

1. Points of finite order on elliptic curves

Objekttyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **24 (1978)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **24.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern. Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden. Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

1. POINTS OF FINITE ORDER ON ELLIPTIC CURVES

Let E be an elliptic curve over the complex numbers with origin \mathfrak{o} . In practice E will have various realizations as an algebraic curve defined by polynomial equations in projective space; e.g., as a plane cubic, the intersection of two quadrics in \mathbf{P}^3 , etc. All of these projective models are birationally isomorphic to the given curve E . It is well known that E admits a commutative group law with \mathfrak{o} being the identity, and we are interested in the points p of finite order n defined by

$$np = \mathfrak{o}$$

where $np = p + \dots + p$ (n times). Specifically, we pose the question of finding a projective model of E relative to which these points have a simple explicit description.

From a complex-analytic point of view we may realize E as the Riemann surface

$$E = \mathbf{C}/\Lambda$$

obtained by factoring the complex u -plane by a lattice Λ with $u = 0$ projecting onto the origin \mathfrak{o} ; this is a consequence of Abel's theorem¹⁾. The group law on E is obtained from the additive structure on \mathbf{C} , and so if $u_0 \in \mathbf{C}$ projects onto $p \in E$ the finite order condition is

$$(1) \quad nu_0 \equiv 0 \text{ modulo } \Lambda.$$

In particular there are n^2 points of finite order n on E corresponding to the points of

$$\frac{1}{n} \Lambda.$$

Our problem may be generalized to that of giving projective meaning to the equation

$$(2) \quad u_1 + \dots + u_n \equiv 0 \text{ modulo } \Lambda,$$

which specializes to (1) when the u_i tend together. Here again the basic step is the following variant of *Abel's theorem*²⁾: Given $u_i, v_i \in \mathbf{C}$ ($i = 1, \dots, n$)

¹⁾ This is the classical version of Abel's theorem used in ¹⁾.

²⁾ C.f. L. Ahlfors, *Complex Analysis*, McGraw-Hill (New York), Exercise 2 on page 267. This may be thought of as providing a converse to the classical Abel's theorem.

there is an entire meromorphic function $f(u)$ with period lattice Λ and having zeroes at $u_i + \Lambda$ and poles at $v_i + \Lambda$ if, and only if,

$$u_1 + \dots + u_n \equiv v_1 + \dots + v_n \text{ modulo } \Lambda.$$

It follows that the vector space $H^0(\mathcal{O}_E([n\mathfrak{o}]))$ of rational functions on E having a pole of order at most n at \mathfrak{o} , or equivalently the entire meromorphic functions $f(u)$ which have period lattice Λ and a pole of order at most n at $u = 0$, has dimension n . If we choose a basis f_1, \dots, f_n for this vector space, then for $n \geq 3$ the mapping

$$F(u) = [f_1(u), \dots, f_n(u)]$$

induces a projective embedding

$$E \rightarrow \mathbf{P}^{n-1}$$

whose image is easily proved to be a smooth algebraic curve of degree n . Thus, for $n = 3$ we have a plane cubic, for $n = 4$ the intersection of two quadrics in \mathbf{P}^3 , etc. In general we shall call the image the *normal elliptic curve of degree n* . According to Abel's theorem the hyperplane sections of this curve, which are just the zeroes of functions $f \in H^0(\mathcal{O}_E([n\mathfrak{o}]))$, are characterized by $u_1 + \dots + u_n \equiv 0$ modulo Λ . Put differently, the condition (2) is equivalent to

$$(3) \quad \det \| f_i(u_j) \| = 0$$

expressing the failure of the points $F(u_1), \dots, F(u_n)$ to be in general position. If we denote by

$$WF(u) = \begin{vmatrix} f_1(u) & \dots & f_n(u) \\ f_1'(u) & & f_n'(u) \\ \cdot & & \cdot \\ \cdot & & \cdot \\ f_1^{(n-1)}(u) & \dots & f_n^{(n-1)}(u) \end{vmatrix}$$

the Wronskian of the functions $f_i(u)$, then by letting the u_i tend together the condition (3) specializes to the equation

$$(4) \quad WF(u) = 0$$

characterizing the solutions to (1). Points satisfying (4) will be called *hyperflexes*, and what we have shown is that:

The points of order n on an elliptic curve are precisely the hyperflexes of the normal elliptic curve of degree n .

Now we observe that the equation (4) is independent of the selection of basis $\{f_i\}$ and local coordinate u on E . To see therefore whether or not a given point p is of finite order n we will make convenient choices. Namely, we may choose a basis $\{1, f(u)\}$ for $H^0(\mathcal{O}_E([2\mathfrak{o}]))$ such that $f(p) = 0$. In other words, the function f induces a 2-to-1 map

$$(5) \quad f: E \rightarrow \mathbf{P}^1$$

with $p \in f^{-1}(0)$. It is well-known that the representation (5) has four branch points, one of which is the point at infinity with $f^{-1}(\infty) = \mathfrak{o}$. If we let x be the coordinate on \mathbf{P}^1 and a, b, c the finite branch points, then E is conformally represented as the Riemann surface of the algebraic function $\sqrt{(x-a)(x-b)(x-c)}$.

