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 $\mathscr{L}(R)$ 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 $\mathscr{L}_e(R)$. One can form a countable set of axioms in $\mathscr{L}_e(R)$ such that a structure

$$(F, \sigma) = \langle F, +, \cdot, \sigma_1, \ldots, \sigma_e, \bar{a} \rangle_{a \in R}$$

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

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

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

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

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

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

$$M^{(m)} = \{\alpha \in F \mid [M(\alpha) : M] \leq m\}.$$

---

*) This work is a version of a part of the doctoral dissertation of the first author done in Tel-Aviv University under the supervision of the second author. The first author was partially supported by the Minerva Foundation while visiting at the Heidelberg University.

A *bounded formula* φ is a formula in $\mathscr{L}_e(R)$, on whose quantifiers appear as superscripts positive integers, so-called *bounds*. Thus in the prenex normal form φ 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 ψ is a quantifier free formula in $\mathscr{L}_e(R)$. As to its meaning: for $(F, \sigma) \in \mathscr{M}(R)$ and $\beta_1, \ldots, \beta_k \in F$ we write $(F, \sigma) \models \varphi(\beta_1, \ldots, \beta_k)$ iff for $M = F(\sigma)$

$$(Q_1 \alpha_1 \in M^{(m_1)}) \cdots (Q_n \alpha_n \in M^{(m_n)}) [(F, \sigma) \models \psi(\alpha, \beta)].$$

(These formulas are definable in the language $\mathscr{L}_e(R)$, 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 $\mathscr{L}_e(K)$, where K is a field.

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

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

For a sentence θ in $\mathscr{L}_e(K)$ we define

$$A(\theta) = A_K(\theta) = \{\sigma = (\sigma_1, \ldots, \sigma_e) \in G(K)^e \mid (\tilde{K}, \sigma) \models \theta\}.$$

We denote by $\tilde{T}(K)$ the theory of all sentences θ for which $A(\theta) \approx G(K)^e$ (i.e., $\mu(A(\theta)) = 1$). Then two sentences θ_1, θ_2 are equivalent modulo $\tilde{T}(K)$ 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 e-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 $\mathscr{L}_e(K)$. The converse of this statement is our main result: Every bounded sentence of $\mathscr{L}_e(K)$ is equivalent modulo $T(K)$ to a Galois sentence.

Having this result we consider a countable Hilbertian field K with elimination theory and use Čebotarev 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 $\tilde{T}(K)$.

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 θ of $\mathscr{L}_1(R)$. For every prime ideal $P \neq 0$ of R we denote $\mathbb{F}_P = R/P$ and let Φ_P be the Frobenius automorphism $\Phi_P(x) = x^{NP}$. It is shown that the Dirichlet density of

$$\{P \mid (\tilde{\mathbb{F}}_P, \Phi_P) \models \theta\}$$

is equal to the Haar measure of the set $A_K(\theta)$.

It can be shown that the bounded sentences of $\mathscr{L}_e(K)$ do not exhaust all the sentences of $\mathscr{L}_e(K)$: there exist sentences in $\mathscr{L}_e(K)$ which are not equivalent modulo $\tilde{T}(K)$ to a bounded sentence. One may therefore ask about the decidability of the theory of all sentences in $\mathscr{L}_e(K)$ which are true in $(\tilde{K}, \sigma)$ for almost all $\sigma \in G(K)^e$. This is yet an open problem.

1. Galois stratifications

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

Lemma 1. 1. *A bounded formula $\varphi = \varphi(Y_1, \ldots, Y_k)$ in $\mathscr{L}_e(R)$ is equivalent modulo $T(R)$ to a formula $\hat{\varphi} = \hat{\varphi}(Y_1, \ldots, Y_k)$ of $\mathscr{L}_e(R)$, i.e., for $(F, \sigma) \in \mathscr{M}(R)$ and $\beta_1, \ldots, \beta_k \in F$*

$$(F, \sigma) \models \varphi(\beta_1, \ldots, \beta_k) \Leftrightarrow (F, \sigma) \models \hat{\varphi}(\beta_1, \ldots, \beta_k).$$

Proof. Assume that φ is $(\exists^m X)\,[\psi(X, Y_1, \ldots, Y_k)]$, where $\psi(X, Y)$ is a formula of $\mathscr{L}_e(R)$. Define $\hat{\varphi}$ to be

$$(\exists X)(\exists X_1') \cdots (\exists X_m') \Big[\psi(X, Y_1, \ldots, Y_k) \wedge \Big(\bigwedge_{i=1}^{m} \bigwedge_{j=1}^{e} \Sigma_j X_i' = X_i' \Big) \wedge (X^m + X_1' X^{m-1} + \cdots + X_m' = 0) \Big].$$

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

$$(\forall^m X)\,[\psi(X, Y)] \equiv \neg (\exists^m X)\,[\neg\, \psi(X, Y)]). \quad \blacksquare$$

Lemma 1. 2. *To every formula $\varphi = \varphi(Y_1, \ldots, Y_k)$ in $\mathscr{L}(R)$ there exists a bounded formula $\varphi = \varphi'(Y_1, \ldots, Y_k)$, equivalent to φ in the following sense: for a couple $(F, \sigma) \in \mathscr{M}(R)$ and $\beta_1, \ldots, \beta_k \in F(\sigma)$ we have*

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

Proof. By induction on the structure of φ. If φ is atomic, put

$$\varphi' = \varphi; \quad (\varphi_1 \vee \varphi_2)' = \varphi_1' \vee \varphi_2'; \quad (\neg\, \varphi)' = \neg\, \varphi';$$

and finally $((\exists X)\, \varphi)' = (\exists^1 X)\, \varphi'$. $\blacksquare$

Let $T' = \{\theta' \in T(R) \mid \theta$ is a sentence in $\mathscr{L}(R)\}$.

