Formal groups and L-series.

Autor(en): **Deninger, Christopher / Nart, Enric**

Objekttyp: **Article**

Zeitschrift: **Commentarii Mathematici Helvetici**

Band (Jahr): **65 (1990)**

PDF erstellt am: **17.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-49728

Comment. Math. Helvetici 65 (1990) 318–333
0010-2571/90/020318-16$1.50 + 0.20/0

Formal groups and L-series

CHRISTOPHER DENINGER AND ENRIC NART*

0. Introduction

For certain commutative group schemes over $\mathbb{Z}$ there is a strong relation between the formal completion along zero and the L-series of the generic fibre. The first instance of such a connection was the following theorem of Honda [Ho 1] and Cartier [C].

(0.1) THEOREM. *Let E be an elliptic curve over $\mathbb{Q}$ with Néron model $\mathscr{E}$* over $\mathbb{Z}$ *and L-series*

$$L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

Let

$$F(X, Y) = f^{-1}(f(X) + f(Y))$$

be the formal group law over $\mathbb{Q}$ with logarithm

$$f(X) = \sum_{n=1}^{\infty} \frac{a_n}{n} X^n \quad \text{in } \mathbb{Q}[\![X]\!].$$

Then F is defined over $\mathbb{Z}$ and it is isomorphic to $\hat{\mathscr{E}}$ the completion of $\mathscr{E}$ along the zero section.

In fact in [Ho 1] this result is not proved in complete generality. This was later done by Hill [Hi] and Honda himself [Ho 2]. In [Ho 1] Honda also showed:

(0.2) THEOREM. *Let $K/\mathbb{Q}$ be a quadratic extension with discriminant d_K ring of integers $\mathcal{O}_K$ and Dirichlet character χ. Then the L-series $L(\chi, s)$ gives rise as above*

*Supported by Grant PB 85-0075 from CAICYT.

to a formal group law over $\mathbb{Z}$ *which over* $\mathcal{O}_K$ *becomes strongly isomorphic to* $X + Y + \sqrt{d_K}XY$.

In this note we will generalize (0.1) to abelian varieties over $\mathbb{Q}$ with real multiplication. Moreover (0.2) will be interpreted as a result on one dimensional algebraic tori. As such it can be extended to all abelian tori over $\mathbb{Q}$. In both cases the completion along zero of the respective Néron model is compared to a formal group law obtained from a suitable matrix valued Dirichlet series. In the case of tori the proof of our main result makes use of Leopoldt's investigations [L] on the galois module structure of the ring of integers in abelian extensions of $\mathbb{Q}$.

In [Ho 2] Honda has obtained a relation between formal Jacobians of modular curves and Dirichlet series involving Hecke operators. For certain curves this also follows from our results on abelian varieties with real multiplication. In fact in these cases we obtain more precise information because we deal with bad reduction primes as well. As an illustration we determine the formal Néron model over $\mathbb{Z}$ of $J_0(N)^{\text{new}}$ for squarefree N in terms of Dirichlet series.

Apart from the cases mentioned there is one other instance where a relation between a formal group scheme and an L-series in the spirit of (0.1) is known. This is in the work of Oda [O] on Artin–Mazur formal groups of fibre products of universal elliptic curves.

Theorem (0.1) is essentially equivalent to the Atkin Swinnerton–Dyer congruences for the coefficients of $L(E, s)$ e.g. [Ha]. Using crystalline techniques such congruences can be obtained in a much more general context. We refer to Stienstra [St] for results and references in this direction.

Some work on this note was done during a stay at the Max-Planck-Institute für Mathematik in Bonn whose hospitality is gratefully acknowledged.

1. Algebraic tori

To construct formal groups from matrix valued L-series we will need certain results of Honda [Ho 2] which are summarized in the following theorem. For a finite subset S of Spec $\mathbb{Z}$ we write $\mathbb{Z}_S$ for the ring obtained from $\mathbb{Z}$ by inverting the primes in S.

(1.1) THEOREM. *For integers r, $d \geq 1$ consider the formal Dirichlet series*

$$\sum_{n=1}^{\infty} A_n n^{-s} = \prod_p (I_d + C_p p^{-s} + \cdots + p^{r-1} C_{p^r} p^{-rs})^{-1}$$

where the matrices C_{pm} in $M_d(\mathbb{Z})$ are assumed to commute with each other for all p, m. Put

$$f(X) = \sum_{n=1}^{\infty} \frac{1}{n} A_n X^n \quad \text{in } \mathbb{Q}[\![X_1, \ldots, X_d]\!]^d,$$

where X^n is the transposed of $(X_1^n, \ldots, X_d^n)$. Then

$$F(X, Y) = f^{-1}(f(X) + f(Y))$$

is a d-dimensional commutative formal group law defined over $\mathbb{Z}$. The endomorphisms

$$[C_{pm}]_F(X) := f^{-1}(C_{pm} f(X))$$

of F are also defined over $\mathbb{Z}$ and for all p the Frobenius endomorphism $\tilde{\pi}(X) = X^p$ of $F \otimes \mathbb{F}_p$ satisfies the relation:

$$(1.2) \quad p\, \mathrm{id}_{F \otimes \mathbb{F}_p} + \sum_{m=1}^{r} [C_{pm}]_{F \otimes \mathbb{F}_p} \tilde{\pi}^m = 0 \quad \text{in } \mathrm{End}\,(F \otimes \mathbb{F}_p).$$

If $H(X, Y)$ is another d-dimensional formal group law over $\mathbb{Z}_S$ satisfying (1.2) for all $p \notin S$ then F and H are strongly isomorphic over $\mathbb{Z}_S$.

