MAT2000
- project on elliptic curves and modular forms

Eivind Dahl (eivinded)

May 16, 2012

Contents

1 Introduction

Elliptic curves are studied in many different branches of mathematics. In order to see why, it might help to look at some of their many guises.

The notion of an elliptic curve first arose in studying arc length on ellipses. In this problem one is led to study path integrals on the complex plane which are not path invariant, i.e., integrals along different paths between two given points may yield different values. This leads one to consider the integral as defined over an associated Riemann surface, where the integral *is* path-invariant. In this case we take the Riemann sphere and make two straight incisions: one from 0 to ∞, and one from 1 to a complex number λ depending on the ellipse in question. Taking

two copies of the resulting space, we glue the produced holes on either copy along "themselves" on the other copy, producing a torus. Indeed, the complex picture of an elliptic curve is just that: a torus, or in other words a Riemann surface of genus 1. The genus is an invariant associated to the curve which roughly counts occurances of what we see as the hole in the middle of the torus. Here *curve* is interpreted broadly as locally homeomorphic to $\mathbb{C}$, i.e., of 1 complex dimension.

In classical algebraic geometry and Diophantine geometry, where the problem is to study geometric and arithmetic properties of polynomial equations – respectively[1] – elliptic curves arise as the smooth curves of genus 1. The genus in this (smooth) setting is exactly related to that of the above. Here the case where genus $= 0$ is pretty well understood: it is the theory of quadratic equations in two variables. The case of curves of genus $= 1$ is far less understood, in contrast to the vast body of work surrounding it. In viewing such an object through the eyes of $\mathbb{C}$, we in fact obtain a Riemann surface as above and so the interpretation of elliptic curves as tori is not altogether lost.

Elliptic curves possess many favourable properties. The circle may be fitted with the structure of an abelian group under "addition of angles," and in viewing the torus as a product of two copies of the circle it inherits a componentwise abelian group structure. In fact, any Riemann surface of genus 1 may be fitted with the structure of an abelian group. This turns out to also be the case with algebraic elliptic curves defined over more general fields. Here an elliptic curve may be given an explicit form as the zero-set of a cubic equation in two variables: the Weierstrass equations, which we will study later. As a particular case, for an elliptic curve over a finite algebraic extension of $\mathbb{Q}$ the set of solutions in the extension is a finitely generated abelian group![2] This group is a much studied invariant of the given extension.

A common approach to studying a class of geometric mathematical objects is to parameterise them over a topological space. In favourable cases one may hope to produce a space on which each isomorphism class of objects uniquely determines and is uniquely determined by a single point. Such a space may informally be called a moduli or a classifying space. Then, studying this space (e.g. its topology, or rings of functions defined on it) may tell us a lot about the class of object under study. Over the complex numbers, an elliptic curve may be represented as a quotient of the complex plane by a rank two lattice $\mathbb{Z}\omega_1 + \mathbb{Z}\omega_2 \subset \mathbb{C}$ where ω_1 and ω_2 are complex numbers which do not lie on the same (real) line. In other

[1] Here 'the geometry' means their sets of solutions over algebraically closed fields k, where a single equation of degree d in a single indeterminate correspond to a single point in a d-dimensional coordinate space $k^d = \{(x_i \in k) \ : \ i = 1, \ldots, d\}$; 'the arithmetic' refers to the set of solutions in e.g. the integers or rational numbers.

[2] This is the Mordell-Weil theorem.

