Local-global principles for norms

André Macedo

A thesis submitted for the degree of
Doctor of Philosophy

Department of Mathematics and Statistics
University of Reading
May 2021

Declaration

This thesis describes the work undertaken at the Department of Mathematics and Statistics of the University of Reading, in fulfilment of the requirements for the degree of Doctor of Philosophy. The results in Chapter 3 and Part II are a reproduction of the author's work in the papers [62] and [65], respectively. The results in Chapters 4, 5 and 6 comprise joint work with Rachel Newton in the paper [64]. The work in the final Chapter 12 will appear in the upcoming preprint [66].

I confirm that this is my own work and the use of all material from other sources has been properly and fully acknowledged.

André Macedo

Acknowledgements

First and foremost, I would like to heartily thank my supervisor, Rachel Newton, for excellent guidance, countless discussions and for being a source of unlimited encouragement and support throughout my PhD. You were truly a fantastic mentor and working with you for the past 3 years has been the most fun I have had doing mathematics.

I am also very grateful to my second supervisor, Titus Hilberdink, for many helpful discussions on the analytic side of my work and to Chris Daw for several interesting number-theoretic conversations and continuous encouragement. I would like to thank Karl-Mikael Perfekt for serving in my monitoring committee as well as Kristine Aldridge, Jani Virtanen and Ruth Harris for their administrative help throughout the entire PhD. I am grateful to Boris Kunyavskiĭ for asking the question that propelled my first research project, to Eva Bayer-Fluckiger for a conversation in Istanbul that made me look at the multinorm principle and to Ila Varma for enlightening discussions about her work on D_4-fields. Thank you to all my past teachers for always encouraging my interest in mathematics and for endless patience in dealing with my excessive curiosity.

I am deeply indebted to several amazing people that made my time in Reading less lonely. Namely, I am very grateful to Anni for huge moral and emotional support at the most crucial times of the PhD and lots of fun weekends, to Abdul for his daily dose of joy and countless soccer conversations and to Maha for her soothing presence around the office and many recharging work breaks.

Finally, a very special "obrigado" goes to my family and friends in Portugal. Thank you mom for all your love and for opening so many doors for me – I hope this PhD completes the dream you had for me years ago when you chose to give me the best education you could. Thank you grandpa and grandma for being the prime example in my life of what hard work can achieve and for showing me that it is more important to be kind than to be right – you were my first and most important teachers and this thesis is dedicated to you. Thank you Félix, Íris, Jéssica and Tiago for your unconditional friendship and reminders that there is so much more to life than mathematics. Thank you Francisca for your treasured love, warm support and for being a rainbow of bliss at the end of this stormy journey.

The research in this thesis was made possible by the generous financial support of the *Fundação para a Ciência e Tecnologia* via the doctoral scholarship SFRH/BD/117955/2016.

Abstract

This thesis is a collection of several qualitative and quantitative studies on local-global principles for norms obtained by the author during the course of his PhD.

In the first part of this thesis we study the *Hasse norm principle*, a classical local-global principle for norms of number fields first introduced by Hasse. We exploit the geometric interpretation of this principle to obtain a new result, namely the validity of the Hasse norm principle for any A_n-extension of degree $n \geq 5$. We also develop theoretical methods and give explicit results on the obstruction to the Hasse norm principle and the defect of *weak approximation* for the associated norm one torus. We describe how to implement these results in order to compute the obstructions to the local-global principles in the computer algebra system GAP. We further apply our methods to do a detailed study of the Hasse norm principle and weak approximation for the norm one torus of *any* extension with normal closure having alternating or symmetric Galois group.

In the second part we investigate the so-called *multinorm principle*, a natural generalization of the Hasse norm principle to a finite number of extensions. We generalize work of Drakokhrust–Platonov to provide explicit and computable formulas for the obstructions to the multinorm principle and weak approximation for the multinorm one torus. These formulas are given in terms of *generalized representation groups* of Galois groups, a tool that makes them fairly easy to manipulate and amenable to computation. We subsequently illustrate the flexibility of our methods by studying the multinorm principle in three concrete families, extending results of Bayer-Fluckiger–Lee–Parimala, Demarche–Wei and Pollio.

In the third and final part of this thesis we obtain several statistical results on the Hasse norm principle and weak approximation for norm one tori. We show that 100% of degree $n \leq 15$ extensions of a number field k with bounded discriminant satisfy the Hasse norm principle. This result is given as conditional on the *weak Malle conjecture*, but we also present unconditional results for $n = 4$ and $n = 6$ by exploiting certain known cases of this conjecture over $k = \mathbb{Q}$. Finally, we capitalize on recent advances in arithmetic statistics by Shankar–Varma and Altuğ–Shankar–Varma–Wilson to determine the density of octic D_4-extensions of $\mathbb{Q}$ that fail the Hasse norm principle, when ordered by discriminant or by conductor.

Notation

Given a field k, we use the notation $\overline{k}$ for a (fixed) algebraic closure of k, unless stated otherwise. If k is a global field and L/k is a Galois extension, we use the following notation:

$\mathbb{A}_k^*$	the idèle group of k
$\mathcal{O}_k$	the ring of integers of k
Ω_k	the set of all places of k
L_v	the completion of L at some choice of place above $v \in \Omega_k$
D_v	the Galois group of L_v/k_v

Given a field K, a variety X over K and an algebraic K-torus T, we use the following notation:

$\mathbb{G}_{m,K}$	the multiplicative group $\operatorname{Spec}(K[t,t^{-1}])$ of K (when K is clear from the context we omit it from the subscript)
X_L	the base change $X \times_K L$ of X to a field extension L/K
$\overline{X}$	the base change of X to an algebraic closure of K
$\operatorname{Pic} X$	the Picard group of X
$R_{K/k}X$	the Weil restriction of X to a subfield k of K such that $[K:k]$ is finite
$\widehat{T}$	the character group $\operatorname{Hom}(\overline{T}, \mathbb{G}_{m,\overline{K}})$ of T

Let G be a finite group. The label 'G-module' shall always mean a free $\mathbb{Z}$-module of finite rank equipped with an action of G. Given a subgroup H of G, a G-module A, an integer q, a non-negative integer i and a prime number p, we use the following notation:

$\lvert G\rvert$	the order of G
$\exp(G)$	the exponent of G
$Z(G)$	the center of G
$[H,G]$	the subgroup of G generated by all commutators $[h,g]$ with $h \in H, g \in G$
$\Phi^G(H)$	the subgroup of H generated by all commutators $[h,g]$ with $g \in G$ and $h \in H \cap gHg^{-1}$
G^{ab}	the abelianization $G/[G,G]$ of G
$G^{\sim}$	the $\mathbb{Q}/\mathbb{Z}$-dual $\operatorname{Hom}(G,\mathbb{Q}/\mathbb{Z})$ of G
G_p	a Sylow p-subgroup of G
$\mathrm{H}_i(G,A)$	the i-th homology group
$\mathrm{H}^i(G,A)$	the i-th cohomology group

$\hat{\mathrm{H}}^q(G, A)$	the q-th Tate cohomology group[1]
$Ш^q_\omega(G, A)$	the kernel of the restriction map $\hat{\mathrm{H}}^q(G, A) \xrightarrow{\mathrm{Res}} \prod_{g \in G} \hat{\mathrm{H}}^q(\langle g \rangle, A)$.

We also use the notation G' for the derived subgroup $[G, G]$ of G. If H is a normal subgroup of G, we write $H \trianglelefteq G$. For $x, y \in G$ we adopt the convention $[x, y] = x^{-1}y^{-1}xy$ and $x^y = y^{-1}xy$. If G is abelian and $d \in \mathbb{Z}_{>0}$, we use the following notation:

$G[d]$	the d-torsion of G
$G_{(d)}$	the d-primary part of G.

We often use '=' to indicate a canonical isomorphism between two objects.

[1] Since $\hat{\mathrm{H}}^q(G, A) = \mathrm{H}^q(G, A)$ for $q \geq 1$, we will omit the hat in this case.

“If you’re walking down the right path and you’re willing to keep walking, eventually you’ll make progress.”

- Barack Obama

Table of Contents

Chapter 1

Background

In this chapter we review several background concepts and results which will be used throughout the thesis.

1.1 Group cohomology

Given a homomorphism $f : G \to H$ of groups and an H-module A, we can regard A as an G-module via f and there are induced homomorphisms of cohomology groups

$$f^* : \mathrm{H}^i(H, A) \to \mathrm{H}^i(G, A)$$

for each $i \in \mathbb{Z}_{\geq 0}$, see [15, III, §8]. Similarly, f gives rise to homomorphisms of homology groups

$$f_* : \mathrm{H}_i(G, A) \to \mathrm{H}_i(H, A)$$

for each $i \in \mathbb{Z}_{\geq 0}$. The most important examples of such maps for us will be the *restriction* and *corestriction* maps.

Definition 1.1.1. Let H be a subgroup of a group G and let A be a G-module. For each $i \in \mathbb{Z}_{\geq 0}$, the embedding $H \hookrightarrow G$ induces maps $\mathrm{Res}^G_H : \mathrm{H}^i(G, A) \to \mathrm{H}^i(H, A)$ and $\mathrm{Cor}^G_H : \mathrm{H}_i(H, A) \to \mathrm{H}_i(G, A)$ called *restriction* and *corestriction*, respectively.

The restriction and corestriction maps commute with the cohomology and homology boundary homomorphisms, respectively. Therefore, by dimension shifting (see [18, p. 104]), these maps can be extended to all Tate cohomology groups $\hat{\mathrm{H}}^i$, $i \in \mathbb{Z}$. We collect some well-known results about these maps below.

Lemma 1.1.2. *Let $K \leq H \leq G$ be a tower of groups with $[G : K]$ finite. Then*

$$\mathrm{Res}^G_K = \mathrm{Res}^H_K \circ \mathrm{Res}^G_H \text{ and } \mathrm{Cor}^G_K = \mathrm{Cor}^G_H \circ \mathrm{Cor}^H_K .$$

Proof. See [15, III, Proposition 9.5(i)]. □

Lemma 1.1.3. *Let G be a finite group and H a subgroup of G. Let A be a G-module. Then*

$$\mathrm{Cor}^G_H \circ \mathrm{Res}^G_H : \hat{\mathrm{H}}^i(G, A) \to \hat{\mathrm{H}}^i(G, A)$$

equals the multiplication by $[G : H]$ map.

Proof. See [15, III, Proposition 9.5(ii)]. □

Lemma 1.1.4. *Let G be a finite group and G_p a Sylow p-subgroup of G. For any G-module A and any $i \in \mathbb{Z}_{>0}$, the restriction map*

$$\mathrm{Res}^G_{G_p} : \mathrm{H}^i(G, A) \to \mathrm{H}^i(G_p, A)$$

maps $\mathrm{H}^i(G, A)_{(p)}$ injectively into $\mathrm{H}^i(G_p, A)$.

Proof. See [15, III, Theorem 10.3]. □

Lemma 1.1.5. *(Inflation-Restriction) Let G be a group, H a normal subgroup of G and A a G-module. Then there is a fundamental exact sequence, called the inflation-restriction exact sequence,*

$$0 \to \mathrm{H}^1(G/H, A^H) \xrightarrow{\mathrm{Inf}} \mathrm{H}^1(G, A) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(H, A)^{G/H} \xrightarrow{\mathrm{Tr}} \mathrm{H}^2(G/H, A^H) \xrightarrow{\mathrm{Inf}} \mathrm{H}^2(G, A),$$

where Inf *denotes the inflation map (see [34, Construction 3.3.9, p. 63]) and* Tr *denotes the transgression map (see [34, Remark 3.3.16, p. 67]).*

Proof. See [34, Proposition 3.3.14]. □

Definition 1.1.6. Let A be an H-module. We define the co-induced module $\mathrm{Ind}^G_H(A)$ to be the set of functions $\varphi : G \to A$ such that $\varphi(hg) = h\varphi(g)$ for all $h \in H, g \in G$. This set naturally has a structure of a G-module via the operations

$$(\varphi + \varphi')(g) = \varphi(g) + \varphi'(g)$$

$$(g'\varphi)(g) = \varphi(gg')$$

for all $\varphi, \varphi' \in \mathrm{Ind}^G_H(A)$, $g, g' \in G$.

