ISRAEL JOURNAL OF MATHEMATICS, Vol. 30, No. 4, 1978

GALOIS GROUPS OF INTERSECTIONS OF LOCAL FIELDS

BY

WULF-DIETER GEYER

ABSTRACT

Let K be a denumerable Hilbertian field with separable algebraic closure $\bar{K}$ and Galois group $\mathfrak{G}_K = \mathrm{Gal}(\bar{K} \mid K)$, let $w_1, \cdots, w_n$ be absolute values on $\bar{K}$. Then for almost all $\sigma \in \mathfrak{G}_K^n$ (in the sense of Haar measure) there are no relations between the decomposition groups $\mathfrak{G}_K(w_1\sigma_1), \cdots, \mathfrak{G}_K(w_n\sigma_n)$ of the absolute values $w_1\sigma_1, \cdots, w_n\sigma_n$, i.e. the subgroup of $\mathfrak{G}_K$ generated by these groups is the free product of these groups.

§1. Galois groups

1.1. Let K be a (commutative) field. Then $\bar{K}$ denotes the separable algebraic closure of K and $\mathfrak{G}_K = \mathrm{Gal}(\bar{K} \mid K)$ the (*absolute*) *Galois group* of K, which is compact under Krull's topology. As a compact group $\mathfrak{G}_K$ carries a unique *Haar measure*. Exploring the existence of certain classes of fields this Haar measure has first been used in [9]. A main tool in Jarden's investigations is the following lemma 4.1 in [10].

LEMMA 1.1. *Let $(N_j \mid K)_{j \in \mathbf{N}}$ be a linear disjoint sequence of finite Galois extensions of the same degree over K. For each j let A_j be a nonempty subset of* $\mathrm{Gal}(N_j \mid K)^n$. *Then*

$$\{\sigma \in \mathfrak{G}_K^n; \exists j \in \mathbf{N} : \sigma \mid N_j \in A_j\}$$

is a set of measure 1 *in* $\mathfrak{G}_K^n$.

1.2. Let $L_1, \cdots, L_n$ be fields between K and $\bar{K}$, let $L = \bigcap_i L_i$ be their intersection. Then the Galois group $\mathfrak{G}_L$ is generated in the topological sense by the subgroups $\mathfrak{G}_{L_i} = \mathfrak{G}_i$ $(i = 1, \cdots, n)$. By the universal property of the free product (which is meant in the category of profinite groups, cf. [13]) there is a canonical surjective homomorphism

Received August 28, 1977

$$\varphi : \mathfrak{G}_1 * \cdots * \mathfrak{G}_n \to \mathfrak{G}_L$$

induced by the injections $\mathfrak{G}_i \to \mathfrak{G}_L$. To see that φ is an isomorphism one has to use the following criterion for free products of profinite groups.

LEMMA 1.2. *φ is injective iff for every system $G_1, \cdots, G_n$ of finite factor groups of $\mathfrak{G}_1, \cdots, \mathfrak{G}_n$ and for every finite factor group G of the free product $G_1 * \cdots * G_n$ there is a surjective homomorphism*

$$\phi : \mathfrak{G}_L \to G$$

such that $\phi\varphi$ is the canonical map

$$\mathfrak{G}_1 * \cdots * \mathfrak{G}_n \to G_1 * \cdots * G_n \to G.$$

It is enough to know this for large factors G_i resp. G, e.g. we assume always that the induced maps $G_i \to G$ are injective.

Lemma 1.2 is easily established. If φ would not be injective, there is an element $\alpha \neq 1$ in $\mathfrak{G}_1 * \cdots * \mathfrak{G}_n$ such that $\varphi(\alpha) = 1$. Now, by the definition of profinite groups, there are finite factor groups $G_1, \cdots, G_n$ of $\mathfrak{G}_1, \cdots, \mathfrak{G}_n$ and a finite factor group G of $G_1 * \cdots * G_n$ such that the image of α under the canonical map

$$\mathfrak{G}_1 * \cdots * \mathfrak{G}_n \to G_1 * \cdots * G_n \to G$$

is nontrivial. But then this canonical map cannot factor through φ.

1.3. The purpose of this paper is to show that under certain assumptions certain subgroups of $\mathfrak{G}_K$ generate free products. The criterion 1.2 for arbitrary profinite groups can be translated in the case of Galois groups in the following way: A factor group G of $\mathfrak{G}_K$ is the Galois group of a normal field extension $N \mid K$ and conversely. If G is finite and $\bar{\varphi} : G \hookrightarrow \mathfrak{S}_d$ is a realization of G as group of permutations, there is a separable polynomial $f \in K[X]$ of degree d with splitting field N over K such that $(G, \bar{\varphi})$ is the Galois group of f over K (if K is infinite which is the case in this paper). The same argument holds for the factor groups G_i of $\mathfrak{G}_i$, and every factor group $G_1 * \cdots * G_n \to G$ such that $G_i \to G$ is injective can be realized by representations $G_i \hookrightarrow \mathfrak{S}_d$, such that G is the group generated by the G_i in $\mathfrak{S}_d$. Therefore we get the following translated criterion for freeness:

LEMMA 1.3. *φ is injective iff for any $d \in \mathbf{N}$ and any set $f_1, \cdots, f_n$ of separable polynomials of degree d with $f_i \in L_i[X]$ and $\mathrm{Gal}(f_i \mid L_i) = G_i \subset \mathfrak{S}_d$ for $i = 1, \cdots, n$, there is a separable polynomial $f \in L[X]$ of degree d such that f has the*

same splitting field over L_i as f_i and $\mathrm{Gal}(f \mid L_i) = G_i$ *for* $i = 1, \cdots, n$ *simultaneously.*

Then automatically $\mathrm{Gal}(f \mid L)$ is generated by the subgroups $G_1, \cdots, G_n$ of $\mathfrak{S}_d$ because $L = L_1 \cap \cdots \cap L_n$. The difficulty in applying this criterion lies in the fact that $\mathrm{Gal}(f \mid L_i) = G_i$ should hold in one numeration of the roots of f simultaneously for all $i = 1, \cdots, n$, while for each i only the conjugacy class of $\mathrm{Gal}(f \mid L_i)$ in $\mathfrak{S}_d$ is well determined. This is the reason why the application of Lemma 1.3 in this paper will only give results for "almost all" cases in the measure-theoretic sense.

