Vol. 46, No. 4 DUKE MATHEMATICAL JOURNAL © December 1979

KUMMER THEORY ON EXTENSIONS OF ABELIAN VARIETIES BY TORI

KENNETH A. RIBET

This paper deals with "Kummer theory" on certain commutative, connected algebraic groups V. More precisely, let V be such a group, given over a field k of characteristic 0 as an extension

$$1 \to T \to V \to A \to 0,$$

where T is a torus and A an abelian variety. (We understand the group law on V to be written additively, although we think of the torus T as a multiplicative group.) For $n \geqslant 1$, multiplication by n on V is surjective, and the kernel V_n of this multiplication is finite. Let $\bar{k}$ be an algebraic closure for k, and let $G = \mathrm{Gal}(\bar{k}/k)$. We view V_n as a submodule of the G-module $V(\bar{k})$.

Now let $P_1, \ldots, P_t \in V(k)$ be a finite family of rational points on V. Extracting the nth roots of the P_i leads to a Kummer-theoretic situation as follows: if $k(V_n)$ is the extension of k obtained by adjoining to k the points of V_n, then the Galois group Δ_n of the extension

$$k\left(V_n; \frac{1}{n}P_1, \ldots, \frac{1}{n}P_t\right)/k(V_n)$$

may be viewed as a subgroup of the product

$$V_n^t = V_n \times \cdots \times V_n \qquad (t \text{ times}).$$

A general problem is to show that Δ_n is "large" when the P_i are "independent." Typically, this means showing, under suitable hypotheses on the P_i, that Δ_l is equal to V_l^t for almost all primes l.

When V is the multiplicative group $\mathbf{G}_m$, Δ_n is described by classical Kummer theory. The case where V is either an abelian variety with complex multiplication, or else an elliptic curve, has been treated by a method first found by Bashmakov [2, 3, 10, 15], at least when k is a number field. In an appendix to [4], one studied the case where V is a product of $\mathbf{G}_m$ and an elliptic curve (and where $t = 1$), obtaining a "mix" between classical Kummer theory and that of Bashmakov. Recently, D. Bertrand studied the case where V is a product of a *power* of an elliptic curve and a *power* of the multiplicative group [6].

Bertrand's theorem, like those of Bashmakov and the author, follows rather directly from certain properties of the Galois modules V_n. The first purpose of

Received May 3, 1976. Revision received June 25, 1979.