Weierstrass equations

Seminar on elliptic curves and the Weil conjectures

Ludwig Bauer

June 5, 2016

This paper refers to the 4th talk in the seminar on elliptic curves and the Weil conjectures supervised by Prof. Dr. Moritz Kerz in the summer term 2016 at the University of Regensburg. It covers the section III.1 of J. H. Silverman's The Arithmetic of Elliptic Curves.

1 Introduction

In this lecture we continue our study of curves. More precisely we want to focus on curves (defined over a perfect field K) given by so called Weierstrass[1] equations.

Definition 1.1. *A Weierstrass equation is an equation of the form*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

with coefficients $a_1,\dots,a_6 \in \overline{K}$.[2] *Further we call a curve given by a Weierstrass equation a Weierstrass curve. Additionally we define*

$$\begin{aligned}
b_2 &:= a_1^2 + 4a_2,\\
b_4 &:= 2a_4 + a_1a_3,\\
b_6 &:= a_3^2 + 4a_6,\\
b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &:= b_2^2 - 24b_4,\\
c_6 &:= -b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &:= c_4^3/\Delta \text{ if } \Delta \neq 0,\\
\omega &:= \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y},
\end{aligned}$$

[1] named after the German mathematician Karl Theodor Wilhelm Weierstrass (1815 - 1897)

[2] by $\overline{K}$ we mean the algebraic closure of the field K

where the quantities Δ, j and ω are called the discriminant, the j-invariant and the invariant differential.

The equivalence of the different representations of ω can be checked by applying d and properties of differential forms on both sides of the Weierstrass equation in non-homogeneous coordinates (see below). We also want to note the two relations

$$4b_8 = b_2b_6 - b_4^2 \quad \text{and} \quad 1728\Delta = c_4^3 - c_6^2$$

which can be verified by simple calculation.

In the following we always consider a fixed Weierstrass curve E with coefficients $a_1,\ldots,a_6 \in \overline{K}$ unless stated otherwise. As usual E is said to be defined over K if all its coefficients lie in K. Moreover we occasionally switch to non-homogeneous coordinates, meaning that we substitute the points of our curve by $x = X/Z$ and $y = Y/Z$ in order to express E by the zero set of the polynomial

$$f(x, y) := y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

plus an extra point at infinity $O := [0, 1, 0]$.

Example 1.2. *Weierstrass curves can best be illustrated for $K = \mathbb{R}$.* Figure 1-6 *depict various examples of the real locus of a Weierstrass curve. Note that the curves shown in* Figure 1 *and* 2 *are singular whereas in* Figure 3-6 *smooth curves can be seen.*

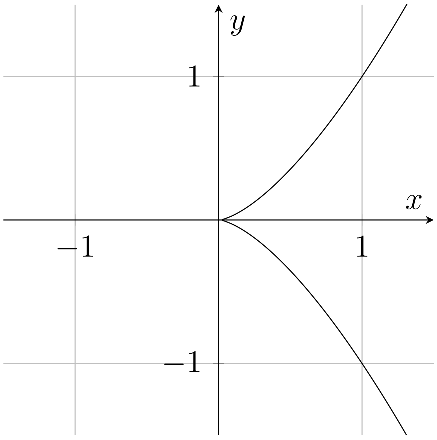

Figure 1: Graph of the curve given by $y^2 = x^3$.

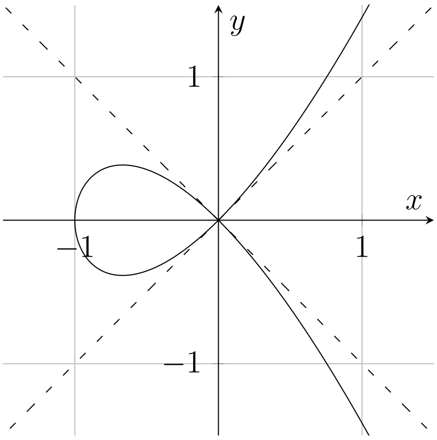

Figure 2: Graph of the curve given by $y^2 = x^3 + x^2$ with (dashed) tangent lines at the origin.

1.1 Motivation

To understand why we are interested in Weierstrass equations we give a short outlook in this section. First we introduce the main objects in this seminar, namely elliptic curves.

