ABELIAN VARIETIES WITH COMPLEX MULTIPLICATION AND MODULAR FUNCTIONS

Goro Shimura

PRINCETON UNIVERSITY PRESS
PRINCETON, NEW JERSEY

Published by Princeton University Press, 41 William Street,
Princeton, New Jersey 08540
In the United Kingdom: Princeton University Press,
Chichester, West Sussex

Library of Congress Cataloging-in-Publication Data

Shimura, Gorō, 1930–
Abelian varieties with complex multiplication and modular functions / Goro Shimura.
p. cm. — (Princeton mathematical series ; 46)
Includes bibliographical references and index.
ISBN 0-691-01656-9 (alk. paper)
1. Abelian varieties. 2. Modular functions. I. Title.
II. Series.
QA564.S458 1997
514.3—dc21 97-8673 CIP

Parts of the present work appeared in an original version in *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*, ©1961 by The Mathematical Society of Japan

This book has been composed in Times Roman

Princeton University Press books are printed on acid-free paper and meet the guidelines for permanence and durability of the Committee on Production Guidelines for Book Longevity of the Council on Library Resources

http://pup.princeton.edu

Printed in the United States of America

1 3 5 7 9 10 8 6 4 2

Contents

	Preface	vii
	Preface to *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory* (1961)	ix
	Notation and Terminology	xiii
CHAPTER I.	Preliminaries on Abelian Varieties	3
1.	Homomorphisms and divisors	3
2.	Differential forms	7
3.	Analytic theory of abelian varieties	19
4.	Fields of moduli and Kummer varieties	25
CHAPTER II.	Abelian Varieties with Complex Multiplication	35
5.	Structure of endomorphism algebras	35
6.	Construction of abelian varieties with complex multiplication	40
7.	Transformations and multiplications	47
8.	The reflex of a CM-type	58
CHAPTER III.	Reduction of Constant Fields	68
9.	Reduction of varieties and cycles	68
10.	Reduction of rational mappings and differential forms	74
11.	Reduction of abelian varieties	83
12.	The theory "for almost all $\mathfrak{p}$"	87
13.	The prime ideal decomposition of an $N(\mathfrak{p})$-th power homomorphism	96
CHAPTER IV.	Construction of Class Fields	101
14.	Polarized abelian varieties of type $(K; \{\varphi_i\})$	101
15.	The unramified class field obtained from the field of moduli	109
16.	The class fields generated by ideal-section points	114
17.	The field of moduli in a generalized setting	118
18.	The main theorem of complex multiplication in the adelic language	121

CHAPTER V. The Zeta Function of an Abelian Variety with Complex Multiplication 132
19. The zeta function relative to a field over which some endomorphisms are defined 132
20. The zeta function over smaller fields 137
21. Models over the field of moduli and models with given Hecke characters 145
22. The case of elliptic curves 149

CHAPTER VI. Families of Abelian Varieties and Modular Functions 151
23. Symplectic and unitary groups 151
24. Families of polarized abelian varieties 156
25. Modular forms and functions 165
26. Canonical models 169

CHAPTER VII. Theta Functions and Periods on Abelian Varieties 173
27. Theta functions 173
28. Proof of Theorem 27.7 and Proposition 27.9 181
29. Theta functions with complex multiplication 188
30. The periods of differential forms on abelian varieties 190
31. Periods in the Hilbert modular case 193
32. Periods on abelian varieties with complex multiplication and their algebraic relations 196
33. Proof of Theorem 32.4 201

Bibliography 209

Supplementary References 213

Index 215

Preface

It was in 1961 that the book *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory*, coauthored by Yutaka Taniyama and myself, appeared as No. 6 of Publications of the Mathematical Society of Japan. In its preface, which the reader will find after this one, I presented a short history of the subject, as well as a brief account of the contents of the book. In view of the progress made after its publication, it is natural to write a sequel to it. The present volume is my attempt, if modest, at the realization of this project. To make it self-contained, I included the essential contents of the first sixteen sections of the 1961 book. In that sense, this may naturally be viewed as an expanded edition, though its raison d'être is mainly in the newly written seventeen sections, and the last two sections of the old book are not included.

When I started to work on this sequel, I was well aware that it would have been more desirable to write a completely reorganized book incorporating both old and new material. Having found the task difficult, I chose a compromise plan as described above. However, I made considerable revisions throughout the old part, stating a few theorems in stronger forms and inserting explanatory sentences at many points.

The principal feature of the new part is as follows. We first reformulate the main theorem of complex multiplication in the adelic language, and next, in Chapter V, we show that the zeta function of an abelian variety A with complex multiplication over a number field k can be given as a product of certain Hecke L-functions. Such was already given in the previous book, but we now try to present more precise results. We first treat the case in which "imaginary endomorphisms" are rational over k, and next the case in which only "real endomorphisms" are rational over k. Eventually we determine the zeta function of A over any number field of definition under a certain condition which is satisfied if A is simple. We then investigate the problem of finding a model of A over a given field and a given Hecke character.

