LOGICAL CLASSIFICATION OF CURVES

DAVID PIERCE

Contents

1. Ellipses and elliptic curves

An **ellipse** is given by an equation

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1.$$

In general, length along a curve from P to Q is given by $\int_P^Q\sqrt{\mathrm{d}\,x^2+\mathrm{d}\,y^2}$. For the ellipse, we compute

$$\frac{2x\,\mathrm{d}\,x}{a^2}+\frac{2y\,\mathrm{d}\,y}{b^2}=0,\qquad \mathrm{d}\,y^2=\frac{b^4x^2}{a^4y^2}\,\mathrm{d}\,x^2=\frac{b^2x^2}{a^2(a^2-x^2)}\,\mathrm{d}\,x^2,$$

so

$$\begin{aligned}\int\sqrt{\mathrm{d}\,x^2+\mathrm{d}\,y^2}&=\int\sqrt{\frac{a^2(a^2-x^2)+b^2x^2}{a^2(a^2-x^2)}}\,\mathrm{d}\,x\\&=\frac{1}{a}\int\sqrt{\frac{a^4-c^2x^2}{a^2-x^2}}\,\mathrm{d}\,x=\frac{1}{a}\int\frac{y}{a^2-x^2}\,\mathrm{d}\,x,\end{aligned}$$

where $b^2+c^2=a^2$ and

$$y^2=(a^2-x^2)(a^4-c^2x^2).$$

Assuming $c\neq 0$, the last equation defines an **elliptic curve** and is equivalent to:

$$y^2=(x^2-a^2)(c^2x^2-a^4),$$

$$\Bigl(\frac{y}{(x+a)^2}\Bigr)^2=\Bigl(\frac{x-a}{x+a}\Bigr)\Bigl(\frac{cx+a^2}{x+a}\Bigr)\Bigl(\frac{cx-a^2}{x+a}\Bigr).$$

We rewrite this as

$$v^2=\beta u(u-\mu)(u-\rho),$$

Date: December 9, 2009.

Notes prepared for the algebra seminar, November 20, 2009.

where

$$v=\frac{y}{(x+a)^2}, \qquad u=\frac{x-a}{x+a},$$

and β, μ, and ρ are such that

$$\begin{aligned}\Big(\frac{cx+a^2}{x+a}\Big)\Big(\frac{cx-a^2}{x+a}\Big)&=\beta(u-\mu)(u-\rho),\\ c^2\Big(x-\frac{a^2}{c}\Big)\Big(x+\frac{a^2}{c}\Big)&=\beta(x-a-\mu(x+a))(x-a-\rho(x+a))\\ &=\beta\big((1-\mu)x-(1+\mu)\big)\big((1-\rho)x-(1+\rho)a\big)\\ &=\beta(1-\mu)(1-\rho)\Big(x-\frac{1+\mu}{1-\mu}\Big)\Big(x-\frac{1+\rho}{1-\rho}\Big).\end{aligned}$$

So it suffices if

$$c^2=\beta(1-\mu)(1-\rho), \qquad \frac{a^2}{c}=\frac{1+\mu}{1-\mu}, \qquad -\frac{a^2}{c}=\frac{1+\rho}{1-\rho},$$

that is,

$$\mu=\frac{a^2-c}{a^2+c}, \qquad \rho=\frac{1}{\mu}, \qquad \beta=-\frac{c^2\mu}{(1+\mu)^2}.$$

After another change of variables, the equation becomes

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

(where $\lambda=\rho/\mu$). On this curve, the differential form $\mathrm{d}\,x/y$ is holomorphic. But

$$Q\mapsto\int_P^Q\frac{\mathrm{d}\,x}{y}$$

is well defined, not on $\mathbb{P}(\mathbb{C})$ (that is, $\mathbb{C}\cup\{\infty\}$), but rather on the Riemann surface got by cutting and gluing two copies of this along lines from 0 to ∞ and 1 to λ: the surface is then a **torus.** This then is the elliptic curve, and the function above is an analytic bijection onto $\mathbb{C}/\Lambda$ for some lattice Λ.

2. Curves and function fields

Let K and L be algebraically closed fields, with $K\subset L$ and $\operatorname{tr-deg}(L/K)=\infty$.

An irreducible f in $K[X,Y]$ defines a **curve** C over K, namely

$$C=\{(x,y)\in L^2\colon f(x,y)=0\}.$$

We define

$$\begin{aligned}K[C]&=K[X,Y]/(f),\\ K(C)&=\text{ fraction field of }K[C];\end{aligned}$$

this is the field of **rational functions** on C over K. Then

$$\begin{aligned}K[C]&=K[a,b]\\ K(C)&=K(a,b),\end{aligned}$$

where

$$\left.\begin{aligned} a &= ((x,y) \mapsto x) \\ b &= ((x,y) \mapsto y) \end{aligned}\right\} \text{ on } C,$$

so that $f(a,b) = 0$ and (a,b) is a **generic point** of C over K; we may assume $(a,b) \in L^2$.