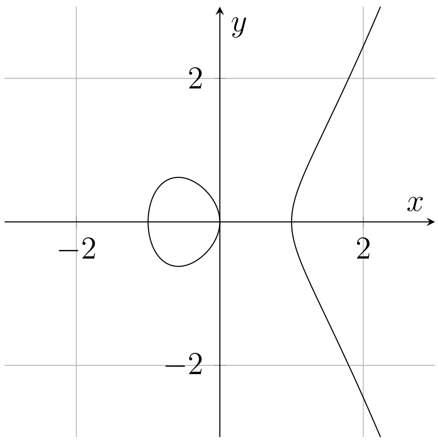

Figure 3: Graph of the curve given by $y^2 = x^3 - x$.

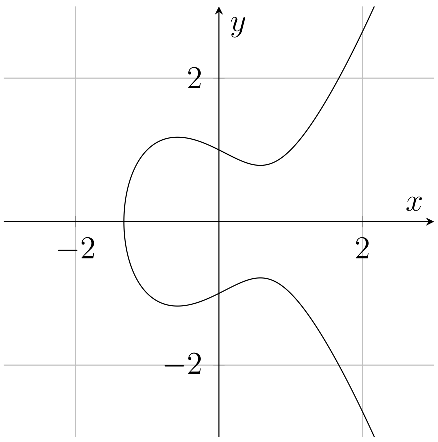

Figure 4: Graph of the curve given by $y^2 = x^3 - x + 1$.

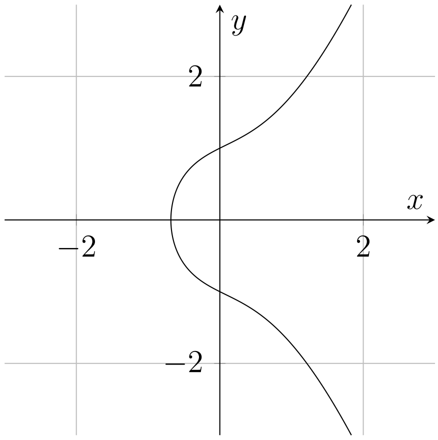

Figure 5: Graph of the curve given by $y^2 = x^3 + x + 1$.

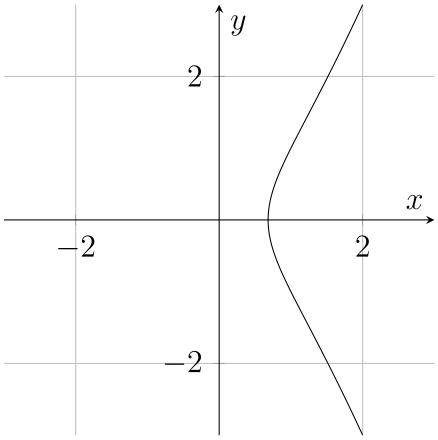

Figure 6: Graph of the curve given by $y^2 = x^3 + x - 1$.

Definition 1.3. *An elliptic curve (defined over K) is pair (C, P), where E is a non-singular curve of genus one (defined over K) and a (K-rational) so called base point $P \in C$. Two elliptic curves (defined over K) (C, O) and (C', P') are called isomorphic (over K) if there exists an isomorphism $\phi : C \to C'$ of curves (defined over K) satisfying $\phi(P) = P'$.*

As we will see now, Weierstrass equations are closely related to elliptic curves.

Proposition 1.4. a) *Every smooth Weierstrass curve defined over K is an elliptic curve defined over K with base point O.*

b) *Conversely, every elliptic curve defined over K is isomorphic over K to an elliptic curve defined over K given by a Weierstrass equation with base point O.*

c) *Any two elliptic curves defined over K given by Weierstrass equations are isomorphic over K if and only if they are related by a change of variables of the form*

$$(x,y) \mapsto (u^2x + r, u^3y + su^2x + t) \tag{1}$$

with u,r,s,$t \in K$ and $u \neq 0$.

The proof of 1.4 will be given later in this seminar. Next we want to look at the substitution (1) in more detail by stating some change-of-variable formulas that can be verified by simple (but tedious) calculation.

Remark 1.5. *Consider two curves given by Weierstrass equations with coefficients a_i,$a_i' \in \overline{K}$ for $i \in \{1,...,6\}$ that are related as in* 1.4 c)*. Then the following is true:*

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

Later on we will often use such a change of coordinates to our convenience. As we already saw, by a substitution like this we do not leave the isomorphism class of a given elliptic curve. But we do not only want to speak about elliptic curves. Instead we are going to look at Weierstrass curves in general and hence do not require them to be smooth.

