ELLIPTIC CURVES AND MODULAR FORMS

CARL MAUTNER

Abstract. In the first section we introduce elliptic curves as certain smooth curves in $\mathbb{P}^2$. In the second section we then consider the group law on their points and formulate an equivalent definition as projective one dimensional group varieties, sketching the equivalence. We conclude by considering the more general notion of a pointed curve of genus 1 over an arbitrary base scheme and define the notion of a modular form. The first two sections follow parts of Silverman's books [3, 4] and the third section is based on the short note [1] by Deligne.

1. Elliptic curves as cubics in $\mathbb{P}^2$...

Definition 1.1. An *elliptic curve* over an algebraically closed field K is a nonsingular curve C in $\mathbb{P}^2$ defined by a cubic equation such that $C \cap \mathbb{P}^1_\infty = [0:1:0]$ (where $\mathbb{P}^1_\infty$ is the points $[*:*:0]$).

If we ask only that the curve be nonsingular at infinity, in coordinates $[X, Y, Z]$, any such cubic can be written in the form

$$Y^2Z + a_1XYZ + a_2YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3.$$

In affine coordinates, this becomes what is called the Weierstrass form:

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

If $\mathrm{char}(K) \neq 2$, then using the change of coordinates

$$\begin{aligned} y_1 &= \tfrac{1}{2}(y - a_1x - a_3), \\ x_1 &= x, \end{aligned}$$

we obtain the equation:

$$\begin{aligned} y_1^2 &= 4x_1^3 + b^2x_1^2 + 2b_4x_1 + b_6, \\ b_2 &= a_1^2 + 4a_2, \\ \text{where} \quad b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

Of course, we do not need any restrictions on K to define these numbers. Similarly, we can define the following objects associated to a fixed Weierstrass equation.

$$\begin{aligned} b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta &= -b_2^2b_8 - 8b_4b^3 - 27b_7^2 + 9b_2b_4b_6, \\ j &= c_4^3/\Delta, \\ \omega &= dx/(2y + a_1x + a_3) = dy/(3x^2 + 2a_2x + a_4 - a_1y). \end{aligned}$$

The last three have names: Δ is called the discrimanent, j the j-invariant, and ω the invariant differential.

If the field's characteristic is neither 2 nor 3, by the following change of coordinates:

$$\begin{aligned} x_2 &= (x_1 - 3b_2)/36 \\ y_2 &= y_1/108, \end{aligned}$$

Date: Yesterday.

$ua_1' = a_1 + 2s$	
$u^2a_2' = a_2 - sa_1 + 3r - s^2$	
$u^3a_3' = a_3 + ra_1 + 2t$	
$u^4a_4' = a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st$	
$u^6a_6' = a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1$	
$u^2b_2' = b_2 + 12r$	$u^4c_4' = c_4$
$u^4b_4' = b_4 + rb_2 + br^2$	$u^6c_6' = c_6$
$u^6b_6' = b_6 + 2rb_4 + r^2b_2 + 4r^3$	$u^{12}\Delta' = \Delta$
$u^8b_8' = b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4$	$j' = j$
	$u^{-1}\omega' = \omega$

TABLE 1. a,b,c's under change of coordinates given in equation 1.

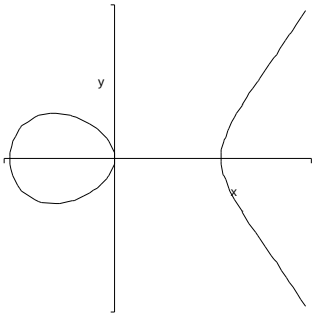

FIGURE 1. Real points of the elliptic curve $y^2 = x^3 - x$.

we obtain

$$y_2^2 = x_2^3 - 27c_4x_2 - 54c_6.$$

Now of course we are really interested in the curve itself and not so much in the equation, so we should try to understand how things change if we change variables in a way which perserves Weierstrass form and fixes the point $[0 : 1 : 0]$.

Such changes of variables are

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

where $r, s, t \in K$ and $u \in K^*$. This changes the quantities above as shown in the table 1.

As an excuse to draw some pictures, we have included plots of real points of some Weiestrass equations in figures 1 and 2.

We conclude the section with a few easy facts, proofs of which can be either be provided by the reader or found in [3].

