INSTITUT DE FRANCE
Académie des sciences

Comptes Rendus

Mathématique

Duc Hiep Pham

p-adic non-commutative analytic subgroup theorem

Volume 360 (2022), p. 933-936

https://doi.org/10.5802/crmath.325

CENTRE MERSENNE

Les Comptes Rendus. Mathématique *sont membres du*
Centre Mersenne pour l'édition scientifique ouverte
www.centre-mersenne.org
e-ISSN : 1778-3569

Comptes Rendus
Mathématique
2022, Vol. 360, p. 933-936
https://doi.org/10.5802/crmath.325

Number theory / *Théorie des nombres*

p-adic non-commutative analytic subgroup theorem

Duc Hiep Pham [a]

[a] University of Education, Vietnam National University, Hanoi, 144 Xuan Thuy, Cau
Giay, Hanoi, Vietnam
E-mail: phamduchiep@vnu.edu.vn

In memory of my father, Duc Hoa Pham

Abstract. In this paper, we formulate and prove the so-called p-adic non-commutative analytic subgroup theorem. This result is seen as the p-adic analogue of a recent theorem given by Yafaev in [11].

2020 Mathematics Subject Classification. 14L10, 22E35, 11F85, 11J81.

Manuscript received 15 July 2021, revised 20 September 2021, accepted 10 January 2022.

1. Introduction

It is known that the analytic subgroup theorem is considered as one of the most powerful theorems in complex transcendental number theory. The theorem was established by Wüstholz in the 1980's based on a very deep auxiliary result on multiplicity estimates on group varieties (see [8] and [9]). To present the theorem, we start with G a commutative algebraic group defined over $\overline{\mathbb{Q}}$, that is a smooth quasi-projective variety defined over $\overline{\mathbb{Q}}$ with a commutative group law for which the composition map $G\times G \to G,\ (g,h)\mapsto g\circ h$ and the inverse map $G\to G,\ g\mapsto g^{-1}$ are regular morphisms between algebraic varieties defined over $\overline{\mathbb{Q}}$. Then the set $G(\mathbb{C})$ of complex points of G is a complex Lie group, and one has the exponential map $\exp_{G(\mathbb{C})}:\mathrm{Lie}(G(\mathbb{C}))\to G(\mathbb{C})$ of G. We say that an element $u\in\mathrm{Lie}(G(\mathbb{C}))$ is an algebraic point of the exponential map of G if $\exp_{G(\mathbb{C})}(u)\in G(\overline{\mathbb{Q}})$. The following theorem is a direct consequence of [7, Theorem 1], and it is still called *the analytic subgroup theorem* (see also [6, Theorem 1.2]).

Theorem 1 (Wüstholz). *Let G be a connected commutative algebraic group defined over $\overline{\mathbb{Q}}$. Let $u\in\mathrm{Lie}(G(\mathbb{C}))$ be an algebraic point of the exponential map of G and V_u the smallest $\overline{\mathbb{Q}}$-vector subspace of*$\mathrm{Lie}(G)$ *such that u lies in the complex vector space $V_u\otimes_{\overline{\mathbb{Q}}}\mathbb{C}$. Then there exists a connected algebraic subgroup H_u of G defined over $\overline{\mathbb{Q}}$ satisfying* $\mathrm{Lie}(H_u)=V_u$.

Many results in transcendence theory can be deduced from Wüstholz analytic subgroup theorem as consequences by choosing suitable commutative algebraic groups. For instance, the theorem generalizes Baker's famous result on linear forms in logarithms and its elliptic analogue in full generality (see [1, Chapter 6]). It implies some important results concerning

ISSN (electronic) : 1778-3569

linear independence of periods of abelian varieties (see [6, Chapter 1]). Furthermore, Wüstholz himself has recently obtained a nice application on elliptic and abelian periods spaces (see[10]).

It is possible to extend Theorem 1 to the non-commutative case. Note that in this case, there is still the exponential map between the Lie algebra and the Lie group as the commutative case. The following theorem has been recently proved by Yafaev (see [11]).

