HASSE NORM PRINCIPLE FOR GALOIS DIHEDRAL EXTENSIONS

FELIPE RIVERA-MESAS

Abstract. Let $L/k$ an Galois extension of number fields with Galois group isomorphic to a dihedral group of order $2n$. In this note, we give a general description of the Hasse norm principle for $L/k$ and the weak approximation for the norm one torus $R_{L/k}^1(\mathbb{G}_m)$ associated to $L/k$.

1. Introduction

Given a number field extension $L/k$, we say that the Hasse norm principle (HNP) holds for $L/k$ if every element of $L$ which is a local norm everywhere is a global norm. In other words, if $A_L$ denotes the adele ring and $N_{L/k}$ denotes the adelic norm induced by the norm $N_{L/k}: L^* \to k^*$, then the HNP holds for $L/k$ if the group

$$K(L/k) = k^* \cap N_{L/k}(A_L^*) / N_{L/k}(L^*)$$

is trivial. Furthermore, we can get a geometric interpretation of the Hasse norm principle for $L/k$ as follows: we have the following exact sequence of algebraic tori

$$1 \to R_{L/k}^1(\mathbb{G}_m) \to R_{L/k}(\mathbb{G}_m) \xrightarrow{N_{L/k}} \mathbb{G}_m, k \to 1,$$

where $R_{L/k}(\mathbb{G}_m)$ denotes the Weil restriction of $\mathbb{G}_m$ from $L$ to $k$ and $N_{L/k}$ is the map induced by the norm from $L$ to $k$. The torus $R_{L/k}^1(\mathbb{G}_m)$ is called the norm one torus associated to $L/k$. In this way, the group $\mathcal{R}(L/k)$ is isomorphic to the Tate-Shafarevich group $\text{III}^1(k, R_{L/k}^1(\mathbb{G}_m))$ of $R_{L/k}^1(\mathbb{G}_m)$. Now, recalling that $\text{III}^1(k, R_{L/k}^1(\mathbb{G}_m))$ is the obstruction to Hasse Principle for torsors under $R_{L/k}^1(\mathbb{G}_m)$, we have that the HNP holds for $L/k$ if and only if the Hasse Principle holds for torsors under $R_{L/k}^1(\mathbb{G}_m)$.

Given a $k$-torus $T$, we say that Weak Approximation (WA) holds for $T$ if its $k$-points are dense in the product of its local points. Equivalently, Weak Approximation holds for $T$ if the group

$$A(T) = \left( \prod_v T(k_v) \right) / T(k)$$

is trivial.

Voskresenski˘ı in [Vos70] gives the following exact sequence, which makes a link between the Hasse principle for torsors under a torus $T$ and the WA for $T$:

$$0 \to A(T) \to H^1(k, \text{Pic} \overline{T}) \xrightarrow{(-)^*} \text{III}^1(k, T) \to 0,$$

where $\overline{T}$ is a smooth compatification of $T$ and $(-)^* = \text{Hom}(-, \mathbb{Q}/\mathbb{Z})$. In particular, when $T$ is the norm one torus $R_{L/k}^1(\mathbb{G}_m)$ associated to a number field extension $L/k$,
the Voskresenskiĭ exact sequence links the HNP for $L/k$ and the WA for $T$. When the extension $L/k$ is Galois we have the following two facts:

- Colliot-Thélène has proved [CTS77, Proposition 7] that the central object of the Voskresenskiĭ exact sequence is isomorphic to $H^3(\text{Gal}(L/k), \mathbb{Z})$;
- Tate has given [CF10, p. 198] an explicit description of $\text{III}^1(k, T)$ as follows:

$$\text{III}^1(k, T) \cong \ker \left[ \text{Res} : H^3(\text{Gal}(L/k), \mathbb{Z}) \to \prod_{v \in \Omega_k} H^3(G_v, \mathbb{Z}) \right],$$

where $\Omega_k$ denotes the set of all places of $k$ and $G_v$ denotes the decomposition group of $v$. Thus, we also have the following isomorphism:

$$A(T) \cong \text{im} \left[ \text{Res} : H^3(\text{Gal}(L/k), \mathbb{Z}) \to \prod_{v \in \Omega_k} H^3(G_v, \mathbb{Z}) \right].$$

We will focus on this case, i.e. when $L/k$ is Galois. In this notes, we will give a general description of the HNP for $L/k$ and the WA for $T$ when $L/k$ has Galois group isomorphic to $D_n$, the dihedral group of order $2n$.

