Cambridge University Press
978-0-521-72866-9 — Elliptic Curves and Big Galois Representations
Daniel Delbourgo
Excerpt
More Information

Introduction

The connection between L-functions and arithmetic must surely be one of the most profound in mathematics. From Dirichlet's discovery that infinitely many primes occur in an arithmetic progression, right through to Wiles' celebrated proof of Fermat's Last Theorem, the applications of L-series to number theory seem to be limitless.

This book is concerned with the special values of L-functions of modular forms. The twentieth century saw many deep conjectures made about the interrelation between L-values and associated arithmetic invariants. Moreover, the last few years have seen a lot of these predictions proved correct, though much is still shrouded in mystery. Very frequently modular forms can be grouped together into families parametrised by a single analytic variable, and it is their properties which we intend to study here. Whilst we shall be primarily interested in the arithmetic of the whole family itself, the control theory often tells us something valuable about each individual member.

What then do we mean by a modular form? Let k and N be positive integers. An analytic function $f_k : \mathfrak{H} \cup \{\infty\} \longrightarrow \mathbb{C}$ is *modular of weight* k *and level* N if

$$f_k\left(\frac{az+b}{cNz+d}\right) \quad = \quad (cNz+d)^k \, f_k(z)$$

at all integers $a, b, c, d \in \mathbb{Z}$ such that $1 + bcN = ad$. In particular, the quadruple $(a, b, c, d) = (1, 1, 0, 1)$ clearly satisfies this condition, so we must have the identity $f_k(z+1) = f_k(z)$ for all $z \in \mathfrak{H}$. Moreover, if $f_k(z)$ is appropriately bounded as z approaches the cusps, we call f_k a modular form.

It follows that f_k is a periodic function of z, with a Fourier expansion

$$f_k(z) \quad = \quad \sum_{n=0}^{\infty} a_n(f_k) q^n \quad \text{where } q = \exp(2\pi i z).$$

Hecke proved that for a fixed level N and weight k, the space of modular forms is finitely-generated over $\mathbb{C}$. He introduced a system of operators 'the Hecke algebra', under whose action a basis of eigenforms can always be found.

N.B. It is very far from being true that every modular form occurring in nature hides deep secrets. For example, the Eisenstein series

$$\mathrm{Eis}_k(z) \quad := \quad \sum_{(0,0)\neq(m,n)\in\mathbb{Z}\times\mathbb{Z}} \frac{1}{(mz+n)^k} \quad \text{for integers } k > 2$$

whilst indispensable tools in the analytic theory, tell us precious little about the arithmetic of Diophantine equations.

We'll concern ourselves exclusively with the study of *newforms* of weight $k \geq 2$, a precise definition of which can be found in the next chapter. For the moment, we just mention that a newform f_k vanishes at the cusp ∞, so the constant term $a_0(f_k)$ in its Fourier expansion must be zero. The complex L-function

$$L(f_k, s) \quad := \quad \sum_{n=1}^{\infty} a_n(f_k).n^{-s}$$

converges in the right-half plane $\mathrm{Re}(s) > \frac{k}{2} + 1$, and can be analytically continued to the whole of the complex numbers. In contrast to the rather crude nature of Eisenstein series, newforms encode a lot of useful arithmetic data.

Let us fix an integer $s_0 \in \{1, ..., k-1\}$, and assume that $L(f_k, s_0)$ is non-zero. The conjectures of Bloch and Kato relate the value of the L-function at $s = s_0$ with the order of a mysterious group $\text{Ш}_k = \text{Ш}(f_k; s_0)$, which can be defined cohomologically. For their conjecture to make any sense, it is essential that the quantity $\#\text{Ш}_k$ be finite. In the special case where the weight $k = 2$, the object Ш_2 is the Tate-Shafarevich group of a modular elliptic curve which has f_2 as its associated newform; the Bloch-Kato Conjecture then reduces to the famous conjectures of Birch and Swinnerton-Dyer (see Chapter I for details).

