and negations of such formulae. By considering intersections of $D_\lambda$'s and their complements we may assume that the $D_\lambda$'s are disjoint. Moreover, with no loss $\bigcup_{\lambda \in \Lambda} D_\lambda = \mathcal{A}^n$ (otherwise add index $\lambda'$ to $\Lambda$ for which $D_{\lambda'} = \mathcal{A}^n - \bigcup_{\lambda \in \Lambda} D_\lambda$ and $\omega_{\lambda'}$: is $\Sigma_1 X_1 = X_1 \land \Sigma_1 X_1 \neq X_1$).

For every $1 \leq j \leq n$ let $\psi^j: B^j \to A^j$ satisfy the conditions of Lemma 1.8. Let $B = B^1 \times \cdots \times B^n$, $A = A^1 \times \cdots \times A^n$, $\psi = \psi^1 \times \cdots \times \psi^n$. 

Consider the sets

\[ D_{\lambda} = \{(z_{11}, \ldots, z_{1m_1}), \ldots, (z_{n1}, \ldots, z_{nm_n}) \in B | (z_{11}, z_{21}, \ldots, z_{n1}) \in D_\lambda \} \]

for every \( \lambda \in \Lambda \). Their intersections with sets \( V(Z_{j_1k_1} - Z_{j_2k_2}) \) and \( V(Z_{j_1k_1} - Z_{j_2k_2}) \) define a K-constructible stratification of \( B \). By the stratification Lemma ([2], Lemma 2.13) we can find a refinement \( B = \bigcup_{i \in I} B_i \) of this stratification (i.e., for every \( i \in I \) there is a unique \( \lambda \in \Lambda \) with \( B_i \subseteq D_{\lambda} \)) and for every \( 1 \leq j_1, j_2 \leq n, 1 \leq k_1 \leq m_{j_1}, 1 \leq k_2 \leq m_{j_2} \), either \( B_i \subseteq V(Z_{j_1k_1} - Z_{j_2k_2}) \) or \( B_i \cap V(Z_{j_1k_1} - Z_{j_2k_2}) = \emptyset \) such that for every \( i \in I \)

\[ B_i \xrightarrow{\text{Res}_{B_i} \psi} A_i = \psi(B_i) \]

is a Galois cover. If \( K(B_i) = K(z) \), where \( z = ((z_{11}, \ldots, z_{1m_1}), \ldots, (z_{n1}, \ldots, z_{nm_n})) \) is a generic point of \( B_i \), denote \( \tilde{z} = (z_{11}, z_{21}, \ldots, z_{n1}) \) and let

\[(19) \quad \text{Con}(B_i) = \{ \tau \in \mathcal{G}(B_i/A_i)^\tau | (K(B_i), \tau) = \omega_{\lambda}(\tilde{z}) \text{ for the unique } \lambda \text{ such that } B_i \subseteq D_{\lambda} \}. \]

(More rigorously we should write instead of \((K(B_i), \tau)\) perhaps \((\text{\hat{K}(B_i)}, \text{\hat{\tau}})\), where \( \text{\hat{\tau}} \in (\text{Aut}(\text{\hat{K}(B_i)})^\tau \) is some extension of \( \tau \).) Then

\[ (20) \quad \mathcal{B} = \langle B, B_i \xrightarrow{\text{id}} B_i \xrightarrow{\text{Res}_{B_i} \psi} A_i, \text{Con}(B_i) \rangle_{i \in I} \]

is a restricted Galois stratification of \( B \). By Lemma 1.7 to end this proof it suffices to show that the corresponding sentence (10) is equivalent to (18).