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 $\mathbb{A}^n$ 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 $C \subseteq \mathbb{A}^n$, $A \subseteq \mathbb{A}^m$ be basic normal sets, and let $\varphi: C \to A$ 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 φ induces a K-embedding $K[A] \to K[C]$, which we regard for simplicity as a ring inclusion. If $K[C] = K[A][u]$, with u integral over $K[A]$, such that $\mathrm{discr}_{K(C)/K(A)}(u) \in K[A]^\times$, we say that $\varphi: C \to A$ 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 a *Galois cover*, and denote $\mathcal{G}(C/A) = \mathcal{G}(K(C)/K(A))$.

Assume that $\varphi: C \to A$ is a Galois cover over K. Let $(F, \sigma = (\sigma_1, \ldots, \sigma_e)) \in \mathcal{M}(K)$ and put $M = F(\sigma_1, \ldots, \sigma_e)$. A point $a \in A(M)$ defines a K-homomorphism $\rho_0: K[A] \to M$, which may be extended to $\rho: K[C] \to \tilde{M}$ (= 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 ρ induces an isomorphism between $\mathcal{G}(K(c)/K(a))$ and the decomposition group of φ (cf. [8], Chpt. IX, Prop. 15). Its inverse, composed with the restriction to $K(c)$ defines a continuous homomorphism

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

defined explicitly by the formula

$$\rho((\rho^* \tau)(u)) = \tau(\rho u), \qquad \tau \in G(M). \tag{1}$$

We lift ρ^* in the obvious way to a map

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

The extension ρ of ρ_0 is not unique; however, the set

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

is uniquely determined by a. We call it the *Artin symbol* of a with respect to (F, σ)[1]. The *conjugation* on $\mathcal{G}(C/A)^e$ (by elements $\tau \in \mathcal{G}(C/A)$): $(\iota_1, \ldots, \iota_e)^\tau = (\tau^{-1} \iota_1 \tau, \ldots, \tau^{-1} \iota_e \tau)$ defines an equivalence relation on $\mathcal{G}(C/A)^e$; the Artin symbol is a *conjugacy class*.

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

$$\mathcal{A} = \langle \mathbb{A}^n, C_i \xrightarrow{\varphi_i} A_i, \mathrm{Con}(A_i) \rangle_{i \in I}, \tag{3}$$

where $\mathbb{A}^n = \bigcup_{i \in I} A_i$ is a finite disjoint union of K-normal basic sets, and for every $i \in I$ $C_i \xrightarrow{\varphi_i} A_i$ is a Galois cover and $\mathrm{Con}(A_i) \subseteq \mathcal{G}(C_i/A_i)^e$ 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

$$\mathrm{Ar}(X_1, \ldots, X_n) \subseteq \mathrm{Con}(\mathcal{A}), \tag{4}$$

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

$$(F, \sigma) \models \mathrm{Ar}(a) \subseteq \mathrm{Con}(\mathcal{A})$$

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

$$\mathrm{Ar}_{A_i, F, \sigma}(a) \subseteq \mathrm{Con}(A_i).$$

[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 $n \geqq 0$ and every Galois stratification $\mathscr{A}$ of $\mathbb{A}^n$ over K one *n-ary* relational symbol (4), — and no other relational symbols (including equality) apart from these.

A structure $(F, \sigma) \in \mathscr{M}(K)$ 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 θ are associated with the same affine space $\mathbb{A}^n$. Then using the concept of refinement (see [2], paragraph preceding Lemma 3. 3) and of complementary stratification ([2], Lemma 3. 5) one converts θ to an equivalent (modulo $T(K)$) sentence θ' in the following prenex normal form:

(5) $$(Q_1 X_1) \cdots (Q_n X_n) [\mathrm{Ar}(X_1, \ldots, X_n) \subseteq \mathrm{Con}(\mathscr{A})],$$

where $Q_1, \ldots, Q_n$ are quantifiers and $\mathscr{A}$ is a Galois stratification.

Next, note that in [2] we define $\mathrm{Con}(A)$ and $\mathrm{Ar}_{A,F,\sigma}$ ($= \mathrm{Ar}_{A,M}$ in [2]) as conjugacy domains of subgroups of $\mathscr{G}(C/A)$, 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 $C \to A$ 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 $\tau = (\tau_1, \ldots, \tau_e) \in \mathscr{G}(C/A)^e$. If $\mathrm{Res}_N \tau = \mathrm{Res}_N \sigma$, then there exists an M-epimorphism $\rho: M[C] \to \tilde{M}$, such that $\rho M[A] = M$, and $\rho^*(\sigma) = \tau$.

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 $\langle \tilde{K}(\sigma), \sigma \rangle$ 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 $\mathscr{L}_e(K)$ in the following sense: for every $(F, \sigma) \in \mathscr{M}(K)$ and $\beta_1, \ldots, \beta_k \in F(\sigma)$*

$$(F, \sigma) \models \theta(\beta_1, \ldots, \beta_k) \Leftrightarrow (F, \sigma) \models \hat{\theta}(\beta_1, \ldots, \beta_k).$$

Proof. It suffices to prove the Lemma for an atomic formula. Indeed, in the general case replace the atomic components of θ 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 $\mathscr{A} = \langle \mathbb{A}^k, C_i \xrightarrow{\varphi_i} A_i, \mathrm{Con}(A_i) \rangle_{i \in I}$ be the underlying stratification for the atomic formula $\theta(Y_1, \ldots, Y_k)$. For every $j \in I$ and $\tau = (\tau_1, \ldots, \tau_e) \in \mathrm{Con}(A_j)$ let

$$\mathscr{A}_{j,\tau} = \langle \mathbb{A}^k, C_i \xrightarrow{\varphi_i} A_i, \mathrm{Con}_{j,\tau}(A_i) \rangle_{i \in I}$$

be a Galois stratification of $\mathbb{A}^k$, where

$$\mathrm{Con}_{j,\tau}(A_i) = \begin{cases} \{\tau^\iota \mid \iota \in \mathscr{G}(C_j/A_j)\} & j = i, \\ \emptyset & j \neq i. \end{cases}$$