words, the data of an elliptic curve may be represented by a pair of complex numbers (ω_1, ω_2) with $\omega_1/\omega_2 \notin \mathbb{R}$. This representation, however, is not unique. The first reduction one may make is that the imaginary part of the ω_i may be taken to be positive, because taking the negative of one or both of the ω_i yields the same lattice and hence the same elliptic curve. In other words, the ω_i may be taken to lie in the *upper half plane* $\mathbb{H} = \{z \in \mathbb{C} : \operatorname{Im} z \geq 0\}$. One may then observe that given a non-zero complex number λ, the elliptic curves determined by (ω_i) and $(\lambda\omega_i)$ are isomorphic. We thus arrive at a second reduction: to normalize the lattice in such a way that $\omega_1 = 1$, replacing ω_2 by whichever one of $\pm\omega_2/\omega_1$ lies in $\mathbb{H}$. So, an elliptic curve may be represented by a single point ω in $\mathbb{H}$. A third natural step is to look at the group of (conformal) automorphisms of $\mathbb{H}$ which respect the isomorphism class of the elliptic curve determined by ω, that is, automorphisms A which are such that the elliptic curves determined by ω and $A\omega$ are the same for all such ω. A large such group turns out to be the of transformations $z \mapsto (az+b)/(cz+d)$ with the coefficients a, b, c, d integers, and $ad - bd = 1$ (i.e., matrices with integer entries whose colums span a parallelepiped of volume 1). The naïve quotient of $\mathbb{H}$ with respect the action of this group, wherein ω and each $A\omega$ become the same point, is not a well behaved topological space: it is in particular not a Riemann surface.[3] However, we may choose to study meromorphic functions defined on $\mathbb{H}$ which act as if they are functions on the quotient, i.e., functions which respect the action of $\{A\}$. This leads us to the theory of modular functions, which (in the complex setting) are meromorphic functions on $\mathbb{H}$ which respect the action of the $\{A\}$, or modular forms which are modular functions with a few.

In this assignment we show that an abstract elliptic curve over a field k may be written on *Weierstrass form*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We then show that if the characteristic of the field k is not 2, we may rid this equation of its a_1 and a_3 terms by choosing appropriate reparameterizations. If the characteristic of k is neither 2 nor 3, we may in addition get rid of the a_2 term. These calculations yield "modular invariants" c_4, c_6, Δ, which are independent of any particular parameterization of E. Such an invariant is called a modular function or form. The initial goal of this was to show that the ring of such modular forms (in a more general setting) is generated over $\mathbb{Z}$ by these three (appropriatly generalized) invariants c_4, c_6, Δ modulo a single relation. This calculation was first done by J. Tate, and later written down in an article by P. Deligne in 1972

[3]The problem is that if the elliptic curve classified by a point $\omega \in \mathbb{H}$ has a non-trivial automorphism, there is a corresponding automorphism of $\mathbb{H}$ which fixes the point ω. A natural interpretation exists as an *orbifold*, which takes account of such 'non-trivial symmetries of points'.

modulo a few details [1]. The assignment was to verify some of the details which were left out. Regrettably, I was unable to do this, and only some of the work on this project made any sense to hand in at all. No less, I now know that the Indian Taipan has the deadliest venom of any snake.

Thanks to John Rognes, for his patience and for giving me such an interesting problem. Thanks also to Geir Ellingsrud for taking the time to help me through some of the algebraic geometry in Deligne's article. Not to mention the people who have been nice enough to read some of this text (in its various forms), and reasonable enough to comment on some of my longer sentences sentences.

2 Divisors on algebraic curves

A rational function f on a curve X over an algebraically closed field k corresponds to a morphism $X \to \mathbb{P}^1$, denoted by abuse of language by the same letter f. A tuple $(f_0, \ldots, f_r)$ of $r+1$ rational functions not all simultaneously vanishing anywhere on X, give a rational morphism

$$X \to \mathbb{P}^r : (f_0 : \cdots : f_r).$$

A divisor on a curve makes it is possible to specify vector spaces of rational functions on X with a given configuration of poles and zeroes. Given the genus of the curve, the dimension of these vector spaces are made accessible through the Riemann-Roch theorem. Using this data it sometimes possible to show the existence of a good morphism of the curve into projective space, realizing it as (say) a closed subvariety of $\mathbb{P}^r$. In the next section we use this to show the existence of an explicit presentation inside $\mathbb{P}^2$ of any elliptic curve.

This section is mostly meant to establish notation. For more on divisors curves and related subjects, see [4]. Throughout, let X be a smooth curve over an algebraically closed field k in the sense of [3] or [2].

