J. Group Theory **26** (2023), 1143–1155
DOI 10.1515/jgth-2022-0110

# Algebraic groups over finite fields: Connections between subgroups and isogenies

Davide Sclosa*

Communicated by Timothy C. Burness

**Abstract.** Let $G$ be a linear algebraic group defined over a finite field $\mathbb{F}_q$. We present several connections between the isogenies of $G$ and the finite groups of rational points $(G(\mathbb{F}_{q^n}))_{n\geq 1}$. We show that an isogeny $\phi\colon G' \to G$ over $\mathbb{F}_q$ gives rise to a subgroup of fixed index in $G(\mathbb{F}_{q^n})$ for infinitely many $n$. Conversely, we show that if $G$ is reductive, the existence of a subgroup $H_n$ of fixed index $k$ for infinitely many $n$ implies the existence of an isogeny of order $k$. In particular, we show that the infinite sequence $H_n$ is covered by a finite number of isogenies. This result applies to classical groups $\mathrm{GL}_m$, $\mathrm{SL}_m$, $\mathrm{SO}_m$, $\mathrm{SU}_m$, $\mathrm{Sp}_{2m}$ and can be extended to non-reductive groups if $k$ is prime to the characteristic. As a special case, we see that if $G$ is simply connected, the minimal indices of proper subgroups of $G(\mathbb{F}_{q^n})$ diverge to infinity. Similar results are investigated regarding the sequence $(G(\mathbb{F}_p))_p$ by varying the characteristic $p$.

## 1 Introduction

Linear algebraic groups are groups of matrices defined by polynomial equations. We adopt the classical notion of algebraic group as a group of rational points over the algebraic closure, following the language of A. Borel, J. Tits and C. Chevalley [2–4]. Throughout the article, we clarify where the modern scheme-theoretic approach [9, 10, 14] differs. We focus on linear algebraic groups over finite fields. They are closely related to the classification of finite simple groups [6].

Before presenting the main results, we introduce some notation. Let $\mathbb{F}_q$ be a finite field with $q$ elements and characteristic $p$. We denote by $\overline{\mathbb{F}_q}$ an algebraic closure. For every $n \geq 1$, we consider the finite extension $\mathbb{F}_{q^n} \subseteq \overline{\mathbb{F}_q}$. A *linear algebraic group* $G$ defined over $\mathbb{F}_q$ is a closed subgroup of $\mathrm{GL}_m(\overline{\mathbb{F}_q})$ defined by polynomial equations with coefficients in $\mathbb{F}_q$. We always assume that $G$ is connected. The *group of* $\mathbb{F}_{q^n}$*-rational points* $G(\mathbb{F}_{q^n})$ is the subgroup of $G$ whose elements have entries in $\mathbb{F}_{q^n}$. The Frobenius automorphism $x \mapsto x^{q^n}$ of $\mathbb{F}_{q^n}$ extends naturally to a group automorphism $g \mapsto \sigma_{q^n}(g)$ of $G$ via the action on the matrix entries. The group of rational points $G(\mathbb{F}_{q^n})$ is exactly the fixed subgroup of $\sigma_{q^n}$. An *isogeny* between connected linear algebraic groups is a surjective homomorphism $\phi\colon G' \to G$ with finite kernel. The *order* of $\phi$ is the cardinality of the kernel $|\operatorname{Ker}\phi|$.

In this paper, we present several connections between the sequence of finite groups $(G(\mathbb{F}_{q^n}))_{n\geq 1}$ and the isogenies $\phi\colon G' \to G$. In Theorem 2.2, we show that if $\phi$ has order $k$, then for infinitely many $n$, the group $G(\mathbb{F}_{q^n})$ contains a subgroup of index $k$. More surprisingly, in Theorem 3.6 and Theorem 4.1, we show that, under suitable hypotheses, if for infinitely many $n$, the group $G(\mathbb{F}_{q^n})$ contains a subgroup of index $k$, then there exist a group $G'$ and an isogeny $\phi\colon G' \to G$ of order $k$. In particular, we show that finitely many isogenies are responsible for the infinite sequence of subgroups of index $k$.

These results constrain the asymptotic behavior of subgroups: the set of positive integers $n$ for which $G(\mathbb{F}_{q^n})$ contains a subgroup of index $k$ is either finite or contains an arithmetic progression (Corollary 4.2).

As a corollary, we obtain the following: if $G$ is semisimple, simply connected and $k > 1$, then for every $n$ large enough, the group $G(\mathbb{F}_{q^n})$ contains no subgroup of index $k$ (Corollary 3.7). Note that, while our result is purely asymptotic, the maximal subgroups of simple groups of Lie type have actually been classified [7].

In the last section, instead of $(G(\mathbb{F}_{q^n}))_{n\geq 1}$, we consider the sequence $(G(\mathbb{F}_p))_p$ by varying the characteristic. In analogy to Corollary 3.7, we show that if $G$ is semisimple, simply connected and $k > 1$, then for every prime $p$ large enough, the group $G(\mathbb{F}_p)$ contains no subgroup of index $k$ (Theorem 5.1).

## 2 From isogenies to subgroups

In this section, we show how one rational isogeny gives rise to an infinite family of subgroups of fixed index.