The following result gives us a general criterion for determining when a Galois extension of number fields with Galois group a dihedral group satisfies the HNP or when its norm one torus associated $R^1_{L/k}(\mathbb{G}_m)$ has WA.

**Theorem 1.1.** Let $L/k$ be a Galois extension of number fields with Galois group isomorphic to $D_n$, the dihedral group of order $2n$. Let $T := R^1_{L/k}(\mathbb{G}_m)$ the norm one torus associated to $L/k$. Then, we have the following

1. if $n$ is odd, then the HNP holds for $L/k$ and the WA holds for $T$;
2. if $n$ is even, then
   a. If there exists $v \in \Omega_k$ such that $G_v$ contains a Klein subgroup of $G$, then HNP holds for $L/k$ and WA fails for $T$;
   b. If for every $v \in \Omega_k$ the group $G_v$ does not contain a Klein subgroup, then HNP fails for $L/k$ and WA holds for $T$.

In particular, the WA holds for $T$ if and only if for every $v \in \Omega_k$ the group $G_v$ does not contain a Klein subgroup of $G$.

2. HNP for $L/k$ and WA for $T := R^1_{L/k}(\mathbb{G}_m)$

The goal of this section is to give an explicit description of the group $H^3(G, \mathbb{Z})$ when $G$ is a dihedral group and a general description of the restriction maps

$$H^3(G, \mathbb{Z}) \to H^3(H, \mathbb{Z}),$$

for every $H \leq G$. Let $G := D_n$ the dihedral group of orden $2n$, i.e.

$$G = \langle r, s \mid r^n = s^2 = e, \ srs = r^{-1} \rangle.$$
2.1. Description of the group $H^3(G, \mathbb{Z})$

The following proposition gives an explicit description of $H^3(G, \mathbb{Z})$.

**Proposition 2.1.** Let $G$ be a dihedral group of order $2n$. The group $H^3(G, \mathbb{Z})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})[2]$.

**Proof.** From the Hochschild-Serre spectral sequence associated to the split exact sequence

$$1 \to \mathbb{Z}/n\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 1$$

and the constant $G$-module $\mathbb{Q}/\mathbb{Z}$, we have the following exact sequence:

$$H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to \ker(\text{Res}) \to H^1(\mathbb{Z}/2\mathbb{Z}, H^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})) \xrightarrow{\lambda} H^3(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z}),$$

where $\text{Res} := \text{Res} : H^2(G, \mathbb{Q}/\mathbb{Z}) \to H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})$. Since $\mathbb{Z}/2\mathbb{Z}$ is cyclic and $\mathbb{Q}$ is uniquely divisible, we have

$$H^2(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \cong H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}) = 0,$$

and similarly we have $H^2(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) = 0$. Thus, the previous exact sequence becomes

$$0 \to H^2(G, \mathbb{Q}/\mathbb{Z}) \to H^1(\mathbb{Z}/2\mathbb{Z}, H^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})) \xrightarrow{\lambda} H^3(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z}).$$

Now, the exact sequence $1 \to \mathbb{Z}/n\mathbb{Z} \to G \to \mathbb{Z}/2\mathbb{Z} \to 1$ is split. Then, since $\mathbb{Q}/\mathbb{Z}$ is constant, we have that the map

$$\text{Inf} : H^3(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \to H^3(G, \mathbb{Q}/\mathbb{Z}),$$

is injective. On the other hand, from the Hochschild-Serre spectral sequence, we have the complex

$$H^1(\mathbb{Z}/2\mathbb{Z}, H^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z})) \xrightarrow{\lambda} H^3(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\text{Inf}} H^3(G, \mathbb{Q}/\mathbb{Z}).$$

