PERIODS OF GENERIC TORSORS OF GROUPS OF MULTIPLICATIVE TYPE

WANSHUN WONG

Abstract. In this paper we establish different ways to compute the period of a generic torsor of a group of multiplicative type. We also study the relationships among the periods of generic torsors of Q, T and W, where Q is a group of multiplicative type, T is the maximal subtorus of Q and W is the maximal finite quotient group of Q.

1. Introduction

Let F be our fixed base field, and let Q be a smooth commutative linear algebraic group over F. For every field extension K/F, there is a bijective correspondence between the set of isomorphism classes of Q-torsors (principal homogeneous spaces) over K and the first Galois cohomology group $H^1(K,Q)$. The period of a Q-torsor is the order of the corresponding element in $H^1(K,Q)$. Note that the period of a Q-torsor is always finite as $H^1(K,Q)$ is a torsion group.

A short exact sequence of linear algebraic groups

$$1 \longrightarrow Q \longrightarrow P \xrightarrow{\phi} S \longrightarrow 1 ,$$

where P is connected, reductive and special, is called a resolution of Q. Since we can embed Q into $\mathbf{GL}_n$ for some positive integer n, resolutions of Q exist. The generic fiber of the morphism $\phi : P \to S$ is a Q-torsor over the function field $F(S)$ of S, moreover it is a generic Q-torsor (see [1, section 6] and [5]). In this paper by a generic Q-torsor, we mean a generic Q-torsor that arises from a resolution of Q as above.

When Q is an algebraic torus, the period of a generic Q-torsor is studied in [7]. Based on the technique developed in [7], we generalize the results to the case where Q is a smooth group of multiplicative type (see Corollary 4.3). We also study in Section 5 the relationships among the periods of generic torsors of Q, T and W, where T is the maximal subtorus of Q and W is the maximal finite quotient group of Q. In Section 6 we give an application of our results.

2. Periods of Generic Torsors

Proposition 2.1. *Let Q be a smooth commutative linear algebraic group over F. Assume that one of the following conditions hold:*

(a) F is infinite.

(b) The connected component Q^0 of Q is reductive.

2000 *Mathematics Subject Classification.* 11E72, 20G15.

Key words and phrases. Generic Torsor, Galois Cohomology, Groups of Multiplicative Type.

Then the period of a generic Q-torsor is divisible by the period of any Q-torsor over any field extension K/F.

Proof. The proof is essentially the same as that of [7, Proposition 1.1]. Suppose that F is a finite field. Then by assumption the connected component Q^0 of Q is reductive.
Claim: The natural map $H^1(F,Q) \to H^1(F((t)),Q)$ is injective.

The following argument is suggested by Philippe Gille. Consider the exact sequence of linear algebraic groups over F

$$\begin{tikzcd} 1 \arrow[r] & Q^0 \arrow[r] & Q \arrow[r] & \pi_0(Q) \arrow[r] & 1 \end{tikzcd}$$

where $\pi_0(Q)$ is finite étale. It induces the following commutative diagram

$$\begin{tikzcd} \pi_0(Q)(F) \arrow[r] \arrow[d, "\cong"] & H^1(F,Q^0) \arrow[r] \arrow[d, "f_1"] & H^1(F,Q) \arrow[r] \arrow[d, "f_2"] & H^1(F,\pi_0(Q)) \arrow[d, "f_3"] \\ \pi_0(Q)(F((t))) \arrow[r] & H^1(F((t)),Q^0) \arrow[r] & H^1(F((t)),Q) \arrow[r] & H^1(F((t)),\pi_0(Q)) \end{tikzcd}$$

By [6, Theorem I.1.2.2] f_1 is injective. Notice that f_3 is injective also, hence by four lemma f_2 is injective.

It follows from the claim that we may replace F by $F((t))$ and assume that our base field is infinite.