Definition 2.1. The group of *divisors* on the curve X, written $D(X)$, is the free abelian group on the set $X(k)$ of points P of X. Hence a *divisor* $D \in D(X)$ may be written as a sum

$$\sum_P n_P P,$$

where $n_P = 0$ for almost all P. The coefficient of D at the point P is then written $v_P(D) = n_P$, and the *degree* of D is the sum

$$\deg(D) = \sum_P n_P,$$

which is well defined, because almost all n_P are 0.

Since X is irreducible and reduced, the sheaf $\mathscr{O}_X$ of regular functions on X is a subsheaf of the constant sheaf $k(X)$ of rational functions on X. Since X is smooth of dimension 1, each stalk $\mathscr{O}_P$ of functions regular near P is a noetherian local ring of dimension 1, meaning the cotangent space $\mathfrak{m}_P/\mathfrak{m}_P^2$ at P is of dimension 1 over $k(P) = \mathscr{O}_P/\mathfrak{m}_P \cong k$. Hence the ring $\mathscr{O}_P$ is a discrete valuation ring, with valuation v_P determined by sending a generator t of $\mathfrak{m}_P/\mathfrak{m}_P^2$ to 1. Writing $v_P(f/g) = v_P(f) - v_P(g)$ for $f/g \in k(X)^*$, we may extend v_P to all of $k(X)^*$.

Definition 2.2. A rational function f is said to *vanish* to – or have a *zero* of – order n at P if $v_P(f) = n$. It is said to have a *pole* if $v_P(f) = -n$. The *divisor* (f) associated to a rational function $f \in k(X)$ is the expression

$$(f) = \sum_P v_P(f)P.$$

This is a finite sum [4] and so (f) is indeed a divisor.

We say that a divisor D is *positive* if

$$v_P(D) \geq 0 \text{ for each } P.$$

This gives the set $D(X)$ a partial order in writing $D \geq D'$ if $D - D'$ is positive.

If D is a divisor on X we may, using the partial order on $D(X)$, form the k-vector space $L(D)$ of rational functions on X with poles of order *at most* that specified by D, and zeroes of order *at least* that prescribed by D. Following this, we define

$$L(D) = \{f \in k(X)^* \,:\, (f) \geq -D\} \cup \{0\}.$$

It is also convenient to write

$$\ell(D) = \dim_k L(D).$$

Note that with these definitions, the divisor nP asks for a pole at P at most of order n, and the divisor $-nP$ asks for a zero at P of at least order P.

The $k(X)$-vector space $\Omega_{k(X)/k}$ of relative differential forms of $k(X)$ over k, as defined in Appendix A, is called the space of *rational (differential) forms* on X and is written here Ω_X, or simply Ω. It is a 1-dimensional vector space over $k(X)$, and if t is a uniformizer at a point P of X, then dt is a $k(X)$-basis for Ω [5]. In other words, given a rational form $\pi \in \Omega$ there is a unique rational function $f \in k(X)$ with

$$\pi = f dt.$$

This f is written π/dt, and the quantity $v_p(\pi) = v_p(\pi/dt)$ does not depend on choice of uniformizer t, and so v_P is a well defined function on $\Omega - \{0\}$ [5]. Using

this, there is a divisor (π) attached to any rational differential form π on X defined along the same lines as the divisor attached to a rational function:

$$(\pi) = \sum_P v_P(\pi)P.$$

The image in $D(X)$ of Ω under this assignment is the space of *canonical divisors* on X. We denote by K any canonical divisor on X.

3 Elliptic curves

An *elliptic curve* E is a smooth curve of genus 1 over a field k, together with a distinguished k-rational point $e \in E(k)$. Throughout, let E be a fixed elliptic curve. We recall the Riemann-Roch theorem.

