Journal of Number Theory 260 (2024) 191–195

Contents lists available at ScienceDirect

Journal of Number Theory

journal homepage: www.elsevier.com/locate/jnt

General Section

Finite flat group schemes over **Z** killed by 19

Lassina Dembélé [a,*], René Schoof [b,1,*]

[a] *Department of Mathematics, King's College London, Strand, London WC2R 2LS, UK*
[b] *Dipartimento di Matematica, 2[a] Università di Roma "Tor Vergata", I-00133 Roma, Italy*

ARTICLE INFO

Article history:
Received 11 September 2023
Received in revised form 20 February 2024
Accepted 24 February 2024
Available online 18 March 2024
Communicated by L. Smajlovic

Keywords:
Finite group schemes
Number fields

ABSTRACT

Since simple commutative finite flat group schemes over **Z** are killed by a prime number p, their order is a power of p. Abraškin and Fontaine have both shown that for primes $p \leqslant 17$ the only simple p-power order group schemes are μ_p and $\mathbf{Z}/p\mathbf{Z}$. We extend their result to $p = 19$.

1. Introduction

A finite flat commutative group scheme G over **Z** is simple, if and only if its set of points $G(\overline{\mathbf{Q}})$ is an irreducible Galois module. Therefore G is annihilated by some prime number p and G is a p-group scheme in the sense that its order is a power of p. For each prime p the constant group scheme $\mathbf{Z}/p\mathbf{Z}$ and its Cartier dual μ_p are simple p-group schemes over **Z**.

* Corresponding authors.
E-mail addresses: lassina.dembele@kcl.ac.uk (L. Dembélé), schoof@mat.uniroma2.it (R. Schoof).

[1] The second author acknowledges GNSAGA and the MIUR Excellence Department Project awarded to the Department of Mathematics, University of Rome Tor Vergata, CUP E83C18000100006.

https://doi.org/10.1016/j.jnt.2024.02.008
0022-314X/

Tate [9] asked whether these are the only simple commutative finite flat group schemes over $\mathbf{Z}$. Abraškin [1] and Fontaine [3] both showed that this is true for primes $p \leqslant 17$. In this paper we extend their result slightly.

Theorem 1.1. *For every prime $p \leqslant 19$ the only simple finite flat commutative group schemes over $\mathbf{Z}$ of p-power order are $\mathbf{Z}/p\mathbf{Z}$ and μ_p.*

Under assumption of the Generalized Riemann Hypothesis (GRH), our result can be extended further. In a separate paper [2] we show under GRH that for $p \leqslant 37$ the only simple p-group schemes over $\mathbf{Z}$ are $\mathbf{Z}/p\mathbf{Z}$ and μ_p.

The strategy of the proof of Theorem 1.1 is the one followed by Abraškin and Fontaine. It is based on the fact that the field generated by the points of a finite flat commutative group scheme G over $\mathbf{Z}$ is a finite Galois extension $\mathbf{Q} \subset F$ which has very little ramification. More precisely, if G is killed by a prime p, the field F has the following two properties, the second of which follows from the work of Abraškin [1] and Fontaine [3]:

- F is unramified outside p and infinity;
- $u_{F_\mathfrak{p}/\mathbf{Q}_p} \leqslant 1 + \frac{1}{p-1}$ for every prime $\mathfrak{p}$ of F lying over p.

Here the invariant $u_{F_\mathfrak{p}/\mathbf{Q}_p}$ depends only on the structure of the group scheme G over $\mathbf{Z}_p$. It is defined as follows. The ring of integers of the local field $F_\mathfrak{p}$ has the form $\mathbf{Z}_p[\alpha]$ for some α. Let $i_\mathfrak{p} = \max_\sigma v(\sigma(\alpha) - \alpha)$. Here σ runs over the non-trivial automorphisms in $\mathrm{Gal}(F_\mathfrak{p}/\mathbf{Q}_p)$. Let $\mathfrak{d}_\mathfrak{p}$ denote the different of $F_\mathfrak{p}$ over $\mathbf{Q}_p$. Then we put

$$u_{F_\mathfrak{p}/\mathbf{Q}_p} = i_\mathfrak{p} + v(\mathfrak{d}_\mathfrak{p}).$$