Hence, $\lambda$ is trivial and then $H^2(G, \mathbb{Q}/\mathbb{Z}) \cong H^1(\mathbb{Z}/2\mathbb{Z}, H^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z}))$. Now,

$$H^1(\mathbb{Z}/2\mathbb{Z}, H^1(\mathbb{Z}/n\mathbb{Z}, \mathbb{Q}/\mathbb{Z})) \cong H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}),$$

with $\mathbb{Z}/2\mathbb{Z}$ acting on $\mathbb{Z}/n\mathbb{Z}$ by taking the inverse. Thus we have that

$$H^3(G, \mathbb{Z}) \cong H^2(G, \mathbb{Q}/\mathbb{Z}) \cong H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})[2],$$

where the last isomorphism is obtained from a direct computation on cocycles and coboundaries. \qed

2.2. Study of restriction maps $H^3(G, \mathbb{Z}) \to H^3(H, \mathbb{Z})$.

Now, in order to find a general description for III$_1(k, T)$, we will study all restriction maps

$$\text{Res}_{G/H} : H^3(G, \mathbb{Z}) \to H^3(H, \mathbb{Z}),$$

with $H \leq G$.

For convenience, we will introduce the following notation: for a subgroup $H \leq G$ and a $G$-module $M$, we denote by $\text{Res}_{G/H}(M)$ the restriction map

$$\text{Res} : H^i(G, M) \to H^i(H, M).$$

The following lemma helps us for this purpose.
Lemma 2.2. Suppose that $n$ is even. If $H \leq G$ is a dihedral subgroup of index 2 and order divisible by 4, then $\ker(\text{Res}_{G/H}^3(\mathbb{Z}))$ is trivial.

Remark 2.3. Note that the condition about the divisibility by 4 of the order of $H$ implies that $H$ contains a Klein subgroup of $G$.

Proof. Without loss of generality, we may suppose that $H = \langle r^2, s \rangle$. We have the following exact sequence

$$0 \to H \to G \to \mathbb{Z}/2\mathbb{Z} \to 0,$$

where $\mathbb{Z}/2\mathbb{Z}$ is generated by $\tau$. Now, by the Hochschild-Serre spectral sequence, we have the inclusion

$$\ker(\text{Res}_{G/H}^2(\mathbb{Q}/\mathbb{Z})) \hookrightarrow H^1(\mathbb{Z}/2\mathbb{Z}, H^1(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}/\mathbb{Z})) \cong H^1(\mathbb{Z}/2\mathbb{Z}, H^{ab}),$$

where $\mathbb{Z}/2\mathbb{Z}$ acts on $H^{ab}$ via $\tau(h[H,H]) = (hr^{-1})[H,H]$. Since $H$ contains a Klein subgroup of $G$ (cf. Remark 2.3), we have that $H^{ab} = \langle s[H,H], sr^2[H,H] \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Now, since $\mathbb{Z}/2\mathbb{Z}$ is cyclic, we have that

$$H^1(\mathbb{Z}/2\mathbb{Z}, H^{ab}) \cong H^{-1}(\mathbb{Z}/2\mathbb{Z}, H^{ab}) = \ker(N)/\langle 1 - \tau \rangle H^{ab},$$

where $N : H^{ab} \to H^{ab}$ is the norm map. We note that

$$N(s[H,H]) = N(sr^2[H,H]) = r^2[H,H] \neq [H,H]$$

and

$$(1 - \tau)s[H,H] = (1 - \tau)(sr^2[H,H]) = r^2[H,H].$$

Hence, $H^1(\mathbb{Z}/2\mathbb{Z}, H^{ab})$ is trivial. Therefore, since $H^i(G, \mathbb{Z}) \cong H^{i-1}(G, \mathbb{Q}/\mathbb{Z})$ for $i > 1$, $\ker(\text{Res}_{G/H}^3(\mathbb{Z})) \cong \ker(\text{Res}_{G/H}^2(\mathbb{Q}/\mathbb{Z}))$ is trivial.

The following result gives a general description of the restriction maps $\text{Res}_{G/H}^3(\mathbb{Z})$.