Let $G'$, $G$ be connected linear algebraic groups defined over $\mathbb{F}_q$. Let $\phi\colon G' \to G$ be an isogeny defined over $\mathbb{F}_q$. For every $n$, the isogeny $\phi$ restricts to a homomorphism of finite groups $\phi\colon G'(\mathbb{F}_{q^n}) \to G(\mathbb{F}_{q^n})$. Note the abuse of notation.

The kernel of $\phi\colon G'(\mathbb{F}_{q^n}) \to G(\mathbb{F}_{q^n})$ coincides with the group of $\mathbb{F}_{q^n}$-rational points of the kernel of $\phi\colon G' \to G$. Thus the notation $\operatorname{Ker}\phi(\mathbb{F}_{q^n})$ is unambiguous.

The same cannot be said of the image since the group $\phi(G'(\mathbb{F}_{q^n}))$ and the group $\phi(G')(\mathbb{F}_{q^n}) = G(\mathbb{F}_{q^n})$ may be different. Indeed, although $\phi$ is surjective at the level of algebraic closure, it may not be surjective at the level of rational points.

**Lemma 2.1.** *The image $\phi(G'(\mathbb{F}_{q^n}))$ has index $|\operatorname{Ker}\phi(\mathbb{F}_{q^n})|$ in $G(\mathbb{F}_{q^n})$.*

*Proof.* Since $G'$ and $G$ are isogenous over $\mathbb{F}_q$, in particular, they are isogenous over $\mathbb{F}_{q^n}$. Two groups isogenous over $\mathbb{F}_{q^n}$ have the same number of $\mathbb{F}_{q^n}$-rational points [1, Proposition 16.8]. Therefore, the cardinality of the kernel is equal to the index of the image. □

The quotient between two groups of rational points may be different from the group of rational points of the quotient. This is caused by the discreteness of the kernel. Indeed, if $N$ is a connected normal subgroup of $G$, then $(G/N)(\mathbb{F}_{q^n})$ is equal to $G(\mathbb{F}_{q^n})/N(\mathbb{F}_{q^n})$; see [1, Corollary 16.5 (ii)].

From Lemma 2.1, we easily obtain the following theorem.

**Theorem 2.2.** *Let $G'$ and $G$ be two connected linear algebraic groups defined over $\mathbb{F}_q$. Let $\phi\colon G' \to G$ be an isogeny of order $k$ defined over $\mathbb{F}_q$. Then, for infinitely many $n$, the group of rational points $G(\mathbb{F}_{q^n})$ has a subgroup of index $k$. The set of integers for which this happens contains an arithmetic progression.*

*Proof.* Since $\operatorname{Ker}\phi$ is finite, we have $\operatorname{Ker}\phi = \operatorname{Ker}\phi(\mathbb{F}_{q^m})$ for some $m$. It follows that $\operatorname{Ker}\phi = \operatorname{Ker}\phi(\mathbb{F}_{q^n})$ for every multiple $n$ of $m$. By Lemma 2.1, the group $G(\mathbb{F}_{q^n})$ has a subgroup of index $k$ for every $n$ multiple of $m$. □

## 3 From subgroups to isogenies: Reductive groups

In this section, we show how the existence of infinitely many subgroups of fixed index $k$ implies the existence of an isogeny of order $k$, in the case of reductive groups.

Let $\phi\colon G' \to G$ be an isogeny defined over $\mathbb{F}_q$. Since $G'$ is connected and $\operatorname{Ker}\phi$ is discrete, the action of $G$ on $\operatorname{Ker}\phi$ by conjugation is trivial. Therefore, the kernel $\operatorname{Ker}\phi$ is a central subgroup of $G'$. Note, however, that not all isogenies are central in the scheme-theoretic sense.

We already observed that, although

$$1 \to \operatorname{Ker}\phi \to G' \to G \to 1$$

is exact, the sequence

$$1 \to \operatorname{Ker}\phi(\mathbb{F}_{q^n}) \to G'(\mathbb{F}_{q^n}) \to G(\mathbb{F}_{q^n}) \to 1$$

may not be exact. The cokernel $G(\mathbb{F}_{q^n})/\phi(G'(\mathbb{F}_{q^n}))$ measures how far this sequence is from being exact. Our next goal is understanding the cokernel.

To this end, we recall a standard tool in the study of algebraic groups over finite fields. Fix $n$. The *Lang map* $\lambda_{q^n}$ is defined by

$$\lambda_{q^n}\colon G' \to G', \quad y \mapsto y^{-1}\sigma_{q^n}(y).$$

Lang's Theorem tells us that this map is surjective [1, Corollary 16.4].

Note that, since $\phi$ commutes with $\sigma_{q^n}$, we have $\lambda_{q^n}(\operatorname{Ker}\phi) \subseteq \operatorname{Ker}\phi$. Since $\operatorname{Ker}\phi$ is central, in particular commutative, it follows that $\lambda_{q^n}(\operatorname{Ker}\phi)$ is a normal subgroup of $\operatorname{Ker}\phi$. Therefore, the group quotient $\operatorname{Ker}\phi/\lambda_{q^n}(\operatorname{Ker}\phi)$ is well defined. It turns out that it is isomorphic to the cokernel.