Theorem 2 (Yafaev). *Let G be a connected algebraic group defined over $\overline{\mathbb{Q}}$. Let $u \in \mathrm{Lie}(G(\mathbb{C}))$ be an algebraic point of the exponential map of G and V_u the smallest $\overline{\mathbb{Q}}$-vector subspace of $\mathrm{Lie}(G)$ such that u lies in the complex vector space $V_u \otimes_{\overline{\mathbb{Q}}} \mathbb{C}$. Then there exists a connected algebraic subgroup H_u of G defined over $\overline{\mathbb{Q}}$ which is commutative and satisfies $\mathrm{Lie}(H_u) = V_u$.*

In 2015, Fuch and Pham obtained the p-adic analytic subgroup theorem (see [3]), and the aim of this paper is to obtain a p-adic analogue of Theorem 2 above. In the p-adic setting, similar to [3, Theorem 2.2], we also use the p-adic logarithm map which is still valid in the non-commutative case. Fix a prime number p, let $\mathbb{Q}_p$ be the field of p-adic numbers. Denote by $\mathbb{C}_p$ the completion of the algebraic closure of $\mathbb{Q}_p$ (with respect to the normalized p-adic absolute value). Let G now be an algebraic group defined over $\overline{\mathbb{Q}}$. Consider the set $G(\mathbb{C}_p)$ of $\mathbb{C}_p$-points of G. This is a Lie group over $\mathbb{C}_p$. Denote by $G(\mathbb{C}_p)_f$ the set of x in $G(\mathbb{C}_p)$ satisfying the condition that there exists a strictly increasing sequence (n_i) of positive integers for which x^{n_i} tends to the identity element of $G(\mathbb{C}_p)$ as i tends to infinity. It follows from [2, Chapter III, 7.6] that there is a $\mathbb{C}_p$-analytic map $\log_{G(\mathbb{C}_p)} : G(\mathbb{C}_p)_f \to \mathrm{Lie}(G(\mathbb{C}_p))$, and it is called the *$p$-adic logarithm map* of G. Then *the p-adic non-commutative analytic subgroup theorem* is formulated as follows.

Theorem 3. *Let G be a connected algebraic group defined over $\overline{\mathbb{Q}}$ of positive dimension, and $\log_{G(\mathbb{C}_p)} : G(\mathbb{C}_p)_f \to \mathrm{Lie}(G(\mathbb{C}_p))$ the p-adic logarithm map of G. Let $\gamma \in G(\mathbb{C}_p)_f$ be an algebraic point of $G(\overline{\mathbb{Q}})$ with $\log_{G(\mathbb{C}_p)}(\gamma) \neq 0$ and V_γ the smallest $\overline{\mathbb{Q}}$-vector subspace of $\mathrm{Lie}(G)$ such that the p-adic vector space $V_\gamma \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p$ contains $\log_{G(\mathbb{C}_p)}(\gamma)$. Then there exists a connected commutative algebraic subgroup $H_\gamma \subseteq G$ defined over $\overline{\mathbb{Q}}$ of positive dimension satisfying $\gamma \in H_\gamma(\overline{\mathbb{Q}})$ and $\mathrm{Lie}(H_\gamma) = V$.*

The proof of our theorem follows closely that of Yafaev's theorem. We also reduce the general case to the commutative case and then apply the p-adic analytic subgroup theorem. The main difference is that, in the p-adic setting, the p-adic exponential map is only defined locally on an open subgroup of the p-adic Lie algebra of the given algebraic group. However, by using the p-adic logarithm map and by taking a certain power of the algebraic point, we are able to still keep the important similar arguments as in the complex case, and based on this to get the derised result.