Lemma 1.1.7 (Shapiro's lemma)**.** *Let H be a subgroup of a group G. Let A be an H-module. Then*

$$\mathrm{H}^i(G, \mathrm{Ind}_H^G(A)) = \mathrm{H}^i(H, A)$$

for each $i \geq 0$.

Proof. See [18, IV, §4, Proposition 2]. □

Lemma 1.1.8. *Let H be a subgroup of a group G. Let A be a G-module and let i be a positive integer. Let $f : \mathrm{H}^i(G, A) \to \mathrm{H}^i(G, \mathrm{Ind}_H^G(A))$ be the map on cohomology induced by the homomorphism $A \to \mathrm{Ind}_H^G(A)$ sending $a \in A$ to the function $g \mapsto ga$ of $\mathrm{Ind}_H^G(A)$. Let* sh *be the canonical isomorphism given in Shapiro's lemma 1.1.7. Then*

$$\mathrm{sh} \circ f = \mathrm{Res}_H^G : \mathrm{H}^i(G, A) \to \mathrm{H}^i(H, A).$$

Proof. See [95, Ex. 3.7.14(iii), p. 131]. □

We will mainly use the concept in Definition 1.1.6 when $A = \mathbb{Z}$ is the H-module with the trivial action. In this case, it is easy to check that the assignment $f \mapsto \sum_{gH \in G/H} f(g^{-1})gH$ identifies $\mathrm{Ind}_H^G(\mathbb{Z})$ with the G-module $\mathbb{Z}[G/H]$.

Lemma 1.1.9. *Let G be a group. Then $\mathrm{H}^i(H, \mathbb{Z}[G]) = 0$ for all integers $i > 0$ and all subgroups H of G.*

Proof. See [34, III, Lemma 3.3.15]. □

1.2 Duality

Definition 1.2.1. Let G be a finite abelian group. The *Pontryagin dual* of G is the group

$$G^\sim := \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z}).$$

Definition 1.2.2. Let G, G' be finite abelian groups. If $f : G \to G'$ is a group homomorphism, then the *dual* $f^\sim$ of f is the homomorphism $f^\sim \colon G'^\sim \to G^\sim$ defined by

$$f^\sim(g')(g) = g'(f(g))$$

for all $g \in G, g' \in G'^\sim$.

Lemma 1.2.3. *If $f\colon G \to G'$ is a homomorphism of finite abelian groups, then*

$$\mathrm{Ker}(f^{\sim}) \cong \mathrm{Coker}(f)^{\sim}$$

Proof. Applying the left-exact contravariant functor $\mathrm{Hom}(-, \mathbb{Q}/\mathbb{Z})$ to the exact sequence

$$G \xrightarrow{f} G' \to \mathrm{Coker}(f) \to 0$$

gives the exact sequence

$$0 \to \mathrm{Hom}(\mathrm{Coker}(f), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(G', \mathbb{Q}/\mathbb{Z}) \xrightarrow{f^{\sim}} \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$$

and the result follows. □

Let G be a group and let A, B be G-modules.

Theorem 1.2.4 (Cup-products)**.** *There exists a unique family of bi-additive pairings (called cup-products)*

$$\begin{aligned} \cup\colon\ \mathrm{H}^i(G, A) \times \mathrm{H}^j(G, B) &\longrightarrow \mathrm{H}^{i+j}(G, A \otimes B) \\ (a, b) &\longmapsto a \cup b \end{aligned}$$

defined for all integers $i, j \geq 0$ satisfying the following conditions:

1. *for any homomorphism $A \to A'$ of G-modules, the induced diagram*

$$\begin{tikzcd} \mathrm{H}^i(G, A) \times \mathrm{H}^j(G, B) \arrow[r, "\cup"] \arrow[d] & \mathrm{H}^{i+j}(G, A \otimes B) \arrow[d] \\ \mathrm{H}^i(G, A') \times \mathrm{H}^j(G, B) \arrow[r, "\cup"] & \mathrm{H}^{i+j}(G, A' \otimes B) \end{tikzcd}$$

   commutes. Similarly, the analogous diagram for a homomorphism $B \to B'$ of G-modules commutes.

2. *if $i = j = 0$, the pairing $\cup$ is simply*

$$\begin{aligned} A^G \times B^G &\longrightarrow (A \otimes B)^G \\ (a, b) &\longmapsto a \otimes b \end{aligned}$$

3. *if $0 \to A \to A' \to A'' \to 0$ is an exact sequence of G-modules such that*

$$0 \to A \otimes B \to A' \otimes B \to A'' \otimes B \to 0$$

is also exact, then

$$(\delta a'') \cup b = \delta(a'' \cup b), \quad \forall a'' \in \mathrm{H}^i(G, A''), \quad \forall b \in \mathrm{H}^j(G, B)$$

where the map δ on the left denotes the connecting homomorphism

$$\mathrm{H}^i(G, A'') \to \mathrm{H}^{i+1}(G, A)$$

and δ on the right denotes the connecting homomorphism

$$\mathrm{H}^{i+j}(G, A'' \otimes B) \to \mathrm{H}^{i+j+1}(G, A \otimes B).$$

4. *if $0 \to B \to B' \to B'' \to 0$ is an exact sequence of G-modules such that*

$$0 \to A \otimes B \to A \otimes B' \to A \otimes B'' \to 0$$

is also exact, then

$$a \cup (\delta b'') = (-1)^i \delta(a \cup b''), \quad \forall a \in \mathrm{H}^i(G, A), \quad \forall b'' \in \mathrm{H}^j(G, B'')$$

where again, by abuse of notation, δ denotes the corresponding boundary maps.