**Lemma 3.1.** *The following group isomorphism holds:*

$$\frac{G(\mathbb{F}_{q^n})}{\phi(G'(\mathbb{F}_{q^n}))} \cong \frac{\operatorname{Ker}\phi}{\lambda_{q^n}(\operatorname{Ker}\phi)}.$$

*In particular, $\phi(G'(\mathbb{F}_{q^n}))$ is a normal subgroup of $G(\mathbb{F}_{q^n})$.*

*Proof.* Take $x \in G(\mathbb{F}_{q^n})$. Since $\phi\colon G' \to G$ is surjective, there is $y \in G'$ such that $\phi(y) = x$. Since $\phi$ commutes with $\sigma_{q^n}$ and $\sigma_{q^n}(x) = x$, we have

$$y^{-1}\sigma_{q^n}(y) \in \operatorname{Ker}\phi.$$

Consider the map

$$\begin{aligned} \mu_{q^n}\colon G(\mathbb{F}_{q^n}) &\to \frac{\operatorname{Ker}\phi}{\lambda_{q^n}(\operatorname{Ker}\phi)}, \\ x &\mapsto \lambda_{q^n}(y)\lambda_{q^n}(\operatorname{Ker}\phi). \end{aligned}$$

First of all, we need to check that $\mu_{q^n}$ is well defined. If a different $y$ is chosen, say $z \in G'$ such that $\phi(z) = x$, then $yz^{-1} \in \operatorname{Ker}\phi$, and so

$$(yz^{-1})^{-1}\sigma_{q^n}(yz^{-1}) \in \lambda_{q^n}(\operatorname{Ker}\phi),$$

which is equivalent to $(z^{-1}\sigma_{q^n}(z))^{-1}y^{-1}\sigma_{q^n}(y) \in \lambda_{q^n}(\operatorname{Ker}\phi)$ since $\lambda_{q^n}(\operatorname{Ker}\phi)$ is central.

Now we prove that $\mu_{q^n}$ is surjective. Let $a \in \operatorname{Ker}\phi$. By Lang's Theorem, there is $y \in G'$ such that $y^{-1}\sigma_{q^n}(y) = a$. Let $x = \phi(y)$. Since $\phi(y^{-1}\sigma_{q^n}(y)) = 1$, we have $\sigma_{q^n}(x) = x$, and so $x \in G(\mathbb{F}_{q^n})$. By definition, $x$ is mapped to $y^{-1}\sigma_{q^n}(y)$ by $\mu_{q^n}$, which is equal to $a$.

Next, we prove that $\mu_{q^n}$ is a homomorphism. Take any $x, w \in G(\mathbb{F}_{q^n})$; let $\phi(y) = x$ and $\phi(z) = w$. We need to show that $(yz)^{-1}\sigma_{q^n}(yz)$ is equal to

$$y^{-1}\sigma_{q^n}(y)z^{-1}\sigma_{q^n}(z).$$

This is the same as

$$z^{-1}y^{-1}\sigma_{q^n}(y) = y^{-1}\sigma_{q^n}(y)z^{-1},$$

which holds since $y^{-1}\sigma_{q^n}(y) \in \operatorname{Ker}\phi$ is central.

Finally, we prove that the kernel of $\mu_{q^n}$ is $\phi(G'(\mathbb{F}_{q^n}))$. Let $x = \phi(y)$ be an element of $G(\mathbb{F}_{q^n})$ such that $y^{-1}\sigma_{q^n}(y)$ belongs to $\lambda_{q^n}(\operatorname{Ker}\phi)$. Then

$$y^{-1}\sigma_{q^n}(y) = a^{-1}\sigma_{q^n}(a)$$

for some $a \in \operatorname{Ker}\phi$. Since $\operatorname{Ker}\phi$ is central and $y^{-1}\sigma_{q^n}(y) = a^{-1}\sigma_{q^n}(a)$, it follows that

$$\sigma_{q^n}(a^{-1}y) = \sigma_{q^n}(y)\sigma_{q^n}(a)^{-1} = a^{-1}y,$$

and so $a^{-1}y \in G'(\mathbb{F}_{q^n})$. Therefore, $x = \phi(y) = \phi(a^{-1}y)$ belongs to $\phi(G'(\mathbb{F}_{q^n}))$. $\square$

Let $H$ be a subgroup of $G(\mathbb{F}_{q^n})$. We say that an isogeny $\phi\colon G' \to G$ *reaches* $H$ if it is defined over $\mathbb{F}_{q^n}$ and $\phi(G'(\mathbb{F}_{q^n})) = H$. In the following lemma, which serves as a bootstrap, we show how to construct an isogeny reaching $H$ from an isogeny whose image is contained in $H$. The idea is simple: in light of Lemma 2.1, in order to make the image larger, we need to make the quotient smaller.

Note that, since $\mu_{q^n}$ is an isomorphism between the group $G(\mathbb{F}_{q^n})/\phi(G'(\mathbb{F}_{q^n}))$ and the group $\operatorname{Ker}\phi/\lambda_{q^n}(\operatorname{Ker}\phi)$, there is a bijection between the subgroups $H$ of $G(\mathbb{F}_{q^n})$ containing $\varphi(G'(\mathbb{F}_{q^n}))$ as a sugroup, and the subgroups $K$ of $\ker\varphi$ containing $\lambda_{q^n}(\ker\varphi)$ as a subgroup.