Let $E \to \operatorname{Spec} F(S)$ be a generic Q-torsor that arises from a resolution of Q

$$\begin{tikzcd} 1 \arrow[r] & Q \arrow[r] & P \arrow[r, "\phi"] & S \arrow[r] & 1 \end{tikzcd} .$$

We denote by $[E]$ the class of Q-torsor $E \to \operatorname{Spec} F(S)$ in $H^1(F(S),Q)$, and $[P]$ the class of $\phi : P \to S$ in the first étale cohomology group $H^1_{ét}(S,Q)$. Then $[E]$ is equal to the image of $[P]$ under the natural map $H^1_{ét}(S,Q) \to H^1_{ét}(\operatorname{Spec} F(S),Q) = H^1(F(S),Q)$. As $H^1(F(S),Q)$ is the colimit of $H^1_{ét}(U,Q)$ over all nonempty open subsets $U \subseteq S$, there exists a nonempty open U such that the order of $[P]_U$, where $[P]_U$ is the image of $[P]$ in $H^1_{ét}(U,Q)$, is equal to the order of $[E]$.

Let R be a Q-torsor over K, where K is a field extension over F. The above resolution induces a long exact sequence

$$\begin{tikzcd} P(K) \arrow[r] & S(K) \arrow[r] & H^1(K,Q) \arrow[r] & H^1(K,P) \end{tikzcd} . \tag{1}$$

Since P is special, $H^1(K,P)$ is trivial. Thus there exists a point $s \in S(K)$ such that the class $[R]$ of R in $H^1(K,Q)$ is equal to the class of the Q-torsor $\phi^{-1}(s)$. Notice that K is infinite, it follows from [2, Corollary 18.3] that the set K-rational points $P(K)$ is dense in P. This implies that $\phi(P(K))$ is dense in S because $\phi : P \to S$ is surjective. Hence $\phi(P(K)) \cdot s$ is also dense in S and there exists a point $s' \in U \cap (\phi(P(K)) \cdot s)$. From the long exact sequence (1) the class of $\phi^{-1}(s')$ is equal to that of $\phi^{-1}(s)$. Therefore by replacing s by s' we may assume $s \in U(K)$. Then the morphism $s : \operatorname{Spec} K \to U \to S$ induces the following map

$$\begin{array}{ccccc} H^1_{ét}(S,Q) & \longrightarrow & H^1_{ét}(U,Q) & \longrightarrow & H^1_{ét}(\operatorname{Spec} K,Q) = H^1(K,Q) \\ [P] & \longmapsto & [P]_U & \longmapsto & [\phi^{-1}(s)] = [R] \end{array}$$

It follows that the order of $[R]$ divides the order of $[P]_U$, which is equal to the order of $[E]$. □

By Proposition 2.1 all generic Q-torsors have the same period. In other words, the period of a generic Q-torsor depends only on Q, and we denote this number by $e(Q)$. Proposition 2.1 also shows that $e(Q)$ is the smallest positive integer that annihilates $H^1(K,Q)$ for every field extension K/F. Thus $e(Q)$ can be viewed as the "exponent" of the first Galois cohomology functor

$$H^1(-,Q) : Fields/F \longrightarrow Ab$$

where $Fields/F$ is the category of field extensions of F and field homomorphisms over F, and Ab is the category of abelian groups.

3. Preliminaries on Groups of Multiplicative Type

Unless otherwise specified, all groups of multiplicative type in this paper are over F and are smooth, and they all split over a finite Galois extension L/F. Let G be the Galois group $Gal(L/F)$, and let Q^* be the character G-module of a group of multiplicative type Q over L. Notice that the connected component of a smooth group of multiplicative type is a torus, which is reductive, hence we can apply Proposition 2.1.

Let

$$\theta : \qquad 1 \longrightarrow Q \longrightarrow R \xrightarrow{g} S \longrightarrow 1$$

be an exact sequence of groups of multiplicative type, where S is a torus.

