Extensions and torsors for finite group schemes

Bruin, P.J.

Available online at www.sciencedirect.com

ScienceDirect

Expositiones Mathematicae 41 (2023) 514–530

EXPOSITIONES MATHEMATICAE

www.elsevier.com/locate/exmath

Extensions and torsors for finite group schemes☆

Peter Bruin

Mathematisch Instituut, Universiteit Leiden, Postbus 9512, 2300 RA Leiden, Netherlands

Received 6 February 2023; accepted 23 February 2023

Dedicated to the memory of Bas Edixhoven, with admiration

Abstract

We give an explicit description of the category of central extensions of a group scheme by a sheaf of Abelian groups. Based on this, we describe a framework for computing with central extensions of finite locally free commutative group schemes, torsors under such group schemes and groups of isomorphism classes of these objects.

MSC: primary 14L15; secondary 14Q25; 11Y40

Keywords: Group schemes; Extensions; Torsors; Algorithms

1. Introduction

Let G be a finite locally free group scheme over a scheme S. We describe the category of central extensions of G by a commutative *fppf* group scheme F affine over S, and for G commutative also the category of G-torsors over S, in a way that is suitable for explicit calculations.

Under certain computational assumptions (which are fulfilled, for example, if K is a number field, S is the spectrum of the ring of Σ-integers in K with Σ a finite set of places of K, and F is itself finite locally free or $F = \mathbf{G}_{\mathrm{m}}$), we give algorithms for computing

- the extension class group $\mathrm{Ext}_S(G, F)$, i.e. the group of isomorphism classes of central extensions of G by F,

☆ This research was partially supported by the Dutch Research Council (NWO/OCW), as part of the Quantum Software Consortium programme (project number 024.003.037).

E-mail address: P.J.Bruin@math.leidenuniv.nl.

https://doi.org/10.1016/j.exmath.2023.02.004

and for commutative G also

- the subgroup of $\mathrm{Ext}_S(G, F)$ classifying commutative extensions, and
- the torsor class group $\mathrm{H}^1(S_{fppf}, G)$, i.e. the group of isomorphism classes of G-torsors over S.

These algorithms ultimately reduce the problem to the computation of unit groups and Picard groups of certain finite locally free S-schemes.

Outline of the paper

In Section 2, we introduce some preliminary notions and define *F-extension data* on a group scheme G over a scheme S, where F is a sheaf of Abelian groups on S_{fppf}. In Section 3, we show that central extensions of G by F are classified by F-extension data on G (Theorem 3.2), and construct an exact sequence relating the group $\mathrm{Ext}_S(G, F)$ to various cohomology groups (Theorem 3.3). For G finite locally free and commutative, we show in Section 4 how to use $\mathbf{G}_{\mathrm{m}}$-extension data on G to describe G^*-torsors over S, making a theorem of Chase explicit. Finally, in Section 5, we show how the theory developed in this paper leads to algorithms for computing the above objects in practice for a finite locally free commutative group scheme over suitable base schemes, and we describe a connection between our results and algorithms for computing Selmer groups of elliptic curves.

2. Extension data on a group scheme

Let S be a scheme, and let G be a group scheme over S. We denote the group operation, identity and inverse morphisms of G by $m : G \times G \to G$, $e : S \to G$ and $\iota : G \to G$.

Let F be a sheaf of Abelian groups on S_{fppf}. We use multiplicative notation for F since important examples are the multiplicative group or the group of nth roots of unity for some $n \geq 1$.

For every S-scheme X, let $\mathcal{T}_F(X)$ be the category of F-torsors on X_{fppf}. We write $T \otimes T'$ for the contracted product of two F-torsors T and T', and $T^\vee$ for the dual of an F-torsor T.

2.1. Some simplicial definitions

For all $k \geq 0$, we write G^k for the k-fold fibre power of G over S. We number the factors by $\{0, 1, \ldots, k-1\}$ and write $p_i : G^k \to G$ for the projection on the ith coordinate.

The morphisms

$$p_0, p_1, m : G^2 \to G$$

give rise to a group homomorphism

$$\begin{aligned} d^1 : F(G) &\longrightarrow F(G^2) \\ x &\longmapsto (p_1^* x)(m^* x)^{-1}(p_0^* x). \end{aligned}$$

The above morphisms also give rise to functors

$$p_0^*, p_1^*, m^* : \mathcal{T}_F(G) \longrightarrow \mathcal{T}_F(G^2)$$

and hence a functor

$$\begin{aligned} \delta^1 : \mathcal{T}_F(G) &\longrightarrow \mathcal{T}_F(G^2) \\ T &\longmapsto p_1^*T \otimes (m^*T)^\vee \otimes p_0^*T. \end{aligned}$$

Similarly, we consider the morphisms

$$p_{0,1}, p_{1,2}, m_{0,1}, m_{1,2} : G^3 \to G^2$$

defined by

$$p_{0,1} = \mathrm{id}_G \times p_0, \quad p_{1,2} = p_1 \times \mathrm{id}_G, \quad m_{0,1} = m \times \mathrm{id}_G, \quad m_{1,2} = \mathrm{id}_G \times m.$$

These give rise to a group homomorphism

$$\begin{aligned} d^2 : F(G^2) &\longrightarrow F(G^3) \\ x &\longmapsto (p_{1,2}^*x)(m_{0,1}^*x)^{-1}(m_{1,2}^*x)(p_{0,1}^*x)^{-1}. \end{aligned}$$

The above morphisms also give rise to functors

$$p_{0,1}^*, p_{1,2}^*, m_{0,1}^*, m_{1,2}^* : \mathcal{T}_F(G^2) \longrightarrow \mathcal{T}_F(G^3)$$

and hence a functor

$$\begin{aligned} \delta^2 : \mathcal{T}_F(G^2) &\longrightarrow \mathcal{T}_F(G^3) \\ T &\longmapsto p_{1,2}^*T \otimes (m_{0,1}^*T)^\vee \otimes m_{1,2}T \otimes (p_{0,1}^*T)^\vee. \end{aligned}$$

The morphisms d^1 and d^2 are part of the *Hochschild complex*

$$F(S) \xrightarrow{d^0} F(G) \xrightarrow{d^1} F(G^2) \xrightarrow{d^2} F(G^3) \xrightarrow{d^3} \cdots, \tag{2.1}$$

whose cohomology groups are the *Hochschild cohomology groups* of G with coefficients in F.

For every F-torsor T on G, there is a canonical trivialisation

$$\kappa_T : F_{G^3} \xrightarrow{\sim} \delta^2(\delta^1 T).$$

2.2. Extension data

The following definition forms the basis for our computational framework for group scheme extensions.