**Lemma 3.2.** *Let $G'$, $G$ and $\phi\colon G' \to G$ be two connected linear algebraic groups and an isogeny defined over $\mathbb{F}_{q^n}$. Let $H$ be a subgroup of $G(\mathbb{F}_{q^n})$ containing $\phi(G'(\mathbb{F}_{q^n}))$. Let $K$ be the subgroup of* $\operatorname{Ker}\phi$ *containing* $\lambda_{q^n}(\operatorname{Ker}\phi)$ *and satisfying*

$$\mu_{q^n}(H/\phi(G'(\mathbb{F}_{q^n}))) = K/\lambda_{q^n}(\operatorname{Ker}\phi).$$

*Then $G'' = G'/K$ is a connected linear algebraic group defined over $\mathbb{F}_{q^n}$; the induced isogeny $\phi''\colon G'' \to G$ reaches $H$.*

*Proof.* The group $K$ is defined over $\mathbb{F}_{q^n}$: since $\lambda_{q^n}(\operatorname{Ker}\phi) \subseteq K \subseteq \operatorname{Ker}\phi$, in particular, $\lambda_{q^n}(K) \subseteq K$, and so $K$ is $\sigma_{q^n}$-invariant. Therefore, the quotient group $G'' = G'/K$ is defined over $\mathbb{F}_{q^n}$. Its group of $\mathbb{F}_{q^n}$-rational points is

$$\begin{aligned} G''(\mathbb{F}_{q^n}) &= (G'/K)(\mathbb{F}_{q^n}) \\ &= \{yK : y \in G',\ \sigma_{q^n}(yK) = yK\} \\ &= \{yK : y \in G',\ \lambda_{q^n}(y) \in K\}. \end{aligned}$$

Since $K \subseteq \operatorname{Ker}\phi$ holds, the isogeny $\phi\colon G' \to G$ induces a well defined isogeny $\phi''\colon G'' \to G$. We claim that the image

$$\phi''(G''(\mathbb{F}_{q^n})) = \{\phi(y) : y \in G',\ \lambda_{q^n}(y) \in K\} \tag{3.1}$$

is equal to $H$, completing the proof.

Let $x \in H$. Then $x = \phi(y)$ for some $y \in G'$. Since $x \in G(\mathbb{F}_{q^n})$, then

$$\lambda_{q^n}(y)\lambda_{q^n}(\operatorname{Ker}\phi) = \mu_{q^n}(x) \in K/\lambda_{q^n}(\operatorname{Ker}\phi).$$

By hypothesis, $K$ contains $\lambda_{q^n}(\operatorname{Ker}\phi)$, and therefore, $\lambda_{q^n}(y) \in K$. This proves that $x$ is an element of (3.1).

Conversely, let $x$ be an element of (3.1). Then $x = \phi(y)$ for some $y \in G'$ satisfying $\lambda_{q^n}(y) \in K$. It follows that $x^{-1}\sigma_{q^n}(x) = \phi(\lambda_{q^n}(y)) = 1$, and therefore, $x \in G(\mathbb{F}_{q^n})$. By definition of $\mu_{q^n}$, the coset $x\phi(G'(\mathbb{F}_{q^n}))$ is mapped to the coset $\lambda_{q^n}(y)\lambda_{q^n}(\operatorname{Ker}\phi)$. Since $\mu_{q^n}$ induces an isomorphism between the quotients, the coset $x\phi(G'(\mathbb{F}_{q^n}))$ is an element of $H/\phi(G'(\mathbb{F}_{q^n}))$. By hypothesis, $H$ contains $\phi(G'(\mathbb{F}_{q^n}))$, and therefore, $x \in H$. □

Lemma 3.2 constructs one isogeny reaching one subgroup. One expects that an infinite family of subgroups require infinitely many isogenies. However, we have the following corollary.

**Corollary 3.3.** *Let $G'$, $G$ and $\phi\colon G' \to G$ be two connected linear algebraic groups and an isogeny defined over $\mathbb{F}_q$. For infinitely many $n$, let $H_n$ be a subgroup of $G(\mathbb{F}_{q^n})$ containing $\phi(G'(\mathbb{F}_{q^n}))$. Then there are finitely many isogenies reaching all $H_n$.*

*Proof.* Fix any $n$ for which $H_n$ is defined. Since $G, G'$ and $\phi$ are defined over $\mathbb{F}_q$, in particular, they are defined over $\mathbb{F}_{q^n}$, so Lemma 3.2 applies.

Now let $n$ vary. Since $K_n \subseteq \operatorname{Ker}\phi$ and $\operatorname{Ker}\phi$ is finite, there are only finitely many possibilities for $\phi''\colon G'' \to G$. □

**Remark 3.4.** In Lemma 3.2, the subgroup $K = K_n$ contains $\lambda_{q^n}(\operatorname{Ker}\phi)$; this implies that the isogeny $\phi''\colon G'' \to G$ is defined over $\mathbb{F}_{q^n}$. In general, the isogenies of Corollary 3.3 are defined over any field $\mathbb{F}_{q^m}$ for which $Z(G(\mathbb{F}_{q^m})) = ZG$ since, in this case, $\lambda_{q^m}(\operatorname{Ker}\phi) = \{1\}$. If, for every $n$, the subgroup $K_n$ contains $\lambda_q(\operatorname{Ker}\phi)$, then the isogenies are all defined over $\mathbb{F}_q$.

Lemma 3.2 and Corollary 3.3 are key in the proof of the main theorems. We also need the following elementary lemma, whose proof is left as an exercise.

