PERSPECTIVES
IN MATHEMATICS

J. COATES, S. HELGASON, EDITORS

Ehud de Shalit

Iwasawa Theory of Elliptic Curves with Complex Multiplication

Iwasawa Theory of Elliptic Curves with Complex Multiplication

p-adic *L* Functions

Ehud de Shalit
Mathematical Sciences Research Institute
Berkeley, California

ACADEMIC PRESS, INC.
Harcourt Brace Jovanovich, Publishers

Boston Orlando San Diego
New York Austin London Sydney
Tokyo Toronto

ACADEMIC PRESS, INC.
Orlando, Florida 32887

United Kingdom Edition published by
ACADEMIC PRESS, INC. (LONDON) LTD.
24-28 Oval Road, London, NW1 7DX

Library of Congress Cataloging-in-Publication Data
De Shalit, Ehud.
Iwasawa theory of elliptic curves with complex multiplication.

(Perspectives in mathematics; vol. 3)
Bibliography: p.
1. L-functions. 2. Curves, Elliptic. 3. Class field theory. I. Title. II. Series.
QA247.D36 1987 512'.74 87-1435
ISBN 0-12-210255-X (alk. paper)

87 88 89 90 9 8 7 6 5 4 3 2 1
Printed in the United States of America

Iwasawa Theory of Elliptic Curves with Complex Multiplication

PERSPECTIVES IN MATHEMATICS, Vol. 3

J. Coates and S. Helgason, editors

TO THE MEMORY OF MY FATHER

ACKNOWLEDGEMENTS

This book, based in part on the author's Ph.D. thesis, summarizes the work of many people, and benefited from diverse sources. I tried to give appropriate credits and references in the text, but there are undoubtedly omissions of which I remain unaware.

Like everybody else in the field, I was heavily influenced by the beautiful ideas of J. Coates and A. Wiles, and by the analogy with Iwasawa's work on cyclotomic fields. In addition, Iwasawa's approach to local class field theory, and the work of R. Coleman, formed the basis of chapter I. Chapter II grew out of, and is a natural continuation to the work of R. Yager. Part of it was planned as a joint paper with him, but due to geographical difficulties, this plan never materialized. To all these people I would like to express my deepest gratitude.

Special thanks go to K. Iwasawa for guiding me in my first steps, to Andrew Wiles for his encouragement and friendship, and to Robert Coleman who read parts of the manuscript and made valuable comments.

I would like to thank all the other teachers and friends from whom I learned the subject, in particular E. Friedman, R. Greenberg, B. Gross, B. Mazur and K. Rubin.

I am also grateful to Harvard University, the Mathematical Sciences Research Institute, and the National Science Foundation for their support during the preparation of this book, and to Faye Yeager for the excellent typing.

Ehud de Shalit
Berkeley, December 8, 1986

Perspectives in Mathematics

Vol. 1	J.S. Milne, *Arithmetic Duality Theorems*
Vol. 2	A. Borel et al., *Algebraic D-Modules*
Vol. 3	Ehud de Shalit, *Iwasawa Theory of Elliptic Curves with Complex Multiplication*

TABLE OF CONTENTS

INTRODUCTION

p-adic L functions are analytical functions of p-adic characters that, one way or another, interpolate special values of classical (complex) L functions. The first such examples were the p-adic L functions of Kubota and Leopoldt [K-Le], interpolating Dirichlet L series. Manin and Vishik [M-V] and Katz [K1] constructed p-adic L functions which interpolate special values of Hecke L series associated with a quadratic imaginary field K, in which p splits. (To fix notation write $p = \mathfrak{p}\overline{\mathfrak{p}}$). Their work gave p-adic interpolation of the Hasse-Weil zeta function of certain elliptic curves with complex multiplication and good ordinary reduction at $\mathfrak{p}$ (those whose division points generate abelian extensions of K). The p-adic L function of Manin-Vishik and Katz is the first object studied in this work.

Our point of view is nevertheless different, and goes back to the two fundamental papers [C-W1] and [C-W2] by Coates and Wiles. The program, pursued by various authors since (see the introduction to chapter II), and which is brought here to its fullest generality (so we hope), may be summarized in two main steps.

Fix an abelian extension F_1 of K, and let K_∞ be the unique $\mathbf{Z}_p$ extension of K unramified outside $\mathfrak{p}$ (one of the two factors of p in K). If we assume that F_1 is the ray class field modulo $\mathfrak{f}\mathfrak{p}$, where $\mathfrak{f}$ is an integral ideal relatively prime to $\mathfrak{p}$, we do not lose any generality, and some notation is simplified. We therefore make this assumption. The p-adic L function, then, is essentially a p-adic integral measure on $\mathcal{G} = Gal(F_1K_\infty/K)$.