Beilinson, and then subsequently Kato, discovered that the critical values of the L-function are governed by certain cohomology classes, which we now refer to as *Kato-Beilinson zeta-elements*.

Our first main result is purely technical, but nonetheless vital:

Theorem 0.1. *The space of zeta-elements generates the algebraic modular symbol associated to the cuspidal eigenform f_k.*

Let's see what the implications of this theorem are in deformation theory.

So far the weight k of our newforms has remained fixed, but we can relax this. We shall allow k to vary over the whole of the p-adic integers $\mathbb{Z}_p$, although only at positive integers can one say anything meaningful about the behaviour of newforms. Let $p > 3$ denote a prime number, and write Λ for the power series ring $\mathbb{Z}_p[\![X]\!]$. Hida showed that whenever the p^{th}-Fourier coefficient is a p-adic unit, these modular forms come in ordinary families

$$\mathbf{f} \quad = \quad \sum_{n=1}^{\infty} a_n(\mathbf{f}; X)\, q^n \quad \in \quad \Lambda[\![q]\!]$$

where at infinitely many weights $k \geq 2$, the expansion

$$\mathbf{f}_k \quad = \quad \sum_{n=1}^{\infty} a_n\Big(\mathbf{f}; (1+p)^{k-2} - 1\Big)\, q^n \quad \in \quad \mathbb{Z}_p[\![q]\!]$$

is a classical eigenform of weight k.

CAMBRIDGE

Cambridge University Press
978-0-521-72866-9 — Elliptic Curves and Big Galois Representations
Daniel Delbourgo
Excerpt
More Information

This means we are no longer dealing with just a single Bloch-Kato Conjecture, rather a continuum of statements relating the quantities

$$\text{the special value } L(\mathbf{f}_k, s_0) \quad \xleftrightarrow{\text{Bloch-Kato}} \quad \text{the } p\text{-part of } \#\mathbf{Ш}_k.$$

We consider only the p-primary part of $\mathbf{Ш}_k$ above, because the choice of prime p is fundamental to the original deformation.

Not surprisingly, this raises a whole host of arithmetic questions:

Q1. *Is there a p-adic analytic L-function of k interpolating these special values?*

Q2. *What is the underlying object governing these Tate-Shafarevich groups $\mathbf{Ш}_k$?*

Q3. *Can the Bloch-Kato Conjecture be formulated for the whole p-ordinary family, so that each individual conjecture is simply a manifestation at weight k?*

We shall look for answers to all these questions.

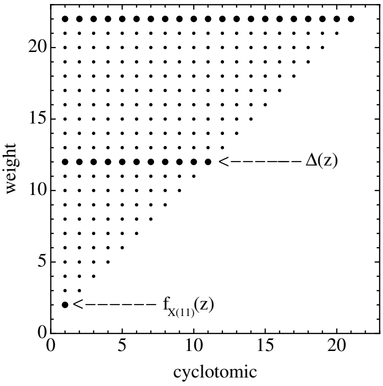
As a first step, we find an analytic parametrisation for the Galois cohomology of the representations interpolating $\{\mathbf{f}_k\}_{k\geq 2}$. Let $\mathbf{F}$ denote an abelian extension of $\mathbb{Q}$.

Theorem 0.2. *The étale Coleman exact sequence over $\mathbf{F}\otimes\mathbb{Z}_p$ deforms along the universal p-ordinary representation $\rho_\infty^{\mathrm{univ}} : G_{\mathbb{Q}} \to \mathrm{GL}_2\big(\mathbb{Z}_p[\![X]\!]\big)$.*

The proof is based on the following generalisation of Theorem 0.1:

Theorem 0.3. *The weight-deformation of the zeta-elements over $\mathbb{Z}_p[\![X]\!]$, generates the universal Λ-adic modular symbol associated to the family $\mathbf{f}$.*

Of course, there is no reason at all why the point $s = s_0$ should have remain fixed. If we allow it to vary in exactly the same manner as the weight k varied, one can consider special values at all points of the critical strip, simultaneously.