In Chapter VI we first consider families of abelian varieties parametrized by the points on certain hermitian symmetric spaces, and then relate them to modular forms and functions on such spaces. The classical theory of complex multiplication asserts that the values of elliptic modular functions at a point on the upper half-plane belonging to an imaginary quadratic field K generate abelian extensions of K. This is essentially a reformulation of our theorem specialized to the one-dimensional case, though naturally it requires some non-

trivial facts on such modular functions. Now the higher-dimensional version of this fact can be formulated in terms of Hilbert or Siegel modular functions. We present here a formulation in a more general setting so that those functions become special cases.

In the historical part of the preface of the 1961 book, I referred to a "successful" work of Hecke on complex multiplication in two variables, but that was an overstatement, because the work was seriously flawed, though he stated basically correct assertions, which could have been proved if everything had been worked out. I also stated that this work of Hecke was included as a special case of the results in the book, but that was another overstatement, since we treated there only abelian functions instead of modular functions. However, the theorems in Section 26 of the present volume include what he expected as one of the easiest cases.

In Chapter VII we first recall the classical theory of theta functions in the sense of Jacobi-Riemann, and study the model of an arbitrary polarized abelian variety $\mathcal{P}$ that is the image of the projective embedding given by theta functions. Our interest is in the field of rationality of the model, which turns out to be an explicitly given finite algebraic extension k of the field of moduli of $\mathcal{P}$. We shall then determine the periods of the holomorphic 1-forms on $\mathcal{P}$ rational over k in terms of the values of certain modular forms.

In the case of complex multiplication, these periods lead to a collection of certain invariants which we call "the period symbol." The final two sections concern various algebraic relations among the periods on several abelian varieties which are not necessarily isogenous. We shall express the relations as certain linear properties of the period symbol. In a sense, this part may be viewed as the culmination of what has been developed in some of the preceding sections.

All these results in the new part were published in my papers listed in the Supplementary References at the end of the book. I have tried, however, to present better formulations than in those papers. I wish to acknowledge my gratitude to Alice Silverberg and Hiroyuki Yoshida, who kindly read the first draft of the entire new part and contributed numerous suggestions, which have been incorporated in the final version.

The 1961 book was published under the names of two authors. Though I believe that was the right thing to do, in fact, I was solely responsible for the whole text of the volume, as I indicated at the end of its preface. The reader who is interested in knowing about the life of Taniyama and the circumstances under which I wrote the book will find relevant pieces of information in my article "Yutaka Taniyama and His Time," published in the *Bulletin of the London Mathematical Society*, 21 (1989), pp. 186–196. It is my hope that the reader will long remember that to a large extent the main results up to §16 of the present volume have their source in our collaborative work until 1956.

Princeton, February 1996 G. S.

Preface to *Complex Multiplication of Abelian Varieties and Its Applications to Number Theory* (1961)

The history of complex multiplication began with the works of Gauss and Abel on elliptic functions. It would be right, however, to call Kronecker the initiator of number-theoretic investigation of the subject. The main theorem of Kronecker's theory asserts that the abelian extensions of every imaginary quadratic field are generated by the special values of certain elliptic or elliptic modular functions; as Kronecker left the work unfinished, the accomplishment needed the efforts of the late authors, Weber and Takagi. A similar and simpler result, which is also due to Kronecker, holds for the field of rational numbers: the abelian extensions of the field of rational numbers are generated by the roots of unity, the special values of the exponential functions. Hilbert conceived an idea to generalize these results, namely, to construct abelian extensions over any given algebraic number field by means of special values of analytic functions; he took this up as the 12th problem in his Paris Vortrag and emphasized its importance in number theory; it should be also mentioned that Kronecker had already thought of the problem. The first essential progress in this direction was made by Hecke, by following the idea of Hilbert. He succeeded in constructing unramified abelian extensions of certain biquadratic fields by means of singular values of Hilbert modular functions of two variables. This was the last work, as well as the first, till recent years, which attacked the problem successfully. On the other hand, a new development took place in the theory of complex multiplication of elliptic functions. First H. Hasse perceived the connection between complex multiplication and the Riemann hypothesis for congruence zeta functions, which was later proved by A. Weil in a fully general form. This observation led M. Deuring to establish a purely algebraic treatment of complex multiplication of elliptic curves. He could, moreover, along the same line of ideas, determine the zeta functions of elliptic curves with complex multiplication. The definition of zeta function of an algebraic curve defined over an algebraic number field is originally due to Hasse; and Weil is the first contributor to this subject.

