

2. ELLIPTIC MODULES: ANALYTIC DEFINITION

Let p be a prime number, d a positive integer, $q = p^d$, \mathbb{F}_q a field of q elements, C an absolutely irreducible smooth projective curve defined over \mathbb{F}_q , and F the function field $\mathbb{F}_q(C)$ of C over \mathbb{F}_q , that is, the field of rational functions on C over \mathbb{F}_q . At each place v of F , namely a closed point of C , let F_v be the completion of F at v and A_v the ring of integers in F_v . Fix a place ∞ of F . Let C_∞ be the completion of an algebraic closure \overline{F}_∞ of F_∞ .

Let $A = H^0(C - \{\infty\}, \mathcal{O}_C)$ be the ring of regular functions on $C - \{\infty\}$, namely the ring of functions in F whose only possible poles are at ∞ . For each v in $\text{Spec } A = C - \{\infty\}$, the quotient field $\mathbb{F}_v = A/v$ is finite. Denote its cardinality by q_v . Note that A_v is the completion of A at v . For any a in A let $(a) = aA$ be the ideal in A generated by a . Let $|\cdot| = |\cdot|_\infty$ be the absolute value on A which assigns to $a \neq 0$ in A the cardinality of the quotient ring $A/(a)$. It extends uniquely to $F, F_\infty, \overline{F}_\infty$, and C_∞ . Let π_∞ be a generator of the maximal ideal of A_∞ . Let q_∞ be the cardinality $|A_\infty/\pi_\infty|$ of the finite field A_∞/π_∞ . If $a \in A$ has a pole of order n at ∞ , then $|a|_\infty = |\pi_\infty^{-n}| = q_\infty^n$.

A function f from C_∞ to C_∞ is called *entire* if it is equal to an everywhere convergent power series. Thus $f = \sum_0^\infty a_n x^n$ ($a_n \in C_\infty$), where $|a_n|^{1/n} \rightarrow 0$.

Lemma 2.1. *Let f be a nonconstant entire function on C_∞ . Then f attains each value of C_∞ .*

Proof. This is the same as the proof in the case of characteristic zero. See [Ko], Ex. 13, Section IV.4 (p. 108), where the lemma is proven with C_∞ replaced by the completion Ω of the algebraic closure $\overline{\mathbb{Q}}_p$ of \mathbb{Q}_p . □

A quotient $f = h/g$ of two entire functions h, g on C_∞ , with $g \neq 0$, is called a meromorphic function on C_∞ . The *divisor* $\text{Div } f$ of a meromorphic function f on C_∞ , with zeroes a_i and poles b_j of multiplicities n_i and m_j (respectively), is the formal sum $\sum_i n_i(a_i) - \sum_j m_j(b_j)$.

Corollary 2.2. *Let f, g be entire functions on C_∞ with $\text{Div } f = \text{Div } g$. Then there is $c \neq 0$ in C_∞ with $f = cg$.*

Proof. If $g \neq 0$ then f/g is entire, as its Taylor expansion at 0 converges everywhere. But f/g has no zeroes. Hence it is constant by Lemma 2.1. □

A set L in C_∞ is called *discrete* if for each positive number c the set $\{x \text{ in } L; |x| \leq c\}$ is finite. Since C_∞ is a non-Archimedean field, then for each discrete set L there is an entire function e_L with $\text{Div } e_L = L$. If L contains zero then there is a unique e_L normalized so that $e_L(0) = 1$. It is given by the product

$$e_L(x) = x \prod_a (1 - x/a) \quad (a \neq 0 \text{ in } L).$$

Proposition 2.3. *Let L be an additive discrete subgroup of C_∞ . Then e_L defines an isomorphism from C_∞/L to C_∞ as additive groups.*

Proof. (i) From Lemma 2.1 it follows that e_L defines a set theoretic surjection from C_∞/L to C_∞ . (ii) To show that e_L is a group homomorphism, we first consider the case where L is finite. It is clear from the definition of e_L that $e_L(x+y) - e_L(x) - e_L(y) = 0$ if x or y lie in L . Hence the polynomial $e_L(x)e_L(y)$, whose degree in x is $|L|$, divides the polynomial $e_L(x+y) - e_L(x) - e_L(y)$, whose degree in x is less than $|L|$. We conclude that $e_L(x+y) = e_L(x) + e_L(y)$. In general we can write L as a union of finite subgroups L_n . Then $e_L = \lim_n e_{L_n}$, and (ii) follows. (iii) Since the kernel of e_L is L , the proposition follows from (i) and (ii). \square

Definition 2.1. A lattice L is a discrete, finitely generated A -submodule of C_∞ .

