國立臺灣大學數學系

碩士論文

Department of Mathematics

National Taiwan University

Master Thesis

P 分解群之概觀

A survey of p-divisible groups

江謝良州

Liang-Chou Chiang-Hsieh

指導教授：余正道 博士

Advisor: Jeng-Daw Yu, Ph.D.

中華民國 99 年 7 月

July, 2010

誌謝:

要畢業了，回到考上研究所的那一刻，跌跌撞撞的走來，心中有無限的感恩。程度很差的我，當連我自己都失去耐心想放棄時，老闆沒有放棄我，用他無比的耐心，幫我度過難關。在這裡向我的老闆說聲“謝謝老師”。

我的家人也等到了這一刻，謝謝這麼多年來他們的支持，您們的辛苦我點滴在心頭，尤其是二姐，這麼多年來的付出，感謝上天有妳們在。還有陪我熬夜趕論文，看著我抱頭痛哭的小黑，讓我在夜裡不那麼孤單，小黑，You are my dog!

最後感謝小秘書蔡包小姐，貼心的照顧以及鼓勵。能夠畢業心裡充滿著感恩，期許未來的我不要丟台大的臉，加油!!

中文摘要：

論文分成兩部份，第一部份介紹 P 可分解群的定義和基本定理；第二部份介紹 Hodge-Tate 的分解，並給予証明。

英文摘要:

In the first part, we will give the definitions, examples and some theorems of p-divisible groups. In the second part, we will obtain the Hodge-Tate decomposition of the Tate module of a p-divisible group over a certain ring.

目　錄

[1] C. Waterhouse, Introduction to a_ne group schemes. vol.66, GTM, Springer, Berlin-Heidelberg New York 1979.
[2] B. Conrad, M. Lieblich: Galois representations arising from p-divisible groups. Available on http://www.math.lsa.umich.edu/~bdconrad/CompleteNotes.pdf.
[3] J. Tate, p-divisible groups, Proc. Conf. Local _elds (Driebergen,1966), 158-183.
[4] R. Pink, Finite group schemes, available on http://www.ma-th.ethz.ch/~pink/ftp/FGS.
[5] J.P. Serre, Lie algebras and Lie groups. New York: Benjamin 1965.
[6] J. Tate, F. Oort, Group schemes of prime order. Annales scienti_ques de l'École Normale Supérieure, Sér. 4, 3 no. 1, 1970.

A SURVEY OF p-DIVISIBLE GROUPS

CHIANG HSIEH LIANG CHOU

Introduction

In the first part, we will give the definitions, examples and some theorems of p-divisible groups. In the second part, we will obtain the Hodge-Tate decomposition of the Tate module of a p-divisible group over a certain ring.

1. Preliminaries

Let R be a complete noetherian local ring and $\boldsymbol{m}$ its maximal ideal. We assume that the residue field $k = R/\boldsymbol{m}$ is of characteristic $p > 0$. We say that *an affine group scheme* $G = Spec(A)$ is a *finite group scheme* over R if it is commutative and A is a finite flat R-algebra, i.e. A is a locally free R-module of finite type. The *rank* $|G|$ of G is defined to be the rank of the R-module A.

If $|G| = m$, then

$$\varphi : G \to G,\ (x \mapsto mx)$$

is the trivial map; this is known as the Deligne theorem ([6], p. 4.). For a finite group scheme G, we can define its Cartier dual ([4], p. 8.) $G^\vee = Spec(A^\vee)$, where $A^\vee = Hom_{R-mod}(A, R)$, and its ring multiplication is given by the dual of the comultiplication

$$m^* : A \to A \otimes A.$$

The dual $G^\vee$ has a natural structure of a group scheme, whose comultiplication comes from the dual of the multiplication of the ring A, and the inverse is induced by the inverse of G. The construction of the dual group scheme is functorial in G and we have a natural isomorphism $G \simeq (G^\vee)^\vee$. An alternative characterization of $G^\vee$ is given by

$$G^\vee(S) = Hom_{S-group}(G \times S, \boldsymbol{G}_m/S)$$

for any R-scheme S. Here $\boldsymbol{G}_m/S$ denotes the multiplicative group over S.

Example 1. (a) The dual of $\mu_{p^n} = Spec(R[T]/(T^n - 1))$ is the constant group scheme $(\mathbb{Z}/n\mathbb{Z})_R$.

(b) There is an equivalence between the category of finite etale group schemes over R and the category of finite continuous $\pi_1^{et}(R)$-modules. Here $\pi_1^{et}(R)$ denotes the etale fundamental group of $Spec(R)$.

We say that a sequence $0 \to G' \xrightarrow{i} G \xrightarrow{j} G'' \to 0$ is a *short exact sequence of finite group scheme* if i is a closed immersion via which G' is identified as the kernel of j and j is faithfully flat. If the order of G (resp. G', G'') is m (resp. m', m''), then $m = m'm''$.

Example 2. The following sequences are short exact:

(a) $0 \to \boldsymbol{\mu}_n \to \boldsymbol{G}_m \xrightarrow{\times n} \boldsymbol{G}_m \to 0$.