Let T be an algebraic torus of dimension d over $\mathbb{Q}$ with character group $X(T) = \mathrm{Hom}_{\mathbb{Q}}(T_{\mathbb{Q}}, \mathbb{G}_{m,\mathbb{Q}})$ and associated galois representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{Aut}\,(X(T)) \cong GL_d(\mathbb{Z}).$$

It is explained in [Ra] that T has a Néron model $\mathscr{T}$ over $\mathbb{Z}$. This is a smooth, separated commutative group scheme with generic fibre T such that for all smooth schemes $\mathscr{S}$ over $\mathbb{Z}$ we have an isomorphism

$$\mathrm{Mor}_{\mathbb{Z}}(\mathscr{S}, \mathscr{T}) \xrightarrow{\sim} \mathrm{Mor}_{\mathbb{Q}}(\mathscr{S}_{\mathbb{Q}}, T) \quad \text{via } f \mapsto f_{\mathbb{Q}}.$$

The connected component $\mathscr{T}^0$ of $\mathscr{T}$ is of finite type over $\mathbb{Z}$.

By definition the good primes for T are those where the reduction of $\mathscr{T}^0$ is a torus or equivalently where the representation of $G_{\mathbb{Q}}$ on $X(T)$ is unramified. There is a non-empty open subset U of Spec $\mathbb{Z}$ where T has good reduction and $\mathscr{T}^0 \times_{\mathbb{Z}} U$ is a torus over U. These remarks follow from [Gl] Theorem (5.16), Corollary (1.2) and the fact that the formation of $\mathscr{T}^0$ commutes with étale base change. The matrix commuting condition in Honda's theorem (1.1) being unavoidable we will have to restrict our attention to abelian tori T i.e. with $\operatorname{Im}\rho$ commutative. Let K be the finite abelian splitting field of T corresponding to $\operatorname{Ker}\rho$ and denote by $G \cong \operatorname{Im}\rho$ its galois group. It is known [C–R] (79.12) that there are only finitely many isomorphism classes of $\mathbb{Z}[G]$-modules which are free of rank d over $\mathbb{Z}$. In particular we conclude:

(1.3) There is a finite set of primes S depending only on G and d such that for any two modules Γ, Γ' as above we have:

$$\Gamma \otimes \mathbb{Q} \overset{G}{\cong} \Gamma' \otimes \mathbb{Q} \quad \text{iff } \Gamma \otimes \mathbb{Z}_S \overset{G}{\cong} \Gamma' \otimes \mathbb{Z}_S.$$

For $d = 1$ we can take $S = \emptyset$.

(1.4) Fixing a basis $\chi_1, \ldots, \chi_d$ of $X(T)$ as a $\mathbb{Z}$-module we can associate matrices A_p in $GL_d(\mathbb{Z})$ to the galois Frobenius σ_p in G for every prime p where T has good reduction. According to (1.1) the L-series

$$\sum_{n=1}^{\infty} A_n n^{-s} = \prod_{p \text{ good}} (I_d - A_p p^{-s})^{-1}$$

leads to a d-dimensional formal group law $\hat{L}$ defined over $\mathbb{Z}$. Different bases of $X(T)$ induce isomorphic (but not strongly isomorphic) group laws $\hat{L}$.

Let S_{bad} be the set of primes p where T has bad reduction and $S'_{\text{bad}} \subset S_{\text{bad}}$ the subset of primes such that $\mathscr{T}^0 \otimes \mathbb{F}_p$ is not isomorphic to $\mathbb{G}_a^d$.

(1.5) THEOREM. *Let $\hat{\mathscr{T}}$ be the completion of $\mathscr{T}$ along the zero section. If $S \supset S'_{bad}$ satisfies* (1.7) *below there is an isomorphism*

$$\hat{\mathscr{T}} \otimes \mathbb{Z}_S \cong \hat{L} \otimes \mathbb{Z}_S$$

of formal groups over $\mathbb{Z}_S$. Possible choices for S are $S = S_{\text{bad}}$ or any $S \supset S'_{\text{bad}}$ for which (1.3) *holds.*

EXAMPLE. For a one-dimensional algebraic torus T over $\mathbb{Q}$ we can take for S the empty set and $\hat{L}$ is obtained from the ordinary Artin L-series $L(\rho, s)$. In the non-split case $L(\rho, s)$ is the Dirichlet L-series of the corresponding quadratic extension $K/\mathbb{Q}$ and it is the Riemann zeta function if $T = \mathbb{G}_m$. By (1.5) we have $\hat{\mathscr{T}} \cong \hat{L}$ over $\mathbb{Z}$. It is not difficult to show directly that $\hat{\mathscr{T}} \otimes \mathcal{O}_K \cong X + Y + \sqrt{d_K}XY$ and hence we find an isomorphism of formal group laws $\hat{L} \otimes \mathcal{O}_K \cong X + Y + \sqrt{d_K}\,XY$. In fact according to Honda (0.2) there is even a strong isomorphism between these two group laws but such a statement does not seem to generalize well to $d > 1$.

Proof of (1.5). Since G is abelian $\rho(\sigma)$ is an automorphism of $X(T)$ as a galois module for every $\sigma \in G$. Hence it induces an automorphism V_σ of T and by the universal property of the Néron model, automorphisms, V_σ of $\mathcal{T}$, $\mathcal{T}^0$ and $T_p = \mathcal{T}^0 \otimes \mathbb{F}_p$. If p is a good reduction prime for T and if π denotes the Frobenius endomorphism of T_p we have

$$(1.6) \quad \pi V_{\sigma_p} = V_{\sigma_p} \pi = p \quad \text{i.e. } V_{\sigma_p} \text{ is the Verschiebung on } T_p.$$

To prove this, observe that T_p is the torus associated to the representation $G_{\mathbb{F}_p} \to \operatorname{Aut}(X(T))$ induced by ρ and V_{σ_p} is the automorphism of T_p corresponding to the $G_{\mathbb{F}_p}$-map $\rho(\sigma_p)$. If Q_p is a Hopf algebra for T_p, $X(T_p) = X(T)$ is isomorphic to the $G_{\mathbb{F}_p}$-module of the group like elements of $Q_p \otimes_{\mathbb{F}_p} \overline{\mathbb{F}}_p$. If $\chi = \Sigma_i a_i \otimes \lambda_i$ is such an element, we have:

$$\pi V_{\sigma_p}(\chi) = \pi\left(\sum_i a_i \otimes \lambda_i^p\right) = \sum_i a_i^p \otimes \lambda_i^p = \chi^p = V_{\sigma_p}\pi(\chi).$$

For a group scheme $\mathcal{H}$ over a ring R with zero section e we write

$$\omega_{\mathcal{H}/R} = H^0(\operatorname{Spec} R, \mathcal{J}/\mathcal{J}^2)$$

where $\mathcal{J}$ is the sheaf of ideals corresponding to the closed immersion e. If $\mathcal{H} = \operatorname{Spec} Q$ is affine and I is the augmentation ideal of Q we have $\omega_{\mathcal{H}/R} = I/I^2$.

