Geometry & Topology Monographs
Volume 3: Invitation to higher local fields
Part II, section 7, pages 273–279

# 7. Recovering higher global and local fields from Galois groups — an algebraic approach

*Ido Efrat*

## 7.0. Introduction

We consider the following general problem: let $F$ be a known field with absolute Galois group $G_F$. Let $K$ be a field with $G_K \simeq G_F$. What can be deduced about the arithmetic structure of $K$?

As a prototype of this kind of questions we recall the celebrated Artin–Schreier theorem: $G_K \simeq G_{\mathbb{R}}$ if and only if $K$ is real closed. Likewise, the fields $K$ with $G_K \simeq G_E$ for some finite extension $E$ of $\mathbb{Q}_p$ are the $p$-adically closed fields (see [Ne], [P1], [E1], [K]). Here we discuss the following two cases:

1. *$K$ is a higher global field*
2. *$K$ is a higher local field*

## 7.1. Higher global fields

We call a field *finitely generated* (or a *higher global field*) if it is finitely generated over its prime subfield. The (proven) 0-dimensional case of Grothendieck's anabelian conjecture ([G1], [G2]) can be stated as follows:

*Let $K, F$ be finitely generated infinite fields. Any isomorphism $G_K \simeq G_F$ is induced in a functorial way by an (essentially unique) isomorphism of the algebraic closures of $K$ and $F$.*

This statement was proven:
- by Neukirch [Ne] for finite normal extensions of $\mathbb{Q}$;
- by Iwasawa (unpublished) and Uchida [U1–3] (following Ikeda [I]) for all global fields;
- by Pop [P2] and Spiess [S] for function fields in one variable over $\mathbb{Q}$;

*Published 10 December 2000:* 

- by Pop ([P3–5]) in general.

For recent results on the 1-*dimensional* anabelian conjecture – see the works of Mochizuki [M], Nakamura [N] and Tamagawa [T].

## 7.2. Earlier approaches

Roughly speaking, the above proofs in the 0-dimensional case are divided into a local part and a global part. To explain the local part, define the Kronecker dimension $\dim(K)$ of a field $K$ as $\mathrm{trdeg}(K/\mathbb{F}_p)$ if $\mathrm{char}(K) = p > 0$, and as $\mathrm{trdeg}(K/\mathbb{Q}) + 1$ if $\mathrm{char}(K) = 0$. Now let $v$ be a Krull valuation on $K$ (not necessarily discrete or of rank 1) with residue field $\overline{K}_v$. It is called 1-*defectless* if $\dim K = \dim \overline{K}_v + 1$. The main result of the local theory is the following *local correspondence*: given an isomorphism $\varphi: G_K \xrightarrow{\sim} G_F$, a closed subgroup $Z$ of $G_K$ is the decomposition group of some 1-defectless valuation $v$ on $K$ if and only if $\varphi(Z)$ is the decomposition group of some 1-defectless valuation $v'$ on $F$. The 'global theory' then combines the isomorphisms between the corresponding decomposition fields to construct the desired isomorphism of the algebraic closures (see [P5] for more details).

The essence of the local correspondence is clearly the detection of valuations on a field $K$ just from the knowledge of the group-theoretic structure of $G_K$. In the earlier approaches this was done by means of various *Hasse principles*; i.e., using the injectivity of the map

$$H(K) \to \prod_{v \in S} H(K_v^h)$$

for some cohomological functor $H$ and some set $S$ of non-trivial valuations on $K$, where $K_v^h$ is the henselization of $K$ with respect to $v$. Indeed, if this map is injective and $H(K) \neq 0$ then $H(K_v^h) \neq 0$ for at least one $v \in S$. In this way one finds "arithmetically interesting" valuations on $K$.

In the above-mentioned works the local correspondence was proved using known Hasse principles for:

(1) Brauer groups over global fields (Brauer, Hasse, Noether);
(2) Brauer groups over function fields in one variable over local fields (Witt, Tate, Lichtenbaum, Roquette, Sh. Saito, Pop);
(3) $H^3(G_K, \mathbb{Q}/\mathbb{Z}(2))$ over function fields in one variable over $\mathbb{Q}$ (Kato, Jannsen).

