EXTENSIONS OF GROUP SCHEMES OF $\mu$-TYPE BY A CONSTANT GROUP SCHEME

HENDRIK VERHOEK

Abstract. For a number field $K$, a finite set of primes $S$ not containing a fixed prime $p$, we explain when extensions of group schemes of $\mu_p$ by $\mathbb{Z}/p\mathbb{Z}$ split over the ring of $S$-integers $O_S$ of $K$.

Contents

1. Introduction 1
2. Extensions of modules 1
3. Extensions of group schemes 3
4. Example calculations 5
References 7

1. Introduction

Let $p$ be a rational prime and $K$ a number field. Let $S$ be a finite set of primes in $K$ that does not contain primes above $p$. Let $\pi$ be a prime ideal above $p$ in $O_S$ and let $\hat{O}_S$ be the completion of $O_S$ at $\pi$. Denote by $\text{Ext}^1_{O_S}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ the group of equivalence classes of extensions of $\mu_p$ by the constant group scheme $\mathbb{Z}/p\mathbb{Z}$ in the category of finite flat commutative group schemes over $O_S$. Our main goal is to calculate the group $\text{Ext}^1_{O_S}(\mu_p, \mathbb{Z}/p\mathbb{Z})$:

Theorem 1.1. Suppose $p$ does not split in $K/\mathbb{Q}$. Let $\hat{L} = \hat{O}_S[\zeta_p/p]$ and $\omega : \text{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \to \mathbb{F}_p^\times$ be the cyclotomic character at $p$. Suppose that the $\omega^2$-eigenspace of the $p$-torsion of the class group of $O_S[\zeta_p/p]$ is trivial. Then

$$\text{Ext}^1_{O_S}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{F}_p \ker \left( (O_S[\zeta_p/p]^*/(O_S[\zeta_p/p]^*)^p)_{\omega^2} \to (\hat{L}^*/(\hat{L}^*)^p)_{\omega^2} \right).$$

Finite flat commutative group schemes of $p$-power order over a base where $p$ is invertible, are étale group schemes and therefore just Galois modules. Therefore we will consider in Section 2 extensions of modules with a group action. In Section 3 we move on to extensions of the finite flat group schemes $\mathbb{Z}/p\mathbb{Z}$ by $\mu_p$ that are killed by $p$ and prove Theorem 1.1. Finally, we calculate for various $K$ and $S$ the group $\text{Ext}^1_{O_S}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ using Theorem 1.1.

2. Extensions of modules

Let $R$ be a commutative unitary ring such that $p \cdot R = 0$ and let $G$ be a group. When we say $R$-module, we mean a left $R$-module. We will consider extensions of $R$-modules with an action of $G$, as a preparation for the next section, where we will discuss extensions of finite flat group schemes. We will use the following theorem of Grothendieck:
Theorem 2.1. Let $C_1, C_2$ and $C_3$ be abelian categories, such that $C_1$ and $C_2$ have enough injectives. Let $F_1 : C_1 \to C_2$ be a left exact functor that maps injective objects in $C_1$ to acyclic objects in $C_2$ and let $F_2 : C_2 \to C_3$ be a left exact functor. Then there is an exact sequence of low degree terms:

$$
0 \to (R^1 F_2)(F_1(A)) \to (R^1 F_2)(F_1)(A) \to F_2((R^1 F_1)(A)) \to (R^2 F_2)(F_1(A)) \to (R^2 F_2)(F_1)(A)
$$

Proof. See [We94] Theorem 5.8.3, p. 151. \(\square\)

Let $A$ and $B$ be two $R[G]$-modules such that $G$ acts trivially on $B$ and such that $H$ acts trivially on $A$. Let $\chi : G \to (\mathbb{Z}/p\mathbb{Z})^*$ and suppose that $H$ is contained in $\ker(\chi)$. Denote by $B(\chi)$ the $G$-module that has underlying group structure the one of $B$ and where the $G$-action is given by $\sigma b := \chi(\sigma)b$ for all $\sigma \in G$ and all $b \in B$. We let $G$ act on $\Hom_H(B, A)$ through the action of $G$ on $A$. Denote by $\Hom_H(B, A)_\chi$ the subgroup of $\Hom_H(B, A)$ on which $\Gamma = G/H$ acts through $\chi$.