Say also

$$D = \{(x,y) \in L^2 \colon g(x,y) = 0\},$$

and φ^* is an embedding of $K(C)$ in $K(D)$ over K. Then

$$0 = \varphi^*(f(a,b)) = f(\varphi^*(a), \varphi^*(b)),$$

so $(\varphi^*(a), \varphi^*(b))$ is a generic point of C and is also a **dominant rational map** φ from D onto C. We recover φ^* by

$$\varphi^*(h) = h \circ \varphi.$$

Indeed,

$$\varphi^*(a) = a(\varphi^*(a), \varphi^*(b)) = a \circ (\varphi^*(a), \varphi^*(b)) = a \circ \varphi,$$

and likewise for b.

Rule. *The K-algebra $K(C)$ embeds in $K(D)$ if and only if C has a generic point with coordinates from $K(D)$.*

We also have

$$K(C) \cong K(D) \iff D \text{ and } C \text{ are } \textbf{birationally equivalent.}$$

For example, the function

$$(u,v) \mapsto \left(\frac{x-a}{x+a}, \frac{y}{(x+a)^2}\right)$$

determines a birational equivalence between the elliptic curves above.

Or let $f = X^2 + Y^2$ and $g = X$. See Figure 1. Then $\varphi \colon C \to D$, where

$$\varphi(x,y) = \frac{y}{1+x}, \qquad \varphi^{-1}(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1-t^2}\right),$$

so C and D are birationally equivalent, and

$$K(D) \cong K(e) \cong K(a,b) \cong K(C)$$

$$e \mapsto \frac{b}{1+a}$$

$$\frac{1-e^2}{1+e^2} \leftarrow a$$

$$\frac{2e}{1-e^2} \leftarrow b$$

Every curve C has a **genus** $\gamma(C)$ in $\mathbb{N}$. If $K(C)$ embeds in $K(D)$ over K, then

$$\gamma(C) \leqslant \gamma(D).$$

If the embedding is *proper,* then either $\gamma(C) < \gamma(D)$ or

$$0 \leqslant \gamma(C) \leqslant \gamma(D) \leqslant 1.$$

If $\gamma(C) = 0$, then $K(C) \cong K(X)$.

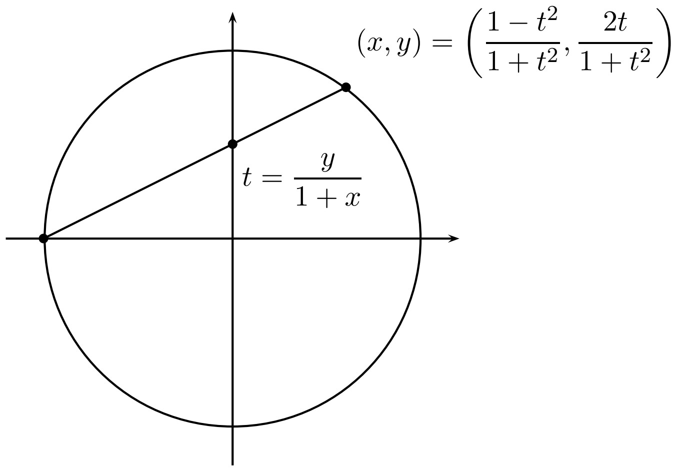

FIGURE 1. Birational equivalence of circle and straight line

3. Logic and elliptic curves

Suppose $K(C) \ncong K(D)$. We may assume $\gamma(C) \leqslant \gamma(D) < \gamma(E)$ for some curve E. Then the formula

$$\exists y\ (x,y) \in E$$

defines K in $K(C)$ and $K(D)$. If $\gamma(C) < \gamma(D)$ or $1 < \gamma(C) = \gamma(D)$, then the sentence

$$\forall x\ \forall y\ \exists z\ ((x,y) \in D \Rightarrow (x,z) \in E)$$

is true in $K(C)$, but not $K(D)$, so these algebras have different **theories;** we say they are not **elementarily equivalent,** and we write

$$K(C) \not\equiv K(D).$$

We cannot then have $0 = \gamma(C) = \gamma(D)$. The remaining possibility is $1 = \gamma(C) = \gamma(D)$, that is, C and D are **elliptic curves.**

An elliptic curve E is also an abelian group; the curve has **complex multiplication** if $\mathrm{End}(E) \ncong \mathbb{Z}$.

