EXPONENTS OF ELLIPTIC CURVES

1957

Abstract

Full Text

MATHEMATICS

I. R. SHAFAREVICH

EXPONENTS OF ELLIPTIC CURVES

(Presented by Academician I. M. Vinogradov on 26 XII 1956)

To an algebraic curve γ, defined over a field k, one may assign, besides the genus g, several further integral invariants: the least positive degree f of a divisor on γ; the least degree d of a curve birationally equivalent to γ over k; the least degree ν of a prime divisor on γ. The relations between these invariants have been little studied in the case of arbitrary curves, but for elliptic curves ($g = 1$) they are all expressed in terms of one of them; namely, as follows easily from the Riemann-Roch theorem, for an elliptic curve $\nu = f$, $d = f$ for $f > 2$; $d = 4$ for $f = 2$ and $d = 3$ for $f = 1$. We shall call the invariant f the **exponent** of the curve γ.

For a curve of genus g, $f \mid 2g - 2$, and therefore for $g \neq 1$ the exponent can assume only a finite number of values. For elliptic curves, as already noted (see, for example, ([1,2])), it is unknown what values the exponent may assume. In this note it will be proved that over the field of rational numbers R there exist elliptic curves γ with arbitrarily large exponent, and moreover the Jacobian curve ω of the curve γ can even be prescribed arbitrarily.

For the proof we use the group $H(\omega)$ formed by the classes of curves birationally equivalent over k with a given Jacobian curve ω. This group was first defined by A. Weil ([3]). In what follows we shall use the construction of the group $H(\omega)$ given in my paper ([4]). As shown in that paper, the exponent of the curve γ is a multiple of the order of γ as an element of the group $H(\omega)$. It is also shown there that the subgroup $H(K, \omega)$ of the group $H(\omega)$, consisting of all curves in $H(\omega)$ that have a prime divisor of first degree in a given normal extension K of the field R, is isomorphic to the group $H^1(G, \mathfrak{A}_K)$, where G is the Galois group K/R; $\mathfrak{A}_K$ is the group of points on ω with coordinates in K, and $H^1(G, \mathfrak{A}_K)$ is the group of crossed homomorphisms of G into $\mathfrak{A}_K$.

If $\mathfrak{p}$ is a prime divisor of K; p is the prime number divisible by it; $G_\mathfrak{p}$ is the decomposition group of $\mathfrak{p}$, and $K_\mathfrak{p}$ and R_p are the corresponding local fields, then there is a natural embedding homomorphism:

$$\varphi_\mathfrak{p}: \quad H^1(G; \mathfrak{A}_K) \to H^1(G_\mathfrak{p}, \mathfrak{A}_{K_\mathfrak{p}}). \tag{1}$$

We shall first consider the group $H^1(G_\mathfrak{p}, \mathfrak{A}_{K_\mathfrak{p}})$.

Let the equation of ω have the form

$$y^2 = x^3 + ax + b, \qquad \Delta = 4a^3 + 27b^2 \neq 0,$$

where a and b may be taken to be rational integers. Denote by H_p the subgroup of those elements of the group H whose orders are relatively prime to p.

In studying the group $H^1(G_\mathfrak{p}, \mathfrak{A}_{K_\mathfrak{p}})_p$ one may assume that the field $K_\mathfrak{p}$ has no higher ramification, since otherwise one can

one could pass to some subgroup of it. Denote by $\mathfrak{A}'_{K_p}$ the subgroup $\mathfrak{A}_{K_p}$, considered by Lutz [5], consisting of the points (x, y) on ω for which $xp^{2(r-1)}$ and $yp^{3(r-1)}$ are integral. It is easy to prove that, for $r > 1$, the group $\mathfrak{A}'_{K_p}/\mathfrak{A}'^{r+1}_{K_p}$ is a p-group. From this it is easy to deduce that the group $H^1(G_p, \mathfrak{A}_{K_p})_p$ is isomorphic to the group $H^1(G_p, \mathfrak{A}'_{K_p}/\mathfrak{A}'^{r}_{K_p})_p$.

Suppose, in addition, that $p \nmid \Delta$. Then, as shown in [5], the group $\mathfrak{A}_{K_p}/\mathfrak{A}^1_{K_p}$ is isomorphic to $\mathfrak{A}_{\mathfrak{K}_p}$, where $\mathfrak{K}_p$ is the residue class field of K_p modulo $\mathfrak{p}$, and $\mathfrak{A}_{\mathfrak{K}_p}$ is the group of points on the curve ω, considered modulo p. Denote by F_p the inertia group of $\mathfrak{p}$ in K_p. Then G_p/F_p is the Galois group of the field $\mathfrak{K}_p$, and G_p is a group of operators for $\mathfrak{A}_{\mathfrak{K}_p}$, with F_p acting trivially. As was said,

$$H^1(G_p, \mathfrak{A}_{K_p})_p \simeq H^1(G_p, \mathfrak{A}_{\mathfrak{K}_p})_p.$$

Consider the restriction homomorphism

$$H^1(G_p, \mathfrak{A}_{\mathfrak{K}_p})_p \to H^1(F_p, \mathfrak{A}_{\mathfrak{K}_p})_p. \tag{2}$$

