國立臺灣大學理學院數學系
碩士論文
Department of Mathematics
College of Science
National Taiwan University
Master Thesis

無全域良化約之阿貝爾簇

There are no abelian schemes over $\mathbb{Z}$

李俊緯
Chun-Wei Lee

指導教授：陳其誠博士
Advisor: Ki-Shen Tan, Ph.D.

中華民國 106 年 7 月
July, 2017

doi:10.6342/NTU201701790

doi:10.6342/NTU201701790

誌謝

能完成這篇論文，我最感謝的是我的指導老師陳其誠老師。在完成這篇論文的過程中，無數次地遇到難以解決的問題，幾乎每次都是在跟老師的討論中茅塞頓開。同時老師的講解也給了我非常多的啟發，了解自己過去所忽略的地方，並且提升研究的能力。老師更常常在我沒有信心的時候給予鼓勵，我都銘記於心。

我還要感謝口試委員謝銘倫老師與紀文鎮老師的建議，指出我的論文不足之處，讓我的論文內容更加完整，架構更加適當。另外，感謝我的同學們平時的陪伴與打氣。以及感謝系辦的王雅真小姐幫我們處理相關的繁雜事物，讓我能專心寫作論文。

最後感謝台灣大學數學系，提供優良的學習環境，讓我在碩士班的兩年裡，有著充實且愉快的學習歷程。

doi:10.6342/NTU201701790

doi:10.6342/NTU201701790

Acknowledgements

I'm glad to thank my advisor Professor Ki-Shen Tan, for begin able to complete this thesis. In completing the thesis, I encountered questions that I find difficult to solve for numerous times, and almost always I was enlightened during discussions with the professor. In the mean time, the professor's explanations inspired me a lot, to understand what I ignored and improve the ability to research. Further, the professor encouraged me when I lacked confidence. I keep all this in mind.

I also want to thank the commitees professor Ming-Lun Hsieh and Wen-Chen Chi for pointing out the inadequacies of the thesis so that it becomes more complete, and with a more adequate structure. In addition, thanks go to my classmates for the companionship and encouragement. Also thanks Miss Ya-Jhen Wang for dealing with the daily businesses, so that I can concentrate on writing the thesis.

Finally I want to thank the department of mathematics of NTU for providing a good environment for learning mathematics so that I have a full and pleasant learning experience during the two years.

doi:10.6342/NTU201701790

doi:10.6342/NTU201701790

摘要

阿貝爾簇是一個有阿貝爾群結構的簇。這些簇是在多個數學領域裡有特別重要性的幾何物件。我們對於有理數上的阿貝爾簇在不同質數下的化約感興趣。特別的，我們想知道是否一個阿貝爾簇的化約仍然是阿貝爾簇。我們知道一個阿貝爾簇只會在有限個質數上的化約不是阿貝爾簇。不過一個阿貝爾簇不會在所有質數上的化約都是阿貝爾簇。這是 Fontaine 的定理。但 Fontaine 的證明對於初學者來說並不容易，所以我展開證明中的細節，讓潛在的讀者更能了解。

doi:10.6342/NTU201701790

doi:10.6342/NTU201701790

Abstract

A variety is called an abelian variety if it has an abelian group structure. These varieties are special geometric objects of particular importance in multiple mathematics fields. We are concerned with the reductions of abelian varieties over the field of rational numbers modulo different primes. In particular, we are interested in whether the reduction of an abelian variety remains an abelian variety. It is well-known for years that the reduction is still an abelian variety, except for finitely many primes. However, it cannot be an abelian variety modulo every prime. This is a theorem of Fontaine. But Fontaine's proof is not easy for beginners. So I expound the details of the proof to make it easier for potential readers.

doi:10.6342/NTU201701790

doi:10.6342/NTU201701790

Contents

誌謝 iii

Acknowledgements v

摘要 vii

Abstract ix

1 Introduction 1

1.1 The main result 1

1.2 Notation 4

2 Group schemes 4

2.1 Examples 5

2.2 The Cartier duality and Deligne's theorem 6

2.3 Étale group schemes 10

2.4 Local group schemes 12

3 Fontaine's bound and its consequences 15

3.1 The ramification theory 16

3.2 Divided power sturctures 21

3.3 The relative differential forms 24

3.4 The proof 28

4 The choice of a prime 32

4.1 The global ramification theory 33

4.2 The decomposition theorem 38

doi:10.6342/NTU201701790

Appendices **45**

1 Rank 2 groups 45

2 An increasing function 46

Bibliography **49**

doi:10.6342/NTU201701790

List of Figures

doi:10.6342/NTU201701790

doi:10.6342/NTU201701790

List of Tables

1 The values of $f(n)$ 34

doi:10.6342/NTU201701790

doi:10.6342/NTU201701790

1 Introduction

Abelian varieties are abelian group objects in the category of complete [1] varieties. An abelian variety A over a field K with a discrete valuation v, valuation ring $\mathcal{O}_v$, and residue field k_v is said to have good reduction at v if there is an abelian scheme $\mathscr{A}_v$ over $\mathrm{Spec}(\mathcal{O}_v)$ such that $A \cong \mathscr{A}_v \otimes_{\mathcal{O}_v} K$. In this case, the special fiber $\bar{A} := \mathscr{A}_v \otimes_{\mathcal{O}_v} k_v$ is an abelian variety over k_v.

An interesting question is: Does there exist an abelian variety over $\mathbb{Q}$ with good reduction at every prime number?

Fontaine proved ([3]) that there cannot exist an abelian variety over $\mathbb{Q}$ with good reduction at every prime number. The proof in [3] is complicated and not easy for beginners. The aim of this article is to expound the details of the proof, and hence make it easier to understand for potential readers.

1.1 The main result

To be precise, the main theorem we are to prove is the following.

Theorem 1.1. *There cannot exist an abelian variety over $\mathbb{Q}$ with good reduction at every prime number.*

Let A be an abelian variety over $\mathbb{Q}$ and let $\mathscr{A}$ denote its Néron model over $\mathbb{Z}$ so that A is the generic fibre of $\mathscr{A}$ and

$$A(\mathbb{Q}) = \mathscr{A}(\mathbb{Q}) = \mathscr{A}(\mathbb{Z}).$$

If A has good reduction everywhere, then $\mathscr{A}$ is an abelian scheme over $\mathbb{Z}$, as the special fibres of $\mathscr{A}$ are abelian varieties, by [7, Proposition 20]; the kernel $\mathscr{A}_n$ of the multiplication by n on $\mathscr{A}$ is a finite flat group scheme over $\mathbb{Z}$. If $v = p$, $\mathcal{O}_v = \mathbb{Z}_{(p)}$, the afore-mentioned $\mathscr{A}_v$ can be taken as $\mathscr{A} \otimes_{\mathbb{Z}} \mathbb{Z}_{(p)}$.

Here we demonstrate how Lemma 1.1 below, together with the more well-known Lemma 1.2, can lead to the proof of the theorem.

[1] A variety X is called complete if for any variety Y, the projection $X \times Y \to Y$ is a closed map.

doi:10.6342/NTU201701790

Proof. Let p be the prime 3. Suppose A is of dimension g. The system $(\mathscr{A}_{p^n})_{n\in\mathbb{N}}$ is a p-divisible group over $\mathbb{Z}$ of dimension $2g$. By Lemma 1.1, we have

$$(\mathscr{A}_{p^n})_n \cong (\mathbb{Q}_p/\mathbb{Z}_p)^g \oplus (\mu_{p^\infty})^g.$$

This shows that $A(\mathbb{Q})$ has infinitely many p-torsion elements. But this is impossible: Let $q \neq p$ be a prime and let $k_q = \mathbb{Z}/q\mathbb{Z}$. We shall show that the reduction map induces an injection into a finite group: $\cup_n A_{p^n}(\mathbb{Q}) \to \cup_n \bar{A}_{p^n}(k_q)$. For this, it suffices to show that $A_{p^n}(\bar{\mathbb{Q}}) \to \bar{A}_{p^n}(\bar{k}_q)$ is injective. By [7, Proposition 20], both $A_{p^n}(\bar{\mathbb{Q}})$ and $\bar{A}_{p^n}(\bar{k}_q)$ are of order p^{2ng}, thus, the map is injective if and only it is surjective.

Then take K such that $A_{p^n}(\bar{\mathbb{Q}}) = A_{p^n}(K)$. By Lemma 1.2, the reduction map is a surjection. □

The following lemma manifests all works in [3] prior to the main theorem.

Lemma 1.1. Let $\mathscr{A}$ be an abelian scheme over $\mathbb{Z}$ of dimension g, and let $p = 3$. Then $\mathscr{A}_{p^n} \cong (\mathbb{Z}/p^n\mathbb{Z})^g \oplus (\mu_{p^n})^g$.

Proof. This will be proved in Proposition 4.1. □

Lemma 1.2. Let K be a field with a discrete valuation v and a complete valuation ring $\mathcal{O}_v$. Denote $k = \mathcal{O}_v/\mathfrak{m}_v$. Let $X = \mathrm{Spec}(B)$ be a finite flat scheme over $\mathcal{O}_v$. Let $\bar{X} = \mathrm{Spec}(\bar{B})$ be the special fiber of X, where $\bar{B} = B \otimes_{\mathcal{O}_v} k$. Suppose $X(K) = X(\bar{K})$. Then the reduction map $X(\mathcal{O}_v) \to X(k) = \bar{X}(k)$ is surjective.

Remark 1.1.

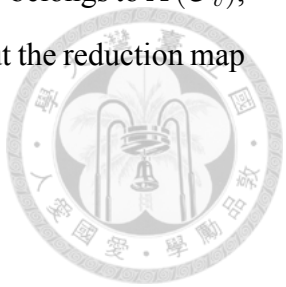
1. Note that the reduction map sends a point $x : B \to \mathcal{O}_v$ to $\bar{x} : B \to k$. And this reduction map is in general not surjective.

   For example, take $\mathcal{O}_v = \mathbb{Z}_{(p)}$, $\mathfrak{m}_v = (p)$, $k = \mathbb{F}_p$, $K = \mathbb{Q}_p$, $B = \mathcal{O}_v[\xi]$, where $\xi = \sqrt{p}$. Then $\bar{B} = \mathbb{F}_p[T]/(T^2)$, so there is a point in $\bar{X}(k)$ sending T to 0.

   But if $x : B \to \mathcal{O}_v$ is a point, then x sends ξ to some η in $\mathcal{O}_v$ such that $\eta^2 = p$, which is impossible. Hence $X(K) = \emptyset$.

doi:10.6342/NTU201701790

2. Moreover, if B is finite over $\mathcal{O}_v$, then any point in $X(K)$ actually belongs to $X(\mathcal{O}_v)$, for $\mathcal{O}_v$ is integrally closed. Therefore it makes sense to talk about the reduction map $X(K) \to \bar{X}(k)$.



Proof. By [6, §1, Theorem 4.2(b)], we have

$$B \cong B_1 \times \cdots B_i \times \cdots \times B_m,$$

where each B_i is a local finite flat algebra over $\mathcal{O}_v$. It is endowed with $\mathfrak{m}_v$-adic topology.

Each point in $X(k)$ corresponds to a homomorphism $\alpha : B \to k$. Since the powers of the elements in $\mathfrak{m}_{B_1} \times \cdots \times \mathfrak{m}_{B_m}$ converge to 0, they are mapped to 0 by α. Thus α factors through $B \to \prod_i B_i/\mathfrak{m}_{B_i} \to k$. And $\prod_i B_i/\mathfrak{m}_{B_i} \to k$ must factor through some $B_i/\mathfrak{m}_{B_i}$, as k is a field.

From the maps $B_i/\mathfrak{m}B_i \twoheadrightarrow k$ and $k \hookrightarrow B_i/\mathfrak{m}_{B_i}$ we see that $B_i/\mathfrak{m}_{B_i} = k$. Thus there can only be one k-homomorphism $B_i/\mathfrak{m}_{B_i} \to k$.

Now we show that there is a $\mathcal{O}_v$-homomorphism $B_i \to \mathcal{O}_v$ so that its reduction must give rise to the unique k-homomorphism $B_i/\mathfrak{m}_{B_i} \to k$, and hence the reduction is surjective.

The Artinian K-algebra $B_i \otimes_{\mathcal{O}_v} K$ can be written as $B_i \otimes_{\mathcal{O}_v} K = \prod_{j=1}^{\ell} A_j$ where each A_j is an Artinian local ring. Let K_j denote the residue field of A_j. Since K is a localisation of $\mathcal{O}_v$, it is a flat $\mathcal{O}_v$-module. Thus we have a monomorphism $K \hookrightarrow \prod_j A_j$. Since K has no non-zero zero-divisors, the image must lie in some A_j. Further, as the elements in K whose powers converge to 0 are zero, its image in A_j is not contained in $\mathfrak{m}_{A_j}$. So there is a non-zero homomorphism between fields $K \to K_j$, hence a monomorphism. This means each K_j is a finite extension of K. So we have a homomorphism $B_i \to K_j \to \bar{K}$. By the assumption this homomorphism has image in K, so we have a homomorphism $B_i \to K$.

Since B_i is finite over $\mathcal{O}_v$, so is its image in K. But $\mathcal{O}_v$ is integrally closed, so we have a $\mathcal{O}_v$-homomorphism $B_i \to \mathcal{O}_v$. This completes the proof. □

The key ingredient in the above proof is Propostion 4.1, which follows from Theorem 4.1. And Theorem 4.1 will be proved in §4.2. The main tools used are the theory of group

doi:10.6342/NTU201701790

schemes and the ramification theory.

In §2, we review basic facts on group schemes for later application. In §3, we study the theory of ramification. Then it will incorporate with the material in §2 as well as tools involving the divided power structures and relative differentials into a proof of Theorem 3.1. That theorem gives a nice bound on the upper numbering for the ramification groups to become trivial. Other than this, the proof of Theorem 4.1 also uses a result of Raynaud, Theorem 4.2. Unfortunately, we can only state it in §4 without further discussion.

Basically, this article is a report on a published paper. Hence the author has no intension to claim that there is any newly proved statement in this article. Any assertion in this article can be found in some published materials, or be deduced straightforwardly form those.

1.2 Notation

In this paper, X denotes a scheme, J denotes a finite flat group scheme, G denotes the Galois group of some extension, B denotes a Hopf algebra, and Γ denotes a finite group. Also, we oft use R to denote the base commutative ring, and S some R-algebra.

If K is a number field or a local field, we write $\mathcal{O}_K$ for its ring of integers. If B is a local ring we use $\mathfrak{m}_B$ to denote the maximal ideal. When K is a local field we often write $\mathfrak{m}_K$ for $\mathfrak{m}_{\mathcal{O}_K}$, and use k to denote the residue field.

2 Group schemes

In this section, we review some basic properties of group schemes. For the purposes of this article, a group scheme over a commutative ring R is defined as a representable functor from the category of R-algebras to the category of groups. By abuse of language, we also say that the representing scheme is a group scheme.