1. A Weierstrass curve is singular if and only if $\Delta = 0$.

2. Two elliptic curves over a field K, C and C', are isomorphic over $\bar{K}$ if and only if the have the same j-invariants, i.e., j(C)=j(C').

3. $div(\omega) = 0$, in other words, the invariant differential is homolomorphic and nonvanishing.

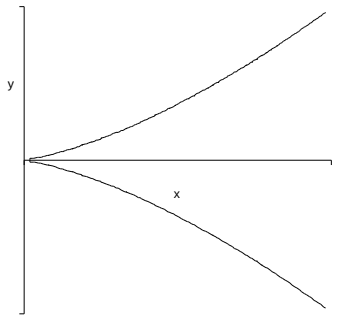

FIGURE 2. Real points of the singular cubic $y^2 = x^3$.

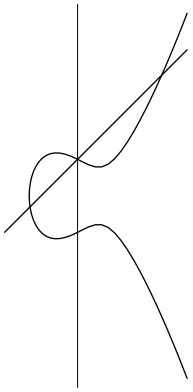

FIGURE 3. Group law on curve $y^2 = x^3 - x + 1$.

2. ... AND AS ONE DIMENSIONAL GROUP VARIETIES

As C is defined by a cubic, interesecting with any line in $\mathbb{P}^2$ will provide three points (when counted with multiplicity) of C. It turns out that one can define a group law on the points of C by declaring that any three points of C obtained from intersection with a line should sum to the identity element. More directly, given two points P and Q on C, we define their sum as follows:

(1) Find the line L containing P and Q (or tangent to C at P if $P = Q$) and let R be the third point on $L \cap C$. (2) Take the line L' passing through R and $O = [0, 1, 0]$ and define $P + Q$ to be the third point of intersection in $L \cap C$.

A picture illustrating this group law is shown in Figure 3.

Theorem 2.1. *The law defined above provides an abelian group structure on the points of C with identity element $O = [0, 1, 0]$. In fact, the maps*

$$+ : E \times E \to E, - : E \to E$$

are morphisms.

Proof: See [3] III.2-3.

Corollary 2.2. *An elliptic curve C over K is a one dimensional group variety over K.*

In fact, there is a rather strong converse to this statement.

Theorem 2.3. *Let G be a one dimensional group variety over an algebraically closed field K. Then either:*

(i) $G \equiv \mathbb{G}_a$ the additive group,
(ii) $G \equiv \mathbb{G}_m$ the multiplicative group,
or (iii) G is an elliptic curve.

Remark: Over a non-algebraically closed field, a very similar statement is true, the only modification being that there can be 'more multiplicative groups.'

We will only sketch a proof, for more details see [4]. We begin by recalling a lemma.

Lemma 2.4. *Let B be a non-singular projective curve of genus g and $S \subset B$ a finite set of points such that:*
(i) $\#S \geq 3$ if $g = 0$, (ii) $\#S \geq 1$ if $g = 1$, and (iii) S is arbitrary if $g \geq 2$.
Then, $Aut(B; S) = \phi \in Aut(B) | \phi(S) \subset S$ is a finite set.

Assuming the lemma, we continue by noting that as G is a group, it is non-singular and irreducible, which together with the fact that it is one dimensional implies that it embeds as a Zariski open subset in a non-singular projective curve $G \subset B$ (cf. [2] I.6).

Let $S = B - G$. Now each point $P \in G$ provides a different translation automorphism $\tau_P : G \to G$ of G as a variety. This extends to a rational map from B to B and as B is non-singular, an element of $\mathrm{Aut}(B; S)$. This gives an injection of G into $\mathrm{Aut}(B; S)$ so this set can not be finite. Applying the lemma above shows that either G if $\mathbb{P}^1$ with 0,1, or 2 points removed or a genus on surface.

A simple argument shows that $\mathbb{P}^1$ does not admit a group structure (even topologically!), and the only group stucture on $\mathbb{A}^1$ (resp. $\mathbb{A}^1 - 0$) is $\mathbb{G}_a$ (resp. $\mathbb{G}_m$). It then remains to show that a genus one curve G with a base point O is isomorphic to an elliptic curve and that the only possible group structures on the genus one surface arise from such an isomorphism. We will ignore the second issue and focus on the first as we will want to generalize the argument later.