(b) $0 \to Spec(R[T]/(T^p)) \to G_a \xrightarrow{x \to x^p} G_a \to 0$. Here, $G_a := Spec(R[T])$ with the operation $(t, t') \mapsto t + t'$ denotes the *additive group over R*.

Proposition 3. *Any finite group scheme $G = Spec(A)$ over the ring R admits a canonical functorial connected-etale short exact sequence*

$$0 \to G^0 \to G \to G^{et} \to 0$$

where $G^0 = Spec(A^0)$ *is the connected component of* G *and* $G^{et}= Spec(A^{et})$ *corresponds to the maximal etale subalgebra of* A *over* R*.*

For a proof, see [2], chap. 1.5.

Remark 4. The exact sequence has a canonical splitting if $R = k$ is a perfect field of characteristic $p > 0$. We recall that a field is perfect if every finite extension is a separable extension.

Definition 5. Let p be a prime and h a nonnegative integer. A $p-$ *divisible group* G *over* R *of height* h is an inductive system

$$G = (G_v, i_v : G_v \to G_{v+1})$$

where G_v is a finite group scheme over R of rank p^{hv}, and for each v we have an exact sequence

$$0 \to G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^v} G_{v+1}.$$

A morphism between p-divisible groups is a collection of morphisms

$$(f_\mu : G_\mu \to H_\mu)$$

on each level, compatible with the structure of a p-divisible groups.

Example 6. (a) $\boldsymbol{G}_m(p) = (\mu_{p^v})$ with the natural inclusion is a p-divisible group of height one.

(b) Let X be an abelian variety over R, $dimX = n$. Let $p^v : X \to X$ be the multiplication by p^v and $X[p^v] = ker(p^v)$. Then $X(p) = (X[p^v])$ has a natural structure of a p-divisible group of height $2n$.

Remark 7. Let G be a p-divisible group. We have

(1) $p^v : G \to G$ is surjective (= faithfully flat) for all v.

(2) $G[p^v] = ker(p^v : G \to G)$ is a finite group scheme over R of rank p^{hv}. In fact, $G[p^v] = G_v$.

(3) $\varinjlim_{v} G[p^v] = G$.

(4) G_μ can be identified with the kernel of

$$p^\mu : G_{\mu+v} \to G_{\mu+v}.$$

(5) The homomorphism $p^\mu : G_{\mu+v} \to G_{\mu+v}$ factors through

$$j_v : G_{\mu+v} \to G_v$$

since $G_{\mu+v}$ is killed by $p^{\mu+v}$.

(6) The sequence

$$0 \to G_\mu \xrightarrow{\mu_v} G_{\mu+v} \xrightarrow{j_v} G_v \to 0$$

is exact.

Definition 8. An $n - dimensional\ formal\ Lie\ group$ over R is the formal power series ring $\mathcal{A} = R[[X_1, ..., X_n]]$ with a suitable comultiplication structure

$$m^* : \mathcal{A} \to \mathcal{A}\widehat{\otimes}\mathcal{A} = R[[Y_1, ..., Y_n, Z_1, ..., Z_n]],$$

which is determined by $F(Y, Z) = (f_i(Y, Z))$, where f_i are the images of X_i, and m^* satisfies the following statements:

(1) $X = F(X, 0) = F(0, X)$

(2) $F(X, F(Y, Z)) = F(F(X, Y), Z)$

(3) $F(X, Y) = F(Y, X)$.

Let $\psi : \mathcal{A} \to \mathcal{A}$ denote the multiplication by p of the formal Lie group $\mathcal{A}$. We say that $\mathcal{A}$ is *divisible* if $\mathcal{A}$ is a finite free module over $\psi(\mathcal{A})$.

Theorem 9. *Let R be a complete notherian local ring whose residue field k of characteristic $p > 0$. We have an equivalence of categories between the category of divisible commutative formal Lie groups over R and the category of connected p-divisible groups over R.*

For a proof, see [3], p. 162.

If $G = (G_v, i_v)$ is a p-divisible group over R, the connected components G_v^0 determine a *connected* p-divisible group G^0. From the exact sequence

$$0 \to G_v^0 \to G_v \to G_v^{et} \to 0$$

one gets an exact sequence

$$0 \to G^0 \to G \to G^{et} \to 0,$$

where G^{et} is an *etale* p-divisible group. The dimension of the formal Lie group corresponding to G^0 is, by definition, the *dimension* of G.

Therefore, for a p-divisible group G there are two invariants: the height h and the dimension n of a p-divisible group.

Example 10. (a) $\boldsymbol{G}_m(p)$ is a p-divisible groups of height 1 and dimension 1. It corresponds to the formal Lie group whose multiplication is given by $F(Y,Z) = Y + Z + YZ$.

(b) For an abelian variety X, $X(p)$ is a p-divisible group of height $2n$ and dimension n.

We fix our notations. Let R be a complete discrete valuation ring with perfect residue field k of characteristic $p > 0$ and fraction field K of characteristic 0.

Definition 11. Let $G = Spec(A)$ be a finite group scheme over R. The trace $Tr : A \otimes A \to R$ extends to a morphism

$$\phi : \Lambda^{top} A \otimes \Lambda^{top} A \to R.$$

The *discriminant* $disc_{G/R}$ of G is defined to be the ideal generated by the image of ϕ.