For any subgroup H of G, we have the following pairing:

$$H^0(H, \mathrm{Hom}_{\mathbb{Z}}(Q^*, \mathbb{Z})) \otimes H^1(H, S^*) \to \mathrm{Ext}^1_G(Q^*, S^*). \tag{2}$$

First we identify

$$H^0(H, \mathrm{Hom}_{\mathbb{Z}}(Q^*, \mathbb{Z})) = \mathrm{Hom}_G(Q^*, \mathbb{Z}[G/H]) = \mathrm{Ext}^0_G(Q^*, \mathbb{Z}[G/H])$$

and

$$H^1(H, S^*) = \mathrm{Ext}^1_H(\mathbb{Z}, S^*) = \mathrm{Ext}^1_G(\mathbb{Z}[G/H], S^*).$$

Then we use the composition product for Ext,

$$\mathrm{Ext}^0_G(Q^*, \mathbb{Z}[G/H]) \otimes \mathrm{Ext}^1_G(\mathbb{Z}[G/H], S^*) \to \mathrm{Ext}^1_G(Q^*, S^*).$$

The following proposition is a slight generalization of [7, Proposition 2.1].

Proposition 3.1. *The following are equivalent:*

(a) For every field extension K/F, the homomorphism $g_K : R(K) \to S(K)$ is surjective.

(b) The generic point ξ of S in $S(F(S))$ is in the image of $g_{F(S)}$.

(c) The exact sequence θ has a rational splitting.

(d) There exists a commutative diagram of morphisms of groups of multiplicative type with splitting field L/F:

$$\begin{tikzcd}
1 \arrow[r] & P \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & S \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & Q \arrow[r] & R \arrow[r, "g"] & S \arrow[r] & 1
\end{tikzcd}$$

with exact rows and P is a quasi-split torus.

(e) The class of the exact sequence θ in $\mathrm{Ext}^1_G(Q^*, S^*)$ lies in the image of the map

$$\varphi : \coprod_{H<G} H^0(H, \mathrm{Hom}_{\mathbb{Z}}(Q^*, \mathbb{Z})) \otimes H^1(H, S^*) \to \mathrm{Ext}^1_G(Q^*, S^*)$$

induced by the pairing (2)*, where the coproduct is taken over all subgroups H of G.*

If S is coflasque, these conditions are also equivalent to

(f) The exact sequence θ splits.

Proof. (a) ⇒ (b): Obvious.

(b) ⇒ (c): Let $x \in R(F(S))$ be a point such that $g_{F(S)}(x) = \xi$. The commutative diagram

$$\begin{tikzcd} \operatorname{Spec} F(S) \arrow[r, "x"] \arrow[dr, "\xi"'] & R \arrow[d, "g"] \\ & S \end{tikzcd}$$

implies that there is a nonempty open subset $U \subseteq S$ together with the following commutative diagram

$$\begin{tikzcd} U \arrow[r] \arrow[dr, "i"'] & R \arrow[d, "g"] \\ & S \end{tikzcd}$$

where $i : U \to S$ is the inclusion.

(c) ⇒ (d): By assumption there exists a rational splitting $h : S \dashrightarrow R$. Let U be the domain of definition of h, and let Λ be the lattice $L[U]^\times/L^\times$. The character lattice S^* of S is isomorphic to $L[S]^\times/L^\times$ which is a sublattice of Λ, and the factor lattice Λ/S^* is permutation by the proof of [3, Proposition 5]. Let M and P be the tori with character lattices Λ and Λ/S^* respectively.

The character group R^* of R is isomorphic to a subgroup of $L[R]^\times$ (the subgroup of group-like elements), therefore there is a natural homomorphism $R^* \to L[R]^\times/L^\times$. The morphism $h : U \to R$ induces a homomorphism $L[R]^\times/L^\times \to \Lambda$. The composition $R^* \to L[R]^\times/L^\times \to \Lambda$ then induces a morphism of groups of multiplicative type $M \to R$. Since h is a splitting, by construction the composition $M \to R \to S$ is equal to the morphism $M \to S$ induced by the inclusion $S^* \hookrightarrow \Lambda$.

(d) ⇒ (a): For every K/F, $H^1(K, P) = 0$ implies $M(K) \to S(K)$ is surjective, so g_K is also surjective.

(d) ⇔ (e): The diagram in (d) exists if and only if there is a quasi-split torus P and a homomorphism $\alpha : Q^* \to P^*$ such that the class of the exact sequence θ lies in the image of the induced map $\alpha^* : \mathrm{Ext}^1_G(P^*, S^*) \to \mathrm{Ext}^1_G(Q^*, S^*)$. Since P is quasi-split, P^* is a direct sum of lattices of the form $\mathbb{Z}[G/H]$, where H is a subgroup of G.