§2. Absolute values

2.1. An *absolute value* on K is a nontrivial homomorphism

$$v : K^\times \to \mathbf{R}_>^\times$$

of the multiplicative group of K into the multiplicative group of the positive real numbers with the property

$$v(a+b) \leqq v(a) + v(b) \qquad \text{if } a, b \in K,$$

where as usual $v(0) = 0$ by definition. Such an absolute value v has extensions to $\bar{K}$ and all such extensions are conjugate under $\mathfrak{G}_K$, cf. [3], §§2 and 14.

If w is some extension of v, let

$$\mathfrak{G}_K(w) = \{\sigma \in \mathfrak{G}_K;\ w\sigma = w\}$$

be the *decomposition group* of w over K. Then the fixed field of $\mathfrak{G}_K(w)$ in $\bar{K}$ is called the decomposition field or *Henselization* K_w of K with respect to w. Henselizations of K with respect to different extensions are again conjugate under $\mathfrak{G}_K$.

2.2. Every absolute value v on K induces a *metric* d on K by $d(x, y) = v(x - y)$. The Henselization of a field K with respect to an absolute value w of $\bar{K}$ can also be seen (cf. [3], §17) as the separable algebraic part of the completion of K with respect to w, i.e. one has

$$K_w = \{x \in \bar{K};\ \forall \varepsilon > 0 \quad \exists y \in K : w(x - y) < \varepsilon\}.$$

In contrast to this fact that the extension $K_w \mid K$ is very rigid from a topological point of view, the extension $\bar{K} \mid K_w$ is topologically soft in the sense of (cf. [1], 2.6)

(Krasner's) LEMMA 2.2. *Let $f \in K_w[X]$ be a separable polynomial of degree d. Then there is an $\varepsilon > 0$, such that every polynomial $g \in K_w[X]$ of degree d with $w(f-g) < \varepsilon$ (this is a conjunction of such inequalities between correspondent coefficients of f and g) has the same splitting field and the same Galois group over K_w as f.*

2.3. Two absolute values v and v' on K are called *different*, if they generate different topologies, i.e. if there is no positive constant c such that $v'(x) = v(x)^c$ for $x \in K$. For different absolute values one has the following ([1], 1.4)

(Approximation) LEMMA 2.3. *Let $v_1, \cdots, v_n$ be different absolute values on K, let $a_1, \cdots, a_n$ be elements of K, let $\varepsilon > 0$ be a positive real number, then there is an $a \in K$ such that*

$$v_i(a - a_i) < \varepsilon \qquad \text{for } i = 1, \cdots, n.$$

2.4. Any field K which is not an algebraic extension of a finite field has an infinite number of different absolute values. The arithmetic structure of the algebraic extensions of K, especially the connection between local and global behaviour, depends (cf. [14]) essentially on the question about the relations of different decomposition groups as subgroups of $\mathfrak{G}_K$. Especially one may ask:

QUESTION I. *If $\mathfrak{G}_1, \cdots, \mathfrak{G}_n$ are decomposition groups in $\mathfrak{G}_K$ with respect to absolute values which are different on K, do $\mathfrak{G}_1, \cdots, \mathfrak{G}_n$ generate a free product in $\mathfrak{G}_K$?*

QUESTION I'. *If $v_1, \cdots, v_n$ are different absolute values on K, are there extensions $w_1, \cdots, w_n$ on $\bar{K}$ such that the decomposition groups of $w_1, \cdots, w_n$ generate a free product?*

QUESTION II. *If $w_1, \cdots, w_n$ are absolute values on $\bar{K}$ extending the same absolute value on K, have there to be relations between the decomposition groups of $w_1, \cdots, w_n$?*

Of course one should extend these questions to more than a finite set of absolute values. If e.g. K is the function field of a complex curve (or compact Riemann surface), and if we look only for places on the Riemann surface, i.e. absolute values on K which are trivial on the field $\mathbf{C}$ of constants, then it is well known (cf. e.g. [12], Kor. 4) that (omitting one place in the rational case) the decomposition groups of all places can be chosen in such a way that they generate a free product. Using a Lefschetz principle this can be generalized to algebraic function fields of one variable over an arbitrary algebraically closed

field of characteristic zero, cf. [7], §3 for the case of a rational function field. But until now all proofs use topological and analytical methods, an algebraic proof is still lacking. Another such global result is the decomposition of the Galois group of the maximal p-extension of the $\hat{\mathbf{Z}}_p$-extension of $\mathbf{Q}$ as a free product of the decomposition groups of all places but one, given by Neukirch [14], §11, cf. also [7], §4. But over finite algebraic number fields as $\mathbf{Q}$ such global independence results cannot be expected.