Lemma 2.4. A finitely generated module over a Dedekind domain (an integral domain in which every nonzero proper ideal factors into a product of prime ideals) is projective if and only if it is torsion free.

Proof. See [BN], VII, Section 4.10, Prop. 22 (p. 543). \square

Since C_∞ is a field, the lattice L is a torsion-free A -module. Since A is a Dedekind domain, L is projective. Denote by $r = \text{rank} L$ the rank of the lattice L . We have

Lemma 2.5. For any $a \neq 0$ in A there is an isomorphism from L/aL to $(A/aA)^r$.

The isomorphism $e_L : C_\infty/L \rightarrow C_\infty$ and the A -module structure on C_∞/L define an A -module structure on C_∞ by $ax = \varphi_{a,L}(x) = e_L(a(e_L^{-1}(x)))$ (a in A , x in C_∞).

Lemma 2.6. For each a in A the function $\varphi_{a,L}$ is a polynomial of degree $|a|^r$ over C_∞ .

Proof. Put $\psi_{a,L}(x) = e_L(ax)$. The kernel of $\psi_{a,L}$ is $a^{-1}L$. Hence there is some $c \neq 0$ with $\psi_{a,L}(x) = c \prod_b (e_L(x) - e_L(b))$ (b in $a^{-1}L/L$). Consequently $\varphi_{a,L}(x) = c \prod_b (x - e_L(b))$ is a polynomial over C_∞ whose degree is equal to the cardinality $|a|^r$ of L/aL . \square

Let E_∞ be a fixed finite extension of F_∞ in C_∞ . Let \overline{E}_s denote the completion of the separable closure E_s of E_∞ in C_∞ . The fields E_∞ , E_s , and \overline{E}_s appear only in Chap. 2.

Definition 2.2. A lattice L is called a lattice over E_∞ if it lies in E_s and it is invariant under the action of the Galois group $\text{Gal}(E_s/E_\infty)$ of E_s over E_∞ .

Example 2.1. The ring $L = A$ is a lattice over F_∞ , of rank one.

Proposition 2.7. If L is a lattice over E_∞ then $\varphi_{a,L}$ is a polynomial over E_∞ .

Proof. The coefficients of the Taylor expansion at 0 of e_L lie in \overline{E}_s , and they are invariant under $\text{Gal}(E_s/E_\infty)$ by definition of L . Hence they lie in E_∞ (by [Ta], Theorem 1, p. 176). The proposition now follows from the proof of Lemma 2.6. \square

Definition 2.3. (i) The lattices L, L' over E_∞ are *isomorphic* if $L' = uL$ for some $u \neq 0$ in E_∞ . (ii) Let L, L' be lattices of rank r . A *morphism* from L to L' is u in E_∞ with $uL \subset L'$.

Lemma 2.8. *If L is a lattice over E_∞ and $u \neq 0$ is in E_∞ , then $u^{-1}\varphi_{a,uL}(ux) = \varphi_{a,L}(x)$.*

Proof. Using the identity $e_{uL}(x) = ue_L(u^{-1}x)$ we rewrite the relation $\varphi_{a,uL}(e_{uL}(x)) = e_{uL}(ax)$ in the form $\varphi_{a,uL}(ue_L(u^{-1}x)) = ue_L(au^{-1}x)$. This implies the required identity

$$u^{-1}\varphi_{a,uL}(ue_L(x)) = e_L(ax) = \varphi_{a,L}(e_L(x)).$$

□

Definition 2.4. A polynomial h in $C_\infty[x]$ is called *additive* if $h(x+y) = h(x) + h(y)$.