**Lemma 3.5.** *Let $G$ be a finite group. Let $N$ and $H$ be two subgroups. Suppose that $N$ is normal. Then*

$$[G : H] = \left[\frac{G}{N} : \frac{HN}{N}\right][N : H \cap N].$$

Following [8,11], we say that a semisimple algebraic group is *simple* if it has no proper positive-dimensional normal subgroup. Note that other authors prefer the name *almost-simple* [10].

The main result about simple groups over finite fields is due to J. Tits: let $G$ be a simple, simply connected linear algebraic group defined over $\mathbb{F}_q$. Unless $G(\mathbb{F}_{q^n})$ is one of

$$\mathrm{SL}_2(\mathbb{F}_2),\ \mathrm{SL}_2(\mathbb{F}_3),\ \mathrm{SU}_3(\mathbb{F}_2),\ \mathrm{Sp}_4(\mathbb{F}_2),\ G_2(\mathbb{F}_2),\ {}^2B_2(\mathbb{F}_2),\ {}^2G_2(\mathbb{F}_3),\ {}^2F_4(\mathbb{F}_2),$$

the group $G(\mathbb{F}_{q^n})/Z(G(\mathbb{F}_{q^n}))$ is simple [8, Theorem 24.17]. We refer to this result as Tits' Theorem in the remainder of the paper. Note that the last three groups in the list are not groups of rational points: they are not fixed subgroups of a Frobenius automorphism, but of a Steinberg endomorphism [8, Definition 21.3]. Therefore, the list of exceptions is actually shorter. The only thing we will need is that it is finite.

**Theorem 3.6.** *Let $G$ be a reductive linear algebraic group defined over $\mathbb{F}_q$. Fix $k \geq 1$ and suppose that, for infinitely many $n$, the group of rational points $G(\mathbb{F}_{q^n})$ contains a subgroup $H_n$ of index $k$. Then there are finitely many isogenies from linear algebraic groups onto $G$ such that all but finitely many of the $H_n$ are reached by at least one of these.*

*Proof.* Reductive groups can be obtained from simple groups and tori by taking products and isogenies. The proof of the theorem, which consists of several steps, shows that the class of algebraic groups satisfying the statement contains simple groups and tori and is closed under the formation of reductive groups.

*Step 1: If $G$ is simple, simply connected, then $k = 1$.* Let $G$ be simple, simply connected and suppose $k > 1$. Choose $n$ such that $H_n$ is defined. Since $H_n$ has index $k$, its normalizer has index at most $k$; therefore, $H_n$ has at most $k$ conjugates. Each of them has index $k$, so their intersection

$$\bigcap\{H_n^g : g \in G(\mathbb{F}_{q^n})\}$$

is a normal subgroup of index between $k$ and $k^k$. Since $k > 1$, for $n$ large enough, Tits' Theorem implies

$$\frac{|G(\mathbb{F}_{q^n})|}{|Z(G(\mathbb{F}_{q^n}))|} \leq k^k.$$

This is a contradiction since $|G(\mathbb{F}_{q^n})|$ grows as $n$ grows (see [8, Table 24.1]), while the size of the center $|Z(G(\mathbb{F}_{q^n}))|$ is bounded by $|ZG|$, which is finite by hypothesis. We conclude that $k = 1$. The statement is trivially satisfied by the identity map $G \to G$.

*Step 2: If $G$ is semisimple, simply connected, then $k = 1$.* Let $G$ be semisimple, simply connected. Then $G$ is direct product of its minimal connected normal subgroups which are simple, simply connected and defined over $\mathbb{F}_q$ (see [10, Paragraphs 17.22, 17.24]). We proceed by induction on the number of simple components. Let $N$ be one simple component. By Step 1, applied to $N$, the intersection $H_n \cap N(\mathbb{F}_{q^n})$ must be equal to $N(\mathbb{F}_{q^n})$ for $n$ large enough. By Lemma 3.5, the index $k = [G(\mathbb{F}_{q^n}) : H_n]$ must be equal to the index of $H_n/N(\mathbb{F}_{q^n})$ in the quotient $G(\mathbb{F}_{q^n})/N(\mathbb{F}_{q^n})$. Since $N$ is connected, we have $(G/N)(\mathbb{F}_{q^n}) = G(\mathbb{F}_{q^n})/N(\mathbb{F}_{q^n})$ by [1, Corollary 16.5 (ii)] and induction applies to $G/N$.

*Step 3: The statement is true if $G$ is semisimple.* Let $G$ be semisimple. Then it admits a universal covering $\phi\colon G' \to G$, where $G'$ is simply connected and $\phi$ is an isogeny, both defined over $\mathbb{F}_q$ (see [10, Paragraph 16.21]). Note that, since $G$ is semisimple, the group $G'$ is semisimple, and so Step 2 applies to $G'$. The preimages of $\phi(G(\mathbb{F}_{q^n})) \cap H_n$ with respect to $\phi$ have index bounded by $k$, and so, by Step 2, they coincide with $G'(\mathbb{F}_{q^n})$ for $n$ large enough. This means that $\phi(G'(\mathbb{F}_{q^n})) \subseteq H_n$. Corollary 3.3 applies.