If J is a finite flat group scheme over R, then J is affine and equals to Spec(B), where B is a Hopf algebra ([13]) finite flat over R. We use $c : B \to B \otimes_R B$, $e : B \to R$, and $i : B \to B$ to denote the co-multiplication, the unit, and the co-inverse maps. We shall assume that R is *Nœtherian*, so that every finite flat R-module is locally free ([13]).

doi:10.6342/NTU201701790

2.1 Examples

Some examples of group schemes are given here, notably the constant and the diagonalisable group schemes. They will play a major role in the demonstration of the main theorem.

Definition 2.1. Let Γ be a finite group. Denote $R^{(\Gamma)} := R[e_\gamma]_{\gamma\in\Gamma}$ where e_γ, $\gamma \in \Gamma$, form an orthogonal system of idempotents with $\sum_{\gamma\in\Gamma} e_\gamma = 1$. Endow $\mathrm{Spec}(R^{(\Gamma)})$ the group scheme structure with the co-multiplication map

$$\begin{aligned} c : R^{(\Gamma)} &\longrightarrow R^{(\Gamma)} \otimes R^{(\Gamma)} \\ e_\gamma &\mapsto \sum_{\sigma\tau=\gamma} e_\sigma \otimes e_\tau, \end{aligned}$$

the unit $e(e_\gamma) = \begin{cases} 1 & \gamma = id \\ 0 & \gamma \neq id \end{cases}$, and the co-inverse given by $i(e_\gamma) = e_{\gamma^{-1}}$. We call it the constant group scheme associated to Γ. For simplicity of notation, we also denote it by Γ.

Definition 2.2. Let Γ be a finitely generated abelian group and let $R[\Gamma]$ denote the group ring. Since for every R-algebra S, the natural bijection $\mathrm{Hom}_R(R[\Gamma], S) \cong \mathrm{Hom}(\Gamma, S^\times)$ gives the left-hand side a group structure, the group ring $R[\Gamma]$ (or its spectrum) is a group scheme in a natural way, with $c(\gamma) = \gamma \otimes \gamma$, for al $\gamma \in \Gamma$. We call such group schemes the diagonalisable group schemes.

Example 2.1. We list below examples of group schemes.

(a) μ_n: The diagonalizable group scheme corresponding to $\Gamma = \mathbb{Z}/n\mathbb{Z}$, which is represented by $\mathrm{Spec}(R[\mathbb{Z}/n\mathbb{Z}]) = \mathrm{Spec}(R[X]/(x^n - 1))$.

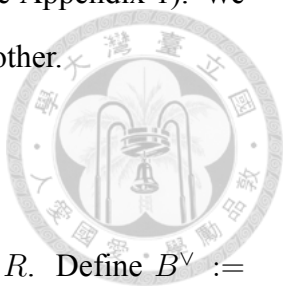
(b) $\mathbb{Z}/n\mathbb{Z}$: The constant group scheme $\mathrm{Spec}(R^{(\mathbb{Z}/n\mathbb{Z})})$.

(c) $\mathrm{G_{a,b}}$: Let $a, b \in R$ be such that $ab = -2$. Define $S = R[X]/(X^2 + aX)$ with $c(X) = X \otimes 1 + 1 \otimes X + bX \otimes X$, $e(X) = 0$ and $i(X) = X$. This defines a group scheme of rank 2 over R.

(d) $\mathrm{G_m}$: This one represents the functor $S \rightsquigarrow S^\times$, with Hopf algebra $R[X, X^{-1}]$, $c(X) = X \otimes X$.

doi:10.6342/NTU201701790

Every free finite group scheme of rank 2 equals to some $G_{a,b}$ (See Appendix 1). We show in Example 2.2 that μ_n and $\mathbb{Z}/n\mathbb{Z}$ are the Cartier duals of each other.



2.2 The Cartier duality and Deligne's theorem

Let $J = \mathrm{Spec}(B)$ be a finite flat commutative group scheme over R. Define $B^\vee := \mathrm{Hom}_R(A, R)$ as the dual module with its module structure defined by

$$(\lambda f)(a) = \lambda \cdot f(a) = f(\lambda a)$$

for $\lambda \in R$, $a \in A$.

Since B is a Hopf algebra, we have the R-algebra homomorphisms:

(the multiplication)	$m : B \otimes B \to B,$	$a \otimes b \mapsto ab,$
(the co-multiplication)	$c : B \to B \otimes B,$	$a \mapsto c(a),$
(the structure map)	$1 : R \to B,$	$\lambda \mapsto \lambda \cdot 1$
(the unity)	$e : B \to R,$	$a \mapsto e(a),$
(the co-inverse)	$i : B \to B,$	$a \mapsto i(a).$

By dualising the above, we have the following homomorphisms:

$$\begin{aligned} m^\vee &: B^\vee \to B^\vee \otimes B^\vee \\ c^\vee &: B^\vee \otimes B^\vee \to B^\vee \\ 1^\vee &: B^\vee \to R \\ e^\vee &: R \to B^\vee \\ i^\vee &: B^\vee \to B^\vee \end{aligned}$$

Note that $e^\vee$ is just the structure map of $B^\vee$ as R-module. If J is commutative, or equivalently, $c^\vee(f \otimes g) = c^\vee(g \otimes f)$, then $B^\vee$ is a commutative R-algebra with the multiplication given by $c^\vee$. In this case, $B^\vee$ is actually a Hopf algebra with $m^\vee$, $1^\vee$ and $i^\vee$ as the co-multiplication, the unity and the co-inverse. We call $J^\vee := \mathrm{Spec}(B^\vee)$ the *Cartier dual* of J. Since B is locally free of finite rank, $(B^\vee)^\vee = B$, hence $(J^\vee)^\vee = J$.

doi:10.6342/NTU201701790

Lemma 2.1. Let $J_{/R}$ be a finite flat group scheme. The Cartier dual $J^\vee$ represents the functor

$$\begin{aligned} S \rightsquigarrow \mathrm{Hom}_{Sgp}(J_{/S}, \mathrm{G_m}) &= \{a \in (B \otimes_R S)^\times \mid c(a) = a \otimes a, e(a) = 1\} \\ &= \{a \in (B \otimes_R S)^\times \mid c(a) = a \otimes a\}, \end{aligned}$$

where $\mathrm{Hom}_{Sgp}(-,-)$ denotes the morphisms in the category of S-group schemes.

Proof. By taking the base change to S, we may assume that $S = R$. The duality $B = (B^\vee)^\vee$ identifies an $a \in B$ with a $\varphi_a \in \mathrm{Hom}_R(B^\vee, R)$ such that $\varphi_a(f) = f(a)$, for all $f \in B^\vee$. That φ_a respects the ring multiplications is equivalent to $f \otimes g(c(a)) = f(a) \cdot g(a) = f \otimes g(a \otimes a)$, for all $f, g \in B^\vee$. The condition, via the duality, becomes $c(a) = a \otimes a$. We check that $\varphi_a(1_{B^\vee}) = 1_{B^\vee}$, if and only if $e(a) = 1$. Thus, $G^\vee(R) = \{a \in B \mid c(a) = a \otimes a, e(a) = 1\}$. Moreover, if $a * b$ is the product of a, b in $J^\vee(R)$, then

$$f(a * b) = a \otimes b(m^\vee(f) = \varphi_{ab}(f) = f(a \cdot b), \quad \text{for all} \quad f \in B^\vee,$$

which shows $a * b = a \cdot b$. Hence $J^\vee(R)$ is a subgroup of $B^\times$. Conversely, if $a \in B^\times$, $c(a) = a \otimes a$, then

$$f(a) = f \otimes e(c(a)) = f \otimes e(a \otimes a) = f(a) \cdot e(a)$$

holds for all $f \in B^\vee$, and hence $e(a) = 1$. Finally, an R-algebra homomorphism $\xi : R[T, \frac{1}{T}] \to B$ is determined by $a := \xi(T) \in B^\times$, and ξ is a homorphism of Hopf algebras, if and only if $c(a) = a \otimes a$ and $e(a) = 1$. □

Example 2.2. We show $\mu_n^\vee = \mathbb{Z}/n\mathbb{Z}$ by computing $\mu_n^\vee(S)$ for R-algebras S. Again, we may assume that $S = R$. Set $B = R[X]/(X^n - 1)$. An element $a \in B$ can be expressed as $a = \sum_{i=0}^{n-1} a_i X^i$. Then the condition $c(a) = a \otimes a$ says that

$$\sum_{i=0}^{n-1} a_i X^i \otimes \sum_{i=0}^{n-1} a_i X^i = \sum_{i=0}^{n-1} a_i (X \otimes X)^i.$$

doi:10.6342/NTU201701790

By comparing coefficients, we see that $a_i a_j = 0$ for $i \neq j$, and $a_i^2 = a_i$. Further, the condition $e(a) = 1$ means $\sum a_i = 1$. Therefore, $\mu^\vee(R)$ consists of those a with $a_0, a_1, ..., a_{n-1}$ forming an orthogonal system of idempotents in R. Note that in this case, for $b = \sum_{i=0}^{n-1} a_{n-i} X^i$, we have $ab = 1$ and hence $a \in B^\times$.

Write $\mathbb{Z}/n\mathbb{Z} = \{[i] \mid i = 0, ..., n-1\}$ as usual. Then each $a \in \mu_n^\vee(R)$ gives an R-algebra homomorphism $\psi_a : R^{(\mathbb{Z}/n\mathbb{Z})} \to R$, $e_{[i]} \mapsto a_i$. This gives a group homomorphism $\mu_n^\vee(R) \to \mathbb{Z}/n\mathbb{Z}(R)$, which is an isomorphism.

Deligne's Theorem

We end this section by showing a theorem of Deligne that is important in the theory of commutative finite flat group schemes. Let S be a finite flat R-algebra, B an R-algebra. Since $B \otimes_R S$ is locally free over B, for $s \in B \otimes_R S$, the determinant of the endomorphism $B \otimes_R S \to B \otimes_R S$, $x \mapsto sx$ is defined. Let $N : B \otimes_R S \to B$ denote this determinant map. If S is of rank n over R , then

$$N(a) = a^n, \quad \text{for } a \in B. \tag{1}$$

Lemma 2.2. If $\psi : B \to C$ is an R-algebra homomorphism, then the following diagram commutes:

$$\begin{array}{ccc} B \otimes_R S & \xrightarrow{\psi \otimes id_S} & C \otimes_R S \\ {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle N} \\ B & \xrightarrow[\psi]{} & C \end{array}$$

Proof. We may assume that S is free over R with a basis $\{e_i\}$. For $\alpha \in B \otimes S$, write $\alpha(1 \otimes e_i) = \sum \mu_{ij}(1 \otimes e_j)$ for $\mu_{ij} \in B$. This implies $N(\alpha) = \det(\mu_{ij})$ and $\psi(\alpha)(1 \otimes e_i) = \psi(\mu_{ij})(1 \otimes e_j)$. Therefore, $N(\psi(\alpha)) = \det(\psi(\mu_{ij})) = \psi(N(\alpha))$. □

Let $J = \mathrm{Spec}(B)$ be a finite flat commutative group scheme over R. Lemma 2.1 says $J(S)$ can be viewed as a subgroup of $(B^\vee \otimes S)^\times$.

doi:10.6342/NTU201701790

Lemma 2.3. There is a determinant map $J(S) \xrightarrow{N} J(R)$ that fits into the commutative diagram:

$$\begin{array}{ccc} J(S) & \hookrightarrow & B^\vee \otimes S \\ {\scriptstyle N}\downarrow & & \downarrow{\scriptstyle N} \\ J(R) & \hookrightarrow & (B^\vee)^\times \end{array}$$

Proof. We complete the proof by showing that the right vertical arrow maps $J(S)$ to $J(R)$. To clarify the notation, write $\tilde{C} := B^\vee$, let $\tilde{c}$ denote the co-multiplication, and denote $\tilde{C}_S = \tilde{C} \otimes_R S$. Since $\tilde{C}_S \otimes_S \tilde{C}_S = (\tilde{C} \otimes_R \tilde{C}) \otimes_R S$, there is the determinant map $\tilde{C}_S \otimes_S \tilde{C}_S \xrightarrow{N_2} \tilde{C} \otimes_R \tilde{C}$. We see directly that if $f \in \tilde{C}_S$, then $N_2(f \otimes 1) = N(f) \otimes 1$. By Lemma 2.2 (taking $\psi = \tilde{c}$), we obtain $\tilde{c}(N(f)) = N_2(\tilde{c}(f))$. If $f \in J(S)$ so that $\tilde{c}(f) = f \otimes f$, then

$$\tilde{c}(N(f)) = N_2(f \otimes f) = N_2(f \otimes 1)N_2(1 \otimes f) = N(f) \otimes 1 \cdot 1 \otimes N(f) = N(f) \otimes N(f),$$

which means $N(f) \in J(R)$. □

By (1), if S is of rank n and $u \in J(R)$, then

$$N(u) = u^n. \tag{2}$$

For a commutative group scheme J, let $[n]$ denote the homomorphism sending each $P \in J(S)$ to P^n.

Theorem 2.1 (Deligne's theorem). *Let J be a finite flat commutative group scheme over R of rank n. Then the map $[n]$ annihilates J.*

Proof. It suffices to show that $[n]$ annihilates $J(R)$. Write $J = \mathrm{Spec}(B)$ and denote $\tilde{C} := B^\vee$. Let $u \in J(R) \subset \tilde{C}^\times$. We shall show $u^n = 1$.

Define $\tau : B \to B$ as $\tau = (id_B \otimes u) \circ c$, which is an R-algebra automorphism of B resulting in the translation by u on J. Then extend τ linearly to $\tilde{C} \otimes_R B$ by $\tau(f \otimes a) =$

doi:10.6342/NTU201701790

$f \otimes \tau(a)$. Take $S = B$ and consider the determinant map $\tilde{C} \otimes_R S \xrightarrow{N} \tilde{C}$. Since τ is an automorphism of the $\tilde{C}$-algebra, we have

$$N(a) = N(\tau(a)), \quad \text{for all } \ a \in \tilde{C} \otimes_R S. \tag{3}$$

The identity map $id_B : B \to S$ extends uniquely to a homomorphism of (right) S-algebra $B \otimes_R S \to S$, and hence can be viewed as an element, also denoted as id_B, of $J(S) \subset \tilde{C} \otimes_R S$. We claim that

$$\tau(id_B) = u \cdot id_B.$$

Then by (3), we have $N(id_B) = N(u \cdot id_B)$. Also, (2) says $N(u) = u^n$. Therefore,

$$N(id_B) = N(u \cdot id_B) = N(u)N(id_B) = u^n N(id_A).$$

Hence $u^n = 1$ as desired.

Since the claim can be proved locally, we may assume that S is free over R. Let $e_1, ..., e_n$ be a basis of S and let $e_1^\vee, ..., e^\vee \in \tilde{C}$ denote the dual basis. Identify $\tilde{C} \otimes_R S$ with $\mathrm{Hom}_R(B, S)$. Then we see that $id_B = \sum_{i=1}^n e_i^\vee \otimes e_i$, and hence $\tau(id_B) = \sum_{i=1}^n e_i^\vee \otimes \tau(e_i)$, which means $\tau(id_B)$ sends every $b \in B$ to $\tau(b)$. But $u \cdot id_B$ sends b to $u \otimes id_B(c(b))$ which is also $\tau(b)$. □

2.3 Étale group schemes

We take the definiton of étale morphism from [6]. For a scheme X, let $\mathcal{O}_X$ denote the structure sheaf; for $x \in X$, let $\mathcal{O}_{X,x}$ denote the local ring at x, $\mathfrak{m}_x \subset \mathcal{O}_{X,x}$ the maximal ideal and $k(x) := \mathcal{O}_{X,x}/\mathfrak{m}_x\mathcal{O}_{X,x}$ the residue field.

