Mathematics

1961

SovietRxiv

Abstract

Full Text

Mathematics

D. K. FADDEEV

ON THE GROUP OF DIVISOR CLASSES ON CERTAIN ALGEBRAIC CURVES

(Presented by Academician I. M. Vinogradov, 23 VII 1960)

1°. The purpose of the present note is to set out a scheme (with details omitted) for proving the finiteness of the group of divisor classes of degree zero in the fields of algebraic functions $k_0(x, y)$, $y^l = x^k(1-x)$ for $l = 5, 7;\ 1 \leq k \leq l-2$, and for $l = 11,\ k = 1, 5, 9$. The field of constants k_0 is the field of rational numbers with an adjoined primitive l-th root ε of unity.

2°. Let k_0 be an arbitrary field of characteristic 0, algebraically closed in the field $S = k_0(x, y)$ of algebraic functions of one variable. Suppose that in the field S there exist divisors of degree one. Let $\bar{k}_0$ be the algebraic closure of k_0 and $\bar{S} = \bar{k}_0(x, y)$. To any divisor class A of the field S one may associate a finite algebraic extension k_A of the field k_0, formed by the elements of the field $\bar{k}$ invariant with respect to the group of all automorphisms $\bar{k}_0/k_0$ that carry some divisor of the class A into equivalent ones. The field k_A has the property that in $S_A = k_A(x, y)$ there exists a divisor rational (with respect to k_A) from the class A (see, for example, ([1]), Theorems 8 and 9), and every field k' such that in the field $k'(x, y)$ there exists a divisor rational (with respect to k') from the class A, contains k_A. Any subfield $k' \supset k_A$ of the field $\bar{k}_0$ will be called a field of definition of the class A.

3°. Let $S = k_0(x, y)$, $y^l = x^k(1-x)$, $1 \leq k \leq l-2$, l prime, and let k_0 contain a primitive l-th root ε of unity. The genus g of the field S is equal to $\dfrac{l-1}{2}$.

The following decompositions into prime divisors hold: $(x) = P_0^l P_\infty^{-l}$; $(1-x) = P_1^l P_\infty^{-l}$; $y = P_0^k P_1 P_\infty^{-l-1}$. On the Jacobian variety of the field $S = \bar{k}_0(x, y)$ a complex multiplication by the integers of the field $R(\varepsilon)$, induced by the automorphism $x \to x,\ y \to y\varepsilon$ of the field S, is defined ([2]). The equation $B^{1-\varepsilon} = A$, for a given class A of divisors of degree zero of the field S, has exactly l solutions, and if B_0 is one of them, then the others are $B_0 M_0^a$, $1 \leq a \leq l-1$, where M_0 is the class containing $P_0 P_\infty^{-1}$. Hence it follows easily that if the class A is rational over the field $k(x, y)$, then the minimal field k' of definition of the classes B over k is either equal to k, or is its cyclic extension of degree l.

4°. To each class A of divisors of degree zero of the field $S(x, y)$, rational over $k \supseteq k_0$, we associate, as an invariant, an element of the group k^*/k^{*l} by the

formula $j(A) = ((x), \mathfrak{A})\, k^{*l}$, where $\mathfrak{A}$ is some divisor rational over k from the class A,

$$\mathfrak{A} = \prod P_i^{a_i}; \qquad [((x), \mathfrak{A})] = \prod_i (x(P_i))^{a_i} \quad (1).$$

In the last product, the factors corresponding to the points P_0 and P_∞, if they are present in the decomposition of the divisor $\mathfrak{A}$, must be omit-

valued. It is easy to verify that $j(A)$ does not depend on the choice of the representative $\mathfrak{A}$ in the class A. The mapping $A \to j(A)$ is, obviously, a homomorphism. The group of values of the invariants (for fixed k) is generated by the norms of the abscissae of points on the curve $y^l = x^k(1-x)$ with coordinates algebraic over k.

5°. **Theorem 1.** *Let A be a divisor class of degree zero of the field $k(x, y)$, $k \supset k_0$. In order that the equation $B^{\varepsilon-1} = A$ be solvable in the group of classes rational over $k(x, y)$, it is necessary and sufficient that $j(A) = 1$.*

Proof. If $A = B^{\varepsilon-1}$, then $j(A) = 1$, since for any $\mathfrak{A} \in A$ the abscissae of the points from which the divisors $\mathfrak{A}^\varepsilon$ and $\mathfrak{A}$ are composed are the same. To prove sufficiency, first note that if $j(A) \neq 1$, then the field

$$k_1 = k(\sqrt[l]{j(A)})$$

is a cyclic extension of degree l over k, and it is contained in the minimal field of definition of the class B, which, by 3°, is itself a cyclic extension of degree l over k. Therefore B is rational over k_1. It remains to verify the validity of this assertion also for the case $j(A) = 1$. This is done by considering the "general class," for which the assertion will be true. On passing to specializations into classes rational over k, the validity of the assertion is not destroyed.

6°. Let now $k_0 = R_l(\varepsilon)$ be the l-adic completion of the field of division of the circle into l parts. It is known that $k_0 = R_l(\lambda)$, where $\lambda^{l-1} = -l$. As representatives of the elements of the group k_0^*/k_0^{*l} one may take $E_0 = \lambda$, $E_1 = \varepsilon$, $E_a = \exp(\lambda^a)$, $2 \leq a \leq l$.

