Math 145. Weierstrass equations

Let C be an irreducible smooth projective curve of genus 1 over an algebraically closed field k. Let $\infty \in E$ be a choice of "base point", so as was explained in class by Riemann-Roch we have $\ell(2\infty) = 2$, $\ell(3\infty) = 3$, and we can choose bases $\{1, x\}$ of $L(2\infty)$ and $\{1, x, y\}$ of $L(3\infty)$. Here x is unique up to $x \rightsquigarrow ax + b$ for $a \in k^\times$, $b \in k$ and y is unique up to $y \rightsquigarrow uy + vx + w$ for $u \in k^\times$, $v, w \in k$. Upon rescaling x and y by $k^\times$ we can even assume, for a fixed choice of uniformizer t at ∞, that $x = 1/t^2 + \ldots$, $y = 1/t^3 + \ldots$ (i.e., $t^2x, t^3y \in \mathscr{O}_{C,\infty}^\times$ have value 1 at ∞). Note that (for fixed t) this makes x unique up to adding a constant and makes y unique up to adding a linear combination of 1 and x. These normalizations ensure that $y^2 - x^3 \in L(5\infty)$, from which we get a Weierstrass equation

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

for some $a_i \in k$.

We therefore have a map $(x, y) : C - \{\infty\} \to \mathbf{A}^2 \hookrightarrow \mathbf{P}^2$ which lands inside of the zero locus of the above Weierstrass equation. Thus, the unique extended map $[x, y, 1] : C \to \mathbf{P}^2$ must factor through

$$E = \underline{Z}(Y^2Z + a_1XYZ + a_3YZ - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3) \hookrightarrow \mathbf{P}^2,$$

with ∞ mapping to the unique point $[0, 1, 0] \in E \cap \{Z = 0\}$ (indeed, since y has a triple pole at ∞ and x has a double pole at ∞ by the very construction of "extended maps" from smooth curves to projective spaces we see that $[x, y, 1]$ extends near ∞ by scaling through by the cube of a uniformizer at ∞, yielding the image point $[0, 1, 0]$ for ∞ under the extended map). The purpose of this handout is to prove, without tedious calculations, the following fundamental fact.

Lemma 0.1. *The above homogenous cubic $Y^2Z + a_1XYZ + \ldots$ is irreducible and the corresponding irreducible degree 3 curve E in $\mathbf{P}^2$ is smooth. Moreover, the factorized map $C \to E$ is an isomorphism.*

Note that by the homework, any smooth irreducible cubic curve in $\mathbf{P}^2$ is automatically of genus

$$(3 - 1)(3 - 2)/2 = 1,$$

so the Riemann-Roch theorem ensures the remarkable converse: *every* abstract genus 1 curve necessarily arises in this way. But the abstract point of view is better, because it shows that in fact *any* point on such a curve can be realized as the "point at infinity" for a suitable closed immersion of the curve into $\mathbf{P}^2$ as a cubic (note that the choice of $\infty \in C$ above was completely arbitrary). Consider the case away from characteristic 2. Then the presence of $1/2 \in k$ permits us to "complete the square" to find $r, s \in k$ so that $(y + rx + s)^2 = y^2 + a_1xy + a_3y + \text{blah}$, so by replacing y with $y + rx + s$ we can put ourselves in the case where $a_1 = a_3 = 0$; note that this step causes $a_2, a_4, a_6 \in k$ to change. Once we know the lemma, our plane cubic curve must be irreducible and smooth, so the (revised and renamed) affine cubic part $x^3 + a_2x^2 + a_4x$ *must* have distinct roots.

In particular, a_2, a_4 cannot both vanish. Thus, we can find $w \in k^\times$ satisfying $1 + a_2w^2 + a_4w^4 = 0$. Then replacing y by $y' = w^3y$ and x by $x' = w^2x$ makes $y' = 1/t'^3 + \ldots$, $x' = 1/t'^2 + \ldots$ for the uniformizer $t' = w^{-1}t$ at ∞ and gives us a similar Weierstrass relation in which the cubic now has both 0 and 1 as roots. That is, we have our curve in *Legendre form*

$$y'^2 = x'(x' - 1)(x' - \lambda)$$

with necessarily $\lambda \neq 0, 1$ (why?). Thus, we see that the Legendre example in characteristic away from 2 captures *all* genus 1 curves (over an algebraically closed field). Of course, different values of $\lambda \in k - \{0, 1\}$ can give rise to isomorphic curves (even fixing ∞), but that is a story that would take us too far afield. One could also ask whether these is a replacement for the Legendre form for characteristic 2, but that is also not something we have the time to discuss.