Definition 2.3.

1. A morphism of scheme $f : Y \to X$ locally of finite type is called unramified at $y \in Y$, if $\mathcal{O}_{Y,y}/\mathfrak{m}_x\mathcal{O}_{Y,y}$ is a finite separable field extension of $k(x)$, where $x = f(y)$.

2. The morphism f is said to be unramified if it is unramified at every $y \in Y$.

doi:10.6342/NTU201701790

3. A morphism of schemes is étale if it is flat and unramified (hence locally of finite type also).

4. A group scheme J over R is étale if the structure morphism $J \to \mathrm{Spec}(R)$ is étale.

Note that the morphism f is unramified at y if and only if the induced $f_x : Y \times_X \mathrm{Spec}(k(x)) \to \mathrm{Spec}(k(x))$ is unramified at $\bar{y} := y \times_X \mathrm{Spec}(k(x))$. Thus, f is unramfied (at every point) on the fibre at x if and only if f_x is unramified.

Let $\mathcal{O}$ be a Dedekind domain with field of fraction E and let B be a finite flat $\mathcal{O}$-algebra. Then $B \otimes_{\mathcal{O}} E$ is a direct product of Artinian local algebras K_i over E and each K_i corresponds to a point y_i in the generic fibre of $f : \mathrm{Spec}(B) \to \mathrm{Spec}(\mathcal{O})$ so that f is unramified at y_i if and only if K_i is a finite separable field extension of E. Thus, the morphism f is unramified on the generic fibre if and only if

$$B \otimes_{\mathcal{O}} E = K_1 \times \cdots \times K_m. \tag{4}$$

with each K_i a finite separable field extension of E. Similarly, for $\mathfrak{m} \subset \mathcal{O}$ a maximal ideal with residue field $k(\mathfrak{m}) = \mathcal{O}/\mathfrak{m}$, the morphism f is unramified at the special fibre at $\mathfrak{m}$ if and only if

$$B \otimes_{\mathcal{O}} k(\mathfrak{m}) = k_1 \times \cdots \times k_l, \tag{5}$$

with each $k_i/k(\mathfrak{m})$ a finite separable field extension.

Proposition 2.1. Let E be a number field with the ring of integers $\mathcal{O}_E$, and let $J = \mathrm{Spec}(B)$ be an $\mathcal{O}_E$-scheme whch is a finite étale scheme over a Zariski open set $U \subset \mathrm{Spec}(\mathcal{O}_E)$. Let $F = E(J(\bar{E}))$. Then F/E is unramified at every $\mathfrak{m}$ in U.

Proof. Since the assertion of the proposition is local, it is sufficient to prove the corresponding statement in which E is the local completion of the given number field. Then the maximal ideal $\mathfrak{m} \subset \mathcal{O}_E$ is generated by a prime element π.

Since B is flat over $\mathcal{O}_E$, the identity (4) gives rise to $B \hookrightarrow K_1 \times \cdots \times K_m$. Let B_i denote the image of B in i-th factor K_i. It follows that K_i is the fraction field of B_i and $B_i \subseteq \mathcal{O}_{K_i} \subseteq K_i$ as B is finite over $\mathcal{O}_E$.

doi:10.6342/NTU201701790

Now (5) says $B/\mathfrak{m}B$ is a product of fields. The surjection $B/\mathfrak{m} \twoheadrightarrow B_i/\mathfrak{m}B_i$ implies $\mathfrak{m}B_i$ is a maximal ideal of B_i and B_i is unramified over $\mathcal{O}_E$. It remains to show that $B_i = \mathcal{O}_{K_i}$.

Let $S = \{0\} \cup S'$ be a set of representatives of B_i modulo $\mathfrak{m}B_i$. Since B_i is a compact $\mathcal{O}_E$-module, it is a closed subring of K_i in the $\mathfrak{m}$-adic topology. The standard argument implies every element ξ in B_i can be written as a power series $\sum_{n=0}^{\infty} a_n \pi^n$ with $a_0, ..., a_n, ... \in S$ and vice versa. Also, $\xi \in B_i^{\times}$ if and only if $a_0 \neq 0$. As K_i is the fraction field of B_i, every $\eta \in K_i$ can be written as $\eta = u \times \pi^{\mu}$. From this, we deduce that $\eta \in \mathcal{O}_{K_i}$ if and only if $\mu \geq 0$, which means $\eta \in B_i$.

□

Proposition 2.2. Every finite flat group scheme over a field annihilated by an integer prime to the characteristic of the field is étale.

Proof. See [13, corollary in 11.4]. □

Proposition 2.3. Let p be a prime number. Every finite flat group scheme J of rank p^n over the ring of integers $\mathcal{O}$ of a number field is étale over $\mathcal{O}[\frac{1}{p}]$.

Proof. Let $f : J \to \mathrm{Spec}(\mathcal{O})$ be the structure morphism of J. Let $x = \mathfrak{m} \subset \mathcal{O}$ be a prime ideal of residual characteristic $\neq p$. Then Proposition 2.2 says f_x is unramified. □

Theorem 2.2. *The category of finite étale group schemes over a field is equivalent to the category of finite abelian group on which the absolute Galois group of the field acts continuously.*

Proof. See [13, Theorem 6.4]. □

2.4 Local group schemes

Let R be a local ring. By *a local group scheme over* R, we mean a group scheme $\mathrm{Spec}(B)$ such that B is *a local algebra* over R.

doi:10.6342/NTU201701790

Local group schemes over a perfect field

By Proposition 2.2, a non-trivial local finite flat group scheme over a field k exists only if char $k > 0$.

Theorem 2.3. *Let k be a perfect filed of characteristic $p > 0$. Then every finite flat group scheme J over k can be expressed as $J = J^0 \rtimes J_{\acute{e}t}$*

Proof. See [13, Theorem 6.8]. □

Theorem 2.4. *Let $J = \mathrm{Spec}(B)$ be a local finite flat group scheme over a perfect field k of characteristic $p > 0$. There exist positive integers $p_1, ..., p_h$ such that*

$$B = k[x_1, ..., x_h]/(x_1^{p^{e_1}}, ..., x_h^{p^{e_h}}).$$

Proof. See [13, Theorem 14.4]. □

Local group schemes over the ring of integers of a local field

Let K be a finite extension of $\mathbb{Q}_p$ and let $\mathcal{O}_K$ denote the ring of integers of K. Let $\mathfrak{m}_K$ be the maximal ideal of $\mathcal{O}_K$ and k be the residue field. Let $J = \mathrm{Spec}(B)$ be a local finite flat group scheme over $\mathcal{O}_K$. Since $\mathcal{O}_K$ is Henselian, we can write (see [6, §I, Theorem 4.2(b)])

$$B = B_1 \times \cdots \times B_m, \tag{6}$$

where each B_i is a finite flat local algebra over $\mathcal{O}_K$.

Definition 2.4. We say that an $\mathcal{O}_K$ local algebra B is a *complete intersection over $\mathcal{O}_K$*, if there are $P_1, ..., P_{h_i} \in \mathcal{O}_K[[X_1, ..., X_{h_i}]]$ with

$$P_j \equiv X^{g_j} \pmod{\mathfrak{m}_K[[X_1, ..., X_h]]},\ g_j > 1, \tag{7}$$

such that

$$B = \mathcal{O}_K[[X_1, ..., X_{h_i}]]/(P_1, ..., P_{h_i})$$

and $\mathfrak{m}_B = \mathfrak{m}_K C + (X_1, ..., X_h)/(P_1, ..., P_{h_i})$.

doi:10.6342/NTU201701790

If B is a finite flat $\mathcal{O}_K$-algebra with the decomposition (6) and each B_i is a complete intersection, then we say that B is *locally a complete intersection over* $\mathcal{O}_K$.[2]

Theorem 2.5. *Let $J = \mathrm{Spec}(B)$ be a local finite flat group scheme over $\mathcal{O}_K$. There exists a finite unramified extension L/K such that $B \otimes_{\mathcal{O}_K} \mathcal{O}_L$ is locally of complete intersection over $\mathcal{O}_L$.*

Proof. Write $\bar{J} := \mathrm{Spec}(\bar{B})$, where $\bar{B} := B \otimes_{\mathcal{O}_K} k$. By replacing K by certain L, we may assume that $\bar{J}(\bar{k}) = \bar{J}(k)$. Here $\bar{k}$ denotes the algebraic closure of k. Then we prove the theorem for $K = L$. By Theorem 2.3, we can write

$$\bar{J} = \bar{J}^0 \rtimes \bar{J}_{\acute{e}t}.$$

Since $\bar{J}_{\acute{e}t}(\bar{k}) = \bar{J}(\bar{k}) = \bar{J}(k) = \bar{J}_{\acute{e}t}(k)$, Theorem 2.2 says $\bar{J}_{\acute{e}t}$ is actually a constant group scheme $\mathrm{Spec}(k^{(\Gamma)})$ for some Γ (see Definition 2.1). Put $\bar{J}^0 = \mathrm{Spec}(C_0)$. Then

$$\bar{B} = C_0 \otimes_k k^{(\Gamma)} = C_0 \times \cdots \times C_l,$$

where each C_i is an artinian local k-algebra isomorphic to C_0. From (6), we also have

$$\bar{B} = \bar{B}_1 \times \cdots \times \bar{B}_m,$$

where each B_i is also an artinian local k-algebra. Now the uniqueness of the decomposition of $\bar{B}$ into a product of artinian local algebras implies that $\bar{B}_i$ must equals C_j for some j, and hence isomorphic to C_0. Thus, by Theorem 2.4, we have the commutative diagram

$$\begin{array}{ccccc} T & \hookrightarrow & \mathcal{O}_K[[X_1, \cdots, X_h]] & \xrightarrow{\alpha} & B_i \\ \downarrow & & \downarrow \pi & & \downarrow \bar{\pi} \\ (x_1^{p^{e_1}}, \cdots, x_h^{p^{e_h}}) & \hookrightarrow & k[[x_1, \cdots, x_h]] & \xrightarrow{\beta} & C_j \end{array},$$

where T and $(x_1^{p^{e_1}}, ..., x_h^{p^{e_h}})$ are respectively, the kernels of α and β, π sends X_j to x_j and $\bar{\pi}$ is the reduction modulo $\mathfrak{m}_K$. Since β is surjective, Nakayama's lemma says α

[2] Our definition is not standard, but it fits in well with our situation.

doi:10.6342/NTU201701790

is also surjective. Because $\beta(\pi(X_j^{p^{e_j}})) = 0$, the element $\alpha(\pi(X_j^{p^{e_j}}))$ is contained in $\mathfrak{m}_K B_i = \ker(\bar{\pi})$. Write $\alpha(\pi(X_j^{p^{e_j}})) = a_j \cdot y_j$, with $a_j \in \mathfrak{m}_K$ and $y_j \in B_i$. Since α is surjective, we can lift y_j to $Y_j \in \mathcal{O}_K[[X_1, ..., X_h]]$. Then set $P_j = X^{p^{e_j}} - a_j Y_j$. We have

$$P_j \equiv X^{p^{e_j}} \pmod{\mathfrak{m}_K[[X_1, ..., X_h]]}$$

and $P_j \in T$. Since $R[[X_1, ..., X_h]]$ is a Nœtherian local ring, Nakayama's lemma says $T = (P_1, ..., P_h)$.

□

3 Fontaine's bound and its consequences

In this section, we review one of the main results in [3], namely the following theorem of Fontaine. Let K denote a finite extension of $\mathbb{Q}_p$ with ring of integers denoted by $\mathcal{O}_K$ and the ramification index of $K/\mathbb{Q}_p$ (the absolute ramification index) denoted by e_K. Let $\mathfrak{m}_K$ and $k := \mathcal{O}_K/\mathfrak{m}_K$ denote the maximal ideal of $\mathcal{O}_K$ and the residue field.

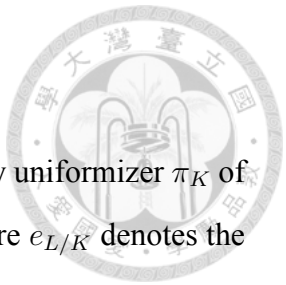
Let L/K be a Galois extension and denote $G := \mathrm{Gal}(L/K)$. By [11, §III.6, Proposition 12], we can write $\mathcal{O}_L = \mathcal{O}_K[\alpha]$ for some α with minimal polynomial $f(X) \in \mathcal{O}_K[X]$. As usual, for i running through $[-1, \infty)$, let G^i denote the ramification subgroups of G *in upper numbering* [11, §IV.3]. By a *p-group scheme over $\mathcal{O}_K$* we mean a finite flat group scheme over $\mathcal{O}_K$ annihilated by some power of p

Theorem 3.1. *Suppose J is a p-group scheme over $\mathcal{O}_K$ annihilated by p^n. Let $L = K(J(\bar{K}))$ be the field obtained by adjoining the geometric points of J, with $G := \mathrm{Gal}(L/K)$. Then $G^u = \{1\}$, for all $u > e_K(n + 1/(p-1))$.*

We will only prove the theorem in §3.4 for the special case where $K = \mathbb{Q}_p$ and $n = 1$. That will be sufficient for the later application.

doi:10.6342/NTU201701790

3.1 The ramification theory



Define $v = v_K$ to be the valuation on $\bar{K}$ such that $v(\pi_K) = 1$ for every uniformizer π_K of K, and similarly define the valuation v_L so that $v_L = e_{L/K} \cdot v_K$, where $e_{L/K}$ denotes the ramification index. Recall the ramification groups in lower numbering [11, §IV.1]

$$G_i = \{\sigma \in G \mid v_L({}^{\sigma}\alpha - \alpha) \geq i + 1\}, \quad i \geq -1.$$

In particular, G_0 is the inertia subgroup of G. For $s \in [-1, \infty)$, put

$$\phi(s) := \int_0^s \frac{dt}{|G_0 : G_t|}.$$

This defines the *Herbrand function* $\phi : [-1, \infty) \to [-1, \infty)$, which is a bijiection [11, §IV.3] such that

$$G^{\phi(s)} = G_s, \text{ for all } s \in [-1, \infty). \tag{8}$$

For each $\sigma \in G$, define

$$i_G(\sigma) = v_L({}^{\sigma}\alpha - \alpha),$$

which is independent of the choice of α. By [11, §IV.3, Lemma 3],

$$\phi(s) + 1 = \frac{1}{e_{L/K}} \sum_{\sigma \in G} \min(i_G(\sigma), s + 1). \tag{9}$$

Lemma 3.1. If $\beta \in \bar{K}$ and $i := \max\{v_L({}^{\sigma}\alpha - \beta) \mid \sigma \in G\}$, then

$$\phi(i - 1) + 1 = v_K(f(\beta)).$$

Proof. Suppose $i = v_L({}^{\tau}\alpha - \beta)$ for some $\tau \in G$. For each $\sigma \in G$,

$$v_L(\beta - {}^{\tau\sigma}\alpha) \geq \min(v_L(\beta - {}^{\tau}\alpha), v_L({}^{\tau}\alpha - {}^{\tau\sigma}\alpha)),$$

doi:10.6342/NTU201701790

in which the equality should actually hold, for otherwise

$$v_L(\beta - {}^{\tau}\alpha) = v_L({}^{\tau}\alpha - {}^{\tau\sigma}\alpha) < v_L(\beta - {}^{\tau\sigma}\alpha),$$

a contradiction to the choice of τ. Therefore, by (9),

$$\begin{aligned}
\phi(i-1)+1 &= e_{L/K}^{-1} \cdot \textstyle\sum_{\sigma\in G} \min(i_G(\sigma), i) \\
&= e_{L/K}^{-1} \cdot \textstyle\sum_{\sigma\in G} \min(v_L({}^{\sigma}\alpha - \alpha), v_L(\beta - {}^{\tau}\alpha)) \\
&= e_{L/K}^{-1} \cdot \textstyle\sum_{\sigma\in G} \min(v_L({}^{\tau\sigma}\alpha - {}^{\tau}\alpha), v_L(\beta - {}^{\tau}\alpha)) \\
&= e_{L/K}^{-1} \cdot \textstyle\sum_{\sigma\in G} v_L(\beta - {}^{\tau\sigma}\alpha) \\
&= v_K(f(\beta)).
\end{aligned}$$

□

Lemma 3.2. (Krasner's lemma) If $\beta \in \bar{K}$ satisfies

$$v_L(\beta - \alpha) > v_L({}^{\sigma}\alpha - \alpha),$$

for all $\sigma \in \mathrm{Aut}(\bar{K})$, ${}^{\sigma}\alpha \neq \alpha$, then $L \subseteq K(\beta)$.