2. The p-adic exponential map and related commutative algebraic subgroups

In this section, we first briefly recall some background on exponential and logarithm maps over p-adic fields. The main reference we follow here is [2]. For an algebraic group G defined over $\overline{\mathbb{Q}}$, by [2, Chapter III, 7.2, 7.6] there exist an open subgroup U_p of $\mathrm{Lie}(G(\mathbb{C}_p))$ and an analytic map $\exp_{G(\mathbb{C}_p)} : U_p \to G(\mathbb{C}_p)$ such that $\exp_{G(\mathbb{C}_p)}(U_p)$ is an open subgroup of $G(\mathbb{C}_p)$, and the map $\exp_{G(\mathbb{C}_p)}$ induces an isomorphism between U_p and $\exp_{G(\mathbb{C}_p)}(U_p) \subseteq G(\mathbb{C}_p)_f$, whose inverse is the restriction of $\log_{G(\mathbb{C}_p)}$ to $\exp_{G(\mathbb{C}_p)}(G_p)$. The map $\exp_{G(\mathbb{C}_p)}$ is called the *p-adic exponential map of G*. For an element u in U_p and for a subset S in $\mathbb{C}_p$, define $S \cdot u$ by the set $\{su; s \in S\}$. The following lemma plays a central role in the proof of the main theorem which allows us to construct a relevant commutative algebraic subgroup of G defined over $\overline{\mathbb{Q}}$.

Lemma 4. *Let G be an algebraic group defined over $\overline{\mathbb{Q}}$. Let u be an element in U_p with* $\exp_{G(\mathbb{C}_p)}(u) \in G(\overline{\mathbb{Q}})$. *Denote by G_u the Zariski closure of the set* $\exp_{G(\mathbb{C}_p)}((\mathbb{C}_p \cdot u) \cap U_p)$ *in $G(\mathbb{C}_p)$. Then G_u is a commutative algebraic subgroup of G defined over $\overline{\mathbb{Q}}$ and* $\exp_{G(\mathbb{C}_p)}(u) \in G_u(\overline{\mathbb{Q}})$.

Proof. Put $\Phi_u := \exp_{G(\mathbb{C}_p)}((\mathbb{C}_p \cdot u) \cap U_p)$. We first see that any two elements $x, y \in \mathbb{C}_p \cdot u$ commute, and therefore

$$\exp_{G(\mathbb{C}_p)}(x)\exp_{G(\mathbb{C}_p)}(y) = \exp_{G(\mathbb{C}_p)}(x+y) = \exp_{G(\mathbb{C}_p)}(y+x) = \exp_{G(\mathbb{C}_p)}(y)\exp_{G(\mathbb{C}_p)}(x),$$

by Campbell–Hausdorff formula (see [5, Section 16]). In particular, this shows that Φ_u is a commutative subgroup of $G(\mathbb{C}_p)$. It follows from [4, Lemma 1.40] that the Zariski closure G_u of Φ_u is an algebraic subgroup of $G(\mathbb{C}_p)$. We now consider the commutator morphism $f : G_u \times G_u \to G_u$ given by $f(x, y) = [x, y]$. Then f is an algebraic morphism and trivial on $\Phi_u \times \Phi_u$. This gives $\Phi_u \times \Phi_u$ is contained in the algebraic set $f^{-1}(e)$, where e denotes the identity element of G. But $\Phi_u \times \Phi_u$ is Zariski-dense in $G_u \times G_u$, this implies that the morphism f must be trivial on $G_u \times G_u$. In other words, G_u is commutative. It remains to show that G_u is defined over $\overline{\mathbb{Q}}$. If $u = 0$ then G_u is the trivial group, and hence clearly defined over $\overline{\mathbb{Q}}$. Assume $u \neq 0$, let Γ_u denote the image of the set $(\mathbb{Q} \cdot u) \cap U_p$ under the map $\exp_{G(\mathbb{C}_p)}$. As above, we also have that Γ_u is a subgroup of $G(\mathbb{C}_p)$, and therefore by [4, Lemma 1.40] again the Zariski closure G'_u of Γ_u in $G(\mathbb{C}_p)$ is an algebraic group. On the other hand, since $\exp_{G(\mathbb{C}_p)}(u) \in G(\overline{\mathbb{Q}})$, it follows that $\exp_{G(\mathbb{C}_p)}(u) \in G_u(\overline{\mathbb{Q}})$. Note that $\exp_{G(\mathbb{C}_p)}(mu) = \exp_{G(\mathbb{C}_p)}(u)^m$ for all $m \in \mathbb{Z}$, and this leads to Γ_u is contained in $G_u(\overline{\mathbb{Q}})$. Hence, the algebraic group G'_u must be defined over $\overline{\mathbb{Q}}$. Moreover, the group Γ_u is infinite (since $u \neq 0$), thus the algebraic group G'_u has positive dimension.