Since $\mathcal{T}^0$ is smooth of finite type over $\mathbb{Z}$ the group $\omega_{\mathcal{T}^0/\mathbb{Z}}$ is $\mathbb{Z}$-free of rank d. It becomes a G-module by letting $\sigma \in G$ act via the automorphism V_σ^* induced by V_σ. Now let $S \supset S'_{\text{bad}}$ be a finite set of primes such that there exists a $\mathbb{Z}_S[G]$-isomorphism

$$(1.7) \quad X(T) \otimes \mathbb{Z}_S \cong \omega_{\mathcal{T}^0/\mathbb{Z}} \otimes \mathbb{Z}_S.$$

Under this isomorphism the above basis $\chi_1, \ldots, \chi_d$ of $X(T)$ determines a basis $\xi_1, \ldots, \xi_d$ of the free $\mathbb{Z}_S$-module $\omega_{\mathcal{T}^0 \otimes \mathbb{Z}_S/\mathbb{Z}_S} = \omega_{\mathcal{T}^0/\mathbb{Z}} \otimes \mathbb{Z}_S$ and hence an isomorphism

$$\hat{\mathcal{T}} \otimes \mathbb{Z}_S \cong \operatorname{Spf} \mathbb{Z}_S[\![X]\!]$$

where $X = (X_1, \ldots, X_d)$ (e.g. [SGA 1] Exp. II). Let $H(X, Y) \in \mathbb{Z}_S[\![X, Y]\!]^d$ be the corresponding formal group law and $h(X) \in \mathbb{Q}[\![X]\!]^d$ its logarithm. An endomorphism $\alpha(X) \in \mathbb{Z}_S[\![X]\!]^d$ of $H(X, Y)$ is determined by its linear component:

$$\alpha(X) \equiv AX \bmod (\deg 2) \quad \text{implies } \alpha(X) = [A]_H = h^{-1}(Ah(X)).$$

The automorphism V_{σ_p} of $\mathscr{T}^0 \otimes \mathbb{Z}_S$ induces an automorphism of $\hat{\mathscr{T}} \otimes \mathbb{Z}_S$ which as an automorphism of H is the formal power series:

$$V_p(X) = h^{-1}(A_p h(X)) \quad \text{with } A_p \text{ as in (1.4).}$$

In fact the linear component of $V_p(X)$ is determined by the action of σ_p on the $\mathbb{Z}_S$-basis $\xi_1, \dots, \xi_d$ of $\omega_{\mathscr{T}^0 \otimes \mathbb{Z}_S/\mathbb{Z}_S}$. By the above this action is identified with the one of $\rho(\sigma)$ on $\chi_1, \dots, \chi_d$. Since V_{σ_p} is a lifting of Verschiebung on T_p by (1.6), we have:

$$p \operatorname{id}_{H \otimes \mathbb{F}_p} - [A_p]_H \hat{\pi} = 0.$$

If p is a prime of bad reduction such that $\mathscr{T}^0 \otimes \mathbb{F}_p \cong \mathbb{G}_a^d$, we have $\hat{\mathscr{T}} \otimes \mathbb{F}_p \cong \hat{\mathbb{G}}_a^d$ and hence $p \operatorname{id}_{H \otimes \mathbb{F}_p} = 0$. Now the first assertion of the theorem follows from Honda's theorem (1.1).

(1.8) It remains to show that for the two choices of S described in the theorem there is a $\mathbb{Z}_S[G]$-isomorphism (1.7). To abbreviate we set $S = S_{\text{bad}}$ and $\mathcal{O} = \mathcal{O}_K \otimes \mathbb{Z}_S$ in the following, where $\mathcal{O}_K$ is the ring of integers in K. Then $\mathcal{O}/\mathbb{Z}_S$ is an étale extension which trivializes the torus $\mathscr{T}^0 \otimes \mathbb{Z}_S$ i.e. $\mathscr{T}^0 \otimes \mathcal{O} \cong \mathbb{G}_{m,\mathcal{O}}^d$.

Let us write $\mathscr{T}^0 \otimes \mathbb{Z}_S = \operatorname{Spec} Q$ for a Hopf algebra Q over $\mathbb{Z}_S$ with augmentation ideal I. Then the Hopf algebra $Q \otimes \mathcal{O}$ for $\mathscr{T}^0 \otimes \mathcal{O}$ has augmentation ideal $I_{\mathcal{O}} = I \otimes \mathcal{O}$. We identify $X(T) = \operatorname{Hom}_{\mathcal{O}}(\mathscr{T}^0 \otimes \mathcal{O}, \mathbb{G}_{m,\mathcal{O}})$ with the set of group like elements in $Q \otimes \mathcal{O}$. By mapping $\chi \otimes 1$ to $(\chi - 1) \bmod I_{\mathcal{O}}^2$ we obtain a canonical $\mathcal{O}$-linear isomorphism compatible with the two G-actions indicated below:

$$\begin{array}{lll}
(1.9) & X(T) \otimes \mathcal{O} \xrightarrow{\sim} I_{\mathcal{O}}/I_{\mathcal{O}}^2 = & \omega_{\mathscr{T}^0/\mathbb{Z}} \otimes \mathcal{O} \\
(I) & \rho(\sigma) \otimes \mathrm{id} & V_\sigma^* \otimes \mathrm{id} \\
(II) & \rho(\sigma) \otimes \sigma & \mathrm{id} \otimes \sigma.
\end{array}$$

That (1.9) is an isomorphism needs only be checked for $\mathbb{G}_{m,\mathcal{O}}$ where it is obvious. In a context where G operates via (I) resp. (II) we write G_I resp. G_{II} for G to indicate the action.