Theorem 2.5. *Let $(B, 0)$ be a genus one curve with marked point $O \in B$. Then $(B, 0)$ is an elliptic curve, i.e. there exist functions $x, y \in K(B)$ such that the map*

$$\phi : B \to \mathbb{P}^2$$

defined by $\phi = [x, y, 1]$ is an isomorphism of B/K onto the elliptic curve

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

for some $a_1, \ldots, a_6 \in K$.

To prove this theorem, we will use the following special case of Riemann-Roch.

Theorem 2.6. *Let B be a curve of genus 1. If $D \in \mathrm{Div}(B)$ has positive degree and $\mathscr{L}(D) = \{f \in \bar{K}(C)^* : div(f) \geq -D\} \cup \{0\}$, then $dim\mathscr{L}(D) = degD$.*

We now apply this version of Riemann-Roch to the sequence of divisors: $O, 2(O), 3(O), \ldots$.

Applied to O we see that $dim\mathscr{L}(O) = 1$ so $\mathscr{L}$ consists of the constant functions $\bar{K}$. $\mathscr{L}(2(O))$ is 2 dimensional and thus will contain a function x with pole of order 2 at O. Similarly, $\mathscr{L}(3(O))$ is three dimensional and thus have anoth function y with a pole of order 3 at O. Continuing on, we see that $(1, x, y, x^2)$ is a basis for $\mathscr{L}(4(O))$ and $(1, x, y, x^2, xy)$ a basis for $\mathscr{L}(5(O))$. However, the dimension of $\mathscr{L}(6(O))$ is 6 and it must contain the functions $(1, x, y, x^2, xy, y^2, x^3)$. Thus there must exist a linear combination of these such that the coefficients of y^2 and x^3 are non-zero. This is precisely a Weierstrass equation.

It remains to show that the map ϕ defined in the statement of the theorem is (1) a surjective morphism, (2) a degree 1 map onto it's image C, and (3) C is smooth.

To see (1) we note that ϕ is a rational map from a smooth curve, and therefore a morphism. Moreover, any morphism between connected curves is surjective.

For (2) it is equivalent to show that $K(B) = K(x, y)$. First consider the map $[x, 1] : B \to \mathbb{P}^1$. It has a pole of order 2 at O and no others, so is of degree 2, i.e., $[K(B) : K(x)] = 2$. On the other hand, mapping E to $\mathbb{P}^1$ by $[y, 1]$ we see that $[K(B) : K(y)] = 3$. As 2 and 3 are relatively prime, $[K(B) : K(x, y)] = 1$ and thus $K(B) = K(x, y)$.

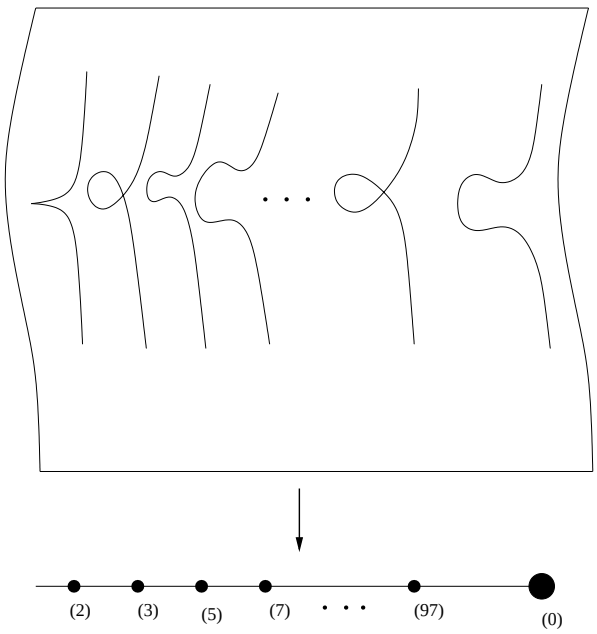

FIGURE 4. The curve $C_1 : y^2 = x^3 + 2x^2 + 6$ over $\operatorname{Spec}\mathbb{Z}$.

Lastly, suppose that C were singular. Then there would be a rational map to $\mathbb{P}^1$ of degree one. But composing this with ϕ would give a degree one map between smooth curves from B to $\mathbb{P}^1$. Any degree one map between smooth curves is an isomorphism which would imply that B was of genus zero, a condradiction.