Lemma 2.2. We have the following isomorphisms of groups:

$$\Hom_G(B(\chi), A) \simeq \Hom_H(B, A)_\chi.$$

Proof. Let $\psi : B \to B(\chi)$ be an $H$-linear isomorphism and let $\phi : \Hom_G(B(\chi), A) \to \Hom_H(B, A)_\chi$ such that $f \mapsto f \circ \psi$. The morphism $f \circ \psi$ is indeed an element in $\Hom_H(B, A)_\chi$ because for all $b$ in $B$ and $\sigma$ in $G$ the following equalities hold:

$$(\sigma(f \circ \psi))(b) = (f \circ \psi)(\sigma b) = f(\psi(\sigma b)) = f(\chi(\sigma)\psi(b)) = \chi(\sigma) f(\psi(b)).$$

Note that the second equality follows because $f$ is $G$-linear. Next we prove that the inverse morphism of $\phi$ is just precomposing with $\psi^{-1}$. For $g \in \Hom_H(B, A)_\chi$ we have $g \circ \psi^{-1} \in \Hom_G(B(\chi), A)$, because for all $b$ in $B(\chi)$ and all $\sigma$ in $G$:

$$(\sigma(g \circ \psi^{-1}))(b) = \chi(\sigma)(g \circ \psi^{-1})(b) = (g \circ \psi^{-1})(\chi(\sigma)b) = (g \circ \psi^{-1})(\sigma \cdot b).$$

\(\square\)

Proposition 2.3. Let $A$ and $B$ be two $R[G]$-modules such that $G$ acts trivial on $B$ and such that $H$ acts trivial on $A$. Then

$$\Ext_H^1(B, A)_\chi \simeq \Ext_G^1(B(\chi), A)$$

as $R$-modules.

Proof. We consider the following two functors: The left exact functor $F_1(\cdot) = \Hom_H(\cdot, A)$ from $R[G]$-modules to $R[G]$-modules and the exact functor $F_2$ “taking $\chi$-eigenspaces” from the category of $R[G]$-modules to $R[G]$-modules. With these two functors $F_1$ and $F_2$, we apply Theorem 2.1. Since $F_2$ is exact, the functors $F_1$ and $F_2$ give rise to the exact sequence

$$0 \to (R^1 F_2)(\Hom_H(B, A)) \to R^1(F_2 F_1)(B) \to \Ext_H^1(B, A)_\chi \to (R^2 F_2)(\Hom_H(B, A)) \to \ldots.$$
Since $F_2$ is exact, the $R[\Gamma]$-modules $R^1(F_2F_1)(B)$ and $\text{Ext}_R^1(B,A)_\chi$ are isomorphic. But $(F_2F_1)(B)$ is isomorphic to $\text{Hom}_G(B(\chi),A)$ by Lemma 2.2.

Define the functor $T_1$ "twisting with $\chi$" from the category of $R[G]$-modules to itself, the functor $T_2(\cdot) = \text{Hom}_G(\cdot,A)$ from the category of $R[G]$-modules to the category of $R$-modules and the forgetful functor $F$ that forgets the $\Gamma$ action and goes from the category of $R[\Gamma]$-modules to the category of $R$-modules. Then we have a natural isomorphism $FF_2F_1 \simeq T_2T_1$. The functor $T_1$ sends injective objects to injective objects, which are in particular acyclic objects. Hence, we can apply Theorem 2.1 to get the following exact sequence:

$$0 \to (R^1T_2)(B(\chi)) \to R^1(T_2T_1)(B) \to T_2(R^1T_1(B)) \to (R^2T_2)(T_1(B)) \to \ldots .$$

Since $T_1$ is exact, we obtain that $(R^1T_2)(B(\chi)) = \text{Ext}_R^1(B(\chi),A)$ is isomorphic to $R^1(T_2T_1)(B)$ as $R$-modules. Putting everything together, we now have isomorphisms of $R$-modules

$$\text{Ext}_R^1(B,A)_\chi \simeq R^1(F_2F_1)(B) \simeq R^1(T_2T_1)(B) \simeq \text{Ext}_G^1(B(\chi),A),$$

which is what we wanted to show.

When we take $\chi$ to be the trivial character in Proposition 2.3, we obtain the $\Gamma$-invariant extensions, which are as expected just extensions of $R[G]$-modules. We conclude by remarking that for two $R[G]$-modules $A$, $B$ and for a character $\chi$ of $G$, the $R$-module $\text{Ext}_G^1(A,B)$ is isomorphic to the $R$-module $\text{Ext}_G^1(A(\chi),B(\chi))$. Here $A(\chi)$ (resp. $B(\chi)$) is the twist of $A$ (resp. $B$) by $\chi$.