Furthermore, in his proof of the 0-dimensional anabelian conjecture in its general case, Pop uses a *model-theoretic* technique to transfer the Hasse principles in (2) to a more general context of conservative function fields in one variable over certain henselian valued fields. More specifically, by a deep result of Kiesler–Shelah, a property is elementary in a certain language (in the sense of the first-order predicate calculus) if and only if it is preserved by isomorphisms of models in the language, and both the property and its negation are preserved by nonprincipal ultrapowers. It turns out that in an appropriate setting, the Hasse principle for the Brauer groups satisfies these conditions, hence has an elementary nature. One can now apply model-completeness results on tame valued fields by F.-V. Kuhlmann [Ku].

This led one to the problem of finding an *algebraic* proof of the local correspondence, i.e., a proof which does not use non-standard arguments (see [S, p. 115]; other model-theoretic techniques which were earlier used in the global theory of [P2] were replaced by Spiess in [S] by algebraic ones).

We next explain how this can indeed be done (see [E3] for details and proofs).

## 7.3. Construction of valuations from $K$-theory

Our algebraic approach to the local correspondence is based on a $K$-theoretic (yet elementary) construction of valuations, which emerged in the early 1980's in the context of quadratic form theory (in works of Jacob [J], Ware [W], Arason–Elman–Jacob [AEJ], Hwang–Jacob [HJ]; see the survey [E2]). We also mention here the alternative approaches to such constructions by Bogomolov [B] and Koenigsmann [K]. The main result of (the first series of) these constructions is:

**Theorem 1.** *Let $p$ be a prime number and let $E$ be a field. Assume that* $\mathrm{char}(E) \neq p$ *and that $\langle -1, E^{*p}\rangle \leqslant T \leqslant E^*$ is an intermediate group such that:*

(a) *for all $x \in E^* \setminus T$ and $y \in T \setminus E^{*p}$ one has $\{x, y\} \neq 0$ in $K_2(E)$*

(b) *for all $x, y \in E^*$ which are $\mathbb{F}_p$-linearly independent mod $T$ one has $\{x, y\} \neq 0$ in $K_2(E)$.*

*Then there exists a valuation $v$ on $E$ with value group $\Gamma_v$ such that:*

(i) $\mathrm{char}(\overline{E}_v) \neq p$;

(ii) $\dim_{\mathbb{F}_p}(\Gamma_v/p) \geqslant \dim_{\mathbb{F}_p}(E^*/T) - 1$;

(iii) *either* $\dim_{\mathbb{F}_p}(\Gamma_v/p) = \dim_{\mathbb{F}_p}(E^*/T)$ *or* $\overline{E}_v \neq \overline{E}_v^p$.

In particular we have:

**Corollary.** *Let $p$ be a prime number and let $E$ be a field. Suppose that* $\mathrm{char}(E) \neq p$, $-1 \in E^{*p}$, *and that the natural symbolic map induces an isomorphism*

$$\wedge^2(E^*/E^{*p}) \xrightarrow{\sim} K_2(E)/p.$$

*Then there is a valuation $v$ on $E$ such that*

(i) $\mathrm{char}(\overline{E}_v) \neq p$;

(ii) $\dim_{\mathbb{F}_p}(\Gamma_v/p) \geqslant \dim_{\mathbb{F}_p}(E^*/E^{*p}) - 1$;

(iii) *either* $\dim_{\mathbb{F}_p}(\Gamma_v/p) = \dim_{\mathbb{F}_p}(E^*/E^{*p})$ *or* $\overline{E}_v \neq \overline{E}_v^p$.

We remark that the construction used in the proof of Theorem 1 is of a completely explicit and elementary nature. Namely, one chooses a certain intermediate group $T \leqslant H \leqslant E^*$ with $(H:T)|p$ and denotes

$$O^- = \{x \in E \setminus H \ : \ 1 - x \in T\}, \qquad O^+ = \{x \in H \ : \ xO^- \subset O^-\}.$$

It turns out that $O = O^- \cup O^+$ is a valuation ring on $E$, and the corresponding valuation $v$ is as desired.