Theorem 3.1. *Let X be a smooth curve of genus g over an algebraically closed field k, and K a canonical divisor on X. Then for any divisor $D \in \mathrm{Div}(C)$,*

$$\ell(D) - \ell(K - D) = \deg(D) - g + 1.$$

Proof. [4] □

The Riemann-Roch theorem requires the base field to be algebraically closed. Hence, the following results are obtained after base change to an algebraic closure $\overline{k}$ of k. Since the divisor determined by the point e is defined over k, the vector spaces $L(ne)$ have bases consisting of functions in $k(E)$, that is, functions stabilized by the Galois action of $\overline{k}$ over k [5]. Hence the following results are true for any field k (within any specified characteristic).

Lemma 3.2. *A choice $\pi \in \Omega_{E/k}$ determines a k-isomorphism between the space $L(K)$ of rational functions as prescribed by K, and the space $\omega \subset \Omega_{E/k}$ of holomorphic differential on E.*

Proof. Let K be the canonical divisor on E determined by the differential form π. If $f \in L(K)$, so $(f) \geq -K$, then $(f\pi) \geq 0$, and hence $f\pi$ is a holomorphic differential. If conversely $f\pi$ is regular, then $f \in L(K)$, so the choice of π establishes a k-isomorphism of $L(K)$ onto the k-vector space ω of holomorphic differential forms on E by mapping f to $f\pi$. □

Note that since $\ell(K) = g = 1$, the vector space ω is of dimension 1.

Definition 3.3. A non-zero element of ω is called an *invariant differential* on E.

Lemma 3.4. *The space $L(ne)$ is an n-dimensional k-vector space for $n > 0$.*

Proof. This is a direct application of the Riemann-Roch theorem after observing that $\deg(K) = 2g-2 = 0$ leads to $\ell(K-ne) = 0$: since $\deg(K-ne) < 0$ for positive n, any non-zero $f \in L(K-ne)$ would have to satisfy

$$0 = \deg(f) \geq -\deg(K-ne) = ne > 0$$

which is absurd. □

Now

$$k = L(e) \subset \cdots \subset L(ne)$$

is an increasing filtration of $L(ne)$. Following [1], the associated graded terms of this filtration are $\omega^{\otimes -(n+1)}$. If π is a non-zero invariant differential form on E, then by this there is a basis of $(x, y, 1)$ of $L(3e)$ with $x \in L(2e)$, $y \in L(3e)$, such that $x \mapsto \pi^{\otimes -2}$ and $y \mapsto \pi^{\otimes -3}$ in the associated graded terms.

Because ω is a 1-dimensional k-vector space, any other such differential π' is of the form $u\pi$ with $u \in k^*$, and hence by the previous lemma any pair of choices π, x, y and π', x', y' are related

$$\begin{aligned} x &= u^2 x' + r \\ y &= u^3 y' + s u^2 x' + t \\ \pi &= u\pi', \end{aligned} \tag{1}$$

for free $r, s, t \in k$ and $u \in k^*$ a unit.

Proposition 3.5. *Let an invariant differential π be given, and let x, y be rational functions as above. Then there is a relation in $L(6e)$ which may be written*

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

Furthermore, the rational map $(x : y : 1) : E \to \mathbb{P}^2$ is an embedding of E onto a curve of this form, with a single point $(0 : 1 : 0)$ at infinity.

Proof. The seven functions

$$1,\ x,\ y,\ x^2,\ xy,\ y^2,\ x^3$$

are all contained in $L(6e)$, which is a vector space of dimension 6. Hence in $L(6e)$ there is a non-trivial linear relation,

$$a + bx + cy + dx^2 + exy + fy^2 + gx^3 = 0,$$

between them. If the coefficient of either one of y^2, x^3 vanished, every term in the resulting relation would have a pole of different order and the relation would be trivial. After scaling y by fg^2 and x by $-gf$, the coefficient of y^2 becomes f^3g^4, and the coefficient of x^3 becomes $-f^3g^4$. By dividing through by f^3g^4, rearranging and relabelling, we arrive at the *Weierstrass form*:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2}$$

(Here the labels a_i of the coefficient of any given term is chosen such that i plus the filtration degree of the term is equal to 6, to signify that the relation is in the vector space $L(6e)$.)

