Труды Матем. Инст. Стеклов.
183(1990)

Proceedings of the Steklov
Institute of Mathematics
1991, Issue 4

ON LÜROTH'S PROBLEM

UDC 512.62

I. R. SHAFAREVICH

ABSTRACT. In this paper the author presents a new way of viewing the example of a nonrational field of invariants of a finite group of linear transformations first constructed by D. Saltman. The proof is based on D. K. Faddeev's theory of simple algebras over a field of algebraic functions of one variable with an algebraically nonclosed field of constants.

Bibliography: 11 titles.

Lüroth's problem, as is well known, is the following one: Is a subfield L of a rational function field, $k(x_1, \ldots, x_n) \supset L \supset k$, itself isomorphic to a rational function field over k? When $n = 1$ the answer is affirmative, without any restrictions, and the proof is completely elementary (see, e.g., [2], §73). When $n = 2$ this assertion is false if the field k is not algebraically closed. For example, if $k = \mathbb{R}$, the field of rational functions on the surface $z^2 + y^2 = x^3 - x$ is isomorphic to a subfield of a rational function field, but is itself not isomorphic to a rational function field, since the surface consists of two connected components. Even for an algebraically closed field of finite characteristic, Lüroth's problem has a negative answer if it is not assumed in addition that the extension $k(x_1, \ldots, x_n)/L$ is separable.

If, however, the field k is algebraically closed and has characteristic 0, or in the case of a finite characteristic the extension $k(x_1, \ldots, x_n)/L$ is separable, then Lüroth's problem has an affirmative solution. This is a subtle result in the theory of algebraic surfaces, proved in the case $k = \mathbb{C}$ by G. Castelnuovo. For $n > 2$ Lüroth's problem long remained an unsolved problem of algebraic geometry. It was settled in 1971 independently in three papers: Iskovskikh and Manin [4], Clemens and Griffiths [8], and Artin and Mumford [7]. They showed that when $n = 3$ (and even when $k = \mathbb{C}$) Lüroth's problem has a negative answer. All three papers use different, but very subtle, methods to prove the nonrationality of the fields they construct.

A completely new light was shed on Lüroth's problem by a recent paper of Saltman [11]. He showed that Lüroth's problem has a negative solution even in the following concrete situation. Suppose G is a finite group of linear transformations of a vector space V over an algebraically closed field k, $k(V)$ is the field of rational functions of the coordinates in V, and $k(V)^G$ is the field of invariants of G. Obviously $k(V)^G \subset k(V)$, hence $k(V)^G$ is a subfield of a rational function field, but $k(V)^G$ need not be isomorphic to a rational function field. The proof is based on ideas simpler by far than those used earlier in [4], [7], [8] in answering Lüroth's problem negatively.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R58.

Then Bogomolov [1] observed that Saltman's proof could be further simplified: some parts of [11] were not at all needed for the solution of Lüroth's problem, e.g. the theory of "universal" central simple Amitsur algebras. The present note is, properly speaking, a commentary on Bogomolov's work, and its aim is to point out the essentially algebraic nature of the whole argument. It will become obvious that a main role is played by Faddeev's theory of simple algebras over algebraic function fields with an algebraically nonclosed field of constants (see [5]). Indeed, except for the element of Galois theory and theory of groups and cohomology of groups, Faddeev's theory is the only tool used and is that on which the whole argument is based. The proof could have been completely found upon the publication of Faddeev's work, i.e. any time during the 20 years until counterexamples to Lüroth's problem were actually constructed. We will begin by recalling the relevant results of Faddeev's theory.

Let us fix some algebraically closed field k of characteristic 0. All fields considered will contain this field. If L/K is a Galois extension, then the cohomology group of its Galois group with coefficients in a module A will be denoted by $H^p(L/K, A)$, and if L is the algebraic closure $\overline{K}$ of K, the cohomology group will be denoted by $H^p(K, A)$.