The second main ingredient is the following henselianity criterion proven in [E1]:

**Proposition 1.** *Let $p$ be a prime number and let $(E, v)$ be a valued field with* $\operatorname{char}(\overline{E}_v) \neq p$, *such that the maximal pro-$p$ Galois group $G_{\overline{E}_v}(p)$ of $\overline{E}_v$ is infinite. Suppose that*

$$\sup_{E'} \operatorname{rk}(G_{E'}(p)) < \infty$$

*with $E'$ ranging over all finite separable extensions of $E$. Then $v$ is henselian.*

Here the *rank* $\operatorname{rk}(G)$ of a profinite group $G$ is its minimal number of (topological) generators.

After translating the Corollary to the Galois-theoretic language using Kummer theory and the Merkur'ev–Suslin theorem and using Proposition 1 we obtain:

**Proposition 2.** *Let $p$ be a prime number and let $E$ be a field such that* $\operatorname{char}(E) \neq p$. *Suppose that for every finite separable extension $E'$ of $E$ one has*
(1) $H^1(G_{E'}, \mathbb{Z}/p) \simeq (\mathbb{Z}/p)^{n+1}$;
(2) $H^2(G_{E'}, \mathbb{Z}/p) \simeq \wedge^2 H^1(G_{E'}, \mathbb{Z}/p)$ *via the cup product;*
(3) $\dim_{\mathbb{F}_p}(\Gamma_u/p) \leqslant n$ *for every valuation $u$ on $E'$.*

*Then there exists a henselian valuation $v$ on $E$ such that* $\operatorname{char}(\overline{E}_v) \neq p$ *and* $\dim_{\mathbb{F}_p}(\Gamma_v/p) = n$.

## 7.4. A Galois characterization of 1-defectless valuations

For a field $L$ and a prime number $p$, we recall that the virtual $p$-cohomological dimension $\operatorname{vcd}_p(G_L)$ is the usual $p$-cohomological dimension $\operatorname{cd}_p(G_L)$ if $\operatorname{char}(L) \neq 0$ and is $\operatorname{vcd}_p(G_{L(\sqrt{-1})})$ if $\operatorname{char}(L) = 0$.

**Definition.** Let $p$ be a prime number and let $L$ be a field with $n = \dim L < \infty$ and $\operatorname{char}(L) \neq p$. We say that $L$ is *$p$-divisorial* if there exist subfields $L \subset E \subset M \subset L^{\mathrm{sep}}$ such that
(a) $M/L$ is Galois;
(b) every $p$-Sylow subgroup of $G_M$ is isomorphic to $\mathbb{Z}_p$;
(c) the virtual $p$-cohomological dimension $\operatorname{vcd}_p(G_L)$ of $G_L$ is $n+1$;

(d) either $n = 1$ or $\mathrm{Gal}(M/L)$ has no non-trivial closed normal pro-soluble subgroups;
(e) for every finite separable extension $E'/E$ one has

$$H^1(G_{E'}, \mathbb{Z}/p) \simeq (\mathbb{Z}/p)^{n+1}, \quad H^2(G_{E'}, \mathbb{Z}/p) \simeq \wedge^2 H^1(G_{E'}, \mathbb{Z}/p)$$

via the cup product.

The main result is now:

**Theorem 2** ([E3]). *Let $p$ be a prime number and let $K$ be a finitely generated field of characteristic different from $p$. Let $L$ be an algebraic extension of $K$. Then the following conditions are equivalent:*
(i) *there exists a 1-defectless valuation $v$ on $K$ such that $L = K_v^h$;*
(ii) *$L$ is a minimal $p$-divisorial separable algebraic extension of $K$.*

*Idea of proof.* Suppose first that $v$ is a 1-defectless valuation on $K$. Take $L = K_v^h$ and let $M$ be a maximal unramified extension of $L$. Also let $w$ be a valuation on $K$ such that $\Gamma_w \simeq \mathbb{Z}^{\dim(K)}$, $\mathrm{char}(\overline{K}_w) \neq p$, and such that the corresponding valuation rings satisfy $\mathcal{O}_w \subset \mathcal{O}_v$. Let $K_w^h$ be a henselization of $(K, w)$ containing $L$ and take $E = K_w^h(\mu_p)$ ($E = K_w^h(\mu_4)$ if $p = 2$). One shows that $L$ is $p$-divisorial with respect to this tower of of extensions.