Let, therefore, \( (F, \sigma) \in \mathcal{M}(K), M = F(\sigma) \). Let \( 0 \leq r \leq n \) and

\[ b_j = (b_{j1}, \ldots, b_{jm_j}) \in B^j(M, \psi^j), \quad j = 1, \ldots, r. \]

Claim. The following two statements are equivalent:

\[ (F, \sigma) \models (Q_{r+1}^m X_{r+1}) \cdots (Q_n^m X_n) \bigcup_{\lambda \in \Lambda} \big( (b_{11}, \ldots, b_{1m_1}, X_{r+1}, \ldots, X_n) \in D_{\lambda} \land \omega_{\lambda}(b_{11}, \ldots, b_{1m_1}, X_{r+1}, \ldots, X_n) \big), \]

(21)

\[ (F, \sigma) \models (Q_{r+1}^m X_{r+1}) \cdots (Q_n^m X_n) \big[ \text{Ar}(b_{11}, \ldots, b_{r1}, X_{r+1}, \ldots, X_n) \subseteq \text{Con}(\mathcal{B}) \big]. \]

(22)

Assume first \( r = n \). There is a unique \( i \in I \) such that \( b = (b_1, \ldots, b_n) \in B_i \) and a unique \( \lambda \in \Lambda \) such that \( B_i \subseteq D_{\lambda} \), hence \( (b_1, \ldots, b_n) \in D_{\lambda} \). The point \( b \) defines a K-homomorphism \( \rho : K[B_i] \to K[b] \subseteq \bar{M} \), and \( \rho K[A_i] \subseteq M \). Let \( \tau = \rho^* \sigma \in \mathcal{G}(B_i/A_i)^\tau \). Then (21) is equivalent to

\[ (21') \quad (F, \sigma) = \omega_{\lambda}(b_{11}, \ldots, b_{1m_1}), \]

and (22) is equivalent to \( \text{Ar}_{B_i, F, \sigma}(b) \subseteq \text{Con}(B_i) \), hence to

\[ (22') \quad (K(B_i), \tau) = \omega_{\lambda}(z_{11}, \ldots, z_{n1}), \]

by the definition (19).
So with no loss we may assume that \( \omega_k \) is \( \Sigma_i X_j = X_j' \). By Lemma 1.8 (b) there is \( 1 \leq k \leq m \) such that \( \tau_i(z_{jk}) = z_{jk} \); hence \( \sigma_i(b_{jk}) = b_{jk} \). But since \( B_i \subseteq V(Z_j) = Z_j' \) or \( B_i \cap V(Z_{jk} - Z_j') = \emptyset \), we have: \( z_{jk} = z_{j'k} \iff b_{jk} = b_{j'k} \). Hence \( \tau_i z_{jk} = z_{j'k} \iff \sigma_i b_{jk} = b_{j'k} \), which proves the equivalence \( (21') \iff (22') \).

We now proceed by induction on \( n - r \) (the case \( r = 0 \) being our aim) which is very easy by the conditions (c), (d) of Lemma 1.8. \( \square \)

For the benefit of the reader we now recapitulate the main features of the proof of Theorem 1.5:

(I) We show that a bounded sentence is equivalent to a restricted Galois sentence, whose covers

\[
C_i \xrightarrow{\varphi_i} B_i \xrightarrow{\psi_i} A_i
\]
satisfy \( \varphi_i = \text{id} \).

(II) We “push the \( B_i \)'s one by one down”, i.e. show by induction, that this restricted Galois sentence is equivalent to another one, whose covers

\[
C_i' \xrightarrow{\varphi_i'} B_i' \xrightarrow{\psi_i'} A_i'
\]

have \( \psi_i' = \text{id} \).

(III) This sentence is equivalent to a (proper) Galois sentence.

**Corollary 1.9.** Let \( \omega \) be a bounded sentence in \( \mathcal{L}_e(K) \). Then we can find (effectively, if \( K \) is a field with elimination theory) a finite Galois extension \( L/K \) and a conjugacy domain \( \text{Con} \) of elements in \( \mathcal{G}(L/K)^e \) such that for an e-free Ax field \( M \) with \( G(M) = \langle \sigma_1, \ldots, \sigma_r \rangle \)

\[
(\bar{M}, \sigma) \models \emptyset \iff \text{Res}_M \sigma \in \text{Con}.
\]

**Proof.** This follows from Theorem 1.5 and an appropriate analogue of Theorem 3.8 in [2]. \( \square \)

**Corollary 1.10.** Let \( \omega \) be a bounded sentence in \( \mathcal{L}_e(K) \) such that \( \omega \in \bar{T}(K) \) and let \( (F, \sigma) \) be a model in \( \mathcal{M}(K) \) such that \( F(\sigma) \) is an e-free Ax field. Then \( (F, \sigma) \models \omega \).