Using [C–R] Theorem (29.11) we obtain from (1.9) a non-canonical $\mathbb{Q}[G_I]$-isomorphism

$$X(T) \otimes \mathbb{Q} \cong \omega_{\mathscr{T}^0/\mathbb{Z}} \otimes \mathbb{Q}$$

and hence for all S' as in (1.3) a $\mathbb{Z}_{S'}[G_I]$-isomorphism (1.7). It remains to establish (1.7) for S. Taking fixed modules under G_{II} in (1.9) we get a canonical $\mathbb{Z}_S[G_I]$-isomorphism:

$$(1.10) \quad (X(T) \otimes \mathcal{O})^{G_{II}} \xrightarrow{\sim} \omega_{\mathscr{T}^0/\mathbb{Z}} \otimes \mathbb{Z}_S$$

because $\omega_{\mathscr{T}^0/\mathbb{Z}}$ is $\mathbb{Z}$-free.

The work of Leopoldt [L] (see also [J]) shows that $\mathcal{O}_K$ is free of rank one over the order in $\mathbb{Q}[G]$ generated by $\mathbb{Z}[G]$ and the idempotents

$$e_H = \frac{1}{|H|} \sum_{\sigma \in H} \sigma$$

where H runs over the higher ramification groups of the prime ideals in $\mathcal{O}_K$. In particular we see that $\mathcal{O} = \mathbb{Z}_S[G] \cdot \theta$ freely for some $\theta \in \mathcal{O}$. Thus $(X(T) \otimes \mathcal{O})^{G_{II}}$ consists of the elements $\Sigma_{\sigma \in G} \chi^\sigma \otimes \theta^\sigma$ with $\chi \in X(T) \otimes \mathbb{Z}_S$ and hence we obtain a $\mathbb{Z}_S[G_I]$-isomorphism

$$\mathrm{Tr}_\theta : X(T) \otimes \mathbb{Z}_S \xrightarrow{\sim} (X(T) \otimes \mathcal{O})^{G_{II}}$$

by setting $\mathrm{Tr}_\theta(\chi \otimes 1) = (\Sigma_{\sigma \in G_{II}} \sigma)(\chi \otimes \theta)$.

Composing with (1.10) we obtain the remaining assertion.

2. Abelian varieties with real multiplication

In this section we will show that there is a generalization of the Cartier Honda theorem (0.1) to a suitable class of abelian varieties of higher dimension. To be specific let A be an abelian variety over $\mathbb{Q}$ of dimension g and let End A be its ring of endomorphisms over $\mathbb{Q}$. We assume there is a homomorphism mapping 1 to id

$$\theta : F \to \mathrm{End}^0 A = (\mathrm{End}\, A) \otimes \mathbb{Q}$$

where F is a totally real number field of degree $g = [F : \mathbb{Q}]$. A more general situation will be considered in (2.7) below.

We recall the definition of the relevant motivic L-series. For a prime p let I_p be an inertia group at p in $G_{\mathbb{Q}}$ and σ_p an arithmetic Frobenius in the corresponding decomposition group. For a prime $l \neq p$ we have a decomposition:

$$F_l = F \otimes \mathbb{Q}_l = \prod_{\mathfrak{l} \mid l} F_{\mathfrak{l}}$$

of F_l into the product of the completions $F_{\mathfrak{l}}$ of F at the primes $\mathfrak{l}$ in F dividing l. Using the $\mathfrak{l}$-adic cohomology groups of A

$$H^1_{\mathfrak{l}}(A) = H^1_{\acute{e}t}(A_{\bar{\mathbb{Q}}}, \mathbb{Q}_l) \otimes_{F_l} F_{\mathfrak{l}}$$

the local L-factor at p relative to F is defined by

$$L_p(A, F, s) = \det_{F_{\mathfrak{l}}}(1 - p^{-s}(\sigma_p^{-1})^* \mid H^1_{\mathfrak{l}}(A)^{I_p})^{-1}.$$

Its inverse is a polynomial with coefficients in $\mathcal{O}_F$ which is independent of $l \neq p$ and $\mathfrak{l} \mid l$. For the good reduction primes this is proved in [Sh 2] (11.10.1). For the primes of bad reduction see below, where it is also shown more precisely that for all p

$$(2.1)\quad L_p(A, F, s) = (1 - c_p p^{-s} + p c_{p^2} p^{-2s})^{-1}$$

with $c_p \in \mathcal{O}_F$ and $c_{p^2} = 0$ or 1.

Consider the order $\mathcal{O}_A = \theta^{-1}(\mathrm{End}\, A)$ in $\mathcal{O}_F$ and let

$$R : \mathcal{O}_A \to M_g(\mathbb{Z})$$

be any faithful representation of $\mathcal{O}_A$ by integral $g \times g$-matrices. If all c_p lie in $\mathcal{O}_A$ we define $C_p = R(c_p)$ and $C_{p^2} = R(c_{p^2})$. Then the formal Dirichlet series

$$\sum_{n=1}^{\infty} A_n n^{-s} = \prod_p (I_g - C_p p^{-s} + p C_{p^2} p^{-2s})^{-1}$$

satisfies the conditions of Honda's theorem (1.1) and we obtain a g-dimensional formal group law $\hat{L}$ over $\mathbb{Z}$.