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

In that case $C_j = V(f_1, \ldots, f_n) - V(g)$, where $f_1, \ldots, f_n, g \in K[X_1, \ldots, X_m]$, is a normal subset of an affine space $\mathbb{A}^m$; there are also $h_1, \ldots, h_k \in K[X_1, \ldots, X_m]$, such that $\varphi_j(x) = (h_1(x), \ldots, h_k(x))$ 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 $C_j \xrightarrow{\varphi_j} A_j$. Let $p_0, p_1, \ldots, p_e \in K[X_1, \ldots, X_m, U]$ be such that

$$z = p_0(x, g(x)^{-1}), \quad \tau_l z = p_l(x, g(x)^{-1}), \quad l = 1, \ldots, e.$$

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

$$(\exists^d X_1) \cdots (\exists^d X_m)(\exists^d U)\Big[\bigwedge_{s=1}^{n} f_s(X) = 0 \wedge g(X)\,U = 1 \wedge \bigwedge_{t=1}^{k} h_t(X) = Y_t \wedge \bigwedge_{l=1}^{e} \Sigma_l p_0(X, U) = p_l(X, U)\Big],$$

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

For $(F, \sigma) \in \mathscr{M}(K)$ and $\beta_1, \ldots, \beta_k \in M = F(\sigma)$ we have $(F, \sigma) \models \hat{\theta}(\beta)$ iff there is a K-homomorphism $\rho : K[C_j] \to F$, such that $\mathrm{Res}_{K[A_j]}\,\rho$ defines β (in particular $\rho K[A_j] \subseteq M$) and $\sigma_l(\rho z) = \rho(\tau_l z)$ for $l = 1, \ldots, e$. This is equivalent to $\mathrm{Ar}_{A_j, F, \sigma}(\beta) \subseteq \mathrm{Con}_{j,\tau}(A_j)$. Thus $\hat{\theta}$ is equivalent to θ. ∎

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

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

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

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

Let $(F, \sigma) \in \mathscr{M}(K)$, $M = F(\sigma)$. 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 $K[B]$, ρ_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

$$(6) \qquad \{\rho_1^* \sigma \mid \rho_1 : K[C] \to F \text{ extends } \rho_0\} = \{(\rho^* \sigma)^\iota \mid \iota \in \mathcal{G}(C/B)\}$$

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 $\mathrm{Ar}_{B,F,\sigma}(b)$.

Let $B^j \xrightarrow{\psi^j} A^j$, $j = 1, \ldots, n$ be K-epimorphisms 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

$$\psi(b_1, \ldots, b_n) = \big(\psi^1(b_1), \ldots, \psi^n(b_n)\big).$$

A *restricted Galois stratification* of *the set* B is a structure

$$(7) \qquad \mathcal{B} = \langle B, C_i \xrightarrow{\varphi_i} B_i \xrightarrow{\psi_i} A_i, \mathrm{Con}(B_i) \rangle_{i \in I},$$

where $B = \bigcup_{i \in I} B_i$ is a finite disjoint union of K-normal basic sets, and for every $i \in I$ $C_i \xrightarrow{\varphi_i} B_i \xrightarrow{\psi_i} A_i$ is a restricted Galois cover with $\psi_i = \mathrm{Res}_{B_i} \psi$, and $\mathrm{Con}(B_i)$ 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

$$(8) \qquad [\mathrm{Ar}(X_1, \ldots, X_n) \subseteq \mathrm{Con}(\mathcal{B})].$$

For $(F, \sigma) \in \mathcal{M}(K)$ and $b = (b_1, \ldots, b_n) \in B(M, \psi)$, where $M = F(\sigma)$, we write

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

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 $B\big(F(\sigma), \psi^i\big)$.

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

$$C'_k \xrightarrow{\varphi'_k} B'_k \xrightarrow{\psi'_k} A'_k, \quad k \in I',$$

where $\psi'_k = \mathrm{Res}_{B'_k} \psi_i$. 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 $\mu_k : K[C_i] \to \widetilde{K(B'_k)}$. Assume that $\mu_k K[C_i] \subseteq K[C'_k]$. Then μ_k induces a group homomorphism $\mu_k^* : \mathcal{G}(C'_k/A'_k)^e \to \mathcal{G}(C_i/A_i)^e$.

This may depend on our choice of the extension μ_k, however

$$\mathrm{Con}\,(B'_k) = \bigcup_{i \in \mathscr{G}(C'_k/B'_k)} [\mu_k^{*\,-1}\,\mathrm{Con}\,(B_i)]^i$$

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

$$\mathrm{Ar}_{B_i, F, \sigma}(b) \subseteq \mathrm{Con}\,(B_i) \Leftrightarrow \mathrm{Ar}_{B'_k, F, \sigma}(b) \subseteq \mathrm{Con}\,(B'_k)\,.$$

Therefore the *refinement* $\mathscr{B}'$ of $\mathscr{B}$ obtained by replacing $\langle C_i \to B_i \to A_i, \mathrm{Con}\,(B_i)\rangle$ in (7) by $\langle C'_k \to B'_k \to A'_k, \mathrm{Con}\,(B'_k)\rangle_{k \in I'}$ is equivalent to $\mathscr{B}$ 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 $A''_i = \psi(B''_i)$ is also a K-normal basic set and $C''_i \xrightarrow{\mathrm{Res}\,\varphi_i} B''_i \xrightarrow{\mathrm{Res}\,\psi_i} A''_i$ 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 $D''_i \xrightarrow{\varphi''} B''_i \xrightarrow{\mathrm{Res}\,\psi_i} A''_i$, 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 $\mathscr{B}$, 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 $\mathscr{M}(K)$.