The critical region at $p = 11$ and tame level one

In terms of the deformation theory, this amounts to adding a second variable to the power series ring Λ, which means we are now working over $\mathbb{Z}_p[\![X,Y]\!]$ instead. The whole picture becomes clearer when we allow this extra cyclotomic variable Y because the full force of Iwasawa theory is at our disposal.

Our intention is to study Selmer groups associated to the following three lines: the vertical line $s=1$, the central line $s=k/2$, and the boundary line $s=k-1$. Let's consider $s=1$ and $s=k-1$ first.

Theorem 0.4. *The Selmer groups along both $s=1$ and $s=k-1$ are Λ-cotorsion, over all abelian extensions $\mathbf{F}$ of the rational numbers $\mathbb{Q}$.*

It is worthwhile remarking that the cotorsion of the cyclotomic Selmer group along the horizontal line $k=2$ was recently proven by Kato, and in the CM case Rubin. This remains one of the crown jewels in the Iwasawa theory of elliptic curves.

Unfortunately for the central line $s=k/2$, things are less clear cut.

Conjecture 0.5. *The Selmer group along $s=k/2$ should have Λ-corank equal to the generic order of vanishing of $L_p(\mathbf{f}_k, k/2)$ for even integers k.*

Greenberg predicted that the order of vanishing along $s=k/2$ was either almost always zero, or almost always one. Without knowing whether this statement holds true in general, alas 0.5 is destined to remain only a conjecture at best.

Granted we know something about the structure of these three Selmer groups, one can then compute the leading terms of their characteristic power series.

Theorem 0.6. *There are explicit formulae relating the Iwasawa invariants along $s=1$, $s=k/2$ and $s=k-1$ to the p-part of the BSD Conjecture.*

The author apologises profusely for stating the result in such a vacuous manner – for the full statements, we refer the reader to Theorems 9.18 and 10.1 in the text. To obtain these formulae is by no means trivial. If the function $L(\mathbf{f}_2, s)$ vanishes at the point $s=1$ it is necessary to define analogues over Λ of the elliptic regulator, which in turn involves constructing 'p-adic weight pairings' on an elliptic curve.

When combined, the results 0.1–0.6 allow us to deduce the arithmetic behaviour of the two-variable Selmer group over $\mathbb{Z}_p[\![X,Y]\!]$, at the critical point $(1,2)$:

Theorem 0.7. *The leading term of the algebraic two-variable p-adic L-function at $(s,k)=(1,2)$ is equal to the order of Ш_2, multiplied by some readily computable Λ-adic Tamagawa numbers.*

In particular, this last theorem shows how the p-primary part of Ш is completely controlled by the arithmetic of the Hida family that lifts the classical eigenform $\mathbf{f}_2$ (c.f. Section 10.3 for the precise formulae).

The organisation of this book is as follows. The first chapter is meant to be purely introductory, containing a very brief review of elliptic curves and modular forms. In Chapter II we recall the work of Perrin-Riou and Kato on the theory of Euler systems for modular forms. Then in Chapter III we describe a brand new method for constructing p-adic L-functions using these tools. The main advantage of our constructions is that each Euler system is assigned a modular symbol, and there is a particularly nice deformation theory for these symbols.

Once we have a working model in place for the cyclotomic variable Y, it is then time to introduce the weight variable X. In Chapter IV we provide a short description of Hida's ordinary deformation theory, which exerts strict control over the modular forms occurring in the family. The two chapters that follow contain the technical heart of the book. We develop a theory of two-variable Euler systems over $\mathbb{Z}_p[\![X,Y]\!]$, in terms of the Λ-deformation of the space of modular symbols. Since there are already ambiguities present in certain of the objects considered, we will give a construction compatible with the analytic theory of Greenberg-Stevens and Kitagawa.