1°. The Brauer group of a local field. Suppose K is a complete, discretely valuated field with residue field $\kappa \supset k$ (from which it follows that κ has characteristic 0). If $\nu: K^* \to \mathbb{Z}$ is the valuation and $t \in K$ with $\nu(t) = 1$, then K is isomorphic to the field $\kappa\{t\}$ of formal Laurent series with coefficients in κ. The we can state the following results (see [5]).

A. If the field κ is algebraically closed, then $H^2(K, \overline{K}^*) = 0$ ($\overline{K}$ denotes the algebraic closure of K). It follows in the general case that $H^2(K, \overline{K}^*) = H^2(\Omega/K, \Omega^*)$, where $\Omega = \overline{\kappa}\{t\}$ and $\overline{\kappa}$ is the algebraic closure of κ. In particular, any element of $H^2(K, \overline{K}^*)$ can be identified with an element $c \in H^2(K'/K, K'^*)$, where K'/K is an unramified extension, $K' = \kappa'\{t\}$, κ' a finite Galois extension of κ.

B. For an unramified extension K'/K we have the decomposition $K'^* = \Gamma \times \kappa'^* \times U_1$, where again $K' = \kappa'\{t\}$, Γ is the infinite cyclic group generated by t, and $U_1 = \{\alpha \in K'^*, \nu(\alpha) = 0, \alpha \equiv 1(t)\}$. Also $H^p(K'/K, U_1) = 0$, $p > 0$, so that when $p > 0$ we have

$$H^2(K'/K, K'^*) = H^2(K'/K, \mathbb{Z}) \oplus H^2(\kappa'/\kappa, \kappa'^*). \tag{1}$$

DEFINITION 1. A cohomology class $c \in H^2(K'/K, K'^*)$ is called a constant if its component corresponding to the first summand in the decomposition (1) is equal to 0. A cohomology class $c \in H^2(K, \overline{K}^*)$ is called a constant if it can be identified with a constant class of the group $H^2(K'/K, K'^*)$ under the homomorphism $H^2(K'/K, K'^*) \to H^2(K, \overline{K}^*)$ for some unramified extension K'/K.

Thus a cohomology class is a constant if it can be identified with a class $c \in H^2(K'/K, U)$, where $U = \{\alpha \in K'^*, \nu(\alpha) = 0\}$ and the extension K'/K is unramified.

C. Finally, let us recall that the Galois group of any Galois extension L/K has a very simple structure: the group $H = \mathrm{Gal}(L/K)$ contains a normal inertia subgroup I, and to the subgroup I corresponds a subfield K' that is an unramified extension of K, and I is a cyclic group lying in the center of H

(the last assertion follows from the fact that, by our assumption, $\kappa \supset k$, where k is an algebraically closed field, hence all roots of 1 lie in κ). (One reference for these results is [3], Chapter III, §10.)

2°. The Faddeev-Brauer group. Suppose K is any field (satisfying the usual condition $K \supset k$). Consider all discrete valuations of the extension K/k, i.e. epimorphisms $\nu: K^* \to \mathbb{Z}$ such that

$$\nu(\alpha+\beta) \geq \min(\nu(\alpha), \nu(\beta)) \quad \text{if } \alpha+\beta \neq 0, \qquad \nu(\alpha) = 0 \quad \text{if } \alpha \in k^*.$$

To each valuation ν corresponds a completion K_ν, a field of the same type considered in § 1°. There is a canonical homomorphism $\varphi_\nu: H^2(K, \overline{K}^*) \to H^2(K_\nu, K_\nu^*)$.

DEFINITION 2. The Faddeev-Brauer group of the extension K/k consists of all elements $c \in H^2(K, \overline{K}^*)$ for which the classes $\varphi_\nu(c)$ are constants for all valuations ν of K/k.

We will denote this group by $\Phi\mathrm{Br}(K/k)$.

FADDEEV'S THEOREM (see [5]). *If T is an independent variable, then* $\Phi\mathrm{Br}(K(T)/k) = \Phi\mathrm{Br}(K/k)$.