We refer to [G 2] for the relevant facts on the Néron model $\mathscr{A}/\mathbb{Z}$ of A. For a prime p we denote by T_p the maximal subtorus of $\mathscr{A}_p = \mathscr{A} \otimes \mathbb{F}_p$ and by B_p, U_p the uniquely determined abelian variety and (smooth connected) unipotent group scheme over $\mathbb{F}_p$ fitting into an exact sequence

$$0 \to U_p \to \mathscr{A}_p^0 / T_p \to B_p \to 0.$$

By the universal property of the Néron model we have a map also called θ given by composition

$$\theta : F \to \mathrm{End}^0 A \to \mathrm{End}^0 \mathscr{A}_p^0.$$

Let S'_{bad} be the set of primes p such that $\dim U_p = g$ and U_p is not isomorphic over $\mathbb{F}_p$ to $\mathbb{G}_a^g$. Choose a finite set of primes S_{pr} such that $\mathcal{O}_A \otimes \mathbb{Z}_{S_{\mathrm{pr}}}$ is a principal ring.

(2.2) THEOREM. *Assume that $c_p \in \mathcal{O}_A$ for all p, e.g. $\mathcal{O}_A = \mathcal{O}_F$.*
(*a*) *Setting $S = S_{\mathrm{pr}} \cup S'_{\mathrm{bad}}$ there is an isomorphism of formal groups over $\mathbb{Z}_S$*

$$\hat{\mathscr{A}} \otimes \mathbb{Z}_S \cong \hat{L} \otimes \mathbb{Z}_S.$$

(*b*) *If R is the representation*

$$\mathcal{O}_A \to \mathrm{End}\,(\omega_{\mathscr{A}^0/\mathbb{Z}})$$

induced by θ it suffices to take $S = S'_{\mathrm{bad}}$ in (*a*).

Remark. For an elliptic curve E over $\mathbb{Q}$ taking $F = \mathbb{Q}$ we obtain $\hat{\mathscr{E}} \cong \hat{L}$ i.e. (0.1).

For the proof of the theorem we have to consider the reduction types of A and the relation between $L_p(A, F, s)$ and the Frobenius endomorphism π of $\mathscr{A}_p^0$. The situation is summarized in the following proposition.

(2.3) PROPOSITION. *The reduction $\mathscr{A}_p^0$ is equal to U_p, T_p or B_p according to $\dim_{F_\mathfrak{l}} H^1_\mathfrak{l}(A)^{I_p} = 0$, 1 or 2. In case $\mathscr{A}_p^0$ is a torus, it is either isomorphic to $\mathbb{G}_m^g$ or to $\mathbb{G}_m^*$ the only g-dimensional torus over $\mathbb{F}_p$ with Verschiebung acting by -1. Moreover*

$$P(X) = \det_{F_\mathfrak{l}}(1 - X(\sigma_p^{-1})^* \mid H^1_\mathfrak{l}(A)^{I_p}) = \begin{cases} 1 - c_pX + pX^2 & \textit{if } \mathscr{A}_p^0 = B_p \\ 1 - X & \textit{if } \mathscr{A}_p^0 = \mathbb{G}_m^g \\ 1 + X & \textit{if } \mathscr{A}_p^0 = \mathbb{G}_m^* \\ 1 & \textit{if } \mathscr{A}_p^0 = U_p \end{cases}$$

with c_p in $\mathcal{O}_F$ independent of $l \neq p$ and $\mathfrak{l}|l$ and such that $\theta(c_p) \in \mathrm{End}\,\mathscr{A}_p^0$. If we set

$$P(X) = 1 - c_pX + pc_{p^2}X^2$$

then for $p \notin S'_{\mathrm{bad}}$ the relation

$$p\,\mathrm{id} - \theta(c_p)\pi + \theta(c_{p^2})\pi^2 = 0$$

holds in $\mathrm{End}\,(\mathscr{A}_p^0)$.

Proof. We set $V_l(A) = (T_l A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ and $V_\mathfrak{l}(A) = V_l(A) \otimes_{F_l} F_\mathfrak{l}$ and similarly for $\mathscr{A}_p^0$. According to [G 2] Proposition 2.2.5 there is an isomorphism

$$V_l(A)^{I_p} \cong V_l(\mathscr{A}_p^0)$$

and hence an isomorphism of $F_\mathfrak{l}$-vector spaces

$$V_\mathfrak{l}(A)^{I_p} \cong V_\mathfrak{l}(\mathscr{A}_p^0).$$

The action of σ_p on the left corresponds to the action of $V_\mathfrak{l}(\pi)$ on the right.

(2.4) First we assume that p is a prime of good reduction i.e. $\mathscr{A}_p^0 = B_p$. For any abelian variety A with multiplication by a number field F it is known that $[F : \mathbb{Q}]$ divides $2 \dim A$ and that equality implies F is a CM field. Hence B_p is isotypical i.e. isogenous to a power of a simple abelian variety over $\mathbb{F}_p$. According to [T] Theorem 1 the center of $\mathrm{End}^0 B_p$ is thus given by $\mathbb{Q}(\pi)$.

Due to good reduction

$$H_\mathfrak{l}^1(A) = \mathrm{Hom}\,(V_l(A), \mathbb{Q}_l) \otimes_{F_l} F_\mathfrak{l}$$
$$= \mathrm{Hom}\,(V_\mathfrak{l}(B_p), \mathbb{Q}_l)$$

and hence

$$P(X) = \det_{F_\mathfrak{l}}(1 - V_\mathfrak{l}(\pi)X \mid V_\mathfrak{l}(B_p)).$$

We distinguish two cases:

(2.4.1) $\pi \notin \theta(F) = F$. Then $(F(\pi) : F) = 2$ and $F(\pi)$ is a CM field. The minimal polynomial of π over F is $Q(X) = X^2 - c_p X + p$ with $c_p = \pi + \bar{\pi} \in (\mathrm{End}\, B_p) \cap F \subset \mathcal{O}_F$, since $\pi\bar{\pi} = p$ by a result of Weil. Let $\mathrm{End}_F^0(B_p)$ be the centralizer of F in $\mathrm{End}^0 B_p$. The $\mathbb{Q}$-algebra map

$$\mathrm{End}_F^0(B_p) \to \mathrm{End}_{F_\mathfrak{l}}(V_\mathfrak{l}(B_p))$$

maps π to $V_\mathfrak{l}(\pi)$ and hence $Q(V_\mathfrak{l}(\pi)) = 0$. According to Shimura [Sh 2] (11.10.1) the characteristic polynomial

$$\det_{F_\mathfrak{l}}(X\,\mathrm{id} - V_\mathfrak{l}(\pi) \mid V_\mathfrak{l}(B_p)) = X^2 P(X^{-1})$$

has degree two and coefficients in F. Since it annihilates $V_{\mathrm{I}}(\pi)$ and since Q is irreducible over F we find

$$P(X) = 1 - c_p X + pX^2.$$

(2.4.2) $\pi \in \theta(F)$. Since F is totally real we have $\pi^2 = p$. Moreover $V_{\mathrm{I}}(\pi) \in F \subset F_{\mathrm{I}}$ and hence

$$P(X) = (1 - V_{\mathrm{I}}(\pi)X)^2 = 1 - c_p X + pX^2$$

where $c_p = 2\pi \in \mathcal{O}_F$. On the other hand $Q(X) = X^2 - c_p X + p$ annihilates π in $\mathrm{End}^0 B_p$.

(2.5) Now assume that $T_p \neq 0$. Since T_p is the uniquely determined maximal torus of $\mathscr{A}_p^0$ we have a homomorphism

$$F \to \mathrm{End}^0 \mathscr{A}_p^0 \to \mathrm{End}^0 T_p.$$

Let $X(T_p)$ be the character group of T_p with galois action

$$\rho : G_{\mathbb{F}_p} \to \mathrm{Aut}\,(X(T_p)) \cong GL_\mu(\mathbb{Z})$$

where $\mu = \dim T_p \leq g$ is the reductive rank of $\mathscr{A}_p$. Since $T_p \neq 0$ we get an embedding of F into $M_\mu(\mathbb{Q})$ hence $\mu = g$ i.e. $\mathscr{A}_p^0 = T_p$ and F is a maximal subfield of $M_\mu(\mathbb{Q})$. If $\bar{\sigma}_p$ denotes a topological generator of $G_{\mathbb{F}_p}$ the matrix $\rho(\bar{\sigma}_p)$ has finite order and commutes with F. Hence $\rho(\bar{\sigma}_p)$ is a root of unity in the totally real field F i.e. $c_p := \rho(\bar{\sigma}_p) = \pm 1$. As in (1.6) we see that Verschiebung on T_p is multiplication by c_p i.e.

$$p\,\mathrm{id} - c_p \pi = 0 \quad \text{in } \mathrm{End}\,(\mathscr{A}_p^0).$$

It remains to show that $P(X) = 1 - c_p X$.

Choosing an $\mathcal{O}_A$-linear polarization of A over $\mathbb{Q}$ (see [R] 1.12) we obtain F_l-linear isomorphisms

$$H^1(A_{\bar{\mathbb{Q}}}, \mathbb{Q}_l) = V_l(A')(-1) \cong V_l(A)(-1)$$

where A' is the dual abelian variety. Since I_p acts trivially on $\mathbb{Q}_l(-1)$ for $l \neq p$ this implies

$$H^1(A_{\bar{\mathbb{Q}}}, \mathbb{Q}_l)^{I_p} = V_l(A)^{I_p}(-1) = V_l(\mathscr{A}_p^0)(-1) = (X(T_p) \otimes_{\mathbb{Z}} \mathbb{Q}_l)^*$$

a free rank one F_l-module because $X(T_p) \otimes \mathbb{Q}$ is a one dimensional F-vector space. The action of $(\sigma_p^{-1})^*$ on the left corresponds to the action by c_p on the right hence the assertion.

(2.6) If $T_p = 0$ the group scheme $\mathscr{A}_p^0$ is an extension of B_p by U_p. Since there is no nontrivial (algebraic) homomorphism from U_p to B_p (e.g. [Ro] Th. 11) we obtain a homomorphism $F \to \mathrm{End}^0 B_p$. If $B_p \neq 0$ this implies $\dim B_p = g$ i.e. $\mathscr{A}_p^0 = B_p$ since F is not a CM field. Thus the only remaining case is $\mathscr{A}_p^0 = U_p$. Since

$$H^1(A_{\mathbb{Q}}, \mathbb{Q}_l)^{I_p} = V_l(U_p)(-1) = 0$$

we find $P(X) = 1$. Moreover $p \,\mathrm{id} = 0$ in $\mathrm{End}\,(\mathscr{A}_p^0)$ if $U_p \cong \mathbb{G}_a^g$ (in fact "iff").

Proof of (2.2). We only consider (a). The proof of (b) is even simpler. Since $\mathscr{A}^0$ is smooth of finite type over $\mathbb{Z}$ the group $\omega_{\mathscr{A}^0/\mathbb{Z}}$ is $\mathbb{Z}$-free of rank g. It is naturally an $\mathcal{O}_A$-module. By the choice of S_{pr} the ring $\mathcal{O}_A \otimes \mathbb{Z}_{S_{\mathrm{pr}}}$ is principal and hence there is an isomorphism of $\mathcal{O}_A \otimes \mathbb{Z}_S$-modules

$$\omega_{\mathscr{A}^0 \otimes \mathbb{Z}_S/\mathbb{Z}_S} = \omega_{\mathscr{A}^0/\mathbb{Z}} \otimes \mathbb{Z}_S \cong \mathbb{Z}_S^g$$

where $\mathcal{O}_A \otimes \mathbb{Z}_S$ operates on the right by the representation R chosen at the beginning of the section. Using the basis of $\omega_{\mathscr{A}^0 \otimes \mathbb{Z}_S/\mathbb{Z}_S}$ corresponding to the canonical basis of $\mathbb{Z}_S^g$ we obtain an isomorphism

$$\hat{\mathscr{A}} \otimes \mathbb{Z}_S \cong Spf \mathbb{Z}_S[\![X]\!]$$

where $X = (X_1, \dots, X_g)$. This determines a formal group law $H(X, Y)$ for $\mathscr{A}^0 \otimes \mathbb{Z}_S$ over $\mathbb{Z}_S$. Any $c \in \mathcal{O}_A$ induces an endomorphism of $\hat{\mathscr{A}}$ and hence of $H(X, Y)$ whose linear component is determined by the action on $\omega_{\mathscr{A}^0 \otimes \mathbb{Z}_S/\mathbb{Z}_S}$. As an endomorphism of $H(X, Y)$ it is therefore represented by the formal power series $h^{-1}(R(c)h(X))$ where h is the logarithm of H. According to (2.3) we have for $p \notin S'_{\mathrm{bad}}$

$$p \,\mathrm{id} - \theta(c_p)\pi + \theta(c_{p^2})\pi^2 = 0 \quad \text{in End}\,(\mathscr{A}_p^0).$$

