Picard Groups of Linear Algebraic Groups

Zev Rosengarten

Contents

1 Introduction 1
   1.1 Notation . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

2 First Results 3

3 Behavior of Pic in Exact Sequences 5

4 Groups With Finite Pic 10

5 $\text{Ext}^1(G, G_m)$ 13

6 Behavior of $\text{Ext}^1(\cdot, G_m)$ in Exact Sequences 20

7 Pseudo-Semisimple Groups 22

8 Completing the Proof of Theorem 5.5 27

9 Forms of $G_a$ 28

A Characters 34

1 Introduction

The purpose of this paper is to investigate the properties of Picard groups of linear algebraic groups, particularly various finiteness properties of such groups. We will see that the situation is relatively simple if the base field $k$ is perfect, so the main case of interest is when $k$ is imperfect. Of particular importance is the case in which $k$ is a local or global function field. In fact, the arithmetic case is the main motivation for writing this paper, the results of which will play a role in a forthcoming work on Tamagawa numbers of linear algebraic groups.

First, §2 gives some simple preliminary results on the structure of Picard groups of linear algebraic groups, and shows in particular that the situation is relatively simple when
$k$ is perfect. Then §3 explores how the Picard group behaves in exact sequences of linear algebraic groups. Next, §4 proves that linear algebraic groups with finite Picard group also behave relatively nicely, under certain mild hypotheses. In §5 we introduce the group $\text{Ext}^1(G, \mathbb{G}_m)$, which is the subgroup of $\text{Pic}(G)$ consisting of line bundles that are, in a sense, “universally translation-invariant”. This group will play a significant role in future work. Our main result about $\text{Ext}^1(G, \mathbb{G}_m)$ is that it is finite for any connected linear algebraic group $G$ over any global field (Theorem 5.5). Next, §6 explores the behavior of $\text{Ext}^1(\cdot, \mathbb{G}_m)$ in exact sequences of linear algebraic groups, which is an essential tool for proving this finiteness, and essentially (by an easy dévissage) reduces us to the cases when $G$ is either pseudo-semisimple or commutative. We treat the pseudo-semisimple case in §7. In fact, in this case the proof works for any field whatsoever (with a mild extra hypothesis when $\text{char}(k) = 2$) by making use of the classification of pseudo-semisimple groups obtained in [CGP]. Then §8 completes the proof of the finiteness in the case when $k$ is a global field. This finiteness does not hold over general fields, and so must use something special about global function fields. The key input is the generalization of Tate duality to positive-dimensional groups obtained in [Ros]. Finally, §9 analyzes the Picard groups of forms of $\mathbb{G}_a$. This analysis is used to provide examples of various pathological behaviors of Picard groups over imperfect fields. In particular, it is shown that $\text{Ext}^1(U, \mathbb{G}_m)$ is almost always infinite for forms $U$ of $\mathbb{G}_a$ over local function fields and over imperfect separably closed fields. These examples, in conjunction with global Tate duality, are also used to show that for almost all nontrivial forms $U$ of $\mathbb{G}_a$ over a global function field $k$ (all, if $\text{char}(k) > 2$), the group

$$\Pi^1_S(U) := \ker \left( H^1(k, U) \to \prod_{v \notin S} H^1(k_v, U) \right)$$

(where the product is over all places $v$ of $k$ not in $S$) is infinite whenever $S \neq \emptyset$ (Corollary 9.14). (It is always finite if $S = \emptyset$ [Oes, Chap. IV., §2.6, Prop.(a)], in fact, in this case it is finite for all affine $k$-group schemes of finite type [Con, Th. 1.3.3(i)]; note that the version of [Con, Th. 1.3.3(i)] given in the original paper is incorrect. One must take $S = \emptyset$, see remark 9.12.)

We note here that all of the results in §§2, 3, and 5 - with the exceptions of Theorems 5.5 and 5.6 - have been known to experts for a long time (and the results of §6 are just a slight, though necessary, modification of those in §3). We have collected them here, however, because of the lack of a reference (as far as the author is aware) where all of these results are collected together. Hopefully this serves to make perusing this paper more convenient for the reader. The rest of this paper is (as far as I am aware) new, however, so those “in the know” can skip the sections listed above, and refer back to them if necessary.
1.1 Notation

Throughout this paper, \( k \) denotes a field, \( k_s, \overline{k} \) denote separable and algebraic closures of \( k \), respectively, and \( \mathfrak{g} := \text{Gal}(k_s/k) \). If \( \text{char}(k) > 0 \), then \( p = \text{char}(k) \). Given \( k \)-group schemes \( G, H \), we have the pullback maps along the two projections \( \text{Pic}(G), \text{Pic}(H) \rightarrow \text{Pic}(G \times H) \). This yields a map \( \text{Pic}(G) \oplus \text{Pic}(H) \rightarrow \text{Pic}(G \times H) \). This map is injective, since if \( p_1^* \mathcal{L}_1 \otimes p_2^* \mathcal{L}_2 \simeq 0 \), then restriction to \( \{1\} \times H \) and \( G \times \{1\} \) shows that \( \mathcal{L}_1 \simeq \mathcal{L}_2 \simeq 0 \). If this map \( \text{Pic}(G) \oplus \text{Pic}(H) \rightarrow \text{Pic}(G \times H) \) is an isomorphism, then we abuse notation and write \( \text{Pic}(G \times H) = \text{Pic}(G) \oplus \text{Pic}(H) \). If \( G \) is smooth and connected, then we define \( \text{Ext}^1(G, \mathbb{G}_m) \) to be the subgroup of \( \text{Pic}(G) \) consisting of primitive line bundles. That is, \( \text{Ext}^1(G, \mathbb{G}_m) := \{ \mathcal{L} \in \text{Pic}(G) | m^* \mathcal{L} \simeq p_1^* \mathcal{L} \otimes p_2^* \mathcal{L} \} \), where \( m, p_i : G \times G \rightarrow G \) are the multiplication and projection maps. This is the same as the set of universally translation-invariant line bundles, as may be seen by restricting the equality \( m^* \mathcal{L} \simeq p_1^* \mathcal{L} \otimes p_2^* \mathcal{L} \) to a fiber \( g \in G(R) \). The reason for the notation \( \text{Ext}^1(G, \mathbb{G}_m) \) will become clear in section 5 where such line bundles will be shown to be in natural bijection with extension classes of \( G \) by \( \mathbb{G}_m \).

2 First Results

In this section we prove some basic results about Picard groups of linear algebraic groups.

Lemma 2.1. Let \( G \) be a connected linear algebraic \( k \)-group. If \( \text{Pic}(G \times G) = \text{Pic}(G) \oplus \text{Pic}(G) \), then \( \text{Pic}(G) = \text{Ext}^1(G, \mathbb{G}_m) \).

Proof. Indeed, let \( \mathcal{L} \in \text{Pic}(G) \). Since \( \text{Pic}(G \times G) = \text{Pic}(G) \oplus \text{Pic}(G) \), we have \( m^* \mathcal{L} \simeq p_1^* \mathcal{L}_1 \otimes p_2^* \mathcal{L}_2 \) for some \( \mathcal{L}_1, \mathcal{L}_2 \in \text{Pic}(G) \). Restricting to \( G \times \{1\} \) and \( \{1\} \times G \), we see that \( \mathcal{L}_1, \mathcal{L}_2 \simeq \mathcal{L} \). Thus \( \mathcal{L} \in \text{Ext}^1(G, \mathbb{G}_m) \).

Proposition 2.2. Let \( G, H \) be connected linear algebraic \( k \)-groups, and suppose that \( G_{k_s} \) is rational. Then \( \text{Pic}(G \times H) = \text{Pic}(G) \oplus \text{Pic}(H) \). In particular, \( \text{Pic}(G) = \text{Ext}^1(G, \mathbb{G}_m) \).

Proof. This is an immediate consequence of [San], Lemme 6.6, (i). The second assertion comes from Lemma 2.1 by applying the first assertion with \( H = G \).

Lemma 2.3. Let \( G \) be a connected linear algebraic \( k \)-group. Then we have an exact sequence, functorial in \( G \),

\[
0 \rightarrow H^1(k, \widehat{G}(k_s)) \rightarrow \text{Pic}(G) \rightarrow \text{Pic}(G_{k_s})^0
\]

Proof. This follows from [San], Lemme 6.3, (ii) and Rosenlicht’s Unit Theorem. The functoriality also follows from the construction of the sequence given there.

Proposition 2.4. Let \( G \) be a linear algebraic \( k \)-group. The pullback map \( \text{Pic}(G) \rightarrow \text{Pic}(G_{k_s}) \) has finite kernel.
Proof. In this proof all cohomology is Galois. Since Pic($G$) = $\prod$ Pic($G_i$), the product being over the connected components of $G$, it suffices to prove this for each connected component $G_i$. We have a Hochschild-Serre spectral sequence

$$H^p(k, H^q((G_i)_{k_s}, G_m)) \implies H^{p+q}(G_i, G_m)$$

hence an exact sequence

$$1 \rightarrow H^1(k, k_s[G_i]^*) \rightarrow \text{Pic}(G_i) \rightarrow \text{Pic}((G_i)_{k_s})$$

so we need to show that $H^1(k, k_s[G_i]^*)$ is finite. Let $L$ be the algebraic closure of $k$ inside $k(G_i)$. Since $G_i$ is normal, we have $L \subset k[G_i]$, so we have an exact sequence of $\text{Gal}(k_s/k)$-modules

$$1 \rightarrow (L \otimes_k k_s)^* \rightarrow k_s[G_i]^* \rightarrow U((G_i)_{k_s}) \rightarrow 1$$

(where $U((G_i)_{k_s})$ is simply defined by this sequence), and $H^1(k, (L \otimes_k k_s)^*) = H^1(L, L^*) = 1$ by [Oes, Chap. IV, §2, Cor.], so it’s enough to show that $H^1(k, U((G_i)_{k_s}))$ is finite. But if $(G_i)_{k_s}$ has $n$ connected components, then $U((G_i)_{k_s}) \simeq (U(G_{k_s}^0))^n$ as groups (since each component of $G_{k_s}$ is isomorphic to $G_{k_s}^0$ as $k_s$-schemes), and the latter group is isomorphic to $\overline{G}_0(k_s)^n$ (essentially by Rosenlicht’s Unit Theorem), hence is free abelian of finite type. Therefore $H^1(k, U((G_i)_{k_s}))$ is indeed finite, as desired. \qed

Proposition 2.5. Let $G$ be a linear algebraic $k$-group. If $G_{k_s}^0$ is rational, then Pic($G$) is finite.

Proof. By Proposition 2.4, we may assume that $k = k_s$. We have Pic($G$) = $\prod$ Pic($G_i$), where the product is over all components $G_i$ of $G$. Every $G_i$ is isomorphic (as a scheme) to $G^0$, since $k = k_s$, so we may assume that $G$ is connected. Then this proposition is [KKLV, Prop. 4.5] when $G$ is connected, except there the proof is only given over $k = \overline{k}$. All that they actually use, however, is the fact that $G$ is rational, which we are assuming to be the case. Alternatively, we may easily deduce the theorem from the algebraically closed case as follows. The argument given in the proof of Proposition 2.8 below shows that the pullback map Pic($G$) → Pic($G_{\overline{k}}$) has torsion (even $p$-power torsion) kernel. It follows that Pic($G$) is torsion, so to show that it is finite, it’s enough to show that it’s finitely generated. But because $G$ is rational, some open subset $U \subset G$ has trivial Picard group, hence the (classes of the) finitely many divisors supported in the complement of $U$ generate Pic($G$), so we’re done. \qed

Proposition 2.6. Let $G$ be a connected linear algebraic $k$-group. For some finite purely inseparable extension $k'/k$, Pic($G_{k'}$) is finite, Pic($G_{k'} \times G_{k'}$) = Pic($G_{k'}$) ⊕ Pic($G_{k'}$), and Pic($G_{k'}$) = Ext$^1(G_{k'}, G_m)$.

Proof. $G_{\overline{k}}$ is rational, so $G_{k'}$ is separably rational for some finite purely inseparable $k'/k$. Thus the proposition follows from Propositions 2.5 and 2.2. \qed
Proposition 2.7. If $k$ is perfect and $G$ is a connected linear algebraic $k$-group, then $\text{Pic}(G)$ is finite, $\text{Pic}(G \times G) = \text{Pic}(G) \oplus \text{Pic}(G)$, and $\text{Pic}(G) = \text{Ext}^1(G, \mathbb{G}_m)$.

Proof. Immediate from Proposition 2.6.

For an abelian group $A$ and a prime number $l$, let $A[l] := A[l^\infty]$ denote the $l$-primary part of $A$. Let $A[\text{non-}l] := \oplus_{q \neq l} A_q$, the sum being over the primes $q \neq l$. The next proposition tells us that in characteristic $p$, all of the possible infinitude of $\text{Pic}(G)$ comes from the $p$-part.

Proposition 2.8. Let $k$ be a field of characteristic $p > 0$. Then $\text{Pic}(G) = \text{Pic}(G)_p \oplus \text{Pic}(G)[\text{non-}p]$, where $\text{Pic}(G)[\text{non-}p]$ is finite, and $\text{Pic}(G)_p$ is of finite exponent.

Proof. By Proposition 2.6, it suffices to show that for a finite purely inseparable extension $k'/k$, $\ker(\text{Pic}(G) \to \text{Pic}(G_{k'})) \subset \text{Pic}(G)[p^n]$ for some $n$. But we have morphisms of sheaves on $G$:

$$\mathcal{O}_G^* \longrightarrow \mathcal{O}_{G_{k'}}^* \xrightarrow{p^n} \mathcal{O}_G^*$$

and the composition is the $p^n$ power map, where $n$ is chosen so that $k'^{p^n} \subset k$. Thus multiplication by $p^n$: $H^1(X, \mathcal{O}_G^*) \to H^1(G, \mathcal{O}_G^*)$ factors through the pullback map $H^1(G, \mathcal{O}_G^*) \to H^1(G_{k'}, \mathcal{O}_{G_{k'}})$, so the kernel of this pullback is killed by $p^n$.

3 Behavior of Pic in Exact Sequences

In this section we will prove various results examining how the Picard group behaves in a short exact sequence of linear algebraic $k$-groups.

Lemma 3.1. Suppose that we have a short exact sequence of finite type $k$-group schemes

$$1 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 1$$

such that $G''$ is smooth and connected. Then we have an exact sequence

$$0 \longrightarrow \widehat{G''}(k) \longrightarrow \widehat{G}(k) \longrightarrow \widehat{G'}(k) \longrightarrow \text{Ext}^1(G'', \mathbb{G}_m)$$

All of the maps in the exact sequence of the lemma are the obvious ones (the last one $\widehat{G'}(k) \to \text{Ext}^1(G'', \mathbb{G}_m)$ being obtained via pushout along the character).

