COMPOSITIO MATHEMATICA

TETSUO NAKAMURA

p-divisible groups with complex multiplication over $W(k)$

Compositio Mathematica, tome 80, nº 2 (1991), p. 229-234
<http://www.numdam.org/item?id=CM_1991__80_2_229_0>

Compositio Mathematica **80**: 229–234, 1991.

p-Divisible groups with complex multiplication over $W(k)$*

TETSUO NAKAMURA

Department of Mathematics, College of General Education, Tohoku University, Kawauchi, Sendai 980, Japan

Received 31 May 1988; accepted 19 February 1991

1. Statement of the result

We refer to Waterhouse [8, §4] for p-divisible groups with complex multiplication. Let R be a complete discrete valuation ring, with residue field k, algebraically closed of characteristic $p > 0$ and fraction field K of characteristic 0. Let $\bar{K}$ be an algebraic closure of K and $\Gamma_K = \mathrm{Gal}(\bar{K}/K)$. For a p-divisible group G over R of height h, denote its Tate module by $T(G)$ and let $V(G) = \mathbf{Q}_p \otimes_{\mathbf{Z}_p} T(G)$. Let E be an extension of $\mathbf{Q}_p$ with degree h. We say G has complex multiplication by E if there is given a homomorphism of E into $\mathbf{Q}_p \otimes \mathrm{End}(G) = \mathrm{End}_{\Gamma_K} V(G)$. Then $V(G)$ is a one-dimensional E-vector space and the action of Γ_K on $V(G)$ is given by a continuous homomorphism $\rho: \Gamma_K \to E^\times$. The action of E on $t_G(K) = K \otimes_R t_G$ (t_G is the tangent space to G) has character $\Sigma_\Phi \tau$ for some subset Φ of $\mathrm{Hom}(E, \bar{K})$ (the set of all $\mathbf{Q}_p$-embeddings of E into $\bar{K}$) and we say G has type (E, Φ). Then on an open subgroup of Γ_K, ρ is determined by Φ and this shows that any two p-divisible groups of prescribed type (E, Φ) are isogenous ([8, Theorem 4.1]).

Let E' be a subextension of E over $\mathbf{Q}_p$. For a subset Φ' of $\mathrm{Hom}(E', \bar{K})$, write $\Phi'^E = \{\lambda \in \mathrm{Hom}(E, \bar{K}): \lambda|_{E'} \in \Phi'\}$. For $\Phi \subset \mathrm{Hom}(E, \bar{K})$, we say that (E, Φ) is elementary if Φ is not of the form Φ'^E for any subextension E' ($\neq E$) of E and for any subset Φ' of $\mathrm{Hom}(E', \bar{K})$. A p-divisible group G of type (E, Φ) is said to be elementary if (E, Φ) is elementary. This is equivalent to saying that $E = \mathbf{Q}_p \otimes \mathrm{End}(G)$. Any p-divisible group with complex multiplication is isogenous to a direct product of elementary groups of the same type ([8, p. 64]).

In this paper we assume that $R = W = W(k)$ the ring of Witt vectors over k and every p-divisible group G with complex multiplication is of type (E, Φ) with non-empty Φ; this implies that G is a formal (Lie) group ([8, Corollary 4.4]). Write σ for the Frobenius automorphism of K. We denote by K_h the unique unramified extension of degree h over $\mathbf{Q}_p$ in K and by W_h its maximal order.

Our theorem gives the complete classification of p-divisible groups with complex multiplication over W up to isomorphism.

*Dedicated to Professor Tsuneo Kanno on his 60th birthday.

THEOREM. (i) *For any type* (K_h, Φ), *there exists a p-divisible group over W of type* (K_h, Φ). *A p-divisible group G over W with complex multiplication of height h is elementary if and only if* $\mathrm{End}(G) \simeq W_h$.

(ii) *Let G be a p-divisible group over W of height h with complex multiplication. Then G is isomorphic over W to a direct product of several copies of an elementary group* G_1 *over W.*

(iii) *Any two p-divisible groups over W with complex multiplication of prescribed type* (K_h, Φ) *are isomorphic over W.*

In case $\dim G = 1$, the assertion of our theorem follows from [4, Proposition 3.6] and [7].