Proposition 2.4. Let $G \cong D_n$ and $H \leq G$. Then

$$\text{Res} : H^3(G, \mathbb{Z}) \to H^3(H, \mathbb{Z}) = \begin{cases} 
\text{id} & \text{if } H \text{ contains a Klein subgroup of } G; \\
0 & \text{if } H \text{ does not contain a Klein subgroup of } G.
\end{cases}$$

Proof. Let us recall that all subgroups of $G$ are either cyclic or a dihedral group $D_k$ with $k$ dividing $n$. Now, if $H$ is cyclic or a dihedral group $D_k$ with $k$ odd, then $H^3(H, \mathbb{Z}) = 0$ by Proposition 2.1. Thus, if $H$ has order non divisible by 4, then $\text{Res}_{G/H}^3(\mathbb{Z})$ is trivial.

In particular, when $n$ is odd, all restriction maps $\text{Res}_{G/H}^3(\mathbb{Z})$ are trivial. Then, we only have to prove the proposition when $n$ is even and $H$ is a dihedral group $D_k$, with $k$ even. If $n = 2^{v_2(n)} \ell$, let $H' \cong D_m$ with $m = 2^{v_2(k)} \ell$ and $H \leq H'$. Now, we can get a sequence of groups

$$H'' = G \supseteq H'_1 \supseteq \ldots \supseteq H'_r = H',$$

where $r = v_2(n) - v_2(k)$, $H'_i \cong D_{k_i}$ and $[H'_{i-1} : H'_i] = 2$ for all $i > 0$. Then, by Lemma 2.2 we have that

$$\text{Res} : H^3(H''_{i-1}, \mathbb{Z}) \to H^3(H'_i, \mathbb{Z}).$$
is injective for all \( i > 0 \). On the other hand, by Proposition 2.1, we have that \( \text{Res} : H^3(H', \mathbb{Z}) \rightarrow H^3(H, \mathbb{Z}) \) is injective since \( [H' : H] \) is odd and \( \text{Cores} \circ \text{Res} = [H' : H] \). Hence,

\[
\text{Res}_{G/H} = \text{Res}_{G/H} \circ \ldots \circ \text{Res}_{H'/H} \circ \text{Res}_{H'/H}
\]

is injective.

The results above allows us to prove the Theorem 1.1:

**Proof of the Theorem 1.1.** When \( n \) is odd the central object of the Voskresenskiĭ exact sequence is trivial and therefore \( \text{III}^1(k, T) = A(T) = 0 \). On the other hand, when \( n \) is even, the group \( H^3(G, \mathbb{Z}) \) is isomorphic to \( \mathbb{Z}/2\mathbb{Z} \), and then the Voskresenskiĭ exact sequence becomes

\[
0 \rightarrow A(T) \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow \text{III}^1(k, T) \rightarrow 0,
\]

Besides, we note that \( \text{III}^1(k, T) \) is trivial iff there exists \( v \in \Omega_k \) such that the restriction map

\[
\text{Res}_v : H^3(G, \mathbb{Z}) \rightarrow H^3(G_v, \mathbb{Z})
\]

is not trivial and, by Proposition 2.4 this occurs iff there exists \( v \in \Omega_k \) such that \( G_v \) contains a Klein group. Whence we conclude the proof of the theorem.

\[ \square \]

**References**

[CF10] J.W.S. Cassels and A. Fröhlich. *Algebraic Number Theory: Proceedings of an Instructional Conference Organized by the London Mathematical Society (a NATO Advanced Study Institute) with the Support of the International Mathematical Union*. London Mathematical Society, 2010.

[CTS77] Jean-Louis Colliot-Thélène and Jean-Jacques Sansuc. La \( R \)-équivalence sur les tores. *Ann. Sci. École Norm. Sup. (4)*, 10(2):175–229, 1977.

[Vos70] V E Voskresenskiĭ. Birational properties of linear algebraic groups. *Mathematics of the USSR-Izvestiya*, 4(1):1–17, feb 1970.

Departamento de Matemáticas, Facultad de Ciencias, Universidad de Chile

Email address: felipe.rivera.m@ug.uchile.cl