Proof. First, the exactness of

$$0 \longrightarrow \widehat{G''}(k) \longrightarrow \widehat{G}(k) \longrightarrow \widehat{G'}(k)$$
(where all of the maps are the obvious ones) is clear. (Just use the fact that $G^{''} = G/G'$, together with the universal property of quotients.) We therefore only have to check exactness at $\hat{G}'(k)$. Suppose that $\chi \in \hat{G}'(k)$ is such that the bottom row of the pushout diagram

$$
\begin{array}{cccccc}
1 & \longrightarrow & G' & \longrightarrow & G & \longrightarrow & G'' & \longrightarrow & 1 \\
\downarrow{\chi} & & \downarrow & & \downarrow & & & \\
1 & \longrightarrow & G_m & \longrightarrow & E & \longrightarrow & G'' & \longrightarrow & 1
\end{array}
$$

splits. Then the composition $G \to E \to G_m$, where the last map is the splitting, yields an extension of $\chi$ to $G$. \hfill \Box

**Lemma 3.2.** Suppose that we have a short exact sequence of $k$-group schemes of finite type

$$
1 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 1
$$

such that $G$ is smooth and connected. Suppose that one of the following holds:

(i) $G'$ is smooth and connected.
(ii) $\text{Pic}(G''_k) = 0$.

Then we have an exact sequence

$$
0 \longrightarrow \hat{G}''(k) \longrightarrow \hat{G}(k) \longrightarrow \hat{G}'(k) \longrightarrow \text{Pic}(G'') \longrightarrow \text{Pic}(G)
$$

We remark that, examining the proof below, one can see that all of the maps are the obvious ones: either pullback, or in the case of the map $\hat{G}'(k) \to \text{Pic}(G'')$, pushout by a character in order to produce a $G_m$-torsor over $G''$.

**Proof.** First, the exactness of

$$
0 \longrightarrow \hat{G}''(k) \longrightarrow \hat{G}(k) \longrightarrow \hat{G}'(k)
$$

(where all of the maps are the obvious ones) is clear. (Just use the fact that $G^{''} = G/G'$, together with the universal property of quotients.) We have the Čech-to-derived functor spectral sequence for the fppf cover $G/G''$ with coefficients in $G_m$:

$$
\tilde{H}^p(G/G'', \mathcal{H}^q(G_m)) \Rightarrow H^{p+q}(G'', G_m)
$$

Here $\mathcal{H}^q$ denotes the $q$th cohomology presheaf, and the cohomology may be taken to be either fppf or étale, by [BrIII Th. 11.7]. This yields an exact sequence

$$
0 \longrightarrow \tilde{H}^1(G/G'', G_m) \longrightarrow \text{Pic}(G'') \longrightarrow \tilde{H}^0(G/G'', \text{Pic})
$$

(3.1)
Since we have an injection \( \check{H}^0(G/G''', \text{Pic}) \hookrightarrow \text{Pic}(G) \), the lemma will follow immediately if we prove that we have an exact sequence

\[
\check{G}(k) \rightarrow \check{G}''(k) \xrightarrow{\phi} \check{H}^1(G/G''', G_m) \rightarrow 0
\]

(3.2)

We first note that the isomorphisms \( G \times \check{G}' \simeq G \times G'/G \) and \( G \times G' \times \check{G}' \simeq G \times G'/G \times G'' G \) defined by \( (g, \alpha) \mapsto (g, \alpha g) \) and \( (g, \alpha_1, \alpha_2) \mapsto (g, \alpha_1 g, \alpha_2 \alpha_1 g) \), respectively, identify the Čech 1-cocycles (with \( G_m \) coefficients) with the set of \( f \in k[G \times G']^* \) such that

\[
f(\alpha_1 g, \alpha_2) f(g, \alpha_1) = f(g, \alpha_2 \alpha_1)
\]

(3.3)

functorially in \( g \in G(R), \alpha_i \in G'(R) \) for \( k \)-algebras \( R \). Now the map \( \phi \) in (3.2) is defined by

\[
\phi(\chi)(g, \alpha) := \chi(\alpha)
\]

First we check that a character \( \chi \in \check{G}''(k) \) lies in ker\( (\phi) \) if and only if it extends to a character in \( G(k) \). We have that \( \phi(\chi) = 0 \) (as an element of \( \check{H}^1(G/G''', G_m) \)) precisely when there exists \( f \in k[G]^* \) such that

\[
\chi(\alpha) = f(\alpha g)/f(g)
\]

for all \( \alpha \in G'(R), g \in G(R) \), functorially in \( R \) (The differential map from \( k[G]^* \) to \( k[G \times G']^* \) is simply \( f \mapsto h(g, \alpha) := f(g \alpha)/f(\alpha) \). But multiplying \( f \) by an element of \( k^* \), we may assume that \( f(1) = 1 \). Since \( G \) is smooth and connected, an application of Rosenlicht’s Unit Theorem \[\text{Con}2\] Cor. 1.2 then implies that \( f \in \check{G}(k) \) is a character. Thus, \( f(\alpha g)/f(g) = f(\alpha) \). In other words, \( \phi(\chi) = 0 \) precisely when there exists \( f \in \check{G}(k) \) such that \( f(\alpha) = \chi(\alpha) \) for \( \alpha \in G'(R) \); that is, when \( \chi \) extends to a character in \( \check{G}(k) \).

So all that remains to prove the first assertion of the lemma is to show that the map \( \phi \) is surjective. We treat the two cases (i) and (ii) separately.

(i) Suppose that we have \( f \in k[G \times G']^* \) satisfying (3.3). We want to show that \( f(g, \alpha) = \chi(\alpha) \) for a character \( \chi \in \check{G}'(k) \). By Rosenlicht’s Unit Theorem, we may write \( f = f_{G'} f_{G} \) for some \( f_{G'} \in k[G]^*, f_{G} \in k[G'']^* \). Multiplying \( f_{G'} \) by \( 1/\lambda \) and \( f_{G} \) by \( \lambda \), where \( \lambda = f_{G'}(1) \), we may assume that \( f_{G'}(1) = 1 \), hence \( f_{G'} \) is a character. Plugging this into (3.3) then gives \( f_{G}(\alpha_1 g) = 1 \) for all \( \alpha_1 \in G'(R), g \in G(R) \). So \( f_{G} = 1 \), hence \( f = f_{G'} \) is a \( k \)-character of \( G' \), as desired.

(ii) We apply (3.1) to the exact sequence of \( k \)-groups obtained via base change to \( \overline{k} \):

\[
1 \rightarrow G'_k \rightarrow G_k \rightarrow G''_k \rightarrow 1
\]

Since \( \text{Pic}(G''_k) = 0 \) by assumption, this yields

\[
\check{H}^1(G_k/G''_k, G_m) = 0
\]
Therefore, any \( f \in \mathbb{K}[G \times G'] \) satisfying (3.3) is necessarily of the form \( f(g, \alpha) = h(\alpha g)/h(g) \) for some \( h \in \mathbb{K}[G]^* \), and scaling \( h \) by some \( \lambda \in \mathbb{K}^* \), we may assume that \( h(1) = 1 \), hence \( h \) is a character, since \( G_\mathbb{K} \) is smooth and connected. So \( f(g, \alpha) = h(\alpha) \). In particular, \( f \) is independent of \( g \). Now let \( f \in k[G \times G']^* \) be a 1-cocycle. Then considering \( f \) as an element of \( \mathbb{K}[G \times G']^* \), it is still a 1-cocycle, hence must be independent of \( g \), i.e. \( f(g, \alpha) = f(1, \alpha) \) for all \( g \in G(R), \alpha \in G'(R) \). But such equality must therefore hold over \( k \). That is, \( f(g, \alpha) = \chi(\alpha) \) for some \( \chi \in k[G']^* \). Plugging into the cocycle equation (3.3), we find that \( \chi \in \hat{G}'(k) \) is a \( k \)-character, hence the map \( \phi \) is surjective.

**Lemma 3.3.** Suppose that we have a short exact sequence of connected linear algebraic \( k \)-groups

\[
1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1
\]

such that \( G'_{k_s} \) is rational. Then we have a long exact sequence

\[
1 \rightarrow \hat{G}''(k) \rightarrow \hat{G}(k) \rightarrow \hat{G}'(k) \rightarrow \text{Pic}(G'') \rightarrow \text{Pic}(G) \rightarrow \text{Pic}(G') \rightarrow \text{Br}(G'')
\]

Actually, the sequence can be extended further, but the above is all that we will need.

**Proof.** This is [San, Cor. 6.11], except there it is assumed that the groups \( G, G', G'' \) are reductive. In fact, all that is used in the proof is the fact that \( \text{Pic}(G'' \times G) = \text{Pic}(G')^{n} \oplus \text{Pic}(G) \) and \( \text{Br}(G'' \times G) = \text{Br}(G')^{n} \oplus \text{Br}(G) \), which follows from [San, Lem. 6.6] due to our assumption that \( G'_{k_s} \) is rational.

As an application, we will now compute the Picard groups of semisimple groups. First, we need the following well-known proposition.

**Proposition 3.4.** Let \( G \) be a simply connected \( k \)-group. Then \( \text{Pic}(G) = \text{Ext}^1(G, \mathbb{G}_m) = 1 \).

**Proof.** The first equality follows from Lemma 2.2 because \( G_{k_s} \) is rational. Indeed, this rationality may be seen by using the open cell decomposition associated to a maximal torus, which is necessarily split over \( k_s \). It remains to show that \( \text{Ext}^1(G, \mathbb{G}_m) \) is trivial. Suppose that we have a (necessarily central) extension

\[
1 \rightarrow \mathbb{G}_m \rightarrow E \rightarrow G \rightarrow 1
\]

We want to find a section \( G \rightarrow E \). In fact, we will show that \( \mathcal{D}E \rightarrow G \) is an isomorphism. First, since \( G = \mathcal{D}G \), the map \( \mathcal{D}E \rightarrow G \) is surjective. If we show that the kernel \( \mathcal{D}E \cap \mathbb{G}_m \) is finite, then the simple-connectedness of \( G \) implies that it has no finite central covers, hence the kernel is trivial, as desired.

To show the desired finiteness, we may extend scalars and thereby assume that \( k = \overline{k} \). More generally, for any connected linear algebraic group \( H \) over \( k = \overline{k} \) and any central \( \mathbb{G}_m \subset H \), the group scheme \( \mathcal{D}H \cap \mathbb{G}_m \) is finite. Indeed, if \( U \) is the unipotent radical of \( H \), then \( \mathbb{G}_m \hookrightarrow H/U \), so we may replace \( H \) with \( H/U \) and thereby assume that \( H \) is reductive. But then the structure theory of reductive groups immediately implies what we want (since it says that \( \mathcal{D}H \cap T \) is finite, where \( T \subset H \) is the maximal central torus).

\[
\square
\]
The following result is also well-known, but we give a proof here.

**Theorem 3.5.** Let $G$ be a semisimple $k$-group, and consider the exact sequence

$$1 \to \mu \to G^{sc} \overset{\pi}{\to} G \to 1$$

where $\pi$ is the simply connected cover of $G$. Then the induced map $\widehat{\mu}(k) \to \text{Pic}(G)$ is an isomorphism.

As an example, let us compute $\text{Pic}(\text{PSL}_n)$. The simply connected cover of $\text{PSL}_n$ is $\text{SL}_n$, with corresponding exact sequence

$$1 \to \mu_n \to \text{SL}_n \to \text{PSL}_n \to 1$$

hence $\text{Pic}(\text{PSL}_n) = \widehat{\mu}_n(k) = \mathbb{Z}/n\mathbb{Z}$.

**Proof.** By Lemma 3.1 the map $\widehat{\mu}(k) \to \text{Pic}(G)$ is injective. In order to show that it is an isomorphism, therefore, it suffices to show that both groups have the same size. Let $\mu \hookrightarrow C$ be an inclusion into a connected commutative rational linear algebraic group with trivial Pic. (One may even take $C$ to be the product of a split unipotent group and a separable Weil restriction of a split torus.) Let $S$ be the cokernel. Consider the following pushout diagram with exact rows and columns:

$$
\begin{array}{cccc}
1 & \to & \mu & \to & G^{sc} & \to & G & \to & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
C & \to & H & \to & G & \to & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
S & \longrightarrow & S & \longrightarrow & 1 & \longrightarrow & 1
\end{array}
$$

(3.4)

Applying Lemma 3.3 to the middle horizontal sequence in (3.4), and using the fact that $\text{Pic}(C) = 0$, yields

$$|\text{Pic}(G)| = |\text{Pic}(H)||\widehat{C}(k)/\widehat{H}(k)|$$

where the notation $\widehat{C}(k)/\widehat{H}(k)$ simply means $\text{coker}(\widehat{H}(k) \to \widehat{C}(k))$, without any implication about the injectivity of this map (though it is in fact injective). On the other hand, applying Lemma 3.3 and Proposition 3.4 to the middle vertical sequence yields

$$|\text{Pic}(H)| = |\text{Pic}(S)|$$
since $\hat{\mu}(k) = 0$. Finally, $S$ is a connected commutative linear algebraic group, hence $S_k$ is the product of a split torus and a split unipotent group, hence has trivial Pic. We may therefore apply Lemma 3.2(ii) to the first vertical sequence to obtain (since $\text{Pic}(C) = 0$)

$$|\text{Pic}(S)| = |\hat{\mu}(k)/\hat{C}(k)|$$

Putting everything together, we obtain

$$|\text{Pic}(G)| = |\hat{\mu}(k)/\hat{C}(k)| |\hat{C}(k)/\hat{H}(k)|$$

Now we claim that we have an exact sequence

$$0 \longrightarrow \hat{H}(k)/\hat{H}(k) \longrightarrow \hat{\mu}(k) \longrightarrow \hat{\mu}(k)/\hat{C}(k) \longrightarrow 0$$

where all of the maps are the obvious ones. Once we show this, the proof will be complete. Let us first note that the map on the left is well-defined, since the pullback to $\hat{\mu}(k)$ of any element of $\hat{H}(k)$ factors through $\hat{G}(k) = 0$. The only point that is now not entirely clear is exactness on the left. So suppose given $\chi \in \hat{C}(k)$ such that its pullback to $\hat{\mu}(k)$ vanishes. Then diagram (3.4) shows that its pullback to $\text{Ext}^1(G, G_m)$ vanishes, hence $\chi$ extends to an element in $\hat{H}(k)$ by Lemma 3.1.

4 Groups With Finite Pic

If $G, H$ are connected linear algebraic $k$-groups such that $G_k$ is rational, then $\text{Pic}(G \times H) = \text{Pic}(G) \oplus \text{Pic}(H)$ (Lemma 2.2). The goal of this section is to prove the following theorem, which roughly says that in this respect groups with finite Pic behave as if they were rational.

**Theorem 4.1.** Let $G, H$ be connected linear algebraic $k$-groups. Assume that $\text{Pic}(G)$ is finite and that $H(k)$ is Zariski dense in $H$. Then $\text{Pic}(G \times H) = \text{Pic}(G) \oplus \text{Pic}(H)$.

**Corollary 4.2.** Let $G$ be a connected linear algebraic $k$-group such that $G(k)$ is Zariski dense inside $G$. If $\text{Pic}(G)$ is finite, then $\text{Pic}(G \times G) = \text{Pic}(G) \oplus \text{Pic}(G)$. In particular, $\text{Pic}(G) = \text{Ext}^1(G, G_m)$.

**Proof.** This follows immediately from Theorem 4.1 and Lemma 2.1.

The following special cases are worth noting.

**Corollary 4.3.** Assume that $k$ is separably closed. Let $G, H$ be connected linear algebraic $k$-groups such that $\text{Pic}(G)$ is finite. Then $\text{Pic}(G \times H) = \text{Pic}(G) \oplus \text{Pic}(H)$.