3°. Construction of an obstruction. Suppose G is a finite group of linear transformations of a vector space V over the field k, $k(V)$ is the field of rational functions of the coordinates in V, and $k(V)^G$ is the field of invariants of G. Since $k(V)^G \subset k(V)$, it follows that $k(V)^G$ is a subfield of a rational function field. To show that $k(V)^G$ is not isomorphic to a rational function field for certain groups G it suffices (in view of Faddeev's theorem) to show that $\Phi\mathrm{Br}(k(V)^G/k) \neq 0$. The group $\Phi\mathrm{Br}(k(V)^G/k)$ can be represented a little more concretely. Since, again by Faddeev's theorem, $\Phi\mathrm{Br}(k(V)/k) = 0$, it follows that under the restriction homomorphism $H^2(k(V)^G, \overline{k(V)}^*) \to H^2(k(V), \overline{k(V)}^*)$ the group $\Phi\mathrm{Br}(k(V)^G/k)$ goes into 0, from which it follows that

$$\Phi\mathrm{Br}(k(V)^G/k) \subset H^2(G, k(V)^*).$$

On the other hand, the embedding $k^* \to k(V)^*$ defines a homomorphism

$$H^2(G, k^*) \to H^2(G, k(V)^*).$$

LEMMA. *The homomorphism $H^2(G, k^*) \to H^2(G, k(V)^*)$ is an embedding.*

PROOF. We prove the lemma by considering the exact sequence

$$1 \to k^* \to k(V)^* \to k(V)^*/k^* \to 1. \tag{2}$$

We obtain from it an exact sequence

$$H^1(G, k(V)^*/k^*) \to H^2(G, k^*) \to H^2(G, k(V)^*), \tag{3}$$

and it suffices to show that $H^1(G, k(V)^*/k^*) = 0$.

Using the uniqueness of a decomposition of a polynomial into irreducible factors, we obtain for the G-module $k(V)^*/k^*$ that

$$k(V)^*/k^* = \bigoplus \left(\bigoplus \mathbb{Z} g^* P \right),$$

where the outer sum extends over all G-orbits of irreducible polynomials P in $k(V)^*/k^*$ and the inner sum extends over the one orbit of P. The inner sum

is an induced module. According to a well-known theorem of the theory of homology of groups (this theorem was proved by Faddeev for the case we need in [5] and in general in [6], and in most papers on the homology of groups is called Shapiro's lemma!), we have

$$H^1\left(G, \bigoplus \mathbb{Z}g^*P\right) = H^1(H, \mathbb{Z}) = \mathrm{Hom}(H, \mathbb{Z}),$$

where $H = \{g \in G, g^*P = \alpha P, \alpha \in k^*\}$. Since the group H is finite, $\mathrm{Hom}(H, \mathbb{Z}) = 0$. This proves the lemma.

We denote by $\mu \subset k^*$ the group of all roots of 1. Since the group k^*/μ is unbounded and uniquely divisible, it follows that $H^2(G, k^*) = H^2(G, \mu)$ is the Schur multiplier of G.

We will look for a nonzero element of $\Phi\mathrm{Br}(k(V)^G/k)$ as an element of $H^2(G, \mu)$. In view of the lemma, it is different from 0 in $\Phi\mathrm{Br}(k(V)^G/k)$ if it is different from 0 in $H^2(G, \mu)$. It remains to find a criterion for showing that an element $c \in H^2(G, \mu)$ is contained in $\Phi\mathrm{Br}(k(V)^G/k)$.

For any valuation ν of the extension $k(V)^G/k$ the homomorphism φ_ν (see § 2°) can be interpreted on the subgroup $H^2(G, k(V)^*)$ as the restriction from the group G to the stationary subgroup of ν. This subgroup is isomorphic to the Galois group of the extension $k(V)_{\nu'}/k(V)_\nu^G$, where ν' is the prolongation of ν to $k(V)$, and the structure of such groups is well known (see § 1°, C). A cocycle $c \in H^2(G, \mu)$, of course, has values in $\mu \subset U$ (cf. § 1°, C), but, in general, it is defined not on the Galois group of the unramified extension $K'/k(V)^G$ corresponding to the inertia subgroup $I \subset H$, but on the whole Galois group H. But if a class $c \in H^2(G, \mu)$, being bounded on the subgroup H, is cohomologous to a cocycle constant on the cosets in H/I, or, in other words, is contained in the image of the inflation homomorphism $\mathrm{Inf}_H^{H/I}$, then we can apply the criterion in § 1°, B. Thus we obtain the following