*Step 4: The statement is true if $G$ is a torus.* Let $G$ be a torus. Since $G(\mathbb{F}_{q^n})$ is isomorphic to a subgroup of $(\mathbb{F}^*_{q^m})^d$ for some $m$ and $d$, the integers $k$ and $q$ must be coprime. Consider the homomorphism $G \to G$ sending $g \mapsto g^k$; it is defined over $\mathbb{F}_q$. Since $k$ and $q$ are coprime, this morphism is an isogeny. Since $G(\mathbb{F}_{q^n})/H_n$ has $k$ elements, we have $G(\mathbb{F}_{q^n})^k \subseteq H_n$. Corollary 3.3 applies.

*Step 5: The statement is true if $G$ is the direct product of a torus and a semisimple group, both defined over $\mathbb{F}_q$.* Let $G = T \times S$, where $T$ is a torus and $S$ is semisimple. The integers $[T(\mathbb{F}_{q^n}) : H_n \cap T(\mathbb{F}_{q^n})]$ and $[S(\mathbb{F}_{q^n}) : H_n \cap S(\mathbb{F}_{q^n})]$ are divisors of $[G(\mathbb{F}_{q^n}) : H_n] = k$. Since the divisors of $k$ are finite in number, we reduce to finitely many cases, so by Step 3 and Step 4, we find finitely many isogenies $\phi \times \psi$ reaching $(H_n \cap T(\mathbb{F}_{q^n})) \times (H_n \cap S(\mathbb{F}_{q^n}))$, which is a subgroup of $H_n$. Once more, Corollary 3.3 applies.

*Step 6: The statement is true if $G$ is reductive.* Let $G$ be reductive. Let $T$ be the identity component of $ZG$ and $S = [G, G]$ the derived subgroup. Since $\mathbb{F}_q$ is perfect, $T$ and $S$ are defined over $\mathbb{F}_q$ (see [12, Section 12.1.7]). The group $T$ is a torus, the group $S$ is semisimple and the product map $\pi\colon T \times S \to G$ is an isogeny [8, Proposition 6.20, Corollary 8.22].

By Lemma 3.5, the index of

$$H_n \cap T(\mathbb{F}_{q^n})S(\mathbb{F}_{q^n})$$

in $T(\mathbb{F}_{q^n})S(\mathbb{F}_{q^n})$ divides $k$, so there are only finitely many possibilities and hence finitely many possibilities for the index of $\pi^{-1}(H_n)$ in $T(\mathbb{F}_{q^n}) \times S(\mathbb{F}_{q^n})$. By Step 5, for every $\pi^{-1}(H_n)$, we find an isogeny $\phi\colon G' \to T \times S$ defined over $\mathbb{F}_{q^n}$

reaching $\phi(G'(\mathbb{F}_{q^n})) = \pi^{-1}(H_n)$, and finitely many isogenies are enough to reach all $\pi^{-1}(H_n)$. For every $\phi$, the composition $\pi \circ \phi\colon G' \to G$ is an isogeny defined over $\mathbb{F}_{q^n}$, and the image $\pi(\phi(G'(\mathbb{F}_{q^n}))$ is contained in $H_n$. Lemma 3.2 applies to each $\phi$, giving finitely many isogenies reaching all $H_n$. □

Some parts of the proof are interesting in their own right. From Step 2, we have the following corollary.

**Corollary 3.7.** *Let $G$ be semisimple, simply connected and $k > 1$. Then, for $n$ sufficiently large, the group $G(\mathbb{F}_{q^n})$ contains no subgroups of index $k$. In particular, the minimal indices of proper subgroups of $G(\mathbb{F}_{q^n})$ diverge to infinity.*

*Proof.* Fix $h > 1$. For every $k \in \{2, \dots, h\}$, there is $n_k$ such that, for every $n > n_k$, the group $G(\mathbb{F}_{q^n})$ contains no subgroups of index $k$. For every $n$ larger than $\max\{n_2, \dots, n_h\}$, the minimal index of proper subgroups of the group $G(\mathbb{F}_{q^n})$ is larger than $h$. □

From Step 3, we have the following corollary.

**Corollary 3.8.** *Let $G$ be semisimple and let $d$ be the order of its universal covering $\phi\colon G' \to G$. Let $H_n \subseteq G(\mathbb{F}_{q^n})$ be an infinite sequence of subgroups of fixed index $k$. Then, for every $n$ large enough, the group $H_n$ contains the image of the universal covering $\phi(G'(\mathbb{F}_{q^n}))$. In particular, $k \leq d$.*

## 4 From subgroups to isogenies: Non-reductive groups

Theorem 3.6 requires $G$ to be reductive. The hypothesis is necessary, due to the abundance of $p$-subgroups in unipotent groups.

For example, consider the additive group $\mathbb{G}_a$ defined over $\mathbb{F}_p$. We have

$$\mathbb{G}_a(\mathbb{F}_{p^n}) = \mathbb{F}_{p^n},$$

endowed with the field addition. The subgroups of index $p$ of $\mathbb{F}_{p^n}$ are the hyperplanes of $\mathbb{F}_{p^n}$, as a vector space over $\mathbb{F}_p$. There are $(p^n - 1)/(p - 1)$ of them. In particular, the subgroups of index $p$ grow in number with $n$. They cannot all be reached by finitely many isogenies.

However, if $k$ is prime to the characteristic, reductiveness is not necessary.

