On Galois groups of functional fields over fields of finite type over $\mathbb{Q}$

1991 Russ. Math. Surv. 46 202

(http://iopscience.iop.org/0036-0279/46/5/L15)

On Galois groups of functional fields over fields of finite type over $\mathbb{Q}$

V.A. Voevodskii

In [1] and in a letter to G. Faltings (1983), A. Grothendieck conjectured the possibility of reconstructing a field E of finite type over a field K of finite type over $\mathbb{Q}$ by means of its Galois group $\mathrm{Gal}(\overline{E}/E)$, considered as a group over $\mathrm{Gal}(\overline{K}/K)$. In this paper this conjecture is proved in the case $\deg \mathrm{tr}_K E = 1$ (for $\deg \mathrm{tr}_K E = 0$ the corresponding assertions are essentially special cases of the fundamental theorem of Galois theory). A similar result was recently announced by F.A. Bogomolov for fields of finite type of degree of transcendence strictly larger than unity over an algebraically closed field.

In what follows K will denote a field of finite type over $\mathbb{Q}$. For any field E, we will denote by $\mathrm{Gal}(E)$ the Galois group of the algebraic completion $\overline{E}$ over E. If L is an extension of E, then there exists a homomorphism $\mathrm{Gal}(L) \to \mathrm{Gal}(E)$ that is unique up to an inner automorphism.

***Theorem* 1.** *Let E_1 and E_2 be fields of degree of transcendence* 1 *over K. Then to every monomorphism* $\mathrm{Gal}(E_2) \to \mathrm{Gal}(E_1)$ *such that the diagram*

$$\begin{array}{ccc} \mathrm{Gal}\,(E_2) & \to & \mathrm{Gal}\,(E_1) \\ & \searrow \quad \swarrow & \\ & \mathrm{Gal}\,(K) & \end{array}$$

is commutative up to an inner automorphism, there corresponds (*functorially*) *a morphism of the fields* $E_1 \to E_2$ *over K.*

Corollary. *Two fields of degree of transcendence* 1 *over a field K of finite type over $\mathbb{Q}$ are isomorphic over K if and only if their Galois groups are isomorphic over* $\mathrm{Gal}(K)$.

The proof of the theorem is essentially based on the technique in [2].

Let E^* be the multiplicative group of E and let $\hat{E}^*$ be the (pro)group $\varprojlim E^*/(E^*)^n$. It follows obviously from Kummer's theory that $\hat{E}^* \cong H^1(\mathrm{Gal}(E), \hat{\mathbb{Z}}(1))$, where $\hat{\mathbb{Z}}(1) = \varprojlim \mu_n$ is the projective limit of the groups of nth roots of unity. Therefore, any homomorphism $f : \mathrm{Gal}(E_2) \to \mathrm{Gal}(E_1)$ over $\mathrm{Gal}(K)$ induces a homomorphism $\hat{E}_1^* \to \hat{E}_2^*$. For a proof of the theorem it is sufficient to verify that in the case where f is a monomorphism, it transforms the "lattice" E_i^* into E_2^* and preserves the additive structures on E_i^*. For this, in turn, it is sufficient to give a description of the lattice $E^* \subset \hat{E}^*$ and of the conditions for the satisfaction of relations of the form $z_3 = z_1 + z_2$ directly in terms of the Galois group of E over K. We may obviously restrict oursleves to the case where E is a purely transcendental extension of K. Under this hypothesis a homomorphism $\mathrm{Gal}(E) \to \mathrm{Gal}(K)$ is surjective and its kernel is isomorphic to $\mathrm{Gal}(E \otimes_K \overline{K})$. We denote the groups $\mathrm{Gal}(E)$, $\mathrm{Gal}(E \otimes_K \overline{K})$, $\mathrm{Gal}(K)$ by G, $\overline{G}$, Γ, respectively. Let $\varepsilon : G \to \hat{\mathbb{Z}}^*$ be the cyclotomic character (that is, the character defined by the natural action of G on $\hat{\mathbb{Z}}(1)$). An essential technical step in the proof of Theorem 1 is the following "arithmetic" analogue of a theorem of Bogomolov.

***Theorem* 2.** *Let $g \in \overline{G}$ be an element such that the set of $h \in G$ for which hgh^{-1} is conjugate to $g^{\varepsilon(h)}$ in $\overline{G}$ is a subgroup of finite index in G. Then g is in the ramification group of some discrete valuation of the field $E \otimes_K \overline{K}$.*

The proof is based on the interpretation of $E \otimes_K \overline{K}$ as a field of functions on a smooth curve $\overline{X}$ over $\overline{K}$ and on an analysis of the action of Γ on the fundamental groups of open subschemes in $\overline{X}$. The key observation is the absence, in the Tate modules of Abelian manifolds over K, of elements on which Γ acts by mutiplication by the value of the cyclotomic character.

Let g be an element of $\overline{G}$ satisfying the condition in Theorem 2. We denote by V_g and H_g the corresponding valuation and subgroup of finite index of G, respectively. We consider $z \in \hat{E}^*$ as a cocycle from $H^1(G, \hat{\mathbb{Z}}(1))$. Its restriction to $\overline{G}$ is an unambiguously defined homomorphism, which we will denote by the same letter. It is easy to see that the following is true.

Lemma. *If $z \in E^*$, then $V_g(z) = 0$ if and only if $z(g) = 0$.*

Since the group $\overline{G}$ is free, the sequence

$$1 \to \{g\} \to N(g) \to \mathrm{Gal}\,(L_g) \to 1$$

is exact, where $\{g\}$ is the maximal cyclic subgroup of $\overline{G}$ contained in g, $N(g)$ is the normalizer of $\{g\}$ in G, and L_g is the subfield in $\overline{K}$ that corresponds to the image of H_g in Γ. If $z(g) = 0$, then the cocycle z determines a cocycle in $\hat{L}_g^*$, which we denote by $r(g, z)$. Let A be the set of conjugacy classes of maximal cyclic subgroups $\langle g\rangle$ of $\overline{G}$ such that g satisfies the conditions in Theorem 2.

***Proposition* 3.** *An element $z \in \hat{E}^*$ lies in E^* if and only if the following conditions are fulfilled*:

a) $z(g) = 0$ *for all $\langle g\rangle \in A$, except possibly finitely many of them,*

b) *if $z(g) = 0$, then $r(g, z) \in L_g^*$.*

In this case $r(g, z)$, as an element of $\overline{K}^*$, is equal to the value of z in V_g.

It is obvious from this proposition that any monomorphism $\mathrm{Gal}(E_2) \to \mathrm{Gal}(E_1)$ over Γ induces a homomorphism $E_1^* \to E_2^*$. The fact that it is compatible with the additive structure follows from the observation that it is sufficient to verify conditions of the form $z_3 = z_1 + z_2$ for the values of the z_i in the residue fields of valuations for which they are defined.

In conclusion, the author remarks that it is not clear in general (although it is very plausible) whether the field homomorphism constructed here induces the initial homomorphism of Galois groups. For a proof of this it is apparently possible to use the technique of [3].

References

[1] A. Grothendieck, Esquissé d'un progamme, Manuscript, 1984.

[2] V.A. Voevodskii, Izv. Akad. Nauk SSSR Ser. Mat. 55:5 (1991).

[3] H. Nakamura, Automorphisms of the étale fundamental group of the projective line minus three points over Q, Preprint, UTYO-MATH 90-5, Tokyo 1990.

Received by the Board of Governors 27 February 1991