As an application consider two restricted Galois stratifications $\mathscr{B}'$, $\mathscr{B}''$ 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: $\mathrm{Con}'\,(B_i)$ for $\mathscr{B}'$ and $\mathrm{Con}''\,(B_i)$ for $\mathscr{B}''$, $i \in I$. It is then clear, that the formula

$$[\mathrm{Ar}\,(X) \subseteq \mathrm{Con}\,(B')] \vee [\mathrm{Ar}\,(X) \subseteq \mathrm{Con}\,(B'')]$$

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

$$\mathrm{Con}\,(B_i) = \mathrm{Con}'\,(B_i) \cup \mathrm{Con}''\,(B_i)\,, \qquad i \in I\,.$$

Moreover, the formula $\neg\,[\mathrm{Ar}\,(X) \subseteq \mathrm{Con}\,(\mathscr{B})]$, associated with (7), is equivalent modulo $T(K)$ to an atomic formula $[\mathrm{Ar}(X) \subseteq \mathrm{Con}\,(\mathscr{B}^c)]$, where $\mathscr{B}^c$ is the *complementary stratification* (cf. [2], Lemma 3. 5):

$$\mathscr{B}^c = \langle B, C_i \xrightarrow{\varphi_i} B_i \xrightarrow{\psi_i} A_i, \mathrm{Con}^c\,(B_i)\rangle_{i \in I} \tag{9}$$

with $\mathrm{Con}^c\,(B_i) = \mathscr{G}(C_i/A_i)^e - \mathrm{Con}\,(B_i)$, $i \in I$.

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 $\mathscr{M}(K)$, to a sentence of the form

$$(Q_1 X_1) \cdots (Q_n X_n)\,[\mathrm{Ar}\,(X_1, \ldots, X_n] \subseteq \mathrm{Con}\,(B)]\,, \tag{10}$$

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

Remark 1. 6. If $\psi = \mathrm{id}$, (10) is equivalent to a Galois sentence. Indeed, for every $1 \leqq j \leqq n$, B^j is in some affine space $\mathbb{A}^{m_j}$, hence $B \subseteq \mathbb{A} \equiv \mathbb{A}^{m_1} \times \cdots \times \mathbb{A}^{m_n}$. We may represent $\mathbb{A} - B$ as a disjoint union $\bigcup_{i \in I'} B_i$ of K-normal sets and for $i \in I'$ define $A_i = B_i$, $\varphi_i = \mathrm{id}$, $\mathrm{Con}(B_i) = \emptyset$. One may in an obvious way identify $\mathbb{A}$ with $\mathbb{A}^m$, where $m = m_1 + \cdots + m_n$.

Then the Galois sentence

$$(Q_1 Y_{11}) \cdots (Q_1 Y_{1m_1}) \cdots (Q_n Y_{n1}) \cdots (Q_n Y_{nm_n}) [\mathrm{Ar}(Y_{11}, \ldots, Y_{1m_1}, \ldots, Y_{n1}, \ldots, Y_{nm_n}) \subseteq \mathrm{Con}(\mathscr{B}')],$$

where

$$\mathscr{B}' = \langle \mathbb{A}^m, A_i \xrightarrow{\varphi_i} B_i, \mathrm{Con}(B_i) \rangle_{i \in I \cup I'},$$

is obviously equivalent to (10).

Lemma 1. 7. *Every restricted Galois sentence θ is equivalent to a Galois sentence $\hat{\theta}$ in the following sense: $(F, \sigma) \models \hat{\theta} \Leftrightarrow (F, \sigma) \models \theta$, for every $(F, \sigma) \in \mathscr{M}(K)$.*

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

Let $1 \leqq r \leqq n$ and put $\hat{B} = B^1 \times \cdots \times B^{r-1} \times A^r \times B^{r+1} \times \cdots \times B^n$. Define epimorphisms $\hat{\psi} : \hat{B} \to A$ by $\hat{\psi} = \psi^1 \times \cdots \times \psi^{r-1} \times \mathrm{id} \times \psi^{r+1} \times \cdots \times \psi^n$ and $\hat{\varphi} : B \to \hat{B}$ by

$$\hat{\varphi} = \mathrm{id} \times \cdots \times \mathrm{id} \times \psi^r \times \mathrm{id} \times \cdots \times \mathrm{id}.$$

(Thus $\hat{\psi} \circ \hat{\varphi} = \psi$.)

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 $\hat{\varphi}(B_i) = \hat{B}_k$. For every $k \in \hat{I}$ pick up an $i \in I$ such that $\hat{\varphi}(B_i) = \hat{B}_k$; then there is a restricted Galois cover $\hat{C}_k \xrightarrow{\hat{\varphi}_k} \hat{B}_k \xrightarrow{\mathrm{Res}\,\hat{\psi}} \hat{A}_k$, where $\hat{C}_k = C_i$, $\hat{A}_k = A_i = \hat{\psi}(\hat{B}_k)$ and $\hat{\varphi}_k = (\mathrm{Res}_{B_i} \hat{\varphi}) \circ \varphi_i$. By a further refinement we may even assume, that for every $i' \in I$ with $\hat{\varphi}(B_{i'}) = \hat{B}_k$ 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 $\mathrm{Con}(\hat{B}_k)$ in $\mathscr{G}(\hat{C}_k/\hat{A}_k)^e$. Then we obtain a restricted Galois stratification of $\hat{B}$

(11) $$\hat{\mathscr{B}} = \langle \hat{B}, \hat{C}_k \xrightarrow{\hat{\varphi}_k} \hat{B}_k \xrightarrow{\mathrm{Res}\,\hat{\psi}} A_k, \mathrm{Con}(\hat{B}_k) \rangle_{k \in \hat{I}}$$

and a corresponding sentence

(12) $$(Q_1 X_1) \cdots (Q_n X_n) [\mathrm{Ar}(X_1, \ldots, X_n) \subseteq \mathrm{Con}(\hat{\mathscr{B}})].$$

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

(13) $$(Q_r X_r) [\mathrm{Ar}(X_1, \ldots, X_n) \subseteq \mathrm{Con}(\mathscr{B})]$$

(14) $$(Q_r X_r) [\mathrm{Ar}(X_1, \ldots, X_n) \subseteq \mathrm{Con}(\hat{\mathscr{B}})],$$