**Corollary 1.11.** Let \( K \) be a countable Hilbertian field with elimination theory. If \( \omega \) is a given bounded sentence in \( \mathcal{L}_e(K) \), then its measure \( \mu(A_K(\omega)) \) can be effectively computed. In particular \( \bar{T}(K) \) is a primitive recursive theory.

In the following Corollary we show that, in a sense, the language \( \mathcal{L}_e(K) \) is stronger than the language \( \mathcal{L}(K) \):

**Corollary 1.12.** Let \( K \) be a countable Hilbertian field. Then there is a bounded sentence \( \omega \) in \( \mathcal{L}_e(K) \) not equivalent modulo \( T(K) \) or even modulo \( \bar{T}(K) \) to any sentence of \( T' \). (Recall the definition of \( T' \) from Lemma 1.2.)

**Proof.** If \( \omega \) is a bounded sentence in \( \mathcal{L}_e(K) \), by Cor. 1.9 there are \( L/K \) and \( \text{Con} \) (as there) such that \( A_K(\omega) \approx \{ \tau \in \mathcal{G}(L/K)^e \mid \text{Res}_L \tau \in \text{Con} \} \) (in particular \( A_K(\omega) \) is measurable). Conversely, for every finite Galois extension \( L/K \) and a conjugacy domain \( \text{Con} \subseteq \mathcal{G}(L/K)^e \) there is a Galois sentence \( \{ \tau \in \text{Con}(\omega) \} \), where \( \omega = \langle A^e, C \rightarrow A^e, \text{Con} \rangle \) such that \( K[C] = L \), hence by Lemma 1.4 there is a bounded sentence \( \omega \in \mathcal{L}_e(K) \) with \( A_K(\omega) = \{ \tau \in \mathcal{G}(K)^e \mid \text{Res}_L \tau \in \text{Con} \} \).
If \( \theta' \in T' \), we obtain by Lemma 1.2 the same characterization of \( A_K(\theta') \); however, from [2], Theorem 3.8 we see that Con also satisfies the following condition:

If \( \tau = (\tau_1, \ldots, \tau_e) \), \( \tau' = (\tau'_1, \ldots, \tau'_e) \in \mathcal{G}(L/K) \), \( \langle \tau_1, \ldots, \tau_e \rangle = \langle \tau'_1, \ldots, \tau'_e \rangle \) and \( \tau \in \text{Con} \), then also \( \tau' \in \text{Con} \).

Conversely, from [2], Cor. 3.9, it follows that for every finite Galois extension and a conjugacy domain \( \text{Con} \subseteq \mathcal{G}(L/K)^e \) satisfying this condition there is a sentence \( \theta \in \mathcal{L}(K) \) such that

\[
A_K(\theta') \approx \{ \sigma \in G(K)^e | \text{Res}_L \sigma \in \text{Con} \}.
\]

Now \( K \), as a Hilbertian field, certainly possesses a cyclic extension \( L \) of degree \( > 2 \) (cf. [3], Lemma 4.3). Let \( \tau_1, \tau_i \) be two distinct generators of \( \mathcal{G}(L/K) \), and let \( \text{Con} = \{ (\tau_1, \text{id}, \ldots, \text{id}) \} \). Then

\[
(\tau'_1, \text{id}, \ldots, \text{id}) \notin \text{Con}, \quad \text{but} \quad \langle \tau'_1, \text{id}, \ldots, \text{id} \rangle = \langle \tau_1, \text{id}, \ldots, \text{id} \rangle = \mathcal{G}(L/K).
\]

Hence the Corollary follows by the characterization above. (E.g., if \( K = \mathbb{Q} \), put \( \omega \) to be \( (3^4 X) [X^4 + X^3 + X^2 + X + 1 = 0 \wedge \Sigma_1 X = X^2] \).