REMARK. Let

$$(K_h, \{\sigma^{e_1}, \ldots, \sigma^{e_n}\})(0 \leqslant e_1 < \cdots < e_n < h)$$

be elementary. Clearly this is the same as to say that the period of the map $\mathbf{i}: \mathbf{Z}/h\mathbf{Z} \to \{0, 1\}$ with $\mathbf{i}(e_k) = 1$ $(k = 1, \ldots, n)$ and $\mathbf{i}(j) = 0$ $(j \neq e_1, \ldots, e_n)$ is h. Define χ_h to be the composite homomorphism

$$\Gamma_K \to I \xrightarrow{d} W_h^{\times} \xrightarrow{i} W_h^{\times}$$

where I is the inertia subgroup of $\mathrm{Gal}(\bar{K}_h/K_h)$, d is the map given by classfield theory, and $i(x) = x^{-1}$ for $x \in W_h^{\times}$. Let G be of type $(K_h, \{\sigma^{e_1}, \ldots, \sigma^{e_n}\})$. Then the p-adic representation $\rho: \Gamma_K \to K_h^{\times}$ attached to G is a crystalline (or B-admissible) abelian representation in the sense of Fontaine [2], [3]. As χ_h is crystalline, it follows that $\rho = \prod_{i=1}^{n} \sigma^{-e_i} \circ \chi_h$ on Γ_K (see [6, Chapter III Appendix] and [2, §3]).

2. A construction of *p*-divisible groups with complex multiplication over *W*

LEMMA 1. *Let G be an n-dimensional p-divisible group over W of height h which has complex multiplication by E, then it has also complex multiplication by* K_h *(but, in general, E is not isomorphic to* K_h*).*

Proof. First assume that G is elementary of type (E, Φ). Let E' be the maximal unramified subextension of E. By the operation of $\mathrm{End}(G)$ on the tangent space of G we obtain a homomorphism $j: E \to M_n(K)$ (the full matrix ring of order n over K). Then the character of j is $\Sigma_{\Phi} \lambda$. If the restriction of j to E' has a character $\Sigma_{\Phi'} \tau$, then j is equivalent to the direct product of the regular representations of E over $\tau(E')$ for $\tau \in \Phi'$. This implies $\Phi = \Phi'^{E}$ and since G is elementary, we have $E = E'$ and $E = K_h$. If G is not elementary, then G is isogenous to a direct product of elementary groups of the same type (cf. [8, p. 64]). One can now verify at once that $\mathbf{Q}_p \otimes \mathrm{End}(G)$ contains a subfield isomorphic to K_h. This completes the proof.

We will now construct an n-dimensional p-divisible group G_0 over W of type (K_h, Φ) where $\Phi = \{\sigma^{e_1}, \ldots, \sigma^{e_n}\}$, $0 \leqslant e_1 < \cdots < e_n < h$. We use a result on a classification of commutative formal groups over W by systems of Honda (cf. [1, Chapter IV and V §2] and [4]). Let $D = W_\sigma[[F]]$ be the non-commutative power series ring on F with the multiplication rule; $Fa = a^\sigma F$ for $a \in W$. Let $A_{n/h} = K_h[\theta]$ denote the associative K_h-algebra with unit generated by θ such that $\theta^h = p^n$, $\theta a = a^\sigma \theta$ $(a \in K_h)$. It is the central simple algebra of rank h^2 over $\mathbf{Q}_p$ and invariant n/h. Consider the left K-space

$$M_{n/h} = K \otimes_{K_h} A_{n/h}.$$

It is a K-space with basis $\theta^i = 1 \otimes \theta^i$ $(i = 0, \ldots, h-1)$ and a right $A_{n/h}$-space. We define a D-module structure on $M_{n/h}$ by putting $F\theta^i = \theta^{i+1}$. The D-endomorphisms of $M_{n/h}$ are the right multiplications by elements of $A_{n/h}$ (cf. [5, Chapter III §4]). Now we put

$$\xi_i = p^{n-i}\theta^{e_i} \ (i = 1, \ldots, n).$$

Let L_0 (respectively M_0) be the W-submodule (respectively D-submodule) of $M_{n/h}$ generated by $\xi_1, \ldots, \xi_n$. Then we can easily check that (L_0, M_0) is a system of Honda. Let G_0 be the p-divisible group over W associated to (L_0, M_0). Put $g(0) = h + e_1 - e_n$ and $g(i) = e_{i+1} - e_i$ $(1 \leqslant i \leqslant n-1)$, then G_0 corresponds to a special element

$$u = pI - \begin{pmatrix} 0 & \cdots & 0 & F^{g(0)} \\ F^{g(1)} & \ddots & & 0 \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & F^{g(n-1)} & 0 \end{pmatrix}$$

Let $D(a) = \mathrm{diag}(a^{\sigma^{e_1}}, \ldots, a^{\sigma^{e_n}})$ for $a \in W_h$. Then we have $D(a)u = uD(a)$. Therefore G_0 is of type (K_h, Φ) and $\mathrm{End}(G_0) \supset W_h$ (see [4, Theorem 3]).