1.2 Short Weierstrass equations

As there are many Weierstrass equations that define isomorphic elliptic curves its only natural to search for equations that are rather short, meaning that we want as many of its coefficients as possible to vanish. It turns out that there is a particularly simple way of describing elliptic curves (or more general Weierstrass curves) if we require the characteristic of K to be different from 2 and 3.

As mentioned earlier, our fixed curve E can be described in non-homogeneous coordinates by

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

for a_1,...,$a_6 \in \overline{K}$. First we only consider the case char(K)$\neq$ 2. Then by the substitution

$$y \mapsto y - \frac{a_1}{2}x - \frac{a_3}{2}$$

we can complete the square on the left side of (2) and E transforms into

$$E' : y^2 = x^3 + a_2'x^2 + a_4'x + a_6'$$

where the coefficients are given by

$$a_2' = a_2 + \tfrac{1}{4}a_1^2, \quad a_4' = a_4 + \tfrac{1}{2}a_1a_3 \quad \text{and} \quad a_6' = a_6 + \tfrac{1}{4}a_3^2.$$

If in addition char(K)$\neq$ 3 holds we can even eliminate the x^2-term by further substituting

$$x \mapsto x - \frac{a_2'}{3}$$

which transforms E' into

$$E'' : y^2 = x^3 + a_4''x + a_6''$$

for

$$a_4'' = a_4' - \tfrac{1}{3}a_2'^2 \quad \text{and} \quad a_6'' = a_6' + \tfrac{2}{27}a_2'^3 - \tfrac{1}{3}a_2'a_4'.$$

Apart from this we also want to remark a representation that is commonly used throughout literature. Therefore we need to scale the variables x and y by another substitution, namely

$$(x, y) \mapsto (u^2x, u^3y) \tag{3}$$

for $u \in \overline{K}^{\times}$. If we apply (3) for $u = 1/2$ and $u = 1/3$ respectively then E' transforms into

$$\tilde{E}' : y^2 = x^3 + b_2x^2 + 8b_4x + 16b_6$$

in the case char(K)$\neq$ 2 and E'' into

$$\tilde{E}'' : y^2 = x^3 - 27c_4x - 54c_6.$$

for char(K)$\notin \{2, 3\}$.

	$\mathrm{char}(K) = 2$	$\mathrm{char}(K) = 3$
$j = 0$	$y^2 + a_3y = x^3 + a_4x + a_6$	$y^2 = x^3 + a_4x + a_6$
$j \neq 0$	$y^2 + xy = x^3 + a_2x^2 + a_6$	$y^2 = x^3 + a_2x^2 + a_6$

Table 1: Short Weierstrass equations for $\mathrm{char}(K) \in \{2, 3\}$.

Remark 1.6. *Let E be a curve given by an equation of the form*

$$y^2 = x^3 + Ax + B.$$

for A,$B \in \overline{K}$. Then by direct calculation we get

$$\Delta = -16(4A^3 + 27B^2) \quad \textit{and} \quad j = -1728(4A)^3/\Delta \textit{ if } \Delta \neq 0.$$

Moreover the substitution (3) *transforms E into*

$$E' : y^2 = x^3 + A'x + B'$$

where the coefficients of E' satisfy

$$u^4A' = A \quad \textit{and} \quad u^6B' = B.$$

In particular we see that a transformation like this preserves the form of the (short) Weierstrass equation of E.

Summing up, we can say that a Weierstrass curve can always be imagined to be given by a short Weierstrass equation as in 1.6 if the characteristic of K is not 2 or 3. In the following we will often restrict to this case since the upcoming proofs become particularly nice to handle. Nevertheless, we also want to briefly introduce the situation $\mathrm{char}(K) \in \{2, 3\}$.

Remark 1.7. *In the case* $\mathrm{char}(K) \in \{2, 3\}$ *by a substitution as in* 1.4 c) *a Weierstrass curve can be always transformed into a curve given by an equation of the form as shown in* Table 1 *for coefficients a_1,...,$a_6 \in \overline{K}$.*

2 Quantities associated to Weierstrass equations

In this chapter we study three quantities associated to Weierstrass equations, namely the discriminant, the j-invariant and the invariant differential.

2.1 The discriminant

As we have already seen, a Weierstrass curve is an elliptic curve if and only it is smooth. Motivated by this observation in this section we want to introduce an easy method to check whether a given Weierstrass curve is smooth or not. Therefore we first look at singular Weierstrass curves in more detail. The next lemma justifies why we can always restrict to non-homogeneous coordinates.