Proof. See [71, II, Proposition 1.38]. □

If G is further assumed to be finite, then for every integer i the cup-product above defines a pairing

$$F_G \colon \hat{\mathrm{H}}^i(G, \mathbb{Z}) \times \hat{\mathrm{H}}^{-i}(G, \mathbb{Z}) \xrightarrow{\cup} \hat{\mathrm{H}}^0(G, \mathbb{Z}) = \mathbb{Z}/|G|\mathbb{Z}.$$

Theorem 1.2.5. *The above pairing induces an isomorphism $F_G : \hat{\mathrm{H}}^{-i}(G, \mathbb{Z}) \cong \hat{\mathrm{H}}^i(G, \mathbb{Z})^{\sim}$ defined by*

$$F_G(g)(f) = \frac{1}{|G|}(f \cup g) \in \mathbb{Z}/|G|\mathbb{Z} = \frac{1}{|G|}\mathbb{Z}/\mathbb{Z} \subset \mathbb{Q}/\mathbb{Z}$$

for any $f \in \hat{\mathrm{H}}^i(G, \mathbb{Z}), g \in \hat{\mathrm{H}}^{-i}(G, \mathbb{Z})$.

Proof. See [15, VI, Theorem 7.4]. □

Lemma 1.2.6. *Let G be a finite group, let H be a subgroup of G and let i be an integer. Then the dual of the restriction map* $\mathrm{Res}^G_H : \hat{\mathrm{H}}^i(G,\mathbb{Z}) \to \hat{\mathrm{H}}^i(H,\mathbb{Z})$ *is the corestriction map* $\mathrm{Cor}^G_H : \hat{\mathrm{H}}^{-i}(H,\mathbb{Z}) \to \hat{\mathrm{H}}^{-i}(G,\mathbb{Z})$.

Proof. The cup-product satisfies the projection formula

$$\mathrm{Cor}^G_H(f \cup \mathrm{Res}^G_H(g)) = \mathrm{Cor}^G_H(f) \cup g$$

for any $f \in \hat{\mathrm{H}}^i(H,\mathbb{Z})$ and $g \in \hat{\mathrm{H}}^{-i}(G,\mathbb{Z})$, see [18, IV, §7, Proposition 9]. As the corestriction map

$$\mathrm{Cor}^G_H : \hat{\mathrm{H}}^0(H,\mathbb{Z}) = \mathbb{Z}/|H|\mathbb{Z} \to \mathbb{Z}/|G|\mathbb{Z} = \hat{\mathrm{H}}^0(G,\mathbb{Z})$$

in dimension 0 is induced by multiplication by $[G : H]$, multiplying the projection formula above by $\frac{1}{|G|}$ on both sides gives

$$\frac{1}{|H|}(f \cup \mathrm{Res}^G_H(g)) = \frac{1}{|G|}(\mathrm{Cor}^G_H(f) \cup g) \Leftrightarrow$$

$$F_H(\mathrm{Res}^G_H(g))(f) = F_G(g)(\mathrm{Cor}^G_H(f)).$$

We thus have a commutative diagram

$$\begin{tikzcd}
\hat{\mathrm{H}}^{-i}(G,\mathbb{Z}) \arrow[r, "F_G"] \arrow[d, "\mathrm{Res}^G_H"] & \hat{\mathrm{H}}^{i}(G,\mathbb{Z})^{\sim} \arrow[d, "(\mathrm{Cor}^G_H)^{\sim}"] \\
\hat{\mathrm{H}}^{-i}(H,\mathbb{Z}) \arrow[r, "F_H"] & \hat{\mathrm{H}}^{i}(H,\mathbb{Z})^{\sim}
\end{tikzcd}$$

Since the horizontal maps are duality isomorphisms by Theorem 1.2.5, the result follows. □

1.3 Covering groups

Let G be a finite group.

Definition 1.3.1. A group $\overline{G}$ is called a *stem extension* of G if there exists a central extension

$$1 \to M \to \overline{G} \xrightarrow{\lambda} G \to 1, \tag{1.3.1}$$

such that $M \subseteq [\overline{G}, \overline{G}]$. We call M the base normal subgroup of $\overline{G}$. A *Schur covering group* of G is a stem extension of G of maximal size.

Definition 1.3.2. The homology group $\hat{\mathrm{H}}^{-3}(G,\mathbb{Z})$ is called the *Schur multiplier* of G.

Lemma 1.3.3. *The base normal subgroup M of any Schur covering group of G is isomorphic to the Schur multiplier $\hat{\mathrm{H}}^{-3}(G,\mathbb{Z})$ of G.*

Proof. See [38, §9.9, p. 214] □

Proposition 1.3.4. *A Schur covering group of G always exists.*

Proof. See [54, Theorem 2.1.4]. □

Remark 1.3.5. Despite the fact that Schur covering groups of G always exist, these are not necessarily unique. For example, it is easy to check that both the group D_4 and the quaternion group $\mathcal{Q}_8$ of order 8 are Schur covering groups of the Klein four-group V_4.

Definition 1.3.6. A finite group $\overline{G}$ is called a *generalized representation group* of G if there exists a central extension

$$1 \to M \to \overline{G} \xrightarrow{\lambda} G \to 1, \tag{1.3.2}$$

such that $M \cap [\overline{G},\overline{G}] \cong \hat{\mathrm{H}}^{-3}(G,\mathbb{Z})$. We again call M the base normal subgroup of $\overline{G}$.

Remark 1.3.7. The isomorphism $M \cap [\overline{G},\overline{G}] \cong \hat{\mathrm{H}}^{-3}(G,\mathbb{Z})$ in Definition 1.3.6 is canonical, since the existence of such a bijection is equivalent to the surjectivity of the transgression map $\mathrm{Tr}_G : \hat{\mathrm{H}}^{1}(M,\mathbb{Q}/\mathbb{Z}) \to \hat{\mathrm{H}}^{2}(G,\mathbb{Q}/\mathbb{Z})$ in the inflation-restriction exact sequence of Lemma 1.1.5. Indeed, note that by Lemma 1.2.3 the surjectivity of Tr_G is equivalent to the injectivity of the dual map $\mathrm{Tr}_{\widetilde{G}}$ in the exact sequence $\hat{\mathrm{H}}^{-3}(G,\mathbb{Z}) \xrightarrow{\mathrm{Tr}_{\widetilde{G}}} \hat{\mathrm{H}}^{-2}(M,\mathbb{Z}) \to \hat{\mathrm{H}}^{-2}(\overline{G},\mathbb{Z})$, where the second map is induced by the inclusion $M \subset \overline{G}$. Hence, a central extension as in (1.3.2) gives a generalized representation group if and only if $\mathrm{Tr}_{\widetilde{G}}$ gives an isomorphism $\hat{\mathrm{H}}^{-3}(G,\mathbb{Z}) \cong M \cap [\overline{G},\overline{G}]$.