Put another way, the plane cubic curve with affine equation

$$(6) \quad y^2 = (x-a)(x-b)(x-c)$$

gives a projective model of E . Setting $x = f(u)$, since the holomorphic differential du is a constant multiple of dx/y it follows that, with a suitable normalization, $2y = f'(u) = \frac{df(u)}{du}$. Consequently the projective model

(6) of E is given by the mapping $E \rightarrow \mathbf{P}^2$ associated to the basis $\{1, f(u), f'(u)\}$ of $H^0(\mathcal{O}_E([3\mathfrak{o}]))$. Of course, $f(u)$ and $f'(u)$ are essentially the Weierstrass functions. We recall that that their Laurent series around $u = 0$ are

$$(7) \quad \left\{ \begin{array}{l} f(u) = \frac{1}{u^2} + \dots \\ f'(u) = \frac{-2}{u^3} + \dots \\ \cdot \\ \cdot \\ \cdot \\ f^{(k)}(u) = \frac{(-1)^k (k+1)!}{u^{k+2}} + \dots \end{array} \right.$$

Returning to our question of whether $p \in f^{-1}(0)$ is of finite order n , we will use $x = f(u)$ as local coordinate around p and choose the functions

$$(8) \quad \begin{cases} 1, x, \dots, x^m; y, xy, \dots, x^{m-1}y & n = 2m + 1 \\ 1, x, \dots, x^m; y, xy, \dots, x^{m-2}y & n = 2m \end{cases}$$

as basis for $H^0(\mathcal{O}_E([n\mathcal{O}]))$. That this choice gives a basis follows from the Laurent series (7). It is now an easy matter to express the Wronskian equation (4) at $x = 0$.

We consider the case $n = 2m + 1$ and let $\frac{dg(x)}{dx}$ be the derivative of $g(x)$ evaluated at $x = 0$. The choice of basis (8) facilitates the evaluation of the Wronskian. For example, from $\frac{d^k(x^l)}{dx^k} = 0$ for $k > l$ the Wronskian has the form

1 ... 0	_____	,
. . .	_____	
. . .	_____	
. . .	_____	
0 ... m!	_____	
0 ... 0	_____	
. . .	_____	
. . .	_____	
. . .	_____	
0 ... 0	_____	

so that (4) is equivalent to

$$(9) \quad \left| \begin{array}{ccc} \frac{d^{m+1}y}{dx^{m+1}} & \frac{d^{m+1}(xy)}{dx^{m+1}} & \dots & \frac{d^{m+1}(x^{m-1}y)}{dx^{m+1}} \\ \frac{d^{m+2}y}{dx^{m+2}} & \frac{d^{m+2}(xy)}{dx^{m+2}} & \dots & \frac{d^{m+2}(x^{m-1}y)}{dx^{m+2}} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \frac{d^{2m}y}{dx^{2m}} & \frac{d^{2m}(xy)}{dx^{2m}} & \dots & \frac{d^{2m}(x^{m-1}y)}{dx^{2m}} \end{array} \right| = 0$$

If the series expansion of $y(x)$ is

$$y(x) = \sum_{k=0}^{\infty} A_k x^k,$$

then (9) is

$$\begin{vmatrix} (m+1)! A_{m+1} & (m+1)! A_m & \dots & (m+1)! A_2 \\ (m+2)! A_{m+2} & (m+2)! A_{m+1} & \dots & (m+2)! A_3 \\ & \cdot & & \cdot \\ & \cdot & & \cdot \\ & \cdot & & \cdot \\ (2m)! A_{2m} & (2m)! A_{2m-1} & \dots & (2m)! A_{m+1} \end{vmatrix} = 0.$$

In summary we have proved

- (10) *Let E be an elliptic curve with origin \mathfrak{o} and $p \in E$ a given point. Then p is of finite order $n \Leftrightarrow$ the following condition is satisfied: Choose rational functions x, y on E having poles of respective orders 2, 3 at \mathfrak{o} but which are regular elsewhere and with $x(p) = 0$. Then there is an equation $y^2 = (x-a)(x-b)(x-c)$ where a, b, c are distinct and non-zero, and we write*

$$y = \sqrt{(x-a)(x-b)(x-c)} = \sum_{k=0}^{\infty} A_k x^k.$$

The finite order condition is

$$\begin{vmatrix} A_2 & A_3 & \dots & A_{m+1} \\ A_3 & A_4 & \dots & A_{m+2} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ A_{m+1} & A_{m+2} & \dots & A_{2m} \end{vmatrix} = 0, \quad n = 2m + 1$$

$$\begin{vmatrix} A_3 & A_4 & \dots & A_{m+1} \\ A_4 & A_5 & \dots & A_{m+2} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ A_{m+1} & A_{m+2} & \dots & A_{2m} \end{vmatrix} = 0, \quad n = 2n.$$