Definition 2.1. Let G be a group scheme over a scheme S, and let F be a sheaf of Abelian groups on S_{fppf}. An *F-extension datum* on G is a pair (T, τ) where T is an F-torsor on G and

$$\tau : F_{G^2} \xrightarrow{\sim} \delta^1 T$$

is an isomorphism of F-torsors on G^2 such that the triangle

$$\begin{array}{ccc} F_{G^3} & \xrightarrow{\sim} & \delta^2 F_{G^2} \\ & \overset{\kappa_T}{\searrow} & \downarrow{\scriptstyle \sim\, \delta^2\tau} \\ & & \delta^2(\delta^1 T) \end{array} \tag{2.2}$$

commutes. Given two F-extension data (T, τ) and (T', τ') on G, an *isomorphism* from (T, τ) to (T', τ') is an isomorphism

$$\phi : T \xrightarrow{\sim} T'$$

of F-torsors on G such that the triangle

$$\begin{array}{ccc} F_{G^2} & \xrightarrow{\tau} & \delta^1 T \\ & \overset{\tau'}{\searrow} & \downarrow{\scriptstyle \sim\, \delta^1\phi} \\ & & \delta^1 T' \end{array} \tag{2.3}$$

commutes. The *groupoid of F-extension data on G*, denoted by $\mathcal{E}(G, F)$, is the groupoid in which the objects are the extension data for (G, F) and the isomorphisms are as above.

Note that the contracted product makes $\mathcal{E}(G, F)$ into a symmetric monoidal category. The neutral object is (F_G, τ_0) where $\tau_0 : F_{G^2} \xrightarrow{\sim} \delta^1 F_G$ is the canonical isomorphism. In particular, we have an Abelian group of isomorphism classes of objects of $\mathcal{E}(G, F)$.

3. Correspondence between extension data and group scheme extensions

3.1. The extension datum defined by a group scheme extension

From now on, we assume that the sheaf F is representable, *fppf* and affine over S. Then every F-torsor over an S-scheme X is representable, *fppf* and affine over X; see for example Oort [11, §17].

Remark 3.1. The assumption that F (and hence every F-torsor) is representable, *fppf* and affine over S is made for convenience and can most likely be omitted.

Consider a central extension

$$1 \longrightarrow F \xrightarrow{j} E \xrightarrow{q} G \longrightarrow 1$$

of sheaves of groups on S_{fppf}. Then q makes E into an F-torsor over G, so E is representable. Let $m_E : E \times_S E \to E$ and $\iota_E : E \to E$ be the multiplication and inverse morphisms.

We have a commutative diagram

$$\begin{array}{ccc} E \times_S E & \xrightarrow{m_E} & E \\ {\scriptstyle q\times q}\downarrow & & \downarrow{\scriptstyle q} \\ G \times_S G & \xrightarrow{m} & G. \end{array}$$

There is a canonical morphism

$$E \times_S E \longrightarrow p_0^* E \otimes p_1^* E$$

of G^2-schemes. It is straightforward to check that m_E induces an F-equivariant morphism

$$\nu_E : p_0^* E \otimes p_1^* E \longrightarrow m^* E,$$

which is automatically an isomorphism because both sides are F-torsors. We therefore obtain a trivialisation

$$\tau_E : F_{G^2} \xrightarrow{\sim} \delta^1 E.$$

By associativity of the group operation of E, we have a commutative diagram

$$\begin{array}{ccc} E \times_S E \times_S E & \xrightarrow{m_E \times \mathrm{id}} & E \times_S E \\ {\scriptstyle \mathrm{id} \times m_E}\downarrow & & \downarrow{\scriptstyle m_E} \\ E \times_S E & \xrightarrow[m_E]{} & E \end{array}$$

lying over the corresponding diagram for G. The commutativity of this diagram is equivalent to the statement that the isomorphisms

$$\begin{aligned} p_0^* E \otimes p_1^* E \otimes p_2^* E &\xrightarrow{\sim} p_{0,1}^*(p_0^* E \otimes p_1^* E) \otimes p_2^* E \\ &\xrightarrow{p_{0,1}^* \nu_E \otimes \mathrm{id}} p_{0,1}^* m^* E \otimes p_2^* E \\ &\xrightarrow{\sim} m_{0,1}^*(p_0^* E \otimes p_1^* E) \xrightarrow{m_{0,1}^* \nu_E} m_{0,1}^* m^* E \end{aligned}$$

and

$$\begin{aligned} p_0^* E \otimes p_1^* E \otimes p_2^* E &\xrightarrow{\sim} p_0^* E \otimes p_{1,2}^*(p_0^* E \otimes p_1^* E) \\ &\xrightarrow{\mathrm{id} \otimes p_{1,2}^* \nu_E} p_0^* E \otimes p_{1,2}^* m^* E \\ &\xrightarrow{\sim} m_{1,2}^*(p_0^* E \otimes p_1^* E) \xrightarrow{m_{1,2}^* \nu_E} m_{1,2}^* m^* E \end{aligned}$$

coincide with each other under the canonical identification of $m_{0,1}^* m^* E$ and $m_{1,2}^* m^* E$ given by the associativity of G. This is in turn equivalent to the commutativity of the triangle (2.2) for $T = E$ and $\tau = \tau_E$. We conclude that (E, τ_E) is an F-extension datum on G.

3.2. The group scheme extension defined by an extension datum

Conversely, let (T, τ) be an F-extension datum on G. As remarked above, T is representable. Let $q : T \to G$ be the structure map. We will use τ to make T into a group scheme over S equipped with a homomorphism $j_\tau : F \to T$ such that T becomes a central extension of G by F. This extends the well-known construction of a central extension of an abstract group by an Abelian group from a 2-cocycle.

The trivialisation τ induces an isomorphism $\nu_\tau : p_0^*T \otimes p_1^*T \to m^*T$ of F-torsors on $G \times G$, and hence a morphism

$$m_\tau : T \times_S T \to T \tag{3.1}$$

of S-schemes fitting in a commutative diagram

$$\begin{array}{ccc} T \times_S T & \xrightarrow{m_\tau} & T \\ {\scriptstyle q\times q}\downarrow & & \downarrow{\scriptstyle q} \\ G \times_S G & \xrightarrow{m} & G. \end{array}$$

By the argument in Section 3.1, m_T is an associative operation on T. Pulling back τ via the morphism

$$(e, e) : S \to G^2$$

gives a trivialisation

$$\tau(e, e) : F \xrightarrow{\sim} e^*T \tag{3.2}$$

and hence an F-equivariant closed immersion $j_\tau : F \to T$ fitting in a commutative diagram

$$\begin{array}{ccc} F & \xrightarrow{j_\tau} & T \\ \downarrow & & \downarrow{\scriptstyle q} \\ S & \xrightarrow{e} & G. \end{array}$$

Next, pulling back τ via the morphisms

$$i_0 = \mathrm{id} \times e : G \to G^2, \quad i_1 = e \times \mathrm{id} : G \to G^2$$

gives trivialisations

$$\tau(\ \ , e) : F_G \xrightarrow{\sim} p^*e^*T, \quad \tau(e, \ \ ) : F_G \xrightarrow{\sim} p^*e^*T$$

It is straightforward to check that pulling back the commutative triangle (2.2) by the morphisms

$$\mathrm{id} \times e \times e, e \times e \times \mathrm{id} : G \to G^3$$

implies that both $\tau(\ \ , e)$ and $\tau(e, \ \ )$ are equal to the pull-back of $\tau(e, e)$ via p. From this it follows that the compositions

$$F \times_S T \xrightarrow{j_\tau \times \mathrm{id}} T \times_S T \xrightarrow{m_\tau} T \quad \text{and} \quad T \times_S F \xrightarrow{\mathrm{id} \times j_\tau} T \times_S T \xrightarrow{m_\tau} T$$

agree with the maps given by the F-torsor structure on T; in particular, j_τ sends the identity section of F to a two-sided identity section for m_τ, and j_τ is a homomorphism of monoid schemes.

