## 1.11 26/07/01 - Weierstrass Equations III and the $j$-Invariant

Today, I want to do a few things. Firstly, I want to start by saying something I haven't yet explicitly, but which has been implicit in what we are doing.

Let $K$ be a field and $E \subset \mathbb{P}^2_K$ be an elliptic curve in Weierstrass form (1.9.2). Since $\Delta \neq 0$, the result of 1.9.9 tells us that $E$ is a smooth cubic curve. Equipping it with the point $\mathscr{O} = [0:1:0] \in E(K)$ at infinity, we can then apply 1.7.7 to get that the $\oplus$ operation on $E(K)$ defined there makes $E(K)$ into an abelian group with identity element $\mathscr{O}$. Let's summarize this in

**Proposition 1.11.1.** Let $K$ be a field, $E \subset \mathbb{P}^2_K$ be an elliptic curve with $\mathscr{O} = [0:1:0] \in E(K)$. Then the operation $\oplus : E(K) \times E(K) \to E(K)$ given by $(P, Q) \mapsto P \oplus Q := \mathscr{O} * (P * Q)$ makes $E(K)$ into an abelian group with identity $\mathscr{O}$. If $L/K$ is any field extension, then the inclusion $E(K) \subset E(L)$ makes $E(K)$ a subgroup of $E(L)$.

Henceforth, we will drop the notation $\oplus$ altogether, and simply refer to the group law using the usual $+$. In particular, we will write $P + Q$ for what we called $P \oplus Q$, and $nP$ for $P + \cdots + P$, where the sum has $n$ terms, for any $n \in \mathbb{Z}_{\geq 0}$. Finally, since an admissible change of coordinates is a linear transformation, it preserves the group law $+$, showing

**Proposition 1.11.2.** Let $K$ be a field, and $E$ and $E'$ elliptic curves in Weierstrass form over $K$. An admissible change of coordinates transforming $E$ to $E'$ yields a group isomorphism $E(K) \to E'(K)$, or indeed $E(L) \to E(L')$ for any field extension $L/K$.

We will use the notation $E \cong_K E'$ to express that two curves are related by an admissible change of coordinates over $K$. (Note that this notion depends on $K$; see 1.11.9.) The above proposition is just saying that if $E \cong_K E'$, then $E(K) \cong E'(K)$ as abelian groups (sometimes denoted $E(K) \cong_{\mathsf{Ab}} E'(K)$.)

Let's see what the group operation $+$ means concretely for two points $P, Q \in E(K)$ in the affine patch $Z \neq 0$, so points on the affine curve given by $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. We draw the line $L_{PQ}$ joining $P$ and $Q$ and take its third point of intersection with $E$, which is $P * Q$. Either $P * Q = \mathscr{O}$ (this happens iff $L_{PQ}$ is vertical), or $P * Q$ lies in this affine patch. If it's the former, then because $\mathscr{O}$ is an inflection point, we get that $P + Q = \mathscr{O}$, i.e., $P = -Q$. If it's the latter, then we draw the line joining $P * Q$ and $\mathscr{O}$, which in this case is just the vertical line through $P * Q$, and take its other intersection point with $E$; this is $P + Q$. Finally, if $P = Q$, then $L_{PQ}$ should be taken to mean the tangent line $\mathrm{T}_P E$ as usual. The figure 1.8.4 illustrates this procedure for the elliptic curve $E : y^2 = x(x+1)(x+4)$ over $K = \mathbb{Q}$ with the points $P = (-4, 0)$ and $Q = (-2, 2)$, where $P * Q = (2, 6)$ and so $P + Q = (2, -6)$.

### 1.11.A Automorphism Groups

We saw last time that an admissible change of coordinates over a field $K$ is given by specifying a quadruple $(u; r, s, t)$, where $u \in K^\times$ and $r, s, t \in K$, with the transformation corresponding to the matrix

$$\begin{bmatrix} u^2 & 0 & r \\ u^2 s & u^3 & t \\ 0 & 0 & 1 \end{bmatrix}. \tag{1.11.3}$$

The set of all such transformations forms a subgroup of $\mathrm{PGL}_3(K)$, which as far as I know doesn't have a standard name, so I'm just going to call it $G(K)$.

**Exercise 1.11.4.** As a set, $G(K) = \{(u; r, s, t) : u \in K^\times, r, s, t \in K\}$. What is the group operation on $G(K)$ corresponding to matrix multiplication when $(u; r, s, t)$ corresponds to the matrix 1.11.3? Fill in the blanks in $(u; r, s, t) \circ (u'; r', s', t') = (uu'; \dots)$.

