J. Math. Soc. Japan
Vol. 20, Nos. 1-2, 1968

Isogeny classes of abelian varieties over finite fields

Dedicated to Professor Shôkichi Iyanaga on his 60th birthday

By Taira HONDA

(Received July 24, 1967)
(Revised Sept. 25, 1967)

In the present paper we shall give a complete classification of isogeny classes of abelian varieties over finite fields in terms of Frobenius endomorphism and indicate some of its applications.

Let p be a fixed prime number and Ω the algebraic closure of the prime field of characteristic p. Let k_a denote the finite field with p^a elements. We consider $k_a \subset \Omega$. By an algebraic number field we mean a subfield of the complex number field $\boldsymbol{C}$ which is of finite degree over the rational number field $\boldsymbol{Q}$. We identify an ideal of an algebraic number field K with its extensions to over-fields of K as usual. We denote by $\boldsymbol{Z}$ the ring of rational integers and by $\boldsymbol{Z}_l$ its l-adic completion for a prime number l.

We shall say that an algebraic integer π (resp. an integral ideal $\mathfrak{a}$ of an algebraic number field) is *of type* (A_0), if we have

$$\pi^{\sigma}\pi^{\sigma\rho}=p^{a} \qquad (\text{resp. } \mathfrak{a}^{\sigma}\mathfrak{a}^{\sigma\rho}=(p^{a}))$$

with a positive integer a for any conjugate π^{σ} of π (resp. $\mathfrak{a}^{\sigma}$ of $\mathfrak{a}$), where ρ denotes the complex conjugacy of $\boldsymbol{C}$. The integer a is called the *order* of π (resp. $\mathfrak{a}$). It is well-known that to every k_a-simple abelian variety A over k_a corresponds a conjugacy class of numbers of type (A_0) with order a by considering the Frobenius endomorphism of A. Thus we obtain a map

Φ_a: {k_a-isogeny classes of k_a-simple abelian varieties over k_a}
$\rightarrow$ {conjugacy classes of numbers of type (A_0) with order a}.

Our main result is as follows:

MAIN THEOREM. *The map Φ_a is bijective for every $a \geqq 1$.*

In §1 of this paper we shall study basic properties of numbers and ideals of type (A_0). It is shown that any ideal of type (A_0) can be represented as a principal ideal with a number of type (A_0) in a suitable extension field (Theorem 1). Our aim in §1 is to prove Theorem 2, which asserts that some power of an ideal of type (A_0) has a prime ideal decomposition attached to a suitable CM-type. This implies that some power of a number of type (A_0) is in fact a value of a suitable "Grössencharakter" of type (A_0). (For the definition of