Reports of the Academy of Sciences of the USSR

Yu. I. Manin

1962

SovietRxiv

Abstract

Full Text

Reports of the Academy of Sciences of the USSR

1962. Volume 145, No. 2

MATHEMATICS

Yu. I. Manin

COMMUTATIVE FORMAL GROUPS

AND ABELIAN VARIETIES

(Presented by Academician I. M. Vinogradov on 22 II 1962)

1. The definition of a formal group and the functor that assigns a formal group to every algebraic group are described in the works ([3,8,9]). The role of formal groups in the theory of algebraic groups, at least externally, is similar to the role of local Lie groups in the theory of Lie groups. However, the parallelism between the local and global theories in the algebraic case (under the assumption of finiteness of the characteristic p of the ground field, which we shall constantly assume in what follows) turns out to be considerably less close than in the case of Lie groups. Slightly generalizing Dieudonné' s definition ([2]), we shall call a formal group G **representable** if there exists a monomorphism of it into a formal group which is the localization of an algebraic group. We shall call a representable formal group G **fully representable** if such a monomorphism can be found which is even an isomorphism. The problem of describing representable formal groups in the noncommutative case was significantly advanced by Dieudonné in the works ([3,4]). In particular, it turned out that all simple noncommutative groups are fully representable. In the commutative case this is certainly not so: from Theorem 2 of ([9]) it follows that the simple groups $G_{n,m}$, for $1 < mn < \infty$, are not fully representable. The main purpose of this note is to show that, nevertheless, **all commutative formal groups over an algebraically closed field of finite characteristic p are representable**.
2. All algebraic and formal groups and their morphisms will henceforth be assumed to be defined over a fixed algebraically closed field of characteristic $p > 0$; departures from this convention will be specifically noted. We shall deal only with commutative groups.

The property of a formal group G of being representable or fully representable is a property of the whole class of groups isogenous to G (cf. ([1])). The groups

$G_{1,0}$, $G_{1,1}$, and $G_{n,\infty}$ $(n \geq 1)$ are fully representable. Therefore it remains to clarify the question of representability of the groups $G_{n,m}$, $1 < mn < \infty$. Any homomorphism of such a group into the localization of a linear commutative group is trivial, for, as follows from the structure theorem for commutative linear algebraic groups, their localizations are isogenous to formal groups of the form

$$r_0 G_{1,0} + \sum_{i \geq 1} r_{iG_{i,\infty}}.$$

Therefore, if the simple groups $G_{n,m}$ $(1 < mn < \infty)$ are representable, they must occur in the localizations of abelian varieties.

3. The initial results on the local structure of abelian varieties were obtained in the author' s paper ([9]). The first theorem, which we formulate below, establishes a close connection between the local structure of an abelian variety defined over a finite field and such a global invariant of this variety as its zeta-function in the sense of Weil. The local decomposition of an abelian variety in the sense of the theory of formal groups turns out, in a certain respect, to be—

is a parallel local (in the p-adic sense) decomposition of the characteristic polynomial of the Frobenius endomorphism. In rudimentary form this connection can already be traced in the paper ([9]).

Theorem 1. *Let X be an abelian variety of dimension n, which has a finite field of definition k_a consisting of p^a elements. Denote by the symbol $\pi : X \to X$ the endomorphism of the k_a-structure of this variety induced by raising elements of local rings to the power p^a. Let*

$$P(T) = T^{2n} + \ldots + p^{an}$$

be the characteristic polynomial of the endomorphism π in the sense of A. Weil; let Ω be the integral closure of the ring of rational p-adic integers; let v be the p-adic valuation on Ω, normalized by the condition $v(p) = 1$. Suppose that the decomposition of the polynomial $P(T)$ in the ring $\Omega[T]$ has the form

$$P(T) = \prod_{i=1}^{2n} (T - \tau_i); \qquad v(\tau_i) = ac_i, \quad 0 \leq c_i \leq 1.$$

Suppose further that all roots τ_i belong to the ring $\Omega_0[p^{1/e}]$, where Ω_0 is an unramified subring of Ω, and e is some integer. Denote by r_c the number of roots τ_i for which $v(\tau_i) = ac$. Put $n_c = cr_c$, $m_c = r_c - n_c$. Then the localization X_* of the abelian variety X over an algebraically closed field of definition is isogenous to a formal group of the form

$$X_* \sim r_0 G_{1,0} + \sum_{0<c<1/2} \left(G_{n_c,m_c} + G_{m_c,n_c} \right) + {}^1/_2 r_{1/2} G_{1,1}. \qquad (1)$$

The formulation of the theorem requires some comments. First of all, the numbers n_c, m_c need not be relatively prime. In this case we agree to identify (up to isogeny) the group $G_{dn,dm}$, $(n,m)=1$, with the group $dG_{n,m}$. Thus decomposition (1) is rather a decomposition into isotypic components than into simple components. Further, taking into account that together with any root τ the polynomial $P(T)$ also has the root $p^a\tau^{-1}$, we obtain the identities

$$n = \sum_{0\le c\le 1} cr_c = r_0 + \sum_{0<c<1} cr_c; \quad r_c = r_{1-c}.$$

Consequently,

$$n = r_0 + \sum_{0<c<1/2} (cr_c + (1-c)r_c) + {}^1\!/_2 r_{1/2},$$

so that the dimensions of the groups on the right and left in relation (1), as they should, coincide. Finally, from decomposition (1) it follows that any group $G_{n,m}$, $1 < mn < \infty$, enters into the local decomposition of an abelian variety X necessarily together with the group $G_{m,n}$. This last fact remains true even if one does not assume the existence of a finite field of definition of the variety X. It is a reflection of a certain duality of Dieudonné modules.