The valuation v is normalized by setting $v(p) = 1$. It follows that both $i_\mathfrak{p}$ and $v(\mathfrak{d}_\mathfrak{p})$ are in $\frac{1}{e_\mathfrak{p}}\mathbf{Z}$, where $e_\mathfrak{p}$ is the ramification index of $F_\mathfrak{p}$ over $\mathbf{Q}_p$. By [3, sect. 3.3] the root discriminant δ_F of the number field F is equal to $p^{v(\mathfrak{d}_\mathfrak{p})}$ for any prime $\mathfrak{p}$ lying over p. Therefore it satisfies

$$\delta_F < p^{1+\frac{1}{p-1}}.$$

The invariant $u_{F_\mathfrak{p}/\mathbf{Q}_p}$ can also be characterized as follows. The i-th ramification subgroup of $\mathrm{Gal}(F_\mathfrak{p}/\mathbf{Q}_p)$ in the upper numbering is trivial for $i > u_{F_\mathfrak{p}/\mathbf{Q}_p}$ and $u_{F_\mathfrak{p}/\mathbf{Q}_p}$ is minimal with respect to this property.

For a given prime p the *Abraškin-Fontaine field* K is the maximal extension $\mathbf{Q} \subset K \subset \overline{\mathbf{Q}}$ for which

- K is unramified outside p and infinity;
- $u_{K_\mathfrak{p}/\mathbf{Q}_p} \leqslant 1 + \frac{1}{p-1}$ for any prime $\mathfrak{p}$ of K lying over p.

The field K is Galois over $\mathbf{Q}$. For every finite flat commutative group scheme G that is killed by p, the subfield $F \subset \overline{\mathbf{Q}}$ generated by its points is contained in K. It is easy to see that the invariant $u_{\mathbf{Q}_p(\zeta_p)/\mathbf{Q}_p}$ is equal to 1. It follows that K contains the cyclotomic field $\mathbf{Q}(\zeta_p)$. Alternatively, one may observe that $\mathbf{Q}(\zeta_p)$ is generated by the points of the group scheme μ_p.

In section 3 we show that for $p = 19$ the Abraškin-Fontaine field is *equal* to $\mathbf{Q}(\zeta_{19})$. Theorems of Oort and Tate [8] then imply that the group scheme G is isomorphic to $\mathbf{Z}/19\mathbf{Z}$ or μ_{19} and Theorem 1.1 follows.

2. Two lemmas

The following two lemmas play a role in the proof of the main result.

Lemma 2.1. *Let Γ be a finite non-commutative simple group of order at most 500000. If $\#\Gamma$ is divisible by 19, then Γ is isomorphic to $\mathrm{PSL}_2(\mathbf{F}_{19})$, $\mathrm{PSL}_2(\mathbf{F}_{37})$ or Janko's sporadic simple group J_1 of orders 3420, 25308 and 175560 respectively. Each of these groups has the property that its 19-Sylow subgroup has order 19 and is equal to its own centralizer.*

Proof. Inspection of the orders of the simple groups order < 500000 shows that Γ is isomorphic to $\mathrm{PSL}_2(\mathbf{F}_{19})$, $\mathrm{PSL}_2(\mathbf{F}_{37})$ or to Janko's sporadic group J_1. We do not need the classification of finite simple groups for this. It already follows from an older table [4]. For $\mathrm{PSL}_2(\mathbf{F}_{19})$ and $\mathrm{PSL}_2(\mathbf{F}_{37})$ it is easy to check that the 19-Sylow subgroup has order 19 and is equal to its own centralizer. For the group J_1 the result follows from the fact that the normalizer of its 19-Sylow subgroup is a Frobenius group of order 114. See [5, Sect. I]. □

Lemma 2.2. *Let p be a prime and let E be a Galois extension of $\mathbf{Q}_p$ containing a p-th root of unity. Let $P \subset \mathrm{Gal}(E/\mathbf{Q}_p)$ be the wild ramification subgroup. If $\#P = p$ and the centralizer of P in $\mathrm{Gal}(E/\mathbf{Q}_p)$ is equal to P itself, then the valuation of the different $\mathfrak{d}_E$ is given by*

$$v(\mathfrak{d}_E) = \frac{p-2}{p-1} + \frac{a}{p}, \qquad \text{for some integer } a \geqslant 2.$$