Even though a generalized representation group is not uniquely determined up to isomorphism, its commutator subgroup is. The existence of such an isomorphism is a classical result dating back to Schur (see [7, II, Corollary 2.4(iii)] for example), but we outline this construction here to verify that it has several properties to be used later on.

Lemma 1.3.8. *Let $\widetilde{G}$ (respectively, $\overline{G}$) be a generalized representation group of G with projection map $\widetilde{\lambda}$ (respectively, $\overline{\lambda}$) and base normal subgroup $\widetilde{M}$ (respectively, $\overline{M}$). For any subgroup B of G, define $\widetilde{B} = \widetilde{\lambda}^{-1}(B)$ and $\overline{B} = \overline{\lambda}^{-1}(B)$.*

There exists an isomorphism

$$\tau : [\widetilde{G},\widetilde{G}] \xrightarrow{\cong} [\overline{G},\overline{G}]$$

with the following properties:

(i) $\overline{\lambda}(\tau(a)) = \widetilde{\lambda}(a)$ *for every* $a \in [\widetilde{G},\widetilde{G}]$*;*

(ii) $\tau([\widetilde{g}_1,\widetilde{g}_2]) = [\overline{g}_1,\overline{g}_2]$ *for all* $\widetilde{g}_1,\widetilde{g}_2 \in \widetilde{G}$ *and* $\overline{g}_1,\overline{g}_2 \in \overline{G}$ *such that* $\widetilde{\lambda}(\widetilde{g}_i) = \overline{\lambda}(\overline{g}_i)$*.*

For any subgroup B *of* G*,* τ *further identifies*

- $[\widetilde{B},\widetilde{B}] \cong [\overline{B},\overline{B}]$ *and*
- $\widetilde{M} \cap [\widetilde{B},\widetilde{B}] \cong \overline{M} \cap [\overline{B},\overline{B}]$.

Proof. Let $\pi : F \to G$ be a surjective homomorphism, where F is a free group generated by a set X. As $\widetilde{\lambda}$ is surjective, for any $x \in X$ there exists $\widetilde{l}_x \in \widetilde{G}$ such that $\widetilde{\lambda}(\widetilde{l}_x) = \pi(x)$. Then $\widetilde{G}$ is generated by $\widetilde{M}$ and the elements $\widetilde{l}_x$ and the group homomorphism $\widetilde{\Lambda} : F \to \widetilde{G}$, defined by $\widetilde{\Lambda}(x) = \widetilde{l}_x$ for all $x \in X$, satisfies $\pi = \widetilde{\lambda} \circ \widetilde{\Lambda}$.

Moreover, if $R = \operatorname{Ker}\pi$, then $1 = \pi(R) = \widetilde{\lambda}(\widetilde{\Lambda}(R))$ and so $\widetilde{\Lambda}(R) \subset \operatorname{Ker}\widetilde{\lambda} = \widetilde{M}$. Thus $\widetilde{\Lambda}([F,R]) = [\widetilde{\Lambda}(F),\widetilde{\Lambda}(R)] \subset [\widetilde{G},\widetilde{M}] = 1$ since $\widetilde{M} \subset Z(\widetilde{G})$. We see also that $[\widetilde{G},\widetilde{G}]$ is generated by the elements $[\widetilde{l}_x,\widetilde{l}_y]$ and thus $\widetilde{\Lambda}$ induces a surjective homomorphism

$$\widetilde{\eta} : [F/[F,R], F/[F,R]] \to [\widetilde{G},\widetilde{G}]$$

Since $|[F/[F,R], F/[F,R]]| = |[\widetilde{G},\widetilde{G}]|$ in the case where $\widetilde{G}$ is a Schur covering group (see [55, Theorem 6.4, Equation (3)]) and $[\widetilde{G},\widetilde{G}]$ does not depend on $\widetilde{G}$ being a Schur covering group (see [26, Lemma 2]), the map $\widetilde{\eta}$ above is an isomorphism. Likewise, there exists a homomorphism $\overline{\Lambda} : F \to \overline{G}$ with analogous properties inducing an isomorphism $\overline{\eta} : [F/[F,R], F/[F,R]] \xrightarrow{\cong} [\overline{G},\overline{G}]$. Setting $\tau := \overline{\eta} \circ \widetilde{\eta}^{-1}$ yields the desired isomorphism and the stated properties are clear from its construction. The additional identifications concerning the subgroup B follow immediately from (i) and (ii). □

We finish this section with a lemma that will enable us to employ generalized representation groups to calculate the image of the corestriction map Cor_H^G inside the Schur multiplier $\hat{\mathrm{H}}^{-3}(G,\mathbb{Z})$:

Lemma 1.3.9. *[27, Lemma 4] Let* H *be a subgroup of* G *and let* $\overline{G}$ *be a generalized representation group of* G *with projection map* λ *and base normal subgroup* M*. Then*

$$\operatorname{Im}\left(\operatorname{Cor}_H^G : \hat{\mathrm{H}}^{-3}(H,\mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G,\mathbb{Z})\right) \cong M \cap [\lambda^{-1}(H), \lambda^{-1}(H)].$$

1.4 Algebraic tori

Let k be a field with (fixed) separable closure $\overline{k}$.

Definition 1.4.1. An *algebraic torus* T (or *torus*, for simplicity) over k is a k-algebraic group such that, over $\overline{k}$, T becomes isomorphic to $d \geq 1$ copies of the multiplicative group $\mathbb{G}_m$. We call d the *rank* of T and if the isomorphism $T \times_k \overline{k} \cong \mathbb{G}_m^d$ is defined over a subfield L of $\overline{k}$, the torus T is said to be *split* by L.

Definition 1.4.2. Let T be a torus defined over k. A *character* of k is a homomorphism of algebraic groups $\chi : \overline{T} \to \mathbb{G}_{m,\overline{k}}$.