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

$$(\forall X_r)\,[\mathrm{Ar}\,(X) \subseteq \mathrm{Con}\,(\mathscr{B})] \equiv \neg\,(\exists X_r)\,[\mathrm{Ar}\,(X) \subseteq \mathrm{Con}\,(\mathscr{B}^c)]$$
$$\equiv \neg\,(\exists X_r)\,[\mathrm{Ar}\,(X) \subseteq \mathrm{Con}\,(\widehat{\mathscr{B}^c})] \equiv (\forall X_r)\,[\mathrm{Ar}\,(X) \subseteq \mathrm{Con}\,((\widehat{\mathscr{B}^c})^c)]\,,$$

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

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

$$\text{(15)} \qquad \mathrm{Con}\,(\hat{B}_k) = \bigcup_{\substack{i \in I \\ \hat{\varphi}(B_i) = \hat{B}_k}} \; \bigcup_{\iota \in \mathscr{G}(\hat{C}_k/\hat{B}_k)} \mathrm{Con}\,(B_i)^{\iota}\,.$$

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

$$\text{(16)} \qquad (F, \sigma) \models (\exists X_r)\,[\mathrm{Ar}\,(b_1, \ldots, b_{r-1}, X_r, b_{r+1}, \ldots, b_n) \subseteq \mathrm{Con}\,(\mathscr{B})]\,,$$

$$\text{(17)} \qquad (F, \sigma) \models (\exists X_r)\,[\mathrm{Ar}\,(b_1, \ldots, b_{r-1}, X_r, b_{r+1}, \ldots, b_n) \subseteq \mathrm{Con}\,(\hat{\mathscr{B}})]\,.$$

Now, if (16) holds, there is a $b_r \in B^r(M, \psi^r)$ such that $b = (b_1, \ldots, b_r, \ldots, b_n) \in B_i$ for some $i \in I$ and $\mathrm{Ar}_{B_i, F, \sigma}(b) \subseteq \mathrm{Con}\,(B_i)$. Then $b'_r = \psi^r(b_r) \in A^r(M, id)$ and

$$b' = (b_1, \ldots, b_{r-1}, b'_r, b_{r+1}, \ldots, b_n) \in \hat{\varphi}(B_i) = \hat{B}_k$$

for a unique $k \in \hat{I}$. Since $\mathrm{Ar}_{\hat{B}_k, F, \sigma}(b') \subseteq \mathrm{Ar}_{B_i, F, \sigma}(b)$, and since $\mathrm{Ar}_{\hat{B}_k, F, \sigma}(b')$ is a restricted conjugacy class of $\mathscr{G}(\hat{C}_k/\hat{A}_k)^e$ with respect to $\hat{B}_k$, we have that

$$\mathrm{Ar}_{\hat{B}_k, F, \sigma}(b') = \bigcup_{\iota \in \mathscr{G}(\hat{C}_k/\hat{B}_k)} \mathrm{Ar}_{B_i, F, \sigma}(b)^{\iota}\,,$$

hence (17) follows.

If (17) is true, there is a $b'_r \in A^r(M, \mathrm{id})$ such that $b' = (b_1, \ldots, b_{r-1}, b'_r, b_{r+1}, \ldots, b_n) \in \hat{B}_k$ for some $k \in \hat{I}$, and $\mathrm{Ar}_{\hat{B}_k, F, \sigma}(b') \subseteq \mathrm{Con}\,(\hat{B}_k)$. Thus the K-map $\rho_0 : K[B_k] \to K[b']$ may be extended to $\rho : K[\hat{C}_k] \to \widetilde{K(b')}$ and $(\rho^* \sigma)^{\iota} \in \mathrm{Con}\,(B_i)$ for some $i \in I$ with $\hat{\varphi}(B_i) = \hat{B}_k$ and some $\iota \in \mathscr{G}(\hat{C}_k/\hat{B}_k)$. Without restriction $\iota = \mathrm{id}$, otherwise replace ρ by $\rho \circ \iota$. Now $\mathrm{Res}_{K[B_i]}\rho$ defines a point $b \in B_i$ with $\mathrm{Ar}_{B_i, F, \sigma}(b) \subseteq \mathrm{Con}\,(B_i)$. Since $\hat{\varphi}(b) = b'$, we have

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

where $\psi^r(b_r) = b'_r \in A^r(M)$, hence $b_r \in B^r(M, \psi^r)$. Thus (16) follows.

This ends the proof of this Lemma, by induction and by Remark 1. 6. ∎

Let m be a positive integer and let $\psi : \mathbb{A}^m \to \mathbb{A}^m$ 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 $z = (z_1, \ldots, z_m) \in \mathbb{A}^m$ the extension $K(z)/K(\psi(z))$ is normal, its automorphisms permute $z_1, \ldots, z_m$ and $[K(\psi(z), z_1) : K(\psi(z))] \leqq m$. This extension need not be separable; however, it is easy to find a K-constructible set $B \subseteq \mathbb{A}^m$, large enough for our purposes, such that $K(z)/K(\psi(z))$ is Galois for every $z \in B$. For example

$$B = \bigcup_{r=0}^{m} \left[V(Z_{r+1}, \ldots, Z_m) - V\left(\prod_{\substack{\alpha, \beta = 1 \\ \alpha \neq \beta}}^{r} (Z_\alpha - Z_\beta) \right) \right].$$

The image $A = \psi(B)$ of B is a K-constructible subset of $\mathbb{A}^m$.

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, $A^j \subseteq \mathbb{A}^{m_j}$ and a K-epimorphism $B^j \xrightarrow{\psi^j} A^j$ such that for every $z = (z_1, \dots, z_{m_j}) \in B^j$ and every $K \subseteq M$:*

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

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

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

(d) *if $z'_1 \in M^{(m_j)}$, there is some $(z_1, \dots, z_{m_j}) \in B^j(M, \psi^j)$ with $z_1 = z'_1$.* (E.g., let $z_1 = z'_1, z_2, \dots, z_r$ be all the distinct conjugates of z'_1 over M and $z_{r+1} = \cdots = z_m = 0$.)

Proof of Theorem 1. 5. By adding new, suitably quantified variables we may assume that the bounded sentence ω is constructed by disjunctions, conjunctions, negations and bounded quantifications from formulae of the form

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

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

(ii) $\Sigma_l X_j = X_{j'}$.