**Corollary 4.4.** Assume that $k$ is separably closed. Let $G$ be a connected linear algebraic $k$-group. If $\text{Pic}(G)$ is finite, then $\text{Pic}(G \times G) = \text{Pic}(G) \oplus \text{Pic}(G)$. In particular, $\text{Pic}(G) = \text{Ext}^1(G, G_m)$. 10
Both corollaries follow immediately from the fact that for \( k \) separably closed and \( G \) smooth over \( k \), \( G(k) \) is Zariski dense in \( G \).

The key to the proof of Theorem 4.1 is the following lemma. Below, \( \mathcal{L}_{k'} \) denotes the pullback of \( \mathcal{L} \) to \( \text{Pic}(G_{k'} \times_{k'} H_{k'}) \).

**Lemma 4.5.** Let \( G, H \) be connected linear algebraic \( k \)-groups, and suppose that \( \mathcal{L} \in \text{Pic}(G \times H) \) satisfies the following two conditions:

(i) \( \mathcal{L}_{k'} \) is trivial for some field extension \( k'/k \) such that \( \hat{G}(k')/\hat{G}(k) \) is finite.

(ii) There is \( g \in G(k) \) such that \( \mathcal{L}|_{(g) \times H} = 0 \), and there is a Zariski dense set of rational points \( S_H \subset H(k) \) such that \( \mathcal{L}|_{G \times \{ h \}} = 0 \) for every \( h \in S_H \).

Then \( \mathcal{L} \) is trivial.

Let us assume the above lemma for the moment, and we will show how to deduce Theorem 4.1. Let \( \mathcal{L} \in \text{Pic}(G \times H) \). Since \( \text{Pic}(G) \) is finite, there is a line bundle \( \mathcal{L}_1 \in \text{Pic}(G) \) and a Zariski dense set \( S_H \subset H(k) \) such that \( \mathcal{L}|_{G \times \{ h \}} \simeq \mathcal{L}_1 \) for all \( h \in S_H \). (Here we have made use of the connectedness of \( H \) to conclude that if a finite union of sets of rational points is Zariski dense, then one of the sets is Zariski dense.) Let \( \mathcal{L}_2 := \mathcal{L}|_{\{1\} \times H} \in \text{Pic}(H) \). We have \( \text{Pic}(G_{k_{\text{per}}} \times_{k_{\text{per}}} H_{k_{\text{per}}}) = \text{Pic}(G_{k_{\text{per}}}) \oplus \text{Pic}(H_{k_{\text{per}}}) \) by Lemma 2.2 (since connected linear algebraic groups over \( k \) are rational), so \( (L \otimes p_1^*L_1^{-1} \otimes p_2^*L_2^{-1})_{k_{\text{per}}} \) is trivial. By Lemmas 4.5 (with \( g = 1 \)) and 4.3, therefore, \( \mathcal{L} \simeq p_1^*\mathcal{L}_1 \otimes p_2^*\mathcal{L}_2 \). By restricting to \( G \times \{1\} \) and \( \{1\} \times H \), we see that \( \mathcal{L}_1 \simeq (\mathcal{L}_G) \) and \( \mathcal{L}_2 \simeq (\mathcal{L}_H) \), where \( \mathcal{L}_G := \mathcal{L}|_{G \times \{1\}} \) and \( \mathcal{L}_H := \mathcal{L}|_{\{1\} \times H} \).

Since \( \mathcal{L} \in \text{Pic}(G \times H) \) was arbitrary, this completes the proof of Theorem 4.1. \( \square \)

It remains to prove Lemma 4.5. First we prove the following simple lemma.

**Lemma 4.6.** Let \( X \) be a regular Noetherian affine scheme, and let \( Z \subset X \) be a closed subscheme. Every \( \mathcal{L} \in \text{Pic}(X) \) is of the form \( \mathcal{L} = \mathcal{O}(D) \) for some effective divisor \( D \) on \( X \) not containing \( Z \).

**Proof.** We may assume that \( Z \) is integral. We proceed by induction on \( n = \text{codim}(Z) \), the case \( n = 0 \) being trivial. So assume that \( n > 0 \). There is an irreducible closed subscheme \( Z' \subset X \) of codimension \( n - 1 \) such that \( Z \subset Z' \), and the generic point \( \eta_Z \) of \( Z \) is a regular point of \( Z' \). Indeed, we may take the vanishing locus of \( n - 1 \) elements of a regular system of parameters at \( \eta_Z \), and take \( Z' \) to be the component containing \( Z \). By induction, we have \( \mathcal{L} = \mathcal{O}(D) \), where \( D \) is an effective divisor such that \( \eta_{Z'} \not\in \text{supp}(D) \), with \( \eta_{Z'} \) the generic point of \( Z' \). Since \( \eta_{Z'} \not\in D \), we may restrict \( D \) to \( Z' \) to obtain a divisor (at least in a regular neighborhood of \( \eta_Z \) \( D_{Z'} := D|_{Z'} \). Since \( \eta_Z \) is a regular point of \( Z' \), we may speak of the multiplicity of \( D_{Z'} \) at \( \eta_Z \), call it \( N \). Choose \( \pi_{Z'} \in \Gamma(Z', \mathcal{O}_{Z'}) \) to be a uniformizer at \( \eta_Z \), and let \( \pi \in \Gamma(X, \mathcal{O}_X) \) be an arbitrary lift of \( \pi_{Z'} \). Then \( E := D - \text{div}(\pi^N) \) is a divisor in the same equivalence class as \( D \) whose support doesn’t contain \( Z \) (since this is even true of its restriction to \( Z' \)). The only problem is that \( E \) may not be effective. To remedy this, let \( p_1, \ldots, p_m \subset A := \Gamma(X, \mathcal{O}_X) \) be the codimension one primes appearing with negative
Proof of Lemma 4.6: By Lemma 4.6 there is an effective divisor $D$ on $G \times H$ such that \{g\} × $H \not\subset \text{supp}(D)$. We will abuse notation and also use the notation $D$ for the divisor $D_\alpha$ on $G_\alpha \times H_\alpha$. By assumption, there exists $f \in k'[G \times H]$ such that $\text{div}(f) = D$. By our assumptions, we also have that $f|_{\{g\} \times H} \in k'[H]^* \cdot k[H]$ and $f|_{G_X(h)} \in k'[G]^* \cdot k[G]$ for all $g \in S_G$, $h \in S_H$. Our goal is to show that $\text{div}(F) = D$ for some $F \in k[G \times H]$.

Now $k'[G]^* = k*[\tilde{G}(k')]$ by Rosenlicht’s Unit Theorem. Since $\tilde{G}(k')/\tilde{G}(k)$ is finite, there is some $\chi \in \tilde{G}(k')$ and some Zariski dense subset $S_H' \subset S_H$ such that $f|_{G_X(h)} \in \chi \cdot k*[\tilde{G}(k)]$ for every $h \in S_H'$. (Here we are using the connectedness of $H$.) Thus, dividing $f$ by $\chi \in k[G]^* \subset k*[G \times H]^*$ (via the map $\alpha \mapsto \alpha \otimes 1$), which doesn’t affect $\text{div}(f)$, and renaming $S_H'$ as $S_H$, we may assume that $f|_{G_X(h)} \in k*[G]$ for every $h \in S_H$. Similarly (actually, even more simply), by dividing $f$ by some element of $\tilde{H}(k')$, we may also assume that $f|_{\{g\} \times H} \in k*[H]$. Under these assumptions, I claim that $f \in k*[G \times H]$, which will prove what we want (by taking $F$ above to be some constant multiple of $f$).

First, let’s instead make the assumption that $f|_{G_X(h)} \in k[G]$ for all $h \in S_H$. (So this is stronger in the sense that the fibral functions are in $k[G]$, not $k*[G]$, but weaker in the sense that we are only making this assumption about the $h$ fibers.) We will then show that $f \in k[G \times H]$. To prove this, let $V := k[G \times H]$. We have $f \in k' \otimes_k V = k'[G \times H]$, and we want to show that $f$ actually comes from an element of $V$. By faithfully flat descent, this is equivalent to showing that the images of $f$ under the two projections $V_{k'} \rightarrow V_{k' \otimes_k k'}$ are equal. Consider the difference between these two images; call it $\alpha$. We want to show that $\alpha = 0$. Since $f|_{G_X(h)} \in k[G]$ for every $h \in S_H$, we know that $\alpha|_{G_X(h)} \in V_{k' \otimes_k k'[G_X(h)]} = (k' \otimes_k k'[G])$ is zero. What we must show, therefore, is that any such $\alpha \in V_{k' \otimes_k k'}$ is 0.

Choose a $k'$-basis $\{e_i\}$ of $k'[G]$. Then we may uniquely write $\alpha = \sum e_i \alpha_i$ for some $\alpha_i \in V$, and we have that $\alpha_i|_{G_X(h)} = 0$ for every $i$ and every $h \in S_H$. What we must show, therefore, is that if $A \in V$ is such that each $A|_{G_X(h)}$ (with $h \in S_H$) is 0, then $A = 0$.

For this, choose a $k'$-basis $\{w_i\}$ of $k[G]$. We may write $A = \sum z_i w_i$ for some $z_i \in k[H]$. We know that $z_i(h) = 0$ for every $h \in S_H$. Since $S_H$ is Zariski dense in $H$, this implies that $z_i = 0$. Since this holds for each $w_i$, we see that $A = 0$.

Now we treat the original problem. That is, suppose that $f|_{\{g\} \times H} \in k*[H]$ and $f|_{G_X(h)} \in k*[G]$ for all $h \in S_H$. We want to show that $f \in k*[G \times H]$. By our choice of $D$, $f|_{\{g\} \times H} \neq 0$. Then shrinking $S_H$ if necessary, we have $f(g, h) \neq 0$ for each $h \in S_H$. By hypothesis, there is $\lambda \in k^*$ such that $\lambda^{-1} f|_{\{g\} \times H} \in k[H]$. Replacing $f$ with $f/\lambda$, we then have $f(g, h) \in k^*$ for each $h \in S_H$. Then for each $h \in S_H$, we have $f|_{G_X(h)} \in k*[G]$, but since $f(g, h) \in k^*$, we see that in fact $f \in k[G]$. Now the claim proved in the preceding paragraphs shows that $f \in k[G \times H]$, completing the proof. □
5 \ Ext^1(G, G_m)

In this section we will relate our earlier definition of \ Ext^1(G, G_m) in terms of line bundles to the expected definition in terms of extensions. Since everything works in the generality of arbitrary smooth connected \(k\)-group schemes (rather than just linear algebraic groups), we will work in this greater generality.

Let \(G\) be a smooth connected \(k\)-group scheme. Then we define \ Ext^1(G, G_m) \ to be the set of extensions \(E\) of \(G\) by \(G_m\). That is, \ Ext^1(G, G_m) \ is the set of short exact sequences of \(k\)-group schemes

\[
1 \rightarrow G_m \rightarrow E \rightarrow G \rightarrow 1
\]

where we define two such extensions \(E, E'\) to be equivalent if there is a commutative diagram

\[
\begin{array}{ccc}
1 & \rightarrow & G_m \\
\downarrow & & \downarrow \phi \\
1 & \rightarrow & G_m \\
\end{array}
\begin{array}{ccc}
E & \rightarrow & G \\
\downarrow & & \downarrow \\
E' & \rightarrow & G \\
\end{array}
\rightarrow 1
\]

Note that the map \(\phi\) above is necessarily an isomorphism. It’s easy to see that this is an equivalence relation.

It is important to note that such \(E\) is (smooth and) connected, hence the normal \(G_m\) is necessarily central in \(E\), since conjugation induces a map from the connected group \(E\) to the étale group \(\text{Aut}_{G_m/k}\), which is necessarily constant. (Of course, if this were not the case, then we would simply have defined \ Ext^1(G, G_m) \ to be the set of central extensions of \(G\) by \(G_m\).) This allows us to endow \ Ext^1(G, G_m) \ with the structure of an abelian group in the usual way, via the Baer sum. That is, we take as the sum of \(E, E'\) above the linear algebraic group \((E \times_G E')/G_m\), where \(G_m \hookrightarrow E \times_G E'\) is embedded antidiagonally: \(t \mapsto (t, t^{-1})\). This is normal (even central) in \(E \times_G E'\) because of the centrality of \(G_m\) just mentioned. The above group \((E \times_G E')/G_m\) becomes an extension of \(G\) by \(G_m\) via the obvious maps. It’s easy to check that this operation respects the above equivalence relation, and is commutative and associative. The identity element is given by the trivial extension

\[
1 \rightarrow G_m \rightarrow G_m \times G \rightarrow G \rightarrow 1
\]

and the inverse of (the class of) the extension

\[
1 \rightarrow G_m \xrightarrow{\phi} E \xrightarrow{\psi} G \rightarrow 1
\]

is the (class of) the extension

\[
1 \rightarrow G_m \xrightarrow{\phi^{-1}} E \xrightarrow{\psi} G \rightarrow 1
\]
We will carry out this calculation, since it is not quite immediate, and makes essential use of the centrality of $G_m$. The Baer sum of the two extensions above is given functorially on $k$-algebras $R$ by the group

$$\{(e_1, e_2) \in E(R) \times E(R) | \psi(e_1) = \psi(e_2)\}$$

$$\{(\phi(t), \phi(t)) | t \in G_m(R)\}$$

The isomorphism from the above group to $G_m(R) \times G(R)$ is given by $(e_1, e_2) \mapsto (e_1^{-1} e_2, \psi(e_1))$. It’s easy to check that this is a well-defined, bijective map making the diagram of extensions commute. The only sticky point is to see that it is a homomorphism. That is, we need to check that given pairs $(e_1, e_2), (e_1', e_2') \in E(R) \times E(R)$ such that $\psi(e_1) = \psi(e_2)$ and $\psi(e_1') = \psi(e_2')$, then

$$e_1^{-1} e_2 e_1' e_2' = (e_1 e_1')^{-1} e_2 e_2'$$

or, canceling $e_2'$,

$$e_1^{-1} e_2 e_1' = e_1^{-1} e_2$$

Rearranging, this is equivalent to

$$e_1' = (e_1^{-1} e_2)^{-1} e_1^{-1} (e_1^{-1} e_2)$$

But $\psi(e_1) = \psi(e_2)$, so $e_1^{-1} e_2 \in G_m(R)$, which is central in $E(R)$, hence conjugating $e_1'$ by $e_1^{-1} e_2$ has no effect, so the above equation holds.

Now we have a natural map of abelian groups $\text{Ext}^1(G, G_m) \to \text{Pic}(G)$ defined by simply viewing any extension of $G$ by $G_m$ as an fppf torsor for $G_m$ over $G$. This gives us an element of $H^1(G, G_m) = \text{Pic}(G)$. It’s straightforward to check that this map is a homomorphism. Here is the crucial point, which also explains our earlier definition of $\text{Ext}^1(G, G_m)$ as the set of translation-invariant line bundles.

**Proposition 5.1.** The above map $\text{Ext}^1(G, G_m) \to \text{Pic}(G)$ induces an isomorphism $\text{Ext}^1(G, G_m) \iso \{\mathcal{L} \in \text{Pic}(G) | m^* \mathcal{L} \simeq p_1^* \mathcal{L} \otimes p_2^* \mathcal{L}\}$.