The remainder of the book is completely devoted to a study of the arithmetic of p-ordinary families. In Chapter VII we explain how to associate Selmer groups over a one-variable deformation ring $\Lambda = \mathbb{Z}_p[\![X]\!]$, and hence compute their Λ-coranks. In the next two chapters we prove formulae for the p-part of the Tate-Shafarevich group of an elliptic curve (under the assumption that the number field is abelian). Finally, Chapter X ties everything together in what is rather grandly called the "Two-Variable Main Conjecture". This statement is now over the larger power series ring $\mathbb{Z}_p[\![X,Y]\!]$, and our previous Euler characteristic computations allow us to formulate the conjecture without error terms.

The reader who has done a graduate-level course in algebraic number theory, should have no trouble at all in understanding most of the material. A passing acquaintance with algebraic geometry could also be helpful. However, someone with a number theory background could easily skip the first couple of chapters, and the battle-hardened Iwasawa theorist could probably dive straight into Chapter IV.

Acknowledgements: Firstly, the author is greatly indebted to Adrian Iovita for explaining his generalisation of $B_{\max}$, and to Denis Benois for sharing his knowledge of the dual exponential map. He also thanks Paul Smith for writing Appendix C, and for both his and John Cremona's computer experiments.

For their moral support, he is particularly grateful to John Coates, David Burns, and his work colleagues at the University of Nottingham. He thanks D.P.M.M.S. for their very kind hospitality during a sabbatical leave period at the end of 2006. Lastly, many thanks to Nigel Hitchin and the team at Cambridge University Press, for their assistance and technical knowhow.

Cambridge University Press
978-0-521-72866-9 — Elliptic Curves and Big Galois Representations
Daniel Delbourgo
Excerpt
More Information

List of Notations

(a) For a field K we write $\overline{K}$ for its separable algebraic closure. At each prime number p, let μ_{p^n} denote the group of p^n-th roots of unity living inside of $\overline{K}$. If M is a $\mathbb{Z}_p[\mathrm{Gal}(\overline{K}/K)]$-module and the integer $j \geq 0$, then '$M(j)$' denotes the Tate twist $M \otimes_{\mathbb{Z}_p} \big(\varprojlim_n \mu_{p^n}\big)^{\otimes j}$. On the other hand, if $j < 0$ then it denotes the twist $M \otimes_{\mathbb{Z}_p} \mathrm{Hom}_{\mathbb{Z}_p}\big(\varprojlim_n \mu_{p^n}^{\otimes -j}, \mathbb{Z}_p\big)$.

(b) Throughout we shall fix embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ at each prime p. We write $\mathbb{C}_p$ for the completion of $\overline{\mathbb{Q}}_p$ with respect to the p-adic metric (it is an algebraically closed field). Thus we may consider all Dirichlet characters $\psi : (\mathbb{Z}/M\mathbb{Z})^\times \to \overline{\mathbb{Q}}^\times$ as taking values in both $\mathbb{C}^\times$ and $\mathbb{C}_p^\times$ under our embeddings.

(c) The maximal unramified extension $\mathbb{Q}_p^{\mathrm{nr}}$ of the p-adic numbers, has Galois group $\mathrm{Gal}\big(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p\big) \cong \mathrm{Gal}\big(\overline{\mathbb{F}}_p/\mathbb{F}_p\big)$. The arithmetic Frobenius element $\mathrm{Frob}_p : x \mapsto x^p$ in the latter group can be considered as generating $\mathrm{Gal}\big(\mathbb{Q}_p^{\mathrm{nr}}/\mathbb{Q}_p\big)$ topologically. Moreover, we abuse notation and write 'Frob_p' for any of its lifts to $\mathrm{Gal}\big(\overline{\mathbb{Q}}_p/\mathbb{Q}_p\big)$, which are only well-defined modulo the inertia group I_p.

(d) For a ring R we denote the i^{th}-étale cohomology group $H^i_{\text{ét}}\big(\mathrm{Spec}(R),\ -\big)$ by $H^i_{\text{ét}}(R,\ -)$, or sometimes just by $H^i(R,\ -)$. Assume further that R is an integral domain with field of fractions K, and write $j : \mathrm{Spec}(K) \to \mathrm{Spec}(R)$ for the inclusion morphism. Then for any sheaf $\mathcal{A}$ of abelian groups on $\mathrm{Spec}(K)$, we abbreviate $H^i\big(R, j_*(\mathcal{A})\big)$ simply by $H^i(R, \mathcal{A})$.