Proof. Since P is normal in $\Gamma = \mathrm{Gal}(E/\mathbf{Q}_p)$ and equal to its own centralizer, conjugation gives rise to an exact sequence

$$1 \longrightarrow P \longrightarrow \Gamma \longrightarrow \mathrm{Aut}(P).$$

It follows that $[\Gamma : P] \leqslant p-1$. Since $\mathbf{Q}_p(\zeta_p)$ is contained in the fixed field of P, we actually have equality. It follows that E is a totally ramified cyclic degree p extension of $\mathbf{Q}_p(\zeta_p)$. Let π be a uniformizer of $\mathbf{Q}_p(\zeta_p)$. Then the conductor of E is π^a for some $a \geqslant 2$. By the conductor discriminant formula the discriminant of E over $\mathbf{Q}_p(\zeta_p)$ is $\pi^{a(p-1)}$. So

the normalized valuation of the different of E over $\mathbf{Q}_p(\zeta_p)$ is $\frac{a}{p}$. Since the normalized valuation of the different of $\mathbf{Q}_p(\zeta_p)$ over $\mathbf{Q}_p$ is $\frac{p-2}{p-1}$, the result follows. □

3. Proof of the theorem

In this section we prove the main result of this note. Since Fontaine and Abraškin took care of the primes $p \leqslant 17$, we may restrict our attention to $p = 19$.

Proof. Let G be a finite flat commutative simple group scheme over $\mathbf{Z}$ that is killed by 19. The points of G are defined over the Abraškin- Fontaine field K. The root discriminant δ_K of K satisfies

$$\delta_K < 19^{1+\frac{1}{19-1}} = 22.3766\ldots$$

This is just a tiny bit smaller than the asymptotic value $4\pi e^{\gamma} = 22.38161\ldots$ of Odlyzko's function. The inequality of [7, Formule (22)] leads to the following upper bound for $[K : \mathbf{Q}]$.

$$[K : \mathbf{Q}] < \left(\frac{8.6}{\gamma + \log 4\pi - \frac{19}{18}\log 19}\right)^{3/2} < 76766981.$$

The field K contains $\mathbf{Q}(\zeta_{19})$. Suppose that K is strictly larger. Then the Jordan-Hölder theorem implies that there is a subfield $\mathbf{Q}(\zeta_{19}) \subset K' \subset K$ for which $\Gamma = \mathrm{Gal}(K'/\mathbf{Q}(\zeta_{19}))$ is a simple group. Since the index $[K' : \mathbf{Q}(\zeta_{19})]$ is at most $76766981/18 < 426499$, we have

$$\#\Gamma < 426499.$$

Since any abelian extension L of $\mathbf{Q}(\zeta_{19})$ inside K satisfies $\delta_L < 19^{19/18}$, its conductor is at most π^2. Here π denotes the unique prime of $\mathbf{Q}(\zeta_{19})$ lying over 19. However, by [10, Ch. 11] the class number of $\mathbf{Q}(\zeta_{19})$ is 1. Moreover, the cyclotomic unit $\eta = \zeta_{19} + 1$ is congruent to the primitive root 2 modulo π and we have

$$\eta^{18} = (\pi + 2)^{18} \equiv 1 - \frac{1}{2}\pi \not\equiv 1 \mod \pi^2.$$

Class field theory implies therefore that the ray class group of $\mathbf{Q}(\zeta_{19})$ of conductor π^2 is equal to $\mathbf{Q}(\zeta_{19})$ itself. It follows that the only abelian extension L of $\mathbf{Q}(\zeta_{19})$ inside K is $\mathbf{Q}(\zeta_{19})$ itself, and hence that Γ is a *non-commutative* simple group.