An admissible change of coordinates takes on elliptic curve $E'$ into another $E$, but nothing is stopping us from taking $E = E'$, in which case an admissible change of coordinates corresponds to a symmetry of the elliptic curve $E$. Such an admissible change of coordinates is called an *automorphism* of

$E$, and the subgroup of $G(K)$ consisting of all such $(u; r, s, t)$ fixing $E$ is called the *automorphism group of $E$ over $K$*, denoted $\mathrm{Aut}_K(E)$ (or more precisely $\mathrm{Aut}_K(E, \mathscr{O})$, but let's not worry too much about that). This depends on $K$ in general.

**Example 1.11.5.** Let $K = \mathbb{Q}$ and $E : y^2 = x^3 + 1$. Consider the following admissible changes of coordinates:

(a) the transformation $(x, y) = (x', -y')$ corresponding to $(u; r, s, t) = (-1; 0, 0, 0)$, and
(b) the transformation $(x, y) = (\omega x', y')$ corresponding to $(u; r, s, t) = (\omega^2; 0, 0, 0)$.

Here $\omega$ denotes a primitive cube root of unity. The first transformation is defined over $\mathbb{Q}$ and expresses a symmetry $E(\mathbb{Q}) \to E(\mathbb{Q})$, i.e., belongs to $\mathrm{Aut}_{\mathbb{Q}}(E)$. The second transformation is *not* defined over $\mathbb{Q}$, but is defined over $\Omega = \overline{\mathbb{Q}}$ or $\Omega = \mathbb{C}$ (or even the number field $L = \mathbb{Q}[\omega] = \mathbb{Q}[\sqrt{-3}]$), and expresses a symmetry $E(\Omega) \to E(\Omega)$, i.e., belongs to $\mathrm{Aut}_{\Omega}(E)$.

In general we have a diagram of subgroups of the form

$$\begin{array}{ccccc} \mathrm{Aut}_K(E) & \hookrightarrow & G(K) & \hookrightarrow & \mathrm{PGL}_3(K) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Aut}_{\overline{K}}(E) & \hookrightarrow & G(\overline{K}) & \hookrightarrow & \mathrm{PGL}_3(\overline{K}). \end{array}$$

The group $\mathrm{Aut}_{\overline{K}}(E)$ is sometimes called the *geometric* automorphism group of the elliptic curve $E$, but we won't use this terminology much. You are invited to explore some more automorphism groups (and geometric automorphism groups) of elliptic curves over some finite fields in 2.3.3.

## 1.11.B Admissible Changes For Curves in Short Weierstrass Form

Suppose now that the field $K$ has $\mathrm{ch}\, K \neq 2$, and the elliptic curves $E$ and $E'$ are in the short Weierstrass form

$$E : y^2 = x^3 + ax^2 + bx + c \text{ and } E' : (y')^2 = (x')^3 + a'(x')^2 + b'x' + c'.$$

Suppose we have an admissible change of coordinates $(x, y) = (u^2x' + r, u^3y' + u^2sx' + t)$ transforming $E$ into $E'$. Then a simple inspection shows that we must in fact have $s = t = 0$. In other words, any admissible change of coordinates taking a curve in short Weierstrass form to another of the same form must look like $(x, y) = (u^2x' + r, u^3y')$. That's a much easier form to work with.

Similarly, suppose now that $\mathrm{ch}\, K \neq 2, 3$, and that $a = a' = 0$ as well. Then a very similar argument to the one above tells us that in fact $r = 0$ as well, i.e., the transformation looks like $(x, y) = (u^2x', u^3y')$. Therefore, if for $b, c \in K$ such that $4b^3 + 27c^2 \neq 0$, we let $E_{b,c}$ denote the elliptic curve

$$E_{b,c} : y^2 = x^3 + bx + c,$$

then for any allowable $b, c, b', c'$, we have that $E_{,b,c} \cong_K E_{b',c'}$ iff there is a $u \in K^\times$ such that $(b, c) = (u^4b', u^6c')$.

**Example 1.11.6.** Let $K = \mathbb{C}$ (or indeed any field of characterstic not 2 or 3). The elliptic curves $E : y^2 = x^3 + x$ and $E' : y^2 = x^3 + 1$ over $K$ are not isomorphic (over $K$, or indeed any field containing $K$).

This leaves the question of whether two curves can be non-isomorphic over $K$ but isomorphic over some bigger field containing $K$. We'll answer this question in the next section (1.11.9).