The proof of Theorem 1 is based on the fact that the polynomial $P(T)$ determines the local structure of the variety X over the field k_a, because the characteristic polynomial of the endomorphism π in the sense of Weil coincides with the characteristic polynomial of the representation of π on the direct sum of the Dieudonné module of the formal group $\hat{X}_*$ and the "Tate p-group" of the variety $\hat{X}$ (dual to X) (cf. ([7]), note on p. 716, and ([6]), Ch. IV, § 4). To the second summand there corresponds the factor

$$\prod_{v(\tau)=1} (T-\tau)$$

of the polynomial $P(T)$, which corresponds to the "toroidal component" $rG_{1,0}$ in decomposition (1). The complementary factor (from it there is split off

also the factor

$$\prod_{\nu(\tau)=0} (T-\tau),$$

describing the components $\sum_{nm>1} G_{n,m}$, should, in order to compute the invariants (n,m), be decomposed in the ring of Hilbert (noncommutative) power series in T (see ([6])). It can be shown that the "ramification indices" under such a decomposition remain the same as under decomposition in the ordinary polynomial ring. This fact constitutes the main content of the theorem.

4. Theorem 2. *Every Abelian formal group is representable.*

Proof. This is an existence theorem; we shall prove it by effectively constructing a sequence of Abelian varieties of increasing dimension whose local decompositions contain all possible groups $G_{n,m}$. It is enough to consider the sequence $\{J_a\}$ of Jacobian varieties of the curves

$$y^p - y = x^{p^a-1}, \quad a = 1, 2, \ldots$$

(Recall that p is the characteristic of the field of constants; on J_a we consider the k_a-structure induced by the natural k_a-structure of the corresponding curve. The Frobenius endomorphism on J_a is thereby induced by the mapping $(x, y) \mapsto (x^{p^a}, y^{p^a})$.) The form of the polynomial $P_a(T)$ is well known; its roots are trigonometric sums of the form

$$\tau(\chi, \psi) = \sum_{t \in k_a^*} \chi(t)\psi(t),$$

where χ runs through the nontrivial multiplicative characters, and ψ through the nontrivial additive characters of the field k_a (see ([2])). The arithmetic of such sums was studied by Stickelberger. For us Dwork' s interpretation ([5]) is especially convenient. Put

$$\begin{aligned} \chi_1(t) &= \tilde{t}^{-1}, \quad & \chi_j(t) &= \tilde{t}^{-j}, \quad & 1 &\le j \le p^a - 2; \\ \psi_1(t) &= \theta_a(\tilde{t}), \quad & \psi_i(t) &= \psi_1(it), \quad & 1 &\le i \le p - 1. \end{aligned}$$

Here $\tilde{t}$ is the multiplicative representative in the ring Ω of the element t of the field k_a, which is regarded as embedded in the residue field of the ring Ω; θ_a is the character defined by Dwork ([5]). Obviously,

$$\nu(\tau(\chi_j, \psi_i)) = \nu(\tau(\chi_j, \psi_1)).$$

This latter number, according to Stickelberger' s congruence, is equal to

$$\frac{\sigma(j)}{p-1},$$

where $\sigma(j)$ is the sum of the digits in the p-adic expansion of the number j:

$$j = \sum_{i=0}^{a-1} j_i p^i, \quad 0 \le j_i \le p - 1; \qquad \sigma(j) = \sum_{i=0}^{a-1} j_i.$$

Thus, among the collection of numbers

$$\frac{\nu(\tau(\chi_j, \psi_i))}{a}$$

there occurs every rational number between zero and one whose denominator divides $a(p-1)$. By Theorem 1, this means that the local decomposition of the Abelian variety J_a contains every simple group $G_{n,m}$ for which $(n+m) \mid a(p-1)$.

(Of course, one could compute the coefficients r_i of the decomposition $(J_a)_*$ "in explicit form,"expressing them in terms of number-theoretic functions connected with counting the number of partitions.) The theorem is proved.

5. It is unknown whether all groups

$$G_{n,m} + G_{m,n}$$

are fully representable. A positive answer to this question would lead to a complete description of fully representable commutative formal groups. The author has directly computed, with the aid of Theorem 1, two examples pertaining to the prime field of characteristic 3.

Example 1. X is the Jacobian variety of the curve

$$y^2 = x^7 - x + 1$$

over the field with three elements. Here

$$P(T) = T^6 + 3T^5 + 6T^4 + 12T^3 + 18T^2 + 27T + 27.$$

By Theorem 1,

$$X_* \sim G_{1,2} + G_{2,1}.$$

Example 2. X is the Jacobian variety of the curve $y^2 = x^9 + x^7 + x + 1$ over the field of three elements. Here

$$P(T) = T^8 + 3T^7 + 6T^6 + 12T^5 + 21T^4 + 36T^3 + 54T^2 + 81T + 81.$$

Therefore $X_* \sim G_{1,3} + G_{3,1}$.

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

Received
19 II 1962

References

[1] P. Cartier, C. R., **244**, 1109 (1957).
[2] H. Davenport, H. Hasse, J. f. reine u. angew. Math., **172**, 151 (1935).
[3] J. Dieudonné, Am. J. Math., **79**, 331 (1957).
[4] J. Dieudonné, Am. J. Math., **80**, 740 (1958).
[5] B. Dwork, Am. J. Math., **82**, 631 (1960).
[6] P. Gabriel, Séminaire Serre, 1960.
[7] J. P. Serre, Am. J. Math., **80**, 715 (1958).
[8] Yu. I. Manin, DAN, **143**, No. 1 (1962).
[9] Yu. I. Manin, Izv. AN SSSR, Ser. Math., **26**, No. 2 (1962).