(e) Given an integer level $N \geq 1$, let $\Gamma_0(N)$ denote the group of unimodular matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ satisfying the congruence $c \equiv 0 \pmod{N}$. Similarly, the subgroup $\Gamma_1(N)$ consists of matrices satisfying $c \equiv 0 \pmod{N}$ and $a \equiv d \equiv 1 \pmod{N}$. If $\Phi = \Gamma_0(N)$ or $\Gamma_1(N)$, then $\mathcal{S}_k(\Phi)$ is the space of cusp forms of weight k on Φ. Finally, for each primitive Dirichlet character $\epsilon : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, we will write $\mathcal{S}_k\big(\Gamma_0(N), \epsilon\big)$ to indicate the ϵ-eigenspace

$$\left\{ f \in \mathcal{S}_k\big(\Gamma_1(N)\big) \text{ such that } f\Big|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \epsilon(d) f \text{ for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \right\}.$$

Cambridge University Press
978-0-521-72866-9 — Elliptic Curves and Big Galois Representations
Daniel Delbourgo
Excerpt
More Information

CHAPTER I

Background

Although the study of elliptic curves can be traced back to the ancient Greeks, even today there remain surprisingly many unanswered questions in the subject. The most famous are surely the conjectures of Birch and Swinnerton-Dyer made almost half a century ago. Their predictions have motivated a significant portion of current number theory research, however they seem as elusive as they are elegant. Indeed the Clay Institute included them as one of the seven millenium problems in mathematics, and there is a million dollar financial reward for their resolution.

This book is devoted to studying the Birch, Swinnerton-Dyer (BSD) conjecture over the universal deformation ring of an elliptic curve. A natural place to begin is with a short exposition of the basic theory of elliptic curves, certainly enough to carry us through the remaining chapters. Our main motivation here will be to state the BSD conjecture in the most succinct form possible (for later reference). This seems a necessary approach, since the arithmetic portion of this work entails searching for their magic formula amongst all the detritus of Galois cohomology, i.e. we had better recognise the formula when it finally does appear!

After defining precisely what is meant by an elliptic curve E, we introduce its Tate module $\mathrm{Ta}_p(E)$ which is an example of a two-dimensional Galois representation. The image of the Galois group inside the automorphisms of $\mathrm{Ta}_p(E)$ was computed by Serre in the late 1960's. We next explain how to reduce elliptic curves modulo prime ideals, which then enables us to define the L-function of the elliptic curve E. This L-function is a pivotal component in the BSD formula in §1.4.

One of the highlights of the subject is the Mordell-Weil theorem, which asserts that the group of rational points on an elliptic curve is in fact finitely-generated. We shall sketch the proof of this famous result, primarily because it involves the application of 'height pairings' which will be invaluable tools in later chapters. Lastly, the connection between elliptic curves and modular forms is covered in §1.5. These important objects are introduced from a purely algebraic standpoint, because this gives us greater flexibility when visualising Beilinson's K_2-elements.

The excellent volumes of Silverman [Si1,Si2] cover just about everything you would want to know about the fundamental theory of elliptic curves, and about two thirds of this chapter is no more than a selective summary of his first tome. For the complex analytic theory there is the book of Knapp [Kn], which covers the connection with modular forms in some detail. A gentler introduction is the volume of Silverman-Tate [ST], and of course Cassels' text [Ca1] is a classic.

1.1 Elliptic curves

We say that E is an elliptic curve if it is a smooth projective curve of genus one, equipped with a specified base-point O_E. Furthermore, E is said to be defined over a field K if the underlying curve is, and in addition the base-point O_E has K-rational coordinates. Since every elliptic curve may be embedded as a cubic in projective space, we can equally well picture it in *Weierstrass form*

$$E \;:\; Y^2Z + a_1XYZ + a_3YZ^2 \;=\; X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

where the a_1, a_2, a_3, a_4, a_6 all lie inside K. Under this identification, the origin O_E will be represented by the point at infinity $(X, Y, Z) = (0, 1, 0)$.