### 3. Extensions of group schemes

Recall that $\pi$ denotes the prime ideal above $p$ in the ring of $S$-integers $O_S$ of the number field $K$. In this section, the ring $R$ will be either the ring of $S$-integers $O_S$, the number field $K$, the completion of $O_S$ with respect to $\pi$ or the fraction field of such a completion of $O_S$. Since $p$ does not split in $K/\mathbb{Q}$, in each case we can talk about the fraction field of $R$, which we denote by $F$. Furthermore, let $L = F(\zeta_p)$ and $\Gamma = \text{Gal}(L/F)$.

First we state some facts from [KM85, Section 8.7-8.10]. Let $r$ be a unit in $R$. Consider the finite flat commutative group scheme

$$T(r) = \text{Spec}(\prod_{i=0}^{p-1} R[X_i]/(X_i^p - r^i)) = \coprod_{i=0}^{p-1} \text{Spec}(R[X_i]/(X_i^p - r^i))$$

over $R$. The scheme $T(r)$ is an extension of $\mathbb{Z}/p\mathbb{Z}$ by $\mu_p$. For an $R$-algebra $A$, the $A$-valued points in $T(r)$ are pairs $(a,i/p) \in (A,\mathbb{Q})$ such that $a^p = r^i$ and $0 \leq i \leq p - 1$. The group law of $T(r)$ can be described by

$$(a,i/p) \times (b,j/p) = \begin{cases} (ab,(i+j)/p), & i+j < p \\ (ab/r,(i+j-p)/p), & i+j \geq p \end{cases} .$$

The group schemes $T(r^p)$ are split extensions of $\mathbb{Z}/p\mathbb{Z}$ by $\mu_p$ and we see that in that case we have:

$$(a,i/p) = (ar^{-i},0) \times (r^i,i/p).$$

If $r$ and $r'$ are units in $R$, then the group schemes $T(r)$ and $T(r')$ are isomorphic if and only if $r$ and $r'$ generate the same subgroup in $R^*/(R^*)^p$. 
Lemma 3.1. The sequence

\[ 0 \to R^*/(R^*)^p \to \text{Ext}^1_{R[p]}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \to \text{Cl}(R)[p] \to 0 \]

is exact.

Proof. (cf. [Maz77] and [Sch09 Proposition 2.2]). Apply Hom(·,µp) to the exact sequence of fppf sheaves 0 → Z → Z → Z/pZ → 0 to obtain

\[ 0 \to \mu_p(R) \to \text{Ext}^1_{R[p]}(\mathbb{Z}/p\mathbb{Z}, \mu_p) \to \text{Ext}^1_{R[p]}(\mathbb{Z}, \mu_p) \simeq H^1_{\text{fppf}}(\text{Spec}(R), \mu_p) \to 0. \]

On the other hand, we apply the global section functor to the Kummer sequence of fppf sheaves

\[ 0 \to \mu_p \to \mathbb{G}_m \to \mathbb{G}_m \to 0 \]

to obtain

\[ 0 \to R^*/(R^*)^p \to H^1_{\text{fppf}}(\text{Spec}(R), \mu_p) \to \text{Cl}(R)[p] \to 0, \]

where Cl(R) is the class group of R. The lemma follows by [Sch09 Proposition 2.2 i)] that says that H^1_{\text{fppf}}(\text{Spec}(R), \mu_p) \simeq \text{Ext}^1_{R[p]}(\mathbb{Z}/p\mathbb{Z}, \mu_p). \qed

We focus again on the group Ext^1_{O_S}(µ_p, Z/pZ). If R is a completion of O_S at π, the group Ext^1_{R[p]}(µ_p, Z/pZ) is trivial since µ_p is connected and the connected-étale exact sequence gives a section for such extensions. Therefore, extensions of µ_p by Z/pZ are locally split and hence killed by p. Since the completion of O_S at π is flat over O_S, extensions of µ_p by Z/pZ over the ring O_S are also killed by p and Ext^1_{O_S}(µ_p, Z/pZ) = Ext^1_{O_S[p]}(µ_p, Z/pZ). Let ω: Γ = Gal(L/F) → F_p^* be the character such that for all σ ∈ Γ we have σ(ζ_p) = ω(σ). The scheme µ_p over R[ζ_p/p] is a constant group scheme and (µ_p)[R[ζ_p/p]] ≃ F_p((Z/pZ)[R[ζ_p/p]]. For integers 0 ≤ i, j ≤ p − 2 we have the following isomorphisms of F_p-modules:

\[ \text{Ext}^1_{R[ζ_p/p]}(Z/pZ(\omega^i), Z/pZ(\omega^j)) \simeq F_p \text{Ext}^1_{R[ζ_p/p]}(Z/pZ, µ_p). \]