Conversely, suppose that $L$ is $p$-divisorial, and let $L \subset E \subset M \subset L^{\mathrm{sep}}$ be a tower of extensions as in the definition above. Proposition 2 gives rise to a henselian valuation $w$ on $E$ such that $\mathrm{char}(\overline{E}_w) \neq p$ and $\dim_{\mathbb{F}_p}(\Gamma_w/p) = \dim(K)$. Let $w_0$ be the unique valuation on $E$ of rank 1 such that $\mathcal{O}_{w_0} \supset \mathcal{O}_w$, and let $u$ be its restriction to $L$. The unique extension $u_M$ of $w_0$ to $M$ is henselian. Since $M/L$ is normal, every extension of $u$ to $M$ is conjugate to $u_M$, hence is also henselian. By a classical result of F.-K. Schmidt, the non-separably closed field $M$ can be henselian with respect to at most one valuation of rank 1. Conclude that $u$ is henselian as well. One then shows that it is 1-defectless.

The equivalence of (i) and (ii) now follows from these two remarks, and a further application of F.-K. Schmidt's theorem.

The local correspondence now follows from the observation that condition (ii) of the Theorem is actually a condition on the closed subgroup $G_L$ of the profinite group $G_K$ (note that $\dim(L) = \mathrm{vcd}(G_K) - 1$).

## 7.5. Higher local fields

Here we report on a joint work with Fesenko [EF].

An analysis similar to the one sketched in the case of higher global fields yields:

**Theorem 3** ([EF]). *Let $F$ be an $n$-dimensional local field. Suppose that the canonical valuation on $F$ of rank $n$ has residue characteristic $p$. Let $K$ be a field such that $G_K \simeq G_F$. Then there is a henselian valuation $v$ on $K$ such that $\Gamma_v/l \simeq (\mathbb{Z}/l)^n$ for every prime number $l \neq p$ and such that $\mathrm{char}\,(\overline{K}_v) = p$ or $0$.*

**Theorem 4** ([EF]). *Let $q = p^r$ be a prime power and let $K$ be a field with $G_K \simeq G_{\mathbb{F}_q((t))}$. Then there is a henselian valuation $v$ on $K$ such that*
(1) $\Gamma_v/l \simeq \mathbb{Z}/l$ *for every prime number* $l \neq p$*;*
(2) $\mathrm{char}\,(\overline{K}_v) = p$*;*
(3) *the maximal prime-to-$p$ Galois group $G_{\overline{K}_v}(p')$ of $\overline{K}_v$ is isomorphic to $\prod_{l\neq p} \mathbb{Z}_l$;*
(4) *if $\mathrm{char}\,(K) = 0$ then $\Gamma_v = p\Gamma_v$ and $\overline{K}_v$ is perfect.*

Moreover, for every positive integer $d$ there exist valued fields $(K, v)$ as in Theorem 4 with characteristic $p$ and for which $\Gamma_v/p \simeq (\mathbb{Z}/p)^d$. Likewise there exist examples with $\Gamma_v \simeq \mathbb{Z}$, $G_{\overline{K}_v} \not\simeq \hat{\mathbb{Z}}$ and $\overline{K}_v$ imperfect, as well as examples with $\mathrm{char}\,(K) = 0$.

## References


[AEJ] J. K. Arason, R. Elman and B. Jacob, Rigid elements, valuations, and realization of Witt rings, J. Algebra 110 (1987), 449–467.

[B] F. A. Bogomolov, Abelian subgroups of Galois groups, Izv. Akad. Nauk SSSR, Ser. Mat. 55 (1991), 32–67; English translation in Math. USSR Izvest. 38 (1992), 27–67.