If the characteristic of K is neither 2 nor 3, one can always change coordinates to obtain (birationally) a simpler affine equation

$$E \;:\; y^2 \;=\; x^3 + Ax + B$$

where again A, B are elements of K. The non-singularity of our curve is then equivalent to the cubic $x^3 + Ax + B$ possessing three distinct roots, i.e. to the numerical condition

$$\Delta(E) \;=\; -16(4A^3 + 27B^2) \;\neq 0.$$

Remark: The above quantity is called *the discriminant of* E and depends on that particular choice of Weierstrass equation. On the other hand, the *j-invariant*

$$j(E) \;:=\; 1728 \times \frac{4A^3}{4A^3 + 27B^2}$$

is independent of this choice, and classifies elliptic curves up to isomorphism.

The principal reason why the theory of elliptic curves is so rewarding is because the points on an elliptic curve are endowed with the structure of an abelian group. If P_1 and P_2 are two such points on E, then their sum $P_3 \;= $ "$P_1 + P_2$" is the unique point satisfying

$$(P_3) - (O_E) \;\sim\; (P_1) + (P_2) - 2(O_E) \qquad \text{inside } \operatorname{Pic}^0(E),$$

the degree zero part of the divisor class group of E. In terms of the Weierstrass equation $y^2 = x^3 + Ax + B$, it can be shown that the x-coordinate of P_3 is

$$x\big(P_3\big) \;=\; x\big(P_1 + P_2\big) \;=\; \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - \;(x_1 + x_2)$$

when $P_1 = (x_1, y_1)$ differs from $P_2 = (x_2, y_2)$, and if they are the same point

$$x\big(P_3\big) \;=\; x\big(P_1 + P_1\big) \;=\; \frac{x_1^4 - 2Ax_1^2 - 8Bx_1 + A^2}{4x_1^3 + 4Ax_1 + 4B}.$$

Geometrically three points sum to zero if and only if they lie on the same line, so the additive inverse of $P_1 = (x_1, y_1)$ must be $-P_1 = (x_1, -y_1)$.

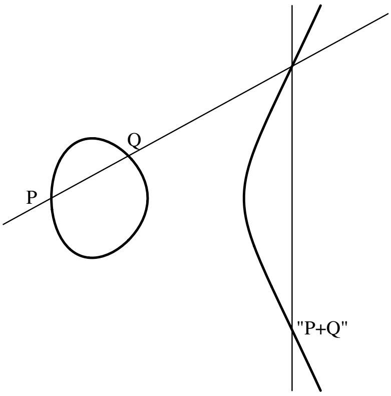


Figure 1.1

Adding the same point repeatedly to itself a fixed number of times gives rise to an endomorphism of E, defined over K. More precisely, for an integer $m \in \mathbb{Z}$ we denote by $[\times m] \in \mathrm{End}(E)$ the map for which

$$[\times m]P \quad = \quad \begin{cases} \quad P + \cdots + P & \text{if } m > 0 \\ \quad O_E & \text{if } m = 0 \\ -P - \cdots - P & \text{if } m < 0 \end{cases} \qquad\qquad \text{“ } \big|m\big|\text{-times ”}$$

at all points $P \in E$.

Actually there are not that many possibilities for the endomorphism ring of E. If the field K has characteristic zero then $\mathrm{End}(E)$ is either $\mathbb{Z}$, or an order in an imaginary quadratic field in which case we say that E has *complex multiplication.* Note that if K has positive characteristic then $\mathrm{End}(E)$ could also be a maximal order in a quaternion algebra.

Isogenies and the Tate module.
Suppose now that E' is another elliptic curve defined over K. An isogeny between E and E' is a non-constant morphism $\phi : E \to E'$ of curves such that $\phi(O_E) = O_{E'}$. In particular, ϕ is a group homomorphism whence $\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2)$. The kernel of ϕ will be a finite subgroup of E, and the degree of ϕ is its degree as a finite map of curves.