**Remark 1.11.7.** When $\mathrm{ch}\, K = 3$, a careful version of the above discussion implies that whether or not $a = 0$ in the short Weierstrass form is a (boolean) invariant of the curve, i.e., does not depend on the choice of coordinates. We will revisit this idea soon.

## 1.11.C The $j$-Invariant and the Isomorphism Classification of Elliptic Curves

The previous discussion suggests that the quantity $b^3/c^2$ is an invariant of the isomorphism type of $E_{b,c}$. Actually, this is slightly imprecise since $c$ could be zero without $b$ being zero, causing this "invariant" to

be undefined. Is there a linear combination of $b^3$ and $c^2$ we know is never going to vanish, and which we could use as the denominator instead? Of course there is, and it is $\Delta = -16(4b^3 + 27c^2)$. This leads us to

**Definition 1.11.8** (The $j$-Invariant). Let $K$ be a field of characteristic other than 2 or 3. For any $b, c \in K$ with $\Delta = -16(4b^3 + 27c^2) \neq 0$, we let the $j$-invariant of the curve $E_{b,c}$ be

$$j(E_{b,c}) := \frac{(-48b)^3}{\Delta}.$$

At this point, we have shown that if $b, c, b', c' \in K$ are such that $\Delta\Delta' \neq 0$, and if $E_{b,c} \cong_K E_{b',c'}$, then $j(E_{b,c}) = j(E_{b',c'})$. Does the converse hold? Well, suppose that $j(E_{b,c}) = j(E_{b',c'})$; we're trying to show that there is a $u \in K^\times$ such that $(b, c) = (u^4 b', u^6 c')$. Let's split into a few cases.

(a) First suppose that $bc \neq 0$. Then $j(E_{b,c}) = j(E_{b',c'})$ forces $b'c' \neq 0$ as well (check!). From the equality $b^3/c^2 = (b')^3/(c')^2$, it follows that if let $v := (b'c)/(bc') \in K^\times$, then $(b, c) = (v^2 b', v^3 c')$. Now if there is a square root $u$ of $v$ in $K$, then this $u$ works and we are done. Therefore, we are certainly done when we can take square roots of elements in $K$, which happens for instance, if $K$ is algebraically closed. In general, however, we may not be able to do this, and this would give us an example of two curves that are isomorphic over $\overline{K}$ but not $K$. Such curves are called *twists* of each other. (In this special case of $bc \neq 0$, they are called *quadratic twists*.) For an explicit example, see 1.11.9(a).

(b) Next, suppose that $b \neq 0$ but $c = 0$, which happens iff $j(E_{b,c}) = 1728$ (check!). Then $j(E_{b',c'}) = j(E_{b,c}) = 1728$ forces $b' \neq 0$ and $c = 0$. Now $E_{b,0} \cong_K E_{b',0}$ iff there is a $u \in K^\times$ such that $b = u^4 b'$. Again, if a fourth root of $b/b'$ exists in $K$ (e.g., $K$ algebraically closed), we are done; else we get curves which are *quartic twists* of each other (in general)–see 1.11.9(b).

(c) Finally, suppose that $b = 0$ but $c \neq 0$, which happens iff $j(E_{b,c}) = 0$ (clear!). Then $j(E_{b',c'}) = j(E_{b,c})$ forces $b' = 0$ and $c' \neq 0$. Now $E_{0,c} \cong_K E_{0,c'}$ iff there is a $u \in K^\times$ such that $c = u^6 c'$. Again, if a sixth root of $c/c'$ exists in $K$ (e.g., $K$ algebraically closed), we are done; else, we get curves which are *sextic twists* of each other (in general)–see 1.11.9(c).

**Example 1.11.9** (Twists). Let $K = \mathbb{Q}$ for simplicity.

(a) (Quadratic Twists) The elliptic curves $E : y^2 = x^3 + x + 1$ and $E' : (y')^2 = (x')^3 + 4x' + 8$ are quadratic twists of each other: they are isomorphic over $\overline{K} = \overline{\mathbb{Q}}$ (or indeed over the smaller subfield $L = \mathbb{Q}[\sqrt{2}]$) by the change of coordinates $(x, y) = (2^{-1}x', 2^{-3/2}y')$, but they are *not* isomorphic over $\mathbb{Q}$, since there does not exist a $u \in \mathbb{Q}^\times$ such that $(1, 1) = (4u^4, 8u^6)$. Note that both curves $E$ and $E'$ have the same $j$-invariant, namely $j(E) = j(E') = 2^8 3^3 31^{-1}$.