In order to prove this we will define maps in both directions that are inverse to each other. We have already defined the map $\text{Ext}^1(G, G_m) \to \text{Pic}(G)$, but we need to check that it actually lands inside the above set of translation-invariant line bundles. (These are also sometimes called primitive line bundles.) This is a straightforward computation. Given an extension

$$1 \to G_m \xrightarrow{\phi} E \xrightarrow{\psi} G \to 1$$

$m^* E$ (which is in general just a $G_m$-torsor over $G \times G$, not a group extension. It is an extension precisely when $m$ is a homomorphism, which holds precisely when $G$ is commutative.) is defined by the Cartesian diagram

$$\begin{array}{ccc}
m^* E & \longrightarrow & G \times G \\
\downarrow & \square & \downarrow m \\
E & \longrightarrow & G
\end{array}$$

14
Functorially, this is given on $k$-algebras $R$ by
\[
\{(e, g_1, g_2) \in E(R) \times G(R) \times G(R) | \psi(e) = g_1g_2 \}
\]
Similarly, $p_1^*E$ is given by $\{(e, g_1, g_2) \in E(R) \times G(R) \times G(R) | \psi(e) = g_1 \}$, and $p_2^*E$ by $\{(e, g_1, g_2) \in E(R) \times G(R) \times G(R) | \psi(e) = g_2 \}$. Then the Baer sum of these two extensions (which also corresponds to their sum as torsors) is given by
\[
\{(e_1, e_2, g_1, g_2) \in (E \times E \times G \times G)(R) | \psi(e_i) = g_i, i = 1, 2 \}
\]
An isomorphism (of torsors! Recall that $m^*E$ is not an extension.) from $p_1^*E + p_2^*E$ to $m^*E$ is then given by $(e_1, e_2, g_1, g_2) \mapsto (e_1e_2, g_1g_2)$. It’s straightforward to check that this is well-defined, bijective, and respects the torsor structures. This completes the proof that $\text{Ext}^1(G, G_m)$ maps to the primitive elements of $\text{Pic}(G)$.

More interesting is the opposite direction. Given a primitive element of $\text{Pic}(G)$, how do we define an extension of $G$ by $G_m$? The key point is the following lemma.

**Lemma 5.2.** Let $G$ be a smooth connected $k$-group scheme, $f : E \to G$ a primitive fppf $G_m$-torsor over $G$; that is, $m^*E \simeq p_1^*E + p_2^*E$. Fix a point $e \in f^{-1}(1)(k)$. This may then be used to identify $f^{-1}(1)$ with $G_m$ via $t \mapsto t \cdot e$. Then there is a unique structure of $k$-group scheme on $E$ such that the sequence

\[
1 \longrightarrow G_m \longrightarrow E \xrightarrow{f} G \longrightarrow 1
\]

is a short exact sequence of $k$-group schemes.

The exactness is automatic; the real point is that the maps in question are homomorphisms of linear algebraic $k$-groups. Note that there is a point $e \in f^{-1}(1)(k)$ as in the lemma by Hilbert 90.

For the existence of such a group structure on $E$, cf. [C-T], Theorem 4.12. Note that, although he assumes in the statement of the theorem that $G$ is reductive, this is unnecessary. All he ever uses is that the torsor is primitive. Without getting into too many details, the idea of the proof is that the primitivity allows one to construct a map $\phi : E \times E \to E$ lying over $m : G \times G \to G$, and by repeatedly modifying $\phi$ using Rosenlicht’s Unit Theorem, one can arrange that $e$ acts as the identity and that the other group axioms are satisfied.

For a somewhat less abstract reformulation of Lemma 5.2 and the proof of the existence statement than the one given in [C-T], cf. [KKLV], Lemma 4.3.

Now let us give the proof of uniqueness. Suppose that we have one $k$-group scheme structure on $E$ as in Lemma 5.2 given by $m : E \times E \to E$ and $i : E \to E$ (multiplication and inversion). Let $m_2 : E \times E \to E$, $i_2 : E \to E$ be another (with $m_2$ giving the new multiplication and $i_2$ the new inversion). We’ll show that $m_2 = m$ is the old multiplication
on $E$. It then follows that $i_2(a) = a^{-1}$, since $e = m_2(a, i_2(a)) = ai_2(a) \implies i_2(a) = a^{-1}$, functorially for $a \in E(R)$, with $R$ a $k$-algebra. Let

$$h(a, a') := aa'm_2(a, a')^{-1}$$

We first note that $f(h(a, a')) = f(a)f(a')(f(a)f(a'))^{-1} = 1$, because $m, m_2$ lie above multiplication on $G$ and inversion on $E$ lies above inversion on $G$. It follows that $h$ factors through $G_m = f^{-1}(1) \subset E$. So $h$ is a global unit on $E$, hence, by Rosenlicht’s Unit Theorem, there exist $h_1, h_2 \in k[E]^*$ such that

$$h(a, a') = h_1(a)h_2(a')$$

functorially in $a, a' \in E(R)$ for $k$-algebras $R$. Now $h(e, e) = 1$ because $e$ is the identity for both $m, m_2$. Thus, scaling $h_1, h_2$ by $1/1(h_1(e), h_1(e))$, respectively, we may assume that $h_1(e) = h_2(e) = 1$. Now setting $a' = e$ yields $h_1(e) = 1$, using the fact that $e$ is the identity for both $m$ and $m_2$. We similarly obtain $h_2(e) = 1$. This shows that $h = 1$, i.e. $m_2(a, a') = aa'$, as desired.

So associated to a $G_m$-torsor $\mathcal{L}$ over $G$, we have a group extension that is unique up to choice of identity $e \in f^{-1}(1)(k)$. But I claim that two distinct $e_1, e_2 \in f^{-1}(1)(k)$ yield equivalent extensions. Indeed, let $m_1, m_2: E \times E$ and $i_1, i_2: E \to E$ be the multiplication and inversion maps associated to $e_1, e_2$. Let $t_{12}, t_{21} \in G_m(k)$ be the unique elements such that $t_{12} \cdot e_1 = e_2$ and $t_{21} \cdot e_2 = e_1$. Note that $t_{12}t_{21} = 1$. Then we have, for $a, a' \in E(R)$ with $R$ a $k$-algebra,

$$m_2(a, a') = t_{12} \cdot m_1(t_{21} \cdot a, t_{21} \cdot a')$$

$$i_2(a) = t_{12} \cdot i_1(t_{21} \cdot a)$$

Indeed, using the fact that $f$ is $G_m$-invariant, and that $m_1, i_1$ yield a group structure with identity $e_1$ such that $f$ is a homomorphism, one checks that the right sides of the the above two equations define a group structure on $E$ satisfying the same properties, but with identity $e_2$, hence this yields the unique such structure on $E$. Now recall that the map $G_m \to E$ for the group structure with identity $e_1$ is defined by $t \mapsto t \cdot e_1$ functorially for $t \in G_m(R)$, and similarly for $e_2$. Thus, in order to show that the two group operations on $E$ yield equivalent extensions, we need to find a map $\phi: E \to E$ such that $\phi$ is a homomorphism from the $e_1$ structure to the $e_2$ structure, and such that the following diagram commutes

$$
\begin{array}{ccc}
1 & \longrightarrow & G_m \\
\downarrow & & \downarrow \phi \\
1 & \longrightarrow & G_m
\end{array}
\begin{array}{ccc}
t \mapsto t \cdot e_1 & \longrightarrow & E \\
f & \longrightarrow & G \\
t \mapsto t \cdot e_2 & \longrightarrow & E
\end{array}
\longrightarrow 1
$$

Such a map is given by $\phi(a) = t_{12} \cdot a$, as is easily checked. Thus we have associated to any primitive fppf $G_m$-torsor over $G$ a unique extensions class in $\text{Ext}^1(G, G_m)$. This yields our map $\{\mathcal{L} \in \text{Pic}(G)|m^*\mathcal{L} \simeq p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}\} \to \text{Ext}^1(G, G_m)$.
Now that we have defined the maps $\psi_1 : \text{Ext}^1(G, G_m) \to \{ \mathcal{L} \in \text{Pic}(G) | m^* \mathcal{L} \simeq p_1^* \mathcal{L} \otimes p_2^* \mathcal{L} \}$ and $\psi_2 : \{ \mathcal{L} \in \text{Pic}(G) | m^* \mathcal{L} \simeq p_1^* \mathcal{L} \otimes p_2^* \mathcal{L} \} \to \text{Ext}^1(G, G_m)$, checking that they are inverse to one another is a tautology. (We also don’t need to bother to check that $\psi_2$ is a homomorphism, as this is automatic once we check that the maps are inverses.) Indeed, starting with an extension
\[ 1 \longrightarrow G_m \longrightarrow E \overset{f}{\longrightarrow} G \longrightarrow 1 \] (5.1)
$\psi_1(E)$ is simply $E$ considered as a $G_m$-torsor over $G$. Then $\psi_2 \circ \psi_1(E)$ is the extension obtained by choosing some point in $f^{-1}(1)(k)$, say $1 \in E(k)$, and endowing $E$ with its unique group structure such that (5.1) is a short exact sequence of $k$-group schemes, and the first map is $t \mapsto t \cdot 1$. Of course, the group structure that we started with on $E$ does the job, so $\psi_2 \circ \psi_1(E) = E$.

In the other direction, given a $G_m$-torsor $f : E \to G$, $\psi_2(E)$ is the associated group structure on $E$ as above (depending on some choice of identity $e \in f^{-1}(1)(k)$), and $\psi_1 \circ \psi_2(E)$ is then simply the torsor obtained by forgetting the group structure, i.e. $E$. So $\psi_1, \psi_2$ are indeed inverse maps. This completes the proof of Proposition 5.1.

Now let us give one more interpretation of $\text{Ext}^1(G, G_m)$ in the case that $G$ is commutative. In this case $G, G_m$ define abelian sheaves on the fppf site on $\text{Spec}(k)$. Associated to these sheaves, we have the usual derived functor $\text{Ext}^1$, defined as the derived functor of $\text{Hom}(G, \cdot)$ in the category of fppf abelian sheaves, applied to $G_m$. Let us temporarily denote this derived functor $\text{Ext}$ by $\text{Ext}^1_{\text{func}}(G, G_m)$. Alternatively, by the general theory of Ext groups in abelian categories, $\text{Ext}^1_{\text{func}}(G, G_m)$ may be thought of as the set of extensions
\[ 1 \longrightarrow G_m \longrightarrow F \longrightarrow G \longrightarrow 1 \]
where $F$ is merely an abelian fppf sheaf, not necessarily (a priori) a scheme. Then any extension of $k$-group schemes
\[ 1 \longrightarrow G_m \longrightarrow E \longrightarrow G \longrightarrow 1 \]
in particular defines an extension of fppf sheaves. If we show that $E$ is commutative, then this yields a commutative extension of abelian sheaves that splits if and only if it splits as an extension of algebraic $k$-groups (by Yoneda’s Lemma), hence $E$ yields an element of $\text{Ext}^1_{\text{func}}(G, G_m)$. We therefore obtain a canonical injective map $\text{Ext}^1(G, G_m) \hookrightarrow \text{Ext}^1_{\text{func}}(G, G_m)$. So we need to prove this commutativity. Note that this is not immediate; not every extension of $G_a$ by $G_a$ is commutative (there exist non-commutative unipotent groups).

**Lemma 5.3.** Suppose that we have an extension of algebraic groups
\[ 1 \longrightarrow T \longrightarrow E \overset{\pi}{\longrightarrow} G \longrightarrow 1 \]
with $T$ a torus and $G$ smooth connected commutative. Then $E$ is commutative.
Proof. We may extend scalars to $\overline{k}$. Let $T' \subset G$ be the maximal torus. Then $\pi^{-1}(T')$ is an extension of tori, hence itself a torus. We may therefore replace $T$ with $\pi^{-1}(T')$ and thereby assume that $G$ contains no nontrivial torus. By Chevalley’s Theorem, $G$ is an extension of an abelian variety by a unipotent group. In particular, $\hat{G}(k) = 0$, where $\hat{G}(k)$ denotes the set of $k$-homomorphisms $\chi : G \to G_m$.

First note that $T \subset E$ is automatically central. Indeed, conjugation yields a map $E \to \text{Aut}_{T/k}$, and this last is an étale $k$-group scheme, so connectedness of $E$ implies that the map is constant; that is, $T \subset E$ is central. In order to prove the lemma, it suffices to show that for any $e \in E(k)$, conjugation by $e$ is trivial on $E$. Consider the map $f : G \to T$ defined functorially by $f(g) := \tilde{g}e\tilde{g}^{-1}e^{-1}$, where $\tilde{g} \in E$ is a lift of $g \in G$ (more precisely, $\tilde{g} \in E(R), g \in G(R)$ for some $k$-algebra $R$). This lands in $T$ because $G$ is commutative, and it is independent of the choice of $\tilde{g}$ due to the centrality of $T$ in $E$. I claim that $f$ is a homomorphism. Since $\hat{G}(k) = 0$, this will prove that conjugation by $e$ is trivial. Functorially for $g, h \in G(R)$, we have

$$f(gh) = \tilde{g}he(\tilde{gh})^{-1}e^{-1} = \tilde{g}(\tilde{he}^{-1}e^{-1})e\tilde{g}^{-1}e^{-1} = (\tilde{g}e\tilde{g}^{-1}e^{-1})(\tilde{he}^{-1}e^{-1}) = f(g)f(h)$$

where the penultimate inequality comes from the fact that $\tilde{he}^{-1}e^{-1} \in T$ (since $G$ is commutative), hence is central in $E$. \hfill $\Box$

We now have the following convenient result.

**Proposition 5.4.** The above canonical map $\Ext^1(G, G_m) \to \Ext^1_{\text{func}}(G, G_m)$ is an isomorphism.

This follows easily from faithfully flat descent, since an abelian sheaf $E$ that is an extension of $G$ by $G_m$ (as abelian sheaves) trivializes over an fppf cover, and then descent implies that this trivialized bundle together with the various isomorphisms of pullbacks must actually come from a scheme downstairs. We leave the details to the reader.

Almost all of the rest of this paper will be concerned with the proof of the following theorem.

**Theorem 5.5.** Let $k$ be a global field, $G$ a connected linear algebraic $k$-group. Then $\Ext^1(G, G_m)$ is finite.

The significance of Theorem 5.5 from our perspective is that $\Ext^1(G, G_m)$ provides us with a canonical finite subgroup of $\text{Pic}(G)$, even when the latter group is infinite. Of course, the above theorem is only interesting when $\text{char}(k) = p > 0$, that is, when $k$ is a global function field, as $\Ext^1(G, G_m)$ is finite over any perfect field $k$ (Lemma 2.7). We remark that Theorem 5.5 is of a genuinely arithmetic nature; it is not true over arbitrary fields. Indeed, for any imperfect separably closed field $k$, and most non-trivial $k$-forms $U$ of $G_a$, the group $\Ext^1(U, G_m)$ is infinite. The same result holds for local function fields, cf. Proposition 9.6.

Let us also note the following easy consequence of Theorem 5.5.
Theorem 5.6. Let $k$ be a global field, $G$ a smooth connected $k$-group scheme. Then $\text{Ext}^1(G, \mathbb{G}_m)$ is a finitely-generated abelian group.