Consider the case $P^* = \mathbb{Z}[G/H]$. The map α is given by an element $a \in H^0(H, \mathrm{Hom}_{\mathbb{Z}}(Q^*, \mathbb{Z}))$. Also, we have shown that $\mathrm{Ext}^1_G(\mathbb{Z}[G/H], S^*) = H^1(H, S^*)$. Then the map α^* coincides with multiplication by a with respect to the pairing (2).

(f) ⇒ (c): Obvious.

(e) ⇒ (f) if S is coflasque: Notice that $H^1(H, S^*) = 0$ for every subgroup H of G because S is coflasque. Therefore $\mathrm{im}(\varphi)$ is trivial, and it implies that θ is a split short exact sequence. □

4. Main result

Let

$$\chi: \qquad 1 \longrightarrow Q \xrightarrow{\iota} P \longrightarrow S \longrightarrow 1$$

be a coflasque resolution of Q, i.e. P is a quasi-split torus and S is a coflasque torus. By [4, Proposition 1.3] coflasque resolutions of Q exist.

Theorem 4.1. *Let $f : Q \to Q'$ be a morphism of groups of multiplicative type. Then the following are equivalent:*

(a) f factors through $\iota : Q \to P$.

(b) f factors through some quasi-split torus.

(c) The induced map $H^1(K, Q) \to H^1(K, Q')$ is the zero homomorphism for every field extension K/F.

Proof. It is clear that (a) ⇒ (b) ⇒ (c), so it suffices to prove (c) ⇒ (a).

Assume (c) holds. Let R be a group of multiplicative type defined by the following commutative diagram

$$\begin{tikzcd}
\chi: & 1 \arrow[r] & Q \arrow[r, "\iota"] \arrow[d, "f"] & P \arrow[r] \arrow[d] & S \arrow[r] \arrow[d, equal] & 1 \\
\theta: & 1 \arrow[r] & Q' \arrow[r] & R \arrow[r, "g"] & S \arrow[r] & 1
\end{tikzcd}$$

where the rows are exact. For every field extension K/F, the commutative diagram

$$\begin{tikzcd}
P(K) \arrow[r] \arrow[d] & S(K) \arrow[r] \arrow[d, equal] & H^1(K, Q) \arrow[d, "0"] \\
R(K) \arrow[r, "g_K"] & S(K) \arrow[r] & H^1(K, Q')
\end{tikzcd}$$

shows that $g_K : R(K) \to S(K)$ is surjective. Since S is coflasque, by Proposition 3.1 θ is a split short exact sequence. Then the result follows easily from the the following commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & Q \arrow[r, "\iota"] \arrow[d, "f"] & P \arrow[r] \arrow[d] & S \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & Q' \arrow[r] \arrow[d, equal] & R \arrow[r, "g"] \arrow[d, "\cong"] & S \arrow[r] \arrow[d, equal] & 1 \\
1 \arrow[r] & Q' \arrow[r, "i_1"] & Q' \oplus S \arrow[r, "p_2"] & S \arrow[r] & 1,
\end{tikzcd}$$

where i_1 and p_2 are canonical inclusion and projection respectively. □

Remark 4.2. Note that (b) ⇒ (a) can be proved directly as follows (see [3, Lemma 4]): Suppose f factors through a quasi-split torus R, our goal is to show that $f : Q \to R \to Q'$ factors as $Q \xrightarrow{\iota} P \to R \to Q'$.

Consider the exact sequence

$$\mathrm{Hom}_G(R^*, P^*) \xrightarrow{\iota^*} \mathrm{Hom}_G(R^*, Q^*) \longrightarrow \mathrm{Ext}^1_G(R^*, S^*)\ .$$

Since R^* is a permutation module and S^* is coflasque, $\mathrm{Ext}^1(R^*, S^*)$ is trivial. Hence $R^* \to Q^*$ factors as $R^* \to P^* \xrightarrow{\iota^*} Q^*$.