Proposition 12. *Let $G = (G_v)$ be a p-divisible group. The discriminant of (G_v) is $p^{nvp^{hv}}$, where $n = dim(G)$, and $h = ht(G)$.*

For a proof, see [2], chap. 6.2, p. 101.

Proposition 13. *Suppose G is a p-divisible group over R, then*

$$dim(G) + dim(G^{\vee}) = ht(G),$$

where $ht(G)$ denotes the height of G.

(Pf):

Let $dim(G^{\vee}) = n^{\vee}$, $dim(G) = n$. The dimension and height of G do not change if we reduce G mod $\boldsymbol{m}$. Hence we may assume that $R = k$ is a field. The maps

$$p : G \to G,$$

$$F : G \to G^{(p)} \text{ (Frobenius)},$$

$$V : G^{(p)} \to G \text{ (Verschiebung)},$$

$$p : G^{(p)} \to G^{(p)}$$

are surjective, and

$$V \circ F = p = F \circ V \ \text{([3], p. 163)}.$$

Therefore, there is an exact sequence

$$0 \to ker(F) \to ker(p) \xrightarrow{F} ker(V) \to 0.$$

Now $ker(p) = G_1$ has order p^h, and $ker(F)$ has order p^n. (F is injective on G^{et}, so the kernel F in G is the same as that of F in the connected component G^0. Viewing G^0 as a formal Lie group on n parameters, we see that the order of $ker(F)$ is p^n ([3], p. 162).) Since F and V are dual to each other with respect to Cartier duality, one checks that $ker(V)$ is the Cartier duality of cokernel of the map $F : G_1^\vee \to (G_1^{(p)})^\vee$, and consequently $ker(v)$ has order p^{n}. Now the assertion follows from the multiplicative property of orders in an exact sequence.

2. The Hodge-Tate decomposition of the Tate modules

We will go through Tate's approach step by step. First we fixed our notations.

Notations and assumptions

$(R, \boldsymbol{m})$: a complete notherian discrete valuation ring.

k: residue field $R/\boldsymbol{m}$ of characteristic $p > 0$; assume k is perfect.

K: fraction field of R; assume it is of characteristic 0.

$\overline{K}$: the algebraic closure of K.

$\boldsymbol{C}$: the completion of $\overline{K}$.

$\mathcal{G}$: $Gal(\overline{K}/K)$

$\mathcal{O}_{\boldsymbol{C}}$: ring of integers of $\boldsymbol{C}$ with maximal ideal $\boldsymbol{m}_{\mathcal{O}_{\boldsymbol{C}}}$.

Let G be a p-divisible group over R and G^0, G^{et} denote its connected and etale part respectively. Let $\mathcal{A}^{(0,et)}=$

$\varprojlim_v A_v^{(0,et)}$ be its ring of functions.

Tate's approach:

We start from the information of the generic fiber by the following two Galois modules:

$$\Phi(G) = \varinjlim_v G_v(\overline{K}) \text{ via the natural inclusion: } G_v \to G_{v+1},$$

$$T(G) = \varprojlim_v G_v(\overline{K}) \text{ via ``multiplication by } p\text{'': } G_{v+1} \to G_v.$$

Since $char K = 0$, $G \otimes K$ is etale. We have

$$T(G) \simeq \mathbb{Z}_p^h$$

and

$$\Phi(G) \simeq (\mathbb{Q}_p/\mathbb{Z}_p)^h$$

both with action of $\mathcal{G}$.

There is a canonical isomorphism of $\mathcal{G}$-modules

$$T(G) \simeq Hom(\mathbb{Q}_p/\mathbb{Z}_p, \Phi(G)),$$

$$\Phi(G) = T(G) \otimes (\mathbb{Q}_p/\mathbb{Z}_p).$$

Since $G \otimes K$ is etale, we conclude that the information of the generic fiber is all contained in the G-module $T(G)$ or $\Phi(G)$. In order to extract information from the two Galois modules, we need to use analytic method.

Definition 14. Define $G(\mathcal{O}_{\boldsymbol{C}}) := Hom_{cont.}(\mathcal{A}; \boldsymbol{C})$ to be the $\mathcal{O}_{\boldsymbol{C}}$-points of G.

Remark 15. $G(\boldsymbol{C}) := G(\mathcal{O}_{\boldsymbol{C}}) = \lim\limits_{\overleftarrow{i}} G(\mathcal{O}_{\boldsymbol{C}}/\boldsymbol{m}^i\mathcal{O}_{\boldsymbol{C}})$

$= \lim\limits_{\overleftarrow{i}} \lim\limits_{\overrightarrow{v}} G_v(\mathcal{O}_{\boldsymbol{C}}/\boldsymbol{m}^i\mathcal{O}_{\boldsymbol{C}})$.

By the continuous version of homomorphism, we can easily identify the points in $G^0(\mathcal{O}_{\boldsymbol{C}})$ with the points in $\boldsymbol{m}^n_{\mathcal{O}_{\boldsymbol{C}}}$, since any such map is determined by the image of X_i of $\mathcal{A}^0 = R[[X_1, ..., X_n]]$ in $\mathcal{O}_{\boldsymbol{C}}$.