Proof. First assume that $\text{char}(k) = 0$, i.e. $k$ is a number field. Then Chevalley’s Theorem and Lemma 6.1 in the next section reduce us to the case in which $G$ is either linear algebraic or an abelian variety. The former case follows from Theorem 5.5 (or even the much easier Lemma 2.5). If $G = A$ is an abelian variety, then $\text{Ext}^1(A, \mathbb{G}_m)$ is the set of primitive line bundles on $A$, which equals $\text{Pic}^0(A) = A'(k)$ (cf. [Mum §13]), where $A'$ is the dual abelian variety. The desired result therefore follows from the Mordell-Weil Theorem in this case.

Now suppose that $\text{char}(k) = p > 0$. There is an anti-affine $k$-group $G_{\text{ant}} \triangleleft G$ (anti-affine means that $H^0(G_{\text{ant}}, \mathcal{O}_{G_{\text{ant}}}) = k$) such that $G/G_{\text{ant}}$ is affine, cf. [CGP, Th. A.3.9]. $G_{\text{ant}}$ is necessarily smooth and connected (loc. cit.). It follows from Lemma 6.1 as well as Theorem 5.5, that we may assume that $G$ is anti-affine. By loc. cit., it follows that $G$ is a semi-abelian variety; that is, an extension of an abelian variety by a torus. By Lemma 6.1 and Theorem 5.5, we may assume that $G = A$ is an abelian variety, and the result once again follows from the Mordell-Weil Theorem.

Before moving on, we would like to describe one last result which will be used in future work, and is of interest in its own right.

Proposition 5.7. Let $G$ be a smooth connected group scheme over a field $k$, and let $G'$ be an inner form of $G$. Then the groups $\text{Ext}^1(G, \mathbb{G}_m)$ and $\text{Ext}^1(G', \mathbb{G}_m)$ are canonically isomorphic, the isomorphism depending only upon the cohomology class by which one twists.

Remark 5.8. There is nothing special about $\mathbb{G}_m$, nor about smooth connected groups in Proposition 5.7. Indeed, the proof below shows that for any commutative $k$-group scheme $H$, the group $\text{Ext}_{\text{cent}}(G, H)$ of central extensions of $G$ by $H$ is canonically invariant under inner twist on $G$ (which is only required to be a $k$-group scheme).

First we need the following simple lemma, which will be used to show that the isomorphism is canonical.

Lemma 5.9. Let $G$ be a smooth connected group scheme over a field $k$, and let $g \in G(k)$. Then conjugation by $g$ on $G$ induces the identity map on $\text{Ext}^1(G, \mathbb{G}_m)$.

Proof. Consider an extension $E$ of $G$ by $\mathbb{G}_m$, and pull it back by conjugation by $g$:

$$
\begin{array}{ccccccccc}
1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & E' & \longrightarrow & G & \longrightarrow & 1 \\
& & \| & & \pi' & & \pi & & \\
1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & E & \longrightarrow & G & \longrightarrow & 1 \\
& & \downarrow F & & \xrightarrow{g} & & \downarrow \pi g^{-1} & & \\
& & \square & & 
\end{array}
$$

Since $E'$ is a central extension of $G$, $G$ acts on $E'$ by conjugation. By abuse of notation, we still denote this action using multiplication notation. Then one easily checks that the map $E' \to E$ defined by $e' \mapsto F(g^{-1}e'g)$ is an isomorphism of extensions. 

\[19\]
Proof of Proposition 5.7. Let $\alpha \in H^1(k,G)$, and fix a torsor/cocycle $x$ (whichever language you are more comfortable with, though to go beyond the smooth case as in Remark 5.8, one requires the torsor language, as cocycles no longer apply since fppf and étale cohomology don’t agree in general for non-smooth $G$) representing $G$. Suppose we have an extension
\[ 1 \to G_m \to E \to G \to 1 \tag{5.2} \]
of $G$ by $G_m$. Since the extension is central, $G$ acts on $E$ by conjugation, so we may twist (5.2) by $x$ (see [Ser, Ch.I,§5.3]) to obtain a new sequence
\[ 1 \to G_m \to E_x \to G_x \to 1 \]
This map $\text{Ext}^1(G,G_m) \to \text{Ext}^1(G_x,G_m)$ is easily checked to be a well-defined homomorphism. It is an isomorphism, as may be seen by twisting back from $G_x$ to $G$.

This yields an isomorphism from $\text{Ext}^1(G,G_m)$ to $\text{Ext}^1(G_x,G_m)$, but why is this isomorphism canonical, i.e., independent of the class of $x$? Given another torsor $y$ representing $\alpha$, the groups $G_x$ and $G_y$ are $k$-isomorphic, but noncanonically so. This isomorphism is canonical, however, up to conjugation by a rational point. Such conjugation induces the identity map on $\text{Ext}^1(\cdot,G_m)$, by Lemma 5.9. Hence the isomorphism on Ext groups is independent of the choice of torsor representing $\alpha$.

6 Behavior of $\text{Ext}^1(\cdot,G_m)$ in Exact Sequences

The purpose of this section is to try to understand the behavior of $\text{Ext}^1(\cdot,G_m)$ in exact sequences. These results will allow us to prove Theorem 5.5 by dévissage.

Lemma 6.1. Let $1 \to G' \xrightarrow{i} G \xrightarrow{\pi} G'' \to 1$ be a short exact sequence of smooth connected $k$-group schemes. Then the following complex has finite homology at $\text{Ext}^1(G,G_m)$:
\[ \text{Ext}^1(G'',G_m) \xrightarrow{\pi^*} \text{Ext}^1(G,G_m) \xrightarrow{i^*} \text{Ext}^1(G',G_m) \]
In particular, if $\text{Ext}^1(G',G_m)$ and $\text{Ext}^1(G'',G_m)$ are finite, then so is $\text{Ext}^1(G,G_m)$.

Proof. It’s easy to see that the above sequence is a complex. For the assertion about the homology, we will make use of our interpretation of elements of $\text{Ext}^1$ as line bundles. We have a Šech-to-derived-functor spectral sequence
\[ \tilde{H}^p(G/G'', \mathcal{H}^q(G_m)) \Rightarrow H^{p+q}(G'',G_m) \]
Now consider the following exact sequence of presheaves
\[ 1 \to k^x \to G_m \to U \to 1 \]
where $k^*$ is the constant presheaf associated to $k^*$ and $U$ is simply defined by the above sequence. Then $\check{H}^2(G/G''\times G''\to k^*) = 0$, and $\check{H}^2(G/G'', U) = 0$ by [San, Lem. 6.12] and Rosenlicht’s Unit Theorem. We therefore have $\check{H}^2(G/G''\times G''\to k^*) = 0$. The above spectral sequence therefore yields a surjective map

$$\text{Pic}(G'') \twoheadrightarrow \check{H}^0(G/G'', \text{Pic})$$

But using the isomorphism of $k$-schemes $G \times G' \simeq G \times G''$ given by $(g, g') \mapsto (g, g'g)$, we see that $\check{H}^0(G/G'', \text{Pic}) = \{\mathcal{L} \in \text{Pic}(G)|M^*\mathcal{L} \simeq P^*_1\mathcal{L}\}$, where $M, P_1 : G \times G' \to G$ are the multiplication and projection maps. So any $\mathcal{L} \in \text{Pic}(G)$ such that $M^*\mathcal{L} \simeq P^*_1\mathcal{L}$ is the pullback of a line bundle on $\text{Pic}(G'')$.

Now suppose we’ve given a primitive line bundle $\mathcal{L} \in \text{Ext}^1(G, \mathbf{G}_m)$ such that $\mathcal{L}|_{G'} = 0$. Then since $m^*\mathcal{L} \simeq p_1^*\mathcal{L} \otimes p_2^*\mathcal{L}$, this implies that $M^*\mathcal{L} \simeq P^*_1\mathcal{L}$. Thus, by the previous paragraph, there exists $\mathcal{M} \in \text{Pic}(G'\times G'')$ such that $\pi^*\mathcal{M} \simeq \mathcal{L}$. Further, because $\mathcal{L} \in \text{Ext}^1(G, \mathbf{G}_m)$, this $\mathcal{M}$ satisfies $(\pi \times \pi)^*(m^*\mathcal{M} \otimes p_1^*\mathcal{M}^{-1} \otimes p_2^*\mathcal{M}^{-1}) = 0$, where $\pi \times \pi : G \times G \to G'' \times G''$ is the product of the map $\pi$ with itself. Furthermore, any such $\mathcal{M}$ satisfies $\pi^*\mathcal{M} \in \text{Ext}^1(G, \mathbf{G}_m)$. Summarizing, we have a surjective map

$$\phi^{-1}(\ker(\pi \times \pi)^* : \text{Pic}(G'\times G'') \to \text{Pic}(G \times G)) \twoheadrightarrow \ker(i^* : \text{Ext}^1(G, \mathbf{G}_m) \to \text{Ext}^1(G', \mathbf{G}_m))$$

where $\phi : \text{Pic}(G'') \to \text{Pic}(G'\times G'')$ is the homomorphism $\phi^*\mathcal{M} := m^*\mathcal{M} \otimes p_1^*\mathcal{M}^{-1} \otimes p_2^*\mathcal{M}^{-1}$. Now $\text{Ext}^1(G'', \mathbf{G}_m) = \ker(\phi)$, hence in order to complete the proof that the middle homology of the complex in the lemma is finite, we only need to show that $\ker(\pi \times \pi)^* : \text{Pic}(G'\times G'') \to \text{Pic}(G \times G)$ is finite. But this follows immediately from Lemmas 3.2 and A.1 applied to the exact sequence

$$1 \longrightarrow G' \times G' \longrightarrow G \times G \longrightarrow G'' \times G'' \longrightarrow 1$$

Although we will not need it, we also mention that one can do a little bit better if we assume that $G'(k) = 0$.

**Lemma 6.2.** Let $1 \longrightarrow G' \longrightarrow G \longrightarrow G'' \longrightarrow 1$ be a short exact sequence of smooth connected $k$-group schemes, and suppose that $G'(k) = 0$. Then the following complex is exact:

$$\text{Ext}^1(G'', \mathbf{G}_m) \xrightarrow{\pi^*} \text{Ext}^1(G, \mathbf{G}_m) \xrightarrow{i^*} \text{Ext}^1(G', \mathbf{G}_m)$$

The proof of the above lemma proceeds along the same lines as that of Lemma 6.1, but we use $G(k) = 0$ to conclude, via Lemma 3.2, that the map $\text{Pic}(G'\times G'') \to \text{Pic}(G \times G)$ is injective, hence the $\mathcal{M}$ mapping to a given $\mathcal{L} \in \text{Ext}^1(G, \mathbf{G}_m)$ such that $\mathcal{L}|_{G'} = 0$ is necessarily itself in $\text{Ext}^1(G'', \mathbf{G}_m)$. An alternative proof uses faithfully flat descent to descend the extension of $G$ to one of $G''$. The key point is that automorphisms of extensions
of a $k$-group $H$ by $G_m$ come from elements of $\widehat{H}(k)$ (via $a \mapsto a\chi(f(a))$ for $a \in E(R)$, where $f$ is the map $E \to H$), hence the assumption that $\widehat{G}'(k) = 0$ implies rigidity of extensions of $G''$. This rigidity is used to verify the cocycle condition necessary to descend the affine $G$-scheme $E$ to a scheme over $G''$.

Finally, let us note that we can also do better if we assume that $G'_{k_s}$ is rational.

**Lemma 6.3.** Let $1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$ be a short exact sequence of smooth connected $k$-group schemes, and suppose that $G'_{k_s}$ is rational. Then the sequence

$$0 \rightarrow \widehat{G''}(k) \rightarrow \widehat{G}(k) \rightarrow \widehat{G}'(k) \rightarrow \text{Ext}^1(G'', G_m) \rightarrow \text{Ext}^1(G, G_m) \rightarrow \text{Ext}^1(G', G_m)$$

is exact.

**Proof.** By Lemma 3.3, we only need to show that the map $\widehat{G}'(k) \rightarrow \text{Pic}(G'')$ lands inside $\text{Ext}^1(G'', G_m)$, and that if we have $\mathcal{L} \in \text{Pic}(G'')$ such that $\pi^*\mathcal{L} \in \text{Ext}^1(G, G_m)$, then necessarily $\mathcal{L} \in \text{Ext}^1(G'', G_m)$. The first assertion is clear, using the fact that if $\chi \in \widehat{G}'(k)$, then $m^*\chi = p_1^*\chi + p_2^*\chi$ as maps to $G_m$, because $\chi$ is a character.

For the second, we note that $\# \ker(\text{Pic}(G'' \times G'') \rightarrow \text{Pic}(G \times G)) = \# \ker(\widehat{G}(k) \rightarrow \widehat{G}'(k))^2$, hence the inclusion $p_1^* \otimes p_2^*$ : $\ker(\text{Pic}(G'') \rightarrow \text{Pic}(G)) \times \ker(\text{Pic}(G'' \times G') \rightarrow \text{Pic}(G \times G))$ is an isomorphism. Since $m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1} \in \ker(\text{Pic}(G'' \times G'') \rightarrow \text{Pic}(G \times G))$ by assumption (because $\pi^*\mathcal{L} \in \text{Ext}^1(G, G_m)$), we deduce that $m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1} = p_1^*\mathcal{M}_1 \otimes p_2^*\mathcal{M}_2$ for some $\mathcal{M}_i \in \text{Pic}(G'')$. Restricting to $G'' \times 1$ and $1 \times G''$ shows that in fact $\mathcal{M}_1 = 0$, hence $m^*\mathcal{L} \otimes p_1^*\mathcal{L}^{-1} \otimes p_2^*\mathcal{L}^{-1} = 0$; that is, $\mathcal{L} \in \text{Ext}^1(G'', G_m)$, as desired. \hfill $\Box$

## 7 Pseudo-Semisimple Groups

First we recall some basic definitions. Let $G$ be a connected linear algebraic $k$-group.

The $k$-unipotent radical of $G$, denoted $R_u,k(G)$, is the maximal smooth connected normal unipotent $k$-subgroup of $G$. We say that $G$ is pseudo-reductive if $R_u,k(G) = 1$, and we say that $G$ is pseudo-semisimple if $G$ is pseudo-reductive and perfect, i.e. $G = \mathcal{P}G$, the derived group of $G$.

The goal of this section is to prove Theorem 5.5 for pseudo-semisimple groups over (almost) arbitrary fields.

**Theorem 7.1.** Let $k$ be a field, and assume that $[k : k^2] \leq 2$ if $\text{char}(k) = 2$. Let $G$ be a pseudo-semisimple $k$-group. Then $\text{Pic}(G \times G) = \text{Pic}(G) \oplus \text{Pic}(G)$, and $\text{Pic}(G) = \text{Ext}^1(G, G_m)$ is finite.

There are two separate assertions in the final statement above: that $\text{Pic}(G) = \text{Ext}^1(G, G_m)$, and that $\text{Pic}(G)$ is finite. Note that the extra assumption in characteristic 2 is satisfied by global function fields.
Remark 7.2. The proof of Theorem 7.1 depends upon the structure theory of pseudo-semisimple groups developed in [CGP]. The lack of a sufficiently explicit description of such groups in characteristic 2 when \([\mathbb{k} : \mathbb{k}^2] > 2\) is the reason for the extra assumption in Theorem 7.1 in characteristic 2. I do not know if Theorem 7.1 holds in general in characteristic 2 without this extra assumption.