Now in the first step we are given a norm-coherent sequence β of semi-local units in the completion of the tower $F_\infty = F_1K_\infty$ at $\mathfrak{p}$. Out of each such sequence we construct a certain measure μ_β on $\mathcal{G}$. We describe this construction in chapter I. In the second step, carried out in chapter II, we introduce special global units, the elliptic units. They come in norm coherent sequences, so we can view them inside the local units. When the procedure from chapter I is applied to them we obtain the p-adic L function.

Chapters I and II are carried out in full generality and are also attempted to be self contained. This results in long tedious computations. The reader who approaches the subject for the first time is advised to make two simplifying assumptions: that K is of class number 1, and that the grossencharacters in question are unramified at $\mathfrak{p}$. These eliminate most of the technical difficulties, yet very little is lost conceptually. If still confused, one may restrict attention to grossencharacters of infinity type $(k, 0)$. This will only give the interpolation formula for the "one variable" p-adic L function. We have actually treated this case separately in II.4, despite some repetition, to facilitate the reading.

Other results obtained in chapters I and II include a new proof of Wiles' explicit reciprocity law, a p-adic analogue of Kronecker's limit formula, and a functional equation for the p-adic L function.

The immense interest in Katz' p-adic L functions arises from their significance to class field theory (abelian extensions of K) and the arithmetic of elliptic curves with complex multiplication. In the last two chapters we give a sample of results in these two directions. Although largely self-contained, these chapters are not intended to be exhaustive, and several topics are omitted. The selection of material, and sometimes the method of proof, were influenced by our desire to show how the results of chapter II are put to use.

Chapter III is mainly concerned with the "main conjecture" in the style of cyclotomic Iwasawa theory. The fundamental idea is that the zeroes of the p-adic L function ought to be those p-adic characters of $\mathcal{G}$ whose reciprocals appear in the representation of $\mathcal{G}$ on a certain free $\mathbf{Z}_p$-module of finite rank. More precisely, this module $\mathcal{X}$ is the Galois group of the maximal abelian p-extension of F_∞ which is unramified outside $\mathfrak{p}$. See the introduction to chapter III for more details. We prove that the Iwasawa invariants of $\mathcal{X}$ and the Iwasawa invariants of the p-adic L function are equal, but we do not go into the recent evidence for this conjecture discovered by K. Rubin, nor do we give Gillard's proof of the vanishing of the μ-invariant.

While elliptic curves are deliberately kept behind the scene in chapter III, their arithmetic, and in particular the conjecture of Birch and Swinnerton-Dyer, is the main topic of chapter IV. First we show how Kummer theory and descent are used to relate the Galois group previously denoted by $\mathcal{X}$ to the Selmer group over F_∞. Then we give a complete proof of two beautiful theorems of Coates-Wiles and of R. Greenberg. These theorems are generalized here to treat elliptic curves with CM by an arbitrary quadratic imaginary field, not necessarily of class number 1. The crucial hypothesis that must be kept is that the division points of the curve in question generate an abelian extension of K.

Of the topics not considered here, let us mention p-adic heights and p-adic sigma functions, the work of Perrin-Riou on the algebraic analogue of the conjecture of Birch and Swinnerton-Dyer [PR1], and her "Gross-Zagier-type" result [PR2]. As this book goes to press, K. Rubin has announced important new results concerning the conjecture of Birch and Swinnerton-Dyer. He kindly allowed me to report on them here, and we refer the reader to his forthcoming papers for details.

The author is well aware of the lack of numerical examples in chapters III and IV. These would illustrate the theory magnificently, but due to lack of skill in computing, I was unable to produce any new examples. There is much relevant numerical data in the paper of Bernardi, Goldstein and Stephens [B-G-S].

CHAPTER I

FORMAL GROUPS, LOCAL UNITS, AND MEASURES

Much of the first half of this book is devoted to the construction of p-adic L functions associated with quadratic imaginary fields. This construction is "formal" and "local" in the beginning. Only at a later stage results from the theory of complex multiplication are incorporated. In chapter I we gather those results which *do not* deal with elliptic curves. Our tools are formal groups and p-adic measures. The key result is theorem 3.7, which describes the structure of a certain module of local units. This module plays a central role in the following three chapters. In section 4 we prove a version of the explicit reciprocity law in local class field theory, that will be needed in chapter IV.

1. Relative Lubin-Tate Groups

1.1 Let R be a commutative ring with identity. For our purpose a (commutative) *one dimensional formal group law* over R is a power series $F \in R[[X,Y]]$, satisfying the following axioms.