Finally, pulling back τ via the morphisms

$$(\iota, \mathrm{id}) : G \to G^2, \quad (\mathrm{id}, \iota) : G \to G^2$$

gives trivialisations

$$(\mathrm{id}, \iota)^*\tau : F_G \xrightarrow{\sim} \iota^*T \otimes (p^*e^*T)^\vee \otimes T,$$
$$(\iota, \mathrm{id})^*\tau : F_G \xrightarrow{\sim} T \otimes (p^*e^*T)^\vee \otimes \iota^*T.$$

Via the isomorphism $\tau(e, e)$ from (3.2), we obtain isomorphisms

$$\phi_0, \phi_1 : T^\vee \xrightarrow{\sim} \iota^*T$$

of F-torsors on G. Composing these with the canonical isomorphism $T \xrightarrow{\sim} T^\vee$ of G-schemes (not an isomorphism of F-torsors since it inverts the action of F) gives isomorphisms $T \xrightarrow{\sim} \iota^*T$ over G, hence automorphisms $T \xrightarrow{\sim} T$ lying over the automorphism ι of G. By construction, these are left inverse and right inverse operations on T, and they are equal by the associativity of m_τ. Thus we have equipped T with the desired structure of central extension of G by F.

3.3. An equivalence of categories and an exact sequence

Theorem 3.2. *Let G be a group scheme over a scheme S, and let F be a sheaf of Abelian groups on G. Assume that F is representable, fppf and affine over S. Then there is a canonical equivalence of categories between $\mathcal{E}(G, F)$ and the category of central extensions of G by F.*

Proof. By the arguments in Sections 3.1 and 3.2, the possible group scheme structures on an F-torsor T on G correspond bijectively to the trivialisations $\tau : F_{G^2} \xrightarrow{\sim} \delta^1 T$ making the triangle (2.2) commute. This gives a canonical bijection between central extensions of G by F and objects of $\mathcal{E}(G, F)$.

Given extension data (T, τ) and (T', τ'), an isomorphism between the corresponding extensions is an isomorphism $T \to T'$ of F-torsors on G that is compatible with the group operations m_τ and $m_{\tau'}$ as well as the inclusions $j_\tau : F \to T$ and $j_{\tau'} : F \to T'$. The first condition corresponds to the commutativity of the diagram (2.3), and the second condition follows from the first by the definition of j_τ and $j_{\tau'}$. □

Via the equivalence of Theorem 3.2, we will identify the group $\mathrm{Ext}_S(G, F)$ of isomorphism classes of central extensions of G by F with the group of isomorphism classes of objects of $\mathcal{E}(G, F)$. Using this identification, we will embed $\mathrm{Ext}_S(G, F)$ into an exact sequence that will allow us to compute this group in various cases.

We first consider F-extension data (T, τ) such that T is a trivial F-torsor. Given an element $u \in F(G^2)$ with $d^2u = 1$, one obtains an extension datum (F, τ) such that τ corresponds to multiplication by u under the canonical identification $F_{G^2} \xrightarrow{\sim} \delta^1 F$. This gives an injective homomorphism

$$\mathrm{H}^2_{\mathrm{H}}(G, F) \longrightarrow \mathrm{Ext}_S(G, F)$$

whose image is the group of isomorphism classes of extension data (T, τ) such that the F-torsor T is trivial; see [13, exposé XVII, appendice I].

Next, we define $K(G, F)$ to be the kernel of the map

$$d^1 : \mathrm{H}^1(G_{fppf}, F) \longrightarrow \mathrm{H}^1(G^2_{fppf}, F)$$

induced by the functor δ^1. By our identification of $\mathrm{Ext}_S(G, F)$ with the group of isomorphism classes of objects of $\mathcal{E}(G, F)$, there is a canonical group homomorphism

$$\mathrm{Ext}_S(G, F) \longrightarrow K(G, F)$$

sending the class of (T, τ) to the class of T.

Furthermore, we construct a homomorphism

$$\xi_{G,F} : K(G, F) \longrightarrow \mathrm{H}^3_{\mathrm{H}}(G, F) \tag{3.3}$$

as follows. Let x be an element of $K(G, F)$, represented by an F-torsor T on G such that $\delta^1 T$ is trivial. Choose a trivialisation

$$\tau : F_{G^2} \xrightarrow{\sim} \delta^1 T.$$

We then define u_τ to be the element of $F(G^3)$ such that the composition

$$F_{G^3} \xrightarrow{\sim} \delta^2 F_{G^2} \xrightarrow{\delta^2 \tau} \delta^2(\delta^1 T) \xrightarrow{\kappa_T^{-1}} F_{G^3}$$

equals multiplication by u_τ. Then we have $d^2 u = 1$, and we define $\xi_{G,F}(x)$ to be the class of u_τ in $\mathrm{H}^2_{\mathrm{H}}(G, F)$. Since a different choice for T or τ changes u_τ by an element in the image of d^2, the map $\xi_{G,F}$ is a well-defined group homomorphism.