Lemma 2.9. *If h is additive then $h(x) = \sum_{i=1}^I a_i x^{p^i}$.*

Proof. If $h(x) = \sum b_i x^i$ is additive, then $b_i((x+y)^i - x^i - y^i) = 0$. If $i = p^n j$ with $j > 1$ prime to p , then $(x+y)^i = (x^{p^n} + y^{p^n})^j$ is not equal to $x^i + y^i$, since it has the term $jx^{p^n(j-1)}y^{p^n}$ in its binomial expansion. Hence $b_i = 0$ if i is not a power of p . □

The map $\varphi_L : a \mapsto \varphi_{a,L}$ has several properties which suggest the following:

Definition 2.5. (1) A map $\varphi : A \rightarrow E_\infty[x]$, $a \mapsto \varphi_a$, is called an *elliptic module* of rank r over E_∞ if (i) $\varphi_a(x+y) = \varphi_a(x) + \varphi_a(y)$ (a in A); (ii) $\varphi_{ab} = \varphi_a \circ \varphi_b$, $\varphi_{a+b} = \varphi_a + \varphi_b$; (iii) $\deg \varphi_a = |a|^r$; and (iv) $\varphi_a(x) \equiv ax \pmod{x^p}$.
 (2) The elliptic modules φ, φ' are *isomorphic* if there is $u \neq 0$ in E_∞ with $\varphi'_a(x) = u\varphi_a(u^{-1}x)$ (a in A).
 (3) Let φ, φ' be two elliptic modules of rank r over E_∞ . A *morphism* from φ to φ' is an additive polynomial P in $E_\infty[x]$ with $P \circ \varphi_a = \varphi'_a \circ P$ (a in A).

Lemma 2.10. *Any morphism P is of the form $P(x) = \sum_i a_i x^{q^i}$, where a_i lie in E_∞ . The group of automorphisms of an elliptic module is \mathbb{F}_q^\times .*

Proof. For any a in the finite subfield \mathbb{F}_q of A we have $\varphi_a(x) = ax$ and $\varphi'_a(x) = ax$. Hence $aP(x) = P(ax)$, and the lemma follows. □

Corollary 2.11. (1) For each b in A , we have $\varphi_b(x) = \sum_{i=1}^{I(b)} a_i x^{q^i}$, where $I(b) = rv_q(b)$, $v_q(b) = \log_q |b|$, and $a_{I(b)} \neq 0$. (2) If $A = \mathbb{F}_q[t]$ then $|t| = q$, and an elliptic module is determined by $\varphi_t(x) = tx + \sum_{i=1}^r a_i x^{q^i}$ with $a_r \neq 0$. (3) In (2), up to isomorphism we may replace a_i by $a_i u^{q^i - 1}$.

Remark 2.1. (1) An elliptic module of rank r over C_∞ is defined on replacing E_∞ by C_∞ in Definition 2.5(1). The following theorem holds also with E_∞ replaced by C_∞ . (2) Since the case of $r = 0$ is trivial, we consider from now on only the case of $r > 0$.

Theorem 2.12. *The map $L \mapsto \varphi_L$ defines an equivalence from the category of (isomorphism classes of) lattices of rank r over E_∞ to the category of (isomorphism classes of) elliptic modules of rank r over E_∞ .*

Proof. (i) Our first aim, accomplished in (iv), is to construct an inverse to the map $L \mapsto \varphi_L$. Thus let φ be an elliptic module over E_∞ , of rank r . Fix a in $A - \mathbb{F}_q$; then $|a| > 1$. We have $\varphi_a(x) = ax + \sum_i a_i x^{q^i}$ with a_i in E_∞ ($1 \leq i \leq s = rv_q(a)$). We claim that there exists a unique power series $e(x) = \sum_{i=0}^\infty e_i x^{q^i}$ with $e_0 = 1$, e_i in E_∞ , and $\varphi_a(e(x)) = e(ax)$. To show this we equate the coefficients of x^{q^n} in $\varphi_a(e(a^{-1}x)) = e(x)$ to obtain

$$e_n \left(1 - a^{1-q^n}\right) = a_n a^{-q^n} + \sum_{i=1}^{n-1} a_i e_{n-i}^{q^i} a^{-q^n}$$

($a_n = 0$ for $n > s$; $e_i = 0$ for $i < 0$); this yields a recursive formula for e_n .