Indeed, e.g. instead of $\Sigma_2 \Sigma_1 X_1 = X_2$ we write $(\exists^m Y_1)[\Sigma_1 X_1 = Y_1 \wedge \Sigma_2 Y_1 = X_2]$, where m is the bound on the quantifier of X_1. Instead of $\Sigma_1 f_1(X_1, \dots, X_n) \neq f_2(X_1, \dots, X_n)$ we insert

$$(\exists^{m_1} Y_1)(\exists^{m_2} Y_2)[Y_1 - f_1(X) = 0 \wedge Y_2 - f_2(X) = 0 \wedge \neg(\Sigma_1 Y_1 = Y_2)],$$

where the bound m_1 (resp. m_2) is determined from the bounds on quantifiers of $X_1, \dots, X_n$ and the polynomial f_1 (resp. f_2). (Note that for $\alpha_1 \in M^{(\mu_1)}$, $\alpha_2 \in M^{(\mu_2)}$ we have $\alpha_1 + \alpha_2$, $c\alpha_1\alpha_2 \in M^{(\mu_1\mu_2)}$ for every $c \in M$; thus by induction on the structure of f_1 one can find $m_1 \in \mathbb{N}$ such that for $K \subseteq M$

$$\alpha_j \in M^{(\mu_j)}, \quad j = 1, \dots, n \Rightarrow f_1(\alpha_1, \dots, \alpha_n) \in M^{(m_1)}.)$$

Therefore ω may be written in the prenex normal form as

$$(18) \qquad (Q_1^{m_1} X_1) \cdots (Q_n^{m_n} X_n) \bigvee_{\lambda \in \Lambda} [(X_1, \dots, X_n) \in D_\lambda \wedge \omega_\lambda(X_1, \dots, X_n)],$$

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

For every $1 \leqq j \leqq n$ let $\psi^j \colon B^j \to A^j$ 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

$$D'_\lambda = \{(z_{11}, \ldots, z_{1m_1}), \ldots, (z_{n1}, \ldots, z_{nm_n}) \in B \mid (z_{11}, z_{21}, \ldots, z_{n1}) \in D_\lambda\}$$

for every $\lambda \in \Lambda$. Their intersections with sets $V(Z_{j_1k_1} - Z_{j_2k_2})$ and $V(Z_{j_1k_1} - Z_{j_2k_2})^c$ 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 $B_i \subseteqq D'_\lambda$ and for every $1 \leqq j_1, j_2 \leqq n$, $1 \leqq k_1 \leqq m_{j_1}$, $1 \leqq k_2 \leqq m_{j_2}$ either $B_i \subseteqq V(Z_{j_1k_1} - Z_{j_2k_2})$ or $B_i \cap V(Z_{j_1k_1} - Z_{j_2k_2}) = \emptyset$) such that for every $i \in I$

$$B_i \xrightarrow{\operatorname{Res}_{B_i}\psi} A_i = \psi(B_i)$$

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 $\bar{z} = (z_{11}, z_{21}, \ldots, z_{n1})$ and let

(19) $\quad \operatorname{Con}(B_i) = \{\tau \in \mathcal{G}(B_i/A_i)^e \mid (K(B_i), \tau) \models \omega_\lambda(\bar{z})$ for the unique λ such that $B_i \subseteqq D'_\lambda\}$.

(More rigorously we should write instead of $(K(B_i), \tau)$ perhaps $(\widetilde{K(B_i)}, \tilde{\tau})$, where $\tilde{\tau} \in (\operatorname{Aut}(\widetilde{K(B_i)}))^e$ is some extension of τ.) Then

$$\mathcal{B} = \langle B, B_i \xrightarrow{\text{id}} B_i \xrightarrow{\operatorname{Res}\psi} A_i, \operatorname{Con}(B_i)\rangle_{i \in I} \tag{20}$$

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 $0 \leqq r \leqq n$ and

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

Claim. *The following two statements are equivalent:*

$$(F, \sigma) \models (Q_{r+1}^{m_{r+1}} X_{r+1}) \cdots (Q_n^{m_n} X_n) \bigvee_{\lambda \in \Lambda} [(b_{11}, \ldots, b_{r1}, X_{r+1}, \ldots, X_n) \in D_\lambda \wedge \omega_\lambda(b_{11}, \ldots, b_{r1}, X_{r+1}, \ldots, X_n)], \tag{21}$$

$$(F, \sigma) \models (Q_{r+1} Z_{r+1}) \cdots (Q_n Z_n) [\operatorname{Ar}(b_1, \ldots, b_r, Z_{r+1}, \ldots, Z_n) \subseteqq \operatorname{Con}(\mathcal{B})]. \tag{22}$$

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 $B_i \subseteqq D'_\lambda$, hence $(b_{11}, \ldots, b_{n1}) \in D_\lambda$. The point b defines a K-homomorphism $\rho: K[B_i] \to K[b] \subseteqq \tilde{M}$, and $\rho K[A_i] \subseteqq M$. Let $\tau = \rho^* \sigma \in \mathcal{G}(B_i/A_i)^e$. Then (21) is equivalent to

$$(F, \sigma) = \omega_\lambda(b_{11}, \ldots, b_{n1}), \tag{21'}$$

and (22) is equivalent to $\operatorname{Ar}_{B_i, F, \sigma}(b) \subseteqq \operatorname{Con}(B_i)$, hence to

$$(K(B_i), \tau) = \omega_\lambda(z_{11}, \ldots, z_{n1}), \tag{22'}$$

by the definition (19).

So with no loss we may assume that ω_λ is $\Sigma_l X_j = X_{j'}$. By Lemma 1. 8 (b) there is $1 \leqq k \leqq m_j$ such that $\tau_l(z_{j1}) = z_{jk}$; hence $\sigma_l(b_{j1}) = b_{jk}$. But since $B_i \subseteqq V(Z_{jk} - Z_{j'1})$ or $B_i \cap V(Z_{jk} - Z_{j'1}) = \emptyset$, we have: $z_{jk} = z_{j'1} \Leftrightarrow b_{jk} = b_{j'1}$. Hence $\tau_l z_{j1} = z_{j'1} \Leftrightarrow \sigma_l b_{j1} = b_{j'1}$, which proves the equivalence (21′) $\Leftrightarrow$ (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. ∎

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 $\varphi_i = \mathrm{id}$.