If Q' is a torus, by [4, Proposition 1.3] there exists a flasque resolution of Q'

$$\kappa : \qquad 1 \longrightarrow S' \longrightarrow P' \xrightarrow{\rho} Q' \longrightarrow 1\ ,$$

i.e. a short exact sequence where P' is a quasi-split torus and S' is a flasque torus. Using the same argument above we can show that the conditions in Theorem 4.1 are also equivalent to

(d) f factors through $\rho : P' \to Q'$.

The following corollary shows that $e(Q)$ can be computed in many different ways.

Corollary 4.3. *The following numbers are the same:*

(i) $e(Q)$*, the period of a generic* Q*-torsor.*

(ii) n_1 := *the smallest positive integer* n *such that the morphism* $Q \xrightarrow{n} Q$ *factors through* $\iota : Q \to P$*.*

(iii) The order of the class of χ *in* $\mathrm{Ext}^1_G(Q^*, S^*)$*.*

(iv) n_2 := *the smallest positive integer* n *such that the morphism* $Q \xrightarrow{n} Q$ *factors through some quasi-split torus.*

If Q *is a torus, then* Q *has a flasque resolution* κ*, and the above numbers are also equal to*

(v) n_3 := *the smallest positive integer* n *such that the morphism* $Q \xrightarrow{n} Q$ *factors through* $\rho : P' \to Q$*.*

(vi) The order of the class of κ *in* $\mathrm{Ext}^1_G(S'^*, Q^*)$*.*

Proof. First, it is clear that n_1 is equal to the order of the class of χ. Then by the equivalence of (a) and (b) in Theorem 4.1 we have $n_1 = n_2$. Finally, recall that $e(Q)$ is equal to the smallest integer n such that $H^1(K, Q) \xrightarrow{n} H^1(K, Q)$ is the zero homomorphism for every field extension K/F, therefore by Theorem 4.1 again we get $e(Q) = n_1 = n_2$.

If Q is a torus, by Remark 4.2 we see that $n_2 = n_3$, which is also equal to the order of class of κ. ☐

Example 4.4. Let Q be a group of multiplicative type. Then $e(Q) = 1$ if and only if Q is a direct summand of a quasi-split torus, i.e. if and only if Q is an invertible torus.

Example 4.5. Let L/F be a finite Galois extension with Galois group $Gal(L/F) = G$. Consider the norm 1 torus $Q = R^{(1)}_{L/F}(\mathbb{G}_{m,L})$, i.e. the torus defined by the short exact sequence

$$\chi : \qquad 1 \longrightarrow Q \longrightarrow R_{L/F}(\mathbb{G}_{m,L}) \xrightarrow{N} \mathbb{G}_m \longrightarrow 1$$

where N is the norm map. Notice that the above exact sequence is a coflasque resolution of Q, hence $e(Q)$ is equal to the order of the class of the following exact sequence of character lattices (also denoted by χ)

$$\chi: \qquad 0 \longrightarrow \mathbb{Z} \xrightarrow{N} \mathbb{Z}[G] \longrightarrow Q^* \longrightarrow 0$$

in $\mathrm{Ext}^1_G(Q^*, \mathbb{Z})$. The norm map of character lattices $N : \mathbb{Z} \to \mathbb{Z}[G]$ is given by $N(1) = \sum_{g \in G} g$. It is then easy to verify that $e(Q) =$ order $([\chi]) = |G| = [L : F]$.

5. Relationships among $e(W), e(T)$ and $e(Q)$

For any group of multiplicative type Q, we have an exact sequence

$$\zeta: \qquad 1 \longrightarrow T \longrightarrow Q \longrightarrow W \longrightarrow 1$$

where T is a torus and W is finite. The existence of the exact sequence ζ comes from the fact that the $\mathbb{Z}$-torsion elements of Q^* form a G-submodule (W^*) of Q^*.

Lemma 5.1. *$e(W) =$ exponent of W.*

Proof. Denote the exponent of W by n. Since $W^n = 1$, the homomorphism $H^1(K, W) \xrightarrow{n} H^1(K, W)$ factors through $H^1(K, 1) = 0$ for every field extension K/F. Hence $e(W) \mid n$.

