1.10 26/06/30 - Weierstrass Equations II and Sage

In the first part of class today, I want to talk a little more about Weierstrass equations and changes of coordinates, and then focus on using Sage for the rest of the lecture.

1.10.A One More Thing About the Elliptic Discriminant

For simplicity now, let us focus on the case of a field K of characteristic not two. We saw last time that any elliptic curve E over K can be put into the shorter Weierstrass form

$$y^2 = x^3 + ax^2 + bx + c$$

for some a, b, c. For this to define a nonsingular curve, we need the discriminant Δ, given by the formula

$$\Delta = -16(4a^3c - a^2b^2 - 18abc + 4b^3 + 27c^2),$$

to be nonzero. In this setting of $\operatorname{ch} K \neq 2$, let us review where this formula comes from. Let $f(x) := x^3 + ax^2 + bx + c \in K[x]$, so E is defined by $y^2 = f(x)$. The singular points of E are cut out by the vanishing locus of $y^2 - f(x)$, and its partial derivatives $2y$ and $-f'(x)$. Since we are assuming $\operatorname{ch} K \neq 2$, if $2y = 0$, then $y = 0$. Therefore, having verified above that the point at infinity is not a singularity for curves in Weierstrass form, we see that E has a singular point iff the polynomials $f(x)$ and $f'(x)$ share a common root. By what you know from the Ross sets, this happens iff a polynomial $\operatorname{disc}(f)$ in the coefficients a, b, c of f vanishes, and indeed we have that

$$\Delta = 16 \cdot \operatorname{disc}(f).$$

This is essentially where Δ comes from, modulo some more care to accommodate all characteristics at once. The 16 is a reminder that the above discussion only works when $\operatorname{ch} K \neq 2$!

1.10.B Admissible Changes of Coordinates

Example 1.10.1. For simplicity, let's work over $K = \mathbb{Q}$.

(a) Consider the two elliptic curves

$$E : y^2 = x(x+1)(x+4) \text{ and } E' : (y')^2 = (x'-1)((x')^2 - 4).$$

Get Desmos to draw plots of both of these curves. What do you notice? Indeed, these curves are related by the change of coordinates $(x, y) = (x' - 2, y')$.

(b) Consider the two elliptic curves

$$E : y^2 + y = x^3 - x \text{ and } E' : (y')^2 = (x')^3 - 16x' + 16.$$

Repeating the above procedure, we see that E and E' are related by the change of coordinates

$$(x, y) = \left(\frac{1}{4}x', \frac{1}{8}y' - \frac{1}{2}\right).$$

At this point, I want to go back to working over general K (of any characteristic). We need a general procedure to understand when two elliptic curves are related by a simple change of coordinates. Suppose that K is a field, and that $E, E' \subset \mathbb{P}^2_K$ are elliptic curves in Weierstrass form with coefficients a_i and a_i' respectively. Suppose that $\varphi : \mathbb{P}^2_K \to \mathbb{P}^2_K$ is a linear change of coordinates (where we think of the first $\mathbb{P}^2_K$ has having coordinates X', Y', Z', and the second one as having coordinates X, Y, Z), taking E' to E and $\mathscr{O}' \in E(K)$ to $\mathscr{O} \in E'(K)$. Then by 2.2.6(b), φ takes $\mathbb{T}_{\mathscr{O}'}E' = \mathbb{V}(Z')$ to $\mathbb{T}_{\mathscr{O}}(E) = \mathbb{V}(Z)$, and fixes the point $[0:1:0]$. It follows from 2.2.2 that φ corresponds to a matrix in $\mathrm{PGL}_3(K)$ of the form

$$\begin{bmatrix} p & 0 & r \\ n & q & t \\ 0 & 0 & 1 \end{bmatrix}$$

for some $n, p, q, r, t \in K$ with $pq \neq 0$. In other words, the change of coordinates is given by $(X, Y, Z) = (pX' + rZ', nX' + qY' + tZ', Z')$, or in affine coordinates $(x, y) = (px' + r, nx' + qy' + t)$. Using this coordinate change to transform the equation of E into that of E', we get immediately by comparing the leading terms in a Weierstrass equation that $q^2 = p^3$. In particular, $(p, q) = (u^2, u^3)$ for some $u \in K^\times$, namely $u := q/p$. Finally, if we let $s := nu^{-2}$, then we end up with the formula

$$(x, y) = (u^2x' + r, u^3y' + u^2sx' + t) \tag{1.10.2}$$

for the change of coordinates. A change of coordinates as in 1.10.2 is said to be an *admissible change of coordinates*. Such a change of coordinates related the coefficients a_i and a_i' in a very particular way; for instance, $ua_1' = a_1 + 2s$.

Exercise 1.10.3. Check this: check that under 1.10.2, the coefficients a_1 and a_1' are related by $ua_1' = a_1 + 2s$. In particular, if $\operatorname{ch} K = 2$, then whether or not $a_1 = 0$ for a particular elliptic curve E/K is a (boolean) invariant of the curve E, invariant under admissible changes of coordinates (and hence by 1.10.6 under isomorphisms). We will revisit this idea later.

Similarly, you can work out for yourself how the rest of the coefficients a_i and a_i' are related (in terms of (u, r, s, t)) (or you can find it at [8, Table 3.1]). I want to highlight two things: that if $r = s = t = 0$, the transformation is simply $u^i a_i' = a_i$ for all $i = 1, 2, 3, 4, 6$ (c.f. 1.9.15(b)), and that the discriminants Δ and Δ' of E and E' are miraculously related by the very simple formula

$$u^{12}\Delta' = \Delta. \tag{1.10.4}$$

(You need not take my word for it, and can verify this for yourselves.) In particular, if $u = 1$, then $\Delta' = \Delta$. In particular, all the changes we did to transform curves into shorter Weierstrass forms when $\operatorname{ch} K \neq 2, 3$, which involved things like completing squares and depressing cubics, did not change Δ (c.f. 1.9.20). We summarize this as:

Proposition 1.10.5. Let K be a field. Two elliptic curves E and E' over K in Weierstrass form are the same iff they are related by an admissible change of coordinates of the form 1.10.2.

Unimportant Remark 1.10.6. Technically speaking, we haven't fully proved 1.10.5; the giveaway is the usage of the imprecise terminology of being "the same". It can be shown that any isomorphism $E \to E'$ of (abstract) elliptic curves in the sense of 1.9.1 taking $\mathscr{O}$ to $\mathscr{O}'$ is induced by an admissible change of coordinates when E and E' are put in Weierstrass form. This again uses the Riemann-Roch Theorem. We will not need this fact, and we won't prove it. The interested reader can find a proof at [8, Proposition III.3.1(b)].

1.10.C Working with Sage

The rest of the lecture was spent discussing how to work with Sage. We learned how to work with various fields in Sage, how to construct elliptic curves over various fields and study their properties, and how to work with explicit admissible changes of coordinates. This is a pain to typeset (well) in LaTeX, so I am not going to do this here, but a version of this discussion can be found in [13, Appendix A], to which I refer the interested reader.