Proof. If τ is an element in $\mathrm{Aut}(\bar{K})$ fixing β, then for all $\sigma \in \mathrm{Aut}(\bar{K})$, ${}^{\sigma}\alpha \neq \alpha$,

$$v_L({}^{\tau}\beta - {}^{\tau}\alpha) = v_L(\beta - \alpha) > v_L({}^{\sigma}\alpha - \alpha),$$

Hence

$$v_L({}^{\tau}\alpha - \alpha) \geq \min(v_L({}^{\tau}\alpha - \beta), v(\beta - \alpha)) > v_L({}^{\sigma}\alpha - \alpha).$$

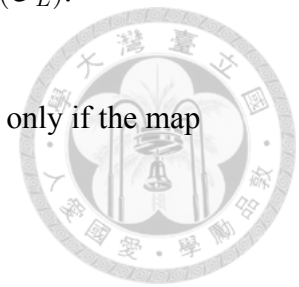
This shows that ${}^{\tau}\alpha = \alpha$. Therefore the field extension $L(\beta)/K(\beta)$ is trivial, and $L \subseteq K(\beta)$. □

For each finite extension E/K and each real number t, set

$$M_E^t = \{x \in \mathcal{O}_E \mid v_K(x) \geq t\}$$

doi:10.6342/NTU201701790

so that the maximal ideal $\mathfrak{m}_K \subset \mathcal{O}_K$ equals M_K^1. Denote $X := \text{Spec}(\mathcal{O}_L)$.



Lemma 3.3. Let $t \in (0,1)$. The extension L/K is unramified if and only if the map

$$X(\mathcal{O}_E) \to X(\mathcal{O}_E/M_E^t)$$

is surjective for every E.

Proof. A point on $X(\mathcal{O}_E/M_E^t)$ is given by an algebra homomorphism

$$\psi_E : \mathcal{O}_L \to \mathcal{O}_E/M_E^t.$$

Suppose L/K is unramified. Then we can find α such that f has monic irreducible image $\bar{f}(X) \in \mathcal{O}_K[X]$. Note that our condition implies if $\bar{f}(\bar{\beta}) = 0$, for some $\bar{\beta} \in \bar{\mathbb{F}}_K$, then $\bar{f}'(\bar{\beta}) \neq 0$.

Choose $\beta \in \mathcal{O}_E$ such that $\beta \equiv \psi_E(\alpha) \pmod{M_E^t}$. Then $f(\beta) \equiv 0 \pmod{M_E^t}$ and $v_K(f'(\beta)) = 0$. Hence, by Hensel's lemma there exist $\tilde{\beta} \in \mathcal{O}_E$ such that $f(\tilde{\beta}) = 0$ and $\tilde{\beta} \equiv \beta \pmod{M_E^t}$. This shows the map in question is surjective.

Let E be the unique unramified sub-extension of L/K with residue field $\mathbb{F}_L$. Consider the surjection

$$\mathcal{O}_L \to \mathbb{F}_L = \mathbb{F}_E = \mathcal{O}_E/M_E^t = \mathcal{O}_E/\pi_K\mathcal{O}_E.$$

This lifts to a K-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E$, if ψ_E is surjective. Under this condition, L/K is a sub-extension of E/K, and hence unramified. □

Define

$$u_{L/K} := \phi(\max\{i_G(\sigma) \mid \sigma \neq id_G\} - 1) + 1,$$

so that by (8),

$$G^\mu = \{id_G\} \iff \mu > u_{L/K} - 1. \tag{10}$$

doi:10.6342/NTU201701790

Lemma 3.4. Let L/K be a finite extension. Then

$$L/K \text{ is } \begin{cases} \text{unramified} & \iff u_{L/K} = 0 \\ \text{tamely ramified} & \iff u_{L/K} = 1 \\ \text{wildly ramified} & \iff u_{L/K} > 1 \end{cases}$$

Proof. For a non-negative integer n, we have $G_x = G_n$, for $x \in (n-1, n]$. Now G_0 is the inertia subgroup, while by [11, Chapter IV. §2. Proposition 6.], $|G_0|/|G_1|$ is of order prime to p and $|G_n|/|G_{n+1}|$ is a power of p for $n \geq 1$. Then we check that $\phi(-1) = -1$ and $\phi(0) = 0$.

□

Proposition 3.1. Let t be a positive number.

(a) If $t > u_{L/K}$, then the implication

$$X(\mathcal{O}_E/M_E^t) \neq \emptyset \implies X(\mathcal{O}_E) \neq \emptyset \tag{11}$$

holds for all finite extension E/K.

(b) Conversely, if the implication (11) holds for all finite extension E/K, then $t > u_{L/K} - 1/e_{L/K}$.

Proof. Suppose $t > u_{L/K}$ and $X(\mathcal{O}_E/M_E^t) \neq \emptyset$ so that there exists $\beta \in \mathcal{O}_E$ with $v_K(f(\beta)) \geq t > u_{L/K}$. By Lemma 3.1 and (10),

$$\phi(\max\{v_L({}^\sigma\alpha - \beta) \mid \sigma \in G\} - 1) > \phi(\max\{v_L(i_G(\sigma) \mid \sigma \in G,\ \sigma \neq id_G\} - 1).$$

Because ϕ is an increasing function, there exists $\tau \in G$ such that

$$v_L(\beta - {}^\tau\alpha) > \max\{v_L({}^\sigma\alpha - \alpha) \mid \sigma \in G,\ \sigma \neq id_G\}.$$

Hence by Krasner's lemma, $L = K({}^\tau\alpha) \subseteq K(\beta) \subseteq E$. Thus $X(\mathcal{O}_E) \neq \emptyset$.

doi:10.6342/NTU201701790

If L/K is unramified, then (b) holds trivially, because in this case $u_{L/K} = 0$, and hence $t > u_{L/K} - 1/e_{L/K}$, while Lemma 3.3 says (11) always holds.

If L/K is ramified, we shall prove (b) by showing that for $t = u_{L/K} - 1/e_{L/K}$, there exists a finite extension E such that $X(\mathcal{O}_E/M_E^t) \neq \emptyset$ but $X(\mathcal{O}_E) = \emptyset$. To do so, we may replace K by the maximal unramified sub-extension of L/K and assume that L/K is totally ramified with α a uniformizer of $\mathcal{O}_L$ and $f(X)$ an Eisenstein polynomial.

Suppose L/K is tamely ramified. Then $u_{L/K} = 1$ and hence $t = 1 - 1/e_{L/K}$. Take E to be a totally ramified extension of K of degree $d < e_{L/K} = [L : K]$, by adjoining a root of some Eisenstein polynomial. Since L can not be embedded into E, we have $X(\mathcal{O}_E) = \emptyset$. In this case,

$$\begin{aligned} M_E^t &= \{x \in \mathcal{O}_E \mid v_K(x) \geq 1 - 1/e_{L/K} > 1 - 1/d\} \\ &= \{x \in \mathcal{O}_E \mid v_K(x) \geq 1\} \\ &= \mathfrak{m}_E. \end{aligned}$$

If β is uniformizer of $\mathcal{O}_E$, then $v_K(\beta) = 1/d$, and hence

$$v_K(f(\beta)) = v_K(\prod_\sigma \beta - {}^\sigma\alpha) = e_{L/K} \cdot 1/e_{L/K} = 1.$$

This shows $X(\mathcal{O}_E/M_E^t) \neq \emptyset$.

Finally consider the case where L/K is wildly ramified, namely, $p \mid e_{L/K}$. Since $G = G_0$ and G_1 is a nontrivial p-group, by (10), we have

$$u_{L/K} \geq \phi(1) + 1 \geq p/e_{L/K} + 1.$$

Hence

$$t = u_{L/K} - 1/e_{L/K} > 1.$$

Now that $t \cdot e_{L/K} \in \mathbb{Z}$, we can write $t \cdot e_{L/K} = r \cdot e_{L/K} + s$ with $r, s \in \mathbb{Z}$ and $0 \leq s < e_{L/K}$. Let $E = K(\beta)$, where β is a root of the polynomial $g(X) = f(X) - \pi_K^r X^s$.

We check that g is an Eisenstein polynomial as follow: First, g is monic, because

doi:10.6342/NTU201701790

$e_{L/K} > s$. Also, $r \geq 1$, because $t > 1$, hence π_K divides all non-leading coefficients of g. If $s = 0$, then $t > 1$ implies $r \geq 2$. Thus the constant term of g is not divisible by π_K^2.

We then deduce that $v_K(\beta) = 1/e_{L/K}$. Since $v_K(f(\beta)) = v_K(\pi_K^r \beta^s) = t$, we see $X(\mathcal{O}_E/M_E^t) \neq \emptyset$. It remains to show $X(\mathcal{O}_E) = \emptyset$.

Suppose $X(\mathcal{O}_E) \neq \emptyset$. Then an K-algebra homomorphism $\mathcal{O}_L \to \mathcal{O}_E$ induces an embedding of L into E. But we actually have $L = E$, because both sides are of the same degree over K. Then α and β both lie in E and by Lemma 3.1,

$$\phi(\max\{v_L({}^\sigma\alpha - \beta) \mid \sigma \in G\} - 1) + 1 = v_K(f(\beta)) = t.$$

Define $\delta = \max\{i_G(\sigma) \mid \sigma \neq id_G\}$ and put

$$d := |G_{\delta-1}| = |\{\sigma \in G \mid i_G(\sigma) \geq \delta\}|.$$

Then by (9) and by the definition of $u_{L/K}$,

$$\phi(\delta - 1/d - 1) + 1 = \phi(\delta - 1) + 1 - 1/e_{L/K} = u_{L/K} - 1/e_{L/K} = t.$$

Thus, there is some $\tau \in G$ such that

$$v_L({}^\tau\alpha - \beta) = \delta - 1/d.$$

This implies $1/d \in \mathbb{Z}$, and hence $d = 1$. But this absurd, since $G_{\delta-1}$ is non-trivial. The proposition is proved.

□

3.2 Divided power sturctures

In this subsection, we review some basic facts about divided power structures.

Definition 3.1. Let R be a commutative ring. A divided power structure on an ideal $I \subset R$ is a collection of maps $\gamma_n : I \to I$, $n = 1, ...$, such that

doi:10.6342/NTU201701790

(a) $\gamma_1(x) = x$, for $x \in I$.

(b) $\gamma_n(x+y) = \sum_{i=0}^{n} \gamma_i(x)\gamma_{n-i}(y)$, for $x, y \in I$.

(c) $\gamma_n(ax) = a^n\gamma_n(x)$, for $a \in R$, $x \in I$.

(d) $\gamma_m(x)\gamma_n(x) = \frac{(m+n)!}{m!n!}\gamma_{m+n}(x)$. for $x \in I$.

(e) $\gamma_n(\gamma_m(x)) = \frac{(mn)!}{(m!)^n n!}\gamma_{mn}(x)$, for $x \in I$.

We say that I is a divided power ideal (with the given divided power structure).

Note that the numbers $\frac{(m+n)!}{m!n!}$ and $\frac{(mn)!}{(m!)^n n!}$ are integers and by [(d)]

$$n!\gamma_n(x) = x^n.$$

For simplicity, we often use the abbreviation $x^{[n]} := \gamma_n(x)$. Put

$$I^{[n]} := (x^{[a_1]} \cdots x^{[a_l]} \mid a_1 + \cdots + a_l \geq n).$$

Lemma 3.5. Let I be a divided power ideal. Then, $I^{[n]}$ is also a divided power ideal. Moreover, we have

$$(I^{[n]})^{[m]} \subseteq I^{[mn]}.$$

Proof. If $i \geq 1$ and $y = x_1^{[a_1]} \cdot \cdots \cdot x_l^{[a_l]}$, $a_1 + \cdots + a_l \geq n$, then, by (c) and (d),

$$\gamma_i(y) = \frac{(in)!}{(i!)^n n!} \cdot (x_1^{[a_1]} \cdot \cdots \cdot x_{l-1}^{[a_{l-1}]})^i \cdot x_l^{[ia_l]},$$

which is contained in $I^{[in]} \subseteq I^{[n]}$. Then we apply (b) to show that if $m \geq 1$, $\gamma_m(z) \in I^{[mn]}$ for all $z \in I^{[n]}$.

□

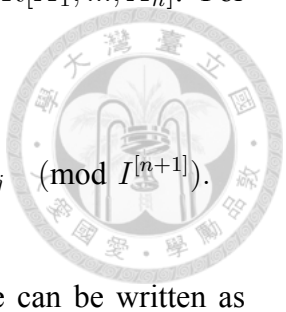
We say I is topologically nilpotent, if it is divided power and

$$\bigcap_n I^{[n]} = 0. \tag{12}$$

doi:10.6342/NTU201701790

Lemma 3.6. Let I be a divided power ideal. Let $P(X_1, ..., X_h) \in R[X_1, ..., X_h]$. For $u_1, ..., u_h \in R$ and $\mu_1, ..., \mu_h \in I^{[n]}$, $n \geq 1$, we have

$$P(u_1 + \mu_1, ..., u_h + \mu_h) \equiv P(u_1, ..., u_h) + \sum_{i=1}^{h} \frac{\partial P}{\partial X_j}(u_1, ..., u_h) \cdot \mu_j \pmod{I^{[n+1]}}.$$



Proof. This is from the Taylor expansion of P. The left-hand side can be written as $P(u_1, ..., u_h) + \sum_{i=1}^{h} \frac{\partial P}{\partial X_j}(u_1, ..., u_h) \cdot \mu_j + Q(\mu_1, ..., \mu_h)$, where $Q(X_1, ..., X_h)$ is a polynomial with coefficients in R such that the constant and degree one terms all vanishes. By Definition 3.1(d) and Lemma 3.5, $Q(\mu_1, ..., \mu_h) \in I^{[n+1]}$. □

As before, let E/K be a finite extension. Let t be a positive real number. The only possible divided power structure on M_E^t is the one such that $x^{[n]} = \frac{x^n}{n!}$.