Now the advancement in algebraic geometry of late years, especially in the abstract theory of abelian varieties, due to Weil, enabled us to approach the problem in a fairly general form, as was shown in three papers, published in

the Proceedings of the International Symposium on algebraic number theory, Tokyo-Nikko, 1955, of Weil and the authors of the present monograph. It is the purpose of the monograph to provide a full exposition of the results announced in these memoirs.

Our chief object is the arithmetic of an abelian variety A of dimension n, whose endomorphism-ring is isomorphic to an order in an algebraic number field K of degree $2n$ over the field of rational numbers. The first task is to show that the field of moduli of A, whose definition must and can be given by virtue of the notion of polarization, and the fields generated by the coordinates of the points on A of finite order, are class fields over a certain algebraic number field K^*, corresponding to the ideal-groups determined by the arithmetical structure of A (Main Theorems 1, 2, 3 in Chapter IV). The number field K cannot be taken arbitrarily; it must be a totally imaginary quadratic extension of a totally real number field. K^* is the algebraic number field determined by K and the representation of K in the linear space of invariant differential forms on A. If $n = 1$, we have $K = K^*$, while if $n > 1$, both the cases $K = K^*$ and $K \neq K^*$ may occur. The abelian extensions of K^* thus obtained from A do not provide all the abelian extensions of K^* unless $n = 1$; at any rate, the classical results of Kronecker and Hecke are included in our main theorems as particular cases. It is noteworthy that the prime ideal decomposition of the $N(\mathfrak{p})$-th power endomorphism $\pi_{\mathfrak{p}}$ of $A(\mathfrak{p})$ is fundamental in our whole theory, where $A(\mathfrak{p})$ denotes the reduction of the variety A modulo a prime ideal $\mathfrak{p}$ of a field of definition k for A. The above result is in close connection with the investigation of the zeta function of the abelian variety A. In fact, a more precise analysis of $\pi_{\mathfrak{p}}$ shows that the correspondence $\mathfrak{p} \to \pi_{\mathfrak{p}}$ determines a Grössen-character of the field k. We are then led to the expression of the zeta function of A by the product of several Hecke L-series attached to Grössen-characters (Main Theorem 4 of Chapter IV); this is a generalization of the results of Weil and Deuring mentioned above.

We now give a summary of the contents. Chapter I is an exposition of more or less known results on abelian varieties, which are mostly given without proofs. The only exception is Section 2, where we have given a detailed (but elementary) treatment of invariant differential forms on abelian varieties. Section 3 deals with the analytic representation of abelian varieties, their homomorphisms and divisors by means of complex tori. In Section 4, first the notion of polarized varieties is introduced and then the definitions of field of moduli and Kummer variety are given. Chapter II is devoted to the algebraic part of the theory of complex multiplication. Sections 5 and 6 contain a necessary and sufficient condition that an algebraic number field K of degree $2n$ be realized as the endomorphism-algebra of an abelian variety of dimension n. Section 7 is the study of mutually isogenous abelian varieties in connection with the ideals of the endomorphism-rings; Section 8 concerns the phenomena which are essential

only in the case of dimension $n > 1$ and related to the definition of the number field K^*. Chapter III contains the theory of reduction of algebraic varieties modulo a prime divisor of the basic field. We shall prove in Section 13 the fundamental theorem concerning the prime ideal-decomposition of $N(\mathfrak{p})$-th power homomorphism. Our final aims are achieved in Chapter IV. The first step (Section 14) is the investigation of the relations between abelian varieties, of the same type of complex multiplication, whose polarizations are also of the "same type." Then, in Section 15, we prove the first main theorem; an unramified class field is obtained by the field of moduli. A similar argument together with the analysis of the points of finite order gives us also class fields, whose characterization is the object of Section 16. These results are obtained assuming the endomorphism-ring to be the principal order of the number field. In Section 17, the case of nonprincipal order is completely investigated. The last section is devoted to the determination of the zeta-function of an abelian variety of the type described above.

A large part of the contents was prepared in collaboration of both authors during 1955–56 and published in 1957 in Japanese as the first six chapters of the book with the title "Kindai-teki Seisu-ron" (Modern number theory). The English version was then planned; but owing to the sudden death of the second named author in the autumn of 1958, the work had to be completed by the person left behind. The present volume is not a mere translation, however; we have written afresh from beginning to end, revising at many points, and adding new results such as Section 17 and several proofs of propositions which were previously omitted.

The present monograph owes much to the idea of Weil [54], though we have not necessarily indicated explicit references in the text. I take this opportunity to acknowledge my cordial gratitude to Professor André Weil for his constant advice, suggestions, and encouragement. I wish to acknowledge also my thanks to Mr. Taira Honda who read the manuscipt and contributed many useful suggestions.