Using this and the assumption $c_p \in \mathcal{O}_A$ we get

$$p \,\mathrm{id}_{H \otimes \mathbb{F}_p} - [C_p]\hat{\pi} + [C_{p^2}]\hat{\pi}^2 = 0 \quad \text{in End}\,(H \otimes \mathbb{F}_p)$$

where $\hat{\pi}(X) = X^p$. Now the assertion follows from Honda's theorem (1.1).

(2.7) In this section we consider a slightly more general situation which is useful for an application to modular forms. Let A be an abelian variety over $\mathbb{Q}$ which admits an embedding θ of a commutative semisimple $\mathbb{Q}$-algebra F with $\dim_{\mathbb{Q}} F = \dim A = g$ into $\mathrm{End}^0 A$. If e runs over the primitive idempotents of F the algebra F decomposes into the product of the fields $F_e = eF$. We assume that they are totally real. Up to isogeny A decomposes into a product of abelian varieties A_e over $\mathbb{Q}$ and we have injections of F_e into $\mathrm{End}^0 A_e$. Since $g_e = \dim A_e$ divides $[F_e : \mathbb{Q}]$ we obtain equality $g_e = [F_e : \mathbb{Q}]$. We define the local Euler factor of A with respect to F by

$$L_p(A, F, s) = (L_p(A_e, F_e, s)) \quad \text{in } F[\![p^{-s}]\!].$$

Because of (2.3) it has the form

$$L_p(A, F, s) = (1 - c_p p^{-s} + p c_{p^2} p^{-2s})^{-1}$$

with c_p, c_{p^2} in $\mathcal{O}_F = \prod_e \mathcal{O}_{F_e}$ the maximal order in F. If $c_p, c_{p^2} \in \mathcal{O}_A$ then as before a faithful representation

$$R : \mathcal{O}_A \to M_g(\mathbb{Z})$$

of the order $\mathcal{O}_A = \theta^{-1}(\mathrm{End}\, A)$ gives rise to a g-dimensional formal group law $\hat{L}$ over $\mathbb{Z}$. Let S_{uni} be the set of primes where A does not have semistable reduction and choose a finite set S_{pr} of primes such that $\mathcal{O}_A \otimes \mathbb{Z}_{S_{\mathrm{pr}}}$ is a product of principal rings.

(2.8) THEOREM. *Assume that* $c_p, c_{p^2} \in \mathcal{O}_A$ *for all* $p \notin S_{\mathrm{uni}}$.
(*a*) *Setting* $S = S_{\mathrm{pr}} \cup S_{\mathrm{uni}}$ *there is an isomorphism of formal groups over* $\mathbb{Z}_S$

$$\hat{\mathscr{A}} \otimes \mathbb{Z}_S \cong \hat{L} \otimes \mathbb{Z}_S.$$

(*b*) *If R is the representation*

$$\mathcal{O}_A \to \mathrm{End}\,(\omega_{\mathscr{A}^0/\mathbb{Z}})$$

induced by θ *it suffices to take* $S = S_{\mathrm{uni}}$ in (*a*).

REMARK. The only case where the assumption $c_p, c_{p^2} \in \mathcal{O}_A$ is obvious is for $\mathcal{O}_A = \mathcal{O}_F$. However in this case A decomposes up to *isomorphism* into the product of the abelian varieties $A_e = eA$ and the assertion of (2.8) follows immediately from (2.2).

In the corollary below we will give an example though where the conditions can be checked in a non-trivial case.

Proof of (2.8). We proceed as in the proof of (2.2). Observe that if $\mathbb{Z}_{S_{\mathrm{pr}}}^{g}$ has a faithful $\Lambda = \mathcal{O}_A \otimes \mathbb{Z}_{S_{\mathrm{pr}}}$-operation it is free of rank one over Λ. Hence $\omega_{\mathscr{A}^0 \otimes \mathbb{Z}_S/\mathbb{Z}_S}$ and $\mathbb{Z}_S^g$ with operation via R are isomorphic over Λ. It now suffices to show that the relation

$$(2.9) \quad p \;\mathrm{id} - \theta(c_p)\pi + \theta(c_{p^2})\pi^2 = 0$$

holds in End $(\mathscr{A}_p^0)$. This is deduced from (2.3) as follows:

Choose $N \geq 1$ such that $Ne \in \mathcal{O}_A$ for all e and set $\varphi_e = \theta(Ne)$. The image A_e of φ_e is an abelian subvariety of A which has real multiplication by the field F_e. There are isogenies with $\varphi\psi = N$ and $\psi\varphi = N$

$$A \underset{\psi}{\overset{\varphi}{\rightleftarrows}} A' = \prod_e A_e$$

given by $\varphi = (\varphi_e)$ and $\psi =$ summation map restricted to A'. Applying Proposition (2.3) to each A_e we find for $p \notin S_{\mathrm{uni}}$ the relation

$$p \;\mathrm{id}_{A'} - \theta'(c_p)\pi_{A'} + \theta'(c_{p^2})\pi_{A'}^2 = 0 \quad \text{in End} \, (\mathscr{A}_p'^{0})$$

where $\theta' = (\theta_e)$ and $\mathscr{A}'$ is the Néron model of A'. Applying ψ to the left and φ to the right in this equation we obtain

$$N(p \;\mathrm{id}_A - \theta(c_p)\pi + \theta(c_{p^2})\pi^2) = 0 \quad \text{in End} \, (\mathscr{A}_p^0).$$

Since $\mathscr{A}_p^0$ is an extension of an abelian variety by a torus, End $(\mathscr{A}_p^0)$ is torsionfree and (2.9) follows.