The dual isogeny $\widehat{\phi} : E' \to E$ is then characterized by the property that

$$\widehat{\phi} \circ \phi \;=\; [\times n]_E \quad \text{and} \quad \phi \circ \widehat{\phi} \;=\; [\times n]_{E'} \quad \text{where } n = \deg(\phi).$$

If $\lambda : E \to E'$ and $\theta : E' \to E$ are two further isogenies, their duals satisfy

$$\widehat{\widehat{\phi}} \;=\; \phi, \qquad \widehat{\phi + \lambda} \;=\; \widehat{\phi} + \widehat{\lambda} \qquad \text{and} \qquad \widehat{\phi \circ \theta} \;=\; \widehat{\theta} \circ \widehat{\phi}.$$

Cambridge University Press
978-0-521-72866-9 — Elliptic Curves and Big Galois Representations
Daniel Delbourgo
Excerpt
More Information

Definition 1.1. *The kernel of the isogeny $[\times m] : E \to E$ is denoted by*

$$E[m] \;\; := \;\; \mathrm{Ker}\big([\times m]\big) \;=\; \Big\{ P \in E \quad \textit{such that} \quad [\times m]P \;=\; O_E \Big\},$$

and consists of geometric points on E defined over a fixed algebraic closure $\overline{K}$. We also write E_{tors} for the union $\bigcup_{m \geq 1} E[m]$.

Remarks: (a) If the characteristic of K is zero or is coprime to $m \geq 1$, then

$$E[m] \;\cong\; \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z};$$

(b) If the characteristic of K equals $p > 0$, then

$$E[p^n] \;\cong\; \mathbb{Z}/p^n\mathbb{Z} \qquad \text{or} \qquad \{0\} \qquad \text{for all} \;\; n \geq 1;$$

if $E[p^n]$ is zero we call the elliptic curve *supersingular*, otherwise it is *ordinary*.

Let us fix a prime number p. The multiplication-by-p endomorphism induces a transition map $[\times p] : E[p^{n+1}] \longrightarrow E[p^n]$ of finite p-groups, for all integers $n \geq 1$. The projective limit is called the p-adic Tate module of E, and is written as

$$\mathrm{Ta}_p(E) \;\;=\;\; \varprojlim_n E[p^n].$$

Whenever the characteristic of K is coprime to p, we see from part (a) of the above remark that there is a naive decomposition

$$\mathrm{Ta}_p(E) \;\cong\; \mathbb{Z}_p \oplus \mathbb{Z}_p,$$

or in terms of $\mathbb{Q}_p$-vector spaces

$$V_p(E) \;:=\; \mathrm{Ta}_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \;\cong\; \mathbb{Q}_p \oplus \mathbb{Q}_p.$$

The advantage of studying torsion points on elliptic curves is that they provide us with many examples of Galois representations, which we describe below.

Recall that E is an elliptic curve defined over K. In addition, we shall now suppose our field K to be perfect. The action of the Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$ commutes with the group law on E, so leaves the finite subgroup $E[p^n]$ stable. Provided the characteristic of K is coprime to p, one obtains a two-dimensional representation

$$\rho_{E,p}^{(n)} : G_K \longrightarrow \mathrm{Aut}\big(E[p^n]\big) \;\cong\; \mathrm{GL}_2\big(\mathbb{Z}/p^n\mathbb{Z}\big)$$

for all integers $n \geq 1$. Passing to the limit over n yields

$$\rho_{E,p} : G_K \longrightarrow \mathrm{Aut}\big(\mathrm{Ta}_p(E)\big) \;\cong\; \mathrm{GL}_2(\mathbb{Z}_p),$$

and we shall also write $\rho_{E,p} : G_K \longrightarrow \mathrm{Aut}\big(V_p(E)\big) \;\cong\; \mathrm{GL}_2(\mathbb{Q}_p)$ for the associated vector space Galois representation.