University of Tokyo
February 1960 *Goro Shimura*

This page intentionally left blank

Notation and Terminology

We denote by $\mathbf{Z}$, $\mathbf{Q}$, $\mathbf{R}$, and $\mathbf{C}$ the ring of rational integers, the fields of rational numbers, real numbers, and complex numbers, respectively, and by $\overline{\mathbf{Q}}$ the algebraic closure of $\mathbf{Q}$ in $\mathbf{C}$. If ℓ is a rational prime, $\mathbf{Z}_\ell$ and $\mathbf{Q}_\ell$ denote the ring of ℓ-adic integers and the field of ℓ-adic numbers, respectively.

Given an associative ring R with identity element and an R-module S, we denote by $R^\times$ the group of all invertible elements of R, and by S_n^m the module of all $m \times n$-matrices with entries in S. We shall often put $S^m = S_1^m$. Thus $\mathbf{C}^n$ (resp. $\mathbf{R}^n$) is the vector space of n-dimensional complex (resp. real) column vectors. If V is a vector space over $\mathbf{C}$ of dimension n, a *lattice of* V means a discrete subgroup of V isomorhic to $\mathbf{Z}^{2n}$.

We denote the identity element of the ring R_n^n by 1_n, or simply by 1, and the transpose of a matrix X by ${}^tX$. We put $GL_n(R) = (R_n^n)^\times$, and

$$SL_n(R) = \{\, \alpha \in GL_n(R) \mid \det(\alpha) = 1 \,\}$$

if R is commutative. For a complex number or more generally for a complex matrix α we denote by $\mathrm{Re}(\alpha)$, $\mathrm{Im}(\alpha)$, and $\overline{\alpha}$ the real part, the imaginary part, and the complex conjugate of α. If $\alpha_1, \ldots, \alpha_r$ are square matrices, $\mathrm{diag}[\alpha_1, \ldots, \alpha_r]$ denotes the matrix with $\alpha_1, \ldots, \alpha_r$ in the diagonal blocks and 0 in all other blocks.

Terminology and basic notation concerning algebraic geometry are essentially the same as in Weil's trilogy [44], [45], and [46]. In particular, a variety or a subvariety always means an absolutely irreducible one. If V is a variety, we view V as the set of all its points rational over the universal domain. For a finite algebraic extension k' of a field k we denote by $[k' : k]_i$ and $[k' : k]_s$ the inseparable and separable factors of the degree of k' over k. If σ is an isomorphism of a field k_1 onto a field k_2, then for $z \in k_1$ we denote by z^σ the image of z under σ with the rule $z^{\sigma\tau} = (z^\sigma)^\tau$ for another isomorphism τ of k_2 onto a field. Furthermore, if Y is an algebro-geometric object defined with respect to k_1, we denote by Y^σ the image of Y under σ. If Y is defined by some polynomial equations, then Y^σ is defined by the transforms of the equations under σ. If k is a field and x is a point of an affine (resp. a projective) space, we denote by $k(x)$ the field generated over k by the coordinates (resp. the quotients of the coordinates) of the point x. We use also the notation $k(x)$ for the points on an abstract variety (cf. [44]).

Method of citation. There are two lists of references: Bibliography and Supplementary References. The former is the same as in the 1961 book and its articles are numbered from 1 through 57. Each item in the latter list contains a roman capital with or without more letters and numerals. Therefore the reader should be able to determine in which list the article in question appears.

Abelian Varieties with Complex Multiplication and Modular Functions

CHAPTER I

Preliminaries on Abelian Varieties

1. Homomorphisms and Divisors

The purpose of this section is to recall briefly some of the basic concepts on abelian varieties defined over arbitrary ground fields. For the general theory of abelian varieties, we refer the reader to Weil [46] and Lang [26].

1.1. By a *group variety* we understand an algebraic variety (affine, projective, or abstract) G with a group structure such that the map $(x, y) \mapsto xy$ of $G \times G$ into G and also the map $x \mapsto x^{-1}$ of G into G are both rational mappings defined everywhere. Such a G must be nonsingular. We say that a group variety G is defined over a field k if the variety G and these maps are defined over k.

A group variety is called an *abelian variety* if it is complete in the sense of [44], which is the case if it is a projective variety. In fact, every (abstract) abelian variety defined over k is biregularly isomorphic to a projective variety over k, and therefore we practically lose nothing by assuming it to be projective. It is a well-known fact that the group law of an abelian variety is commutative. Therefore we use the additive notation and denote the zero element by 0. Whenever we speak of *an abelian variety A defined over a field k*, we always assume that A as a group variety is defined over k in the above sense. If a subvariety of an abelian variety A is a subgroup, then it has a natural structure of abelian variety, and is called an *abelian subvariety* of A. An abelian variety is called *simple* if it has no abelian subvarieties other than $\{0\}$ and itself. (Some authors call it *absolutely simple*.)