Recall that L is a splitting field of W, so $W_L = \mu_{n_1} \times \cdots \times \mu_{n_r}$ for some positive integers $n_1, \ldots, n_r$, where the least common multiple $\mathrm{lcm}\{n_1, \ldots, n_r\}$ of $n_1, \ldots, n_r$ is equal to n. Then for every field extension K/L,

$$\begin{aligned} H^1(K, W_L) &= H^1(K, \mu_{n_1}) \times \cdots \times H^1(K, \mu_{n_r}) \\ &= K^\times/(K^\times)^{n_1} \times \cdots \times K^\times/(K^\times)^{n_r}. \end{aligned}$$

Therefore $n = \mathrm{lcm}\{n_1, \ldots, n_r\} = e(W_L) \mid e(W)$ by Proposition 2.1. □

Remark 5.2. Lemma 5.1 can also proved by using Corollary 4.3. First, $e(W)$ is the smallest positive integer n such that the morphism $W^* \xrightarrow{n} W^*$ factors through a permutation module. Since W^* is finite and any permutation module is $\mathbb{Z}$-torsion free, $e(W)$ equals the smallest integer n such that $nw = 0$ for every $w \in W^*$, which is just the exponent of W.

Example 5.3. Let Q be the group scheme of n-th roots of unity μ_n over F, where $char(F)$ does not divide n. The exact sequence

$$\chi: \qquad 1 \longrightarrow \mu_n \longrightarrow \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \longrightarrow 1$$

is a coflasque resolution of Q. It is known that $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$, and $[\chi]$ is the canonical generator of $\mathrm{Ext}^1_{\mathbb{Z}}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})$. Hence we recover the result $e(\mu_n) = n$.

Next we are going to find a lower bound for $e(Q)$ in terms of $e(T)$ and $e(W)$.

Lemma 5.4. *$e(W) \mid e(Q)$.*

Proof. Since L is a splitting field of Q, we have $Q_L = T_L \times W_L$ and T_L is a split torus. Therefore $e(W_L) = e(Q_L)$. It remains to observe that $e(W) = e(W_L)$ by Lemma 5.1, and $e(Q_L) \mid e(Q)$ by Proposition 2.1. □

Lemma 5.5. *$e(T) \mid e(Q)$.*

Proof. By Theorem 4.1 $Q^* \xrightarrow{e(Q)} Q^*$ factors through $\iota^* : P^* \to Q^*$. Since P^* is a permutation module, it is $\mathbb{Z}$-torsion free and the homomorphism $Q^* \to P^*$ factors through T^*. This is illustrated in the following commutative diagram

$$\begin{tikzcd}
Q^* \arrow[rr, "e(Q)"] \arrow[d, two heads, "\pi"] & & Q^* \\
T^* \arrow[r] & P^* \arrow[ur, "\iota^*"] &
\end{tikzcd}$$

Then the composition $T^* \longrightarrow P^* \xrightarrow{\iota^*} Q^* \xrightarrow{\pi} T^*$ is just the homomorphism of multiplication by $e(Q)$. Therefore $e(T) \mid e(Q)$. ☐

Corollary 5.6. $\operatorname{lcm}\{e(T), e(W)\} \mid e(Q)$.

Let λ be the order of $[\zeta]$ in $\operatorname{Ext}^1_G(T^*, W^*)$. Then λ is the smallest positive integer such that $T^* \xrightarrow{\lambda} T^*$ factors through Q^*,

$$\begin{tikzcd}
T^* \arrow[r, "\psi"] & Q^* \arrow[r, two heads] & T^*
\end{tikzcd}$$

for some $\psi : T^* \to Q^*$. Since $Q^* = T^* \oplus W^*$ as an abelian group, we can write every element in Q^* in the form (x, y) where $x \in T^*, y \in W^*$.