Theorem 3.3. *There is an exact sequence*

$$1 \longrightarrow \mathrm{H}^2_{\mathrm{H}}(G, F) \longrightarrow \mathrm{Ext}_S(G, F) \longrightarrow K(G, F) \xrightarrow{\xi_{G,F}} \mathrm{H}^3_{\mathrm{H}}(G, F).$$

Proof. We define a sequence using the maps constructed above. Exactness at $\mathrm{H}^2_{\mathrm{H}}(G, F)$ and $\mathrm{Ext}_S(G, F)$ follows from the above arguments. It remains to show exactness at $K(G, F)$. Given an F-extension datum (T, τ) on G, the element u_τ equals 1 by the commutativity of (2.2), so the class of T is in the kernel of $\xi_{G,F}$. Conversely, let $x \in K(G, F)$ be in the kernel of $\xi_{G,F}$. Choosing T and τ as in the construction of $\xi_{G,F}$, the element $u_\tau \in F(G^3)$ is then in the image of d^2, say $u_\tau = d^2 y$ with $y \in F(G^2)$. Dividing τ by y, we obtain a trivialisation $\tau' : F_{G^2} \xrightarrow{\sim} \delta^1 T$ such that $u_{\tau'} = 1$, so the diagram (2.2) for τ' commutes; therefore, (T, τ') is in $\mathcal{E}(G, F)$ and maps to $x \in K(G, F)$. It follows that the kernel of $\xi_{G,F}$ equals the image of $\mathrm{Ext}_S(G, F)$ in $K(G, F)$. □

Remark 3.4. It is well known that extensions of an abstract group Γ by a Γ-module A are classified by the group $\mathrm{H}^2(\Gamma, A)$ where $\mathrm{H}^i(\Gamma, \quad)$ is the ith derived functor of the functor of Γ-invariants. For a group scheme G over a scheme S, there is a functor of G-invariants defined for a sheaf F of G-modules on S by $\mathrm{H}^0(G, F) = F^G(S)$, where F^G is the sheaf of G-invariants. There is a homomorphism $\mathrm{Ext}_S(G, F) \longrightarrow \mathrm{H}^2(G, F)$, but this is part of a long exact sequence and is in general not an isomorphism; see Demazure and Gabriel [8, III, §6, 3.1].

Remark 3.5. Demazure and Gabriel constructed a spectral sequence involving certain Ext groups of presheaves [8, III, §6, 2.3], of which the exact sequence of low-degree terms [8, III, §6, 2.5] agrees with the exact sequence of Theorem 3.3. To show that the various groups in the respective exact sequences agree, one can use results from [8, II, §3,

1.3; III, §6, n° 1–2]. Some of these are only stated for affine group schemes because of the setting in which Demazure and Gabriel work, but can be generalised without difficulty to arbitrary group schemes.

3.4. The subgroup of commutative extensions

Given a group scheme G over S, let $\sigma_G : G^2 \to G^2$ be the involution switching the factors. We have an obvious notion of opposite group scheme G^{op} (replace the multiplication morphism $m : G^2 \to G$ by $m \circ \sigma_G$). Given a central extension

$$1 \longrightarrow F \longrightarrow E \longrightarrow G \longrightarrow 1$$

we obtain a corresponding extension

$$1 \longrightarrow F \longrightarrow E^{\mathrm{op}} \longrightarrow G^{\mathrm{op}} \longrightarrow 1.$$

Let (T, τ) be an F-extension datum on G. There is a canonical isomorphism $\delta^1_{G^{\mathrm{op}}} T \xrightarrow{\sim} \sigma_G^*(\delta^1 T)$, where we write $\delta^1_{G^{\mathrm{op}}}$ for the functor δ^1 associated with G^{op}. Let $\tau^{\mathrm{op}} : F_{G^2} \xrightarrow{\sim} \delta^1_{G^{\mathrm{op}}} T$ be the isomorphism making the diagram

$$\begin{array}{ccc} F_{G^2} & \xrightarrow{\tau^{\mathrm{op}}} & \delta^1_{G^{\mathrm{op}}} T \\ \downarrow \sim & & \downarrow \sim \\ \sigma_G^* F_{G^2} & \xrightarrow{\sigma_G^* \tau} & \sigma_G^*(\delta^1 T) \end{array}$$

commutative. If (T, τ) defines the extension E of G, then (T, τ^{op}) defines the extension E^{op} of G^{op}.

Now suppose that G is commutative, so $G = G^{\mathrm{op}}$. Then E is commutative if and only if $\tau^{\mathrm{op}} = \tau$. We use this to compute the subgroup $\mathrm{Ext}^1_S(G, F)$ of $\mathrm{Ext}_S(G, F)$ classifying commutative extensions as follows. Given an extension datum (T, τ), the composed isomorphism

$$F_{G^2} \xrightarrow{\tau^{\mathrm{op}}} \delta^1 T \xrightarrow{\tau^{-1}} F_{G^2}$$

of F-torsors on G^2 equals multiplication by some element $\Sigma(T, \tau) \in F(G^2)$. We have a group homomorphism

$$\Sigma : \mathrm{Ext}_S(G, F) \longrightarrow F(G^2) \tag{3.4}$$

sending the extension class defined by an extension datum (T, τ) to the section $\Sigma(T, \tau)$. Then $\mathrm{Ext}^1_S(G, F)$ is the kernel of Σ.

3.5. Some results on $\boldsymbol{\mu}_n$-extension data

Let n be a positive integer, and let $\boldsymbol{\mu}_n$ be the group scheme of nth roots of unity. We now collect some results on $\boldsymbol{\mu}_n$-torsors and central extensions by $\boldsymbol{\mu}_n$ that will be used in Section 5.3.

The groupoid $\mathcal{T}_{\boldsymbol{\mu}_n}(X)$ of $\boldsymbol{\mu}_n$-torsors over a scheme X is canonically equivalent to the following groupoid. The objects are pairs (T, λ) where T is a $\mathbf{G}_{\mathrm{m}}$-torsor on X and

$\lambda : \mathbf{G}_{\mathrm{m},X} \xrightarrow{\sim} T^{\otimes n}$ is an isomorphism of $\mathbf{G}_{\mathrm{m}}$-torsors. The isomorphisms from (T, λ) to (T, λ') are the isomorphisms $\alpha : T \xrightarrow{\sim} T'$ of $\mathbf{G}_{\mathrm{m}}$-torsors satisfying $\alpha^{\otimes n} \circ \lambda = \lambda'$. The canonical functor $\mathcal{T}_{\boldsymbol{\mu}_n}(X) \to \mathcal{T}_{\mathbf{G}_{\mathrm{m}}}(X)$ obtained from the inclusion $\boldsymbol{\mu}_n \to \mathbf{G}_{\mathrm{m}}$ is given by sending (T, λ) to T.

Given a group scheme G over a scheme S, a $\boldsymbol{\mu}_n$-extension datum on G therefore consists of a $\boldsymbol{\mu}_n$-torsor (T, λ) on G and a trivialisation

$$\tau : \mathbf{G}_{\mathrm{m},G} \xrightarrow{\sim} \delta^1 T$$

of $\mathbf{G}_{\mathrm{m}}$-torsors such that the diagram

$$\begin{array}{ccc} \mathbf{G}_{\mathrm{m},G^2} & \xrightarrow{\tau^{\otimes n}} & (\delta^1 T)^{\otimes n} \\ \downarrow{\scriptstyle \sim} & & \downarrow{\scriptstyle \sim} \\ \delta^1 \mathbf{G}_{\mathrm{m},G} & \xrightarrow[\delta^1 \lambda]{} & \delta^1 (T^{\otimes n}) \end{array}$$

commutes.