(i) $F(X,Y) \equiv X + Y \; mod \; deg \; 2$

(ii) $F(X,0) = X = F(0,X)$

(iii) $F(X,F(Y,Z)) = F(F(X,Y),Z)$ (associativity)

(iv) $F(X,Y) = F(Y,X)$ (commutativity).

We use the notation $f \equiv g \; mod \; deg \; n$ to mean that $f - g$ involves only monomials of total degree not less than n. It can be shown ([Haz] 1.1.4) that there exists a unique power series $\iota(X) \in R[[X]]$ such that $F(X,\iota(X)) = 0$.

Let A be an R-algebra and $\mathfrak{a}$ an ideal such that A is complete and separated in its $\mathfrak{a}$-adic topology (i.e. $A = \varprojlim A/\mathfrak{a}^n$). Then if $f,g \in \mathfrak{a}$, $F(f,g)$ and

$\iota(f)$ converge to elements of $\mathfrak{a}$. We denote them by $f[+]g$ and $[-]f$ respectively, and observe that with $[+]$ as addition $\mathfrak{a}$ becomes an abelian group, written $F(\mathfrak{a})$ ("the $\mathfrak{a}$-valued points of F"), to distinguish from the ordinary addition on $\mathfrak{a}$. These remarks apply in particular to $A = R[[X]]$ and $\mathfrak{a} = (X)$, and to the case where $A = R$ is a complete local ring and $\mathfrak{a}$ is its maximal ideal. Almost everything we shall need about formal groups can be found in the book of Hazewinkel [Haz]. Henceforth we let "formal group" stand for "commutative one-dimensional formal group law", unless otherwise specified.

A *homomorphism* f between two formal groups F and F' over R is a power series without constant term such that $F'(f(X), f(Y)) = f(F(X,Y))$. The collection $Hom(F,F')$ of such homomorphisms forms a group with respect to the addition law of F' : $(f+g)(X) = f(X)[+]'g(X)$, and $End\,(F)$ becomes a *ring* under *composition* as product.

Let R be a domain of characteristic 0, and $f \in Hom(F,F')$. Then $f(X) = aX$ + (higher terms) and the map $f \mapsto a = f'(0)$ is an *injective* group homomorphism of $Hom(F,F')$ into R ([Haz] 20.1). When $F = F'$ this is a ring homomorphism. We shall write $[a]_{F,F'}$ or $[a]_F$, or simply $[a]$ instead of f in such a case. Over the field of fractions K of R all formal groups are isomorphic. Any isomorphism $\lambda : F \simeq \hat{\mathbf{G}}_a$ over K ($\hat{\mathbf{G}}_a(X,Y) = X + Y$ is the *additive formal group*) is called a *logarithm* of F. If λ is normalized so that $\lambda'(0) = 1$, then $\lambda'(X) \in R[[X]]^x$ has coefficients in R ([Haz] 5.8). All these statements are blatantly false (or void) in non-zero characteristic.

Let F be a formal group over a field of characteristic $p > 0$. Then $[p]_F(X) = X[+]\ldots[+]X$ (p times) is a power series in X^q with $q = p^h$ for some $h \geq 1$. The largest possible h is called the *height* of F ([Haz] 18.3). If $[p]_F = 0$ F is of infinite height.

Finally, we shall need the concept of a *translation-invariant derivation* on F. This is a continuous derivation D of $R[[X]]$ (over R) satisfying $D(f(X[+]Y)) = Df(X[+]Y)$, where Y is treated here as a constant for D (i.e. D is extended to

$R[[X,Y]]$ via $DY = 0$). If R is a domain of characteristic 0, then $D = \dfrac{c}{\lambda'(X)} \dfrac{d}{dX}$ where $c \in R$ and λ is the logarithm of F, normalized to $\lambda'(0) = 1$.

The *multiplicative formal group* $\hat{\mathbf{G}}_m$ is given by $\hat{\mathbf{G}}_m(X,Y) = X + Y + XY = (1 + X)(1 + Y) - 1$.

1.2 Let k be a finite extension of $\mathbf{Q}_p$, the field of p-adic numbers. Let $\mathcal{O}$ and $\wp$ be its valuation ring and maximal ideal. Let the residue field $\mathcal{O}/\wp$ have q elements. Lubin and Tate introduced an extremely useful class of formal groups defined over $\mathcal{O}$ [L-T]. Their handiness stems from the fact that they each possess a special endomorphism which "lifts" the Frobenius substitution $X \mapsto X^q$ in characteristic p. Here we generalize a little (see [dS1]), and as usual in this theory, focus first on the lifting of Frobenius, and web the formal group around it.