Lemma 3.7. The ideal M_E^t of $\mathcal{O}_E$ is divided power if and only if $M_E^t = M_E^{t'}$ for some $t' \geq \frac{e_K}{p-1}$. It is topologically nilpotent if and only if t' can be chosen to be greater than $\frac{e_K}{p-1}$.

Proof. Let x be a generator of M_E^t with $v_K(x) = t' \geq t$. Then t' is the maximum of the numbers ν satisfying $M_E^t = M_E^\nu$. By replacing t with t', we may assume that $t = t'$. Thus, M_E^t is divided power if and only if for each positive n, $v_K(x^n) - v_K(n!) \geq t$, or equivalently,

$$(n-1)t \geq \sum_{i=1}^{\infty} \lfloor \frac{n}{p^i} \rfloor \cdot e_K. \tag{13}$$

Take $n = p^k$ for an integer k so that the right-hand side of (13) equals $\frac{p^k-1}{p-1} \cdot e_K$. Hence (13) implies $t \geq \frac{e_K}{p-1}$.

For the opposite implication, write $n = \sum_i a_i p^i$, $0 \leq a_i < p$. Then

$$\sum_{j=1}^{\infty} \lfloor \frac{n}{p^j} \rfloor \cdot e_K = \sum_i a_i \cdot \frac{p^i - 1}{p-1} \cdot e_K \leq (n-1) \cdot \frac{e_K}{p-1}.$$

Therefore the condition $t \geq e_K/(p-1)$ implies (13).

Now, if $t = \frac{e_K}{p-1}$, then by the above computation, $v_K(x^{p^k}/p^k!) = t$, for all $k \geq 1$.

doi:10.6342/NTU201701790

Consequently, M_E^t is not topologically nilpotent. On the other hand, if $t > \frac{e_K}{p-1}$, then

$$v_K(x^{p^k}/p^k!) = p^k \cdot t' - \frac{p^k - 1}{p-1} \cdot e_K = p^k \cdot (t' - \frac{e_K}{p-1}) - \frac{e_K}{p-1},$$

which tends to ∞ as $k \to \infty$. This implies M_E^t is topologically nilpotent. □

3.3 The relative differential forms

Let R be a commutative ring and B an R-algebra. Recall that the module of relative differential forms of B over R is a a B-module $\Omega^1_{B/R}$, together with an R-derivation $d : B \to \Omega^1_{B/R}$, which satisfies the universal property: for any B-module M, and for any R-derivation $d' : B \to M$, there exists a unique B-module homomorphism $f : \Omega^1_{B/R} \to M$ such that $d' = f \circ d$ [5, §II.8].

Let $f : B \otimes_R B \to B$ be the homomorphism sending $a \otimes b$ to $a \cdot b$ and write T for $\ker(f)$. Then $\Omega^1_{B/R} = T/T^2$ with the derivation $d : B \to T/T^2$ defined by $db = 1 \otimes b - b \otimes 1 \pmod{T^2}$ [5, §II.8, Proposition 8.1A].

Relative differentials of group schemes

If $G := \mathrm{Spec}(B)$ is a group scheme, then $\Omega^1_{B/R}$ can also be described as follow. Let e be the unity of G. Denote $I_G := \ker(e)$, the augmentation ideal.

Lemma 3.8. Let $G = \mathrm{Spec}(B)$ be a group scheme over R with augmentation ideal I_G. Then $\Omega^1_{B/R} \cong B \otimes_R I_G/I_G^2$.

Proof. See [13, Theorem 11.3]. □

Since R is free over R, the exact sequence

$$0 \longrightarrow I_G \longrightarrow B \xrightarrow{e} R \longrightarrow 0$$

splits, and hence

$$B = R \oplus I_G.$$

doi:10.6342/NTU201701790

Lemma 3.9. Let $G = \mathrm{Spec}(B)$ be a group scheme with co-multiplication $B \xrightarrow{c} B \otimes B$. Then

$$c(x) \equiv 1 \otimes x + x \otimes 1 \pmod{I_G \otimes_R I_G},\ \forall x \in I_G.$$

Proof. Express $B \otimes_R B$ as the direct sum of $R \otimes_R R$, $R \otimes_R I_G$, $I_G \otimes_R R$ and $I_G \otimes_R I_G$. For $x \in I_G$, write $c(x) = \alpha + \beta + \gamma + \delta$ where $\alpha, \beta, \gamma, \delta$ are in the corresponding components. By the commutative diagram:

$$\begin{array}{ccc} R \otimes_R B & \xleftarrow{e \otimes id_B} & B \otimes_R B \\ \uparrow{\scriptstyle 1 \otimes id_B} & & \uparrow{\scriptstyle c} \\ & & B, \end{array}$$

we obtain

$$1 \otimes x = (e \otimes id_B) \circ c(x) \quad = \alpha + \beta\ .$$

This implies that $\alpha = 0$ and $\beta = 1 \otimes x$, since $x \in I_G$. Then a similar argument implies $\gamma = x \otimes 1$. □

Lemma 3.10. Let $G = \mathrm{Spec}(B)$ be a group scheme annihilated by some integer n. Then $n \cdot \Omega^1_{B/R} = 0$.

Proof. Let $B^{\otimes n}$ denote the tensor product of B with itself n-times over R so that $B^{\otimes 1} = B$. Define $c^n : B \to B^{\otimes n+1} = B^{\otimes n} \otimes_R B$ be such that $c^1 = c$ and $c^n = (id_{B^{\otimes n-1}} \otimes c) \circ c^{n-1}$. Let $m_n : B^{\otimes n} \to B$ denote the multiplication sending $a_1 \otimes \cdots \otimes a_i \otimes \cdots \otimes a_n$ to $a_1 \cdot \cdots \cdot a_i \cdot \cdots \cdot a_n$. Then $m_n \circ c^{n-1} : B \to B$ is the morphism dual to $[n] : G \to G$ that sends each point to its nth power. Therefor $m_n \circ c^{n-1}$ factors through the structure map $1 : R \to B$, and hence induces the trivial map on $\Omega^1_{B/R}$. But Lemma 3.9 says it sends $x \in I_G/I_G^2$ to $n \cdot x \pmod{I_G^2}$.

□

doi:10.6342/NTU201701790

Relative differentials over $\mathcal{O}_K$

Now consider the situation in which B is a local algebra over $\mathcal{O}_K$. Let $\mathfrak{m}_B$ denote the maximal ideal of B. For latter application, we prove the following technical lemmas.

Lemma 3.11. Let B be a finite flat local algebra over $\mathcal{O}_K$ with the residue field $B/\mathfrak{m}_B = \mathcal{O}_K/\mathfrak{m}_K = k$. Suppose there is some non-zero $a \in \mathcal{O}_K$ annihilating $\Omega^1_{B/\mathcal{O}_K}$ to make $\Omega^1_{B/\mathcal{O}_K}$ a free B/aB-module. Let $\{x_1, \cdots, x_h\}$ be elements in $\mathfrak{m}_B$ lifting a basis of $\mathfrak{m}_B/(\mathfrak{m}_B^2 + \mathfrak{m}_K B)$ over k. Then $\{dx_i\}$ is a basis of $\Omega^1_{B/\mathcal{O}_K}$ over B/aB.

Proof. The assumption implies

$$B = \mathcal{O}_K + \mathfrak{m}_B. \tag{14}$$

Hence $\Omega^1_{B/\mathcal{O}_K}$ is generated by

$$d(\mathfrak{m}_B) := \{dx \mid x \in \mathfrak{m}_B\}.$$

Every $x \in \mathfrak{m}_B$ can be written as $x = \sum b_i x_i + z$, $b_i \in \mathcal{O}_K$, $z \in \mathfrak{m}_B^2 + \mathfrak{m}_K B$. Thus $dx = \sum b_i dx_i + dz$. Now (14) implies $\mathfrak{m}_K B = \mathfrak{m}_K \mathcal{O}_K + \mathfrak{m}_K \mathfrak{m}_B$, and hence

$$dz \in d(\mathfrak{m}_B^2 + \mathfrak{m}_K B) = d(\mathfrak{m}_B^2).$$

Consequently,

$$\Omega^1_{B/\mathcal{O}_K} = \text{span}_{\mathcal{O}_K}\{dx_i\} + d(\mathfrak{m}_B^2) \subseteq \text{span}_B\{dx_i\} + \mathfrak{m}_B \Omega^1_{B/\mathcal{O}_K}.$$

Then Nakayama's lemma says $\Omega^1_{B/\mathcal{O}_K} = \text{span}_B\{dx_i\}$.

Put $B' := B/(\mathfrak{m}_B^2 + \mathfrak{m}_K B)$. We have a surjection $\Omega^1_{B/\mathcal{O}_K} \twoheadrightarrow \Omega^1_{B'/\mathcal{O}_K}$ (see [5, §II.8, Proposition 8.3A]), and hence also

$$\Omega^1_{B/\mathcal{O}_K} \otimes_B (B/\mathfrak{m}_B) \twoheadrightarrow \Omega^1_{B'/\mathcal{O}_K} \otimes_B (B/\mathfrak{m}_B) .$$

Thus, if r denote the (B/aB)-rank of $\Omega^1_{B/\mathcal{O}_K}$, then

$$r \geq \dim_k \Omega^1_{B'/\mathcal{O}_K} \otimes_B (B/\mathfrak{m}_B) =: s.$$

doi:10.6342/NTU201701790

Since $k \subset B'$ and is isomorphic to the residue field of B', Proposition 8.7 of [5, §II.8] says

$$\mathfrak{m}_B/(\mathfrak{m}_B^2 + \mathfrak{m}_K B) \simeq \Omega^1_{B'/\mathcal{O}_K} \otimes_B (B/\mathfrak{m}_B).$$

Let d denote the $\mathcal{O}_K$-rank of B, which equals the $(\mathcal{O}_K/a\mathcal{O}_K)$-rank of B/aB. This implies that the $(\mathcal{O}_K/a\mathcal{O}_K)$-rank of $\Omega^1_{B/\mathcal{O}_K}$ equals dr. Hence

$$|\Omega^1_{B/\mathcal{O}_K}| = |\mathcal{O}_K/a\mathcal{O}_K|^{dr}.$$

On the other hand, since $\text{span}_B\{dx_i\}$ can be generated by ds elements over $\mathcal{O}_K$,

$$|\Omega^1_{B/\mathcal{O}_K}| = |\text{span}_B\{dx_i\}| \leq |\mathcal{O}_K/a\mathcal{O}_K|^{ds}.$$

By counting, the equality holds and $r = s$. This means $\{dx_i\}$ is actually a (B/aB)-basis.

□

Suppose in addition to the condition of the previous lemma, B is also a complete intersection over $\mathcal{O}_K$: $B = \mathcal{O}_K[[X_1, \cdots, X_h]]/(P_1, ..., P_h)$, each P_i satisfing the congruence (7). This assumption ensures that if x_i denotes the image of X_i in B, then the image of $\{x_1, ..., x_h\}$ in $\mathfrak{m}_B/(\mathfrak{m}_B^2 + \mathfrak{m}_K B)$ forms a basis over k. Hence

$$r = s = h. \tag{15}$$

For every i,

$$\sum \frac{\partial P_i}{\partial x_j}(x_1, \cdots, x_h)dx_j = dP_i(x_1, ..., x_h) = 0.$$

By Lemma 3.11, we can write

$$\frac{\partial P_i}{\partial x_j}(x_1, \cdots, x_h) = ap_{ij} \tag{16}$$

for some $p_{ij} \in B$. Since B is free over $\mathcal{O}_K$, these p_{ij} are unique. In this circumstance, we have the following lemma.

doi:10.6342/NTU201701790

Lemma 3.12. The matrix (p_{ij}) is invertible over B.

Proof. Denote $C = \mathcal{O}_K[[X_1, \cdots, X_h]]$, $J = (P_1, ..., P_h)$ so that $B = C/J$. Proposition 8.3A of [5, §II.8] says that kernel of the homomorphism $\Omega^1_{C/\mathcal{O}_K} \otimes_C B \to \Omega^1_{B/\mathcal{O}_K}$, $dX_i \otimes b \mapsto bdx_i$, is generated by $dP_1, ..., dP_h$ over B. Since adX_i is in the kernel, we have $a \cdot dX_i = \sum_j q_{ij} \cdot dP_j$, for some $q_{ij} \in B$. We check that (q_{ij}) is the inverse of (p_{ij}). □

Lemma 3.13. If B is a finite flat $\mathcal{O}_K$-algebra with $\Omega^1_{B/\mathcal{O}_K} = 0$, then B is étale over $\mathcal{O}_K$.

Proof. We have to show that $B \otimes K/K$ and $B \otimes k/k$ are étale. By [13, §11.2 (a)], both $\Omega^1_{B\otimes K/K}$ and $\Omega^1_{B\otimes k/k}$ are 0. Thus, by [13, §11.2 (e)], both $B \otimes K/K$ and $B \otimes k/k$ are étale.

□

3.4 The proof

As mentioned before, Theorem 3.1 is going to be proved, but only for $K = \mathbb{Q}_p$ and $n = 1$.

The proof of Theorem 3.1

We shall apply the following proposition whose proof will be given in §3.4

Proposition 3.2. Let B be a finite flat $\mathcal{O}_K$-algebra locally of complete intersection. Suppose there exists an $a \in \mathcal{O}_K$ such that $\Omega^1_{B/\mathcal{O}_K}$ is flat over B/aB. Denote $Y = \text{Spec}(B)$. The following holds:

(i) For every finite flat $\mathcal{O}_K$-algebra S and for all topologically nilpotent divided power ideal $I \subseteq S$, we have

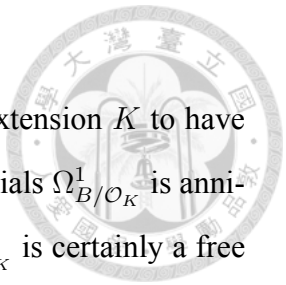
$$Y(S) \cong \text{img}(Y(S/aI) \to Y(S/I)).$$

(ii) Write L for the Galois extension $K(Y(\bar{K}))$. Then

$$u_{L/K} \leq v_K(a) + e_K/(p-1).$$

doi:10.6342/NTU201701790

Now we prove our theorem.