Next, one has $\exp_{G(\mathbb{C}_p)}(u) \in G'_u(\overline{\mathbb{Q}}) \cap G(\mathbb{C}_p)_f \subseteq G'_u(\mathbb{C}_p)_f$. This gives

$$u = \log_{G(\mathbb{C}_p)}\left(\exp_{G(\mathbb{C}_p)}(u)\right) = \log_{G'_u(\mathbb{C}_p)}\left(\exp_{G(\mathbb{C}_p)}(u)\right) \in \mathrm{Lie}(G'_u(\mathbb{C}_p)).$$

Since $\mathrm{Lie}(G'_u(\mathbb{C}_p))$ is a vector space over $\mathbb{C}_p$, it follows that the line $\mathbb{C}_p \cdot u$ is also contained in $\mathrm{Lie}(G'_u(\mathbb{C}_p))$. From this, we get

$$\Phi_u \subseteq \exp_{G(\mathbb{C}_p)}\left(\mathrm{Lie}(G'_u(\mathbb{C}_p)) \cap U_p\right) = \exp_{G'_u(\mathbb{C}_p)}\left(\mathrm{Lie}(G'_u(\mathbb{C}_p)) \cap U_p\right) \subseteq G'_u(\mathbb{C}_p).$$

This allows us to deduce that $G_u(\mathbb{C}_p) \subseteq G'_u(\mathbb{C}_p)$. But, by definition, $G'_u(\mathbb{C}_p)$ is obviously contained in $G_u(\mathbb{C}_p)$. Therefore, we conclude that $G_u = G'_u$, and this completes the proof of the lemma. □

3. Proof of the main theorem

We are now ready to prove the main theorem. Let $\exp_{G(\mathbb{C}_p)} : U_p \to G(\mathbb{C}_p)$ be the p-adic exponential map of G defined as in Section 2. By definition of the set $G(\mathbb{C}_p)_f$, there is a positive integer k such that $\gamma^k \in U_p$. Let u be the point $\log_{G(\mathbb{C}_p)}(\gamma^k)$. We have

$$\exp_{G(\mathbb{C}_p)}(u) = \exp_{G(\mathbb{C}_p)}\left(\log_{G(\mathbb{C}_p)}(\gamma^k)\right) = \gamma^k \in G(\overline{\mathbb{Q}}).$$

Using Lemma 4, there exists a commutative algebraic subgroup G_u of G defined over $\overline{\mathbb{Q}}$ of positive dimension with $\exp_{G(\mathbb{C}_p)}(u) \in G_u(\overline{\mathbb{Q}})$. This also gives $\exp_{G(\mathbb{C}_p)}(u) \in G_u(\mathbb{C}_p)_f$, and hence

$$\log_{G(\mathbb{C}_p)}(\gamma^k) = u \in \mathrm{Lie}(G_u(\mathbb{C}_p)) \subseteq \mathrm{Lie}(G(\mathbb{C}_p)).$$

On the other hand, it follows from [2, Chapter III, 7.6] that

$$\log_{G(\mathbb{C}_p)}(\gamma^k) = k\log_{G(\mathbb{C}_p)}(\gamma) \in V_\gamma \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p.$$

In particular, this implies that $V_\gamma \subseteq \mathrm{Lie}(G_u)$. This enables us to apply the p-adic analytic subgroup theorem ([3, Theorem 2.2]) to the commutative algebraic group G_u, the algebraic point γ^k and the $\overline{\mathbb{Q}}$-vector space V_γ to obtain an algebraic (commutative) subgroup H of G defined over $\overline{\mathbb{Q}}$ of positive dimension such that $\mathrm{Lie}(H) \subseteq V_\gamma$ and $\gamma^k \in H(\overline{\mathbb{Q}})$. Let H^0 be the connected component of