(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 $\psi_i' = \mathrm{id}$.

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

Corollary 1. 9. *Let ω be a bounded sentence in $\mathscr{L}_e(K)$. Then we can find* (effectively, if K is a field with elimination theory) *a finite Galois extension L/K and a conjugacy domain* Con *of elements in $\mathscr{G}(L/K)^e$ such that for an e-free Ax field M with $G(M) \models \langle \sigma_1, \ldots, \sigma_e \rangle$*

$$(\tilde{M}, \sigma) \models \theta \Leftrightarrow \mathrm{Res}_L \sigma \in \mathrm{Con}.$$

Proof. This follows from Theorem 1. 5 and an appropriate analogue of Theorem 3. 8 in [2]. ∎

Corollary 1. 10. *Let ω be a bounded sentence in $\mathscr{L}_e(K)$ such that $\omega \in \tilde{T}(K)$ and let (F, σ) be a model in $\mathscr{M}(K)$ 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 ω is a given bounded sentence in $\mathscr{L}_e(K)$, then its measure $\mu(A_K(\omega))$ can be effectively computed. In particular $\tilde{T}(K)$ is a primitive recursive theory.*

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

Corollary 1. 12. *Let K be a countable Hilbertian field. Then there is a bounded sentence ω in $\mathscr{L}_e(K)$ not equivalent modulo $T(K)$ or even modulo $\tilde{T}(K)$ to any sentence of T'.* (Recall the definition of T' from Lemma 1. 2.)

Proof. If ω is a bounded sentence in $\mathscr{L}_e(K)$, by Cor. 1. 9 there are L/K and Con (as there) such that $A_K(\omega) \approx \{\tau \in \mathscr{G}(L(K)^e | \mathrm{Res}_L \tau \in \mathrm{Con}\}$ (in particular $A_K(\omega)$ is measurable). Conversely, for every finite Galois extension L/K and a conjugacy domain $\mathrm{Con} \subseteq \mathscr{G}(L/K)^e$ there is a Galois sentence $[\mathrm{Ar} \subseteq \mathrm{Con}(\mathscr{A})]$, where $\mathscr{A} = \langle A^\circ, C \to A^\circ, \mathrm{Con} \rangle$ such that $K[C] = L$, hence by Lemma 1. 4 there is a bounded sentence $\omega \in \mathscr{L}_e(K)$ with $A_K(\omega) = \{\tau \in G(K)^e | \mathrm{Res}_L \tau \in \mathrm{Con}\}$.

If $\theta' \in T'$, we obtain by Lemma 1. 2 the same characterization of $A_K(\theta\cdot)$; however, from [2], Theorem 3. 8 we see that Con also satisfies the following condition:

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

Conversely, from [2], Cor. 3. 9. it follows that for every finite Galois extension and a conjugacy domain $\mathrm{Con} \subseteqq \mathscr{G}(L/K)^e$ satisfying this condition there is a sentence $\theta \in \mathscr{L}(K)$ such that

$$A_K(\theta') \approx \{\sigma \in G(K)^e \mid \mathrm{Res}_L \sigma \in \mathrm{Con}\}.$$

Now K, as a Hilbertian field, certainly possesses a cyclic extension L of degree >2 (cf. [3], Lemma 4. 3). Let τ_1, τ'_1 be two distinct generators of $\mathscr{G}(L/K)$, and let $\mathrm{Con} = \{(\tau_1, \mathrm{id}, \ldots, \mathrm{id})\}$. Then

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

Hence the Corollary follows by the characterization above. (E.g., if $K = \mathbb{Q}$, put ω to be

$$(\exists^4 X)\,[X^4 + X^3 + X^2 + X + 1 = 0 \wedge \Sigma_1 X = X^2].) \qquad \blacksquare$$

2. The transfer principle

Let R be an integrally closed integral domain with a quotient field K. The treatment of models $\mathscr{M}(K)$ 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 $V \subseteqq \mathbb{A}^n$ 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 $\varphi: R \to \bar{R}$ 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 $\mathbb{A}^n$.

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

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

---

[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 $\mathbb{Z}[A_1] = \mathbb{Z}[2i]$ differs from $\mathbb{Z}[A_2] = \mathbb{Z}[2i, 2^{-1}] = \mathbb{Z}[i]$. Moreover: A_2 is $\mathbb{Z}$-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 $\mathbb{Z}$, 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 $\mathbb{Z}$ (cf. [5], p. 89).

The sets A^φ, $\bar{A}^\varphi$ are not necessarily equal. However, one may show, that there is a constant $0 \neq \gamma \in R$, such that $A^\varphi = \bar{A}^\varphi$, whenever $\varphi(\gamma) \neq 0$. Furthermore, by [2], Cor. 2. 9, γ may be chosen such that if $\varphi(\gamma) \neq 0$ then: A^φ is also a non-empty set; it has the same number of components over $\tilde{K}$ as V has over $\tilde{K}$; given another R-normal set B, then $B^\varphi \subseteq A^\varphi$ iff $B \subseteq A$ (of course, γ depends on B too).