We now give an application of (2.8) to modular forms. For background we refer to [Ri] and [Sh 1]. Let $N \geq 1$ be a squarefree integer and let $A = J_0(N)^{\mathrm{new}}$ be the new part of the modular variety $J_0(N)$ over $\mathbb{Q}$ associated with $\Gamma_0(N)$. Then A has semistable reduction for all primes p. Let $\mathbf{T}$ be the subring of End A generated by the Hecke operators T_p for $p \nmid N$ and by the Atkin–Lehner operators U_p for $p \mid N$. It is known that $F = \mathbf{T} \otimes \mathbb{Q} = \mathrm{End}^0 A$ decomposes into a product of totally real fields F_e and $\dim_{\mathbb{Q}} F = \dim A$. At all primes the factors A_e have the same reduction type i.e. good or multiplicative since the abelian varieties attached to newforms have bad reduction exactly at the primes dividing N. For $p \nmid N$ using

(2.4) we find:

$$c_p = (\pi_e + \bar{\pi}_e) \in \prod_e \operatorname{End} (\mathscr{A}_e)_p$$

and thus

$$c_p = \pi + \bar{\pi} \in \operatorname{End} \mathscr{A}_p.$$

By the Eichler–Shimura relation we obtain $c_p = T_p$ in $\mathbf{T}$. For $p \mid N$ it can be shown that $c_p = U_p$ and hence

$$L(A, F, s) = \prod_{p \mid N} (1 - U_p p^{-s})^{-1} \prod_{p \nmid N} (1 - T_p p^{-s} + p^{1-2s})^{-1}$$

in the ring of formal Dirichlet series with coefficients in F. If R is the natural representation of End A on a $\mathbb{Z}$-basis of $\omega_{\mathscr{A}^0/\mathbb{Z}}$ consider the matrix valued L-series

$$L = \prod_{p \mid N} (I - R(U_p) p^{-s})^{-1} \prod_{p \nmid N} (I - R(T_p) p^{-s} + I p^{1-2s})^{-1}.$$

From Theorem (2.8) we now deduce the following satisfactory result:

(2.9) COROLLARY. *$\hat{\mathscr{A}} \cong \hat{L}$ over $\mathbb{Z}$.*

REFERENCES

[C] P. CARTIER, *Groupes formels, fonctions automorphes et fonctions zêta des courbes elliptiques.* Actes du Congrès Int. Math. Nice 1970, Tome *2*: 290–299 Paris, Gauthiers-Villars 1971.

[C-R] Ch. CURTIS and I. REINER, *Representation theory of finite groups and associative algebras.* New York, Interscience Publishers 1962.

[G 1] A. GROTHENDIECK, *Groupes de type multiplicatif: Homomorphismes dans un schema en groupes.* Exp. IX in SGA 3, II, Springer Lect. Notes in Math. 152 (1970).

[G 2] A. GROTHENDIECK, *Modèles de Néron et Monodromie.* Exp. IX in SGA 7, I. Lect. Notes in Math. Vol. 288, Springer 1972.

[Ha] M. HAZEWINKEL, *Formal Groups and Applications.* New York, Academic Press 1978.

[Hi] W. HILL, *Formal groups and zeta-functions of elliptic curves.* Invent. Math. *12*, 321–336 (1971).

[Ho 1] T. HONDA, *Formal groups and zeta-functions.* Osaka J. Math. *5*, 199–213 (1968).

[Ho 2] T. HONDA, On *the theory of commutative formal groups.* J. Math. Soc. Japan *22*, 213–246 (1970).

[J] H. JACOBINSKI, *Über die Hauptordnung eines Körpers als Gruppenmodul.* J. reine angew. Math. *213*, 151–164 (1963).

[L] H. W. LEOPOLDT, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers.* J. reine angew. Math. *201*, 119–149 (1959).

[O] T. ODA, *Formal groups attached to elliptic modular forms*. Inv. Math. *61*, 81–102 (1980).
[R] M. RAPOPORT, *Compactifications de l'espace de modules de Hilbert-Blumenthal*. Comp. Math. *36*, 255–335 (1978).
[Ra] M. RAYNAUD, *Modèles de Néron*. C. R. Akad. Sc. Paris *262*, 345–347 (1966).
[Ri] K. RIBET, *Endomorphisms of semi-stable abelian varieties over number fields*. Ann. Math. *101*, 555–562 (1975).
[Ro] M. ROSENLICHT, *Some basic theorems on algebraic groups*. Am. J. Math *78*, 401–443 (1956).
[Sh 1] G. SHIMURA, *Introduction to the arithmetic theory of automorphic functions*. Princeton University Press, Princeton 1971.
[Sh 2] G. SHIMURA, *Algebraic number fields and symplectic discontinuous groups*. Ann. Math. *86*, 503–592 (1967).
[St] J. STIENSTRA, *Formal groups and congruences for L-functions*. Am. J. Math. *109*, 1111–1127 (1987).
[T] J. TATE, *Classes d'isogénie des variétés abéliennes sur un corps fini* (d'après T. Honda), Sém. Bourbaki 21é année, no^0 352, Springer Lect. Notes in Math. Vol. 179, 1971.
[SGA 1] A. GROTHENDIECK and M. RAYNAUD, *Revêtements étales et groupe fondamental*, Springer Lect. Notes in Math. Vol. 224 (1971).

C. Deninger
Mathematisches Institut
der Universität
Einsteinstr. 62
D-4400 Münster

E. Nart
Departament de Matemàtiques
Universitat Autònoma de Barcelona
08193 Bellaterra
Catalunya
Spain

Received June 26, 1989.