The result that we need, which we will deduce from the structure theory just mentioned, is the following:

**Lemma 7.3.** Let \(\mathbb{k}\) be a field, and assume that \([\mathbb{k} : \mathbb{k}^2] \leq 2\) if \(\text{char}(\mathbb{k}) = 2\). Let \(G\) be a pseudo-semisimple \(\mathbb{k}\)-group. Then there are \(\mathbb{k}\)-group schemes \(B, H', R\) satisfying the following properties: \(H'_k, R\) are smooth, connected, and rational; \(R\) is commutative; \(\text{Pic}(R) = 0\); there is an embedding \(\phi : B \hookrightarrow R\); and there is an exact sequence

\[
1 \longrightarrow B \xrightarrow{\psi} H' \longrightarrow G \longrightarrow 1
\]

Let us assume the above lemma for the moment, and we will show how to deduce Theorem 7.1. We will establish the finiteness of \(\text{Pic}(G)\) and the equality \(\text{Pic}(G \times G) = \text{Pic}(G) \oplus \text{Pic}(G)\) together. This latter equality will also imply that \(\text{Pic}(G) = \text{Ext}^1(G, \mathbb{G}_m)\), by Lemma 2.1. We have the antidiagonal embedding \(B \hookrightarrow H' \times R\) defined via \(b \mapsto (\psi(b), \phi(b)^{-1})\). Let \(H := (H' \times R)/B\), and let \(S := R/B\). Consider the following pushout diagram in which all sequences are exact:

\[
\begin{array}{ccc}
1 & \longrightarrow & B & \longrightarrow & H' & \longrightarrow & G & \longrightarrow & 1 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \longrightarrow & R & \longrightarrow & H & \longrightarrow & G & \longrightarrow & 1 \\
& & S & & S & & S & & S \\
\end{array}
\]

First we establish that \(\text{Pic}(S)\) is finite and that

\[
\text{Pic}(S \times S) = \text{Pic}(S) \oplus \text{Pic}(S)
\]  \hspace{1cm} (7.1)

Since \(R\) is commutative, \(S\) is smooth connected commutative, hence \(\text{Pic} (S_k) = 0\). (It is a product of \(\mathbb{G}_m^n\) and \(\mathbb{A}^r\) for some \(n, r\).) By Lemma 3.2 and the fact that \(\text{Pic}(R) = 0\), we therefore have an exact sequence

\[
\widehat{R}(k) \longrightarrow \widehat{B}(k) \longrightarrow \text{Pic}(S) \longrightarrow 0
\]

so by Lemma A.1, \(\text{Pic}(S)\) is finite. As for (7.1), we have, again by Lemma 3.2 a commutative diagram with exact rows

\[
\begin{array}{ccc}
\widehat{B}(k) \times \widehat{B}(k) & \longrightarrow & \text{Pic}(S) \oplus \text{Pic}(S) & \longrightarrow & 0 \\
\downarrow & & \downarrow \alpha_S & & \\
\widehat{B} \times \widehat{B}(k) & \longrightarrow & \text{Pic}(S \times S) & \longrightarrow & 0 \\
\end{array}
\]

23
where the zeroes come from the fact $\text{Pic}(R) = 0$ and $\text{Pic}(R \times R) = \text{Pic}(R) \oplus \text{Pic}(R) = 0$, with the first equality following from the fact that $R_{k_s}$ is rational (Lemma 2.2). It follows that $\alpha_S$ is an isomorphism; that is, $\text{Pic}(S \times S) = \text{Pic}(S) \oplus \text{Pic}(S)$.

Next we check that $\text{Pic}(H)$ is finite and that

$$\text{Pic}(H \times H) = \text{Pic}(H) \oplus \text{Pic}(H)$$

Indeed, since $H'_{k_s}$ is rational, Lemma 3.3 implies that we have an exact sequence

$$\text{Pic}(S) \longrightarrow \text{Pic}(H) \longrightarrow \text{Pic}(H')$$

so the finiteness of $\text{Pic}(H)$ follows from the already established finiteness of $\text{Pic}(S)$ and the finiteness of $\text{Pic}(H')$ (Lemma 2.5). Now Lemma 3.3 again implies that we have a commutative diagram with exact rows

$$\begin{array}{cccccc}
\text{Pic}(S) \oplus \text{Pic}(S) & \longrightarrow & \text{Pic}(H) \oplus \text{Pic}(H) & \longrightarrow & \text{Pic}(H') \oplus \text{Pic}(H') & \longrightarrow & \text{Br}(S) \oplus \text{Br}(S) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\text{Pic}(S \times S) & \longrightarrow & \text{Pic}(H \times H) & \longrightarrow & \text{Pic}(H' \times H') & \longrightarrow & \text{Br}(S \times S)
\end{array}$$

The isomorphism in the third column is because $H'_{k_s}$ is rational (Lemma 2.2), and the map $\gamma$ is the one induced on each component by pullback along the corresponding projection. This map is injective for the same reason that $\text{Pic}(S) \oplus \text{Pic}(S) \rightarrow \text{Pic}(S \times S)$ is: Restriction to $\{1\} \times S$ and $S \times \{1\}$ shows that if $\gamma(x) = 0$, then $x = 0$. A simple diagram chase now shows that $\text{Pic}(H \times H) = \text{Pic}(H) \oplus \text{Pic}(H)$.

Finally, we check that $\text{Pic}(G)$ is finite and that

$$\text{Pic}(G \times G) = \text{Pic}(G) \oplus \text{Pic}(G)$$

Since $R_{k_s}$ is rational, Lemma 3.3 furnishes an exact sequence

$$\hat{H}(k) \longrightarrow \hat{R}(k) \longrightarrow \text{Pic}(G) \longrightarrow \text{Pic}(H)$$

so Lemma A.1 and the already established finiteness of $\text{Pic}(H)$ imply that $\text{Pic}(G)$ is finite. Now Lemma 3.3 again yields a commutative diagram with exact rows

$$\begin{array}{cccccc}
\hat{R}(k) \times \hat{R}(k) & \longrightarrow & \text{Pic}(G) \oplus \text{Pic}(G) & \longrightarrow & \text{Pic}(H) \oplus \text{Pic}(H) & \longrightarrow & \text{Pic}(R) \oplus \text{Pic}(R) \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\hat{R} \times \hat{R}(k) & \longrightarrow & \text{Pic}(G \times G) & \longrightarrow & \text{Pic}(H \times H) & \longrightarrow & \text{Pic}(R \times R)
\end{array}$$

A simple diagram chase now yields that $\text{Pic}(G \times G) = \text{Pic}(G) \oplus \text{Pic}(G)$. This completes the proof of Theorem 7.1 modulo Lemma 7.3. \qed
Let us now discuss Lemma 7.3 which is an easy consequence of the structure theory of pseudo-reductive groups developed in [CGP]. By [CGP, Th. 10.2.1], we may write $G = G_1 \times G_2$, where $(G_1)_{k_s}$ has a reduced root system and $G_2$ is totally non-reduced. This latter adjective means that every irreducible component of the root system of $G_2$ is non-reduced, i.e. has some root $\alpha$ such that $2\alpha$ is also a root. $G_2 = 1$ if $\text{char}(k) \neq 2$, so the reader not interested in small characteristics can ignore this case. This decomposition implies that in order to prove Lemma 7.3, we may assume that either $G = G_1$ or $G = G_2$. (If $R_1, R_2$ are the $R$ for $G_1, G_2$, respectively, from Lemma 7.3 then we have $\text{Pic}(R_1 \times R_2) = 0$ by Lemma 2.2)

Let us first treat the case $G = G_1$, i.e. $G_{k_s}$ has reduced root system. Then $G$ is a so-called generalized standard pseudo-reductive group, cf. [CGP, Th. 10.2.1, (2)]. Before describing what this is, we first define basic exotic pseudo-reductive groups. (This discussion can be skipped by the reader uninterested in small characteristics, as these groups only show up in characteristics 2 and 3.) For more details, cf. [CGP, Chapter 7].

Let $\text{char}(k) = p \in \{2, 3\}$, and let $G$ be an absolutely simple $k$-group such that its Dynkin diagram has an edge of multiplicity $p$. Then there an isogeny, the so-called very special isogeny, $\pi : G \rightarrow \overline{G}$, characterized by the following properties: There is a factorization $G \xrightarrow{\pi} \overline{G} \rightarrow G^{(p)}$ of the relative Frobenius morphism; $\pi$ is non-central; and $\pi$ admits no nontrivial factorization.

Now suppose that $k'/k$ is an extension such that $k'^p \subset k$, and let $G'$ be an absolutely simple $k'$-group such that its Dynkin diagram has an edge of multiplicity $p$. Let $\pi : G' \rightarrow \overline{G}'$ be the very special isogeny, and let $f = R_{k'/k}(\pi) : R_{k'/k}(G') \rightarrow R_{k'/k}(\overline{G}')$. Note that $f$ is not surjective, since its kernel $R_{k'/k}(\ker(\pi))$ is positive-dimensional. Suppose that there is a Levi $k$-subgroup $\overline{G} \subset R_{k'/k}(\overline{G}')$, and let $\mathcal{G} := f^{-1}(\overline{G}) \subset R_{k'/k}(G')$. If $\mathcal{G}_{k_s}$ contains a Levi $k_s$-subgroup of $R_{k'/k}(G')$, then $\mathcal{G}$ is called a basic exotic pseudo-reductive group. A crucial point is that in the pseudo-split case, i.e. when $\mathcal{G}$ admits a split maximal torus $T$ contained in the Levi subgroup, the Cartan subgroup $Z_\mathcal{G}(T)$ is commutative, rational, and has trivial Pic. Indeed, the commutativity follows from [CGP, Prop. 1.2.4], and the rationality and triviality of Pic follow from [CGP, Th. 7.2.3(2)], which describes $Z_\mathcal{G}$ (as a $k$-scheme) as a product of $G_m$'s and Weil restrictions thereof.

Now we may define a generalized standard pseudo-semisimple group. Let $k'$ be a finite reduced $k$-algebra (so $k'$ is a product of finite field extensions of $k$), and let $G'$ be a $k'$-group such that each of its fibers is either a simply-connected semisimple group, or a basic exotic pseudo-reductive group. Let $Z_{G'} \subset G'$ be the (scheme-theoretic) center of $G'$, and let $B \subset R_{k'/k}(Z_{G'})$ be a closed $k$-subgroup scheme, and let $G := R_{k'/k}(G')/B$. Such a $G$ is called a generalized standard pseudo-semisimple group. A standard pseudo-semisimple group is the same thing, but without the basic exotic pseudo-reductive fibers. Every pseudo-semisimple group with reduced root system is generalized standard, and in characteristic greater than 3, every such group is even standard.
So let us prove Lemma 7.3 in the generalized standard case. We will take the \( H' \) of the lemma to be \( R_{k'/k}(G') \). This is of course smooth and connected. To check that it’s rational over \( k_s \), we may proceed fiber by fiber on \( G' \), so we may assume that \( k' \) is a field, and \( G' \) is either simply-connected semisimple or basic exotic pseudo-reductive. In the former case, we are done because any semisimple group over a separably closed field is rational, and Weil restriction preserves rationality. In the latter case, we have over a separably closed field the open cell decomposition ([CGP Cor. 3.3.16]), and since each of the root groups is rational ([CGP Prop. 2.3.11]), we see that basic exotic pseudo-reductive groups over separably closed fields are rational. Hence \( H'_{k_s} \) is rational. We of course take \( B \) to be the subgroup \( B \subset R_{k'/k}(Z_{G'}) \) such that \( G = R_{k'/k}(G')/B \). We need to show that there is an embedding \( B \hookrightarrow R \) for some smooth connected commutative \( k \)-group \( R \) with trivial Pic such that \( R_{k_s} \) is rational.

In fact, such an embedding exists for any commutative affine \( k \)-group scheme of finite type. Indeed, first suppose that \( B \) is finite. Then by [Me, II, 3.2.5], there is an inclusion \( B \hookrightarrow C \) with \( C \) smooth, connected, commutative, and affine. For general \( B \), [Ros Lem. 2.1.1] furnishes an exact sequence

\[
0 \rightarrow F \rightarrow B \rightarrow D \rightarrow 0
\]

with \( D \) smooth, connected, and affine. Pushing out by an embedding \( F \hookrightarrow C \) with \( C \) smooth, connected, and affine, we see that \( B \) embeds into a smooth connected affine \( k \)-group. We may therefore assume that \( B \) is smooth and connected. Then \( B_{\overline{k}} \) is the product of a split unipotent \( k \)-group and a split torus, hence the same holds for \( B_{k'} \) for some finite field extension \( k'/k \). Then \( R_{k'/k}(B_{k'}) \) is smooth, connected, commutative, affine, rational, and has trivial Pic. The embedding \( B \hookrightarrow R_{k'/k}(B_{k'}) \) therefore allows us to take \( R := R_{k'/k}(B_{k'}) \).

It remains to treat that case in which \( G \) is totally non-reduced. This only occurs in characteristic 2. For more details than those given here, cf. [CGP Chapter 9]. In this case I claim that \( G_{k_s} \) is rational, so we may take \( B = R = 1 \). To see this, we must first recall a definition. If \( \text{char}(k) = 2 \), then a basic non-reduced pseudo-simple \( k \)-group is an absolutely pseudo-simple \( k \)-group \( G \) such that \( G_{k_s} \) has non-reduced root system, and the minimal field of definition \( k'/k \) for the radical \( \mathfrak{r}(G_{\overline{k}}) \) of \( G_{\overline{k}} \) is a quadratic extension of \( k \). Every totally non-reduced pseudo-reductive \( k \)-group is of the form \( R_{k'/k}(G') \), where \( k' \) is a finite reduced \( k \)-algebra, and the fibers of \( G' \) are basic non-reduced pseudo-simple groups, cf. [CGP Prop. 10.1.4(1)]. It therefore suffices in order to prove the claim to show that basic non-reduced pseudo-simple \( k \)-groups are rational whenever \( k = k_s \). But this follows from the way that such groups are constructed. They contain an open subscheme that is a product of Weil restrictions (from finite extensions) of \( G_{\alpha} \)’s and tori, hence are rational over a separably closed field, cf. [CGP Chapter 9]. This completes the proof of Lemma 7.3. \[\square\]
8 Completing the Proof of Theorem 5.5

We will repeatedly use without comment the fact that if we have a short exact sequence

$$1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$$

of connected linear algebraic $k$-groups, and Theorem 5.5 holds for $G', G''$, then it holds for $G$. This follows from Lemma 6.1.

Let $G$ be a connected linear algebraic $k$-group. If $U := R_{u,k}(G)$ is the $k$-unipotent radical of $G$, then $G' := G/U$ is pseudo-reductive, so we may assume that $G$ is either unipotent or pseudo-reductive. Unipotent groups are solvable, so we may assume that $G$ is either commutative or pseudo-reductive. If $G$ is pseudo-reductive, then $G'/G$ normal in $G$. Since its $k$-unipotent radical is a characteristic subgroup (i.e., it is preserved by all $k$-automorphisms of $G$), $G'/G$ is therefore pseudo-reductive. By [CGP, Prop. 1.2.6], it is also perfect, hence it is pseudo-semisimple. Since $G/G'$ is commutative, we may assume that $G$ is either commutative or pseudo-semisimple. The pseudo-semisimple case is handled by Theorem 7.1, hence we are reduced to the case in which $G$ is commutative.