Lemma 2.1. *The point at infinity of a Weierstrass curve is smooth.*

Proof. Considering our Weierstrass curve E we can define

$$F(X,Y,Z) := Y^2Z + a_1XYZ + a_3YZ^2 - X^3 + a_2X^2Z - a_4XZ^2 - a_6Z^3$$

and compute

$$\frac{\partial F}{\partial Z}(X,Y,Z) = Y^2 + a_1XY + 2a_3YZ + a_2X^2 - 2a_4XZ - 3a_6Z^2.$$

Since the partial derivative of F with respect to Z does not vanish[3] at $O = [0,1,0]$ the curve can not be singular at infinity by definition. □

Let P be a singular point of our curve E. Since we can always translate a fixed point by an admissible substitution as in 1.4 c) without loss of generality we can assume P to be at the origin. Therefore the conditions

$$f(P) = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0 \tag{4}$$

cause the coefficients a_3, a_4 and a_6 to vanish and hence we get

$$f(x,y) = y^2 + a_1xy - a_2x^2 - x^3. \tag{5}$$

If we let (α, β) be a solution to the problem

$$\alpha + \beta = -a_1 \quad \text{and} \quad \alpha\beta = a_2$$

in $\overline{K}^2$ we can also write

$$f(x,y) = (y - \alpha x)(y - \beta x) - x^3.$$

Note that whether α is equal to β does not depend on the choice of the solution (α, β).

Definition 2.2. *Let $P = (x_0, y_0)$ be a singular point of a Weierstrass curve. Then as above there are quantities α,$\beta \in \overline{K}$ that we can associate to P. We call P a cusp if $\alpha = \beta$ and a node if $\alpha \neq \beta$. We call the line(s) given by*

$$y - y_0 = \alpha(x - x_0) \quad \textit{and} \quad y - y_0 = \beta(x - x_0).$$

[3] in the sense that a homogeneous polynomial vanishes at a projective point

the tangent line(s) at P.

An example of a node and a cusp can be seen in the first two figures. In both pictures the origin is singular. The difference is that there are two (dashed) tangent lines at the singular point in Figure 2 whereas in Figure 1 only one single tangent line exists at $(0, 0)$, the latter coinciding with the x-axis.

Proposition 2.3. *A Weierstrass curve is singular if and only if $\Delta = 0$. If it is singular it has exactly one singular point that is a cusp if $c_4 = 0$ and a node if $c_4 \neq 0$.*

Proof. As mentioned before we only consider the case $\operatorname{char}(K) \notin \{2, 3\}$. Then we can assume our curve E to be given by a short Weierstrass equation

$$y^2 = x^3 + Ax + B$$

for A,$B \in \overline{K}$. Note that according to 1.5 the property of Δ and c_4 to be zero or not is preserved by a change of variables as in 1.4 c). As in (4), E is singular if and only if there is a solution to the problem

$$3x^2 + A = 2y = y^2 - x^3 - Ax - B = 0 \tag{6}$$

which can be rewritten to

$$y = 0, \quad x^2 = -\tfrac{1}{3}A \quad \text{and} \quad x^3 + Ax + B = 0.$$

If $A \neq 0$ we can plug in the second equation in the third and obtain $x = -\frac{3B}{2A}$. Then again using the second equation leads us to $(\frac{3B}{2A})^2 = -\frac{A}{3}$ that finally is the same as $\Delta = 0$ since after 1.6 the discriminant of E is given by $-16(4A^3 - 27B^2)$. By this representation of Δ the case $A = 0$ follows similarly as well. Further we see that E can not have more than one singular point since (6) can have at most one solution as can easily be checked.

Let us assume that E has a singular point P that is without loss of generality at the origin. By definition the point P is a cusp if and only if the function $y^2 + a_1xy - a_2x^2$ in y factors in $(y - \alpha x)^2$ for some $\alpha \in \overline{K}$. This is the case if and only if the polynomials discriminant $x^2(a_1^2 + 4a_2) = x^2c_4$ is zero for all x which is equal to $c_4 = 0$. Because P is a node if it is not a cusp this already completes the proof. □

Proposition 2.4. *A singular Weierstrass curve is birational to $\mathbb{P}^1$ (i.e., there is a rational map to $\mathbb{P}^1$ that has a rational inverse).*