Proof of Theorem 3.1. We may replace Q_p by a finite unramified extension K to have Theorem 2.5 holds for $L = K$. By Lemma 3.10, the relative differentials $\Omega^1_{B/\mathcal{O}_K}$ is annihilated by p. Since the residue field $\mathcal{O}_K/p\mathcal{O}_K = \mathbb{F}_p$ is a field, $\Omega^1_{B/\mathcal{O}_K}$ is certainly a free module over $\mathcal{O}_K/p\mathcal{O}_K$. Therefore, Proposition 3.2 is applicable to our situation. Hence by the assertion (ii) of the proposition, we have

$$u_{L/K} \leq 1 + 1/(p-1).$$

□

The proof of Proposition 3.2

To prove Proposition 3.2(i), we may assume that B is a local algebra over $\mathcal{O}_K$. Hence $B = \mathcal{O}_K[[X_1, ..., X_h]]/(P_1, ..., P_h)$, where P_j satisfies the congruence (7). As before, let x_i denote the image of X_i in B. Let S be a finite flat $\mathcal{O}_K$-algebra, I a topological nilpotent divided power ideal in S and $Y = \text{Spec}(B)$. Write y_n for $\text{img}(Y(S/aI^{[n]}) \to Y(S/I^{[n]}))$.

Lemma 3.14. For $n \geq 1$, the natural map

$$Y(S/aI^{[n+1]}) \to Y(S/aI^{[n]})$$

is surjective. It induces a bijection $y_n \to y_{n+1}$.

Proof. An element of $Y(S/aI^{[n]})$ corresponds to a $\mathcal{O}_K$-algebra homomorphism $\psi : B \to S/aI^{[n]}$, or equivalently, $u_1, ..., u_h \in S$ such that $P_i(u_1, ..., u_h) \in aI^{[n]}$, for $i = 1, ..., h$. We need to find $\mu_1, ..., \mu_h \in I^{[n]}$ to have $P_i(u_1 + \mu_1, ..., u_h + \mu_h)$ belonging to $aI^{[n+1]}$ and show that $\mu_1, ..., \mu_h$ is unique in $I^{[n]}/I^{[n+1]}$.

By (16), we can write $\frac{\partial P_i}{\partial X_j}(u_1, ..., u_h) = a\bar{p}_{ij}$ (which equals $\psi(p_{ij})$), for some $\bar{p}_{ij} \in S/aI^{[n]}$. Lemma 3.12 implies that the matrix $(\bar{p}_{ij})$ is invertible. Let λ_i denote $P_i(u_1, ..., u_h)$.

doi:10.6342/NTU201701790

Then Lemma 3.14 gives

$$P_i(u_1+\mu_1,\cdots,u_h+\mu_h) \equiv a(\lambda_i + \sum_j \bar{p}_{ij}\cdot\mu_j) \pmod{aI^{[n+1]}}.$$

Since $(\bar{p}_{ij})$ is invertible, there are unique $\mu_1, ..., \mu_h \in I^{[n]}$ to have

$$\lambda_i + \sum_j \bar{p}_{ij}\cdot\mu_j \equiv 0 \pmod{I^{[n+1]}}. \tag{17}$$

The congruence (17) is a sufficient condition for $P_i(u_1+\mu_1, ..., u_h+\mu_h) \in aI^{[n+1]}$. To complete the proof, we need to show that it is also a necessary condition. But this is actually a consequence of the fact that S is a free $\mathcal{O}_K$-module, and hence $aI^{[n+1]}$ is a free submodule, consequently, $a\cdot z \in aI^{[n+1]}$ if and only if $z \in I^{[n+1]}$.

□

Proof of Proposition 3.2. Denote $S_\infty := \varprojlim_n S/I^{[n]}$ and consider the natural homomorphism $S \to S_\infty$ whose image is a dense set in S_∞. Since S, being a finite free $\mathcal{O}_K$-module, is compact in the $\mathfrak{m}_K$-adic topology, the image in question is compact, and hence the whole S_∞. Also, because I is topological nilpotent, the homomorphism is injective. Therefore, we can identify S with S_∞.

An $\mathcal{O}_K$-homomorphism $B \to S$ induces homomorphisms $B \to S/aI \to S/I$. This defines the map

$$Y(S) \to \text{img}(Y(S/aI) \to Y(S/I)) = y_1.$$

Lemma 3.14 says an element in y_1 determines an element in $Y(S_\infty) = Y(S)$. Hence we have $y_1 \to Y(S)$. These two maps are inverse to each other. This proves (i).

Suppose a is a unit. Then $\Omega^1_{B/\mathcal{O}_K} = 0$, which by Lemma 3.13 implies $B/\mathcal{O}_K$ is étale. Hence L/K is unramified by Proposition 2.1 together with its proof. By Lemma 3.4, $u_{L/K} = 0$. In this case, (ii) trivially holds.

For the rest of the proof, we assume that $a \in \mathfrak{m}_K$. If L/K is tamely ramified, then $u_{L/K} = 1$ by Lemma 3.4. In this case, (ii) also holds trivially. It remains to treat the wildly ramified case.

doi:10.6342/NTU201701790

Denote $X := \text{Spec}(\mathcal{O}_L)$. We claim that if

$$t > v_K(a) + e_K/(p-1),$$

then the implication (11) holds for every finite extension E/K. Then by Proposition 3.1, the above inequality implies

$$t > u_{L/K} - 1/e_{L/K}.$$

This shows

$$u_{L/K} \leq v_K(a) + e_K/(p-1) + 1/e_{L/K}. \tag{18}$$

Write $G = \text{Gal}(L/K)$. The wild ramification assumption implies p divides $|G_s|$, for $s > 0$. Because $\phi(0) = 0$, by the definition of ϕ, we deduce that p divides $e_{L/K} \cdot \phi(s)$ for all positive integer s. In particular, $p \mid e_{L/K} \cdot u_{L/K}$. Hence (18) implies

$$u_{L/K} \leq v_K(a) + e_K/(p-1)$$

as desired.

To prove the claim, assuming $t > v_K(a) + e_K/(p-1)$ and $X(\mathcal{O}_E/M_E^t)$ contains an element $\mathcal{O}_L \xrightarrow{\eta} \mathcal{O}_E/M_E^t$, we have to show the existence of some $\mathcal{O}_K$-homomorphism $\mathcal{O}_L \to \mathcal{O}_E$, or equivalently, some K-embedding $L \to E$.

Denote $B_K := B \otimes_{\mathcal{O}_K} K$, it contains $\mathcal{O}_K$ and is finite over K. Proposition 2.2 says B_K/K is étale. Hence B_K can be written as $\prod_{i=1}^{m} L_i$, where each L_i is a finite extension of K. For each finite extension E/K, we have

$$\begin{aligned} Y(E) &= Y(\mathcal{O}_E) \\ &= \text{Hom}_{\mathcal{O}_K\text{-alg}}(B, \mathcal{O}_E) \\ &= \text{Hom}_{K\text{-alg}}(B_K, E) \\ &= \coprod_{i=1}^{m} \text{Hom}_K(L_i, E). \end{aligned}$$

The number of K-homomorphisms from L_i to E is $\leq [L_i : K]$, and the equality holds

doi:10.6342/NTU201701790

if and only if E contains a field isomorphic to the Galois closure of L_i over K. Hence

$$|Y(E)| \leq |Y(L)|,$$

and the equality holds if and only if L/K can be embedded into E/K. Thus, it remains to show $|Y(E)| \geq |Y(L)|$.

For each E, write $M_E^t = aI_E$ with

$$I_E = \{c \in \mathcal{O}_E \mid v_K(c) \geq t - v_K(a)\},$$

which by Lemma 3.7 is a topologically nilpotent divided power ideal. Now, for every $u \in Y(\mathcal{O}_L)$, the assertion (i) (applied to the case where $S = \mathcal{O}_E$) says the composition $\eta \circ u : B \to \mathcal{O}_E/aI_E$ determines uniquely an $u^\eta \in Y(\mathcal{O}_E)$ such that the following diagram commutes:

$$\begin{array}{ccc} B & \xrightarrow{\eta \circ u} & \mathcal{O}_E/aI_E \\ {\scriptstyle u^\eta}\downarrow & & \downarrow{\scriptstyle \text{projection}} \\ \mathcal{O}_E & \xrightarrow[\text{projection}]{} & \mathcal{O}_E/I_E. \end{array}$$

This defines a mapping $Y(L) \to Y(E)$. It remains to prove that this mapping is injective. But, since aI_L is the kernel of η, and hence each u^η factors through

$$\mathcal{O}_L \xrightarrow{\bar{u}^\eta} \mathcal{O}_L/aI_L \hookrightarrow \mathcal{O}_E/aI_E \ .$$

If $u^\eta = w^\eta$, then $\bar{u}^\eta = \bar{w}^\eta$. By applying (i) to the $S = L$ case, we conclude that $u = w$.

□

4 The choice of a prime

In this section, let J denote a finite flat group scheme over $\mathbb{Z}$ annihilated by a power of a prime number p. We shall investigate the structure of J for the case where $p =$

doi:10.6342/NTU201701790

$3, 5, 7, 11, 13, 17$. It is known that for such p the cyclotomic field $\mathbb{Q}(\sqrt[p]{1})$ has class number 1 (see [12, Table §3]).

4.1 The global ramification theory

Denote $F := \mathbb{Q}(J(\bar{\mathbb{Q}}))$, $n = [F : \mathbb{Q}]$, and $G := \mathrm{Gal}(F/\mathbb{Q})$. Then $F/\mathbb{Q}$ is unramified out side $\{p, \infty\}$. Let w be a place of F sitting over p. Take $L = F_w$, $K = \mathbb{Q}_p$ and apply Theorem 3.1, we obrain

$$u_{F_v/\mathbb{Q}_p} \leq 1 + \frac{1}{p-1}. \tag{19}$$

Minkowski's lower bounds of the discriminant

If $\mathfrak{D}_{F_w/\mathbb{Q}_p}$ denotes the different of $F_w/\mathbb{Q}_p$, then (see [1, §I.9, Propostion 4])

$$v_p(\mathfrak{D}_{F_w/\mathbb{Q}_p}) = u_{F_w/\mathbb{Q}_p},$$

which, together with (19), lead to the inequality for the discriminant d_F of F:

$$d_F^{\frac{1}{n}} \leq p^{1+\frac{1}{p-1}}. \tag{20}$$

Thus, the Minkowski's lower bound

$$d_F^{\frac{1}{n}} \geq \frac{\pi}{4} \cdot (\frac{n}{n!^{\frac{1}{n}}})^2$$

implies

$$p^{1+\frac{1}{p-1}} \geq \frac{\pi}{4} \cdot (\frac{n}{n!^{\frac{1}{n}}})^2. \tag{21}$$

For simplicity, call the right-hand side of the above $f(n)$. The following is a hand-made table of $f(n)$ for some small integers n.

Lemma 4.1. The function $f(n)$ is an increasing function of n.

Proof. This is proved in Theorem 2.1 in Appendix A. It can also be proved by using the

doi:10.6342/NTU201701790

Table 1: The values of $f(n)$

n	1	2	3	4	5	6	7	8	9	10
f(n)	0.78	1.57	2.13	2.56	2.89	3.15	3.36	3.55	3.70	3.82
n	15	20	25	30	35	40	45	50	52	53
f(n)	4.28	4.55	4.74	4.87	4.97	5.01	5.12	5.17	5.191	5.198

Stirling's formula for $n!$. □

Now $3^{1.5} = 5.19615....$ Thus, by (21), Table 1 and Lemma 4.1, for $p = 3$, the order of G can not exceed 52. Indeed, by using a better estimation and the table given by Diaz y Diaz [2], one can deduce that, for $p = 3, 5, 7, 11, 13, 17$ respectively, the order of G can not exceed $6, 12, 18, 50, 88, 574$.

For the remaining of this thesis, the symbol p will stand for one of the above six prime numbers. We shall consider the case where F contains $F_0 := \mathbb{Q}(\sqrt[p]{1})$ and write $H := \mathrm{Gal}(F/F_0)$, $n' = |H|$. By the above discussion, n' is at most 35. Hence H is a solvable group. That will be crucial for later discussion.

The field extension $F/\mathbb{Q}$

Because of our choice of p, the field extension $F/\mathbb{Q}$ turns out to be small in the following sense.

Lemma 4.2. Suppose J is a finite flat group scheme over $\mathbb{Z}$ annihilated by a power of p. Let $F = \mathbb{Q}(J(\bar{\mathbb{Q}}))$. Then $F \subseteq \mathbb{Q}(\sqrt[p]{1})$.

Proof. By replacing J with the direct product $J \times \mu_p$ if necessary, we may assume that μ_p is a subgroup of J, and hence $\mathbb{Q}(\sqrt[p]{1}) \subset F$. We use the notation introduced above so that $F_0 = \mathbb{Q}(\sqrt[p]{1})$ and so on. We are in the situation where (a) The inequality (19) holds, (b) $F/\mathbb{Q}$ is a Galois extension, (c) F/F_0 only ramified at the unique place v of F_0 sitting over p, (d) F_0 has class number 1, and (e) H is solvable. It remains to show that these five conditions imply $H = \{id\}$. We shall give a proof by contradiction, hence at first assume H non-trivial.

Denote $\Gamma := \mathrm{Gal}(F_0/\mathbb{Q})$. Let $\gamma \in \Gamma$ and let $\tilde{\gamma} \in G$ be a lift of γ. The conjugation $\tau \mapsto \tilde{\gamma}\tau\tilde{\gamma}^{-1}$ defines an automorphism on H. The commutator subgroup $[H : H]$ is

doi:10.6342/NTU201701790

invariant under the automorphism. This induces an action of γ on $H^{ab} := H/[H : H]$. It is independent of the choice of $\tilde{\gamma}$. Thus, we have the conjugate action of Γ on H^{ab}.

Since H is solvable and non-trivial, so is H^{ab}. Hence, by replacing H by the quotient H^{ab}, or equivalently replacing F by the subfield $F^{[H:H]}$, we reduce the proof to case where H is commutative. Note that (10) says the inequality (19) holds for the new F, since the upper numbering is stable under going down form a Galois extension to a Galois sub-extension (see [1, §I.9, Theorem 2(ii)]).

We may make further reduction by choosing a proper Γ-invariant subgroup N (so that $F^N/\mathbb{Q}$ is also a Galois extension) then replace H by H/N (F by F^N). Again, the condition (a)-(e) also holds for the new F.

Let w be a place of F sitting over p and let $H_{0,w} \subset H$ denote the inertia subgroup at w. Since H is commutative, if w' is another place of F sitting over p, then $H_{0,w'} = H_{0,w}$. Since the conjugate action of each $\gamma \in \Gamma$ sends $H_{0,w}$ to some $H_{0,w'}$, we conclude that $H_{0,w}$ is invariant under the action of Γ. We claim that $H_{0,w} = H$, and hence w is totally ramified under $F/\mathbb{Q}$. If the claim does not hold, then by replacing H with $H/H_{0,w}$, we may assume that F/F_0 is unramified at every place. Then F is a sub field of the Hilbert class field of F_0, but because of (d), the Hilbert class fields is F_0 itself, and hence $F = F_0$, a contradiction.

We can make another type of reduction. Because every Sylow l-subgroup H_l of H is invariant under the conjugate action of Γ, we may choose a non-trivial H_l and replace H by H/H_l to make the order of H smaller, unless $H_l = H$. Thus, by keeping doing so, we can reduce the proof to the case where H is an l-group for some l.

Because $F/\mathbb{Q}$ is totally ramified at p, the residue field $\mathbb{F}_w$ at w is the same as $\mathbb{F}_p$. If $l \neq p$, then $F/\mathbb{Q}$ is tamely ramified at w, and hence there is an injection $\mathrm{Gal}(F/\mathbb{Q}) \to \mathbb{F}_p^\times$ [1, §I.8, Theorem 1]. This means $[F : \mathbb{Q}] \leq p - 1 = [F_0 : \mathbb{Q}]$, a contradiction.