Lemma 3.6. *There is a short exact sequence of Abelian groups*

$$1 \longrightarrow G^*(S)/G^*(S)^n \longrightarrow \mathrm{Ext}_S(G, \boldsymbol{\mu}_n) \longrightarrow \mathrm{Ext}_S(G, \mathbf{G}_{\mathrm{m}})[n] \longrightarrow 1,$$

and similarly with Ext_S *replaced by* Ext^1_S.

Proof. We construct a sequence as follows. Representing $\boldsymbol{\mu}_n$-torsors as above, we define a map $G^*(S) \to \mathrm{Ext}_S(G, \mathbf{G}_{\mathrm{m}})$ sending an element $\lambda \in G^*(S)$ to the class of $((\mathbf{G}_{\mathrm{m},G}, \tilde{\lambda}), \tau_0)$, where the isomorphism $\tilde{\lambda} : \mathbf{G}_{\mathrm{m},G} \xrightarrow{\sim} \mathbf{G}_{\mathrm{m},G}^{\otimes n}$ is multiplication by λ (viewing λ as an element of $\mathbf{G}_{\mathrm{m}}(G)$ and identifying $\mathbf{G}_{\mathrm{m},G}^{\otimes n}$ with $\mathbf{G}_{\mathrm{m},G}$) and τ_0 is the canonical isomorphism $\mathbf{G}_{\mathrm{m},G^2} \xrightarrow{\sim} \delta^1 \mathbf{G}_{\mathrm{m},G}$. Furthermore, we define a map $\mathrm{Ext}_S(G, \boldsymbol{\mu}_n) \to \mathrm{Ext}_S(G, \mathbf{G}_{\mathrm{m}})$ by sending $((T, \lambda), \tau)$ to (T, τ). One now verifies that this gives the desired short exact sequence. □

Remark 3.7. Short exact sequences analogous to those in Lemma 3.6 can be constructed from the long exact sequences obtained by applying suitable derived functors to the Kummer sequence

$$1 \longrightarrow \boldsymbol{\mu}_n \longrightarrow \mathbf{G}_{\mathrm{m}} \xrightarrow{n} \mathbf{G}_{\mathrm{m}} \longrightarrow 1$$

on S_{fppf}. An argument of Demazure and Gabriel [8, III, §6, 1.10] shows that these agree with the exact sequences from Lemma 3.6, at least up to a sign.

4. From extension data to G^*-torsors

Let G be a finite locally free commutative group scheme over a scheme S, and let G^* denote its Cartier dual. By a theorem of Chase [4, Theorem 16.14], generalised by Shatz [15] and Waterhouse [16], there is a canonical isomorphism

$$\mathrm{H}^1(S_{fppf}, G^*) \xrightarrow{\sim} \mathrm{Ext}^1_S(G, \mathbf{G}_{\mathrm{m}}). \tag{4.1}$$

The explicit description of $\mathrm{Ext}^1_S(G, \mathbf{G}_\mathrm{m})$ given in the previous section leads to the following explicit description of G^*-torsors. For simplicity, we describe the case where S is affine, say $S = \operatorname{Spec} R$. Then G and G^* are also affine, say

$$G = \operatorname{Spec} B \quad \text{and} \quad G^* = \operatorname{Spec} B^\vee$$

where B is a finite locally free commutative and cocommutative Hopf algebra over R and

$$B^\vee = \operatorname{Hom}_{R\text{-Mod}}(B, R)$$

is the Hopf algebra dual to B. We write $\mu : B \to B \otimes_R B$ for the comultiplication map. Furthermore, $\mathbf{G}_\mathrm{m}$-torsors on G correspond to invertible B-modules, which are locally trivial for the Zariski topology. In particular, we identify $\mathrm{H}^1(G_{fppf}, \mathbf{G}_\mathrm{m})$ with the Picard group $\operatorname{Pic} G$ of invertible B-modules.

Consider a $\mathbf{G}_\mathrm{m}$-extension datum (U, τ) on G defining a commutative extension, where B is now an invertible B-module and τ is a trivialisation (given by a generating section, for example) of the invertible $(B \otimes_R B)$-module

$$(U \otimes_R B) \underset{B\otimes_R B}{\otimes} (\mu^* U)^\vee \underset{B\otimes_R B}{\otimes} (B \otimes_R U) \cong (U \otimes_R U) \underset{B\otimes_R B}{\otimes} (\mu^* U)^\vee.$$

The morphism m_τ from (3.1) corresponds to an R-algebra homomorphism

$$\mu_\tau : U \to U \otimes_R U$$

satisfying $\mu_\tau(bu) = \mu(b)\mu_\tau(u)$ for all $b \in B$ and $u \in U$. Following Chase's construction in [4, proof of Theorem 16.14], we obtain the following description of the G^*-torsor corresponding to (U, τ). The finite locally free R-module

$$U^\vee = \operatorname{Hom}_{R\text{-Mod}}(U, R)$$

equipped with the R-bilinear map $U^\vee \times U^\vee \to U^\vee$ obtained by dualising μ_τ is a commutative R-algebra, and the R-linear map

$$\alpha : U^\vee \longrightarrow B^\vee \otimes_R U^\vee \tag{4.2}$$

obtained by dualising the B-module structure on U defines a $B^\vee$ comodule structure on $U^\vee$. The corresponding S-scheme $X = \operatorname{Spec} U^\vee$ together with the morphism $\operatorname{Spec} \alpha : G^* \times X \to X$ is then the desired G^*-torsor.

5. Computational aspects

We will now outline how the methods of this article can be used to do explicit calculations with extensions and torsors under the assumption that we can represent and compute with various more basic objects; see Assumption 5.1. In Section 5.5, we show that these assumptions are fulfilled for finite locally free commutative group schemes over a localised order in a product of number fields.

The algorithms described below have been implemented as part of the author's software package [2] for computing with finite group schemes in SageMath [12].

5.1. Presentations of finitely generated Abelian groups

We briefly describe the tools that we will use for computing with finitely generated Abelian groups; see Cohen [6, §4.1] for details.

Let A be a finitely generated Abelian group. We assume that we have a way of computationally representing elements of A and performing the multiplication and inversion in A. (We allow for the possibility that an element of A has several different computational representations.) By a *presentation of* A we mean non-negative integers r and k, integers $d_1, \dots, d_k \geq 2$ with $d_1 \mid d_2 \mid \cdots \mid d_k$ together with mutually inverse group isomorphisms

$$\exp_A : B \xrightarrow{\sim} A, \quad \log_A : A \xrightarrow{\sim} B$$

given by algorithms, where $B = \mathbf{Z}^r \oplus \bigoplus_{i=1}^k \mathbf{Z}/d_i\mathbf{Z}$. We view $\log_A$ as a discrete logarithm function for A. By an *algorithm for finding linear relations in* A we mean an algorithm that given $a_1, \dots, a_n \in A$ outputs the kernel of the group homomorphism $\mathbf{Z}^n \to A$ sending the ith standard basis element to a_i. Note that having a presentation for A is equivalent to having a finite set of generators for A together with an algorithm for finding linear relations in A. Furthermore, if we can find linear relations, then we can compare elements: two elements $a, a' \in A$ are equal if and only if the homomorphism $\mathbf{Z} \to A$ sending 1 to $a'a^{-1}$ is trivial.