**Theorem 4.1.** *Let $G$ be a linear algebraic group defined over $\mathbb{F}_q$. Let $k \geq 1$ such that $k$ and $q$ are coprime and, for infinitely many $n$, the group of rational points $G(\mathbb{F}_{q^n})$ contains a subgroup $H_n$ of index $k$. Then there are finitely many linear algebraic groups $G'$ and isogenies $G' \to G$ such that, except for finitely many $n$, every $H_n$ is reached by one of them.*

*Proof.* Let $U$ be the unipotent radical of $G$. As $\mathbb{F}_q$ is perfect, $U$ is defined over $\mathbb{F}_q$ (see [12, Section 12.1.7]). Since $U(\mathbb{F}_{q^n})$ is a $p$-group, the index of $U(\mathbb{F}_{q^n}) \cap H_n$ in $U(\mathbb{F}_{q^n})$ divides both $q$ and $k$, so it must be 1, and hence $U(\mathbb{F}_{q^n}) \subseteq H_n$. Theorem 3.6 applied to the quotient $G/U$ gives finitely many isogenies $\phi\colon G' \to G/U$ reaching $H_n/U(\mathbb{F}_{q^n})$ for $n$ large.

Fix $n$ and one isogeny $\phi\colon G' \to G/U$ reaching $H_n/U(\mathbb{F}_{q^n})$. We want to lift $\phi$ to $G$. Consider the fiber product $G' \times_{G/U} G$ whose elements are the pairs $(g', g) \in G' \times G$ satisfying $\phi(g') = \pi(g)$, where $\pi\colon G \to G/U$ is the canonical projection. We have the following commutative diagram:

$$\begin{tikzcd} G' \times_{G/U} G \arrow[r] \arrow[d] & G \arrow[d, "\pi"] \\ G' \arrow[r, "\phi"] & G/U, \end{tikzcd}$$

where the unlabelled arrows are the canonical projections.

For now, suppose that $G' \times_{G/U} G$ is connected. The top arrow

$$\phi'\colon G' \times_{G/U} G \to G$$

is an isogeny since its kernel is $\mathrm{Ker}(\phi) \times 1$. Since $\phi$, $\pi$ and $U$ are defined over $\mathbb{F}_q$ and $U$ is connected, we have

$$(G' \times_{G/U} G)(\mathbb{F}_{q^n}) = G'(\mathbb{F}_{q^n}) \times_{G(\mathbb{F}_{q^n})/U(\mathbb{F}_{q^n})} G(\mathbb{F}_{q^n}),$$

and by commutativity of the diagram, we have

$$\pi(\phi'((G' \times_{G/U} G)(\mathbb{F}_{q^n}))) = \phi(G'(\mathbb{F}_{q^n})),$$

where the right-hand side equals $H_n/U(\mathbb{F}_{q^n})$. We conclude that

$$\phi'((G' \times_{G/U} G)(\mathbb{F}_{q^n})) = H_n.$$

Finally, if $G' \times_{G/U} G$ is not connected, replace it by its identity component: since $G$ and $G'$ are connected, the projections remain surjective, and the same argument applies. $\square$

From Theorem 2.2, Theorem 3.6 and Theorem 4.1, we obtain a remarkable fact.

**Corollary 4.2.** *Let $k \geq 1$, and assume that either $G$ is reductive or $k$ is prime to $q$. The set of $n$ such that $G(\mathbb{F}_{q^n})$ contains a subgroup of fixed index $k$ is either finite, or it contains an arithmetic progression.*

**Remark 4.3.** Lemma 3.1 can be generalized to Steinberg endomorphisms; see [5, Proposition 1.4.13] and [13, Proposition 4.5]. Indeed, if $F\colon G \to G$, $F'\colon G' \to G'$ are Steinberg endomorphisms satisfying $\phi \circ F' = F \circ \phi$, the groups $G^F/\phi(G'^{F'})$ and $\operatorname{Ker}\phi/L(\operatorname{Ker}\phi)$ are isomorphic, where $G^F$ and $G'^{F'}$ denote the fixed point subgroups and $L(y) = y^{-1}F'(y)$. This suggests a generalization of Theorem 3.6 and Theorem 4.1 to groups arising as fixed points of Steinberg endomorphisms. However, it is not clear to the author how to generalize Steps 2 and 3 of the proof of Theorem 3.6.

## 5 Varying the characteristic

In this section, $G$ is a linear algebraic group defined over $\mathbb{Q}$. Except for finitely many primes, the group $G$ is well defined modulo $p$ and we can consider $G(\mathbb{F}_p)$. In analogy with the previous result, we ask whether subgroups of fixed index in $(G(\mathbb{F}_p))_p$ are related to isogenies $\phi\colon G' \to G$ defined over $\mathbb{Q}$.

Corollary 3.7 about simply connected groups has a perfect analogue.

**Theorem 5.1.** *Let $G$ be a semisimple, simply connected linear algebraic group defined over $\mathbb{Q}$. Let $k > 1$. Then, for $p$ sufficiently large, the group $G(\mathbb{F}_p)$ contains no subgroup of index $k$.*

*Proof.* Suppose that $G$ is simple and simply connected; the general case follows by induction on the number of simple factors.