Example 16. (a) For $G = G_m(p)$, $G(\mathcal{O}_C)$ is the group of units in $\mathcal{O}_{\boldsymbol{C}}$ whose reductions modulo $m_{\mathcal{O}_C}$ are 1. $\Phi(G)$ consists of all p-power roots of unity.

(b) For an abelian variety X and $G = X(p)$, $G(\mathcal{O}_{\boldsymbol{C}})$ consists of the points whose reductions modulo $\boldsymbol{m}_{\mathcal{O}_{\boldsymbol{C}}}$ are p power torsions. $\Phi(G)$ are all p power torsions ([3], p. 169).

Proposition 17. *The torsion part $G(\mathcal{O}_{\boldsymbol{C}})_{tor}$ of $G(\mathcal{O}_{\boldsymbol{C}})$ equals $\Phi(G)$.*

(Pf):

The p^v-torsions of $G(\mathcal{O}_{\boldsymbol{C}}/\boldsymbol{m}^i\mathcal{O}_{\boldsymbol{C}})$ are exactly $G_v(\mathcal{O}_{\boldsymbol{C}}/\boldsymbol{m}^i\mathcal{O}_{\boldsymbol{C}})$. Therefore, the p^v- torsions of $G(\mathcal{O}_{\boldsymbol{C}})$ are $G_v(\mathcal{O}_{\boldsymbol{C}})= G_v(\overline{K})$.

Taking direct limit on v, we get this proposition.

To study the analytic structure of $G(\mathcal{O}_{\boldsymbol{C}})$, we observe that $G(\mathcal{O}_{\boldsymbol{C}})$ has a structure of an analytic p-adic Lie group. ([3], p.167) So, we have a logarithm map from $G^0(\mathcal{O}_{\boldsymbol{C}})$ to the tangent space

$$t_G(\mathcal{O}_{\boldsymbol{C}}) =\{\ d \mid d : I^0/(I^0)^2 \to \boldsymbol{C}\},$$

where I^0 is the augmentation ideal of $\mathcal{A}^0$. The *log* map is defined by

$$logx(f) := \lim_{i\to\infty}(\frac{f(p^i x)-f(0)}{p^i}),$$

where $x \in G(\mathcal{O}_{\boldsymbol{C}})$, $f \in \mathcal{A}^0$ ([3], p. 168).

This map is a $\mathbb{Z}_p$-homomorphism, and well-defined on $G(\mathcal{O}_{\boldsymbol{C}})$ since the etale part is torsion. Moreover, restricted to $G^0(\mathcal{O}_{\boldsymbol{C}})$, log is a local analytic isomorphism to $t_G(\mathcal{O}_{\boldsymbol{C}})$ and is surjective. Therefore, the kernel of log can be identified with the torsion part of $G(\mathcal{O}_{\boldsymbol{C}})$, which is exactly $\Phi(G)$.

Summing up these results, we have an exact sequence

$$0 \to \Phi(G) \to G(\mathcal{O}_{\boldsymbol{C}}) \xrightarrow{log} t_G(\boldsymbol{C}) \to 0.$$

Theorem 18. *Let G be a p-divisible group. We have the Hodge-Tate decomposition*

$$Hom(T(G), C) \simeq t_{G^\vee}(\boldsymbol{C}) \oplus t_G^\star(\boldsymbol{C}) \otimes_{\boldsymbol{C}} Hom(H, \boldsymbol{C}),$$

where $H = T(G_m(p))$ and $t_G^\star$ is the cotangent space of G at the origin.

For proving the Hodge-Tate decomposition, we need some facts.

Theorem 19. *Let $\chi : \boldsymbol{\mathcal{G}} \to K^\times$ be a multiplicative character, and K_∞ denote the fixed field of $ker(\chi)$. Suppose that there is a finite Galois extension K_0 of K contained in K_∞ such that K_∞/K_0 is totally ramified and $Gal(K_\infty/K_0) \simeq \mathbb{Z}_p$. Then*

$$H^0(\boldsymbol{\mathcal{G}}; \boldsymbol{C}(\chi)) = H^1(\boldsymbol{\mathcal{G}}; \boldsymbol{C}(\chi)) = 0.$$

In particular, if ϵ_p is the p-adic cyclotomic character on $\mathcal{G}$, then for all $n \neq 0$,

$$H^0(\boldsymbol{\mathcal{G}}; \boldsymbol{C}(n)) = H^1(\boldsymbol{\mathcal{G}}; \boldsymbol{C}(n)) = 0.$$

where $\boldsymbol{C}(n) = \boldsymbol{C}(\chi^n)$ is the twist of $\boldsymbol{C}$ by χ^n .

(Pf):

Case 1: Suppose that $K_0 = K$.