(ii) We claim that e is entire. To see this we note that for $n > s$ we have

$$e_n(a^{q^n} - a) = \sum_{i=1}^s a_i e_{n-i}^{q^i}.$$

Then

$$|a| r_n \leq \max \left\{ |a_i|^{p^{-n}} r_{n-i}; 1 \leq i \leq s \right\},$$

where $r_j = |e_j|^{q^{-j}}$. For θ with $|a|^{-1} < \theta < 1$, there is n' such that for $n > n'$ we have $r_n \leq \theta \max \{r_{n-i}; 1 \leq i \leq s\}$. Hence $r_n \rightarrow 0$, and e is entire.

(iii) For any b in A we claim that $\varphi_b(e(x)) = e(bx)$. Indeed, if $b \neq 0$, then we have

$$(\varphi_b \circ e \circ b^{-1})(x) = (\varphi_b \circ \varphi_a \circ e \circ a^{-1} \circ b^{-1})(x) = (\varphi_a \circ (\varphi_b \circ e \circ b^{-1}) \circ a^{-1})(x).$$

But then the uniqueness of the solution e for the equation $\varphi_a \circ e \circ a^{-1} = e$ implies the claim.

(iv) Let L be the kernel of e . Since the derivative e' of e is identically one, the zeroes of e are simple. Hence L lies in E_s . The group L is a discrete, $\text{Gal}(E_s/E_\infty)$ -invariant A -module, and we have $|L/aL| = |a|^r$. Hence L is finitely generated. Indeed, if $\{b_i\}$ are $|a|^r$ representatives in L for L/aL , then the finite set of x in L with $|x| \leq \max_i \{|b_i|\}$ generates L as an A -module. Now since L is torsion free and A is a Dedekind domain, L is flat. A finitely generated flat module over a Noetherian ring is projective. Hence L is a lattice of rank r . Since we have $e = e_L$ and $\varphi_{a,L} = \varphi_a$ for all a in A , we constructed an inverse to the map $L \mapsto \varphi_L$, establishing a set theoretic isomorphism.

(v) Let L, L' be lattices of rank r over E_∞ with $uL \subset L'$ for some u in E_∞ . Then $e_{L'}(ux)$ is L -invariant. The proof of Lemma 2.6 shows that

there is a polynomial P over E_∞ with $P(e_L(x)) = e_{L'}(ux)$. But then P is additive, and

$$\begin{aligned} (P \circ \varphi_{a,L})(e_L(x)) &= P(e_L(ax)) = e_{L'}(uax) \\ &= \varphi_{a,L'}((e_{L'} \circ u)(x)) = (\varphi_{a,L'} \circ P)(e_L(x)) \end{aligned}$$

implies that P is a morphism from φ_L to $\varphi_{L'}$.

(vi) Conversely, if P is a polynomial over E_∞ with $P \circ \varphi_L = \varphi_{L'} \circ P$, then

$$(P \circ e_L)(x) = (P \circ \varphi_{a,L} \circ e_L)(a^{-1}x) = (\varphi_{a,L'}(P \circ e_L))(a^{-1}x).$$

Hence we conclude from the uniqueness assertion of (i) that there is $u \neq 0$ in E_∞ with $(P \circ e_L)(x) = e_{L'}(ux)$. Then $uL \subset L'$, and the theorem follows. □

Remark 2.2. It is clear from the proof of (vi) that any polynomial P in $E_\infty[x]$ with $P \circ \varphi_a = \varphi'_a \circ P$ for all a in A has to be additive.



<http://www.springer.com/978-1-4614-5887-6>

Drinfeld Moduli Schemes and Automorphic Forms

The Theory of Elliptic Modules with Applications

Flicker, Y.Z.

2013, V, 150 p. 5 illus., Softcover

ISBN: 978-1-4614-5887-6