We could treat this directly, but we prefer to carry the dévissage even further, in order to illustrate where the potential infinitude may come from over general fields. (Note that we have so far not made use of the assumption that $k$ is a global field.) So let $G$ be a connected commutative linear algebraic $k$-group. Let $T \subset G$ be its maximal torus. Then $U := G/T$ is unipotent, so we may assume that $G$ is either a torus or commutative unipotent. In the former case, $G = T$ is split, hence rational, over $k_s$, so we are done by Proposition 2.5.

To handle the unipotent case, we claim that any (smooth connected) unipotent $k$-group $U$ admits a filtration by forms of $G_a$. In fact, this is obvious in characteristic 0, where $U$ is $k$-split (and which is uninteresting anyway, since Theorem 5.5 is only interesting for imperfect fields), so we may assume that char($k$) = $p > 0$. We may assume that $U$ is commutative (as we already may for our purposes), and, since $U$ is killed by some power of $p := \text{char}(k)$, we may even assume that $U$ is killed by $p$, by making use of dimension induction and the exact sequence

$$0 \rightarrow [p]U \rightarrow U \rightarrow U/[p]U \rightarrow 0$$

where $[p] : U \rightarrow U$ is the multiplication by $p$ map. By [CGP, Lem. B.1.10], there is a finite étale $k$-subgroup $E \subset U$ such that $U := U/E$ is split unipotent. Let $\pi : U \rightarrow \overline{U}$ denote the quotient map. Since $U$ is split, there is a filtration $0 = \overline{U}_0 \subset \overline{U}_1 \subset \ldots \overline{U}_n = \overline{U}$ with $\overline{U}_{i+1}/\overline{U}_i \simeq G_a$. Let $U_i := \pi^{-1}(\overline{U}_i)^0$. Then $U_i$ is smooth connected unipotent of dimension $i$, so $U_{i+1}/U_i$ is a $k$-form of $G_a$. This proves our claim.

In order to prove Theorem 5.5 therefore, we are reduced to the case when $G = U$ is a $k$-form of $G_a$. The whole point of this discussion was to show that for any field $k$, Theorem 5.5 holds for $k$ if and only if it holds for all $k$-forms of $G_a$.

Now Theorem 5.5 does not hold for every field $k$. In fact, it fails over every imperfect separably closed field and every local function field by Proposition 9.6 below, so we have to
use special properties of global function fields. These will come from Tate duality for positive
dimensional groups \cite{Ros}. Before turning to this, however, we need one more observation. By Proposition 5.4, 
\[
\text{Ext}^1(U, \mathbb{G}_m) \ 	ext{may be interpreted as the usual derived functor Ext. Then}
\]
\cite{Ros, Cor. 2.2.9} says that we have a natural isomorphism 
\[
H^1(k, \hat{U}) \cong \text{Ext}^1(U, \mathbb{G}_m),
\]
where \(\hat{U}\) denotes the fppf dual sheaf \(\text{Hom}(U, \mathbb{G}_m)\). So we need to show that if \(k\) is a global 
function field, then the group 
\[
H^1(k, \hat{U})
\]
is finite for any \(k\)-form \(U\) of \(\mathbb{G}_a\).

For an abelian group \(B\), let \(B^\ast := \text{Hom}(B, \mathbb{Q}/\mathbb{Z})\) denote the \(\mathbb{Q}/\mathbb{Z}\) dual group. Tate
duality \cite{Ros, Th. 1.2.8} furnishes an exact sequence 
\[
H^1(k, U) \rightarrow H^1(A, U) \rightarrow H^1(k, \hat{U})^\ast \rightarrow H^2(k, U)
\]
Since \(U\) is unipotent, \(H^2(k, U) = 0\) \cite{Ros, Lem. 2.4.4}. Also, since \(U\) is smooth and con-
ected, the natural map 
\[
H^1(A, U) \rightarrow \prod_v H^1(k_v, U)
\]
identifies 
\[
H^1(A, U)
\]
with 
\[
\bigoplus_v H^1(k_v, U)
\]
\cite{Ros, Prop. 6.1.1}. We therefore need to show that the map 
\[
H^1(k, U) \rightarrow \bigoplus_v H^1(k_v, U)
\]
has finite cokernel. This is \cite{Oes, Chap. IV, §2.6, Prop.(b)]. This completes the proof of
Theorem 5.5.

9 Forms of \(\mathbb{G}_a\)

The main thrust of the discussion in this section concerns forms of \(\mathbb{G}_a\), but we also use
these groups to construct examples of various types of pathological behavior. First we turn
to the study of Picard groups of forms of \(\mathbb{G}_a\).

**Definition 9.1.** Let \(k\) be a field, \(U\) a \(k\)-form of \(\mathbb{G}_a\). Let \(C\) be the regular compactification
of \(U\). That is, \(C\) is the unique regular proper curve over \(k\) equipped with an open embedding
\(U \hookrightarrow C\) with dense image. Then we define the genus of \(U\) to be the arithmetic genus
\(h^1(C, \mathcal{O}_C)\) of \(C\).

Since \(C\) is proper, its Picard functor \(\text{Pic}_{C/k}\) is representable by a locally finite type
\(k\)-group scheme. We will use this group scheme to study the Picard group of \(U\).

**Proposition 9.2.** Let \(U\) be a \(k\)-form of \(\mathbb{G}_a\). Then the Jacobian \(\text{Jac}(C) := \text{Pic}_C^0\) is a
smooth connected commutative wound unipotent \(k\)-group of dimension equal to the genus of
\(U\).

**Proof.** The group \(\text{Jac}(C)\) is connected by definition, and clearly commutative. It is smooth
of dimension equal to the arithmetic genus of \(C\), as holds for any curve, by cohomological
considerations. The only thing that has to be checked, therefore, is that \(\text{Jac}(C)\) is wound
unipotent. We first check that it is unipotent.

I claim that the restriction map \(\text{Pic}_C^0(C) \rightarrow \text{Pic}(U)\) is injective. Indeed, any line bundle
in the kernel is represented by a degree 0 divisor supported on \(C - U\), which I claim consists
of a single closed point. Assuming this claim, it follows that the divisor is 0. To prove the
claim, note that over \(\bar{k}\), we have a dense open embedding \(U_{\bar{k}} \cong \mathbb{G}_a \hookrightarrow C_{\bar{k}}\). This extends to
a surjective map $\mathbf{P}^1 \to C_k$, so since $\mathbf{P}^1 - \mathbf{G}_a$ consists of a single closed point, the same is true of $C - \mathbf{G}_a$.

Now we may show that $\text{Jac}(C)$ is unipotent. For this, we may assume that $k = k_s$, since $C_{k_s}$ is still regular (because étale base change preserves regularity). The preceding paragraph yields an inclusion $\text{Jac}(C)(k) = \text{Pic}^0(C) \hookrightarrow \text{Pic}(U)$. The proof of Proposition 2.8 shows that this last group is $p$-power torsion, since $U$ splits over some finite purely inseparable extension. (Actually, the argument we are about to make also goes through just using the result of that proposition, rather than checking that the proof shows that $\text{Pic}(U)$ is $p$-power torsion.) Since $\text{Jac}(C)$ is smooth and $k = k_s$, $\text{Jac}(C)(k)$ is dense in $\text{Jac}(C)$, so $\text{Jac}(C)$ is $p$-power torsion. The structure theory of smooth connected $k$-group schemes then implies that $\text{Jac}(C)$ is unipotent.

In order to show that $\text{Jac}(C)$ is wound, we need to show that any map of $k$-schemes $\mathbf{A}^1_k \to \text{Jac}(C)$ is constant. Such a map corresponds to an element of $\text{Pic}(C \times \mathbf{A}^1)$.

Proposition 9.3. Let $U$ be a form of $\mathbf{G}_a$ over the field $k$. Let $J$ denote the Jacobian of the regular compactification $C$ of $U$. Then we have an exact sequence

$$0 \to J(k) \to \text{Pic}(U) \xrightarrow{\text{deg}} \mathbb{Z}/p^n \mathbb{Z} \to 0$$

where $p^n$ is the degree of the unique point of $C - U$. Here, the first map is the restriction map $\text{Pic}^0(C) \to \text{Pic}(U)$, and the second is the degree of any divisor representing the divisor.

Proof. It was shown in the proof of Proposition 9.2 that the restriction map $J(k) = \text{Pic}^0(C) \to \text{Pic}(U)$ is injective. It was also shown in that proof that the complement $C - U$ consists of a single closed point. Since this remains true over $k_s$ (and $C_{k_s}$ is still the regular compactification of $U_{k_s}$), it follows that this point is still a single point over $k_s$, hence it becomes rational over a purely inseparable extension of $k$. In particular, it has degree $p^n$ for some nonnegative integer $n$. Then given an element $\mathcal{L} \in \text{Pic}(U)$ represented by some divisor $D$, the degree $\text{deg}(D)$ is independent of $D$ modulo $p^n$, since the difference between two such divisors differs from the divisor of a function on $C$ by a multiple of the point at infinity. So we have a degree map $\text{Pic}(U) \to \mathbb{Z}/p^n \mathbb{Z}$ such that a line bundle on $U$ lifts to a degree-$0$ line bundle on $C$ if and only if it has degree $0$ modulo $p^n$. The degree map is clearly surjective, since the divisor $[0]$ has degree one.

Proposition 9.4. A $k$-form $U$ of $\mathbf{G}_a$ has genus $0$ if and only if it is rational. If $p > 2$, then this holds if and only if $U \simeq \mathbf{G}_a$, while if $p = 2$, then this holds if and only if $U \simeq \mathbf{G}_a$ or $U$ is $k$-isomorphic to the subgroup of $\mathbf{G}_a^2$ given by the equation $Y^2 = X + aX^2$ for some $a \in k - k^2$.

Proof. The group $U$ is a so-called Russell group [KMT §2.6], so the second assertion is [KMT] Th 6.9.2.
If $U$ is rational, then the same holds for its regular compactification $C$. We therefore obtain a finite flat map $\mathbb{P}^1_k \to C$ with generic fiber of degree 1, hence the map is an isomorphism, so $U$ has genus 0. Conversely, suppose that $U$ is a $k$-form of $G_a$ with genus 0, and let $C$ be its regular compactification. Then $0 \in U(k) \subset C(k)$, so $C(k) \neq \emptyset$. Let $Q = C - U$ be the unique closed point of $C$ not contained in $U$. The uniqueness of this point was shown in the proof of Proposition 9.2. In fact, the proof given there even shows that $C_k - U_k$ consists of a single point. It follows that $Q$ becomes rational over a finite purely inseparable extension of $k$. The hypotheses of [KMT, Th. 6.7.9] are therefore satisfied, so the equivalence of conditions (ii) and (iii) in that theorem implies that $C \simeq \mathbb{P}^1_k$. It follows that $U$ is rational.

Consider the action of $U$ on itself by multiplication. We claim that this extends uniquely to an action $U \times C \to C$ of $U$ on $C$. Indeed, $U \times C$ is smooth over $C$, hence regular. In particular, $U \times C$ is reduced and $C$ is separated, so if the action extends, then it extends uniquely. Further, for the same reason, if the multiplication map $U \times U \to U$ extends at all to a map $U \times C \to C$, then that map is a group scheme action of $U$ on $C$.

To show that it extends, we may extend scalars to $k = k_s$ by using Galois descent and the uniqueness of the extension. We note that the regularity of $U \times C$ and the properness of $C$ together imply that the map $U \times U \to U \subset C$ extends to a rational map $\pi : U \times C \dashrightarrow C$ defined away from finitely many closed points of $U \times C$. Since $k = k_s$, we may therefore choose $u_0 \in U(k)$ such that $\pi$ is defined on $u_0 \times C$, and such that the locus on which the maps $\pi(u, c)$ and $\pi(u + u_0, c)$ are not defined are disjoint. Then the map $f(u, c) := \pi(-u_0, \pi(u + u_0, c))$ is defined everywhere that $\pi$ is not, and they agree on $U \times U$, hence on their entire locus of common definition. They therefore glue to give a map $U \times C \to C$ extending the left action $U \times U \to U$. This yields an action $U \times \text{Jac}(C) \to \text{Jac}(C)$.

Now we adapt an idea of Totaro’s from the proof of [Tot, Lem. 9.4]. Consider the unipotent group $N := U \times \text{Jac}(C)$. Consider the sequence of smooth connected $k$-subgroups $P_i \subset \text{Jac}(C)$ defined inductively by $P_0 = \text{Jac}(C)$, and by letting $P_{i+1}$ be the $k$-subgroup generated by the $k_s$-points $u \ast p - p$ for $u \in U(k_s)$ and $p \in P_i(k_s)$. The unipotence of $N$ implies that $P_n = 0$ for some $n$. If $U$ has positive genus, and if we let $n$ be the first such index, then $n > 0$, and $U$ acts trivially on $P_{n-1}$. We therefore deduce the following result.

**Proposition 9.5.** Let $U$ be a $k$-form of $G_a$ of positive genus. Then there is a smooth connected positive-dimensional closed $k$-subgroup scheme $G \subset \text{Jac}(C)$ such that $G(k) \subset \text{Ext}^1(U, G_m)$ via the inclusion $G(k) \subset \text{Jac}(C)(k) = \text{Pic}^0(C) \hookrightarrow \text{Pic}(U)$.

Let us remark that Proposition 9.5 applies to a nonempty set of examples! In fact, there are many examples over any imperfect field $k$ of $k$-forms of $G_a$ of positive genus. First consider the case $p > 2$, let $a \in k - k^p$, and let $U := \{y^p = x + ax^p\} \subset G_a^2$. Then the regular compactification of $U$ is the curve $C := \{y^p = xz^{p-1} + ax^p\} \subset \mathbb{P}^2_k$, which has genus $(p-1)^2 > 0$. 

30
Now suppose that \( p = 2 \). Then we take \( U := \{ y^{p^2} = x + ax^2 \} \), where once again \( a \in k - k^p \). Then the regular compactification of \( U \) is \( C := \{ y^{p^2} = x^2 + ax^2 \} \), which has genus \( \left( \frac{p^2 - 1}{2} \right) \) > 0. Note that this example also works for \( p > 2 \), but we wanted to give as simple an example as possible in each case.

As an immediate consequence of Proposition \[9.5\] we obtain the following result.

**Proposition 9.6.** Let \( k \) be an imperfect separably closed field, or a local function field. Then \( \text{Ext}^1(U, \mathbb{G}_m) \) is finite if and only if \( U \simeq \mathbb{G}_a \), or \( p = 2 \) and \( U \simeq \{ Y^2 = X + aX^2 \} \) for some \( a \in k - k^2 \).

**Remark 9.7.** Proposition \[9.6\] shows that Theorem \[5.5\] is not true over any imperfect separably closed field or any local function field.

**Proof.** The proposition is saying that \( \text{Ext}^1(U, \mathbb{G}_m) \) is finite if and only if \( U \) is rational. First, suppose that \( U \) is rational. Then \( U \) has genus 0, so if \( C \) is the regular compactification of \( U \), then \( \text{Pic}^0(C) = 0 \). Let \( Q \) be the unique (closed) point of \( C - U \), and let \( m := \text{deg}(Q) \).