(a) Let $\boldsymbol{\mathcal{H}} = Gal(\overline{K}/K_\infty)$, $\eth = Gal(K_\infty/K_0)$. Since $(\boldsymbol{C}(\chi))^{\boldsymbol{\mathcal{G}}} = ((\boldsymbol{C}(\chi))^{\mathcal{H}})^{\eth}$, where the isometric action of $\eth$ on K_∞ extends to an action on the completion $\widehat{K_\infty}$ of K_∞ with respect to the valuation metric and $\mathcal{H}$ acts on $C(\chi)$ without a twist. Since

$$H^0(\mathcal{H}; C) = \widehat{K_\infty}(\chi)$$

and

$$H^0(\eth; \widehat{K_\infty}(\chi)) = 0 \text{ ([3], p. 174)},$$

we get $H^0(\boldsymbol{\mathcal{G}}; \boldsymbol{C}(\chi)) = 0$.

(b) We have the infation-restriction exact sequence

$$0 \to H^1(\eth; \widehat{K_\infty}(\chi)) \to H^1(\boldsymbol{\mathcal{G}}; \boldsymbol{C}) \to H^1(\boldsymbol{\mathcal{H}}; \boldsymbol{C}).$$

Since

$$H^1(\boldsymbol{\mathcal{H}}; \boldsymbol{C}) = 0$$

and

$$H^1(\eth; \widehat{K_\infty}(\chi)) = 0 \text{ ([3], p. 174)}$$

we get $H^1(\boldsymbol{\mathcal{G}};\boldsymbol{C}(\chi)) = 0$.

Case 2: Suppose that K_0 is an arbitrary finite Galois extension of K.

Let $\mathcal{U}$ be the subgroup of G fixing K_0. By the Case 1 just proven,

$$H^0(\mathcal{U};\boldsymbol{C}(\chi)) = H^1(\mathcal{U};\boldsymbol{C}(\chi)) = 0,$$

Therefore, in the infation-restriction sequence

$$0 \to H^1(\boldsymbol{\mathcal{G}}/\mathcal{H};H^0(\mathcal{U};\boldsymbol{C}(\chi))) \to H^1(\boldsymbol{\mathcal{G}};\boldsymbol{C}(\chi)) \to H^1(\mathcal{U};\boldsymbol{C}),$$

the outer terms are zero. So we get the general case.

Proposition 20. *$H^0(\mathcal{G};\boldsymbol{C}) = K$ and $dim_K H^1(\mathcal{G};\boldsymbol{C}) = 1$.*

(Pf):

(a) Since $\boldsymbol{C}^{\boldsymbol{\mathcal{G}}} = (\boldsymbol{C}^{\mathcal{H}})^{\eth}$ and $H^r(\mathcal{H};\boldsymbol{C}) = 0$ *for* $r > 0$,

$$H^0(\mathcal{H};\boldsymbol{C}) = \widehat{K_\infty},$$

and

$$H^0(\eth;\widehat{K_\infty}) = K \text{ ([2], chap. 1.9, p. 130)},$$

we get $H^0(\mathcal{G};\boldsymbol{C}) = K$.

(b) We have the infation-restriction sequence

$$0 \to H^1(\eth;\widehat{K_\infty}) \to H^1(\boldsymbol{\mathcal{G}};\boldsymbol{C}) \to H^1(\mathcal{H};\boldsymbol{C}).$$

Since

$$H^1(\mathcal{H};\boldsymbol{C}) = 0$$

and

$$dim_K H^1(\eth; \widehat{K_\infty}) = 1 \text{ ([2], chap. 1.9, p. 130),}$$

we get $dim_K H^1(\mathcal{G}; \boldsymbol{C}) = 1$.

We show the Hodge-Tate decomposition from the following proposition and theorem.

Proposition 21. *In the following diagram, α_0 is a bijection and α and $d\alpha$ are injective.*

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Phi(G) & \longrightarrow & G(\mathcal{O}_{\mathbb{C}}) & \xrightarrow{\log} & t_G(\mathbb{C}) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_0} & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle d\alpha} & & \\ 0 & \longrightarrow & \mathrm{Hom}(T(G^\vee), U_{\mathrm{tors}}) & \longrightarrow & \mathrm{Hom}(T(G^\vee), U) & \xrightarrow{\log} & \mathrm{Hom}(T(G^\vee), \mathbb{C}) & \longrightarrow & 0 \end{array}$$

.

Here

$(\alpha_0(g))(f) = \varinjlim_v f_v(g_v)$, where $g = (g_v) \in G$, and $f = (f_v) \in T(G^\vee)$.

$\alpha(g)(f) = \varprojlim_i \varinjlim_v (f_v(g_{i,v}))$, where $g = (\varprojlim_i \varinjlim_v (g_{i,v})) \in G(\mathcal{O}_{\boldsymbol{C}})$, $g_{i,v} \in G_v(\mathcal{O}_{\boldsymbol{C}}/\boldsymbol{m}^i\mathcal{O}_{\boldsymbol{C}})$, and $f = (f_v) \in T(G^\vee)$, $f_v \in G_v^\vee(\mathcal{O}_{\boldsymbol{C}}) = Hom_{\mathcal{O}_{\boldsymbol{C}}}(G_v, \mathbf{G}_m)$.

Proof:

Step 1: The map α_0 is bijective.