So Neukirch suggested studying the independence of a finite number of decomposition groups. But even then one is unlikely to get good answers for arbitrary fields. E.g. there are infinite number fields K such that there are lots of nontrivial decomposition groups, but $\mathfrak{G}_K$ is "too small" to contain free products. For a certain class of algebraic number fields Globig could answer in his thesis [7], §6 similar questions to those stated above using cohomological methods, but he had to restrict himself to the solvable part of the Galois group $\mathfrak{G}_K$.

In this paper we will attack the questions above without such limitations, using quite different methods. For a certain class of fields, which includes all finitely generated fields, the following answers will be given:

I. yes, in general; I'. yes; II. in general not.

The answer to question II cannot be sharpened to "never", already in the case $K = \mathbf{Q}$. Also the answer to question I is not always "yes"; a counterexample for $K = \mathbf{Q}(\sqrt{2})$ is given in 4.4.

§3. Hilbertian fields

3.1. A field K is called *Hilbertian* (cf. [5]), if to every irreducible polynomial $f \in K[X, Y]$ separable in Y, there is a $\xi \in K$ such that $f(\xi, Y)$ is irreducible in $K[Y]$. This definition differs slightly from the usual one (cf. [11], ch. VIII), because looking at applications we are considering here only separable polynomials. The difference for fields K of prime characteristic is the following: For nonperfect fields both definitions coincide; and whereas perfect fields cannot be Hilbertian by Lang's definition, in the definition given here every purely inseparable extension of an Hilbertian field is again Hilbertian.

If K is Hilbertian, then using the theorem of the primitive element for finite separable field extensions it is easy to see that, given irreducible polynomials $f_1, \cdots, f_r \in K[X_1, \cdots, X_d, Y]$ separable in Y, the $\boldsymbol{\xi}$'s in K^d such that $f_1(\boldsymbol{\xi}, Y), \cdots, f_r(\boldsymbol{\xi}, Y)$ are simultaneously irreducible in $K[Y]$ form a Zariski-dense set in K^d. The intersections of these sets with Zariski open sets in K^d are called *Hilbertian sets* in K^d.

Examples of Hilbertian fields are (finite) algebraic number fields and algebraic function fields.

3.2. Let $f \in K[X, Y]$ be an irreducible polynomial separable in Y, and let $g \in K[X, Y]$ be a Galois resolvent of f over $K(X)$. If $g(\xi, Y)$ is irreducible and remains a Galois resolvent of $f(\xi, Y)$ which is true on a Zariski open set of ξ's, then $f(\xi, Y)$ has over K the same Galois group as $f(X, Y)$ over $K(X)$. This remark was used by Hilbert [8], to construct extension fields of $\mathbf{Q}$ with Galois groups $\mathfrak{S}_n$ and $\mathfrak{A}_n$.

3.3. A finite separable extension L of a Hilbertian field K is again Hilbertian. More precisely, every Hilbertian set in L^d contains a Hilbertian set in K^d, i.e., to each irreducible polynomial $f \in L[X, Y]$ separable in Y, there is an irreducible polynomial $g \in K[X, Y]$ separable in Y, such that for all ξ in a Zariski open set of K^d the following holds: $f(\xi, Y)$ is irreducible in $L[Y]$ if $g(\xi, y)$ is irreducible in $K[Y]$, cf. [11], p. 151.

From this one gets the following lemma 2.2 in [9].

LEMMA 3.3. *Let K be a Hilbertian field, $f \in K[X, Y]$ an irreducible polynomial separable in Y and such that* $\mathrm{Gal}(f \mid \bar{K}(X)) = \mathrm{Gal}(f \mid K(X))$, *then there is a sequence $\xi_i \in K^d$, $i \in \mathbf{N}$, such that all $f(\xi_i, Y)$ are irreducible over K and the sequence of their splitting fields N_i is linearly disjoint over K.*

For by 3.2 we may assume f being Galois and absolutely irreducible. Having constructed $\xi_1, \cdots, \xi_t$ with linear disjoint splitting fields N_i, we consider f as polynomial over $N_1 \cdot \cdots \cdot N_t = N$. By the first statement in this section there is $\xi_{t+1} \in K^d$, such that $f(\xi_{t+1}, Y)$ is irreducible over N. But this means that the splitting field N_{t+1} of $f(\xi_{t+1}, Y)$ over K is linearly disjoint to N.

3.4. Now assume that v is an absolute value on the Hilbertian field K. In [6], lemma 4.1 it is shown that the Hilbertian sets in K^d are dense in the v-topolgoy. More general the following is true:

LEMMA 3.4. *Let K be a Hilbertian field, $v_1, \cdots, v_n$ different absolute values on K. Denote by K_i the field K with the v_i-topology, $i = 1, \cdots, n$. If H is a Hilbertian set in K^d, then the diagonal map*

$$H \to K_1^d \times \cdots \times K_n^d$$

has a dense image.

PROOF. By the Approximation Lemma, the image of K^d in $K_1^d \times \cdots \times K_n^d$ under the diagonal map is dense; moreover for each hypersurface $g = 0$ in K^d,

the open set $\{\xi \in K^d;\ g(\xi) \neq 0\}$ is dense in each K_i^d. Therefore it is enough (using an easy reduction to one polynomial) to show the following:

If $f \in K[X_1, \cdots, X_d, Y]$ is irreducible, separable in Y, if $a \in K^d$ and $\varepsilon > 0$, there is a $\xi \in K^d$ such that $f(\xi, Y)$ is irreducible and $v_i(\xi - a) \leqq \varepsilon$ for $i = 1, \cdots, n$.