Then we have an exact sequence

\[
\text{Pic}^0(C) \rightarrow \text{Pic}(U) \xrightarrow{\text{deg}} \mathbb{Z}/m\mathbb{Z}
\]

Indeed, an element of \( \text{Pic}(U) \) extends to an element of \( \text{Pic}^0(C) \) if and only if its degree is a multiple of \( m \). Since \( \text{Pic}^0(C) = 0 \), the finiteness of \( \text{Pic}(U) \), hence also that of \( \text{Ext}^1(U, \mathbb{G}_m) \), follows.

Next suppose that \( U \) is not rational. By Proposition \[9.4\] \( \text{Jac}(C) \) is then positive-dimensional. Choosing \( G \) as in Proposition \[9.5\] we see that it suffices to show that any smooth \( k \)-group scheme \( G \) of positive dimension has infinitely many rational points. This is true when \( k = k_s \), since then \( G(k) \) is Zariski dense in \( G \), and when \( k \) is a local function field, since then \( G(k) \) is a positive-dimensional Lie group over \( k \).

**Proposition 9.8.** Let \( U \) be a one-dimensional smooth connected unipotent group over a field \( k \) (i.e., a \( k \)-form of \( \mathbb{G}_a \)). Then \( \text{Pic}(U) = \text{Ext}^1(U, \mathbb{G}_m) \) if and only if \( U \simeq \mathbb{G}_a \) or \( p = 2 \) and \( U \) is \( k \)-isomorphic to a group of the form \( \{ Y^2 = X + aX^2 \} \subset \mathbb{G}_a \times \mathbb{G}_a \) for some \( a \in k - k^2 \).

**Proof.** By Proposition \[9.4\] the proposition is the same as saying that \( \text{Pic}(U) = \text{Ext}^1(U, \mathbb{G}_m) \) if and only if \( U \) has genus 0. First suppose that \( U \) has genus 0. We want to prove that \( \text{Pic}(U) = \text{Ext}^1(U, \mathbb{G}_m) \). It suffices to check this after extending scalars to \( k_s \), since this preserves the genus of \( U \). But then \( J = 0 \) by Proposition \[9.2\] so \( \text{Pic}(U) \) is finite by Proposition \[9.3\]. By Corollary \[1.4\] therefore, \( \text{Pic}(U) = \text{Ext}^1(U, \mathbb{G}_m) \).

Conversely, suppose that \( U \) has positive genus. We claim that the line bundle \( \mathcal{L} := \mathcal{O}(0) \) corresponding to the divisor \( 0 \in U(k) \) is not in \( \text{Ext}^1(U, \mathbb{G}_m) \). This may be checked after extending scalars to \( k_s \). Since \( U_{k_s} \) has the same genus as \( U \), we may assume that \( k = k_s \). In particular, \( U(k) \neq \{ 0 \} \). For any \( 0 \neq u \in U(k) \), I claim that \( T_u \mathcal{L} \not\simeq \mathcal{L} \), where
$T_u : U \to U$ is translation by $u$. This would show that $\mathcal{L}$ is not translation-invariant, hence not in $\text{Ext}^1(U, \mathbf{G}_m)$. To prove the claim, we need to show that the divisors $[0]$ and $[-u]$ are not linearly equivalent. But a function $f$ on $U$ with divisor $[0] - [-u]$ would yield a map $f : U \to \mathbf{P}^1_k$ such that $f^{-1}(0) = [0]$ and $f^{-1}(\infty) = [-u]$ scheme-theoretically. Since $C$ is regular, this extends to a map $\mathcal{f} : C \to \mathbf{P}^1_k$, which still has divisor $[0] - [-u]$, since $\deg(\text{div}(\mathcal{f})) = 0$, and $C - U$ consists of a single closed point. Then $\mathcal{f}$ has degree one, hence is an isomorphism, which violates our assumption that $U$ has positive genus. \hfill \Box

We now give examples of of various pathologies.

Example 9.9. Let $U$ be a $k$-form of $\mathbf{G}_a$ such that $\text{Pic}(U)$ is infinite. Proposition 9.6 provides such examples over every local function field and every imperfect separably closed field. We will use $U$ to construct a commutative pseudo-reductive $k$-group with infinite Picard group.

The group $U$ is $k$-wound, because it has infinite Picard group. By [104, Cor. 9.5], there is a (smooth connected) commutative pseudo-reductive $k$-group $G$ such that we have an exact sequence

$$1 \to T \to G \to U \to 1$$

with $T$ the maximal torus of $G$. I claim that $\text{Pic}(G)$ is infinite. Indeed, by Lemma 3.2 we have an exact sequence

$$\hat{G}(k) \to \hat{T}(k) \to \text{Pic}(U) \to \text{Pic}(G)$$

Since $\text{coker}(\hat{G}(k) \to \hat{T}(k))$ is finite (Lemma A.1), and $\text{Pic}(U)$ is infinite, we must have that $\text{Pic}(G)$ is infinite, as claimed.

Example 9.10. Let us construct an example to show that the hypothesis that $G(k)$ is Zariski dense in $G$ is necessary in Corollary 4.2 and therefore the corresponding hypothesis for $H$ is necessary in Theorem 4.1.

By Propositions 9.8 and 9.9, we may construct a $k$-form $U$ of $\mathbf{G}_a$ such that $\text{Pic}(U)$ is finite but not equal to $\text{Ext}^1(U, \mathbf{G}_m)$. Indeed, $J(k)$ is finite but not equal to $\text{Ext}^1(U, \mathbf{G}_m)$ is the same as giving such a form of positive genus but such that $J(k)$ is finite.

If $k$ is an arbitrary imperfect field of characteristic greater than 2, then there may not exist such $U$. For example, if $k$ is an imperfect separably closed field, then $J(k)$ must be infinite if $J \neq 0$. The same holds if $k$ is a local function field, because $J(k)$ is a positive-dimensional Lie group over $k$.

But let $k$ be a global function field, and $U$ a wound $k$-form of $\mathbf{G}_a$ such that the genus $g$ of $U$ satisfies $0 < g < p - 1$. Then we claim that $J(k)$ is finite, and so $\text{Pic}(U)$ is finite but not equal to $\text{Ext}^1(U, \mathbf{G}_m)$. Indeed, $J$ is a wound unipotent group of dimension $g < p - 1$ by Proposition 9.2, so by [Oes, Ch. VI, §3.1, Th.], $J(k)$ is finite. Here is an example when $\text{char}(k) = 3$. Consider the group $U := \{Y^3 = X + aX^3\} \subset \mathbf{G}_a \times \mathbf{G}_a$ with $a \in k - k^3$. Then one may check as before that the projectivization $\{Y^3 = XZ^2 + aX^3\} \subset \mathbf{P}^2_k$ is regular, hence yields the regular compactification of $U$. Further, one may compute its genus to be $1 < 3 - 1$.
Let us give some applications to the cohomology of local and global fields; in particular, we will show that certain pathologies occur over such fields. Recall that if $k$ is a local field of characteristic $0$, then for any affine commutative $k$-group scheme $G$ of finite type, the group $H^1(k, G)$ is finite. This is completely false over local function fields, e.g., for $G = \alpha_p$, $\mu_p$, or $\mathbb{Z}/p\mathbb{Z}$. But one would like to give smooth connected examples. In fact, the following proposition provides a plethora of such examples.

**Proposition 9.11.** Let $k$ be a local function field, $G$ a connected commutative linear algebraic $k$-group. Then $H^1(k, G)$ is infinite if and only if $\text{Ext}^1_k(G, G_m)$ is infinite. In particular, if $U$ is a $k$-form of $G_a$, then $H^1(k, U)$ is finite if and only if $U \cong G_a$ or $p = 2$ and $U \cong \{ Y^2 = X + aX^2 \}$ for some $a \in k - k^2$.

**Proof.** The second assertion follows from the first and Proposition 9.6. To prove the first assertion, we use the fact that local Tate duality implies that the groups $H^1(k, G)$ and $H^1(k, \hat{G})$ are Pontryagin dual [Ros, Th. 1.2.4], so one is finite if and only if the other is. The proposition therefore follows from the isomorphism $H^1(k, \hat{G}) \cong \text{Ext}^1_k(G, G_m)$ [Ros, Cor. 2.2.9] (and the fact that the functorial Ext and our Ext agree in this setting, by Proposition 5.4).

Let $G$ be a group scheme over a global field $k$, and let $S$ be a finite set of places of $k$. Then we define the pointed set $\Pi_S(G)$ (often also denoted $\Pi^1_S(G)$) in the usual manner:

$$\Pi_S(G) := \ker \left( H^1(k, G) \to \prod_{v \in S} H^1(k_v, G) \right)$$

If $k$ is a number field, then this set is finite for any affine $k$-group scheme of finite type. This also holds in the function field setting if $S = \emptyset$ [Con, Th. 1.3.3(i)]. It is not generally true, however, for nonempty $S$ (contrary to the original version of [Con, Th. 1.3.3(i)]), as we show in Corollary 9.14 below.

**Remark 9.12.** The mistake in the proof of [Con, Th. 1.3.3(i)] creeps in when invoking [Oes, Chap. IV, §2.6, Prop.(a)] at the very end of §6.3 and in the first paragraph of §6.4. In fact, [Oes, Chap. IV, §2.6, Prop.(a)] only asserts the finiteness of $\Pi^1_S(G)$ (for $G$ a smooth affine commutative group over a global function field); that is, it only treats the case $S = \emptyset$. For this reason, all of the arguments in [Con], and especially [Con, Th. 1.3.3(i)], are valid when $S = \emptyset$. But as we are about to show, they fail badly when $S \neq \emptyset$.

**Proposition 9.13.** Let $G$ be a connected commutative linear algebraic group over a global function field $k$, and let $S$ be a finite set of places of $k$. Then the group $\Pi^1_S(G)$ is finite if and only if $\text{Ext}^1_k(G, G_m)$ is finite for all $v \in S$.

**Proof.** Let $A^S$ denote the ring of $S$-adeles, i.e., the subset of $\prod_{v \in S} k_v$ defined by the usual restricted product condition. Then [Ros, Prop. 6.1.1] implies that $\Pi^1_S(G) = \{ \}$. 

33
ker(H^1(k, G) \longrightarrow H^1(A^S, G)). Global Tate duality [Ros, Th. 1.2.8] furnishes an exact sequence
\[ \text{III}^1(G) \longrightarrow \text{III}^1_S(G) \longrightarrow \prod_{v \in S} H^1(k_v, G) \longrightarrow H^1(k, \hat{G})^* \]
where, as before, \( \hat{G} := \text{Hom}(G, \mathbb{G}_m) \) denotes the fppf \( \mathbb{G}_m \)-dual sheaf of \( G \), and for an abelian group \( B, B^* := \text{Hom}(B, \mathbb{Q}/\mathbb{Z}) \). The group \( \text{III}^1(G) \) is finite [Oes, Chap. IV, §2.6, Prop.(a)], and the group \( H^1(k, \hat{G}) \) is isomorphic to \( \text{Ext}^1(G, \mathbb{G}_m) \) [Ros, Cor. 2.2.9], which is also finite, by Theorem 5.5. It follows that \( \text{III}^1_S(G) \) is finite if and only if \( H^1(k_v, G) \) is finite for all \( v \in S \). By Proposition 9.11 these groups are finite if and only if the groups \( \text{Ext}^1_{k_v}(G, \mathbb{G}_m) \) are finite for all \( v \in S \).

The following result shows that, in contrast to the number field setting, the set \( \text{III}^1_S(G) \) can be infinite even for smooth connected affine groups over global function fields if \( S \neq \emptyset \). (This cannot happen if \( S = \emptyset \); see Remark 9.12.)

**Corollary 9.14.** Let \( k \) be a global function field, \( U \) a nontrivial form of \( G_a \) over \( k \). If \( \text{char}(k) = 2 \), then further assume that \( U \) is not isomorphic to a conic in the affine plane (equivalently, by Proposition 9.4, \( U \) has positive genus). Let \( S \) be a nonempty set of places of \( k \). Then \( \text{III}^1_S(U) \) is infinite.

**Proof.** We may assume that \( S \) is finite. Then this is an immediate consequence of Propositions 9.13 and 9.6 together with the fact that the genus of \( U \) (and woundness of \( U \)) is preserved upon passage from \( k \) to \( k_v \), since \( k_v \) is a (non-algebraic) separable extension of \( k \). 

**A Characters**

For a \( k \)-group scheme \( G, \hat{G}(k) \) denotes the group \( \text{Hom}(G, \mathbb{G}_m) \) of characters of \( G \) defined over \( k \). The following result is [Oes, Prop. A.1.4]. We state it here for convenience.

**Lemma A.1.** Let \( G \) be a connected linear algebraic \( k \)-group, and \( H \trianglelefteq G \) a closed normal \( k \)-subgroup scheme. Then the restriction map \( \hat{G}(k) \to \hat{H}(k) \) has finite cokernel.

**Lemma A.2.** If \( G \) is a \( k \)-group scheme of finite type, then \( \hat{G}(k) \) is finitely generated.

**Proof.** We may assume that \( k = \overline{k} \). Given a short exact sequence
\[ 1 \to G' \to G \to G'' \to 1 \]
of finite type \( k \)-group schemes, we get an exact sequence
\[ 0 \to \hat{G}''(k) \to \hat{G}(k) \to \hat{G}'(k) \]
so if the Lemma holds for $G'$ and $G''$, then it holds for $G$. The lemma is clear for finite group schemes, so replacing $G$ with $G^0_{\text{red}}$, we may assume that $G$ is smooth and connected. By Chevalley’s Theorem, we may assume that $G$ is either an abelian variety or a linear algebraic group. In the former case, $\hat{G}(k)$ since $G$ is proper and $G_m$ is affine. In the latter case, we may replace $G$ with $G/\mathcal{P} G$ and thereby assume that $G$ is commutative. Letting $T \subset G$ be the maximal torus, $G/T$ is unipotent and therefore has no nontrivial characters. We may therefore assume that $G = T$ is a torus, and since $k = \overline{k}$, we are reduced to the case $G = G_m$, which is clear.

Let $k_{\text{per}}$ denote the perfect closure of $k$.

**Lemma A.3.** Let $G$ be a $k$-group scheme of finite type. Then $\hat{G}(k_{\text{per}})/\hat{G}(k)$ is finite.

**Proof.** The quotient group is finitely generated by Lemma [A.2] so in order to show that it is finite, it suffices to show that it is torsion. But this is clear: given $\chi \in \hat{G}(k_{\text{per}})$, we have $\chi^{p^n} \in \hat{G}(k)$ for some $n > 0$.

**Lemma A.3** is not true if we replace the extension $k_{\text{per}}/k$ with even arbitrary finite extensions. For example, let $T$ be a $k$-torus with no nontrivial characters over $k$. For example, any nontrivial form of $G_m$ satisfies this, since any isogeny of tori has an isogeny splitting. This may also be seen by noting that the anti-equivalence between tori and Galois lattices (via $T \mapsto \hat{T}(k_s)$) implies that any such $T$ corresponds to a nontrivial action of $\text{Gal}(k_s/k)$ on $\mathbf{Z}$, and any such action has no nonzero fixed elements. At any rate, if $L/k$ is a finite separable extension splitting $T$, then of course $\hat{T}(L)/\hat{T}(k)$ is infinite.

**References**