Now $\varphi = (x : y : 1)$ is a rational map of E into a projective plane. Because E is a smooth curve, this is a regular map. If X denotes the image of E under φ, then $\varphi : E \to X \subset \mathbb{P}^2$ is a non-constant morphism of curves, and hence it is surjective. To see that it is an isomorphism, observe that $x : E \to \mathbb{P}^1$ has degree 2, and $y : E \to \mathbb{P}^1$ degree 3. Then $k(E)$ is a field extension of $k(X) = k(x,y)$ of degree dividing 2 and 3 of $k(X) = k(x,y)$, and hence ϕ is an isomorphism onto its image. □

Note that the differential π given coordinates x, y, may be written

$$\pi = \frac{dx}{2y + a_1x + a_3} = -\frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}.$$

4 The Weierstrass equations

4.1 Variance of the a-parameters

If two choices π, x, y and π', x', y' are given, producing two Weierstrass relations with coefficients a_i and a_i' respectively, we will need to know how a change of coordinates taking the first form to the second relates the a_i to the a_i'. These and various other such relations are listed in Deligne's paper, but it seems appropriate to verify some of them here. This is a direct calculation (recall that u is a unit):

		a_1	a_3	a_2	a_4	a_6
y'^2	$u^{-6}y'^2$	$+2su^{-5}xy$	$+2tu^{-3}y$	$+s^2u^{-4}x^2$	$+stu^{-2}x$	$+t^2$
a_1xy		$a_1u^{-5}xy$	$+a_1ru^{-3}y$	$+a_1su^{-4}x^2$	$+a_1(t+rs)u^{-2}x$	$+a_1rt$
a_3y			$a_3u^{-3}y$		$+a_3su^{-2}x$	$+a_3t$
x^3	$u^{-6}x^3$			$+3ru^{-4}x^2$	$+r^2u^{-2}x$	$+r^3$
a_2x^2				$a_2u^{-4}x^2$	$+2a_2ru^{-2}x$	$+a_2r^2$
a_4x					$a_4u^{-2}x$	$+a_4r$
a_6						a_6.

Here an entry in the left-most column is sent to the sum in the corresponding row under such a transformation. The terms in the successive columns correspond to the a_i in the upper-most row.

Using this, remembering to introduce signs if we move a term in either of the three first rows from the l.h.s. to the r.h.s. of

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

we may immediatly verify Deligne's assertions:

$$\begin{aligned} ua_1' &= a_1 + 2s \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\ u^3a_3' &= a_3 + ra_1 + 2t \\ u^4a_4' &= a_4 - sa_3 + 2a_2r - (t+rs)a_1 + 3r^2 - 2st \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{aligned} \tag{3}$$

4.2 The first and second canonical form

Assume the characteristic of k is not 2. Then we may eliminate a_1 and a_3 from (2) by transforming by $r = 0$, $s = -\frac{1}{2}a_1$, $t = -\frac{1}{2}a_3$. The resulting a_i-coefficients are by (3) thus

$$a_1' = 0 \qquad a_2' = a_2 + \frac{1}{4}a_1^2 \qquad a_3' = 0$$
$$a_4' = a_4 + \frac{1}{2}a_1a_3 \qquad a_6' = a_6 + \frac{1}{4}a_3^2.$$

It is customary to write

$$b_2 = 4a_2 + a_1^2 \qquad b_4 = 2a_4 + a_1a_3 \qquad b_6 = a_3^2 + 4a_6,$$

arriving at the expression

$$y^2 = x^3 + \frac{1}{4}b_2x^2 + \frac{1}{2}b_4x + \frac{1}{4}b_6. \tag{4}$$

The variance of the b-parameters are written down in Deligne's paper:

$$\begin{aligned} u^2b_2' &= b_2 + 12r \\ u^4b_4' &= b_4 + rb_2 + 6r^2 \\ u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3. \end{aligned}$$