Now let $f = (h, n)$ and $h = fh_1$, $n = fn_1$. We extend g to a function on $\mathbf{Z}/n\mathbf{Z}$ by

$$g(i + n\mathbf{Z}) = g(i) \quad \text{for } i = 0, \ldots, n-1.$$

LEMMA 2. *Let r be the least positive divisor of n such that g is a function on $\mathbf{Z}/r\mathbf{Z}$. Put $\Phi_1 = \{\sigma^{e_1}, \ldots, \sigma^{e_r}\}$.*

(i) *Then r is a multiple of n_1 and if we put $r = f_0 n_1$, we have*

$$e_{k+r} = e_k + f_0 h_1 \ (1 \leqslant k \leqslant n - r).$$

(ii) *Let G_1 be the group which is constructed from $(K_{f_0h_1}, \Phi_1)$ as above. Then G_1 is elementary and* $\mathrm{End}(G_1) \simeq W_{f_0h_1}$.

(iii) *G_0 is isomorphic over W to $(G_1)^{f/f_0}$.*

Proof. Since $\Sigma_{i=0}^{n-1} g(i) = h$, we have for $1 \leqslant k \leqslant n - r$

$$g(k) + \cdots + g(k + r - 1)(= e_{k+r} - e_k) = hr/n = h_1 r/n_1.$$

This shows that r is a multiple of n_1 and (i) follows. If $(K_{f_0h_1}, \Phi_1)$ is not elementary, there exists a divisor f' $(\neq f_0)$ of f_0 such that $\{e_1, \ldots, e_{f'n_1}\}$ $(e_{f'n_1} < f'h_1)$ is a complete system of representatives of $\{e_1, \ldots, e_r\}$ mod $f'h_1$ and it is also that of $\{e_1, \ldots, e_n\}$ mod $f'h_1$. This gives $e_{k+f'n_1} - e_k = f'h_1$. Then

$$g(i + f'n_1) - g(i) = (e_{i+1+f'n_1} - e_{i+1}) - (e_{i+f'n_1} - e_i) = 0.$$

This contradicts to the choice of r. Since $\mathrm{End}(G_1) \supset W_{f_0h_1}$, (ii) is clear. Let us prove (iii). Put $s = f/f_0$ and $\eta_i = \Sigma_{k=0}^{s-1} \xi_{i+kr}$ $(i = 1, \ldots, r)$. Let L_1 (respectively M_1) be the W-submodule (respectively D-submodule) of M_0 generated by $\eta_1, \ldots, \eta_r$. Then (L_1, M_1) is isomorphic to the system of Honda associated to G_1 and

$$(L_0, M_0) = (L_1, M_1)\omega_1 \oplus \cdots \oplus (L_1, M_1)\omega_s$$

for a basis $\{\omega_1, \ldots, \omega_s\}$ of $W_h/W_{f_0h_1}$. This proves (iii).

LEMMA 3. *Let (L, M) be a system of Honda such that*

$$(L_0, M_0) \supset (L, M) \supset p(L_0, M_0).$$

Then we have $\mathrm{End}(L, M) \supset W_{f_0h_1}$ *where f_0h_1 is as in Lemma* 2.

Proof. We may suppose that $L \neq pL_0$. Let $x \in L - pL_0$. As x can be uniquely expressed in the form

$$x = \sum_{i=1}^{n} a_i \xi_i \ (a_i \in W)$$

we write

$$S(x) = \{i: 1 \leqslant i \leqslant n, a_i \not\equiv 0 \bmod p\}.$$

Put

$$d = \mathrm{Max}\{g(i): i \in S(x)\}, \ A = \{i \in S(x): d = g(i)\} \quad \text{and} \quad y = \sum_{i \in A} a_i \xi_i.$$

Since

$$F^d\xi_i = F^{d-g(i)}F^{g(i)}\xi_i = pF^{d-g(i)}\xi_{i+1},$$

we have

$$F^d y = p\sum_{i\in A} a_i^{\sigma^d}\xi_{i+1} = F^d x - F^d(x-y) \in pL_0 \cap FM.$$