2. The transfer principle

Let \( R \) be an integrally closed integral domain with a quotient field \( K \). The treatment of models \( M(K) \) in section 1 is based on rings finitely generated over \( K \); however, one may replace them by rings finitely generated over \( R \). E.g., if \( A = V - V(g) \), where \( V \subseteq A^n \) is a \( K \)-irreducible set defined by polynomials over \( R \), with a generic point \( x \) over \( K \) and \( g \in R[X_1, \ldots, X_n] \), we let \( R[A] = R[x, g(x)^{-1}] \) be the coordinate ring of \( A \). We shall say that \( A \) is an \( R \)-normal basic set if \( R[A] \) is integrally closed \(^2\).

Let \( \varphi : R \rightarrow \bar{R} \) be an epimorphism onto a ring \( \bar{R} \) with a quotient field \( \bar{K} \). Extend it in the obvious way to polynomials over \( R \). Now if \( A = V(f_1, \ldots, f_m)^- - V(g) \) is a \( K \)-constructible set defined by polynomials over \( R \), we put

\[
A^\varphi = V(f_1^\varphi, \ldots, f_m^\varphi)^- - V(g^\varphi),
\]

which is a \( \bar{K} \)-constructible set defined over \( \bar{R} \).

Assume, in addition, that \( A \) is an \( R \)-normal basic set in \( A^n \).

Let \( \Omega \) be some universal domain over \( \bar{R} \). Define

\[
A^\varphi = \{ a \in \bar{\Omega} | \varphi \text{ can be extended to a homomorphism } R[A] \rightarrow \bar{R}[\bar{a}] \text{ such that } x \rightarrow a \}.
\]

\(^2\) Let \( R = \mathbb{Z} \), \( K = \mathbb{Q} \); then \( A_1 = V(X^2 + 4) \) and \( A_2 = V(X^2 + 4) - V(2) \) are equal as sets over \( \mathbb{Q} \), but \( \mathbb{Z}[A_1] - \mathbb{Z}[2] \) differs from \( \mathbb{Z}[A_2] = \mathbb{Z}[2, \mathbb{Z}^{-1}] = \mathbb{Z}[2] \). Moreover, \( A_2 \) is \( Z \)-normal, while \( A_1 \) is not. This peculiarity is rigorously explained, in the terms of modern algebraic geometry, by observation, that we actually have here two different affine schemes over Spec \( Z \), and then consider their fibres over their generic points, which turn out to be equal. In what follows we consider the reductions of these schemes over primes in \( Z \) (cf. [5], p. 89).
The sets $A^\varphi, \overline{A}^\varphi$ are not necessarily equal. However, one may show, that there is a constant $0 \neq \gamma \in R$, such that $A^\varphi = \overline{A}^\varphi$, whenever $\varphi(\gamma) \neq 0$. Furthermore, by [2], Cor. 2.9, $\gamma$ may be chosen such that if $\varphi(\gamma) \neq 0$ then: $A^\varphi$ is also a non-empty set; it has the same number of components over $\overline{K}$ as $V$ has over $\overline{K}$; given another $R$-normal set $B$, then $B^\varphi \subseteq A^\varphi$ iff $B \subseteq A$ (of course, $\gamma$ depends on $B$ too).

Following this idea one may generalize the theory of Galois stratification: Let $C \to A$ be a Galois cover of sets defined over $R$ (i.e. $R[A] \subseteq R[C]$ are integrally closed, $R[C] = R[A][z], z$ integral over $R[A], \text{disc}_{K(A)}z \in R[A]^*$) and let $a \in A^\varphi(M)$, where $M$ is a field extension of $K$. Then $R \cong R \leftarrow M$ can be extended to a map $\rho_0 : R[A] \to M[a] = M$, and its extension $\rho : R[C] \to \overline{M}$ induces a group homomorphism $\rho^* : G(M) \to \mathcal{G}(C/A) = \mathcal{G}(K(C)/K(A))$. This $\rho^*$ is used to define the Artin symbol, etc.