If you look in Silverman's introductory book on elliptic curves you'll find a proof of the above lemma based on explicit computations of discriminants. We prefer to avoid any explicit computations and to rather let the geometry guide us (plus a little calculation).

Proof. Note that a priori we do not yet know that E is even irreducible. One can certainly write down plane cubic equations that are not irreducible, or irreducible and not smooth (e.g., $Y^2Z = X^3$), so we of course have to use that C is irreducible and smooth somewhere in the proof. We begin by analyzing the situation near $[0,1,0] \in E$. Dehomogenizing with respect to Y gives in $\mathbf{P}^2 \cap \{Z \neq 0\}$ the equation

$$z' + a_1x'z' + a_3z'^2 = x'^3 + a_2x'^2z' + a_4x'z'^2 + a_6z'^3$$

(with $x' = X/Y$, $z' = Z/Y$), so the presence of a linear term z' and vanishing constant term tells us that through $(x', z') = (0, 0)$ this polynomial has only 1 irreducible factor. That is, if the homogenous Weierstrass cubic were to factor non-trivially, only one factor would pass through [0,1,0] and this factor would have to appear with *multiplicity* 1. Let E_∞ be the zero locus of this unique irreducible factor, so E_∞ is an irreducible projective curve and is the unique irreducible component of E through $[0, 1, 0]$ (why?). Moreover, $E_\infty \hookrightarrow E$ is an irreducible projective curve, and from the multiplicity 1 condition we see that $E_\infty = E$ as sets if and only if the original Weierstrass equation is irreducible. Since the equation of E_∞ in terms of x' and z' has linear term z' and vanishing constant term, we see that E_∞ is smooth at $(x', z') = (0, 0)$ with x' a uniformizer.

Since E_∞ is an irreducible component of E, if E' denotes the (possibly empty) union of the other irreducible components of E we have that $E_\infty - E'$ is a non-empty open set in E. Under the map $C \to E$, the preimage of the $E_\infty - E'$ is non-empty (it contains ∞), so the preimage of E_∞ is a closed set in C which contains a non-empty open. But C is irreducible! Thus, we conclude that the map $C \to E$ must factor through a map $C \to E_\infty$ to the irreducible projective curve E_∞. We still don't know if E_∞ is smooth (or if it is all of E, which we have seen is equivalent to the irreducibility of the original Weierstrass equation). The map $C \to E_\infty$ is *non-constant*, since the preimage of $[0, 1, 0]$ is a single point ∞, as $C - \{\infty\}$ maps into $\mathbf{P}^2 - \{Z = 0\}$ (by construction). Being a map between irreducible curves, it must be dominant, so in particular we get a pullback map $k(E_\infty) \to k(C)$ over k. Under this map, $x' \mapsto x/y$, $z' \mapsto 1/y$ (*carefully check this*, motivated by the idea $x' = X/Y = (X/Z)/(Y/Z)$, $z' = Z/Y = 1/(Y/Z)$; note that E_∞ has an open neighborhood of ∞ on which the defining equation coincides with the equation defining E). But $x/y \in k(C)^\times$ has order $-2 - (-3) = 1$ at ∞, so we conclude that the map $C \to E_\infty$ between irreducible projective curves not only has ∞ as the *unique* point over $[0, 1, 0]$, but both points are smooth on the respective *irreducible* curves and a uniformizer at $[0, 1, 0]$ pulls back to a uniformizer at ∞.

Now consider a general situation where we have a non-constant map $f : C \to C'$ between irreducible projective curves, with C smooth and C' possibly singular, but assume that there is a smooth point $x' \in C'$ such that $f^{-1}(x') = \{x\}$ with ramification degree $e(x'|x) = 1$ (this makes sense, since the definition of ramification degree just requires smoothness at the two points under consideration). In such a situation, f is certainly non-constant, hence dominant, so by normality of C there is a unique factorization $C \to \widetilde{C'}$ through the normalization of C'. But C' is an irreducible *projective* curve, and in the handout on resolution of singularities for curves we saw that the normalization $\widetilde{C'}$ of an irreducible projective curve *is* automatically projective. Thus, $C \to \widetilde{C'}$ is a non-constant map between irreducible smooth projective curves, whence it is *finite*, and its degree can be computed as the sum of the ramification degrees in a single fiber. But $C \to C'$ has a unique point over a smooth point $x' \in C'$ and the normalization map $\widetilde{C'} \to C'$ is certainly an isomorphism over the (open) smooth locus, so we can view $x' \in \widetilde{C'}$ and so $C \to \widetilde{C'}$ has a unique point over x', with ramification degree 1 by hypothesis. Adding up ramification degrees in the fiber over $x' \in \widetilde{C'}$, the degree of $C \to \widetilde{C'}$ is 1. That is, this map between irreducible smooth projective curves is a birational isomorphism and hence an isomorphism.