Let $\widehat{T} = \operatorname{Hom}(\overline{T}, \mathbb{G}_{m,\overline{k}})$ denote the set of all characters of T. This set is naturally an abelian group under pointwise product. Additionally, one can give $\widehat{T}$ the structure of a $G_k := \operatorname{Gal}(\overline{k}/k)$-module via the action

$$(g.\chi)(x) = g\chi(g^{-1}x)$$

for all $g \in \operatorname{Gal}(\overline{k}/k), \chi \in \widehat{T}$ and $x \in T$. Note that if T is split by a Galois subextension L/k of $\overline{k}/k$, then $\operatorname{Gal}(\overline{k}/L)$ acts trivially on the character group $\widehat{T}$ and thus $\widehat{T}$ is a $\operatorname{Gal}(L/k)$-module.

Theorem 1.4.3. *Let L/k be a finite Galois extension with Galois group G. Let $\mathcal{A}$ be the category of algebraic tori over k that are split by L and let $\mathcal{B}$ be the category of finitely generated torsion-free G-modules. Then taking character groups gives a contravariant equivalence of categories $\Phi : \mathcal{A} \to \mathcal{B}$.*

Proof. See [75, Theorem 2.1]. □

This theorem makes it possible to study properties of algebraic tori via the corresponding properties of their character modules, a tool that will be very useful for us in this thesis.

Lemma 1.4.4. *The G_k-module $\widehat{\mathbb{G}_m}$ is isomorphic to $\mathbb{Z}$ (with the trivial G_k-action), being generated by the identity morphism.*

Proof. See [87, Example 3.2.2]. □

We now analyze tori of the form $R_{K/k}\mathbb{G}_m$, where K/k is a finite separable field extension and $R_{K/k}$ is the *Weil restriction* functor (recall that this functor is characterized by the property $(R_{K/k}X)(S) = X(S \times_k K)$ for any K-scheme X and any k-algebra S).

Lemma 1.4.5. *Let L/k be the Galois closure of K/k. Set $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$. Then $T = R_{K/k}\mathbb{G}_m$ is a torus split by L/k of rank $d = [K : k]$. Moreover, we have $\widehat{T} \cong \mathbb{Z}[G/H]$ as G-modules.*

Proof. Write $K = k(\alpha)$ for some primitive element α of K/k and let f be the minimal polynomial of α over k. We have

$$T(\overline{k}) \cong (K \otimes_k \overline{k})^* \cong (\overline{k}[x]/(f(x)))^* \cong \bigoplus_{gH \in G/H} (\overline{k}[x]/(x - g\alpha))^* \cong (\overline{k}^*)^d, \tag{1.4.1}$$

where we used the Chinese remainder theorem in the third isomorphism. It follows that T is a torus of rank d and since the isomorphisms in (1.4.1) are defined over L, T is split by L/k.

Moreover, the isomorphism (1.4.1) allows us to write any $x \in T(\overline{k})$ as $x = \bigoplus_{gH \in G/H} x_{gH}$ for uniquely determined $x_{gH} \in \overline{k}^*$. Define $\chi_{gH} : \overline{T} \to \mathbb{G}_{m,\overline{k}}$ by $x \mapsto x_{gH}$. It is clear that χ_{gH} is a character of T and, conversely, any character of T can be uniquely written as a product of characters of this form. In other words, the homomorphism of abelian groups

$$\begin{aligned} \xi \colon \mathbb{Z}[G/H] &\longrightarrow \widehat{T} \\ gH &\longmapsto \chi_{gH} \end{aligned}$$

is an isomorphism. We prove that ξ is G-equivariant, finishing the proof of the lemma. Note that the action of $G_k = \mathrm{Gal}(\overline{k}/k)$ on $\mathbb{Z}[G/H]$ is induced by its G-action and the projection map $\pi : G_k \to G$. Similarly, the action of G on $\widehat{T}$ is induced by the action of G_k on $\widehat{T}$ and π. It thus suffices to check that ξ is G_k-equivariant. Since the G_k-action on $T(\overline{k})$ is given by $(\sigma x)_{gH} = \sigma(x_{\pi(\sigma)^{-1}gH})$, we have

$$(\sigma.\chi_{gH})(x) = \sigma(\chi_{gH}(\sigma^{-1}x)) = \sigma((\sigma^{-1}x)_{gH}) = \sigma(\sigma^{-1}(x_{\pi(\sigma)gH})) = x_{\pi(\sigma)gH} = x_{\sigma.gH}$$

for all $\sigma \in G_k, gH \in G/H$ and $x = \bigoplus_{gH \in G/H} x_{gH} \in T(\overline{k})$. □

1.5 Arithmetic of tori

Let T be an algebraic torus over a global field k.

Definition 1.5.1. The *Tate-Shafarevich group* $Ш(T)$ of T is defined as the kernel of the product of the restriction maps

$$Ш(T) := \operatorname{Ker}\left(\mathrm{H}^1(k,T) \to \prod_{v\in\Omega_k} \mathrm{H}^1(k_v,T)\right).$$

Definition 1.5.2. A *principal homogeneous space* (or *torsor*) for T (or under T) is a non-trivial variety X/k equipped with a free and transitive action of T by regular functions.

It is easy to verify that a principal homogeneous space X for T has a k-rational point if and only if $X \cong T$ over k. Moreover, it is a well-known fact that isomorphism classes of k-torsors under T are classified by the cohomology group $\mathrm{H}^1(k,T)$, see [86, §2.2]. In this way, we obtain the following characterization of the Tate–Shafarevich group of T.

Definition 1.5.3. Let C be a class of algebraic varieties defined over k. The *Hasse principle* is said to hold for C if, for every $X \in C$, the existence of k_v-points on X for all $v \in \Omega_k$ implies the existence of a k-point on X.

Lemma 1.5.4. $Ш(T) = 0$ *if and only if the Hasse principle holds for all principal homogeneous spaces for T.*

Assuming that a variety does have a k-point, it is natural to ask if it is possible to approximate a finite number of local points of the variety by a single global point, i.e. whether weak approximation holds.