By the Approximation Lemma there is a $b \in K^\times$ with $v_i(b) \leqq \varepsilon$ for $i = 1, \cdots, n$. Considering the transformed polynomial $f(a + bX, Y)$ we see: It is enough to prove the above claim for $a = 0$ and $\varepsilon = 1$. We will do this using certain radical extensions of K, so we divide the proof in two parts, corresponding to the characteristic of K.

First suppose $2 \neq 0$ in K. By Lemma 3.3 applied to the polynomial $f = Y^2 - X$, there is an infinite sequence of elements in $K^\times$, we write (t_{kj}) with $k \in \mathbf{N}_0$ and $j = 1, \cdots, d$, which are independent modulo $K^{\times 2}$. Changing the t_{kj} by squares (using the Approximation Lemma) we may assume that the t_{kj} satisfy the following approximation conditions:

If

$$k \equiv \sum_{j=1}^{d} \sum_{i=1}^{n} \varepsilon_{ij} 2^{i-1+n(j-1)} \bmod 2^{nd}, \qquad \varepsilon_{ij} = 0 \text{ or } 1,$$

then

$$v_i(t_{kj}) \leqq 1 \quad \text{if } \varepsilon_{ij} = 0; \qquad v_i(t_{kj}) \geqq \alpha \quad \text{if } \varepsilon_{ij} = 1$$

for all $j = 1, \cdots, d$; $i = 1, \cdots, n$; $k \in \mathbf{N}_0$, where $\alpha = 2 + \sqrt{5}$.

Coming back to our original problem, we consider the transformed polynomials

$$f_k = f((X_1 - t_{k1}x_1^{-1})^{-1}, \cdots, (X_d - t_{kd}X_d^{-1})^{-1}, Y)$$

in $K(X_1, \cdots, X_d)[Y]$ for $k \in \mathbf{N}_0$. For a fixed k we set

$$Z_j = X_j - t_{kj}X_j^{-1} \qquad (j = 1, \cdots, d),$$

so the field extension $K(\boldsymbol{X}) \mid K(\boldsymbol{Z})$ is given by the equations

$$X_j^2 - Z_jX_j - t_{kj} = 0 \qquad (j = 1, \cdots, d)$$

and may be seen geometrically as a 2^d-sheeted covering of the affine d-space by another affine d-space. Looking at the residue extensions above the point $Z_1 = \cdots = Z_d = 0$ we see that all these coverings of the affine $\boldsymbol{Z}$-space are linearly disjoint (with varying k we fix $\boldsymbol{Z}$ and vary $\boldsymbol{X}$!). Now the polynomial $f(Z_1, \cdots, Z_d, Y)$ is irreducible in $K(Z_1, \cdots, Z_d)[Y]$ by assumption, so remains irreducible over almost all members of a linear disjoint family of field extensions of $K(\boldsymbol{Z})$. Therefore nearly all f_k are irreducible in $K(\boldsymbol{X})[Y]$.

Forgetting some indices we may assume that all f_k are irreducible. Now take $\eta \in K^{\times d}$ such that all the polynomials $f_k(\eta, Y)$ with $k < 2^{nd}$ are irreducible over K. Taking $\beta = \frac{1}{2}+\frac{1}{2}\sqrt{5}$ we define for $i = 1, \cdots, n$; $j = 1, \cdots, d$

$$\varepsilon_{ij} = 0 \quad \text{if } v_i(\eta_j) \geqq \beta; \qquad \varepsilon_{ij} = 1 \quad \text{if } v_i(\eta_j) < \beta.$$

If $v_i(\eta) \geqq \beta$ and $v_i(t) \leqq 1$ one has

$$v_i(\eta - t\eta^{-1}) \geqq v_i(\eta) - v_i(t\eta^{-1}) \geqq \beta - \beta^{-1} = 1,$$

if $v_i(\eta) \leqq \beta$ and $v_i(t) \geqq \alpha$ one has

$$v_i(\eta - t\eta^{-1}) \geqq v_i(t\eta^{-1}) - v_i(\eta) \geqq \alpha\beta^{-1} - \beta = 1.$$

Therefore, setting

$$k = \sum_{i,j} \varepsilon_{ij} 2^{i-1+n(j-1)}$$

we have

$$v_i(\eta_j - t_{kj}\eta_j^{-1}) \geqq 1$$

for all $i = 1, \cdots, n$; $j = 1, \cdots, d$, and with

$$\xi_j = (\eta_j - t_{kj}\eta_j^{-1})^{-1}$$

we have

$$v_i(\xi) \leqq 1 \qquad (i = 1, \cdots, n)$$

and $f_k(\eta, Y) = f(\xi, Y)$ is irreducible over K, so the proof of Lemma 3.4 is finished, if K does not have characteristic 2.

If $2 = 0$ in K, we consider the polynomial $f = Y^3 - X$ and get a sequence (t_{kj}) of elements in $K^\times$ which are independent modulo $K^{\times 3}$. Substituting

$$f_k = f(Z_1^{-1}, \cdots, Z_d^{-1}, Y) \qquad (k \in \mathbf{N})$$

with

$$Z_j = X_j - t_{kj}X_j^{-2} \qquad (j = 1, \cdots, d)$$

the proof of the first case goes through also in this case, one has only to change the constants α, β which have now to be defined by $\beta^3 - \beta^2 - 1 = 0$ and $\alpha = 2\beta^2 + 1$.

3.5. A consequence of 3.2, 3.3 and 3.4 is the following proposition, which is one main step in proving our results, and generalizes lemma 3.1 in [10].