Let A and B be two abelian varieties. By a *homomorphism* of A into B, or an *endomorphism* when $A = B$, we shall always understand a rational mapping λ of A into B satisfying $\lambda(x + y) = \lambda(x) + \lambda(y)$ generically. If that is so, then λ is defined everywhere and $\lambda(x + y) = \lambda(x) + \lambda(y)$ for every $x, y \in A$. We denote by $\mathrm{Ker}(\lambda)$ the kernel of λ. We shall often write λx for $\lambda(x)$. If such a λ is birational, then it must be biregular, and we call it an *isomorphism*, or an *automorphism* when $A = B$. We denote by $\mathrm{Hom}(A, B)$ the set of all homomorphisms of A into B, defined over any extension of a given field of definition for A and B, and put $\mathrm{End}(A) = \mathrm{Hom}(A, A)$. It is a basic fact

that $\mathrm{Hom}(A, B)$ is a free $\mathbf{Z}$-module of finite rank; moreover if A and B are defined over k, then every element of $\mathrm{Hom}(A, B)$ is defined over a separably algebraic extension of k. We put also $\mathrm{Hom}_{\mathbf{Q}}(A, B) = \mathrm{Hom}(A, B) \otimes_{\mathbf{Z}} \mathbf{Q}$ and $\mathrm{End}_{\mathbf{Q}}(A) = \mathrm{End}(A) \otimes_{\mathbf{Z}} \mathbf{Q}$. Clearly $\mathrm{End}_{\mathbf{Q}}(A)$ has a structure of an algebra over $\mathbf{Q}$, and $\mathrm{End}(A)$ is an order of the algebra. We denote the identity element of $\mathrm{End}_{\mathbf{Q}}(A)$ by 1_A. More generally, if $\lambda \in \mathrm{Hom}_{\mathbf{Q}}(A, B)$ and $\mu \in \mathrm{Hom}_{\mathbf{Q}}(B, C)$, then we can define the product $\mu\lambda$ naturally as an element of $\mathrm{Hom}_{\mathbf{Q}}(A, C)$.

For two abelian varieties A and B of the same dimension, there exists a homomorphism of A onto B if and only if there exists a homomorphism of B onto A, in which case A and B are called *isogenous*, and any such homomorphism is called an *isogeny*. Given $\lambda \in \mathrm{Hom}(A, B)$ with A and B of the same dimension, take a field of definition k for A, B, and λ and take also a generic point x of A over k. If λ is an isogeny, we put

$$\nu(\lambda) = [k(x) : k(\lambda x)],$$

$$\nu_s(\lambda) = [k(x) : k(\lambda x)]_s, \qquad \nu_i(\lambda) = [k(x) : k(\lambda x)]_i,$$

and otherwise we put $\nu(\lambda) = \nu_s(\lambda) = \nu_i(\lambda) = 0$. These numbers do not depend on the choice of k and x. If λ is an isogeny, then $\nu_s(\lambda)$ is the order of $\mathrm{Ker}(\lambda)$. For every isogeny λ of A onto B there is a unique element λ' of $\mathrm{Hom}_{\mathbf{Q}}(B, A)$ such that $\lambda'\lambda = 1_A$ and $\lambda\lambda' = 1_B$. We write then $\lambda' = \lambda^{-1}$.

1.2. The ℓ-adic representation of homomorphisms. For an abelian variety A and a rational prime ℓ we put

$$\mathfrak{g}_\ell(A) = \bigcup_{\alpha=1}^{\infty} \mathrm{Ker}(\ell^\alpha 1_A).$$

If A is of dimension n and ℓ is different from the characteristic of a field of definition for A, then $\mathfrak{g}_\ell(A)$ is isomorphic to the direct sum $\mathfrak{M}$ of $2n$ copies of the additive group $\mathbf{Q}_\ell/\mathbf{Z}_\ell$. We call any one of the isomorphisms of $\mathfrak{g}_\ell(A)$ onto $\mathfrak{M}$ an *ℓ-adic coordinate-system of* $\mathfrak{g}_\ell(A)$. We consider every element of $\mathfrak{M}$ a column vector of dimension $2n$ with components in $\mathbf{Q}_\ell/\mathbf{Z}_\ell$. Let B be another abelian variety of dimension m and λ a homomorphism of A into B. Choose ℓ-adic coordinate systems $\mathfrak{v}$ of $\mathfrak{g}_\ell(A)$ and $\mathfrak{w}$ of $\mathfrak{g}_\ell(B)$. Then there exists an element M of $(\mathbf{Z}_\ell)_{2n}^{2m}$ such that $\mathfrak{w}(\lambda t) = M\mathfrak{v}(t)$ for every $t \in \mathfrak{g}_\ell(A)$. If we fix $\mathfrak{v}$ and $\mathfrak{w}$, the correspondence $\lambda \mapsto M$ can be uniquely extended to a $\mathbf{Q}$-linear map of $\mathrm{Hom}_{\mathbf{Q}}(A, B)$ into $(\mathbf{Q}_\ell)_{2n}^{2m}$, which we call the ℓ-adic representation of $\mathrm{Hom}_{\mathbf{Q}}(A, B)$ with respect to $\mathfrak{v}$ and $\mathfrak{w}$. In particular, if $A = B$ and $\mathfrak{v} = \mathfrak{w}$, this is a ring-homomorphism of $\mathrm{End}_{\mathbf{Q}}(A)$ into $(\mathbf{Q}_\ell)_{2n}^{2n}$.