Remark about elliptic curves over $\mathbb{C}$

3. Elliptic curves over arbitrary schemes

Now that we have a sense of what an elliptic curve looks like, we would like to understand how they behave in families. Once we do so, it makes sense to allow some singularities. For example, if one wants to understand the rational points of an elliptic curve, say $y^2 = x^3 + 2x^2 + 6$, it makes sense to look at its points after reducing modulo 2 or 3. However, in characteristic 2 (respectively 3), the curve becomes singular as $y^2 = x^3 + 2x^2 + 6 \equiv x^3$ (resp. $y^2 = x^3 + 2x^2$). So if we think of our curve as being a scheme over $\operatorname{Spec}\mathbb{Z}$, over most primes the geometric fiber will be an elliptic curve, but over 2 and 3 for example, it will become singular. We will examine this more carefully below.

This motivates the following definition.

Definition 3.1. A pointed curve of genus 1 over a scheme S is a proper, flat, finitely presented morphism $p : C \to S$ together with a section $e : S \to C$ such that the section is contained in the smooth locus of the fibers and every geometric fiber of p is either

(i) an elliptic curve,
(ii) a singular cubic in $\mathbb{P}^2$ with a node (multiplicative), or
(iii) a singular cubic in $\mathbb{P}^2$ with a cusp (additive).

Example 3.2. Consider the scheme over $\operatorname{Spec}\mathbb{Z}$ given in affine coordinates as $C_1 : y^2 = x^3 + 2x^2 + 6$. The discrimanant of this curve $-18624 = -2^6 \cdot 3 \cdot 97$. It follows that C_1 is singular only over the primes $(2), (3), (97)$. As we saw above, C has a cusp over (2) and a node over (3), similarly one can check that it also has a node over (97). See Figure 4.

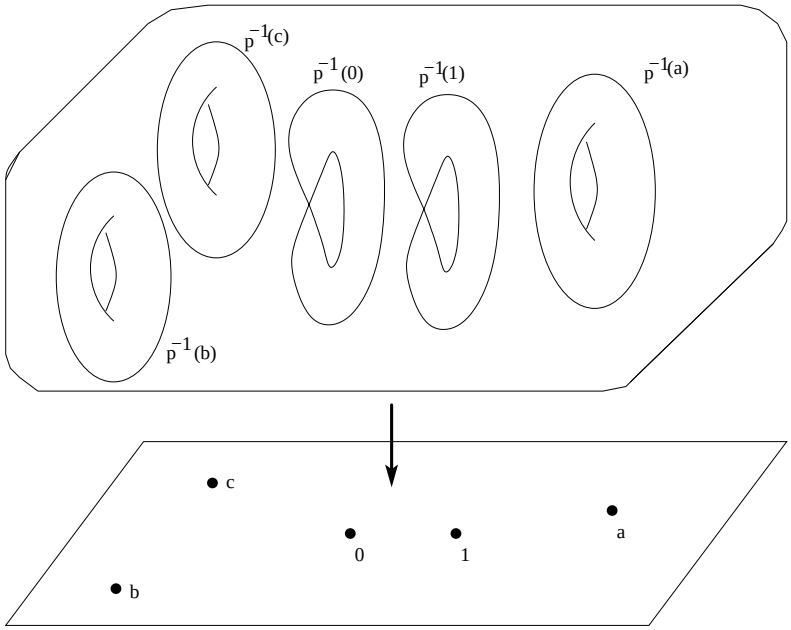

FIGURE 5. The curve $C_2 : y^2 = x(x-1)(x-\lambda)$ over $\mathrm{Spec}(\mathbb{C}[\lambda]) = \mathbb{A}^1$.

Example 3.3. Over the base $\mathrm{Spec}(\mathbb{C}(\lambda)) = \mathbb{A}^1$ we can consider the scheme $C_2 : y^2 = x(x-1)(x-\lambda)$. Over 0 and 1, the fibers are multiplicative and all other fibers are smooth. See Figure 5.

Definition 3.4. Let ω be the invertable sheaf $\omega = e^*\Omega^1_{C/S}$.

In other words, ω is the sheaf over S whose stalk at a closed point $s \in S$ is the restriction of the cotangent space of the geometric fiber over s to $e(s)$.