PROPOSITION 3.5. *Let K be a Hilbertian field, $v_1, \cdots, v_n$ different absolute values on K and $f_1, \cdots, f_n$ polynomials of degree d in $K[Y]$. Let $\varepsilon > 0$ be a positive real number. Then there is a sequence of polynomials $g_j \in K[Y]$ of degree d such that for all $j \in \mathbf{N}$*

(i) $v_i(g_j - f_i) < \varepsilon$ *for* $i = 1, \cdots, n$,

(ii) $\mathrm{Gal}(g_j \mid K) = \mathfrak{S}_d$,

(iii) *the splitting fields of g_j over K are linearly disjoint.*

PROOF. Consider the general polynomial $f = Y^d + X_1 Y^{d-1} + \cdots + X_d$ in $K[X_1, \cdots, X_d, Y]$. By the theory of symmetric functions we have $\mathrm{Gal}(f \mid K(X)) = \mathrm{Gal}(f \mid \bar{K}(X)) = \mathfrak{S}_d$. Applying the arguments of 3.3 and using the density property given in 3.4 we get the proposition.

§4. Statement of results

4.1. With the definitions of §§1–3 we are now able to state the following main result:

THEOREM 4.1. *Let K be a denumerable Hilbertian field with separable algebraic closure $\bar{K}$ and Galois group $\mathfrak{G}_K$, let $w_1, \cdots, w_n$ be absolute values on $\bar{K}$ (different or not). Then for almost all $\sigma \in \mathfrak{G}_K^n$ the decomposition groups $\mathfrak{G}_K(w_1\sigma_1), \cdots, \mathfrak{G}_K(w_n\sigma_n)$ generate a free product $\mathfrak{G}_K(w_1)^{\sigma_1} * \cdots * \mathfrak{G}_K(w_n)^{\sigma_n}$ in $\mathfrak{G}_K$.*

It should be remarked that in Theorem 4.1 it is not just the denumerability of K which is needed in the proof, but one needs the separability (in the topological sense) of the decomposition groups. Therefore Theorem 4.1 is also true e.g. for K being an algebraic function field of one variable over k with $\mathrm{Gal}(\bar{k} \mid k)$ separable, if the absolute values are trivial on k.

4.2. For convenience of the reader, we first prove Theorem 4.1 in the special case, where all w_i induce the same absolute value on K, i.e. where all w_i are conjugate under $\mathfrak{G}_K$. This corresponds to question II in 2.4. Then we consider the case where all w_i induce different absolute values on K, answering question I' and I in 2.4. At the end we consider the general (mixed) case.

4.3. Theorem 4.1 may be generalized to higher rank valuations. I will state another generalization in the archimedean case. Theorem 4.1 says especially: Given some involutions $\sigma_1, \cdots, \sigma_n$ in $\mathfrak{G}_K$ such that the fixed fields have archimedean orderings, then in general $\langle \sigma_1, \cdots, \sigma_n \rangle = \langle \sigma_1 \rangle * \cdots * \langle \sigma_n \rangle$. But this is true for arbitrary real closed fields:

THEOREM 4.3. *Let K be a Hilbertian field, let $\sigma_1, \cdots, \sigma_n$ be involutions in $\mathfrak{G}_K$. Then for almost all $\tau \in \mathfrak{G}_K^n$ we have*

$$\langle \sigma_1^{\tau_1}, \cdots, \sigma_n^{\tau_n} \rangle \simeq \langle \sigma_1^{\tau_1} \rangle * \cdots * \langle \sigma_n^{\tau_n} \rangle.$$

4.4. To see that it is reasonable to state the above theorems in a probabilistic habit, here is a counterexample of two decomposition groups which do not generate a free product. Let K be a real quadratic number field, e.g. $K = \mathbf{Q}(\sqrt{2})$. Then K has two different archimedean absolute values. By Theorem 4.1 or 4.3 there are two involutions σ and τ in $\mathfrak{G}_K$, generating two corresponding decomposition groups, such that $\mathfrak{G} = \langle \sigma, \tau \rangle = \mathbf{Z}/2\mathbf{Z} * \mathbf{Z}/2\mathbf{Z}$ is the free diedral group, i.e. $\rho = \sigma\tau$ generates a free pro-cyclic group (this remark fills a gap in [4], §5, where only diedral groups are constructed such that $\sigma\tau$ had an odd order, cf. the footnote[1] in [2] where Theorem 4.3 is stated for $K = \mathbf{Q}$, $n = 2$). Then $\mathfrak{G}$ has two conjugacy classes of involutions, represented by σ and τ. If $n = 1 + 2m$ with $m \in \hat{\mathbf{Z}}$, then the subgroup $\langle \sigma, \rho^n \rangle$ is again a diedral group with two conjugacy classes of involutions, represented by σ and $\sigma\rho^n$, corresponding to different absolute values on K. So $\langle \sigma \rangle$ and $\langle \sigma\rho^n \rangle$ are again two decomposition groups of K, but if an infinite power of some prime number divides n, then $\langle \sigma, \sigma\rho^n \rangle$ is not a free product, because ρ^n does not generate a free pro-cyclic group.

§5. Proof in the first case

5.1. Let K be a Hilbertian field, w an absolute value on $\bar{K}$ with the decomposition group $\mathfrak{G}_1$ in $\mathfrak{G}_K$ and the Henselization $L_1 = \mathrm{Fix}(\mathfrak{G}_1)$. Assuming $\mathfrak{G}_1$ to be separable, we will show in this paragraph that for almost all $\sigma \in \mathfrak{G}_K^n$ the groups $\mathfrak{G}_1^{\sigma_1}, \cdots, \mathfrak{G}_1^{\sigma_n}$ generate a free product in $\mathfrak{G}_K$.