Because $char(K) = 0$, there is a natural isomorphism of $\mathcal{G}$-modules

$$G_n^\vee(\boldsymbol{C}) \simeq Hom(G_n(\boldsymbol{C}), G_m(\boldsymbol{C}))$$

$$= Hom(G_n(\boldsymbol{C}), \boldsymbol{m}_{p^\infty}(\boldsymbol{C}))$$

$$= Hom(G_n(\boldsymbol{C}), (U_{\mathcal{O}_{\boldsymbol{C}}})_{tors})$$

Therefore, Cartier duality provides a perfect pairing of abelian groups

$$G_n(C) \times G_n^\vee(C) \to \boldsymbol{m}_{p^{nh}}(\mathcal{O}_{\boldsymbol{C}}) \hookrightarrow (U_{\mathcal{O}_{\boldsymbol{C}}})_{tors},$$

so there is an isomorphism of $\mathcal{G}$-modules

$$G_n(\boldsymbol{C}) \simeq Hom(G_n^\vee(\boldsymbol{C}), (U_{\mathcal{O}_{\boldsymbol{C}}})_{tors}) \text{ .... } \spadesuit$$

Note that $T(G^\vee)$ is a finitely generated Z_p-module, while $(U_{\mathcal{O}_{\boldsymbol{C}}})_{tors}$ is torsion, so any map $T(G^\vee) \to (U_{\mathcal{O}_{\boldsymbol{C}}})_{tors}$ must factor through some $T(G^\vee)/p^nT(G^\vee)$, i.e.

through some $G_n^\vee(\boldsymbol{C})$. Thus, passing to the limit in $\spadesuit$, we see that there is a natural isomorphism of $\mathcal{G}$-modules

$$\Phi(G) \tilde{\to} \varinjlim Hom(G_n^\vee(\boldsymbol{C}), (U_{\mathcal{O}_{\boldsymbol{C}}})_{tors}) \tilde{\to} Hom(T^\vee, (U_{\mathcal{O}_{\boldsymbol{C}}})_{tors}),$$

and this is the map α_0.

Step 2: The Z_p-modules $ker(\alpha)$ and $coker(\alpha)$ are Q_p-vector spaces.

Applying the Snake Lemma to the diagram, we see that $ker(\alpha) \to ker(d\alpha)$ and $coker(\alpha) \to coker(d\alpha)$ are isomorphisms of $Z_p[\mathcal{G}]$-modules. Thus, we only need to show that $d\alpha$ is Q_p-linear. By functoriality, $d\alpha$ is Q_p-linear.

Step 3: $G(R) = G(\mathcal{O}_{\boldsymbol{C}})^{\mathcal{G}}$ and $t_G(K) = t_G(\boldsymbol{C})^{\mathcal{G}}$.

Using Proposition 20 , we have

$$C^{\mathcal{G}} = K \text{ and } (U_{\mathcal{O}_{\boldsymbol{C}}})^{\mathcal{G}} = R.$$

On the other hand the $\mathcal{G}$-action on $G(\mathcal{O}_{\boldsymbol{C}})$ and $t_G(\boldsymbol{C})$ are induced by the action on $U_{\mathcal{O}_{\boldsymbol{C}}}$ and $\boldsymbol{C}$ respectively. Thus Step 3 follows.

Step 4. The map α is injective on $G(R)$.

By step 3 and the left-exactness of the fixed-points functor, we see that

$$ker(\alpha|_{G(R)}) = (ker(\alpha))^{\mathcal{G}}.$$

By step 2, we see that $(ker(\alpha))$ is a Q_p-vector space. Since Q_p is also fixed by $\mathcal{G}$,

$$ker(\alpha)\bigcap G(R) = (ker(\alpha))^{\mathcal{G}}$$

is a Q_p-vector space. Therefore is $p-$divisible.

Claim: The Q_p-vector space $ker(\alpha)\bigcap G(R)$ is zero.

Case 1: If G is connected.

Given $x \in ker(\alpha)\bigcap G(R)$, $x = p^n(p^{-n}x)$ for any positive integer n. Because $x \in p^nG(R)$ for any positive integer n and $\bigcap p^nG(R) = 0$ ([2], chap. 6.3), $x = 0$.

Case 2: If G is arbitrary.

Given $x \in ker(\alpha)\bigcap G(R)$. We have that $p^nx \in ker(\alpha)\bigcap G^0(R)$ for some n ([2], chap. 6.3, p. 105.) and the commutative diagram

$$\begin{array}{ccccccc} 0 & \to & ker(\alpha|_{G^0(R)}) & \to & G^0(R) & \to & Hom(T((G^0)^\vee;U)) \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \to & ker(\alpha|_{G(R)}) & \to & G(R) & \to & Hom(T(G^\vee);U)). \end{array}$$

Since $G^0 \hookrightarrow G$ yields $T(G^\vee) \twoheadrightarrow T(G^0)^\vee$, $Hom(T((G^0)^\vee;U)) \hookrightarrow Hom(T(G^\vee);U))$. By case 1 and the injective property, we therefore see that $\alpha|_{G(R)}(p^nx) = 0$ induces $\alpha|_{G^0(R)}(p^nx) = 0$ (i.e. $p^nx = 0$), so $x = 0$.