PROPOSITION. *A class $c \in H^2(G, \mu)$ belongs to the group $\Phi\mathrm{Br}(k(V)^G/k)$ if, for any subgroup $H \subset G$ and central cyclic subgroup I of H, the restriction $\rho_H^G(c)$ is contained in the image of the inflation $\mathrm{Inf}_H^{H/I}$.*

4°. Construction of an example. To construct an example of a nonrational field $k(V)^G$ it suffices to construct a finite group G and cohomology class $c \in H^2(G, \mu)$ satisfying the conditions of the proposition. For this purpose we consider for $p > 2$ a reduced free p-group $\overline{G}$ of class 2 and period p. Its elements have the form $\Pi_i a_i^{k_i} \Pi_{i<j}(a_i, a_j)^{l_{ij}}$, $k_i, l_{ij} \pmod p$, where $a_i^p = (a_i, a_j)^p = 1$ and the (a_i, a_j) lie in the center of the group. Here (a_i, a_j) denotes the commutator of the elements a_i, a_j. Suppose $z = \Pi_{i<j}(a_i, a_j)^{l_{ij}}$ is some central element. Put $G = \overline{G}/\{z\}$ and take as $c \in H^2(G, \mu)$ the cohomology class corresponding to the extension $1 \to \{z\} \to \overline{G} \to G \to 1$ under some isomorphism $\{z\} \simeq \mu_p \subset \mu$, where μ_p is the group of pth roots of 1.

We must show that, for any subgroup $H \subset G$ and any central element u of H, the restriction $\rho_H^G(c)$ of the class c is a class defined on $H/\{u\}$, i.e., is contained in the image of the inflation $\mathrm{Inf}_H^{H/\{u\}}$. Note that the class c is

even defined on G/Z, where Z is the center of G, i.e., c is contained in the image of $\mathrm{Inf}_Z^{G/Z}$. Therefore if the central element u of H is also central in G, then the desired property is obviously satisfied. Suppose $u \notin Z$. If the group $H/H\cap Z$ is generated by the image of u, then H is Abelian and even its preimage $\overline{H}$ in $\overline{G}$ will be Abelian. Then the element z is in a direct summand of $\overline{G}$, hence $\rho_H^G(c) = 0$.

Thus there remains only the case where $H/H\cap Z$ contains two independent elements whose preimages in H commute (since one of them lies in the center of H). But for a suitable choice of z even G/Z will not contain such elements. Indeed, two independent elements of $\overline{G}$ whose images are independent in $\overline{G}/Z(\overline{G})$ never commute, and their images x, y in G commute only if $(x, y) = z^k$. Viewing $\overline{G}/Z(\overline{G}) = G/Z$ as a vector space L over the field $\mathbb{F}_p$, we can identify $Z(\overline{G})$ with $\Lambda^2 L$ and the element z with a bivector $\zeta \in \Lambda^2 L$. Commutation can be expressed as exterior multiplication, hence we must choose a ζ inexpressible in the form $x \wedge y$, i.e., an indecomposable bivector. The simplest case is $n = 4$ and $z = (a_1, a_2)(a_3, a_4)$.

5°. **Remarks.** A. In constructing the example we chose the group G and cohomology class $c \in H^2(G, \mu)$, but never mentioned the representation V, hence any faithful representation will do. This is not accidental: the group $\Phi\mathrm{Br}(k(V)^G/k)$ does not depend on the choice of faithful representation V of G. Indeed, for two faithful representations V_1, V_2 of dimensions n_1, n_2 the fields $k(V_1)^G, k(V_2)^G$ are stably isomorphic, i.e.,

$$k(V_1)^G(T_1, \ldots, T_{n_2}) = k(V_2)^G(U_1, \ldots, U_{n_1}). \tag{4}$$

It follows from the theorem of Faddeev stated in § 2° that $\Phi\mathrm{Br}(k(V_1)^G/k) \simeq \Phi\mathrm{Br}(k(V_2)^G/k)$. The proof of (4) follows at once from the main theorem on finite groups of semilinear transformations, also known as Speiser's theorem (see, e.g., [10]). The action of G on $V_1 \oplus V_2$ can be regarded as a representation of G by semilinear transformations of V_2 over the field $k(V_1)$. By Speiser's theorem, there exists a G-invariant basis, hence $k(V_1 \oplus V_2)^G = k(V_1)^G(T_1, \ldots, T_{n_2})$. Interchanging V_1 and V_2, we obtain (4).