Theorem 2. *The group of invariants of divisor classes of degree zero of the field $k_0(x, y)$, $y^l = x^k(1-x)$, is generated by the numbers E_a for $a = \dfrac{l-1}{2}$, $\dfrac{l+3}{2} \leq a \leq l$, if $\left(\dfrac{W}{l}\right) = 1$, or $\dfrac{l+1}{2} \leq a \leq l$, if $\left(\dfrac{W}{l}\right) \neq 1$. Here the parentheses denote the quadratic Legendre symbol,*

$$W = \frac{2k}{(k+1)^3} \frac{1}{l} \left[\frac{k^{k(l-1)}}{(k+1)^{(k+1)(l-1)}} - 1 \right].$$

Proof is based on the consideration of explicit formulas (in the form of infinite series) for the abscissae of the solutions of the equation $x^k(1-x) = y^l$ in algebraic extensions of the field k_0, followed by passage to norms. The Riemann-Roch theorem makes it possible to restrict oneself to extensions whose degree does not exceed $g = \dfrac{l-1}{2}$.

7°. If k_0 is a finite extension of the field $R(\varepsilon)$, then, according to A. Weil' s theorem ([3]), the number of generators of the group of divisor classes of degree zero is finite. It is easy to see that the number of generators of the group of invariants (coinciding with the number of generators of the group $A/A^{\varepsilon-1}$) is equal to $\dfrac{r}{l-1}+1$, where r is the number of generators of infinite order of the group of divisor classes of degree zero. The summand 1 appears on account of the classes with period l^m, $m \geq 1$, which for the curves $y^l = x^k(1-x)$ certainly exist. On the other hand, it is easy to see that the group of invariants is contained in the group $(\alpha : k_0^{*l})$, where α are numbers whose principal ideals are l-th powers. Therefore

$$\frac{r}{l-1}+1 \leq \frac{n}{2}+\rho.$$

Here n is the absolute degree of the field k_0; ρ is the number of generators of the l-primary part of the ideal class group of the field k_0.

8°. Let now $k_0 = R(\varepsilon)$ and let l be a regular prime. In this case $\rho = 0$. The fundamental units may be chosen to be l-equal (after embedding in the field $R_l(\varepsilon)$) to the units $E_1 = \varepsilon$, E_{2a}, $a = 1, \ldots, \dfrac{p-3}{2}$, and the units of the field $R(\varepsilon)$ that are l-th powers in the field $R_l(\varepsilon)$ will be l-th powers also in the field $R(\varepsilon)$. As class invariants in the field $R(\varepsilon)$ only those units of the field $R(\varepsilon)$ can be realized which are invari-

classes in the field $R_l(\varepsilon)$. Applying Theorem 2, it is easy to obtain the estimates

$$\frac{r}{l-1}+1 \leq M,$$

where

$$\begin{aligned}
M &= \frac{l-1}{4} \quad \text{for } l \equiv 1 \pmod 4, \quad \left(\frac{W}{l}\right) = 1;\\
M &= \frac{l-5}{4} \quad \text{for } l \equiv 1 \pmod 4, \quad \left(\frac{W}{l}\right) \neq 1;\\
M &= \frac{l-3}{4} \quad \text{for } l \equiv 3 \pmod 4, \quad \left(\frac{W}{l}\right) \neq 1;\\
M &= \frac{l-7}{4} \quad \text{for } l \equiv 3 \pmod 4, \quad \left(\frac{W}{l}\right) = 1.
\end{aligned}$$

These estimates give, for $l = 5$ and $l = 7$, that $r = 0$, i.e., for $l = 5$ and $l = 7$ the divisor class group turns out to be finite. For $l = 11$, when $k = 1, 5, 9$ (the

corresponding curves are birationally equivalent), one also obtains $r = 0$. For the curves with $k = 2, 3, 4, 6, 7, 8$ (which are also birationally equivalent), the question of finiteness of the divisor class group of degree zero remains open. It remains open also for all primes $l \geq 13$.

9°. For the Fermat curves $x^5 + y^5 = 1$, $x^7 + y^7 = 1$, the divisor class group of degree zero is finite, for the Jacobian variety of the curve $x^l + y^l = 1$ is mapped with finite kernel onto the direct sum of the Jacobian varieties of the curves

$$x^k(1 - x) = y^l, \quad k = 1, 2, \ldots, l - 2 \quad (^4).$$

10°. The curve $x^2(1 - x) = y^7$ is birationally equivalent to the Klein curve

$$x^3y + y^3 + x = 0,$$

so that the class group for this curve over the field $R(\sqrt[7]{1})$ is finite. This can also be verified by decomposing the Jacobian variety (see $(^2)$) into three curves of genus 1, each of which is birationally equivalent (over the field $R(\varepsilon)$) to the curve

$$y^2 = x^3 - \frac{5}{7}x + \frac{2}{7},$$

on which the number of points in the field $R(\varepsilon)$ is computed directly and turns out to be equal to 28.

11°. For the curve $x^6 + y^6 = 1$ over the field of rational numbers, the divisor class group of degree zero is infinite, for it is infinite for the subfield $R(u, v)$ of the field $R(x, y)$,

$$u = \frac{x^6 - y^6}{x^3y^3}, \quad v = \frac{1}{x^2y^2}, \quad u^2 + 4 = v^3.$$

Leningrad Branch
of the V. A. Steklov Mathematical Institute
Academy of Sciences of the USSR

Received
20 VII 1960

REFERENCES

1. D. K. Faddeev, *Vestn. LGU*, No. 7 (1957).
2. S. Lefschetz, *Trans. Am. Math. Soc.*, **22**, No. 3, 327 (1922).
3. A. Weil, *Acta Math.*, **52** (1959).
4. D. K. Faddeev, *DAN*, **134**, No. 4 (1950).

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

Source: Math-Net.Ru and CyberLeninka. Machine translation. Verify with the original.