H, then $\mathrm{Lie}(H^0) = \mathrm{Lie}(H)$ and there is a positive integer m for which $(\gamma^k)^m \in H^0(\overline{\mathbb{Q}})$. Put $n = km$ and take the algebraic subgroup H_γ of G_u with $H_\gamma(\overline{\mathbb{Q}}) = \{\alpha \in G_u(\overline{\mathbb{Q}}) : \alpha^n \in H^0(\overline{\mathbb{Q}})\}$. Then $\gamma \in H_\gamma$ and $\mathrm{Lie}(H_\gamma) \subseteq V_\gamma$. This leads to

$$\log_{G(\mathbb{C}_p)}(\gamma) = \log_{H_\gamma(\mathbb{C}_p)}(\gamma) \in \mathrm{Lie}(H_\gamma(\mathbb{C}_p)) = \mathrm{Lie}(H_\gamma) \otimes_{\overline{\mathbb{Q}}} \mathbb{C}_p.$$

By the minimality of the $\overline{\mathbb{Q}}$-vector space V_γ, we conclude that $\mathrm{Lie}(H_\gamma) = V_\gamma$. The theorem is therefore proved. □

Remark. Using the same arguments as in the proof of [11, Theorem 1.5] to deduce it from the non-commutative analytic subgroup theorem, we use our p-adic analogue to deduce the following:

Theorem 5. *Let G be an algebraic group defined over* $\overline{\mathbb{Q}}$ *and* $\exp_{G(\mathbb{C}_p)} : U_p \to G(\mathbb{C}_p)$ *be the p-adic exponential map of G. Let u be a non-zero element of* $U_p \cap \mathrm{Lie}(G)$ *such that* $\exp_{G(\mathbb{C}_p)}(u)$ *lies in* $G(\overline{\mathbb{Q}})$.

(1) *The element* $\exp_{G(\mathbb{C}_p)}(u)$ *is contained in a subgroup isomorphic to the additive group* $\mathbb{G}_a$.

(2) *Assume G is an affine algebraic group. The element u is a nilpotent element of* $\mathrm{Lie}(G(\mathbb{C}_p))$, *and hence* $\exp_{G(\mathbb{C}_p)}(u)$ *is a unipotent element of* $G(\mathbb{C}_p)$.

Acknowledgements

The author would like to thank the anonymous referee for careful reading of this manuscript and useful comments.

References

[1] A. Baker, G. Wüstholz, *Logarithmic Forms and Diophantine Geometry*, New Mathematical Monographs, vol. 9, Cambridge University Press, 2007.

[2] N. Bourbaki, *Elements of Mathematics. Lie groups and Lie algebras. Part I: Chapters 1-3. English translantion*, Actualités Scientifiques et Industrielles, Addison-Wesley Publishing Group, 1975.

[3] C. Fuchs, D. H. Pham, "The p-adic analytic subgroup theorem revisited", *p-Adic Numbers Ultrametric Anal. Appl.* **7** (2015), no. 2, p. 143-156.

[4] J. S. Milne, *Algebraic Groups. The theory of group schemes of finite type over a field*, Cambridge Studies in Advanced Mathematics, vol. 170, Cambridge University Press, 2017.

[5] P. Schneider, *p-adic Lie groups*, Grundlehren der Mathematischen Wissenschaften, Springer, 2011.

[6] P. Tretkoff, *Periods and Special Functions in Transcendence*, Advanced Textbooks in Mathematics, World Scientific, 2017.

[7] G. Wüstholz, "Some remarks on a conjecture of Waldschmidt", in *Approximations diophantiennes et nombres transcendants*, Progress in Mathematics, vol. 31, Birkhäuser, 1983, p. 329-336.

[8] ———, "Multiplicity estimates on group varieties", *Ann. Math.* **129** (1989), p. 471-500.

[9] ———, "Algebraische Punkte auf Analytischen Untergruppen algebraischer Gruppen", *Ann. Math.* **129** (1989), p. 501-517.

[10] ———, "Elliptic and abelian period spaces", *Acta Arith.* **198** (2021), p. 329-357.

[11] A. Yafaev, "Non-commutative analytic subgroup theorem", *J. Number Theory* **230** (2022), p. 233-237.