Reports of the Academy of Sciences of the USSR

1957

SovietRxiv

Abstract

Full Text

Reports of the Academy of Sciences of the USSR

1957. Volume 114, No. 2

MATHEMATICS

I. R. SHAFAREVICH

ON THE BIRATIONAL EQUIVALENCE OF ELLIPTIC CURVES

(Presented by Academician I. M. Vinogradov on 13 XI 1956)

1. Let us consider elliptic curves (curves of genus 1) over an arbitrary field k, about which we shall assume only that its characteristic is different from 2 and 3. The classification of such curves from the point of view of birational equivalence is well known in the case of an algebraically closed field k ([1]). In this case every elliptic curve γ is birationally equivalent to a curve ω having the Weierstrass normal form

$$y^2 = x^3 + ax + b; \quad a, b \in k. \tag{1}$$

In turn, two curves having the Weierstrass form are birationally equivalent if and only if their absolute invariants j, defined by the formula

$$j = \frac{4a^3}{4a^3 + 27b^2},$$

coincide.

If the field k is not algebraically closed, then an elliptic curve defined over k can be brought to Weierstrass form over some finite extension of the field k, and its absolute invariant will lie in k ([2]).

Since among the curves with a given absolute invariant there are also those which have Weierstrass form over k, we shall obtain all elliptic curves over k with a given value of the absolute invariant by taking a curve ω with equation (1) and considering all elliptic curves over k that are birationally equivalent to it over finite extensions of the field k.

2. Let us consider some finite normal extension K/k of the field k and investigate elliptic curves γ defined over k and birationally equivalent to ω over K. Denote by M the generic point of γ over k, and by $k(M)$ and $K(M)$ the fields of rational

functions on γ with coefficients in k and K, respectively. By assumption the field $K(M)$ is isomorphic to $K(x, y)$, where (x, y) is the generic point of ω.

Any automorphism σ of the field K/k can be extended to an automorphism $\varphi_\gamma(\sigma)$ of the field $K(M)$ by putting $M^\sigma = M$, and, in view of the isomorphism of $K(M)$ with $K(x, y)$, transferred to $K(x, y)$. Obviously,

$$\varphi_\gamma(\sigma\tau) = \varphi_\gamma(\sigma)\varphi_\gamma(\tau). \tag{2}$$

Conversely, if such an isomorphism $\sigma \to \varphi(\sigma)$ of the Galois group K/k into the automorphism group of the field $K(x, y)$ is given, with $\sigma = \varphi(\sigma)$ on K, then the subfield of functions in $K(x, y)$ invariant with respect to all $\varphi(\sigma)$ defines some elliptic curve over k, birationally equivalent to ω over K. It is not difficult to verify that two curves γ_1 and γ_2 of the class under consideration

of the type will then, and only then, be birationally equivalent over k when

$$\varphi_{\gamma_1}(\sigma) = t\varphi_{\gamma_2}(\sigma)t^{-1}, \tag{3}$$

where t is some automorphism of the field $K(x, y)$ that does not change the elements of the field K.

The automorphism $s_\gamma(\sigma)$ of the field $K(x, y)$, defined by the equality

$$\varphi_\gamma(\sigma) = s_\gamma(\sigma)\varphi_\omega(\sigma),$$

obviously does not change the elements of the field K, i.e. is an automorphism of $K(x, y)/K$. In order that relation (2) be satisfied, it is necessary and sufficient that $s_\gamma(\sigma)$ satisfy the conditions

$$s_\gamma(\sigma\tau) = s_\gamma(\sigma)s_\gamma(\tau)^{\varphi_\omega(\sigma)},$$

where

$$s_\gamma(\tau)^{\varphi_\omega(\sigma)} = \varphi_\omega(\sigma)s_\gamma(\tau)\varphi_\omega(\sigma)^{-1},$$

and condition (3) is rewritten in the form

$$s_{\gamma_1}(\sigma) = ts_{\gamma_2}(\sigma)t^{-\varphi_\omega(\sigma)}.$$

The automorphisms s of the field $K(x, y)/K$ are well known ([3]). They have the form

$$s(x, y) = \varepsilon(x, y) + P, \tag{4}$$

where P is some point on ω with coordinates in K, and addition is understood in the sense of addition of points on ω. If $j \neq 0, 1$, then

$$\varepsilon(x, y) = (x, \pm y),$$

whereas if $j = 0$ or 1, then ε may be one of six or four automorphisms not changing the point at infinity of ω. Writing the automorphisms $s_\gamma(\sigma)$ in the form (4), we arrive at the following result:

Theorem 1. *Each elliptic curve γ over k, birationally equivalent over K to the curve ω with equation (1), determines a system of automorphisms $\varepsilon_\gamma(\sigma)$ of the field $K(x, y)$ and of points $P_\gamma(\sigma)$ of the curve ω over K. The relations*

$$\begin{aligned} \varepsilon_\gamma(\sigma\tau) &= \varepsilon_\gamma(\sigma)\varepsilon_\gamma(\tau)^\sigma, \\ P_\gamma(\sigma\tau) &= P_\gamma(\sigma)\varepsilon_\gamma(\tau)^\sigma + P_\gamma(\tau)^\sigma. \end{aligned} \tag{5}$$

hold.

Every system of automorphisms and points satisfying these conditions is determined by some curve γ. The curves γ_1 and γ_2 are birationally equivalent over k if and only if there exist an automorphism ε and a point P on ω such that

$$\varepsilon_{\gamma_1}(\sigma) = \varepsilon_{\gamma_2}(\sigma)\varepsilon^{1-\sigma},$$

$$P_{\gamma_1}(\sigma) = \varepsilon^{-\sigma}(P_{\gamma_2}(\sigma) + \varepsilon_{\gamma_2}(\sigma)P - P^\sigma). \tag{6}$$

3. In the set of curves under consideration there may be several curves having Weierstrass form. We could take any one of them as ω. It can be shown that the curve γ can be reduced over k to Weierstrass form if and only if γ is birationally equivalent over k to a curve γ' for which $P_{\gamma'}(\sigma) = O$ (the zero of the group of points on ω). Thus, in the totality of all curves with one system of automorphisms $\varepsilon_\gamma(\sigma)$, there is, up to birational equivalence, exactly one curve having Weierstrass form over k. If we took it as ω, then all curves to which, in the first description, the system of automorphisms $\varepsilon_\gamma(\sigma)$ corresponded would correspond, as can be shown,

it is, the identity system of automorphisms. In view of this we shall restrict ourselves to considering curves for which $\varepsilon_\gamma(\sigma) = 1$. The equalities (5) and, for $\varepsilon = 1$, (6) then pass into the definitions of a crossed homomorphism and of a principal crossed homomorphism [4].

If for the curve γ $\varepsilon_\gamma(\sigma) = 1$, then the curve ω is its Jacobian variety [5].

Indeed, in view of the fact that $K(x, y) = K(M)$,

$$(x, y) = \Phi(M),$$

where Φ is a birational mapping of γ onto ω over K. For the divisor $\mathfrak{A} = \mathfrak{P}_1^{a_1} \cdots \mathfrak{P}_r^{a_r}$ on γ put

$$\Phi(\mathfrak{A}) = a_1\Phi(\mathfrak{P}_1) + \cdots + a_r\Phi(\mathfrak{P}_r).$$

As is known, if $d(\mathfrak{A}) = d(\mathfrak{B}) = 0$, then $\mathfrak{A} \sim \mathfrak{B}$ on γ if and only if $\Phi(\mathfrak{A}) = \Phi(\mathfrak{B})$. It remains only to verify that if $d(\mathfrak{A}) = 0$ and $\mathfrak{A}$ is defined over some field $k' \supset k$, then $\Phi(\mathfrak{A})$ is also defined over k'. This follows easily from (4): if σ is an isomorphism Kk'/k', then

$$(\Phi(\mathfrak{A}))^\sigma = \Phi^\sigma(\mathfrak{A}^\sigma) = \Phi(\mathfrak{A}^\sigma) + (\Sigma a_r)P_\sigma = \Phi(\mathfrak{A}) + d(\mathfrak{A})P_\sigma = \Phi(\mathfrak{A}).$$

Thus the set of elliptic curves over k having ω as their Jacobian variety and birationally equivalent to ω over K is mapped onto the set of crossed homomorphisms of the Galois group G of the field K/k into the group of points $\mathfrak{A}_K$ on ω with coordinates in K. Formulas (6) show that two curves of the type under consideration are birationally equivalent over k only if: either 1) the corresponding crossed homomorphisms differ by a principal crossed homomorphism, or 2) one of them is obtained from the other by applying an automorphism ε of the curve ω, considered as an algebraic group. If we include in the concept of an elliptic curve with given Jacobian variety ω also the canonical function Φ, mapping the group of divisor classes of degree zero on γ onto the curve ω, then transformations of the second type with $\varepsilon \neq 1$ disappear, and the birational (in the new sense) classes of curves γ will be in one-to-one correspondence with the elements of the one-dimensional cohomology group [4] $H^1(G, \mathfrak{A}_K)$. The group operation defined on $H^1(G, \mathfrak{A}_K)$ is naturally transferred to these classes. All curves with Jacobian variety ω are obtained if one considers the union of all fields K and correspondingly the inductive limit of the group $H^1(G, \mathfrak{A}_K)$. Thus we arrive at the following result:

Theorem 2. *The birational classes of elliptic curves over k with given Jacobian variety ω form a group isomorphic to $H(\mathfrak{G}, \mathfrak{A}_{\tilde{k}})$, where $\mathfrak{G}$ is the Galois group of the separable algebraic closure $\tilde{k}$ of the field k, and $\mathfrak{A}_{\tilde{k}}$ is the group of points on ω with coordinates in $\tilde{k}$. Here crossed homomorphisms are regarded as continuous, $\mathfrak{G}$ is topologized by Krull' s topology [6], and $\mathfrak{A}_{\tilde{k}}$ is discrete.*

As the union of cohomology groups of finite groups, the group $H^1(\mathfrak{G}, \mathfrak{A}_{\tilde{k}})$ is periodic. It can be shown that the order of an elliptic curve γ in this group is divisible by the least order of a divisor class on γ.

4. If k is a field of algebraic numbers, then by the Mordell-Weil theorem [7] the group $\mathfrak{A}_K$ has a finite number of generators. Consequently the same is

true for $H^1(G, \mathfrak{A}_k)$; but since this group is periodic, it is finite. Together with Theorems 1 and 2 this leads us to the following result:

Theorem 3. *There are only finitely many birationally inequivalent curves over the field of algebraic numbers k that have*

a given value of the absolute invariant j and a divisor of the first degree in a given finite extension K/k.

In view of Lutz' s theorem [8] the same is true when k is the field of p-adic numbers. But since over the field of p-adic numbers there are only finitely many extensions of a given degree, the following stronger assertion holds:

Theorem 4. *All elliptic curves of a given degree and with a given value of the absolute invariant j split into a finite number of birational classes over the field k of p-adic numbers.*

The analogous theorem is not true for the rational numbers, even if one restricts oneself to curves with a given Jacobian variety. Indeed, the curves with equation (in homogeneous coordinates)

$$a_0 x_0^3 + a_1 x_1^3 + a_2 x_2^3 = 0$$

have as their Jacobian variety the curve

$$a_0 a_1 a_2 x_0^3 + x_1^3 + x_2^3 = 0.$$

Consequently, for $a_i = p^i$ $(i = 0, 1, 2)$ and an arbitrary prime p, we obtain infinitely many curves with a common Jacobian variety and birationally inequivalent to one another, since they are not equivalent even over the field of p-adic numbers.

5. In a recently published paper [9], Weil defines the group of principal homogeneous algebraic spaces with a given abelian group of operators. Since every elliptic curve is a homogeneous space with respect to its Jacobian variety, Weil' s result is applicable to our case. It can be shown that the group he defines is isomorphic to that described by Theorem 2. The same considerations that we used in deriving this theorem are also applicable to the case considered by Weil, so that the following theorem holds.

Theorem 5. *The group of principal homogeneous algebraic spaces over k with a given commutative abelian group G is isomorphic to the one-dimensional cohomology group $H^1(\mathfrak{G}, \mathfrak{A}_{\tilde{k}})$, where $\mathfrak{G}$ is the Galois group of the separable algebraic closure $\tilde{k}/k$; $\mathfrak{A}_{\tilde{k}}$ is the group of points on ω with coordinates in $\tilde{k}$.*

Received12 XI 1956

CITED LITERATURE

[1] R. Walker, *Algebraic Curves*, IL, 1951.
[2] M. Deuring, *Math. Zs.*, **47**, 4756 (1941).
[3] H. Hasse, *J. f. Math.*, **175**, No. 2 (1936).
[4] A. G. Kurosh, *Group Theory*, Moscow, 1953.
[5] W. L. Chow, *Am. J. Math.*, **76**, No. 2 (1954).
[6] W. Krull, *Math. Ann.*, **100**, 687 (1928).
[7] A. Weil, *Bull. Sci. Math.*, 2 ser., **54**, 182 (1930).
[8] E. Lutz, *J. f. Math.*, **177**, No. 4 (1937).
[9] A. Weil, *Am. J. Math.*, **77**, No. 3 (1955).

Note: Figure translations are in progress. See original paper for figures.