Lemma 3.2. Ext^1_{R[1/p],|p|}(Z/pZ(ω^i), µ_p) ≃ F_p Ext^1_{R[ζ_p/p],|p|}(Z/pZ, µ_p)ω^i.

Proof. This follows immediately from Proposition 2.3. \qed

Corollary 3.3. If ζ_p ∉ R, then Ext^1_{R[ζ_p/p],|p|}(Z/pZ, µ_p) ≃ F_p \bigoplus_{i=0}^{p-2} \text{Ext}^1_{R[1/p],|p|}(Z/pZ(ω^i), µ_p).

Proof. The group Ext^1_{R[ζ_p/p],|p|}(Z/pZ, µ_p) is an F_p[Γ]-module. Hence it can be decomposed as

\[ \text{Ext}^1_{R[ζ_p/p],|p|}(Z/pZ, µ_p) \simeq F_p[Γ] \oplus \text{Ext}^1_{R[1/p],|p|}(Z/pZ, µ_p). \]

By Lemma 3.2 each summand is isomorphic to Ext^1_{R[1/p],|p|}(Z/pZ(ω^i), µ_p) as an F_p-module. \qed

Lemma 3.4 (Sch03, Corollary 2.4). Let J' and J'' be two finite flat commutative group schemes over O_S, let p be a prime and let O_S = (O_S ⊗ Z_p). Then the following sequence is exact:

\[ 0 \to \text{Hom}_{O_S}(J'', J') \to \text{Hom}_{O_S}(J'', J') \times \text{Hom}_{O_S[1/p]}(J'', J') \to \text{Hom}_{O_S[1/p]}(J'', J') \]

\[ \to \text{Ext}_{O_S}(J'', J') \to \text{Ext}_{O_S[1/p]}(J'', J') \times \text{Ext}_{O_S[1/p]}(J'', J') \to \text{Ext}_{O_S[1/p]}(J'', J'). \]

Lemma 3.5. If p does not split in K/Q, then \text{Hom}_{O_S[1/p]}(µ_p, Z/pZ) ≃ \text{Hom}_{O_S[1/p]}(µ_p, Z/pZ).
Proof. If \( \zeta_p \in K \) then both groups are cyclic of order \( p \). If \( \zeta_p \notin K \) then both groups are trivial. \( \square \)

We are now ready to prove Theorem 1.1.

Proof of Theorem 1.1. Consider the exact sequence of \( F_p[\Gamma] \)-modules of Lemma 3.1:

\[
0 \to \mathcal{O}_S[\zeta_p/p]^{*}/(\mathcal{O}_S[\zeta_p/p]^{*})^p \to \mathrm{Ext}^1_{\mathcal{O}_S[\zeta_p/p]}(\mathcal{O}_S[\zeta_p/p]/p^2 \mathcal{O}_S[\zeta_p/p], \mu_p) \to \mathrm{Cl}(\mathcal{O}_S[\zeta_p/p]/[p]) \to 0.
\]

The sequence is still left exact after taking \( \omega^2 \)-eigenspaces. The condition that the \( \omega^2 \)-eigenspace of the \( p \)-torsion of the class group \( \mathcal{O}_S[\zeta_p/p] \), denoted by \( \mathrm{Cl}(\mathcal{O}_S[\zeta_p/p]/[p])_{\omega^2} \), is trivial implies that

\[
(\mathcal{O}_S[\zeta_p/p]^{*}/(\mathcal{O}_S[\zeta_p/p]^{*})^p)_{\omega^2} \cong F_p[\Gamma] \mathrm{Ext}^1_{\mathcal{O}_S[\zeta_p/p]}(\mathcal{O}_S[\zeta_p/p]/p^2 \mathcal{O}_S[\zeta_p/p], \mu_p)_{\omega^2}.
\]