Finally, we consider the case where H is a p-group. Since $N := p \cdot H$ is Γ-invariant, we can replace H by H/N to make H an $\mathbb{F}_p$-vector space. Also, because H is decomposed into the direct sum of 1-dimensional χ-eigenspaces of characters $\chi \in \mathrm{Hom}(\Gamma, \mathbb{F}_p)$, we may further reduce the condition to the case where H is an 1-dimensional eigenspace,

doi:10.6342/NTU201701790

hence cyclic of order p. Let δ denote $\max\{i_G(\sigma) \mid \sigma \neq id_G\}$, which is the smallest integer u such that $G_u = \{id_G\}$. By the definition (9) of the Herbrand function and by the definition of $u_{F_w/\mathbb{Q}_p}$,

$$\begin{aligned} u_{F_w/\mathbb{Q}_p} &= \phi(\delta-1)+1 \\ &= \tfrac{1}{p(p-1)}\left(\sum_{i_G(\sigma)\leq\delta} i_G(\sigma)\right)+\delta \\ &= \tfrac{1}{p(p-1)}\left(\sum_{i=0}^{\delta-1}|G_i|-|G_{i+1}|\cdot(i+1)\right)+\delta \\ &= \tfrac{1}{p(p-1)}(|G_0|+|G_1|+\cdots+|G_{\delta-1}|). \end{aligned}$$

In our case, $|G_0| = p(p-1)$ and $|G_1| = p$. Thus, Fontaine's bound (19) implies

$$\delta = 2. \tag{22}$$

That means for every non-trivial $\sigma \in H$,

$$i_H(\sigma) = i_G(\sigma) = 2.$$

Hence $H_0 = H_1 = H$ and H_2 is trivial. Write L, K for F_w, $F_{0,w}$. Then similar computation leads to

$$u_{L/K} = \frac{1}{p}(|H_0|+|H_1|) = 2.$$

Thus, by (10), H^μ is trivial for $\mu > 1$. Let ζ be a primitive pth root of 1 and write $\xi := \zeta - 1$, which is a uniformizer of $\mathcal{O}_K$. Denote $U_\mu := 1 + \xi^\mu \mathcal{O}_K$, for $\mu = 1, 2, \ldots$. The local class field theory says that the local reciprocity map

$$\theta : K^\times \to H$$

factors through $K^\times \to K^\times/U_2$ (see [1, §VI.4, Theorem 1]). Because L/K is totally ramified, we have $\theta(\mathcal{O}_K^\times) = H$ [1, §VI.2.5, Corollary]. Moreover, since $\mathcal{O}_K^\times/U_1 \simeq \mathbb{F}_p^\times$ has order prime to p, we have the isomorphism

doi:10.6342/NTU201701790

$$U_1/U_2 \xrightarrow[\sim]{\theta} H \ .$$

The above isomorphism respects the actions of Γ, which acts on the left-hand side via the Galois action on $\mathcal{O}_K^\times$, and on the right-hand side by sending $\tau \in H$ to the above conjugate: ${}^\gamma\tau := \tilde{\gamma}\tau\tilde{\gamma}^{-1}$ [11, §XIII.3]. Let $t : \Gamma \to \mathbb{F}_p^\times$ be the character such that ${}^\gamma\zeta = \zeta^{t(\gamma)}$. Then γ sends $1 + \xi \pmod{U_2}$, a generator of U_1/U_2, to $1 + t(\gamma)\xi \pmod{U_2}$. This means

$$ {}^\gamma\tau = \tau^{t(\gamma)}. \tag{23}$$

Kummer theory tells us that if $\bar{a}$ denotes $a \pmod{(F_0^\times)^p}$ for $a \in F_0^\times$, then the mapping

$$F_0^\times/(F_0^\times)^p \xrightarrow{\psi} \mathrm{Hom}(\mathrm{Gal}(\bar{F}_0/F_0), \mu_p)$$

$$\bar{a} \longrightarrow \psi_{\bar{a}} : \sigma \mapsto \frac{{}^\sigma\sqrt[p]{a}}{\sqrt[p]{a}}$$

is a Γ-isomorphism in the sense that

$$\psi_{{}^\gamma\bar{a}}(\sigma) = {}^\gamma\psi_{\bar{a}}({}^{\gamma^{-1}}\sigma). \tag{24}$$

We can write $F = F_0(\sqrt[p]{a})$ for some $a \in F_0^\times$. Then F is the fixed field of $\ker(\psi_{\bar{a}})$. Also, since ${}^\gamma\zeta = \zeta^{t(\gamma)}$, the equalities (23) and (24) together imply that $\psi_{{}^\gamma\bar{a}} = \psi_{\bar{a}}$. This means

$$\rho(\gamma) := \frac{{}^\gamma a}{a} \in (F_0^*)^p.$$

Since the cocycle condition $\rho(\gamma_1\gamma_2) = {}^{\gamma_1}\rho(\gamma_2) \cdot \rho(\gamma_2)$ is satisfied, our ρ gives rise to a class $[\rho] \in \mathrm{H}^1(\Gamma, (F_0^*)^p)$. Now the exact sequence

$$1 \to \mu_p \to F_0^* \to (F_0^*)^p \to 1,$$

induces the exact sequence

$$\mathrm{H}^1(\Gamma, F_0^*) \to \mathrm{H}^1(\Gamma, (F_0^*)^p) \to \mathrm{H}^2(\Gamma, \mu_p).$$

doi:10.6342/NTU201701790

Hilbert's Theorem 90 says $\mathrm{H}^1(\Gamma, F_0^*) = 0$, and since Γ is cyclic,

$$\mathrm{H}^2(\Gamma, \mu_p) \cong \widehat{\mathrm{H}}^0(\Gamma, \mu_p) \cong \mu_p^\Gamma / N_{F_0/\mathbb{Q}}(\mu_p) = 0$$

Hence $\mathrm{H}^1(\Gamma, (F_0^*)^p) = 0$. This shows that there exists $b \in (F_0^*)^p$ such that $\rho(\gamma) = {}^\gamma b/b$, for all $\gamma \in H$. This means that a/b is fixed by Γ. Thus, by replacing a by a/b, we may assume that $a \in \mathbb{Q}$. We may further assume that $a \in \mathbb{Z}$, not divisible by any non-trivial pth power of integer. Then a can not be divided by any prime number l other than p, for otherwise F/F_0 would be ramified at l. Since -1 is a pth power, and $F_0(\sqrt[p]{p^\nu}) = F_0(\sqrt[p]{p})$, for $\nu = 1, ..., p-1$, we can conclude that $F = F_0(\sqrt[p]{p})$.

Set $\alpha := \frac{\xi}{\sqrt[p]{p}}$. The valuation $v_L(\alpha) = 1$, and hence α is a uniformizer of $\mathcal{O}_L$. If γ is a non-trivial element of Γ, then ${}^\gamma\alpha = \zeta' \cdot \alpha$. for some $\zeta' \in \mu_p$. This shows $i_H(\gamma) = v_L({}^\gamma\alpha - \alpha) = p + 1$ and leads to

$$2 = \delta \geq p + 1.$$

That is absurd.

□

4.2 The decomposition theorem

The rest of this section is to verify the following decomposition theorem. In this subsection by a group scheme we shall understand a commutative group scheme, and we say a p-group scheme is constant (resp. diagonalisable) if it is isomorphic to a direct sum of $\mathbb{Z}/p^a\mathbb{Z}$ (resp. μ_{p^a}). We sometimes use *commutative* group scheme to emphasize its commutativity.

Theorem 4.1. *Let p be one of the primes $3, 5, 7, 11, 13, 17$. Then any commutative finite flat group scheme J over $\mathbb{Z}$ which is annihilated by a power of p is a direct sum of constant and diagonalisable group schemes.*

The proof will be completed in §4.2.

Remark 4.1. Let $\mathscr{A}$ be the Néron model of an abelian variety A over $\mathbb{Q}$. By Theorem

doi:10.6342/NTU201701790

4.1, $\mathscr{A}_p \cong (\mathbb{Z}/p\mathbb{Z})^a \oplus \mu_p^b$ for some $a,\ b$ such that $a+b=2g$. Then the same theorem says that $\mathscr{A}_{p^2} \cong (\mathbb{Z}/p\mathbb{Z})^{a_1} \oplus (\mathbb{Z}/p^2\mathbb{Z})^{a_2} \oplus \mu_p^{b_1} \oplus \mu_{p^2}^{b_2}$ with $a_1+a_2+b_1+b_2=2g$.

By [7, Proposition 20.7], the multiplication-by-p map [p] on $\mathscr{A}$ is surjective, so we have a surjection $\mathscr{A}_{p^2} \longrightarrow\!\!\!\!\rightarrow \mathscr{A}_p$. This means $a_2 \geq a$ and $b_2 \geq b$. Since $a_2+b_2 \leq 2g = a+b$, we have $a_2=a,\ b_2=b$, and $a_1=b_1=0$, i.e. $\mathscr{A}_{p^2} \cong (\mathbb{Z}/p^2\mathbb{Z})^a \oplus \mu_{p^2}^b$.

Applying similar arguments, we see that $\mathscr{A}_{p^n} \cong (\mathbb{Z}/p^n\mathbb{Z})^a \oplus \mu_{p^n}^b$.

Proposition 4.1. Let $\mathscr{A}$ be an abelian scheme over $\mathbb{Z}$ of dimension g, and let $p=3$. Then $\mathscr{A}_{p^n} \cong (\mathbb{Z}/p^n\mathbb{Z})^g \oplus (\mu_{p^n})^g$.

Proof. By Theorem 4.1 and the discussions that follow it, $\mathscr{A}_{p^n} \cong (\mathbb{Z}/p^n\mathbb{Z})^a \oplus (\mu_{p^n})^b$ with $a+b=2g$. Then $\bar{A}_{p^n}$ is the special fiber of $\mathscr{A}_{p^n}$, hence of the form $(\mathbb{Z}/p^n\mathbb{Z})^a \oplus (\mu_{p^n})^b$ over the residue field k_p. This means the geometric points of $\bar{A}_{p^n}$ form $(\mathbb{Z}/p^n\mathbb{Z})^a$. But it is known that the geometric points of $\bar{A}_{p^n}$ is of rank $\leq g$. Thus $a \leq g$. Take the dual abelian variety A^t of A and let $\mathscr{A}^t$ denote the Néron model of A^t. Then $\mathscr{A}^t_{p^n}$ is the Cartier dual (see §2.2) of $\mathscr{A}_{p^n}$ (Cf [8, III.15 Theorem 1, p143]), hence of the form $(\mathbb{Z}/p^n\mathbb{Z})^b \oplus (\mu_{p^n})^a$. But we have already proved $b \leq g$. Therefore $a=b=g$. □

Raynaud's theorem

First we recall the following result of Raynaud [10, Theorem 3.3.3].

Theorem 4.2. *Let p be an odd prime. Then a finite flat commutative p-group X over $\mathbb{Q}$ has at most one extension to $\mathbb{Z}$. That is, there is at most one finite flat group scheme $\mathscr{X}$ over $\mathbb{Z}$ such that $\mathscr{X}_{\mathbb{Q}} \cong X$.*

Let J be a finite p-group over $\mathbb{Z}$. Denote $E := \mathbb{Q}(J(\bar{\mathbb{Q}}))$ and $G := \mathrm{Gal}(E/\mathbb{Q})$.

Lemma 4.3. J is uniquely determined (up to isomorphism) by the G-module structure of $J(\bar{\mathbb{Q}})$.

Proof. Theorem 4.2 says J is determined by $J_{\mathbb{Q}}$, while Theorem 2.2 tells us that $J_{\mathbb{Q}}$ is uniquely determined by the abelian group $J(\bar{\mathbb{Q}})$ together with the action of G. □

doi:10.6342/NTU201701790

Lemma 4.4. Suppose J is an extension of a constant group by a constant group. Then $E = \mathbb{Q}(J(\bar{\mathbb{Q}}))/\mathbb{Q}$ is a p-extension.

Proof. Suppose we have an exact sequence

$$0 \to A \to J \to B \to 0.$$

By Theorem 2.2, this corresponds to an exact sequence of G-modules:

$$0 \to A \to J \to B \to 0.$$

Define $f : G \times J \to A$ by $f(\sigma, x) = {}^{\sigma}x - x$ which is in A as G acts trivially on B. It follows that $f(-, x)$ defines a 1-co-cycle:

$$\begin{aligned} f(\sigma_1\sigma_2, x) &= {}^{\sigma_1\sigma_2}x - x \\ &= {}^{\sigma_1\sigma_2}x - {}^{\sigma_1}x + {}^{\sigma_1}x - x \\ &= {}^{\sigma_1}f(\sigma_2, x) + f(\sigma_1, x). \end{aligned}$$

However, because G acts trivially on A as well, so that $f(-, x)$ is a group homomoorphism for every $x \in J$. Since the intersection $\bigcap_{x\in J} \ker(f(-, x))$ is trivial, $\oplus_x f(-, x)$ defines an embedding of G into a direct sum of copies of A. Therefore G is a p-group. □

The proof of Theorem 4.1

Before proving the theorem, we first discuss about the sub-objects and the quotients of group schemes.

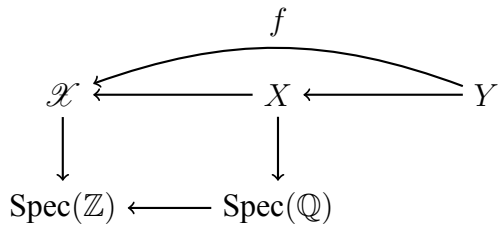
Remark 4.2. Sub-objects and quotients.

1. Recall the results of Raynaud (see [10, §2]).

   Let R be a discrete valuation ring with fraction field K and residue field k of characteristic p.

   Let $\mathscr{X}$ be a flat R-scheme of finite type with generic fiber $X = \mathscr{X} \otimes_R K$. Let Y be a closed sub-scheme of X. See the following diagram.

doi:10.6342/NTU201701790



Then the *scheme-theoretic image* of the map $f : Y \to X \to \mathscr{X}$ is the closed subscheme Z of $\mathscr{X}$ such that f factors through Z and that for every closed $Z' \hookrightarrow \mathscr{X}$ through which f factors, we have $Z \subseteq Z'$. Namely, it is the smallest closed subscheme through which f factors. Denote the scheme-theoretic image of f as $\mathrm{SchIm}(f)$.

If $\mathscr{X} = \mathrm{Spec}(B)$, then $X = \mathrm{Spec}(B \otimes_{\mathbb{Z}} \mathbb{Q})$ and $Y = \mathrm{Spec}(B \otimes_{\mathbb{Z}} \mathbb{Q}/I)$ for some ideal I of $B \otimes_{\mathbb{Z}} \mathbb{Q}$. Since B is flat, we may regard B as a sub-algerba of $B \otimes_{\mathbb{Z}} \mathbb{Q}$. Then we see that f factors through $\mathrm{Spec}(B/J)$ for some ideal J if and only if $J \subseteq B \cap I$. Thus $\mathrm{Spec}(B/B \cap I) = \mathrm{SchIm}(f)$.