Here we put $\xi_{n+1} = \xi_1$. As $L \cap FM = pL$, we obtain an element $\delta(x) = \Sigma_{i\in A} a_i^{\sigma^d}\xi_{i+1}$ of L. The nth iteration of the operation δ gives an element x' of $L - pL_0$ which satisfies

$$g(i+k) = g(j+k) \quad \text{for } i, j \in S(x') \quad \text{and} \quad k \in \mathbf{Z}. \tag{$*$}$$

Clearly L is generated by $\{x' : x \in L - pL_0\}$ and pL_0 over W. Now ($*$) implies that g is a function on $\mathbf{Z}/(j-i)\mathbf{Z}$. Then $j-i$ is a multiple of r and by Lemma 2(i) we have $e_i \equiv e_j \bmod f_0h_1$. Therefore for $i \in S(x')$, $x'a = a^{\sigma^{e_i}}x'$ ($a \in W_{f_0h_1}$). This shows that $\mathrm{End}(L, M) \supset W_{f_0h_1}$.

3. Proof of the theorem

Let G be a p-divisible group with complex multiplication over W of height h. By Lemma 1 G is of type (K_h, Φ). Let G_0 be the group of type (K_h, Φ) constructed in Section 2. We claim that G and G_0 are isomorphic. By [8, Theorem 4.1] there exists an isogeny $\alpha: G \to G_0$ over W and α defines an injection $T(G) \to T(G_0)$. Hence we may assume that $T(G) \subset T(G_0)$. There is an integer m such that $p^m T(G_0) \subset T(G)$. Let $T_i = T(G) + p^i T(G_0)$ ($i = 0, 1, \ldots, m$). Then T_i is a Γ_K-sublattice of $T(G_0)$. Hence $T_i = T(H_i)$ for some group H_i over W ([8, Theorem 1.3]). Since $T_0 \supset T_1 \supset pT_0$, the system of Honda of H_1 satisfies the condition of Lemma 3. Therefore $\mathrm{End}(H_1) \supset W_{f_0h_1}$. By Lemma 2, $T_0 = T(G_0) \simeq \oplus_s T(G_1)$ is a free $W_{f_0h_1}$-module of rank s and T_1 is a $W_{f_0h_1}$-sublattice of T_0. Then T_0 and T_1 are $W_{f_0h_1}$-isomorphic, and also Γ_K-isomorphic, since the operation of Γ_K is given by the p-adic representation

$$\Gamma_K \to W_{f_0h_1}^\times = \mathrm{Aut}_R T(G_1) \subset \mathrm{Aut}(\mathbf{Q}_p \otimes T_0) = \mathrm{Aut}(\mathbf{Q}_p \otimes T_1)$$

where $R = \mathrm{End}(G_1) \simeq W_{f_0h_1}$. Proceeding inductively, we see that $T_m = T(G)$ is Γ_K-isomorphic to $T(G_0)$. This implies that G and G_0 are isomorphic over W. Our theorem now follows immediately from Lemma 2 (ii), (iii).

References

1. J.-M. Fontaine, Groupes p-divisible sur les corps locaux. *Astérisque* 47–48, Soc. Math. de France, 1977.
2. J.-M. Fontaine, Modules galoisiens, modules filtrés et anneaux de Barsotti–Tate, in *Journées de Géométrie Algébrique de Renne, Astérisque* 65, Soc. Math. de France, 1979, pp. 3–80.
3. J.-M. Fontaine, Sur certains types de représentations p-adiques du groupe de Galois d'un corps local: construction d'un anneau de Barsotti–Tate, *Ann Math.* 115 (1982) 529–577.
4. T. Honda, On the theory of commutative formal groups, *J. Math. Soc. Japan* 22 (1970) 213–246.
5. Yu. I. Manin, The theory of commutative formal groups over fields of finite characteristic, *Russian Math. Surveys* 18 (1963) 1–83.
6. J.-P. Serre, Abelian l-adic Representations and Elliptic Curves, Benjamin, New York, 1968.
7. W. Waterhouse, A classification of almost full formal groups, *Proc. Amer. Math. Soc.* 20 (1969) 426–428.
8. W. Waterhouse, On p-divisible groups over complete valuation rings, *Ann. Math.* 95 (1972) 55–65.