Proof. As usual we assume the singular point of a given singular Weierstrass curve E to be at the origin and thus by (5) we can write

$$E : y^2 + a_1xy = x^3 + a_2x^2.$$

Clearly we have a rational map ϕ from E to $\mathbb{P}^1$ by the mapping $(x, y) \mapsto [x, y]$. To find an inverse we divide the Weierstrass equation by x^2 which yields

$$\left(\frac{y}{x}\right)^2 + a_1\frac{y}{x} = x + a_2. \tag{7}$$

Now we define another rational map

$$\psi : \mathbb{P}^1 \to E, \quad [x,y] \mapsto \left(\left(\tfrac{y}{x}\right)^2 + a_1 \tfrac{y}{x} - a_2, \left(\tfrac{y}{x}\right)^3 + a_1 \left(\tfrac{y}{x}\right)^2 - a_2 \tfrac{y}{x} \right).$$

One easily checks $\psi([x,y]) \in E$ for all $[x,y]$ with $x \neq 0$ to verify that ψ is indeed rational. Finally by taking compositions we obtain $\psi \circ \phi = \mathrm{id}_{\mathbb{P}^1}$ and using (7) we get $\phi \circ \psi = \mathrm{id}_E$ as well. □

Note that after all a singular Weierstrass curve can never be isomorphic to $\mathbb{P}^1$ since the projective space is nonsingular.

2.2 The j-invariant

By 1.5 we already know that isomorphic elliptic curves have the same j-invariant. Next we proof that the converse also holds what makes j an important invariant of elliptic curves and thus justifies its name. Note that j is well-defined for elliptic curves since smoothness implies $\Delta \neq 0$ as we have shown before.

Proposition 2.5. a) *Two elliptic curves are isomorphic if and only if they have the same j-invariant.*

b) *For each $j_0 \in \overline{K}$ there exists an elliptic curve defined over $K(j_0)$ with j-invariant j_0.*

Proof. For a) as before we only consider the case $\mathrm{char}(K) \notin \{2,3\}$. Then two elliptic curves E and E' can be given by short Weierstrass equations

$$y^2 = x^3 + Ax + B \quad \text{and} \quad y^2 = x^3 + A'x + B'.$$

As noted above we only need to consider the case where E and E' have the same j-invariant. Therefore we by 1.6 we get

$$\frac{(4A)^3}{4A^3 + 27B^2} = \frac{(4A')^3}{4A'^3 + 27B'^2}$$

which yields

$$A^3 B'^2 = A'^3 B^2. \tag{8}$$

Now again with 1.6 we can state isomorphisms of the form (3) between E and E' where we have to separate three cases to define $u \in \overline{K}$. First if $A = 0$ we have $B' \neq 0$ since otherwise (8) would imply $A' = 0$ or $B = 0$ and hence by computing the discriminant one of the curves would not be smooth. Then defining u as a solution of $u^6 B' = B$ gives the desired isomorphism. In the same way one concludes $A' \neq 0$ if $B = 0$ and chooses u by $u^4 A' = A$ in this case. Finally if neither A and B are zero again by arguing with (8) and the discriminant one concludes that both A' and B' don't vanish as well. Now we can use either $u^6 B' = B$ or $u^4 A' = A$ to determine u.

To proof b) we first consider the curve

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728} x - \frac{1}{j_0 - 1728}$$

in the case $j_0 \notin \{0, 1728\}$. Then one easily computes

$$\Delta_E = j_0^3/(j_0 - 1728) \neq 0 \quad \text{and} \quad j_E = j_0.$$

Next we look at the curves

$$E' : y^2 + y = x^3 \quad \text{and} \quad E'' : y^2 = x^3 + x$$

which yield

$$\Delta_{E'} = -27, \quad \Delta_{E''} = -64, \quad j_{E'} = 0 \quad \text{and} \quad j_{E''} = 1728.$$

If $\mathrm{char}(K) \notin \{2,3\}$ the curves E' and E'' both are smooth and hence suffice as examples in the remaining case. If $\mathrm{char}(K) = 2$ the curve E' is smooth and its j-invariant is given by $0 = 1728$. Conversely, if the characteristic of K is 3 we also have $0 = 1728$ and can use E'' to argue the other way round. □

2.3 The invariant differential

At last we want to discuss the invariant differential of a Weierstrass equation.