(b) (Quartic Twists) The elliptic curves $E_i : y^2 = x^3 + 2^i x$ for $i = 0, 1, 2, 3$ are pairwise isomorphic over $\overline{K} = \overline{\mathbb{Q}}$ (or indeed over $L = \mathbb{Q}[2^{1/4}]$), but they are pairwise non-isomorphic over $K = \mathbb{Q}$. Note that all the curves $E_i$ have the same $j$-invariant $j(E_i) = 1728$. For each $i = 0, 1, 2, 3$ (considered cyclically), the curves $E_i$ and $E_{i+1}$ are quartic twists of each other. (Note that the curve $E_4 : y^2 = x^3 + 16x$ *is* isomorphic to $E_0 : y^2 = x^3 + x$ over $K = \mathbb{Q}$! The curves $E_0 : y^2 = x^3 + x$ and $E_2 : y^2 = x^3 + 4x$ are technically *quadratic* twists of each other, since they are isomorphic over $L = \mathbb{Q}[\sqrt{2}]$ (check!); in general, the degree of a twist is the smallest degree of the field extension of $K$ over which the resulting curves are truly isomorphic.)

(c) (Sextic Twists) The elliptic curves $E_i : y^2 = x^3 + 2^i$ for $i = 0, 1, \ldots, 5$ are pairwise isomorphic over $\overline{K} = \overline{\mathbb{Q}}$ (or indeed over $L = \mathbb{Q}[2^{1/6}]$), but they are pairwise non-isomorphic over $K = \mathbb{Q}$. Note that all the curves $E_i$ have the same $j$-invariant $j(E_i) = 0$. For each $i = 0, 1, \ldots, 5$ (considered cyclically), the curves $E_i$ and $E_{i+1}$ are sextic twists of each other. Again, $E_0$ and $E_6$ are isomorphic over $\mathbb{Q}$, the curves $E_0$ and $E_3$ are technically quadratic twists of each other, and $E_0, E_2, E_4$ and $E_1, E_3, E_5$ are triples of *cubic twists*.

We have proven

**Theorem 1.11.10.** Let $K$ be a field with $\operatorname{ch} K \neq 2, 3$. Let $b, c, b', c' \in K$ be such that $\Delta\Delta' \neq 0$, and let $E_{b,c}$ and $E_{b',c'}$ denote the corresponding elliptic curves. If $E_{b,c} \cong_K E_{b',c'}$, then $j(E_{b,c}) = j(E_{b',c'})$. The converse holds if $K$ is algebraically closed, but not in general (1.11.9).

This is really cool: one number determines whether or not two curves are isomorphic! Suppose I hand you two elliptic curves $E$ and $E'$ over $\mathbb{C}$, and ask you to tell me whether they are isomorphic over $\mathbb{C}$, all you have to do is compute their $j$-invariants and check if they agree. If they do, these are isomorphic; if they don't, they aren't. This basically gives us a complete understanding of isomorphism classes of elliptic curves over algebraically closed fields of characteristic other than 2 or 3. (It still leaves the question of exactly which $j$-invariants are possible; this I leave for an exercise on the Exercise Sheet for next week.)

While we are here, we might as well prove

**Theorem 1.11.11.** Let $K$ be a field with $\operatorname{ch} K \neq 2, 3$, and let $\overline{K}$ denote an algebraic closure of $K$. Let $E$ be an elliptic curve over $K$. The size of the geometric automorphism group of $E$ is given by

$$\#\operatorname{Aut}_{\overline{K}}(E) = \begin{cases} 2 & j \neq 0, 1728, \\ 4 & j = 1728, \\ 6 & j = 0. \end{cases}$$

*Proof.* Since any curve $E$ can be put[5] into the shortest Weierstrass form $y^2 = x^3 + bx + c$, and this transformation only changes the (geometric) automorphism group up to isomorphism, we might as well assume that $E$ is in this form. A geometric automorphism then corresponds to a $u \in \overline{K}^\times$ such that $(b, c) = (u^4 b, u^6 c)$. Let's split into the same cases as before:

(a) If $bc \neq 0$, which happens iff $j \neq 0, 1728$, then such a $u$ must satisfy $u^4 = u^6 = 1$ and hence $u^2 = 1$, which implies $u \in \{\pm 1\}$. This gives us precisely two automorphisms $(x, y) \mapsto (x, \pm y)$.
(b) If $b \neq 0$ but $c = 0$, which happens iff $j = 1728$, then such a $u$ must satisfy $u^4 = 1$, which gives us four automorphisms corresponding to $u = \pm 1, \pm i$.
(c) Finally, if $b = 0$ and $c \neq 0$, which happens iff $j = 0$, then such a $u$ must satisfy $u^6 = 1$, which gives us six automorphisms corresponding to $u = \pm\omega^k$ for $k = 0, 1, 2$, where $\omega$ is a primitive cube root of unity.