B. If the group is commutative, then the criterion of the proposition in § 3° can be satisfied only for the zero class. This is understandable, since for a commutative group G the field $k(V)^G$ is isomorphic to a rational function field [9] (a simple exposition of Fischer's proof was given by Lenstra [10]). It follows that a class $c \in H^2(G, \mu)$ belonging to the group $\Phi\mathrm{Br}(k(V)^G/k)$ must be decomposable on any commutative subgroup $H \subset G$. On the other hand, the argument used in considering the example in § 4° shows at once that a class $c \in H^2(G, \mu)$ decomposable on all commutative subgroups satisfies the conditions of the proposition in § 3°. Thus the following three conditions are equivalent: 1) a class $c \in H^2(G, \mu)$ belongs to the group $\Phi\mathrm{Br}(k(V)^G/k)$; 2) this class is decomposable on any commutative subgroup $H \subset G$; 3) it satisfies the conditions of the proposition in § 3°.

C. The choice of a nonzero class $c \in \Phi\mathrm{Br}(k(V)^G/k)$ as an element of the group $H^2(G, \mu)$ is also not accidental. Namely, it follows easily from the exact sequence (3) that the entire subgroup $\Phi\mathrm{Br}(k(V)^G/k) \subset H^2(G, k(V)^*)$

is contained in the image of $H^2(G, \mu)$ (see [1]). From this there follows a beautiful characterization of $\Phi\mathrm{Br}(k(V)^G/k)$ due to Bogomolov: this group is equal to the subgroup of the Schur multiplier of G consisting of the classes decomposable on restriction to all commutative subgroups.

Bibliography

1. F. A. Bogomolov, *The Brauer group of quotient spaces by linear group actions*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), 485–516; English transl. in Math. USSR Izv. **30** (1988).
2. B. L. van der Waerden, *Algebra*, Vols. I (8th ed.), II (5th ed.), Springer-Verlag, 1971, 1967.
3. Hermann Weyl, *Algebraic theory of numbers*, Princeton Univ. Press, Princeton, N.J., 1940.
4. V. A. Iskovskikh and Yu. I. Manin, *Three-dimensional quartics and counterexamples to the Lüroth problem*, Mat. Sb. **86 (128)** (1971), 140–166; English transl. in Math. USSR Sb. **15** (1971).
5. D. K. Faddeev, *Simple algebras over a field of algebraic functions of one variable*, Trudy Mat. Inst. Steklov. **38** (1951), 321–344; English transl. in Amer. Math. Soc. Transl. (2) **3** (1956).
6. ——, *On homology theory in groups*, Izv. Akad. Nauk SSSR Ser. Mat. **16** (1952), 17–22. (Russian)
7. M. Artin and D. Mumford, *Some elementary examples of unirational varieties which are not rational*, Proc. London Math. Soc. (3) **25** (1972), 75–95.
8. C. Herbert Clemens and Phillip A. Griffiths, *The intermediate Jacobian of the cubic threefold*, Ann. of Math. (2) **95** (1972), 281–356.
9. E. Fischer, *Die Isomorphie der Invariantenkörper der endlichen Abel'schen Gruppen linearer Transformationen*, Nachr. Königl. Ges. Wiss. Göttingen Math.-Phys. Kl. **1915**, 77–80.
10. H. W. Lenstra, Jr., *Rational functions invariant under a finite Abelian group*, Invent. Math. **25** (1974), 299–325.
11. David J. Saltman, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984), 71–84.

Translated by G. A. KANDALL