Since for every $x \in I$, there is an integer n such that $n \cdot x \in B \cap I$, we have $(B \cap I) \otimes \mathbb{Q} = I$. Therefore $\mathrm{SchIm}(f) \otimes \mathbb{Q} \cong Y$.

This shows that the subgroups of a group over $\mathbb{Q}$, which admits an extension to $\mathbb{Z}$, have extensions to $\mathbb{Z}$.

2. Let J be a finite flat group scheme over $\mathbb{Q}$ and let $\mathscr{J}$ be a finite flat group scheme over $\mathbb{Z}$ with generic fiber J. Let H be a flat closed subgroup of J. Then since $\mathbb{Q}$ is Artinian, by [9, page 82, (i)], the quotient J/H is representable.

   Further, let $\mathscr{H}$ be the scheme-theoretic image of H in $\mathscr{J}$ as above. By [4, page 71, Corollaire 17.6.2.] and [9, page 82, (a) (ii)], the quotient $\mathscr{J}/\mathscr{H}$ is representable as well. And it is evident that the generic fiber of $\mathscr{J}/\mathscr{H}$ is J/H.

Now we are ready to complete the proof.

Proof of Theorem4.1. The proof is divided in six steps.

1. *Every finite p-group over $\mathbb{Z}$, which is an extension of a constant group by a constant group is constant.*

doi:10.6342/NTU201701790

Let J be such a group, and let E be as in Lemma 4.4. By Lemma 4.4, we know $E/\mathbb{Q}$ is a p-extension, hence solvable. Furthermore, $E/\mathbb{Q}$ is everywhere unramified, since an extension of an étale group by an étale group is étale. But $\mathbb{Q}$ is of class number 1, hence $E = \mathbb{Q}$. By Lemma 4.3, we conclude that J is constant.

2. *Every finite commutative p-group over $\mathbb{Z}$, which is an extension of a diagonalisable group by a diagonalisable group is diagonalisable.*

   Apply the argument in step 1. to the Cartier dual sequence.

3. *In the category of finite p-groups over $\mathbb{Z}$, every extension of $\mathbb{Z}/p\mathbb{Z}$ by a diagonalisable group μ is trivial.*

   Given an exact sequence

$$0 \to \mu \to J \to \mathbb{Z}/p\mathbb{Z} \to 0,$$

   we shall show it splits.

   Let u be a lift of a generator of $\mathbb{Z}/p\mathbb{Z}$ in $J(\bar{\mathbb{Q}})$. Then $v = p \cdot u \in \mu(\bar{\mathbb{Q}})$. Also, for every $g \in G$, $w_g := {}^g u - u \in \mu(\bar{\mathbb{Q}})$ since G acts trivially on $\mathbb{Z}/p\mathbb{Z}$. Then ${}^g v = p \cdot ({}^g u) = p \cdot (w_g + u) = v + p \cdot w_g$. But μ is diagonalisable, so ${}^g v = \chi_1(g) \cdot v$. If we choose g such that $\chi_1(g) \neq 1$, then we see u can be choosen so that $p \cdot u = 0$. Therefore, as abelian groups, the following splits.

$$0 \to \mu(\bar{\mathbb{Q}}) \to J(\bar{\mathbb{Q}}) \to \mathbb{Z}/p\mathbb{Z} \to 0. \tag{25}$$

   And it suffices to show the sequence (25) splits as Galois modules.

   By Lemma 4.2, we know the field $E := \mathbb{Q}(J(\bar{\mathbb{Q}}))$ is equal to $\mathbb{Q}(\sqrt[p]{1})$. This shows that the sequence (25) splits as Galois modules as well.

4. *In the category of finite p-groups over $\mathbb{Z}$, every extension of μ_p by a constant group Γ is trivial.*

doi:10.6342/NTU201701790

Given an exact sequence

$$0 \to \Gamma \to J \to \mu_p \to 0,$$

we shall show it splits.

Let u be a lift of a generator of μ_p in $J(\bar{\mathbb{Q}})$. Then $v = p \cdot u \in \Gamma(\bar{\mathbb{Q}})$. Also, for every $g \in G$, $w_g := {}^g u - \chi_1(g) \cdot u \in \Gamma(\bar{\mathbb{Q}})$ since μ_p is diagonalisable. Then ${}^g v = p \cdot ({}^g u) = p \cdot (w_g + \chi_1(g) \cdot u) = \chi_1(g) \cdot v + p \cdot w_g$. But Γ is constant, so ${}^g v = v$. This means $v = \chi_1(g) \cdot v + p \cdot w_g$. If we choose g such that $\chi_1(g) \neq 1$, then we see u can be choosen so that $p \cdot u = 0$. Therefore, as abelian groups, the following splits.

$$0 \to \Gamma(\bar{\mathbb{Q}}) \to J(\bar{\mathbb{Q}}) \to \mu_p(\bar{\mathbb{Q}}) \to 0. \tag{26}$$

It remains to show (26) splits as Galois modules. But again $\mathbb{Q}(J(\bar{\mathbb{Q}})) = \mathbb{Q}(\sqrt[p]{1})$ so (26) splits as Galois modules as well.

5. *The only simple objects in the category of finite p-groups over $\mathbb{Z}$ are $\mathbb{Z}/p\mathbb{Z}$ and μ_p.*

   The group $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on the p-th roots of unity. Let $\chi_1 : G \to \mathbb{F}_p^*$ be the character of this action.

   If J is a simple object, then the sub-object of J formed by the p-torsion is equal to J, so that J is killed by p. The action of G on $J(\bar{\mathbb{Q}})$ factors through $\mathrm{Gal}(E/\mathbb{Q})$, where $E = \mathbb{Q}(J(\bar{\mathbb{Q}}))$.

   Lemma 4.3 says $J(\bar{\mathbb{Q}})$ is a simple $\mathbb{F}_p[\mathrm{Gal}(E/\mathbb{Q})]$-module. Moreover, by Lemma 4.2, $E \subset \mathbb{Q}(\sqrt[p]{1})$. Since $\mathrm{Gal}(E/\mathbb{Q})$ is abelian, its simple module $J(\bar{\mathbb{Q}})$ is an 1-dimensional $\mathbb{F}_p$-vector space, on which the Galois action is given by χ_1^i for some $i \in \{0, \cdots, p-2\}$. By [10, Colloraire 3.4.4], we only have two cases to consider: $i = 0$ and $i = 1$. Now Lemma 4.3 implies that in the first case $J \cong \mathbb{Z}/p\mathbb{Z}$ and in the second case $J \cong \mu_p$.

6. *Every finite flat commutative group scheme J over $\mathbb{Z}$ which is killed by a power of p is a direct sum of constant and diagonalisable group schemes.*

doi:10.6342/NTU201701790

Let J be a finite commutative p-group over $\mathbb{Z}$, let $G = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and let

$$\begin{aligned} V_0 &= \{x \in J(\bar{\mathbb{Q}}) \mid gx = x,\ \forall g \in G\} \\ V_1 &= \{x \in J(\bar{\mathbb{Q}}) \mid gx = \chi_g(x),\ \forall g \in G\} \end{aligned}$$

Clearly $V_0 \oplus V_1 \hookrightarrow J(\bar{\mathbb{Q}})$ and we only have to show

$$J(\bar{\mathbb{Q}}) = V_0 \oplus V_1. \tag{27}$$

If equation (27) holds, we say J is admissible. We know that the category of admissible finite commutative p-groups over $\mathbb{Z}$ is stable under the sub-objects, quotients, and direct sums.

Suppose there exist finite non-admissible commutative p-groups over $\mathbb{Z}$, and choose J such that the order of $J(\bar{\mathbb{Q}})$ is minimal. We can choose a sub-group J' of J such that J/J' is simple. By our choice of J, $J' = J'_0 \oplus J'_1$ with J'_0 constant and J'_1 diagonalisable. If $J'_0 \neq 0$ and $J'_1 \neq 0$, then J/J'_0 and J/J'_1 are admissible, so that $J \hookrightarrow J/J'_0 \oplus J/J'_1$ is admissible.

If $J'_0 = 0$, then J' is diagonalisable, and J/J', being simple, is either μ_p or $\mathbb{Z}/p\mathbb{Z}$. In the first case, J is an extension of a diagonalisable by a diagonalisable, hence diagonalisable. In the second case we have an exact sequence

$$0 \to J' \to J \to \mathbb{Z}/p\mathbb{Z} \to 0. \tag{28}$$

By Step 4, this sequence splits, and J is admissible.

For the remaining case $J'_1 = 0$, $J'_2 = J'$, J' is constant. A parallel argument to the above finishes the proof.

□

doi:10.6342/NTU201701790

Appendices

1 Rank 2 groups

We classify free group schemes of rank 2 in this section.

Proposition 1.1. Every free group scheme Spec(A) of rank 2 is isomorphic to some $G_{a,b}$.

Proof. Consider the split exact sequence:

$$0 \to I_G \to R \times R = A \to R \to 0. \tag{29}$$

Here we identify $R \hookrightarrow A$ with $\{(r, r) \mid r \in R\}$. Now $(1, 1)$ and $(1, 0)$ forms a basis for the free module A, so $I_G \cong A/R \cong R$, and hence I_G is free of rank 1. This means $I_G = R \cdot x$ for some $x \in I_G$.

Then $x^2 = ax$ for some $a \in R$. Moreover, by Lemma 3.9,

$$c(x) = 1 \otimes x + x \otimes 1 + bx \otimes x,$$

for some $b \in R$.

From the relation $c(x)^2 = c(x^2) = a \cdot c(x)$ we see that

$$1 \otimes x^2 + x^2 \otimes 1 + b^2x^2 \otimes x^2 + 2x \otimes x + 2bx^2 \otimes x + 2bx \otimes x^2 = a(1 \otimes x + x \otimes 1 + bx \otimes x).$$

After rearranging, we find

$$(a^2b^2 + 2 + 4ab)(x \otimes x) = abx \otimes x.$$

From the freeness of A it follows that

$$(ab + 2)(ab + 1) = 0. \tag{30}$$

Write $i(x) = r + sx$ for some $r, s \in R$. By the axioms, $m \circ (id_A \otimes i) \circ c = e$. Apply

doi:10.6342/NTU201701790

this to x and obtain

$$m(1 \otimes (r + sx) + x \otimes 1 + bx \otimes (r + sx)) = 0.$$

Thus $r = 0$ and $s + 1 + br + abs = 0$, namely, $(ab + 1)s = -1$. Combined with (30), this yields $ab = -2$ and $s = 1$.

Therefore Spec$(A) \cong$ G$_{\text{a,b}}$. □

2 An increasing function

We show that a function is increasing in this section.

Lemma 2.1.

$$\prod_{k=1}^{n} \left(1 + \frac{1}{k}\right) = n + 1$$

Lemma 2.2.

$$(1 + \frac{1}{k})^k < e < (1 + \frac{1}{k})^{k+1}$$

Proof. Take log and get

$$k \ln(1 + \frac{1}{k}) < 1 < (k + 1) \ln(1 + \frac{1}{k}).$$

Now the inequality follows from the Taylor expansion of $\ln(1 + x)$. □

Lemma 2.3.

$$\frac{n^n}{n!} = \prod_{i=1}^{n-1} (1 + \frac{1}{i})^i.$$

Proof.

$$\begin{aligned} \tfrac{n^n}{n!} &= \textstyle\prod_{k=1}^{n-1} \left(1 + \frac{1}{k}\right)^n \cdot \prod_{i=1}^{n-1} \prod_{k=1}^{i} \left(1 + \frac{1}{k}\right)^{-1} \\ &= \textstyle\prod_{k=1}^{n-1} \left(1 + \frac{1}{k}\right)^n \cdot \prod_{i=1}^{n-1} \left(1 + \frac{1}{i}\right)^{-(n-i)} \\ &= \textstyle\prod_{i=1}^{n-1} \left(1 + \frac{1}{i}\right)^i \end{aligned}$$

□

doi:10.6342/NTU201701790

Theorem 2.1. *Define* $f(n) = \frac{n}{(n!)^{\frac{1}{n}}}$ *for* $n = 1, 2, \cdots$. *Then*

$$f(n) < f(n+1),\ \forall\, n = 1, 2, \cdots .$$

Proof.

When raised to the $n(n+1)$-th power, this inequality is transformed into

$$\frac{n^{n(n+1)}}{(n!)^{n+1}} < \frac{(n+1)^{n(n+1)}}{((n+1)!)^n}.$$

After rearranging, this becomes

$$\frac{(n+1)^n}{n!} < (\frac{n+1}{n})^{n(n+1)}.$$

Namely, $\frac{n^n}{n!} \cdot (\frac{n+1}{n})^n < (\frac{n+1}{n})^{n(n+1)}$. Hence it is equivalent with

$$\frac{n^n}{n!} < (\frac{n+1}{n})^{n^2}. \tag{31}$$

By Lemma 2.3, the L.H.S. of equation (31) is $\prod_{k=1}^{n-1}(1+\frac{1}{k})^k$.

By Lemma 2.2, we have

$$(1+\frac{1}{k})^k < e < (1+\frac{1}{n})^{n+1},\ \forall k = 1, 2, \cdots .$$

Therefore

$$\prod_{k=1}^{n-1}(1+\frac{1}{k})^k < (1+\frac{1}{n})^{(n+1)(n-1)} < (1+\frac{1}{n})^{n^2}. \qquad \square$$

doi:10.6342/NTU201701790

doi:10.6342/NTU201701790

Bibliography

[1] J. Cassels and A. F. eds. *Algebraic Number Theory*. Academic Press, 1967.

[2] F. D. Y. Diaz. *Tables minorant la racine n-ième du discriminant d'un corps de degré n*. Publications mathématiques d'Orsay, 1980.

[3] J. M. Fontaine. Il n'y a pas de variété abélienne sur $\mathbb{Z}$. *Inventiones mathematicæ*, pages 515–538, 1985.

[4] A. Grothendieck. *Éléments de géométrie algébrique: IV.Étude locale des schémas et des morphismes de schémas*. Publications mathématiques de l'I.H.É.S., 1964.

[5] R. Hartshorne. *Algebraix Geometry*. Springer-Verlag, 1977.

[6] J. Milne. *Étale Cohomology*. Princeton University Press, 1980.

[7] J. Milne. Abelian varieties. In G. Cornell and J. H. Silverman, editors, *Arithmetic Geometry*, chapter 5, pages 103–150. Springer-Verlag, 1986.

[8] D. Mumford. *Abelian Varieties*. Oxford University Press, 1985.

[9] M. Raynaud. Passage au quotient par une relation d'équivalence plate. In T.A.Springer, editor, *Proceedings of a Conference on Local Fields*, pages 78–85. Springer-Verlag, 1966.

[10] M. Raynaud. Schémas en groupes de type (p,...,p). *Bulletin de la S.M.F.*, pages 241–280, 1974.

[11] J. P. Serre. *Local Fields*. Springer-Verlag, 1979.

doi:10.6342/NTU201701790

[12] L. C. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag, 1980.

[13] W. C. Waterhouse. *Introduction to affine group schemes*. Springer-Verlag, 1979.

doi:10.6342/NTU201701790