Hence, if we let $1/3 \in k$, we may get rid of the x^2 term by choosing $r = -\frac{1}{12}b_2$ (with $s,t = 0$, or we would introduce non-zero $a_1' = 2s$ and $a_3' = 2t$). We get

$$b_2' = 0 \qquad b_4' = b_4 - \frac{1}{24}b_2^2 \qquad b_6' = b_6 - \frac{1}{6}b_2b_4 + \frac{1}{216}b_2^3,$$

and clearing denominators we put

$$\begin{aligned} -c_4 &:= 24b_4 - b_2^2 \\ -c_6 &:= 216b_6 - 36b_2b_4 + b_2^3 \\ 4y^2 &= 4x^3 - \frac{1}{24}c_4x - \frac{1}{216}c_6. \end{aligned}$$

The classical way to write this equation is setting $g_2 = \frac{1}{12}c_4$ and $g_3 = \frac{1}{216}c_6$, clearing denominators (multiplication by 2) and setting $Y = 2y,\ X = x$ so:

$$W : Y^2 = 4X^3 - g_2X - g_3.$$

4.3 The modular discriminant and the c-invariants.

The discriminant of the cubic on the right hand side of this equation is

$$\delta = \frac{1}{64}b_2^2b_4^2 - \frac{1}{64}b_2^3b_6 - \frac{1}{2}b_4^3 - \frac{27}{16}b_6^2 + \frac{9}{16}b_2b_4b_6.$$

Writing

$$-4b_8 = b_4^2 - b_2b_6$$

we see that

$$\delta = -\frac{1}{16}b_2^2b_8 - \frac{1}{2}b_4^3 - \frac{27}{16}b_6^2 + \frac{9}{16}b_2b_4b_6.$$

Clearing denominators we get

$$\Delta = 16\delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

In fact, a curve of the affine form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

over a field k is smooth if and only if $\Delta \neq 0$. [1, 5]

By the expressions

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ -c_6 &= 216b_6 - 36b_2b_4 + b_2^3 \end{aligned}$$

we see that there is a relation

$$c_4^3 - c_6^2 = 1728\Delta.$$

5 The ring of integral modular functions

Consider an elliptic curve E together with a choice of invariant differential π and coordinates x, y. Let A be a change of coordinates as in (1), and let f be a law which associates to any such E an element $f(E) \in \omega^{\otimes n}$ and satisfies

$$f(A \cdot E) = u^{-n} f(E)$$

for all such coordinate changes A. Then by (1) the quantity $f(E)\pi^{\otimes n}$ is independent of choice of π, x, y. In other words, f assigns invariants to isomorphism classes of elliptic curves. We call such an f a *modular function of weight n*.

By Deligne's article,

$$u^4 c_4' = c_4 \qquad u^6 c_6' = c_6 \qquad u^{12}\Delta' = \Delta,$$

so these are modular in the sense that $c_4\pi^{\otimes 4}$, $c_6\pi^{\otimes 6}$, and $\Delta\pi^{\otimes 12}$ are invariants of the isomorphism class of E independent of choice of π, x, y.

In general, a family of curves of genus 1 over a base scheme S is an proper flat morphism $p : E \to S$ of finite presentation, together with a section $e : S \to E$ landing where the fibers of p are smooth. The fibers of p are taken to be integral curves of arithmetic genus 1, which means that they are either smooth (elliptic), or have a nodal or cusp singularity. The latter are called multiplicative and additive fibers respectively, and the smooth subscheme of any fiber is a either an elliptic curve, or isomorphic to $\mathbb{G}_m$ or $\mathbb{G}_a$ (respectively) with identity as picked out by e. In the case where 2 and 3 are invertible in the base S, such a family may be represented by morphism to a scheme

$$\mathscr{S} : \mathrm{Spec}(\mathbb{Z}[2^{-1}, 3^{-1}][g_2, g_3]),$$

and the family p is acquired by pulling back a "universal family"

$$\mathscr{E} : Y^2 = X^3 - g_2 X - g_3,$$

so:

$$\begin{array}{ccc} E & \longrightarrow & \mathscr{E} \\ \downarrow & & \downarrow \\ S & \longrightarrow & \mathscr{S}. \end{array}$$

If if this pullback is taken to preserve a single piece of extra (an appropriate variant of the invariant differential form above) the morphism to $\mathscr{S}$ is unique up to unique isomorphism. This preserving of extra structure to ensure uniqueness is termed to

"rigidify" the classification problem, eliminating automorphisms of p. Here, no restriction is made on the smoothness of the fibers of p.