■

Note that the statement of 1.11.11 really needs geometric automorphism groups to be true.

**Example 1.11.12.** Let $K = \mathbb{Q}$. The curve $E : y^2 = x^3 + x$ has $j(E) = 1728$ and geometric automorphism group $\operatorname{Aut}_{\overline{K}}(E)$ of size 4. In fact, these geometric automorphisms are given explicitly by $(x, y) \mapsto (x, \pm y)$ and $(x, y) \mapsto (-x, \pm iy)$. Of these, only the first two are defined over $\mathbb{Q}$, and hence $\operatorname{Aut}_{\mathbb{Q}}(E) \cong \mathbb{Z}/2$ of size 2.

In fact, a slight strengthening of the above argument (left to the readers) shows easily that the geometric automorphism groups when $j = 1728$ and $j = 0$ are necessarily isomorphic to $\mathbb{Z}/4$ and $\mathbb{Z}/6$.

**Exercise 1.11.13.** Check this!

## 1.11.D The Case of Characteristics 2 and 3

So far, we have stuck with the case of characteristics other than 2 or 3. The story in these characteristics is very similar. In general, we have

**Definition 1.11.14.** Let $K$ be any field (of any characteristic!), and let $a_1, \ldots, a_6 \in K$ be as usual, such that $\Delta \neq 0$, so that the usual equation (1.9.10) defines an elliptic curve $E$ over $K$. In this case, we define the quantity $c_4$ associated to the elliptic curve $E$ by

$$c_4 := a_1^4 + 8a_1^2 a_2 - 24 a_1 a_3 + 16 a_2^2 - 48 a_4,$$

[5] Technically, we haven't even defined the $j$-invariant for curves not in the shortest Weierstrass form. We will rectify this below (1.11.14); see also 1.11.16. For now, you can take this to be a statement about curves in the shortest Weierstrass form.

and the $j$-invariant of $E$ to be

$$j(E) := \frac{c_4^3}{\Delta}.$$

Note how this specializes to the definition 1.11.8 when $a_1 = a_2 = a_3 = 0$. Note also that $c_4$ is homogeneous of degree 4 in the $a_i$ with the usual weights, and actually similarly to $\Delta$ (1.10.3), transforms very cleanly under admissible changes of coordinates: namely via

$$u^4 c_4' = c_4. \tag{1.11.15}$$

(Again, don't take this on faith–you can check it for yourself!) These two equations (1.11.15 and 1.10.3) combined imply that $j(E)$ is actually invariant under admissible changes of coordinates, proving one half of

**Theorem 1.11.16.** Let $K$ be any field (of any characteristic). Let $a_i, a_i' \in K$ for $i = 1, 2, 3, 4, 6$ be such that $\Delta\Delta' \neq 0$, and let $E$ and $E'$ denote the corresponding elliptic curves. If $E \cong_K E'$, then $j(E) = j(E')$. The converse holds if $K$ is algebraically closed, but not in general.

To prove this theorem, it only remains to show that if $j(E) = j(E')$, then there is an admissible change of coordinates over $\overline{K}$ taking $E$ to $E'$. The proof of this statement is very similar to what we did above in $\operatorname{ch} K \neq 2, 3$, and again when the characteristic is 2 or 3, you have to treat the cases $j = 0 = 1728$ and $j \neq 0$ separately. In characteristic 2, you also see *octic twists* showing up. I won't bother to type out the details; the interested readers can either supply the proof themselves, or can they can find it in [8, Proposition III.1.4(b)]. See also [14] for more on twisting in characteristics 2 and 3. Finally, analogously to 1.11.11, in $\operatorname{ch} K = 2, 3$ a curve with $j \neq 0$ still has geometric automorphism group $\mathbb{Z}/2$; when $\operatorname{ch} K = 3$ and $j = 0 = 1728$, you get the geometric automorphism group $\mathrm{Dic}_3$ of size 12, and when $\operatorname{ch} K = 2$ and $j = 0 = 1728$, you get the geometric automorphism group $\mathrm{SL}_2(\mathbb{F}_3) \cong Q_8 \rtimes C_3$ of size 24; see [8, Theorem III.10.1 and Exercise A.1]. All I want to emphasize is that there is nothing particularly deep going on here, and the dedicated reader(s) could work these ideas out for themselves.