Now let M_ℓ denote an ℓ-adic representation of $\mathrm{End}_{\mathbf{Q}}(A)$ with respect to a fixed $\mathfrak{v}$ as above. Given $\xi \in \mathrm{End}_{\mathbf{Q}}(A)$, let

$$P(x) = X^{2n} + a_1 X^{2n-1} + \cdots + a_{2n}$$

be the characteristic polynomial of $M_\ell(\xi)$. Then the following facts are known: *the a_i are rational numbers, and*

$$P(\xi) = \xi^{2n} + a_1\xi^{2n-1} + \cdots + a_{2n} = 0;$$

moreover, the polynomial P is determined by ξ independently of the choice of ℓ and ℓ-adic coordinate-system; furthermore, if $\xi \in \mathrm{End}(A)$, then $a_i \in \mathbf{Z}$ and

$$\nu(\xi) = \det\big(M_\ell(\xi)\big). \tag{1}$$

We call *P the characteristic polynomial* of ξ and the roots of *P the characteristic roots of* ξ; we also put

$$\mathrm{tr}(\xi) = \mathrm{tr}\big(M_\ell(\xi)\big). \tag{2}$$

1.3. The Picard variety of an abelian variety. Given an abelian variety A, let $\mathcal{G}_a(A)$ and $\mathcal{G}_l(A)$ denote, respectively, the set of divisors on A algebraically equivalent to 0 and the set of divisors on A linearly equivalent to 0. Then there exists an abelian variety A^* canonically isomorphic to $\mathcal{G}_a(A)/\mathcal{G}_l(A)$, which is called the *Picard variety* of A. Every divisor Y contained in $\mathcal{G}_a(A)$ defines a point of A^*, which we denote by $\mathrm{Cl}(Y)$. Let B be an abelian variety and B^* the Picard variety of B. For every homomorphism λ of A into B, we obtain a homomorphism λ^* of B^* into A^* such that

$$\lambda^*(\mathrm{Cl}(Y)) = \mathrm{Cl}(\lambda^{-1}(Y)) \tag{3}$$

whenever $\lambda^{-1}(Y)$ is defined. The mapping $\lambda \to \lambda^*$ is uniquely extended to an isomorphism of $\mathrm{Hom}_{\mathbf{Q}}(A, B)$ onto $\mathrm{Hom}_{\mathbf{Q}}(B^*, A^*)$; we denote by ${}^t\alpha$ the image of α by this isomorphism and call it the *transpose* of α. If $\alpha \in \mathrm{Hom}_{\mathbf{Q}}(A, B)$ and $\beta \in \mathrm{Hom}_{\mathbf{Q}}(B, C)$, we have ${}^t(\beta\alpha) = {}^t\alpha\,{}^t\beta$. Let X be a divisor on A; we shall denote by X_u the transform of X by the translation $x \to x + u$ on A. Now define the mapping φ_X of A into A^* by the relation

$$\varphi_X(u) = \mathrm{Cl}(X_u - X) \tag{4}$$

for $u \in A$. Then φ_X is a homomorphism of A into A^*. The divisor X is said to be *non-degenerate* if φ_X is an isogeny. For any two divisors X, Y on A, we have $\varphi_X = \varphi_Y$ if and only if X and Y are algebraically equivalent (Barsotti [3], Serre [31]). Assuming X to be non-degenerate, put for every $\xi \in \mathrm{End}_{\mathbf{Q}}(A)$,

$$\xi' = \varphi_X^{-1}\,{}^t\xi\,\varphi_X. \tag{5}$$

Then, it can be proved that $\xi \to \xi'$ is an involution of $\mathrm{End}_{\mathbf{Q}}(A)$ and if a suitable multiple of X is ample, we have, for every $\xi \neq 0$,