This is, in fact, the approach, in which Galois stratification have been originally defined by Fried and Sacerdote in [4]. Since a rigorous exposition is not very difficult but rather lengthy, we here content ourselves only with the statement of the relevant results and some comments upon them.

**Theorem 2.1.** Let $\theta$ be a bounded sentence in $\mathcal{L}_\nu(R)$. Then one can find — effectively, if $R$ is presented — a Galois sentence $\psi$ (associated to a Galois stratification over $R$) and an element $0 \neq \gamma \in R$ such that for every $(F, \sigma) \in \mathcal{M}(R)$ with $\varphi : R \to F(\sigma)$ we have: if $\varphi(\gamma) \neq 0$, then

$$(F, \sigma) \models \theta \iff (F, \sigma) \models \psi.$$  

If $M = F(\sigma)$ is a Čebotarev field, one can find a quantifier free Galois sentence $\psi_0$ and $0 \neq \gamma^\prime \in R$ such that if $\varphi(\gamma^\prime) \neq 0$, then

$$(F, \sigma) \models \psi \iff (F, \sigma) \models \psi_0.$$  

Actually it is even not necessary that $M$ in Theorem 1 be Čebotarev: it suffices that $M$ have the Čebotarev property of Section 1 with respect to all the regular Galois covers $C^\prime \to A^\prime$ over $M$, whose Čebotarev property is actually used in the proof of: $(M, \sigma) \models \psi \iff \psi_0$ (see [2], Lemma 3.1). In all of these covers $A^\prime \cong A^1 - V(g)$ with $g \in M[Y]$ and deg $g$ and deg $C^\prime$ are bounded by some constant dependent on the sentence $\psi$.

Such is the situation in the finite fields: if $M$ has $q$ elements, then $G(M)$ is (topologically) generated by $\Phi_M$, where $\Phi_M(x) = x^q$, $\forall x \in \overline{M}$; the above-mentioned condition is summed up in

**Theorem 2.2.** Let $d \geq 1$ and let $M$ be a field with $q$ elements, $q > d^4$. Let $A = A^1 - V(g)$, where $g \in M[Y]$, deg $g < d$, and let $C \to A$ be a Galois cover with deg $C \leq d$. Denote $N = \overline{M} \cap M(C)$. If an element $\tau \in \mathcal{G}(C/A)$ satisfies $\text{Res}_N \tau = \text{Res}_N \Phi_M$, then there exists an $M$-homomorphism $\rho : M[C] \to \overline{M}$ such that $\rho M[A] = M$ and $\rho^* \Phi_M = \tau$. (This theorem also follows from [1], Proposition 2 which is proved by analytic methods.)
Proof. Denote $E = M(A)$, $F = M(C)$. Since $F, \tilde{M}$ are linearly disjoint over $N$, we can extend $\tau$ to a unique element $\tilde{\tau} \in \mathcal{G}(F \tilde{M}/E)$ such that $\text{Res}_{\tilde{M}} \tilde{\tau} = \Phi_M$. Let $D = F \tilde{M}(\tilde{\tau})$. Since the map $\text{Res}_{\tilde{M}} : \mathcal{G}(F \tilde{M}/D) \to G(M)$ maps a generator $\tilde{\tau}$ on a generator $\Phi_M$ and since $G(M) = \mathcal{G}(\tilde{M}/M) \cong \tilde{\tau}$, it is clearly an isomorphism. Hence $D$ and $\tilde{M}$ are linearly disjoint over $M$, whence $D/M$ is regular and $[D : E] = [F \tilde{M} : E \tilde{M}] \leq [F : E] \leq d$, also $D \tilde{M} = F \tilde{M}$.