Lemma 5.7. *ψ can be chosen so that $\psi(x) = (\lambda x, 0)$ for every $x \in T^*$.*

Proof. First note that T^* is isomorphic to λT^* as a G-module, because T^* is $\mathbb{Z}$-free. Consider the following exact sequence of G-modules

$$0 \longrightarrow W^* \longrightarrow \lambda Q^* + W^* \longrightarrow \lambda T^* \longrightarrow 0 \tag{3}$$

where $\lambda Q^* + W^*$ is a submodule of Q^*, and the homomorphisms are the canonical ones. The composition

$$\lambda T^* \xrightarrow{\cong} T^* \xrightarrow{\psi} \lambda Q^* + W^*$$

is a splitting homomorphism for (3). Therefore $\lambda Q^* + W^*$ is isomorphism to $\lambda T^* \oplus W^*$ as G-modules. ☐

Proposition 5.8. $\operatorname{lcm}\{e(T), e(W)\} \mid e(Q) \mid \operatorname{lcm}\{\lambda e(T), e(W)\}$.

Proof. By Corollary 5.6 it suffices to prove the second divisibility. Choose ψ such that $\psi(x) = (\lambda x, 0)$ for every $x \in T^*$. Let $n = \operatorname{lcm}\{e(T), \frac{e(W)}{\lambda}\}$, where λ divides $e(W)$ because λ is also the smallest positive integer such that $W^* \xrightarrow{\lambda} W^*$ factors through Q^*. Then we consider the composition

$$\begin{array}{ccccccccc}
\beta : & Q^* & \longrightarrow & T^* & \xrightarrow{n} & T^* & \xrightarrow{\psi} & Q^* \\
& (x, y) & \longmapsto & x & \longmapsto & nx & \longmapsto & (\lambda n x, 0).
\end{array}$$

Since $e(W)$ is equal to the exponent of W^*, β is just the endomorphism of Q^* given by multiplication by λn. By Theorem 4.1, $T^* \xrightarrow{n} T^*$ factors through a permutation module. Therefore β also factors through a permutation module, and it implies that

$$e(Q) \mid \lambda n = \operatorname{lcm}\{\lambda e(T), e(W)\}.$$ ☐

The following examples show that the inequalities in Proposition 5.8 are sharp.

Example 5.9. Let L/F be a quadratic field extension and $char(F) \neq 2$, and let σ be the generator of $G = Gal(L/F)$. Consider the group of multiplicative type Q given by $Q^* = \mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ (as abelian group) with G-action $\sigma(a, b) = (-a, a + b)$, where $char(F)$ does not divide n. By [7, Example 4.1] $e(T) = [L : F] = 2$, and by Lemma 5.1 $e(W) = n$.

By using [4, Lemma 0.6] we can construct a coflasque resolution of Q^* explicitly and show that $e(Q) = 2n$. In particular, if $n = 2$, then $\lambda = 2$ also and we have $\operatorname{lcm}\{\lambda e(T), e(W)\} = 4 = e(Q) > \operatorname{lcm}\{e(T), e(W)\}$.

Example 5.10. Let L/F be a field extension such that $G = Gal(L/F)$ is a cyclic group of order 4, for example $F = \mathbb{Q}(i)$ and $L = \mathbb{Q}(\xi_{16})$, and let σ be a generator of G. Let T be the torus given by

$$\begin{tikzcd} 1 \arrow[r] & \mathbb{G}_m \arrow[r] & R_{L/F}(\mathbb{G}_m) \arrow[r] & T \arrow[r] & 1 \end{tikzcd} .$$

Then T^* is (isomorphic to) the kernel of the augmentation map $\mathbb{Z}[G] \to \mathbb{Z}$. As an abelian group T^* is generated by $a := 1 - \sigma,\ b := 1 - \sigma^2,\ c := 1 - \sigma^3$.

Consider $Q^* = T^* \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ (as abelian group) with G-action

$$\sigma(xa + yb + zc,\ \overline{u},\ \overline{v}) = ((-x - y - z)a + xb + yc,\ \overline{x} + \overline{y} + \overline{v},\ \overline{u})$$

for every $x, y, z \in \mathbb{Z}$ and for every $\overline{u}, \overline{v} \in \mathbb{Z}/2\mathbb{Z}$. By direction verification

$$\begin{tikzcd} 0 \arrow[r] & \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \arrow[r] & Q^* \arrow[r] & T^* \arrow[r] & 0 \end{tikzcd}$$

does not split, hence $\lambda = 2$. By [7, Example 4.1] $e(T) = [L : F] = 4$. We claim that $e(Q) = 4$ also by noting that $Q^* \xrightarrow{4} Q^*$ factors as

$$\begin{tikzcd} Q^* \arrow[r, two heads] & T^* \arrow[r, "i"] & \mathbb{Z}[G] \arrow[r, "\phi"] & Q^* \end{tikzcd}$$

where i is the inclusion, and ϕ is given by $\phi(1) = (a+b+c, 0, 0)$. Hence $\operatorname{lcm}\{e(T), e(W)\} = 4 = e(Q) < \operatorname{lcm}\{\lambda e(T), e(W)\}$.