$$\mathrm{tr}(\xi\xi') > 0. \tag{6}$$

We call this involution *the involution of* $\mathrm{End}_{\mathbf{Q}}(A)$ *determined by* X. Let λ be a homomorphism of A into B and Y a divisor on B; assume that $\lambda^{-1}(Y)$ is defined. Then, putting $X = \lambda^{-1}(Y)$, we have

$$\varphi_X = {}^t\lambda\varphi_Y\lambda. \tag{7}$$

1.4. l-adic representations of divisors. Let a be an integer and Y a divisor on A such that aY is linearly equivalent to 0. Then there exist two functions Φ and Ψ on A such that $(\Phi) = aY$, $\Phi(ax) = \Psi(x)^a$, where (Φ) denotes the divisor of Φ. For every point u on A such that $au = 0$, put

$$e_a(u, Y) = \Psi(x + u)\Psi(x)^{-1};$$

then $e_a(u, Y)$ is an a-th root of unity. Now let X be a divisor on A, and let u, v be two points on A such that $au = av = 0$. Since $a(X_v - X)$ is linearly equivalent to 0, we can consider $e_a(u, X_v - X)$. Put

$$e_{X,a}(u, v) = e_a(u, X_v - X).$$

Let k be a field of definition for A; and let l be a rational prime other than the characteristic of k. Let U_l denote the set of roots of unity, contained in the algebraic closure of k, whose orders are powers of l; then U_l is isomorphic to $\mathbf{Q}_l/\mathbf{Z}_l$. Take an isomorphism of U_l onto $\mathbf{Q}_l/\mathbf{Z}_l$ and denote it by lg; choose an l-adic coordinate-system $\mathfrak{v}$ of $\mathfrak{g}_l(A)$. Then there exists a matrix $E_l(X)$ with coefficients in $\mathbf{Z}_l$ satisfying

$$\lg e_{X,l^\nu}(s, t) \equiv l^\nu \cdot {}^t\mathfrak{v}(s)E_l(X)\mathfrak{v}(t) \qquad \mod \mathbf{Z}_l$$

for every point s, t on A such that $l^\nu s = l^\nu t = 0$. We call $E_l(X)$ the *l-adic representation* of X with respect to $\mathfrak{v}$. We have $E_l(X) = 0$ if and only if X is algebraically equivalent to 0.

1.5. q-th power homomorphisms. Let A be an abelian variety defined over a field k and σ an isomorphism of k onto a field k^σ. Then we obtain in a natural way an abelian variety A^σ, defined over k^σ, taking the transform 0^σ of the origin 0 of A as the origin of A^σ. If B is an abelian variety and λ is a homomorphism of A into B, both defined over k, we denote by λ^σ the homomorphism of A^σ into B^σ, whose graph is the transform by σ of the graph of λ. Now suppose that the characteristic p of the universal domain is not 0; let $q = p^f$ $(f > 0)$ be a power of p. We shall denote by X^q the transform of any algebro-geometric object X by the automorphism $z \to z^q$ of the universal domain. We can define a homomorphism π of A onto A^q by

$$\pi x = x^q$$

for $x \in A$. We call π the *q-th power homomorphism* of A. If A is defined over a finite field with q elements, A^q coincides with A, and hence π is an endomorphism of A; we call then π the *q-th power endomorphism* of A. All the characteristic roots of the q-th power endomorphism have absolute value $q^{1/2}$; this is the so-called "Riemann hypothesis for congruence zeta-functions" proved by A. Weil. Let λ be a homomorphism of A into B; let π_A and π_B denote respectively the q-th power homomorphisms of A and B. We have then

$$\lambda^q \pi_A = \pi_B \lambda.$$

In particular, if A is defined over a finite field k with q elements, we have

$$\alpha \pi_A = \pi_A \alpha$$

for every endomorphism α of A, defined over k.