Definition 1.5.5. The *defect of weak approximation* for T is defined as

$$A(T) := \left(\prod_{v\in\Omega_k} T(k_v)\right)/\overline{T(k)},$$

where $\overline{T(k)}$ denotes the closure of $T(k)$ in $\prod_v T(k_v)$ with respect to the product topology. *Weak approximation* is said to hold for T if $A(T) = 0$.

Example 1.5.6. Weak approximation holds for the torus $\mathbb{G}_m$ by the approximation theorem of algebraic number theory, see [72, II, §3, Theorem 3.4].

We now present one of the main results in the arithmetic of algebraic tori, tying together weak approximation for a torus T and the Hasse principle for principal homogeneous spaces under T. We will make use of the following lemma:

Lemma 1.5.7. *There exists a smooth complete k-variety X containing T as an open subset.*

Proof. See [22, Corollary 1]. □

Throughout the thesis, we will refer to a variety X in the conditions of Lemma 1.5.7 as a *smooth compactification* of T.

Theorem 1.5.8 (Voskresenskiĭ). *Let T be a torus defined over a number field k and let X/k be a smooth compactification of T. Then there exists an exact sequence*

$$0 \to A(T) \to \mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim} \to Ш(T) \to 0. \tag{1.5.1}$$

Proof. See [91, Theorem 6]. □

Theorem 1.5.9. *If X_1 and X_2 are two smooth compactifications of a torus T defined over a number field k, then*

$$\mathrm{H}^1(k, \operatorname{Pic} \overline{X_1}) = \mathrm{H}^1(k, \operatorname{Pic} \overline{X_2}).$$

In particular, the group $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ is a birational invariant of T.

Proof. Voskresenskiĭ showed (see [91, Theorem 1]) that there exists a canonical isomorphism of G_k-modules $\operatorname{Pic}(\overline{X_1}) \oplus P_1 = \operatorname{Pic}(\overline{X_2}) \oplus P_2$ for some *permutation* G_k-modules (see below for the definition of a permutation module) P_1, P_2. Since a permutation module is a sum of induced G_k-modules of the form $\mathbb{Z}[G_k/H]$, where H is a closed subgroup of finite index of G_k, and $\mathrm{H}^1(k, \mathbb{Z}[G_k/H]) = \mathrm{H}^1(H, \mathbb{Z}) = \operatorname{Hom}(H, \mathbb{Z}) = 0$ by Shapiro's lemma 1.1.7, we deduce that $\mathrm{H}^1(k, \operatorname{Pic} \overline{X_1}) = \mathrm{H}^1(k, \operatorname{Pic} \overline{X_2})$. □

Remark 1.5.10. The group $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ admits another interpretation, namely using the Hochschild–Serre spectral sequence one obtains an isomorphism $\operatorname{Br} X / \operatorname{Br}_0 X \cong \mathrm{H}^1(k, \operatorname{Pic} \overline{X})$, where $\operatorname{Br}_0 X = \operatorname{Im}(\operatorname{Br} k \to \operatorname{Br} X)$ and $\operatorname{Br} X$ denotes the Brauer–Grothendieck group of X. In this way, the study of this invariant can be put into the framework of the well-known *Brauer–Manin obstruction*, which by work of Sansuc [81] is the only one to the Hasse principle and weak approximation for any principal homogeneous space S of T. Therefore, if Y is a smooth compactification of S, the analysis of the group $\operatorname{Br} Y / \operatorname{Br}_0 Y$ (which injects into $\operatorname{Br} X / \operatorname{Br}_0 X$ by results in [6, §5]) is of considerable interest. For examples of work on the construction of these groups, see [6] or [23].

Voskresenskiĭ proved Theorem 1.5.8 by working with a *flasque resolution* of $\widehat{T}$, a notion that was later put into a general framework by Colliot-Thélène and Sansuc ([20]). We explain this concept below as it will be useful for us in later chapters.

Let G be a finite group and let A be a G-module. We say that A is a *permutation* module if it has a $\mathbb{Z}$-basis permuted by G. We say that A is *flasque* if $\hat{\mathrm{H}}^{-1}(G', A) = 0$ for all subgroups G' of G. A *flasque resolution* of A is an exact sequence of G-modules

$$0 \to A \to P \to F \to 0,$$

where P is a permutation module and F is flasque. We say two G-modules A_1 and A_2 are similar if $A_1 \oplus P_1 \cong A_2 \oplus P_2$ for permutation modules P_1, P_2 and denote the similarity class of A by $[A]$.

Proposition 1.5.11. *Every G-module A admits a flasque resolution.*

Proof. See [20, Lemme 3]. □

The following result shows that the group $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ appearing in Voskresenskiĭ's exact sequence 1.5.1 has a simple cohomological description and can be computed using *any* flasque resolution of the Galois module $\widehat{T}$.

Theorem 1.5.12 (Colliot-Thélène and Sansuc)**.** *Let T be a torus defined over a number field k and split by a finite Galois extension L/k with $G = \mathrm{Gal}(L/k)$. Let*

$$0 \to \widehat{T} \to P \to F \to 0$$

be a flasque resolution of $\widehat{T}$ and let X/k be a smooth compactification of T. Then the similarity class $[F]$ and the group $\mathrm{H}^1(G, F)$ are uniquely determined and

$$\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) = \mathrm{H}^1(G, \operatorname{Pic} X_L) = \mathrm{H}^1(G, F). \tag{1.5.2}$$

Additionally,

$$\mathrm{H}^1(G, F) = \text{Ш}^2_\omega(G, \widehat{T}) := \operatorname{Ker}\Big(\mathrm{H}^2(G, \widehat{T}) \xrightarrow{\text{Res}} \prod_{g \in G} \mathrm{H}^2(\langle g \rangle, \widehat{T})\Big). \tag{1.5.3}$$

Proof. See [20, Lemme 5 and Proposition 6] for the proof of (1.5.2). The isomorphism $\mathrm{H}^1(G, F) = \text{Ш}^2_\omega(G, \widehat{T})$ is proved in [21, Proposition 9.5(ii)]. □

The Tate–Shafarevich group $Ш(T)$ also has a description in terms of the cohomology of $\widehat{T}$:

Theorem 1.5.13 (Tate). *Let T be a torus defined over a number field k and split by a finite Galois extension L/k with $G = \mathrm{Gal}(L/k)$. Then Poitou–Tate duality gives a canonical isomorphism*

$$Ш(T)^\sim = Ш^2(G, \widehat{T}), \tag{1.5.4}$$

where $Ш^2(G, \widehat{T}) = \mathrm{Ker}\Big(\mathrm{H}^2(G, \widehat{T}) \xrightarrow{\mathrm{Res}} \prod_{v \in \Omega_k} \mathrm{H}^2(D_v, \widehat{T})\Big)$.