Lemma 2.6. *Let E be an elliptic curve. Then the order of $x \in K(E)$ at infinity is -2 and the order of $y \in K(E)$ at infinity is -3.*

Proof. We only deduce the order of x at infinity as the other order can be obtained analogously. The monomial x is associated to the morphism $\phi : E \to \mathbb{P}^1$ that maps $[x : y : 1]$ to $[x : 1]$ by the correspondence $K(E) \cup \{\infty\} \leftrightarrow \{\psi : E \to \mathbb{P}^1 \mid \psi \text{ map defined over } K\}$ we explained earlier in this seminar. First we calculate the degree of ϕ as

$$\begin{aligned} \deg(\phi) &= [K(E) : \phi^* K(\mathbb{P}^1)] \\ &= [\mathrm{Quot}(K[x,y]/(f(x,y)) : K(x)] \\ &= [K(x)[y]/(y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6) : K(x)] \\ &= 2. \end{aligned}$$

Next by the formula $\deg(\phi) = \sum_{P \in \phi^{-1}(\infty)} e_\phi(P)$ we can deduce that O is mapped to ∞ and $e_\phi(O) = 2$ holds since $\phi^{-1}(\infty)$ contains at most the point O. If we now compare the integer associated to the divisor (O) on the left and right side of

$$\sum_{P \in E} \mathrm{ord}_P(\phi)(P) = \mathrm{div}(\phi) = \phi^*((0) - (\infty)) = \sum_{P \in \phi^{-1}(0)} e_\phi(P)(P) - \sum_{P \in \phi^{-1}(\infty)} e_\phi(P)(P)$$

we finally obtain $\mathrm{ord}_O(x) = \mathrm{ord}_O(\phi) = -2$. □

Proposition 2.7. *Let E be an elliptic curve. Then the invariant differential ω associated to a Weierstrass equation for E is holomorphic and nonvanishing. In particular* $\mathrm{div}(\omega) = 0$ *holds.*

Proof. First we consider $P = (x_0, y_0) \in E$. Since we know

$$M_P = \langle x - x_0, y - y_0 \rangle_{\overline{K}} \quad \text{and} \quad \dim_{\overline{K}} M_P/M_P^2 = 1$$

either $x - x_0$ or $y - y_0$ has to be a uniformizer at P. Without loss of generalization we suppose $\mathrm{ord}_P(x - x_0) = 1$ as we can proceed in the same way otherwise. Using the definition and the fact that f_y^{-1} does not vanish at P we obtain

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P \frac{d(x - x_0)}{f_y(x, y)} = \mathrm{ord}_P(f_y^{-1}) \leq 0.^4$$

Let $\mathrm{ord}_P(\omega)< 0$ or equally $\mathrm{ord}_P(f_y)> 0$ which yields $f_y(P) = 0$. By applying a formula we learned in the previous talk we can estimate

$$\mathrm{ord}_P(\omega) = \mathrm{ord}_P \frac{d(y - y_0)}{f_x(x, y)} \geq \mathrm{ord}_P(f_x^{-1}) + \mathrm{ord}_P(y - y_0) - 1 \geq \mathrm{ord}_P(f_x^{-1})$$

and in total we get $\mathrm{ord}_P(f_x)> 0$ which implies $f_x(P) = 0$. This is a contradiction as E is smooth so both partial derivatives can not vanish at P. Hence the order of ω at P has to be zero.

At last we have to consider the point at infinity. For that we fix a uniformizer t at O. In 2.6 we saw $\mathrm{ord}_O(x) = -2$ and $\mathrm{ord}_O(y) = -3$ and thus we can write $x = t^{-2}g$ and $y = t^{-3}h$ for functions $g, h \in \overline{K}(E)$ satisfying $g(O), h(O) \notin \{0, \infty\}$. Now we compute

$$\omega = \frac{dx}{f_y(x, y)} = \frac{-2t^{-3}g + t^{-2}g'}{2t^{-3}h + a_1 t^{-2} g + a_3} dt = \frac{-2g + tg'}{2h + a_1 tg + a_3 t^3} dt$$

where $g' \in \overline{K}(E)$ denotes the uniquely determined functions with $dg = g'dt$. In particular we proofed g' to be regular at O as well earlier in this seminar. Hence if $\mathrm{char}(K) \neq 2$ we can further compute

$$\mathrm{ord}_O(\omega) = \mathrm{ord}_O \frac{-2g + tg'}{2h + a_1 tg + a_3 t^3} = 0$$

In the case $\mathrm{char}(K) = 2$ we can use the representation $\omega = dy/f_x(x, y)$ and continue equally. □

[4] by f_x and f_y we mean the partial derivative of f with respect to x and y