Let $n$ be the number of $M$-rational places of $D$. By the Riemann hypothesis for curves

$$|n - (q + 1)| \leq 2g(D) \sqrt{q},$$

where the genus $g(D)$ satisfies (cf. [9])

$$g(D) = g(C) \leq \frac{1}{2} (d - 1) (d - 2) \leq \frac{1}{2} (d - 1)^2.$$

Now

$$\sqrt{q} \geq d^2 \geq (d - 1)^2 + 1,$$

hence

$$n \geq (q + 1) - 2g(D) \sqrt{q} \geq (q + 1) - (d - 1)^2 \sqrt{q} = 1 + \sqrt{q - (d - 1)^2} \geq 1 + \sqrt{q} \geq 1 + d^2.$$

Thus there are at least $d^2 + 1$ $M$-rational places of $D$. There are also at most $(1 + \deg g) \leq d$ non-equivalent places of $E$, which are not finite on $M[A]$; each of them has at most $[D : E] \leq d$ extensions on $E$. Hence there is at least one $M$-place $\rho_0 : D \to M$ finite on $M[A]$. Extend it to a place $\tilde{\rho} : D \tilde{M} \to \tilde{M}$ such that $\text{Res}_{\tilde{M}} \tilde{\rho} = \text{id}$ and denote $\rho = \text{Res}_{MC} \tilde{\rho}$. Then $\rho : M[C] \to \tilde{M}$ is an $M$-homomorphism, $\rho(M[A]) = M$, and it follows from definitions that for every $x \in \tilde{M}$ or $x \in D$ finite under $\tilde{\rho}$

$$\tilde{\rho}(\tilde{\tau}x) = \Phi_M(\tilde{\rho}x).$$

In particular for every $x \in M[C] \subseteq D \tilde{M}$ this gives

$$\rho(\tau x) = \Phi_M(\rho x),$$

hence $\rho^* \Phi_M = \tau$.
We apply this to the following situation: Let $K$ be a global field and $R$ its ring of integers. Let $\theta$ be a bounded sentence in $\mathcal{L}_1(R)$. By Theorem 2.1 find the corresponding equivalent Galois sentence $\psi_\theta$ with no quantifiers. Thus by Theorem 2.2 there is a finite Galois extension $L/K$ and a conjugacy domain $\text{Con}$ in $\mathcal{G}(L/K)$ and an element $0 \neq \gamma \in R$ such that:

1.) If $P$ is a prime ideal in $R$ and $M$ is a finite extension field of $\mathbb{F}_p \cong R/P$ and $\gamma \notin P$, then

$$(\bar{M}, \Phi_M) \models \theta \iff \left( \frac{L/K}{p} \right) \in \text{Con}.$$ 

2.) If $\sigma \in G(K)$ and $M = \bar{K}(\sigma)$ is a Êebotarev field, then

$$(\bar{M}, \sigma) \models \theta \iff \text{Res}_L \sigma \in \text{Con}.$$ 

In particular we obtain the following strengthening of Theorem 3.17 of [6] (which has been proved by ultraproduct methods):

**Theorem 2.3.** Let $R$ be a ring of integers of a global field $K$ and let $\theta$ be a bounded sentence in $\mathcal{L}_1(R)$. Then:

1.) $(\bar{K}, \sigma) \models \theta$ for almost all $\sigma \in G(K)$ — in the sense of the Haar measure $\mu$ on $G(K)$ —

$$(\bar{F}_p, \Phi_{\bar{F}_p}) \models \theta \text{ for almost all primes } P \text{ in } R \text{ (i.e., except for a finite subset of them)} \iff$$

$$(\bar{M}, \Phi_M) \models \theta \text{ for all finite extensions } M \text{ of almost all residue fields of } K.$$ 

2.) Let $A(\theta) = \{ \sigma \in G(K) \mid (\bar{K}, \sigma) \models \theta \}$, $B(\theta) = \{ 0 \neq P \in \text{Spec } R \mid (\bar{F}_p, \Phi_{\bar{F}_p}) \models \theta \}$. Then $A(\theta)$ is $\mu$-measurable, $B(\theta)$ has a Dirichlet density $\delta$ and $\mu(A(\theta)) = \delta(B(\theta))$ is a rational number in $[0, 1]$.

**References**