Theorem (Jean-Louis Duret (1992); D.P. (1998))**.** *If C and D are curves over K, and C is not an elliptic curve with complex multiplication, then*

$$K(C) \ncong K(D) \implies K(C) \not\equiv K(D).$$

In general, if $\varphi\colon D \to C$, then

$$\deg(\varphi) = [K(D) : K(C)]$$

Theorem (D.P. (1998))**.** *Suppose C and D are elliptic curves over K with complex multiplication. The following are equivalent.*

(1) *There are φ and φ' from C onto D with*

$$\gcd(\deg(\varphi), \deg(\varphi')) = 1.$$

(2) *$K(C)$ and $K(D)$ agree on all sentences*

$$\forall(x_0,\dots,x_{n-1})\ \exists y\ \psi(x_0,\dots,x_{n-1},y),$$

where ψ is quantifier-free.

If $\operatorname{char}(K)=0$, *then the foregoing are equivalent to the following.*

(3) $\operatorname{End}(C)\cong\operatorname{End}(D)$.

Say E_0 and E_1 are elliptic curves over $\mathbb{C}$. For each i in $\{0,1\}$ there are A_i and B_i in $\mathbb{C}$ such that E_i is birationally equivalent to the curve defined by

$$y^2=4x^3-A_ix-B_i.$$

So we may assume E_i is this curve. There is a lattice Λ_i, namely $\langle 1,\tau_i\rangle$, where $\Im(\tau_i)>0$, and there is a function $\wp_i$, namely

$$z\mapsto\frac{1}{z^2}+\sum_{\omega\in\Lambda_i\smallsetminus\{0\}}\left(\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right),$$

such that $(\wp_i,\wp_i{}')$ is a generic point of E_i and is a bijection from $\mathbb{C}/\Lambda_i$ to E_i. Say $\varphi\colon E_0\to E_1$. There are α and ω in $\mathbb{C}$ such that the following commutes.

$$\begin{tikzcd}
\mathbb{C}/\Lambda_0 \arrow[r, "(\wp_0,\wp_0{}')"] \arrow[d, "z\mapsto\alpha z"'] & E_0 \arrow[dd, "\varphi"] \\
\mathbb{C}/\Lambda_1 \arrow[d, "z\mapsto z+\omega"'] & \\
\mathbb{C}/\Lambda_1 \arrow[r, "(\wp_1,\wp_1{}')"'] & E_1
\end{tikzcd}$$

We may assume $\omega=0$, so φ is an **isogeny** and, in particular, a homomorphism. We must have

$$\alpha\Lambda_0\subseteq\Lambda_1,$$

and then

$$\deg(\varphi)=[\Lambda_1:\alpha\Lambda_0].$$

Also, if $\alpha\neq0$, there is a matrix $\begin{pmatrix}a&b\\c&d\end{pmatrix}$ or M in $\mathrm{M}_n(\mathbb{Z})$ such that

$$\alpha\begin{pmatrix}1\\\tau_0\end{pmatrix}=\begin{pmatrix}a+b\tau_1\\c+d\tau_1\end{pmatrix}=\begin{pmatrix}a&b\\c&d\end{pmatrix}\begin{pmatrix}1\\\tau_1\end{pmatrix}=M\begin{pmatrix}1\\\tau_1\end{pmatrix},$$

and then

$$\deg(\varphi)=\det(M).$$

Also

$$\begin{pmatrix}d&-b\\-c&a\end{pmatrix}\begin{pmatrix}1\\\tau_0\end{pmatrix}=\alpha^{-1}\det(M)\begin{pmatrix}1\\\tau_1\end{pmatrix}=\alpha^{-1}\deg(\varphi)\begin{pmatrix}1\\\tau_1\end{pmatrix},$$

so

$$z\mapsto\alpha^{-1}\deg(\varphi)z\colon\mathbb{C}/\Lambda_1\to\mathbb{C}/\Lambda_0$$