Remember that we assume that \( p \) does not split in \( K/Q \), hence \( \mathcal{O}_S[1/p] \) is a field. We obtain from Lemma 3.4 together with Lemma 3.3 the following exact sequence of \( F_p \)-modules:

\[
0 \to \mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mu_p, \mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p) \to \mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p) \to \mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p).
\]

Twisting by the character \( \omega \) gives the following two isomorphisms:

\[
\begin{align*}
\mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mu_p, \mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p) & \cong \mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p) \\
\mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mu_p, \mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p) & \cong \mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p).
\end{align*}
\]

In particular, we have isomorphisms between the \( p \)-torsion subgroups of these extension groups. From (1) we obtain

\[
0 \to \mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mu_p, \mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p) \to \mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p) \to \mathrm{Ext}^1_{\mathcal{O}_S[1/p]}(\mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p).
\]

By Lemma 3.2 we obtain

\[
0 \to \mathrm{Ext}^1_{\mathcal{O}_S}(\mu_p, \mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p) \to (\mathcal{O}_S[\zeta_p/p]^{*}/(\mathcal{O}_S[\zeta_p/p]^{*})^p)_{\omega^2} \to (\mathcal{O}_S[\zeta_p/p]^{*}/(\mathcal{O}_S[\zeta_p/p]^{*})^p)_{\omega^2}.
\]

\( \square \)

4. Example calculations

We calculate, using the isomorphism of Theorem 1.1, for specific \( p \) and \( \mathcal{O}_S \) the extension group \( \mathrm{Ext}^1_{\mathcal{O}_S}(\mu_p, \mathcal{O}_S[1/p]/p^2 \mathcal{O}_S[1/p], \mu_p) \). We will use the following lemma in the computations:

Lemma 4.1. The group \( Q_2^*/(Q_2^*)^2 \) is generated by 2, 3 and 5. For \( p > 2 \) the group \( Q_p^*/(Q_p^*)^p \) is generated by \( p \) and \( 1 + p \).

Proof. We have the following isomorphism of groups:

\[
Q_p^* \cong \mu_{p-1} \times p^2 \mathcal{O}_S[1/p] \times (1 + p^2 \mathcal{O}_S[1/p]).
\]

First we consider the case \( p > 2 \). Then \( (Q_p^*)^p = \mu_{p-1} \times p^{2p} \mathcal{O}_S[1/p] \times (1 + p^{2p} \mathcal{O}_S[1/p]) \). This follows from Hensel’s Lemma. The lemma follows from the fact that 3 and 5 are independent mod \( Q_2^* \), if they were not independent, 15 would be a square in \( Q_2 \), but 15 \( \neq 1 \) (mod 8). \( \square \)
The extension group $\text{Ext}_{\mathbb{Z}[\frac{1}{7}]}^1(\mu_2, \mathbb{Z}/2\mathbb{Z})$. We show that $\text{Ext}_{\mathbb{Z}[\frac{1}{7}]}^1(\mu_2, \mathbb{Z}/2\mathbb{Z})$ is trivial. Let $K = \mathbb{Q}$, $p = 2$ and $S = \{3\}$. It suffices to show that the homomorphism

$$(3) \quad \mathbb{Z}[\frac{1}{6}]^*/\mathbb{Z}[\frac{1}{6}]^{*2} \rightarrow \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$$

is injective. The non-squares in $\mathbb{Z}[\frac{1}{6}]^*$ are generated by 2, 3 and $-1$. By Lemma 4.1, the non-squares in $\mathbb{Q}_2^*$ are generated by 2, 3 and 5. Hence the homomorphism in (3) is injective.

The extension group $\text{Ext}_{\mathbb{Z}[\frac{1}{7}]}^1(\mu_3, \mathbb{Z}/3\mathbb{Z})$. Let $K = \mathbb{Q}(i)$, $p = 3$ and $S = \{(1 + i)\}$. Hence $O_S = \mathbb{Z}[i, \frac{1}{2}]$. The group $\Gamma$ is the Galois group of the extension $\mathbb{Q}(\zeta_{12})/\mathbb{Q}(i)$ and has order 4. The cyclotomic character $\omega$ at 3 is quadratic, so $\omega^2$ is trivial. The Hilbert class field of $\mathbb{Q}(\zeta_{12})$ is trivial. We will show that the group $\text{Ext}_{\mathbb{Z}[\frac{1}{7}]}^1(\mu_3, \mathbb{Z}/3\mathbb{Z})$ is trivial. It suffices to show that

$$\left(\mathbb{Z}[\zeta_{12}, \frac{1}{6}]^*/\mathbb{Z}[\zeta_{12}, \frac{1}{6}]^{*3}\right)^\Gamma \rightarrow \left(\mathbb{Q}_3(\zeta_{12})^*/\mathbb{Q}_3(\zeta_{12})^{*3}\right)^\Gamma$$

is injective.