Let d be a positive integer and k' the unique unramified extension of k of degree d. Let k^{ur} be the maximal unramified extension of k, and K its completion. The Frobenius automorphism (relative to k) φ generates $Gal(k^{ur}/k)$ topologically, and extends by continuity to K. It is characterized by $\varphi(x) \equiv x^q \; mod \; \wp^{ur}$ for all $x \in \mathcal{O}^{ur}$. We let $\mathcal{O}', \wp', \varphi'$ denote the corresponding objects for k', so that $\varphi' = \varphi^d$. Finally let $\nu : K^x \to \mathbf{Z}$ be the normalized valuation (normalized in the sense that $\nu(K^x) = \mathbf{Z}$).

Fix $\xi \in k^x$, $\nu(\xi) = d$, and consider

$$\mathcal{F}_\xi = \{f \in \mathcal{O}'[[X]] \mid f \equiv \pi' X \; mod \; deg \; 2, \; N_{k'/k}(\pi') = \xi \text{ and } f \equiv X^q \; mod \; \wp'\}.$$

Any f in $\mathcal{F}_\xi$ is going to play the role of an endomorphism lifting Frobenius. Its differential is $f'(0) = \pi'$, and its reduction is X^q.

1.3 Theorem. *For every $f \in \mathcal{F}_\xi$ there exists a unique one-dimensional commutative formal group law F_f defined over $\mathcal{O}'$ satisfying $F_f^\varphi \circ f = f \circ F_f$.*

In other words, $f \in Hom(F_f, F_f^\varphi)$. Here, and elsewhere, the superscript φ means that we apply φ to the coefficients of the power series. Note that $F_f^\varphi \in \mathcal{F}_\xi$ too, and $F_f^\varphi = F_{\varphi(f)}$ (apply φ to the equation defining F_f). When $d = 1$ we are in the situation studied by Lubin and Tate. When $d \geq 1$ we call F_f a *relative Lubin Tate* group (relative to the extension k'/k). For the proof we need a lemma.

1.4 Lemma. *Let $f, g \in \mathcal{F}_\xi$ and let $F_1(X_1, \ldots, X_n)$ be a linear form in $\mathcal{O}'[X_1, \ldots, X_n]$. Suppose $f \circ F_1 \equiv F_1^\varphi \circ (g, \ldots, g)$ mod deg 2. Then there exists a unique $F \in \mathcal{O}'[[X_1, \ldots, X_n]]$ satisfying (i) $F \equiv F_1$ mod deg 2, (ii) $f \circ F = F^\varphi \circ (g, \ldots, g)$.*

PROOF: (Compare [Se] p. 149). Let $f = \pi_1 X + \ldots, g = \pi_2 X + \ldots$. Set $F^{(1)} = F_1$ and define successive approximations $F^{(m)}$ satisfying (ii) *mod deg* $m+1$ through $(m \geq 2)$ $F^{(m)} = F^{(m-1)} + F_m$ where F_m is homogeneous of degree m. For this we need

$$f \circ \left(F^{(m-1)} + F_m\right) \equiv \left(F^{(m-1)} + F_m\right)^\varphi \circ g \textit{ mod deg } m + 1$$

or

$$f \circ F^{(m-1)} + \pi_1 F_m \equiv F^{(m-1)\varphi} \circ g + \pi_2^m F_m^\varphi.$$

Let t be the homogeneous part of degree m of $F^{(m-1)\varphi} \circ g - f \circ F^{(m-1)}$. Since $F^{(m-1)\varphi} \circ g \equiv F^{(m-1)\varphi}(X_1^q, \ldots, X_n^q) \equiv (F^{(m-1)})^q \equiv f \circ F^{(m-1)}$ *mod* $\wp'$, $t \equiv 0$ *mod* $\wp'$. We have to find F_m satisfying

$$F_m - \pi_1^{-1} \pi_2^m F_m^\varphi = \pi_1^{-1} t.$$

This is possible because $m \geq 2$ and $\mathcal{O}'$ is complete (proceed by induction *mod* $\wp'^r$). Setting $F = \sum_{m=1}^\infty F_m$ concludes the proof.

PROOF OF THEOREM 1.3: In the lemma, let $f = g$ and $F_1 = X_1 + X_2$. We have to show that F_f = the resulting F, is a formal group law. This is done by repeated application of lemma 1.4 and is left as an exercise (or look it up in [Se] p. 150).

Let $\tilde{F}$ be the reduction of F_f, i.e. the formal group over $\mathcal{O}'/\wp'$ obtained by "reading F_f modulo $\wp'$". It is easily verified that $\tilde{F}$ is of height $[k : \mathbf{Q}_p]$. By abuse of language we refer to it as the *height* of F_f too.