The section e is a relative Cartier divisor of C over S and one can check, fiber-by-fiber, that $R^1p_*\mathcal{O}(ne) = 0$ for all $n > 0$. Riemann-Roch tells us that $p_*\mathcal{O}(ne)$ is locally free of rank n and the long exact sequence in cohomology gives the short exact sequence for $n > 0$:

$$0 \to p_*\mathcal{O}(ne) \to p_*\mathcal{O}((n+1)e) \to \omega^{\otimes -(n+1)} \to 0.$$

Further one can check fiber by fiber that $\mathcal{O}_S$ is isomorphic to $p_*\mathcal{O}(e)$. Putting this together we see that we have a filtration of $p_*\mathcal{O}(ne)$ by $p_*\mathcal{O}(me)$ for $1 \leq m \leq n$ with associated graded

$$\mathrm{Gr}\ p_*\mathcal{O}(ne) = \mathcal{O}_S \oplus \bigoplus_{i=2}^{n} \omega^{\otimes -i}.$$

We will use this to show that we can (locally) embed any pointed curve of genus 1 into $\mathbb{P}^2_S$ by a Weierstrass equation, just as we did for genus 1 curves over algebraically closed fields.

Let π be an invertable section of ω. In analogy to the simpler case, we choose a basis $\{1, x, y\}$ of $p_*\mathcal{O}(3e)$ such that $x \in p_*\mathcal{O}(2e) \subset p_*\mathcal{O}(3e)$ and under the projections to the pieces of the associated graded:

$$\begin{gathered} p_*(\mathcal{O}(3e)) \to \omega^{\otimes -3} \\ y \mapsto \pi^{\otimes -3} \\ p_*(\mathcal{O}(2e)) \to \omega^{\otimes -2} \\ x \mapsto \pi^{\otimes -2} \end{gathered}$$

If instead of π, we had chosen a different section $\pi' = u\pi$ where u is an invertable function, then all such bases with respect to u' can be written in terms of the old as

$$x = u^2x' + r$$
$$y = u^3y' + su^2x' + t.$$

We notice that this is just a global version of formula 1 from the first section and that all of the formulas in Table 1 still hold. Moreover, the section of $\omega^{\otimes 4}$ given by $c_4\pi^{\otimes 4}$ changes to $c_4'(\pi')^{\otimes 4}$, so it does not depend on the choice of π, x, and y. The same goes for $c_6\pi^{\otimes 6}$ and $\Delta\pi^{\otimes 12}$ which are sections respectively of ω^6 and ω^{12}. This suggests the following definition.

Definition 3.5. An integral modular form of weight n is a law associating to every pointed curve of genus 1 a section of $\omega^{\otimes n}$ in a way compatible with base change.

From the discussion above, examples of integral modular forms of weight 4, 6, and 12 are $c_4\pi^{\otimes 4}$, $c_6\pi^{\otimes 6}$, and $\Delta\pi^{\otimes 12}$.

Remark 3.6. The product of two integral modular forms f and g of weights n and m produces an integral modular form of weight $n + m$. If we let modular forms live in the direct sum of the tensor powers of ω, we can then consider integral modular forms as making up a ring.

Remark 3.7. As any pointed curve of genus 1 embeds locally in $\mathbb{P}^2_S$ by a Weierstrass equation, the curve $C : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ defined over $\operatorname{Spec}\mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ is universal and any modular form will be a polynomial in the a_i.

As we saw in section 1, if we only consider bases in which 2 and 3 are invertable (i.e., if we work over $\mathbb{Z}[1/6]$), then for a fixed choice of π, there exists a unique choice of x, y such that $a_1 = a_2 = a_3 = 0$. In analogy to the previous remark, this says that the curve given by $y^2 = x^3 - 27c_4x - 54c_6$ defined over $\mathbb{Z}[1/6][c_4, c_6]$ is universal over $\mathbb{Z}[1/6]$. This then implies that every $\mathbb{Z}[1/6]$-modular form is a polynomial in $\mathbb{Z}[1/6][c_4, c_6]$. But as both c_4 and c_6 are integral modular forms as shown above, we are left with the following theorem.

Theorem 3.8. *The ring of $\mathbb{Z}[1/6]$-modular forms is the polynomial ring $\mathbb{Z}[1/6][c_4, c_6]$.*

With a little more work the ring of integral modular forms can be calculated.

Theorem 3.9. *The ring of integral modular forms is generated over $\mathbb{Z}$ by c_4, c_6, and Δ and has only one relation:*

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

The proof can be found in [1].

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] 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.

[4] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.