5.2. By Lemma 1.2 we have to realize large finite factors G of $\mathfrak{P} = \mathfrak{G}_1 * \cdots * \mathfrak{G}_1$ (n times) as Galois groups over the intersection L of the Henselizations $\sigma_i^{-1} L_1$ of K. Now $\mathfrak{S}_n$ operates on $\mathfrak{P}$ by permuting the factors. Therefore we form the semi-direct product

$$\mathfrak{E} = \mathfrak{P} \cdot \mathfrak{S}_n$$

with normal subgroup $\mathfrak{P}$. With $\mathfrak{G}_1$ also $\mathfrak{P}$ and $\mathfrak{E}$ are separable, so we have

$$\mathfrak{E} = \varprojlim_{i \in \mathbf{N}} E_i$$

with finite factors $\phi_i : \mathfrak{E} \to E_i$. Setting $G_i = \phi_i \mathfrak{P}$, then also

$$\mathfrak{P} = \varprojlim_{i \in \mathbf{N}} G_i$$

so it is enough to realize these groups G_i over L. We may assume that $\phi_i \mid \mathfrak{S}_n$ is injective, so

$$E_i = G_i \cdot \mathfrak{S}_n$$

is again a semi-direct product of finite groups. The image of the first factor $\mathfrak{G}_1$ in $\mathfrak{P}$ under ϕ_i we call H_i, the images of the other factors $\mathfrak{G}_1$ in $\mathfrak{P}$ under ϕ_i are then conjugate to H_i under transpositions $(1j)$ of $\mathfrak{S}_n$, $j = 2, \cdots, n$. Therefore E_i is generated by H_i and the $(1j)$.

5.3. If $|E_i| = m_i$, we take a regular embedding

$$\varphi_i : E_i \hookrightarrow \mathfrak{S}_{m_i}.$$

The restriction of φ_i onto subgroups as H_i is a multiple of the regular representation there.

Now, because H_i is a factor group of $\mathfrak{G}_1$, there is a normal extension $M \mid L_1$ with Galois group H_i. If $r_i = [E_i : H_i]$, we choose r_i different normed polynomials $f_l \in K[X]$ of degree m_i/r_i irreducible over L_1 such that M is the splitting field of each f_l over L_1. Then $f = \Pi_l f_l$ has the Galois group (H_i, φ_i) over L_1. By Proposition 3.5 (used for only one absolute value w) in combination with Krasner's lemma applied to f, we get a sequence g_k of polynomials in $K[X]$ of degree m_i such that for all $k \in \mathbf{N}$

(i) $\mathrm{Gal}(g_k \mid L_1) = (H_i, \varphi_i)$,

(ii) $\mathrm{Gal}(g_k \mid K) = \mathfrak{S}_{m_i}$,

(iii) the splitting fields K_k of g_k over K are linearly disjoint.

5.4. Let $s_j \in \mathfrak{S}_{m_i}$ be the φ_i-images of the transpositions $(1j)$. By Lemma 1.1 the set

$$\Sigma_i = \{\tau \in \mathfrak{G}_K^n;\ \exists k : \tau_j \mid K_k = s_j \text{ for } j = 1, \cdots, n\}$$

is of measure 1. Now for $\tau \in \Sigma_i$ the subgroup $\langle \mathfrak{G}_1, \tau_1, \cdots, \tau_n \rangle$ of $\mathfrak{G}_K$ induces on a certain K_k the group $\varphi_i E_i = \langle \varphi H_i, s_2, \cdots, s_n \rangle$ in $\mathfrak{S}_{m_i} = \mathrm{Gal}(K_k \mid K)$. Therefore the subgroup $\langle \mathfrak{G}_1^{\tau_1}, \cdots, \mathfrak{G}_n^{\tau_n} \rangle$ of $\mathfrak{G}_K$ induces on K_k the subgroup $\varphi_i G_i = \langle \varphi H_i, \varphi H_i^{s_2}, \cdots, \varphi H_i^{s_n} \rangle$ and so G_i is realized as Galois group over $L = \bigcap_{j=1}^n \tau_j^{-1} L_1$.

5.5. Also $\Sigma = \bigcap_{i \in \mathbf{N}} \Sigma_i$ is a set of measure 1 in $\mathfrak{G}_K^n$ and for $\tau \in \Sigma$ all mappings $\mathfrak{P} \to G_i$ can be factored over $\mathfrak{G}_L$. By Lemma 1.2 the claim 5.1 follows.

§6. Proof in the second case

6.1. Let K be a Hilbertian field, $w_1, \cdots, w_n$ be absolute values on $\bar{K}$ which

induce different absolute values $v_1, \cdots, v_n$ on K. Let $\mathfrak{G}_1, \cdots, \mathfrak{G}_n$ be the decomposition groups of $w_1, \cdots, w_n$, the $\mathfrak{G}_i$ being separable, we will show in this paragraph that for almost all $\sigma \in \mathfrak{G}_K^n$ the groups $\mathfrak{G}_1^{\sigma_1}, \cdots, \mathfrak{G}_n^{\sigma_n}$ generate a free product in $\mathfrak{G}_K$.

6.2. Let L_i be the fixed field of $\mathfrak{G}_i$. To apply Lemma 1.3, we take (using Krasner's lemma) separable polynomials $f_i \in K[X]$ of degree d with Galois groups $G_i \subset \mathfrak{S}_d$ over L_i for $i = 1, \cdots, n$. By Proposition 3.5 and Krasner's lemma we get a sequence g_j of polynomials of degree d in $K[X]$ such that

(i) $\mathrm{Gal}(g_j \mid L_i)$ is conjugate in $\mathfrak{S}_d$ to G_i $(i = 1, \cdots, n)$,

(ii) $\mathrm{Gal}(g_j \mid K) = \mathfrak{S}_d$,

(iii) the splitting fields K_j of g_j over K are linearly disjoint.