Step 5: The map $d\alpha|_{t_G(K)}$ is injective.

By steps 1 and 4, along with the Snake Lemma, $d\alpha|_{t_G(K)}$ is injective.

Step 6: The map $d\alpha$ is injective.

We can factorize $d\alpha$ as

$$t_G(\boldsymbol{C}) \simeq t_G(K) \otimes_K \boldsymbol{C} \to Hom_{\mathbb{Z}_p}(T(G^\vee), \boldsymbol{C})^{\mathcal{G}} \otimes_K \boldsymbol{C} \to Hom_{\mathbb{Z}_p}(T(G^\vee), \boldsymbol{C}).$$

By step 5, the middle map is an injection. We need the following lemma: (Hodge-Tate Lemma) If W is a finite-dimensional $\boldsymbol{C}$-vector space admitting a continuous semi-linear $\mathcal{G}$-action, then the natural $\boldsymbol{C}$-linear map $W^{\mathcal{G}} \otimes_K \boldsymbol{C}$ of $\mathcal{G}$-modules is injective. In particular, $dim_K W^{\mathcal{G}}$ is finite ([2], chap 7.1, p 107.). So the last map is an injection.

Theorem 22. *There are natural isomorphisms*

$$G(R) \overset{\alpha_R}{\to} Hom_{\mathbb{Z}_p}(T(G^\vee), U)^{\mathcal{G}}$$

of groups and

$$t_G(K) \overset{d\alpha_R}{\to} Hom_{\mathbb{Z}_p}(T(G^\vee), C)^{\mathcal{G}}$$

of K-vector spaces, where U denotes 1+ $\boldsymbol{m}_{\mathcal{O}_{\boldsymbol{C}}}$.

(Pf):

Proposition 21 implies the injectivity of these maps, and also, via $G(R) = G(\mathcal{O}_{\boldsymbol{C}})^{\mathcal{G}}$and $t_G(K) = t_G(K)^{\mathcal{G}}$,that we have

$$coker(\alpha_R) \to (coker(\alpha_R))^{\mathcal{G}}$$

and

$$coker(d\alpha_R) \to (coker(d\alpha_R))^{\mathcal{G}}$$

are injective. Since $coker(\alpha) \to coker(d\alpha)$ is bijective, it follows that the map

$$coker(\alpha_R) \to coker(d\alpha_R)$$

is injective, so we are reduced to proving $d\alpha$ is surjective. Since

$$t_G(K) \stackrel{d\alpha_R}{\to} Hom_{\mathbb{Z}_p}(T(G^\vee); \boldsymbol{C})^{\mathcal{G}}$$

is a K-linear map and injective, this is a question of dimension.

Let $W = Hom_{\mathbb{Z}_p}(T(G); \boldsymbol{C})$ and $W^\vee = Hom_{\mathbb{Z}_p}(T(G^\vee); \boldsymbol{C})$.

They are $\boldsymbol{C}$-vector spaces of dimension $h = ht(G)$ on which $\mathcal{G}$ operates semilinearly.

Put

$$dim_K(t_G(K)) = dim(G) = n,$$

$$dim_K(t_{G^\vee}(K)) = dim(G^\vee) = n^{'}$$

and

$$d = dim_K(W)^{\mathcal{G}}, d^{'} = dim_K(W^\vee)^{\mathcal{G}}.$$

By the injectively of $d\alpha_R$ we already know $n \leq d^{'}$ and $n^{'} \leq d$, and we wish to show that equality holds. Since $n + n^{'} = h$, it will suffice to show that $d + d^{'} \leq h$.

Since

$$T(G) \backsimeq Hom_{\mathbb{Z}_p}(T(G^{\vee}), \mathbb{Z}_p(1)),$$

we have

$$W^{\vee} = T(G) \otimes Hom(H; \boldsymbol{C}),$$

so that there is a canonical non-degenerate $\mathcal{G}$-pairing

$$W \times W^{\vee} \to Y,$$

where $Y = Hom(H; \boldsymbol{C})$.

$Y^{\mathcal{G}} = H^0(\mathcal{G}; Y) = 0$, and also $H^1(\mathcal{G}; Y) = 0$([2], p 176). Since $W^{\mathcal{G}}$ and $(W^{\vee})^{\mathcal{G}}$ are paired into $Y^{\mathcal{G}}$, it follows that $W^{\mathcal{G}}\boldsymbol{C}$ and $(W^{\vee})^{\mathcal{G}}\boldsymbol{C}$ are orthogonal C-subspaces of W and $W^{\vee}$. Their dimensions are d and $d^{\vee}$. Hence $d + d^{\vee} \leq dim_{\boldsymbol{C}} W$, as required.

Proof of the Hodge-Tate decomposition.

(1) Let $W = Hom_{\mathbb{Z}_p}(T(G), \boldsymbol{C})$ and $W^{\vee} = Hom_{\mathbb{Z}_p}(T(G^{\vee}), \boldsymbol{C})$.