To summarize, back in our original situation the map $C \to E_\infty$ *is* the normalization of the irreducible projective curve E_∞. Now suppose that the original Weierstrass equation were not irreducible, so the irreducible homogenous polynomial defining E_∞ has degree 1 or 2. But we know from an earlier homework that an irreducible curve in $\mathbf{P}^2$ of degree 1 or 2 is automatically smooth, and then in fact isomorphic to $\mathbf{P}^1$, hence of genus 0. In particular, it is its own normalization and thus the normalization C of E_∞ would be of genus 0. But it is of genus 1. Contradiction! Thus, we obtain the irreducibility of our original Weierstrass equation and so now write E rather than E_∞.

The remaining issue is to prove that the map $C \to E$ is an isomorphism. Note that since both are irreducible curves and the map is non-constant, it is at least dominant, so E is the closure of the image of $[x, y, 1] : C \to \mathbf{P}^2$. But as we just saw, the map $C \to E$ is the normalization map of the irreducible projective curve $E = E_\infty$, so as long as E is intrinsically smooth this map $C \to E$ will have to be an isomorphism. Suppose that E has a singularity at a point P. We have seen that $E = E_\infty$ is smooth at the unique point $[0, 1, 0]$ in $E \cap \{Z = 0\}$, so $Z(P) \neq 0$. Translating x and y by constants (which amounts to using a certain homogenous linear change of coordinates $[X, Y, Z] \mapsto [X - aZ, Y - bZ, Z]$ on $\mathbf{P}^2$ fixing $[0, 1, 0]$, and so may change the specific Weierstrass equation but is harmless for our purposes of proving that the abstract map $C \to \mathbf{P}^2$ is an isomorphism onto its the closure of its image), we may assume $P = [0, 0, 1]$. Then if we let f denote the dehomogenization of our *irreducible* Weierstrass cubic, we know that $f \in k[x, y]$ is *irreducible* (why?) and f has a singularity at $(x, y) = (0, 0)$ by hypothesis. Thus, $f(0, 0) = (\partial f/\partial x)(0, 0) = (\partial f/\partial y)(0, 0) = 0$. But from the Weierstrass equation these three values are respectively a_6, a_4, and a_3. In other words, in $\mathbf{P}^2 \cap \{Z \neq 0\}$ our irreducible curve is defined by an irreducible polynomial of the form

$$y^2 + a_1xy - a_2x^2 - x^3 = 0.$$

The homogenous quadratic term $y^2 + a_1xy - a_2x^2$ factors as $(y + \alpha_1 x)(y + \alpha_2 x)$ for some $\alpha_i \in k$, so upon replacing y by $y + \alpha_1 x$ (which we may do without harming any of the running hypotheses and standardizations) we may suppose our equation has the form

$$y(y + cx) = x^3,$$

with some $c \in k$. We claim that the normalization of such an affine curve is $\mathbf{A}^1$. Once this is shown, then the (irreducible projective smooth) normalization curve C of the irreducible projective curve E will contain $\mathbf{A}^1$ as a dense open and so will be birational, and hence isomorphic, to $\mathbf{P}^1$. But C does not have genus 0, so this would be a contradiction.

It remains to exhibit $\mathbf{A}^1$ as the normalization of the visibly *irreducible* affine curve $\underline{Z}(y(y+cx)-x^3) \subseteq \mathbf{A}^2$ for any $c \in k$. Being a little careful with characteristics 2 and 3, we see by direct calculation of partial derivatives that the visibly singular point (0,0) is the only singularity. When $c = 0$ then we have seen explicitly that $\mathbf{A}^1$ is the normalization, with the normalization map given by $t \mapsto (t^2, t^3)$. Thus, we may consider $c \neq 0$, in which case the singularity is an ordinary double point and so has distinct tangent directions. Rather than blindly compute integral closures explicitly, we realize that we know from our study of blow-ups with distinct tangent directions that blow-up at an ordinary double point resolves the singularity and so gives us the normalization. Thus, to compute the normalization we simply need to calculate the blow-up of this curve at (0,0); recall we did this in class in the case $c = 0$ and got two open affines, one $\mathbf{A}^1$ and the other chart inside of this. The same calculation adapts readily to the case $c \neq 0$ giving the same conclusion (whence the normalization is $\mathbf{A}^1$, as desired). Explicitly, this blow-up computation shows that the normalization map from $\mathbf{A}^1$ is given by $t \mapsto (t(t+c), t^2(t+c))$ for any $c \in k$, even $c = 0$ (so I could have just pulled this formula out of a hat rather than invoke the motivation via blow-ups, but that would be unnatural).

■