For each j we have elements $s_{ji} \in \mathrm{Gal}(K_j \mid K) = \mathfrak{S}_d$ such that

(i)' $$\mathrm{Gal}(g_j \mid L_i)^{s_{ji}} = G_i.$$

Now the set

$$\Sigma_f = \{\sigma \in \mathfrak{G}_K^n;\ \exists j\ \forall i : \sigma_i \mid K_j = s_{ji}\}$$

is of measure 1 by Lemma 1.1, and for $\sigma \in \Sigma_f$ we have for a special j

(i)'' $$\mathrm{Gal}(g_j \mid \sigma_i^{-1} L_i) = G_i \qquad \text{for } i = 1, \cdots, n.$$

6.3. Because $\mathfrak{G}_i$ are separable, it is enough to do the construction of 6.2 for a denumerable set of n-tuples $f = (f_1, \cdots, f_n)$. Now

$$\Sigma = \bigcap_f \Sigma_f$$

is again of measure 1 in $\mathfrak{G}_K^n$, and for $\sigma \in \Sigma$ we get for each system $(G_1, \cdots, G_n)$ of factor groups of $(\mathfrak{G}_1, \cdots, \mathfrak{G}_n)$ in $\mathfrak{S}_d$ a polynomial g_j with (i)''. By Lemma 1.3, the groups $\mathfrak{G}_1, \cdots, \mathfrak{G}_n$ generate a free product.

§7. Proof in the general case

7.1. Let K be a Hilbertian field, let w_{ij} with $i = 1, \cdots, n$; $j = 1, \cdots, r_i$ be absolute values on $\bar{K}$ such that w_{ij} induces on K the absolute value v_i, and $v_1, \cdots, v_n$ are distinct. Let $N = \Sigma_{i=1}^n r_i$ and $\mathfrak{G}_{ij}$ be the decomposition groups for w_{ij}. Then we will show now, combining the methods of §5 and §6, that $\mathfrak{G}_{ij}^{\sigma_{ij}}$ generate a free product for almost all $\sigma = (\sigma_{ij}) \in \mathfrak{G}_K^N$.

7.2. From the results of §5 we get: Let L_{ij} be the fixed field of $\mathfrak{G}_{ij}$. Let

$\mathfrak{P} = \mathfrak{P}_1 * \cdots * \mathfrak{P}_n$ with $\mathfrak{P}_i = \mathfrak{G}_{i1} * \cdots * \mathfrak{G}_{ir_i}$, let $\phi : \mathfrak{P} \to G$ be a finite factor such that the $G_{ij} = \phi\mathfrak{G}_{ij}$ are isomorphic for fixed i under the operation of a symmetric group on $\mathfrak{P}_i$, let $\varphi : G \hookrightarrow \mathfrak{S}_d$ be a regular representation, then there are separable polynomials $g_i \in K[X]$ of degree d such that

$$\mathrm{Gal}(g_i \mid \sigma_{ij}^{-1} L_{ij}) = \varphi G_{ij}$$

for $j = 1, \cdots, r_i$ for almost all $(\sigma_{ij}) \in \mathfrak{G}_K^{r_i}$.

7.3. With Proposition 3.5 we get from 7.2:

There is a sequence f_k of polynomials in $K[X]$ of degree d such that

(i) $v_i(f_k - g_i) < \varepsilon$ for $i = 1, \cdots, n$,

(ii) $\mathrm{Gal}(f_k \mid K) = \mathfrak{S}_d$,

(iii) the splitting fields of f_k over K are linearly disjoint.

The condition (i) shows by Krasner's lemma that

(i)′ $$\mathrm{Gal}(f_k \mid L_{ij}) \text{ is conjugate to } \varphi G_{ij}$$

(the φG_{ij} being conjugate for fixed i).

7.4. Now one specifies the conjugations of (i)′ by elements in $\mathfrak{S}_d = \mathrm{Gal}(f_k \mid K)$, and as in §6 we get the result 7.1, so Theorem 4.1 is proved.

§8. Proof of Theorem 4.3

8.1. The proof of Theorem 4.3 (which existed before Theorem 4.1 and was presented at the conference of algebraic number theory in Silivri, 1975) can be given along the same lines as the proof of Theorem 4.1. One has only to check that the used tools are valid (in some sense) also in this case. This is not so clear for Krasner's lemma, the Approximation Lemma and the density lemma 3.4.

8.2. Krasner's lemma indeed holds true for arbitrary real closed fields, but there is more known under the name of

(Sturm's) LEMMA 8.2. *Let K be a real closed field, $f \in K[X]$ separable. Then the number of real roots of f is locally constant under variation of the coefficients of f.*

This follows e.g. by the classical method of Sturm's chains.

8.3. There is no Approximation Lemma for a finite set of orderings on a field K, as can be seen from the two orderings of the power series field $K = \mathbf{R}((T))$, which are both non-archimedean, T being infinitely small, and differ in the sign

of T. There is no $x \in K$ such that $|1-x|<1$ holds in one ordering and $|3-x|<1$ in the other.

Even the following weak independence is not true for orderings, namely that there is an $x \in K$ with prescribed sign for each ordering. This can be seen from the four orderings of the power series field $K = \mathbf{R}((X))((Y))$, an $x \in K$ which is positive for 3 orderings is also positive in the fourth.

8.4. In the same way density arguments may become wrong, because an ordered field is not necessarily dense in its real closure. But one has the following substitute for Lemma 3.4.