If K' is at most tamely ramified at the prime over 19, then its root discriminant satisfies $\delta_{K'} < 19$. Odlyzko's discriminant bounds [6, Table 2] then imply the bound $[K' : \mathbf{Q}] < 280$. It follows that $[K' : \mathbf{Q}(\zeta_{19})]$ is at most $280/18 < 16$. Since non-commutative simple groups of order at most 16 do not exist, this is impossible. Therefore

K' is wildly ramified over $\mathbf{Q}(\zeta_{19})$ and $\#\Gamma$ is divisible by 19. Lemma 2.1 implies then that Γ is isomorphic to $\mathrm{PSL}_2(\mathbf{F}_{19})$, $\mathrm{PSL}_2(\mathbf{F}_{37})$ or to Janko's sporadic group J_1.

Next we observe that K' is a Galois extension of $\mathbf{Q}$. Indeed, if it were not, then there would be an automorphism $\sigma \in \mathrm{Gal}(K/\mathbf{Q})$ for which $\sigma\Gamma\sigma^{-1} \neq \Gamma$. This means that $\Gamma \cdot \sigma\Gamma\sigma^{-1}$ is equal to $\mathrm{Gal}(K/\mathbf{Q}(\zeta_{19}))$, so that $\Gamma \cap \sigma\Gamma\sigma^{-1}$ has index $\#\Gamma^2 \geqslant 3420^2$ in $\mathrm{Gal}(K/\mathbf{Q}(\zeta_{19}))$. However, this is impossible since we have $\mathrm{Gal}(K/\mathbf{Q}(\zeta_{19})) < 426499$.

Since K' is a subfield of K, its root discriminant $\delta_{K'}$ satisfies $\delta_{K'} \leqslant \delta_K < 19^{19/18}$. An application of Lemma 2.2 to the completion at a prime over 19 of the extension K' of $\mathbf{Q}$ shows that the root discriminant $\delta_{K'}$ is of the form $19^{17/18+a/19}$ for some integer $a \geqslant 2$. Since we have $\frac{17}{18} + \frac{a}{19} < \frac{19}{18}$, this implies $a = 2$ and hence

$$\delta_{K'} = 19^{17/18+2/19} = 21.9946\ldots$$

This estimate is a little better than the Abraškin-Fontaine bound $19^{19/18} = 22.3766\ldots$. Odlyzko's discriminant bounds [6, Table 2] therefore imply the somewhat sharper inequality

$$[K' : \mathbf{Q}] < 8862,$$

contradicting the fact that $[K' : \mathbf{Q}]$ is at least $18\#\Gamma \geqslant 18 \cdot 3420$. It follows that K is equal to $\mathbf{Q}(\zeta_{19})$. Theorems of Oort and Tate [8] imply then that G is isomorphic to $\mathbf{Z}/19\mathbf{Z}$ or μ_{19}. □

Data availability

Data will be made available on request.

References

[1] V.A. Abraškin, Galois moduli of period p group schemes over a ring of Witt vectors, Izv. Akad. Nauk SSSR, Ser. Mat. 51 (1987). English translation in Math. USSR, Izv. 31 (1988) 1–46.
[2] L. Dembélé, R. Schoof, GRH and finite flat group schemes over $\mathbf{Z}$, J. Théor. Nr. Bordx. (2024), in preparation.
[3] J.-M. Fontaine, Il n'y a pas de variété abélienne sur $\mathbf{Z}$, Invent. Math. 81 (1985) 515–538.
[4] M. Hall Jr., Simple groups of order less than one million, J. Algebra 20 (1972) 98–102.
[5] Z. Janko, A new finite simple group with abelian Sylow 2-subgroups and its characterization, J. Algebra 3 (1966) 147–186.
[6] A. Odlyzko, Discriminant bounds, http://www.dtc.umn.edu/~odlyzko/unpublished/index.html, November 29, 1976.
[7] G. Poitou, Minorations de discriminants (d'après A.M. Odlyzko), in: Séminaire Bourbaki, Vol. 1975/76, Exp. No. 479, in: Lecture Notes in Math., vol. 567, Springer-Verlag, 1977, pp. 136–153.
[8] J.T. Tate, F. Oort, Group schemes of prime order, Ann. Sci. Éc. Norm. Supér. 3 (1970) 1–21.
[9] J.T. Tate, p-divisible groups, in: Conference on Local Fields, Driebergen, Springer, 1967.
[10] L.C. Washington, Introduction to Cyclotomic Fields, 2nd ed., GTM, vol. 83, Springer-Verlag, 1997.