Following this idea one may generalize the theory of Galois stratification: Let $C \xrightarrow{\varphi} A$ 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 $R[A]$, $\mathrm{discr}_{K(A)} z \in R[A]^\times$) and let $a \in A^\varphi(M)$, where M is a field extension of $\bar{K}$. Then $R \xrightarrow{\varphi} \bar{R} \hookrightarrow M$ can be extended to a map $\rho_0 : R[A] \to M[a] = M$, and its extension $\rho : R[C] \to \tilde{M}$ induces a group homomorphism $\rho^* : G(M) \to \mathcal{G}(C/A) = \mathcal{G}(K(C)/K(A))$. This ρ^* 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 θ be a bounded sentence in $\mathcal{L}_e(R)$. Then one can find — effectively, if R is presented — a Galois sentence ψ (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*

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

If $M = F(\sigma)$ is a Čebotarev field, one can find a quantifier free Galois sentence ψ_0 and $0 \neq \gamma' \in R$ such that if $\varphi(\gamma') \neq 0$, then

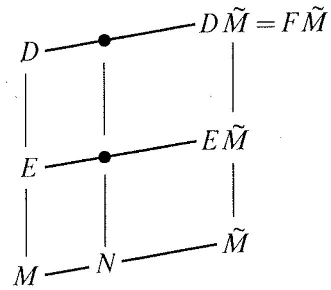
$$(F, \sigma) \models \psi \Leftrightarrow (F, \sigma) \models \psi_0.$$

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 $C' \to A'$ over M, whose Čebotarev property is actually used in the proof of: $(M, \sigma) \models \psi \leftrightarrow \psi_0$ (see [2], Lemma 3. 1). In all of these covers $A' \underset{M}{\cong} \mathbb{A}^1 - V(g)$ with $g \in M[Y]$ and $\deg g$ and $\deg C'$ are bounded by some constant dependent on the sentence ψ.

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

Theorem 2. 2. *Let $d \geqq 1$ and let M be a field with q elements, $q > d^4$. Let $A = \mathbb{A}^1 - V(g)$, where $g \in M[Y]$, $\deg g < d$, and let $C \to A$ be a Galois cover with $\deg C \leqq d$. Denote $N = \tilde{M} \cap M(C)$. If an element $\tau \in \mathcal{G}(C/A)$ satisfies $\mathrm{Res}_N \tau = \mathrm{Res}_N \Phi_M$, then there exists an M-homomorphism $\rho : M[C] \to \tilde{M}$ 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 τ to a unique element $\tilde{\tau}\in\mathcal{G}(F\tilde{M}/E)$ such that $\mathrm{Res}_{\tilde{M}}\,\tau=\Phi_M$. Let $D=F\tilde{M}(\tilde{\tau})$. Since the map $\mathrm{Res}_{\tilde{M}}:\mathcal{G}(F\tilde{M}/D)\to G(M)$ maps a generator $\tilde{\tau}$ on a generator Φ_M and since $G(M)=\mathcal{G}(\tilde{M}/M)\cong\hat{\mathbb{Z}}$, it is clearly an isomorphism. Hence D and $\tilde{M}$ are linearly disjoint over M, whence D/M is regular and $[D:E]=[F\tilde{M}:E\tilde{M}]\leqq[F:E]\leqq d$; also $D\tilde{M}=F\tilde{M}$.



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

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

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

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

Now

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

hence

$$n\geqq(q+1)-2g(D)\sqrt{q}\geqq(q+1)-(d-1)^2\sqrt{q}=1+\sqrt{q}\,[\sqrt{q}-(d-1)^2]\geqq 1+\sqrt{q}\geqq 1+d^2.$$

Thus there are at least d^2+1 M-rational places of D. There are also at most $(1+\deg g)\leqq d$ non-equivalent places of E, which are not finite on $M[A]$; each of them has at most $[D:E]\leqq d$ 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 $\mathrm{Res}_{\tilde{M}}\,\tilde{\rho}=\mathrm{id}$ and denote $\rho=\mathrm{Res}_{M[C]}\tilde{\rho}$. 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 $x\in M[C]\subseteqq D\tilde{M}$ 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 θ be a bounded sentence in $\mathscr{L}_1(R)$. By Theorem 2. 1 find the corresponding equivalent Galois sentence ψ_0 with no quantifiers. Thus by Theorem 2. 2 there is a finite Galois extension L/K and a conjugacy domain Con in $\mathscr{G}(L/K)$ 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

$$(\tilde{M}, \Phi_M) \models \theta \Leftrightarrow \left(\frac{L/K}{p}\right) \in \mathrm{Con}.$$

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

$$(\tilde{M}, \sigma) \models \theta \Leftrightarrow \mathrm{Res}_L \sigma \in \mathrm{Con}.$$

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 θ be a bounded sentence in $\mathscr{L}_1(R)$. Then:*

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

$(\tilde{\mathbb{F}}_P, \Phi_{\mathbb{F}_P}) \models \theta$ for almost all primes P in R (i.e., except for a finite subset of them) $\Leftrightarrow$

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

2.) *Let $A(\theta) = \{\sigma \in G(K) \mid (\tilde{K}, \sigma) \models \theta\}$, $B(\theta) = \{0 \neq P \in \mathrm{Spec}\,(R) \mid (\tilde{\mathbb{F}}_P, \Phi_{\mathbb{F}_P}) \models \theta\}$.*

Then $A(\theta)$ is μ-measurable, $B(\theta)$ has a Dirichlet density δ and $\mu(A(\theta)) = \delta(B(\theta))$ = a rational number in $[0, 1]$.

References

[1] *M. Fried*, On Hilbert's irreducibility theorem, J. Number Theory **6** (1974), 211—231.

[2] *M. Fried, D. Haran* and *M. Jarden*, Galois stratification over Frobenius fields, Advances in Mathematics to appear.

[3] *M. Fried* and *M. Jarden*, Diophantine properties of subfields of $\mathbb{Q}$, Amer. J. Math. **100** (1978), 653—666.

[4] *M. Fried* and *G. Sacerdote*, Solving diophantine problems over all residue class fields of a number field and all finite fields, Ann. Math. **104** (1976), 203—233.

[5] *R. Hartshorne*, Algebraic geometry, Berlin-Heidelberg-New York 1977.

[6] *M. Jarden*, Elementary statements over large algebraic fields, Trans. AMS **164** (1972), 67—91.

[7] *M. Jarden* and *U. Kiehne*, The elementary theory of algebraic fields of finite corank, Invent. math. **30** (1975), 275—294.

[8] *S. Lang*, Algebra, Reading, Mass., 1974.

[9] *P. Samuel*, Lectures on old and new results on algebraic curves, Bombay 1966.

[10] *O. Zariski* and *P. Samuel*, Commutative Algebra. I, Princeton 1959.