Suppose that, for infinitely many $p$, the group $G(\mathbb{F}_p)$ contains a subgroup of index $k > 1$. Then, as in the proof of Theorem 3.6, for $p$ large enough, we obtain

$$\frac{|G(\mathbb{F}_p)|}{|Z(G(\mathbb{F}_p))|} \le k^k.$$

This is a contradiction since $G(\mathbb{F}_p)$ grows as $p$ grows (see [8, Table 24.1]), while the size of the center $|Z(G(\mathbb{F}_p))|$ is bounded by $|ZG|$, which is finite by hypothesis. We conclude that $k = 1$. □

We now show, by an explicit example, that infinitely many subgroups of fixed index may be unreachable by a rational isogeny. Consider the torus

$$G = \left\{ \begin{pmatrix} a & -b \\ b & a-b \end{pmatrix} \,\middle|\, a^2 - ab + b^2 \neq 0 \right\}.$$

Note that $G(\mathbb{F})$ is split if and only if the field $\mathbb{F}$ contains a primitive third root of unity. Indeed, let $\xi^3 = 1$ and $\xi \neq 1$. We have $a^2 - ab + b^2 = (a + \xi b)(a + \xi^2 b)$

and

$$\begin{pmatrix} 1 & \xi \\ 1 & \xi^2 \end{pmatrix} \begin{pmatrix} a & -b \\ b & a-b \end{pmatrix} \begin{pmatrix} 1 & \xi \\ 1 & \xi^2 \end{pmatrix}^{-1} = \begin{pmatrix} a+\xi b & 0 \\ 0 & a+\xi^2 b \end{pmatrix}.$$

As variety over $\mathbb{C}$, the group $G(\mathbb{C})$ is equal to the projective plane minus three lines: the line at infinity, which is defined over $\mathbb{Q}$, and two conjugated lines $a + \xi b$ and $a + \xi^2 b$. This gives three 2-fold coverings of which only one can be defined over $\mathbb{Q}$. The rational covering actually corresponds to a rational isogeny, namely

$$\begin{pmatrix} a & -b & 0 \\ b & a-b & 0 \\ 0 & 0 & c \end{pmatrix} \mapsto \begin{pmatrix} a & -b \\ b & a-b \end{pmatrix},$$

where $c^2 = a^2 - ab + b^2$. Matrices of the form on the left form a two-dimensional torus.

On the other hand, for every prime $p$ satisfying $p \equiv 1 \bmod 3$, the field $\mathbb{F}_p$ contains a primitive third root of unity. Therefore, the group $G(\mathbb{F}_p)$ is isomorphic to ${\mathbb{F}_p}^* \times {\mathbb{F}_p}^*$. In particular, it has three subgroups of index 2. We deduce that at least two subgroups cannot be reached by rational isogenies. However, this suggests that infinitely many subgroups of fixed index in $(G(\mathbb{F}_p))_p$ correspond to isogenies over a finite extension of $\mathbb{Q}$. We leave this as a conjecture.

**Acknowledgments.** This work is part of a *Tesi di Laurea* at the University of Udine. The author is grateful to his advisor, Prof. Pietro Corvaja, for many inspiring discussions, support and patience. The author would also like to thank Prof. Gunter Malle for his time and precious comments that helped improve the manuscript.

## Bibliography

[1] A. Borel, *Linear Algebraic Groups*, 2nd ed., Grad. Texts in Math. 126, Springer, New York, 1991.

[2] A. Borel, *Essays in the History of Lie Groups and Algebraic Groups*, Hist. Math. 21, American Mathematical Society, Providence, 2001.

[3] C. Chevalley, Algebraic Lie algebras, *Ann. of Math. (2)* **48** (1947), 91–100.

[4] C. Chevalley, On algebraic group varieties, *J. Math. Soc. Japan* **6** (1954), 303–324.

[5] M. Geck and G. Malle, *The Character Theory of Finite Groups of Lie Type: A Guided Tour*, Cambridge Stud. Adv. Math. 187, Cambridge University, Cambridge, 2020.

[6] D. Gorenstein, *Finite Simple Groups: An Introduction to Their Classification*, Univ. Ser. Math., Plenum, New York, 1982.

[7] P. B. Kleidman and M. W. Liebeck, A survey of the maximal subgroups of the finite simple groups, *Geom. Dedicata* **28** (1988), 375–389.

[8] G. Malle and D. Testerman, *Linear Algebraic Groups and Finite Groups of Lie Type*, Cambridge Stud. Adv. Math. 133, Cambridge University, Cambridge, 2011.

[9] J. S. Milne, *Algebraic Groups*, Cambridge Stud. Adv. Math. 170, Cambridge University, Cambridge, 2017.

[10] J. S. Milne, Reductive Groups, https://www.jmilne.org/math/CourseNotes/RG.pdf, 2018.

[11] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory*, Pure Appl. Math. 139, Academic Press, Boston, 1993.

[12] T. A. Springer, *Linear Algebraic Groups*, 2nd ed., Mod. Birkhäuser Class., Birkhäuser, Boston, 1998.

[13] R. Steinberg, *Endomorphisms of Linear Algebraic Groups*, Mem. Amer. Math. Soc. 80, American Mathematical Society, Providence, 1968.

[14] W. C. Waterhouse, *Introduction to Affine Group Schemes*, Grad. Texts in Math. 66, Springer, New York, 1979.

Received June 29, 2022; revised February 8, 2023

**Author information**

Corresponding author:
Davide Sclosa, Mathematics Department, Vrije Universiteit Amsterdam,
Amsterdam, Netherlands.
E-mail: d.sclosa@vu.nl