[E1] I. Efrat, A Galois-theoretic characterization of $p$-adically closed fields, Isr. J. Math. 91 (1995), 273–284.

[E2] I. Efrat, Construction of valuations from $K$-theory, Math. Research Letters 6 (1999), 335–344.

[E3] I. Efrat, The local correspondence over absolute fields – an algebraic approach, Internat. Math. Res. Notices, to appear.

[EF] I. Efrat and I. Fesenko, Fields Galois-equivalent to a local field of positive characteristic, Math. Research Letters 6 (1999), 245–356.

[G1] A. Grothendieck, Esquisse d'un program, In: L. Schneps et al. (Eds.), Geometric Galois actions. 1. Around Grothendieck's esquisse d'un programme, Cambridge: Cambridge University Press, Lond. Math. Soc. Lect. Note Ser. 242, 5–48 (1997).

[G2] A. Grothendieck, A letter to G. Faltings, In: L. Schneps et al. (Eds.), Geometric Galois actions. 1. Around Grothendieck's esquisse d'un programme, Cambridge: Cambridge University Press, Lond. Math. Soc. Lect. Note Ser. 242, 49–58 (1997).

[HJ] Y. S. Hwang and B. Jacob, Brauer group analogues of results relating the Witt ring to valuations and Galois theory, Canad. J. math. 47 (1995), 527–543.

[I] M. Ikeda, Completeness of the absolute Galois group of the rational number field, J. reine angew. Math. 291 (1977), 1–22.

[J] B. Jacob, On the structure of pythagorean fields, J. Algebra 68 (1981), 247–267.

[K] J. Koenigsmann, From $p$-rigid elements to valuations (with a Galois-characterisation of $p$-adic fields) (with an appendix by F. Pop), J. reine angew. Math. 465 (1995), 165–182.

[Ku] F.-V. Kuhlmann, Henselian function fields and tame fields, Heidelberg, 1990.

[M] S. Mochizuki, The local pro-$p$ anabelian geometry of curves, Invent. math. 138 (1999), 319–423.

[N] H. Nakamura, Galois rigidity of the étale fundamental groups of the punctured projective line, J. reine angew. Math. 411 (1990), 205–216.

[Ne] J. Neukirch, Kennzeichnung der $p$-adischen und endlichen algebraischen Zahlkörper, Invent. math. 6 (1969), 269–314.

[P1] F. Pop, Galoissche Kennzeichnung $p$-adisch abgeschlossener Körper, J. reine angew. Math. 392 (1988), 145–175.

[P2] F. Pop, On the Galois theory of function fields of one variable over number fields, J. reine angew. Math. 406 (1990), 200–218.

[P3] F. Pop, On Grothendieck's conjecture of birational anabelian geometry, Ann. Math. 139 (1994), 145–182.

[P4] F. Pop, On Grothendieck's conjecture of birational anabelian geometry II, Preprint, Heidelberg 1995.

[P5] F. Pop, Alterations and birational anabelian geometry, In: Resolution of singularities (Obergurgl, 1997), 519–532, Progr. Math. 181, Birkhauser, Basel, 2000.

[S] M. Spiess, An arithmetic proof of Pop's theorem concerning Galois groups of function fields over number fields, J. reine angew. Math. 478 (1996), 107–126.

[T] A. Tamagawa, The Grothendieck conjecture for affine curves, Compositio Math. 109 (1997), 135–194.

[U1] K. Uchida, Isomorphisms of Galois groups of algebraic function fields, Ann. Math. 106 (1977), 589–598.

[U2] K. Uchida, Isomorphisms of Galois groups of solvably closed Galois extensions, Tohôku Math. J. 31 (1979), 359–362.

[U3] K. Uchida, Homomorphisms of Galois groups of solvably closed Galois extensions, J. Math. Soc. Japan 33 (1981), 595–604.

[W] R. Ware, Valuation rings and rigid elements in fields, Canad. J. Math. 33 (1981), 1338–1355.

*Department of Mathematics, Ben Gurion University of the Negev*
*P.O. Box 653, Be'er-Sheva 84105 Israel*
*E-mail: efrat@math.bgu.ac.il*