Let $f : A \to A'$ be a homomorphism of finitely generated Abelian groups as above. Assume that we can evaluate f using the given computational representation of elements of A and A'. If we have presentations of A and A', we can compute a matrix for f with respect to these presentations using $\exp_A$ and $\log_{A'}$. From such a matrix, we can compute presentations for the kernel and cokernel of f. Note that to compute a presentation for the kernel of f, we do not need a presentation for A'; it suffices to have a presentation for A and an algorithm for finding linear relations in A'. Similarly, to compute a presentation for the cokernel of F, it suffices to have a presentation for A' and a finite set of generators of A.

5.2. Computing extension class groups

Let G be a group scheme over a scheme S, and let F be a sheaf of Abelian groups on S that is representable, *fppf* and affine over S.

Assumption 5.1. We make the following computational assumptions about the group scheme G and the sheaf F:

- The groups $F(G^i)$ (for $i \in \{1, 2, 3\}$) and $\mathrm{H}^1(G^i_{fppf}, F)$ (for $i \in \{1, 2\}$) are finitely generated.
- We have computational representations for elements of $F(G)$, $F(G^2)$ and $F(G^3)$, and we can perform multiplication and inversion in these groups.
- We have a finite set of generators for $F(G)$, a presentation of $F(G^2)$ and an algorithm for finding linear relations in $F(G^3)$.
- We have computational representations for F-torsors on G, G^2 and G^3, and for isomorphisms between such torsors.

- Given two F-torsors T, T', we can compute $T \otimes T'$, and given trivialisations of T and T', we can compute the resulting trivialisation of $T \otimes T'$; similarly for dual torsors.
- Given an F-torsor T on G^2 that is known to be trivial, we can find a trivialisation $F_{G^2} \xrightarrow{\sim} T$.
- Given an F-torsor T on G^3 and an F-torsor automorphism $f : T \xrightarrow{\sim} T$, we can find the unique element $u_f \in F(G^3)$ such that f equals multiplication by u_f.
- We have a presentation for $\mathrm{H}^1(G_{fppf}, F)$, and we can find linear relations in $\mathrm{H}^1(G^2_{fppf}, F)$, using the given computational representation of F-torsors to represent elements of these groups.
- We have algorithms for computing the various group homomorphisms and functors defined in Section 2.1.

We use these assumptions and the exact sequence from Theorem 3.3 to compute a presentation for $\mathrm{Ext}_S(G, F)$ as follows:

- Compute a presentation for $\mathrm{H}^2_{\mathrm{H}}(G, F)$ as the second cohomology group of the complex (2.1).
- Compute a matrix for the homomorphism $d^1 : \mathrm{H}^1(G_{fppf}, F) \longrightarrow \mathrm{H}^1(G^2_{fppf}, F)$.
- Compute a presentation for the group $K(G, F) = \ker d^1$.
- Compute a matrix for the homomorphism $\xi_{G,F}$ from (3.3).
- Use Cohen's algorithm for computing a presentation for the second term in a left four-term exact sequence [6, §4.1.7] to compute a presentation for $\mathrm{Ext}_S(G, F)$.

In the last step, we use the description of the map $\mathrm{H}^2_{\mathrm{H}}(G, F) \longrightarrow \mathrm{Ext}_S(G, F)$ given in Section 3.3 to map elements of $\mathrm{H}^2_{\mathrm{H}}(G, F)$ to F-extension data, and we use the construction in Theorem 3.3 to lift elements of the kernel of $\xi_{G,F}$ to F-extension data.

We note that after computing $\mathrm{Ext}_S(G, F)$, we can also compute the homomorphism (3.4) and its kernel, which is the group $\mathrm{Ext}^1_S(G, F)$ of isomorphism classes of commutative extensions of G by F.

Remark 5.2. For each $n \in \mathbf{Z}$, let $[n] : G \to G$ denote the multiplication-by-n map. The kernel $K(G, F)$ of $d^1 : \mathrm{H}^1(G_{fppf}, F) \longrightarrow \mathrm{H}^1(G^2_{fppf}, F)$ is contained in the subgroup $\mathrm{H}^1(G_{fppf}, F)^{(1)}$ of isomorphism classes of torsors T such that for all $n \in \mathbf{Z}$ the torsors $[n]^*T$ and $T^{\otimes n}$ are isomorphic. In practice, it may be useful to compute $\mathrm{H}^1(G_{fppf}, F)^{(1)}$ first and then to compute $K(G, F)$ as the kernel of the restriction of d^1 to $\mathrm{H}^1(G_{fppf}, F)^{(1)}$. An analogous remark in the context of Galois modules annihilated by a prime number p was made by Schaefer and Stoll [14, Corollary 5.3], who used this in their algorithm for computing p-Selmer groups of elliptic curves.

5.3. Computing torsor class groups

Let G be a finite locally free and commutative group scheme over a scheme S. We now consider the problem of computing the group $\mathrm{H}^1(S_{fppf}, G^*)$ of isomorphism classes of G^*-torsors. In light of the isomorphism (4.1) between this group and $\mathrm{Ext}^1_S(G, \mathbf{G}_{\mathrm{m}})$, it is natural to represent a G^*-torsor over S by the corresponding $\mathbf{G}_{\mathrm{m}}$-extension datum

on G, and to view the actual G^*-torsor (the S-scheme with G^*-action) as a "secondary" object to be computed from the $\mathbf{G}_{\mathrm{m}}$-extension datum.

For simplicity, as in Section 4, we assume $S = \operatorname{Spec} R$, $G = \operatorname{Spec} B$ and $G^* = \operatorname{Spec} B^\vee$ with R a commutative ring and B a finite locally free commutative cocommutative Hopf algebra over R. A $\mathbf{G}_{\mathrm{m}}$-extension datum on G is therefore of the form (U, τ) where U is an invertible B-module. Using the description in Section 4, the R-algebra structure on $U^\vee$ and the comultiplication map (4.2) can be extracted from (U, τ) using linear algebra over R.

Remark 5.3. This representation of G^*-torsors fits very naturally into the author's framework of *dual pair of algebras* for computing with finite group schemes [1]. In this setting, neither the comultiplication map μ nor the comodule map α needs to be written down explicitly. This allows efficient computation with G^*-torsors once $\mathrm{H}^1(S_{fppf}, G^*)$ has been computed using one of the methods described below.