Given a family p, there is in particular a quantity c_4 (locally the above) which does not depend on any particular choices of coordinates, i.e., it is an invariant of the isomorphism class of the curve. If c_4 is an invertible section in a sheaf on S the given family is without fibers with a cusp singularity. It may then be classified by a morphism to

$$\mathrm{Spec}(\mathbb{Z}[2^{-1}][a_2,a_3,(a_2^2-3a_4)^{-1}]/(a_2a_4-9a_6)),$$

and acquired by pulling back the universal family

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

(uniquely, given that an invariant differential form is preserved).

Given a family of curves of genus 1 over S, one may define a sheaf $\omega = e^*\Omega^1_{E/S}$ on S. An *integral modular form of weight n* is one which assigns to any E/S a section $f(E/S) \in \omega^{\otimes n}$ in a manner compatible with base change. Using data such as the classifications hinted at above (which are made in Deligne's paper), one may prove:

Theorem 5.1. *The ring of integral modular functions is generated on $\mathbb{Z}$ by c_4, c_6 and Δ, subject to the relation*

$$c_4^3 - c_6^2 = 1728\Delta.$$

Proof. [1] □

A Relative differential forms

The following is more or less from [2]. Let k be a ring, A a k-algebra and M an A-module. A k-derivation of A into M is a k-linear map $f : A \to M$ such that

$$f(rs) = f(r)\cdot s + r\cdot f(s) \quad \text{and} \quad f(u\cdot 1) = 0,\ u \in k.$$

Proposition A.1. *There is an A-module $\Omega_{A/k}$, unique up to unique isomorphism, together with an initial derivation*

$$d : A \to \Omega_{A/k},$$

such that any k-derivation $f : A \to M$ factors uniquely through d by an A-linear map $\widetilde{f} : \Omega_{A/k} \to M$.

Proof. Take $\Omega_{A/k}$ to be the A-module generated by symbols $df, f \in A$, subject to the three relations

$$\begin{aligned} d(r+s) &= dr+ds \\ d(rs) &= dr\cdot s + r\cdot ds \\ d(u\cdot 1) &= 0, \end{aligned}$$

for $r,s \in A$ and $u \in k$. There is a natural k-derivation $d : A \to \Omega_{A/k}$ which takes an element $r \in A$ to $dr \in \Omega_{A/k}$.

If $f : A \to M$ is any k-derivation, take $\widetilde{f} : \Omega_{A/k} \to M$ to be $dr \mapsto fr$.

Since $d : A \to \Omega_{A/k}$ is taken to be initial with respect to these properties, it is unique by properties of limits in category theory. □

If $\mathrm{Der}_k(A,M)$ denotes the set of k-derivations of A into M, then the property of $(\Omega_{A/k}, d)$ in the proposition above simply states

$$\mathrm{Der}_k(A,M) \cong \mathrm{Lin}_A(\Omega_{A/k}, M),$$

where the right side is the set of A-linear morphisms $\Omega_{A/k} \to M$.

Definition A.2. The *relative differential forms of A over k* is the module $\Omega_{A/k}$, together with the k-derivation d.

References

[1] P. Deligne. Courbes elliptiques: formulaire d'après J. Tate. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 53–73. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[2] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

[3] Jean-Pierre Serre. Faisceaux algébriques cohérents. *Ann. of Math. (2)*, 61:197–278, 1955.

[4] Jean-Pierre Serre. *Groupes algébriques et corps de classes*. Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris, 1959.

[5] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1992. Corrected reprint of the 1986 original.