The kernel of this mapping consists of homomorphisms that become 0 on F_p and, consequently, are homomorphisms of G_p/F_p into $\mathfrak{A}_{\mathfrak{K}_p}$. Since for curves over finite fields, as is known [6], $f = 1$, we have

$$H^1(G_p/F_p, \mathfrak{A}_{\mathfrak{K}_p}) = 0,$$

and therefore the homomorphism (2) is a monomorphism. It is easy to see that the image of this homomorphism coincides with the group $\mathrm{Hom}_{G_p/F_p}(F_p, \mathfrak{A}_{\mathfrak{K}_p})$ of operator G_p/F_p-homomorphisms of F_p into $\mathfrak{A}_{\mathfrak{K}_p}$. We arrive at the following result:

Theorem 1. If $p \nmid \Delta$ and the field K_p has no higher ramification, then

$$H^1(G_p, \mathfrak{A}_{K_p})_p \simeq \mathrm{Hom}_{G_p/F_p}(F_p, \mathfrak{A}_{\mathfrak{K}_p}).$$

Now we shall construct a field K in which there is a crossed homomorphism $f \in H(G, \mathfrak{A}_K)$ of a prescribed order m. To do this, consider all algebraic points

P on ω for which $mP = 0$. They form a group $\mathfrak{A}_m$, which is the sum of two cyclic groups of order m. Denote by T_m the field obtained by adjoining to R the coordinates of $P \in \mathfrak{A}_m$. This field is normal. Denote its Galois group by $\overline{G}$. Obviously, for $\sigma \in \overline{G}$, $P \in \mathfrak{A}_m$ and $P^\sigma \in \mathfrak{A}_m$, and σ defines an automorphism of the group $\mathfrak{A}_m$. Consider the group G, containing a normal divisor A, isomorphic to $\mathfrak{A}_m$, and which is the semidirect product of $\overline{G}$ and A with automorphisms

$$\alpha^\sigma = \varphi^{-1}(\varphi(\alpha)^\sigma), \qquad \alpha \in A, \tag{3}$$

where φ is some fixed isomorphism of A onto $\mathfrak{A}_m$.

Construct a field K, containing T_m, normal over R, and having over it Galois group G. The existence of such a field follows from the results of Scholz [7] and Delone and Faddeev [8]. Constructing the field K by any of these methods, one may arrange that any prime divisor $\mathfrak{p}$ of the field T_m has ramification exponent m in K. We shall choose $\mathfrak{p}$ relatively prime to the discriminant of T_m/R, to m, to Δ, and to 2.

Define a mapping f of the group G into $\mathfrak{A}_K$ as follows:

$$f(\sigma\alpha) = \varphi(\alpha), \qquad \sigma \in \overline{G}, \quad \alpha \in A.$$

From (3) it is easy to derive that f is a crossed homomorphism, i.e. $f \in H'(G, \mathfrak{A}_K)$. Obviously, $mf = 0$. We shall show that f has in $H'(G, \mathfrak{A}_K)$ order exactly equal to m. For this it suffices to prove that its image $\varphi_\mathfrak{p} f$ under the homomorphism $\varphi_\mathfrak{p}$, defined in (1), has order m. By Theorem 1 this will be proved if we prove that $\varphi_\mathfrak{p} f$, as an operator homomorphism $F_\mathfrak{p}$ into $\mathfrak{A}_{\overline{K}_\mathfrak{p}}$, has order m. The latter assertion follows from the fact that, by the choice of $\mathfrak{p}$, the group $F_\mathfrak{p}$ is cyclic of order m, and f maps its generator to an element P of $\mathfrak{A}_m$ which has order m; and since $\mathfrak{p}$ is not critical in T_m, the image of P in $\mathfrak{A}_{\overline{K}_\mathfrak{p}}$ has the same order.

We have arrived at the final result:

Theorem 2. *In the group of elliptic curves having over the field of rational numbers a prescribed Jacobian curve, there exist elements of any order.*

Corollary. Among the elliptic curves having over the field of rational numbers a prescribed Jacobian curve, there exist curves whose exponent is divisible by any preassigned number.

All the proofs, with considerable simplifications, also carry over to the field of rational functions over the field of complex numbers. The fact itself was noted in this case without detailed proofs by Enriques[9].

Let us note that for the field of p-adic numbers the analogous theorem is not true. Indeed, Theorem 1 shows that if the discriminant ω is not divisible by p, then the exponents of curves having ω as their Jacobian curve can be divisible

only by p and by the prime divisors of the number of points on ω in the residue field modulo p.

Received
20 XII 1956

CITED LITERATURE

[1] H. Hasse, *Zahlentheorie*, Berlin, 1949.
[2] A. Weil, *Arch. d. Math.*, **5**, No. 1–3, 197 (1954).
[3] A. Weil, *Am. J. Math.*, **77**, No. 3, 493 (1955).
[4] I. R. Shafarevich, *DAN*, **114**, No. 2 (1957).
[5] E. Lutz, *J. f. reine u. angew. Math.*, **177**, No. 4, 238 (1937).
[6] F. K. Schmidt, *Math. Zs.*, **33**, No. 1, 1 (1931).
[7] A. Scholz, *Math. Zs.*, **30**, 332 (1929).
[8] B. N. Delaunay, D. K. Faddeev, *Matem. sborn.*, **15** (57), 243 (1944).
[9] F. Enriques, *Math. Ann.*, **51**, 134 (1899).

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