Let $F_1$ be the functor from the category of $\mathbb{Z}[GQ]$-modules to the category of $\mathbb{Z}[\Gamma]$-modules defined by taking $\text{Gal}(\mathbb{Q}/\mathbb{Q}(\zeta_{12}))$-invariants. The functor $F_1$ sends injective objects to acyclic ones. Similarly, let $F_2$ be the functor of taking $\Gamma$-invariants from the category of $\mathbb{Z}[\Gamma]$-modules to the category of abelian groups. We apply Theorem 2.1 with the two functors $F_1$ and $F_2$ described above, and we take the object $A$ of Theorem 2.1 to be the $GQ(i)$-module $\mu_3$. Since the order of $\Gamma$ is coprime with the order of $\mu_3$, the derived functors of $F_2$ are zero. From the long exact sequence of Theorem 2.1 we see that

$$\left(\mathbb{Z}[\zeta_{12}, \frac{1}{6}]^*/\mathbb{Z}[\zeta_{12}, \frac{1}{6}]^{*3}\right)^\Gamma \simeq \mathbb{Z}[\frac{1}{6}]^*/\mathbb{Z}[\frac{1}{6}]^{*3}$$

and that

$$\left(\mathbb{Q}_3(\zeta_{12})^*/\mathbb{Q}_3(\zeta_{12})^{*3}\right)^\Gamma \simeq \mathbb{Q}_3^*/\mathbb{Q}_3^{*3}.$$

We proceed as in the previous example.

The extension group $\text{Ext}_{\mathbb{Z}[\frac{1}{7}]}^1(\mu_2, \mathbb{Z}/2\mathbb{Z})$. Let $K = \mathbb{Q}$, $p = 2$ and $S = \{7\}$. Note that $-7$ is a 2-adic square. Hence the kernel of

$$\mathbb{Z}[\frac{1}{14}]^*/\mathbb{Z}[\frac{1}{14}]^{*2} \rightarrow \mathbb{Q}_2^*/\mathbb{Q}_2^{*2}$$

is non-trivial and of order 2. A non-trivial extension of $\mu_2$ by $\mathbb{Z}/2\mathbb{Z}$ over $\mathbb{Z}[\frac{1}{7}]$ is generically isomorphic to the extension $T(-7)$ of $\mathbb{Z}/2\mathbb{Z}$ by $\mu_2$. However, this extension is locally at 2 a trivial extension. The Hopf algebra of such a non-trivial extension is given by

$$\mathbb{Z}[\frac{1}{7}][X, Y]/(X^2 - X - Y, Y^2 + 2Y)$$

with coalgebra maps $\Delta$ (comultiplication), $\epsilon$ (counit) and $S$ (coinverse):

$$\Delta(X) = X \otimes 1 + 1 \otimes X - 2X \otimes X + \frac{1}{7}Y \otimes Y - \frac{2}{7}(Y \otimes XY + XY \otimes Y) + \frac{4}{7}(XY \otimes XY)$$

$$\Delta(Y) = Y \otimes 1 + 1 \otimes Y + Y \otimes Y$$

$$\epsilon(X) = 0, \quad \epsilon(Y) = 0$$

$$S(X) = -X, \quad S(Y) = Y.$$
This group scheme is isomorphic to the 2-torsion subgroup scheme of the elliptic curve $J_0(49)$.

References

[KM85] Nicholas M. Katz and Barry Mazur. Arithmetic moduli of elliptic curves, volume 108 of Annals of Mathematics Studies. Princeton University Press, Princeton, NJ, 1985.

[Maz77] B. Mazur. Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math., (47):33–186 (1978), 1977.

[Sch03] René Schoof. Abelian varieties over cyclotomic fields with good reduction everywhere. Math. Ann., 325(3):413–448, 2003.

[Sch09] René Schoof. Semistable abelian varieties with good reduction outside 15, 2009. preprint.

[Wei94] Charles A. Weibel. An introduction to homological algebra, volume 38 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 1994.