2. *Differential Forms*

2.1. Definitions. In this section, the varieties are all assumed to be defined over fields contained in a universal domain Ω which we fix once for all. Let V be a variety and k a field of definition for V. We shall denote by $k(V)$ the field of rational functions on V defined over k and by $\Omega(V)$ the field of all rational functions on V. If x is a generic point of V over k, the mapping $k(V) \ni f \to f(x)$ gives an isomorphism of $k(V)$ onto $k(x)$. We denote by $\mathcal{D}(V)$ and $\mathcal{D}(V; k)$ respectively the set of all derivations of $\Omega(V)$ over Ω and the set of all derivations of $k(V)$ over k. If V is of dimension n, $\mathcal{D}(V; k)$ is a vector space of dimension n over $k(V)$ and $\mathcal{D}(V)$ is a vector space obtained from $\mathcal{D}(V; k)$ by the scalar extension $\Omega(V)$ over $k(V)$. We shall denote by $\mathfrak{D}(V)$ the dual space of $\mathcal{D}(V)$ and by $\eta \cdot D$ the scalar product of $\eta \in \mathfrak{D}(V)$ and $D \in \mathcal{D}(V)$; then $(\eta, D) \to \eta \cdot D$ is a bilinear mapping of $\mathfrak{D}(V) \times \mathcal{D}(V)$ into $\Omega(V)$. Now, by a *differential form* of degree m on V, we shall understand a homogeneous element of degree m in the Grassmann algebra defined over $\mathfrak{D}(V)$. If f is a function on V, the mapping $\mathcal{D}(V) \ni D \to Df$ gives a linear mapping of $\mathcal{D}(V)$ into $\Omega(V)$, and hence defines an element of $\mathfrak{D}(V)$, a differential form of degree one on V; we denote it by df; then we have $df \cdot D = Df$. We see that $\mathfrak{D}(V)$ is generated over $\Omega(V)$ by the forms df for $f \in \Omega(V)$. If V is of dimension n, then there exists a set of n functions $\{g_1, \ldots, g_n\}$ in $k(V)$ such that $k(V)$ is separably algebraic over $k(g_1, \ldots, g_n)$. If $\{g_1, \ldots, g_n\}$ is such a set, $dg_1, \ldots, dg_n$ form a basis of $\mathfrak{D}(V)$ over $\Omega(V)$. By our definition, every differential form ω on V has an expression

$$\omega = \sum_{(i)} f_{(i)} dg_{i_1} \cdots dg_{i_r},$$

where the $f_{(i)}$ are elements of $\Omega(V)$. We shall say that a differential form ω on V is *defined over* k if ω can be written in the form

$$\omega = \sum_{(i)} \varphi_{(i)} d\psi_{i_1} \cdots d\psi_{i_r},$$

with the $\varphi_{(i)}$ and the ψ_i in $k(V)$. The set $\{g_1, \ldots, g_n\}$ being as above, a differential form

$$\sum_{i_1 < \cdots < i_r} f_{(i_1 \cdots i_r)} dg_{i_1} \cdots dg_{i_r}$$

is defined over k if and only if the $f_{(i)}$ are contained in $k(V)$.

Let V' be a simple subvariety of V. We shall say that a differential form ω on V is *finite along* (or *at*) V' if ω can be written in the form $\omega = \sum_{(i)} f_{(i)} dg_{i_1} \cdots dg_{i_r}$ where the $f_{(i)}$ and the g_i are functions on V which are all defined and finite along V'. If that is so, denoting by the $f'_{(i)}$ and the g'_i the functions on V' induced by the $f_{(i)}$ and the g_i, we obtain a differential form $\omega' = \sum_{(i)} f'_{(i)} dg'_{i_1} \cdots dg'_{i_r}$ on V' which is determined only by ω and V'; ω' does not depend upon the choice of the $f_{(i)}$ and the g_i. We call ω' the differential form on V' induced by ω.

2.2. Local parameters. Let K be a field and $u_1, \ldots, u_n$ be n independent variables over K. If K_1 is a separably algebraic extension of $K(u_1, \ldots, u_n)$, there exist n derivations $D_1, \ldots, D_n$ of K_1 over K such that

$$D_i u_i = 1, \quad D_i u_j = 0 \quad \text{for } i \neq j.$$

The D_i are uniquely determined by these relations; we shall denote D_i by $\partial/\partial u_i$ for each i.

Now let V be a variety of dimension n, defined over k, and y a simple point on V. We call a set of n functions $\{\tau_1, \ldots, \tau_n\}$ in $k(V)$ a *system of local parameters* for V at y defined over k, if the following conditions are satisfied.

(L1) *$k(V)$ is separably algebraic over $k(\tau_1, \ldots, \tau_n)$.*
(L2) *The τ_i are all defined and finite at y.*
(L3) *For every f in $k(V)$, defined and finite at y, the function $\partial f/\partial \tau_i$ is defined and finite at y for every i.*

Let x be a generic point of V over k; let V_α, y_α, x_α be affine representatives of V, y, x and S the ambient space for V_α; let N be the dimension of S. Then, by Koizumi [23], we know that n functions $\tau_1, \ldots, \tau_n$ in $k(V)$ form a system of local parameters for V at y, defined over k, if and only if the following conditions are satisfied.

(L'1) *The τ_1 are all defined and finite at y.*
(L'2) *There exists a set of N polynomials $F_i(X_1, \ldots, X_N, T_1, \ldots, T_n)$ with coefficients in k such that $F_i(x_\alpha, \tau(x)) = 0$ for $1 \leq i \leq N$ and $\det(\partial F_i/\partial X_j(y_\alpha, \tau(y))) \neq 0$.*