We now sketch two algorithms: one for computing $\mathrm{H}^1(S_{fppf}, G^*)$, and another for computing $\mathrm{H}^1(S_{fppf}, G^*)[n]$ for a given positive integer n. We assume that S and G are such that our computational Assumption 5.1 holds for the sheaf $\mathbf{G}_{\mathrm{m}}$ (for the first algorithm) and for the sheaf $\boldsymbol{\mu}_n$ (for the second algorithm). For suitable rings R, namely localised orders, this will be justified in Section 5.5.

Computing torsor class groups from $\mathbf{G}_{\mathrm{m}}$-extensions

The first method proceeds directly via the identification (4.1) of $\mathrm{H}^1(S_{fppf}, G^*)$ with $\mathrm{Ext}^1_S(G, \mathbf{G}_{\mathrm{m}})$, and is conceptually more straightforward than the method described below. The algorithm is simply to compute a presentation for $\mathrm{Ext}^1_S(G, \mathbf{G}_{\mathrm{m}})$ using the algorithm from Section 5.2, and then to compute, for each extension datum (U, τ) in some finite generating set, the resulting R-algebra structure on $U^\vee$ and the comodule map $\alpha : U^\vee \longrightarrow B^\vee \otimes_R U^\vee$.

Computing torsor class groups from $\boldsymbol{\mu}_n$-extensions

In the second method, we replace $\mathbf{G}_{\mathrm{m}}$ by $\boldsymbol{\mu}_n$, where n is a positive integer; this leads to an algorithm for computing the n-torsion subgroup of $\mathrm{Ext}^1_S(G, \mathbf{G}_{\mathrm{m}})$ and hence of $\mathrm{H}^1(S_{fppf}, G^*)$. The case where n is (a divisor of) the exponent of G is the most interesting in practice, but we do not need this assumption.

In this approach, we first compute $\mathrm{Ext}^1_S(G, \boldsymbol{\mu}_n)$ using the algorithm from Section 5.2, and compute $\mathrm{Ext}^1_S(G, \mathbf{G}_{\mathrm{m}})[n]$ as the cokernel of the map $G^*(S) \to \mathrm{Ext}^1_S(G, \boldsymbol{\mu}_n)$ from Lemma 3.6. We then proceed as in the first method, using the isomorphism (4.1) to identify $\mathrm{Ext}^1_S(G, \mathbf{G}_{\mathrm{m}})[n]$ with $\mathrm{H}^1(S_{fppf}, G^*)[n]$.

5.4. Comparison to algorithms for computing Selmer groups

Part of the motivation behind the present work was to understand the geometry behind existing algorithms for computing Selmer groups. We sketch briefly how these algorithms can be interpreted in the framework described in this paper.

Let E be an elliptic curve over a number field K. A standard way of determining the Mordell–Weil group $E(K)$ starts by computing the *n-Selmer group* $\mathrm{Sel}_n(E)$ inside

the Galois cohomology group $\mathrm{H}^1(K, E[n])$ for some $n \geq 2$ (or more generally the Selmer group associated with an isogeny). Algorithms for computing these Selmer groups were given by Schaefer and Stoll [14] (for n prime) and by Cremona, Fisher, O'Neil, Simon and Stoll [7], among others. These algorithms are based on mapping $\mathrm{Sel}_n(E)$ to a subgroup of the Galois cohomology group $\mathrm{H}^1(R, \boldsymbol{\mu}_n) \cong R^\times/(R^\times)^n$ for a certain étale K-algebra R. This in turn uses the embedding of $E[n]$ into the Galois module of functions $E[n] \to \boldsymbol{\mu}_n$ defined by the Weil pairing; see [14, §3] and [7, §3]. In [7, §1.5] it was noted that the group $\mathrm{H}^1(K, E[n])$ classifying $E[n]$-torsors also classifies commutative extensions of $E[n]$ by $\mathbf{G}_\mathrm{m}$. This point of view was used in [7, §3] to identify $\mathrm{Sel}_n(E)$ as a subquotient of $(R \otimes_K R)^\times$.

In this paper, we consider group schemes over more general base schemes and use *fppf* cohomology instead of Galois cohomology together with local conditions. The link between the two approaches is that Selmer groups of Abelian varieties can be interpreted as *fppf* cohomology groups, as shown by Česnavičius [3, §4]. Computing the n-Selmer group of an elliptic curve over a number field K can therefore be viewed as computing $\mathrm{H}^1(S_{fppf}, E[n])$, with S the spectrum of the ring of Σ-integers in K for a finite set Σ of places of K, followed by computing a subgroup defined by local conditions at the places in Σ.

Of the two methods given in Section 5.3 for computing $\mathrm{H}^1(S_{fppf}, G^*)$ (note that if G is the n-torsion of an elliptic curve, then we can identify G with G^* via the Weil pairing), the second method is closest to the algorithms of [7,14]. This second method also has certain (potential) practical advantages over the first:

(1) Computing presentations for the groups $\boldsymbol{\mu}_n(G^i)$ is easier than for $\mathbf{G}_\mathrm{m}(G^i)$, because one only needs to know the nth roots of unity rather than the full unit groups of the algebras in question. The same holds for finding linear relations in $\mathrm{H}^3_\mathrm{H}(G, \boldsymbol{\mu}_n)$ as opposed to $\mathrm{H}^3_\mathrm{H}(G, \mathbf{G}_\mathrm{m})$.

(2) At least in certain cases, it may be easier to compute the subgroup $K(G, \boldsymbol{\mu}_n)$ of $\mathrm{H}^1(G_{fppf}, \boldsymbol{\mu}_n)$ than to compute the subgroup $K(G, \mathbf{G}_\mathrm{m})$ of $\mathrm{H}^1(G_{fppf}, \mathbf{G}_\mathrm{m})$. In the case where p is an odd prime number and E is an elliptic curve over a number field K, Schaefer and Stoll [14, §5] showed that the Galois cohomology group $\mathrm{H}^1(K, E[p])$ and the p-Selmer group of E can be computed as certain subgroups of the kernel of a homomorphism $A^\times/(A^\times)^p \to B^\times/(B^\times)^p$, where A and B are K-algebras of degree $p^2 - 1$. Translating this to our setting, and taking n to be an odd prime number p and G to be a group scheme over S annihilated by p, we may wonder if $K(G, \boldsymbol{\mu}_p)$ can similarly be computed as the kernel of a homomorphism $\mathrm{H}^1(G_{fppf}, \boldsymbol{\mu}_p)^{(1)} \longrightarrow \mathrm{H}^1(X_{fppf}, \boldsymbol{\mu}_p)$ (see Remark 5.2 for the definition of the left-hand side) for a suitable finite locally free S-scheme X of substantially smaller degree than that of G^2.

5.5. *Results over localised orders*

We conclude by showing how the algorithms from this paper can be implemented concretely for suitable base schemes, based on the computation of unit groups and Picard groups of (localisations of) orders in number fields.

Definition 5.4. A (reduced) *order* is a reduced commutative ring that is free of finite rank as a $\mathbf{Z}$-module.