LEMMA 8.4. *Let K be a formal real Hilbertian field with n orderings $>_i$ given. If $\boldsymbol{a} \in K^d$ and $\varepsilon_i >_i 0$ with $\varepsilon_i \in K$, any Hilbertian set in K^d contains elements $\boldsymbol{\xi}$ such that for $i = 1, \cdots, n$ one has in the i-th ordering $|\boldsymbol{a} - \boldsymbol{\xi}| \leqq \varepsilon_i$.*

This is essentially lemma 11.1 of [10]. Assuming $\varepsilon_i <_i 1$ and setting $\varepsilon = (\varepsilon_1^{-2} + \cdots + \varepsilon_n^{-2})^{-1}$ we may take $\varepsilon_i = \varepsilon$ for $i = 1, \cdots, n$. Given an irreducible polynomial $f(\boldsymbol{X}, Y)$, the transformed polynomial

$$f(a_1 + \varepsilon(X_1 - 1)(X_1 + 1)^{-1}, \cdots, a_n + \varepsilon(X_n - 1)(X_n + 1)^{-1}, Y)$$

shows it is enough to prove that every Hilbertian set contains elements which are positive for all orderings. This can be seen by considering the polynomial $f(X_{11}^2 + X_{12}^2 + X_{13}^2, \cdots, X_{n1}^2 + X_{n2}^2 + X_{n3}^2, Y)$ which is irreducible by lemma 10.3 of [10].

8.5. With these tools we can give a proof of Theorem 4.3 along even simplified lines. Let L_i be the fixed real closed field of σ_i. Let

$$\mathfrak{P} = \langle \sigma_1 \rangle * \cdots * \langle \sigma_n \rangle$$

be the free product of n copies of $\mathbf{Z}/2\mathbf{Z}$. Let $\phi : \mathfrak{P} \to G$ be a finite factor goup of $\mathfrak{P}$ of order $2m$, we may assume $\phi\sigma_i \neq 1$ for $i = 1, \cdots, n$. Let

$$\varphi : G \hookrightarrow \mathfrak{S}_{2m}$$

be the regular representation of G and $\varphi\sigma_i = s_i$, which are products of m transpositions, so all conjugate in $\mathfrak{S}_{2m}$. The separable polynomial

$$f = \prod_{j=1}^{m} (X^2 + j^2)$$

has over any real closed field a Galois group conjugate to $\langle s_i \rangle$. Now looking at the proof of Proposition 3.5 and using Lemma 8.4 instead of 3.4, we get a sequence of polynomials $g_j \in K[X]$ of degree $2m$ such that

(i) g_j close to f in all orderings,

(ii) $\mathrm{Gal}(g_j \mid K) = \mathfrak{S}_{2m}$,

(iii) the splitting fields of g_j over K are linearly disjoint.

From (i) with the aid of 8.2 it follows that

$$\text{(i)}' \qquad \mathrm{Gal}(g_j \mid L_i) \text{ conjugate to } \langle s_i \rangle \qquad (i = 1, \cdots, n).$$

Specifying these conjugations by elements in $\mathfrak{S}_{2m}$ we proceed as in 6.2 and see that $\phi : \mathfrak{P} \to G$ factors over $\langle \sigma_1^{\tau_1}, \cdots, \sigma_n^{\tau_n} \rangle$ for almost all $\tau \in \mathfrak{G}_K$. Now G is running over a denumerable set of finite factor groups; by the argument of 6.3 and Lemma 1.2 we get Theorem 4.3.

Acknowledgment

This work was done during the author's stay at Tel Aviv University in March 1977. He would like to thank the University for their kind hospitality and especially M. Jarden for stimulating conversations.

References

1. E. Artin, *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, New York, 1967.

2. E. Becker, *Euklidische Körper und euklidische Hüllen von Körpern*, J. Reine Angew. Math. **268/269** (1974), 41–52.

3. O. Endler, *Valuation Theory*, Springer, 1972.

4. W.-D. Geyer, *Unendliche algebraische Zahlkörper, über denen jede Gleichung auflösbar von beschränkter Stufe ist*, J. Number Theory **1** (1969), 346–374.

5. W.-D. Geyer, *Variations on Hilbert's Irreducibility Theorem*, to appear.

6. W.-D. Geyer and M. Jarden, *Fields with the density property*, J. Algebra **35** (1975), 178–189.

7. E. Globig, *Freie proendliche Produktzerlegungen von Galoisgruppen durch Zerlegungsgruppen*, Dissertation, Regensburg, 1976.

8. D. Hilbert, *Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten*, J. Reine Angew. Math. **110** (1892), 104–129 (= Ges. Abh. II. 264–286).

9. M. Jarden, *Elementary statements over large algebraic fields*, Trans. Amer. Math. Soc. **164** (1972), 67–91.

10. M. Jarden, *Algebraic extensions of finite corank of Hilbertian fields*, Israel J. Math. **18** (1974), 279–307.

11. S. Lang, *Diophantine Geometry*, Interscience Publ., New York, 1962.

12. G. Martens, *Galoisgruppen über aufgeschlossenen reellen Funktionenkörpern*, Math. Ann. **217** (1975), 191–199.

13. J. Neukirch, *Freie Produkte pro-endlicher Gruppen und ihre Kohomologie*, Arch. Math. **22** (1971), 337–357.

14. J. Neukirch, *Einbettungsprobleme mit lokaler Vorgabe und freie Produkte lokaler Galoisgruppen*, J. Reine Angew. Math. **259** (1973), 1–47.

Mathematisches Institut
Universität Erlangen
FRG