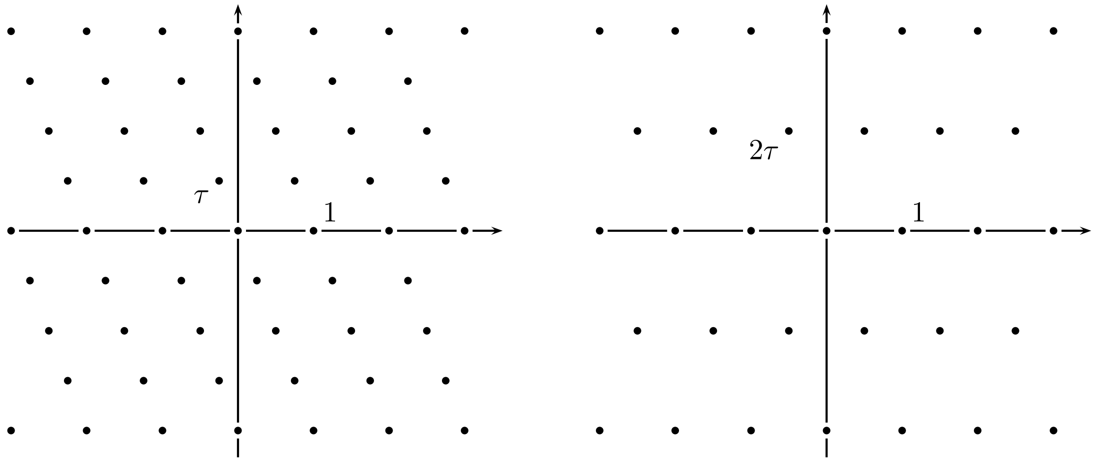

FIGURE 2. A lattice and its endomorphisms

corresponding to an isogeny $\hat{\varphi}$ from E_1 to E_0. Then

$$\deg(\hat{\varphi}) = \deg(\varphi),$$
$$\hat{\varphi}\varphi = [\deg(\varphi)]$$

where $[n]$ is multiplication by n.

If E corresponds to $\mathbb{C}/\Lambda$, then

$$\operatorname{End}(E) \cong \{z \in \mathbb{C} \colon z\Lambda \subseteq \Lambda\}.$$

For example, if

$$\tau = \frac{-1 + \sqrt{-7}}{4}.$$

then (see Figure 2)

$$\operatorname{End}(E) = \langle 1, 2\tau \rangle.$$

In general, if E has complex multiplication, this means, for some α in $\mathbb{C} \smallsetminus \mathbb{R}$, we have

$$\alpha \begin{pmatrix} 1 \\ \tau \end{pmatrix} = \begin{pmatrix} a + b\tau \\ c + d\tau \end{pmatrix},$$

so

$$\alpha = a + b\tau,$$
$$c + d\tau = \alpha\tau = (a + b\tau)\tau,$$
$$b\tau^2 + (a - d)\tau - c = 0.$$

So E has complex multiplication if and only if τ is quadratic. If indeed

$$b\tau^2 + a\tau - c = 0$$

in lowest terms, then one shows

$$\operatorname{End}(E) \cong \langle 1, b\bar{\tau} \rangle;$$

in any case, $\operatorname{End}(E)$ embeds in Λ.

In general, since $\operatorname{End}(E)$ embeds in $\mathbb{C}$, it is commutative. Suppose φ and ψ are isogenies from E_0 to E_1 of relatively prime degrees. There are integers m and n such that

$$m\deg(\varphi) + n\deg(\psi) = 1.$$

Then $\operatorname{End}(E_1) \cong \operatorname{End}(E_0)$ by

$$\alpha \mapsto m\hat{\varphi}\alpha\varphi + n\hat{\psi}\alpha\psi.$$

Now suppose conversely $\operatorname{End}(E_1) \cong \operatorname{End}(E_0)$, and each curve has complex multiplication. Then Λ_0 and Λ_1 have a common sublattice, so by linear algebra we may assume $\tau_1 = n\tau_0$ for some n.

Theorem (D.P.)**.** *Say* $\operatorname{End}(E_1) \cong \operatorname{End}(E_0) \ncong \mathbb{Z}$*, and*

$$b{\tau_0}^2 + a\tau_0 - c = 0$$

in lowest terms, and $\tau_1 = n\tau_0$*. Then*

$$\operatorname{Hom}(E_0, E_1) \cong \langle n, b\bar{\tau}\rangle.$$

If this takes φ *to* $nx + by\bar{\tau}$*, then*

$$\deg(\varphi) = nx^2 - axy - \frac{bc}{n}y^2,$$

a quadratic form with relatively prime coefficients, so it represents coprime numbers.

Suppose now p divides the degree of every isogeny from E_0 to E_1. Then there is a finite set $\mathcal{L}$ of lattices, each having index p in Λ_1, such that, if

$$\alpha\Lambda_0 \subseteq \Lambda_1,$$

then, for some Λ in $\mathcal{L}$,

$$\alpha\Lambda_0 \subseteq \Lambda \subset \Lambda_1.$$

Hence

$$K(E_0) \ncong K(E_1),$$

because $K(E_0)$ but not $K(E_1)$ is a field L such that, if

$$\varphi^*[K(E_1)] \subseteq L,$$

then

$$\varphi^*[K(E_1)] \subset F \subseteq L,$$

where the isomorphism-class of F over $\varphi^*[K(E_1)]$ has finitely many possibilities.

Mathematics Dept, Middle East Technical University, Ankara 06531, Turkey
E-mail address: `dpierce@metu.edu.tr`
URL: `http://metu.edu.tr/~dpierce/`