An order is in particular Noetherian and one-dimensional, but not necessarily regular, and is of finite index in a product of maximal orders of number fields.

Definition 5.5. A *localised order* is a ring of the form R_Σ, where R is an order, Σ is a finite set of maximal ideals of R, and R_Σ is the coordinate ring of the complement of Σ in $\operatorname{Spec} R$.

Example 5.6. Let K be a number field, and let Σ be a finite set of places of K. Then the ring $\mathbf{Z}_{K,\Sigma}$ of Σ-integers in K is a localised order.

Let R be a localised order, and let G be a finite locally free group scheme over $S = \operatorname{Spec} R$. Then each G^i is the spectrum of a finite locally free R-algebra B^i. Furthermore, G^i is generically étale over S, so B^i is again a localised order.

There are algorithms for computing presentations of unit groups and Picard groups of orders; see Cohen [5, §6.5] for maximal orders in number fields, Klüners and Pauli [9] for general orders in number fields and Marseglia [10, Remark 3.8] for arbitrary orders. These algorithms can be extended to localised orders as in [6, §7.4]. If R' is a localised order, we represent $\mathbf{G}_\mathrm{m}$-torsors (or invertible sheaves) on $\operatorname{Spec} R'$ by invertible fractional ideals of R'.

Similarly, if R' is a localised order and n is a positive integer, then as in Section 3.5 we represent $\boldsymbol{\mu}_n$-torsors over $S' = \operatorname{Spec} R'$ by pairs (J, x) where J is an invertible fractional ideal of R' and x is a generator of J^n. By the long exact cohomology sequence obtained from the Kummer sequence, the group $\mathrm{H}^1(S'_{fppf}, \boldsymbol{\mu}_n)$ of isomorphism classes of $\boldsymbol{\mu}_n$-torsors fits in a short exact sequence

$$1 \longrightarrow R'^{\times}/(R'^{\times})^n \longrightarrow \mathrm{H}^1(S'_{fppf}, \boldsymbol{\mu}_n) \longrightarrow (\operatorname{Pic} R')[n] \longrightarrow 1,$$

which we can use to compute a presentation of $\mathrm{H}^1(S'_{fppf}, \boldsymbol{\mu}_n)$.

The above implies that if R is a localised order and G is a finite locally free group scheme over $S = \operatorname{Spec} R$, then our computational Assumption 5.1 is fulfilled both for the sheaf $\mathbf{G}_\mathrm{m}$ and for the sheaf $\boldsymbol{\mu}_n$. We can therefore apply the method from Section 5.2 and both methods from Section 5.3 to compute presentations for the groups $\operatorname{Ext}_S(G, \mathbf{G}_\mathrm{m})$, $\operatorname{Ext}^1_S(G, \mathbf{G}_\mathrm{m})$ and $\mathrm{H}^1(S_{fppf}, G^*)$ (in the case of the second method, for the n-torsion of these groups).

Finally, we consider two finite locally free commutative group schemes G and F over S. Then we can compute $\operatorname{Ext}_S(G, F)$ using the following "bootstrap" argument. We can compute presentations for the finite Abelian groups $F(G^i)$ for $i \in \{1, 2, 3\}$; this comes down to computing homomorphisms between subrings of products of number fields. Furthermore, we can compute $\mathrm{H}^1(G^i_{fppf}, F)$ for $i = 1$ and $i = 2$ as described above (with (G^i, F^*) in place of (S, G)) because the G^i are again spectra of localised orders. Finally, using the representation of F-torsors as $\mathbf{G}_\mathrm{m}$-extension data allows us to perform the remaining tasks in Assumption 5.1. Therefore our computational assumptions are fulfilled for the group scheme G over S and the sheaf F, and we can use the algorithm from Section 5.2 to compute the group $\operatorname{Ext}_S(G, F)$.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Code is in the GitLab repository linked to in reference [2].

References

[1] Peter Bruin, Dual pairs of algebras and finite commutative group schemes, 2017, Preprint, https://arxiv.org/abs/1709.09847.
[2] Peter Bruin, `dual_pairs`, SageMath package for computing with finite group schemes as dual pairs of algebras, 2022, Available at https://gitlab.com/pbruin/dual-pairs/.
[3] Kęstutis Česnavičius, Selmer groups as flat cohomology groups, J. Ramanujan Math. Soc. 31 (1) (2016) 31–61.
[4] Stephen U. Chase, Moss E. Sweedler, Hopf algebras and Galois theory, Lecture Notes in Mathematics, Vol. 97, Springer-Verlag, Berlin-New York, 1969.
[5] Henri Cohen, A course in computational algebraic number theory, Graduate Texts in Mathematics, Vol. 138, Springer-Verlag, Berlin, 1993.
[6] Henri Cohen, Advanced topics in computational number theory, Graduate Texts in Mathematics, Vol. 193, Springer-Verlag, New York, 2000.
[7] J.E. Cremona, T.A. Fisher, C. O'Neil, D. Simon, M. Stoll, Explicit n-descent on elliptic curves. I. Algebra, J. Reine Angew. Math. 615 (2008) 121–155.
[8] Michel Demazure, Pierre Gabriel, Groupes algébriques. Tome I: Géométrie algébrique, généralités, groupes commutatifs, Masson & Cie, Éditeurs, Paris; North-Holland Publishing Co., Amsterdam, 1970, Avec un appendice *Corps de classes local* par Michiel Hazewinkel.
[9] Jürgen Klüners, Sebastian Pauli, Computing residue class rings and Picard groups of orders, J. Algebra 292 (1) (2005) 47–64.
[10] Stefano Marseglia, Computing the ideal class monoid of an order, J. Lond. Math. Soc. (2) 101 (3) (2020) 984–1007.
[11] F. Oort, Commutative group schemes, Lecture Notes in Mathematics, Vol. 15, Springer-Verlag, Berlin-New York, 1966.
[12] The Sage Developers, SageMath, the Sage Mathematics Software System, 2022, http://dx.doi.org/10.5281/zenodo.7132659, version 9.7.
[13] Schémas en groupes, II: Groupes de type multiplicatif, et structure des schémas en groupes généraux, Lecture Notes in Mathematics, Vol. 152, Springer-Verlag, Berlin-New York, 1970, Séminaire de Géométrie Algébrique du Bois Marie 1962/64 (SGA 3), Dirigé par M. Demazure et A. Grothendieck.
[14] Edward F. Schaefer, Michael Stoll, How to do a p-descent on an elliptic curve, Trans. Amer. Math. Soc. 356 (3) (2004) 1209–1231.
[15] Stephen S. Shatz, Principal homogeneous spaces for finite group schemes, Proc. Amer. Math. Soc. 22 (1969) 678–680.
[16] William C. Waterhouse, Principal homogeneous spaces and group scheme extensions, Trans. Amer. Math. Soc. 153 (1971) 181–189.