By Hodge-Tate Lemma, we have

$$t_G(\boldsymbol{C}) = t_G(K) \otimes_K C = t_G(\boldsymbol{C})^{\mathcal{G}} \otimes_K C \hookrightarrow W^{\vee},$$

and

$$t_{G^{\vee}}(\boldsymbol{C}) = t_{G^{\vee}}(K) \otimes_K C = t_{G^{\vee}}(\boldsymbol{C})^{\mathcal{G}} \otimes_K \boldsymbol{C} \hookrightarrow W.$$

(2) We have a perfect pairing $W \times W^{\vee} \to Hom(H; C) = Y$.

(3) $t_G(\boldsymbol{C})$ and $t_{G^{\vee}}(\boldsymbol{C})$ are orthogonal.

(4) $0 \to t_{G^\vee}(\boldsymbol{C}) \overset{d\alpha^\vee}{\to} W \to Hom_{\boldsymbol{C}}(t_G(\boldsymbol{C}); Y) = t^\star_G(\boldsymbol{C}) \otimes Hom(H; \boldsymbol{C}) \to 0$.

(5) The sequence in (4) is of the type

$$0 \to \boldsymbol{C}^{n'} \to W \to \boldsymbol{C}(\chi^{-1})^n \to 0.$$

$\xrightarrow{\otimes C(\chi)}$

$$0 \to \boldsymbol{C}(\chi)^{n'} \to W \otimes \boldsymbol{C}(\chi) \to \boldsymbol{C}^n \to 0.$$

Here $\mathcal{G}$ acts on H as the cyclotomic character χ.

(6) By $H^1(\mathcal{G}; \boldsymbol{C}(\chi)) = 0$, the sequence splits and by $H^0(\mathcal{G}; \boldsymbol{C}(\chi)) = 0$ we know the sequence splits uniquely.

Example 23. If $G = X(p)$ for some abelian variety X, then the Hodge-Tate decomposition implies that we have a decomposition of the first p-adic etale cohomology of $X \otimes K$.

Theorem 24. *Let R be an integrally closed notherian domain, whose function field is of characteristic 0. Let G and H be p-divisible groups over R. A homomorphism*

$$f : G \otimes_R K \to H \otimes_R K$$

of the generic fiber extends uniquely to a homomorphism $G \to H$.

For povering this theorem, we need following lemma.

Lemma 25. *(1) If $f : G \to H$ is a homomorphism such that $f \otimes_R K$ is an isomorphism, then f is an isomorphism.*

(2) Let H^* be a p-divisible subgroup of $G \otimes_R K$, then there exists a p-divisible subgroup H of G such that $H \otimes_R K$ is H^*.

Proof of theorem 24:

Since R is integrally closed domain, we have $R = \bigcap R_p$, where p runs through all minimal primes of R. Therefore we are reduced to the case of discrete valuation ring. By passing to the completion, we only need to consider the case of complete discrete valuation ring by faithfully flat descent. If the residue field has characteristic $\neq p$, the category of finite flat group schemes is equivalent to the category of finite Galois modules. In this case we are working with etale group schemes and the lifting is trivial.

Assume the **lemma 25** be hold. Given a map

$$f : G \otimes_R K \to H \otimes_R K,$$

We can consider its graph $\Gamma^* \subset (G \times H) \otimes_R K$. By the second statement of the lemma, we can find a p-divisible subgroup $\Gamma \subset (G \times H)$. Since

$$pr_1 \otimes_R K : \Gamma^* \to G \otimes_R K$$

is an isomorphism, by the first statement of lemma, we have

$$pr_1 : \Gamma \to G$$

is an isomorphism. Therefore, we have an extended map

$$pr_2 \circ pr_1^{-1} : G \to \Gamma \to H.$$

The uniqueness is trivial.

For lemma 25 (2):

Pick the closure $\tilde{H}_v$ of each H_v^* in G_v .Take

$$H_v = \varprojlim_{\mu} Ker(p^v : \tilde{H_{\mu+v}} \to \tilde{H_{\mu+v}}).$$

One checks that H_v is desired the p-divisible group.

For lemma 25 (1):

The discriminants of the two p-divisible groups are equal. Thus f must be an isomorphism.

Corollary 26. *There is a fully faithful functor $G \to T(G)$ from the category of p-divisible groups over R to the category of the Tate modules (with Galois action). Precisely, we have*

$$Hom(G, H) = Hom_{\mathcal{G}}(T(G), T(H)).$$

([3], p. 181)

References

[1] C. Waterhouse, Introduction to affine group schemes. vol. 66, GTM, Springer, Berlin-Heidelberg New York 1979.

[2] B. Conrad, M. Lieblich: Galois representations arising from p-divisible groups. Available on http://www.math.lsa.umich.edu/~bdconrad/CompleteNotes.pdf.

[3] J. Tate, p-divisible groups, Proc. Conf. Local fields (Driebergen,1966), 158-183.

[4] R. Pink, Finite group schemes, available on http://www.ma-th.ethz.ch/~pink/ftp/FGS.

[5] J.P. Serre, Lie algebras and Lie groups. New York: Benjamin 1965.

[6] J. Tate, F. Oort, Group schemes of prime order. Annales scientifiques de l'École Normale Supérieure, Sér. 4, 3 no. 1 1970.