6. Application

In the proof of Lemma 5.5 we have shown that $Q^* \xrightarrow{e(Q)} Q^*$ factors as

$$\begin{tikzcd} Q^* \arrow[r, two heads, "\pi"] & T^* \arrow[r] & P^* \arrow[r] & Q^* \end{tikzcd}$$

where P^* is a permutation module. If we write $Q^* = T^* \oplus W^*$ (as an abelian group), the composition homomorphism $T^* \to Q^*$ above is injective as it is given by $x \mapsto (e(Q) \cdot x, 0)$. Let Z be the group of multiplicative type defined by $Z^* = Q^* / \operatorname{im}(T^*)$, and we have an exact sequence

$$\begin{tikzcd} 1 \arrow[r] & Z \arrow[r] & Q \arrow[r] & T \arrow[r] & 1 \end{tikzcd} .$$

Passing to cohomology we obtain

$$\begin{tikzcd} H^1(K, Z) \arrow[r] & H^1(K, Q) \arrow[rr, "0"] \arrow[dr] & & H^1(K, T) \\ & & H^1(K, P) \arrow[ur] & \end{tikzcd} .$$

Therefore Z is a finite subgroup of Q, with exponent $e(Q)$, such that the natural map $H^1(K, Z) \to H^1(K, Q)$ is surjective for every field extension K/F.

The following proposition shows that the exponent of any finite subgroup of Q with such property must be at least $e(Q)$.

Proposition 6.1. *Let Q be a group of multiplicative type, and Z be any finite subgroup of Q such that $H^1(K, Z) \to H^1(K, Q)$ is surjective for every field extension K/F. Then $e(Q)$ divides the exponent of Z.*

Proof. First we recall that by Lemma 5.1 the exponent of the finite group Z is equal to $e(Z)$. For every field extension K/F, $e(Z) \cdot H^1(K, Z) = 0$. By assumption $H^1(K, Z) \to H^1(K, Q)$ is surjective, hence $e(Z) \cdot H^1(K, Q) = 0$ also. It follows that $e(Q)$ divides $e(Z)$. ☐

Acknowledgements

The author would like to thank his adviser Alexander Merkurjev for his help.

References

[1] G. Berhuy and G. Favi, *Essential dimension: a functorial point of view (after A. Merkurjev)*, Documenta Math. **8** (2003), 279–330.

[2] A. Borel, *Linear Algebraic Groups*, Graduate Texts in Mathematics **126**, 2nd Enlarged Edition, Springer-Verlag, New York, 1991.

[3] J.-L. Colliot-Thélène and J.-J. Sansuc, *La R-équivalence sur les tores*, Ann. Sci. Éc. Norm. Sup. (4) **10** no. 2 (1977), 175–229.

[4] J.-L. Colliot-Thélène and J.-J. Sansuc, *Principal Homogeneous Spaces under Flasque Tori: Applications*, Journal of Algebra **106** (1987), 148–225.

[5] S. Garibaldi, A. Merkurjev, and J.-P. Serre, *Cohomological Invariants in Galois Cohomology*, University Lecture Series **28**, American Mathematical Society, Providence, RI, 2003.

[6] P. Gille, *Torseurs sur la droite affine et R-équivalence*, Orsay (1994), Author's website.

[7] A. S. Merkurjev, *Periods of principal homogeneous spaces of algebraic tori*, Vestnik St. Petersburg University, Mathematics **43** no. 1 (2010), 39–43.

Department of Mathematics, University of California, Los Angeles, CA 90095-1555, USA
E-mail address: `wanshunwong@gmail.com`