Proof. This is the case $i = 1$ of [75, Theorem 6.10]. □

Proposition 1.5.14. *Let T be a torus defined over a number field k and split by a finite Galois extension L/k with $G = \mathrm{Gal}(L/k)$. Then taking duals in Voskresenskiĭ's exact sequence (1.5.1) yields the exact sequence*

$$0 \to Ш^2(G, \widehat{T}) \to Ш^2_\omega(G, \widehat{T}) \to A(T)^\sim \to 0, \tag{1.5.5}$$

where the map $Ш^2(G, \widehat{T}) \to Ш^2_\omega(G, \widehat{T})$ is the natural inclusion arising from the Chebotarev density theorem.

Proof. This follows from the proof of [91, Theorem 6] and isomorphisms (1.5.2), (1.5.3) and (1.5.4). □

1.6 The norm one torus

Let K/k be a finite separable extension of fields and let L/k be a finite Galois extension containing K/k. Set $G = \mathrm{Gal}(L/k), H = \mathrm{Gal}(L/K)$ and $d = [K : k]$.

Definition 1.6.1. The *norm one torus* of K/k is defined as

$$R^1_{K/k}\mathbb{G}_m := \mathrm{Ker}(R_{K/k}\mathbb{G}_m \xrightarrow{N_{K/k}} \mathbb{G}_m).$$

Remark 1.6.2. On k-points, the morphism $R_{K/k}\mathbb{G}_m \xrightarrow{N_{K/k}} \mathbb{G}_m$ is just the usual norm map $N_{K/k} : K^* \to k^*$ and so the norm one torus $R^1_{K/k}\mathbb{G}_m$ is represented by the hypersurface $N_{K/k}(x_1, \ldots, x_d) = 1$ in affine space $\mathbb{A}^d_k$ (where $x_1, \ldots, x_d$ denote the coordinates of an element of K in some k-basis).

More concretely, one can also view the algebraic group $R^1_{K/k}\mathbb{G}_m$ as follows: embed $R_{K/k}\mathbb{G}_m \hookrightarrow \mathrm{GL}_d$ by considering the left regular representation of K/k (with respect to some k-basis)

$$\rho\colon K \to M_d(k).$$

Taking the algebraic group defined by the equations describing $\operatorname{Im}\rho$ gives exactly $R_{K/k}\mathbb{G}_m$. Note that changing the basis with respect to which ρ is defined has the effect of conjugating $\operatorname{Im}\rho$, so that $R_{K/k}\mathbb{G}_m$ is well-defined up to k-isomorphism. In this way, the norm one torus $R^1_{K/k}\mathbb{G}_m$ is simply defined as the subgroup of matrices in $R_{K/k}\mathbb{G}_m$ with determinant 1.

Lemma 1.6.3. *$T = R^1_{K/k}\mathbb{G}_m$ is a torus of rank $d-1$ and split by L/k.*

Proof. In the proof of Lemma 1.4.5 it was shown that the group $R_{K/k}\mathbb{G}_m(\overline{k})$ is diagonalisable, isomorphic to $(\overline{k}^*)^d$ and that this isomorphism is already defined over L. As $N_{K/k} = \det \circ \rho$, it is easy to check that $N_{K/k}(x) = \prod_{i=1}^{d} x_i$ for any $x = \bigoplus_{i=1}^{d} x_i \in R_{K/k}\mathbb{G}_m(\overline{k})$ and therefore $T(\overline{k}) \cong (\overline{k}^*)^{d-1}$. Since this isomorphism is defined over L, T is split by L/k. □

Definition 1.6.4 (Chevalley module)**.** Let G be a finite group and H a subgroup of G. The map $\eta : \mathbb{Z} \to \mathbb{Z}[G/H]$ defined by $\eta : 1 \mapsto N_{G/H} = \sum_{gH \in G/H} gH$ produces the exact sequence of G-modules

$$0 \to \mathbb{Z} \xrightarrow{\eta} \mathbb{Z}[G/H] \xrightarrow{\pi} J_{G/H} \to 0, \tag{1.6.1}$$

where $J_{G/H} = \operatorname{coker}\eta$ is called the *Chevalley module of G/H*.

Proposition 1.6.5. *$\widehat{R^1_{K/k}\mathbb{G}_m} \cong J_{G/H}$ as G-modules.*

Proof. The result follows from taking character groups in the exact sequence

$$1 \to R^1_{K/k}\mathbb{G}_m \to R_{K/k}\mathbb{G}_m \xrightarrow{N_{K/k}} \mathbb{G}_m \to 1,$$

using Lemmas 1.4.4, 1.4.5 and noticing that $\chi \circ N_{K/k} = \prod_{gH \in G/H} \chi_{gH}$, where $\chi : \mathbb{G}_{m,\overline{k}} \to \mathbb{G}_{m,\overline{k}}$ is the identity morphism and χ_{gH} are the characters constructed in the proof of Lemma 1.4.5. □

The next lemma will be useful when taking the cohomology of the module $J_{G/H}$:

Lemma 1.6.6. *Let G be a finite group and H a subgroup of G. Then, for every $i \in \mathbb{Z}_{\geq 0}$ and for every subgroup G' of G, the diagram obtained by taking the group cohomology of the exact sequence* (1.6.1)

$$\begin{tikzcd}
\mathrm{H}^i(G,\mathbb{Z}) \arrow[r, "\eta^*"] \arrow[d, "\mathrm{Res}^G_{G'}"] & \mathrm{H}^i(G,\mathbb{Z}[G/H]) \arrow[r, "\pi^*"] \arrow[d, "\mathrm{Res}^G_{G'}"] & \mathrm{H}^i(G,J_{G/H}) \arrow[r, "\delta_i"] \arrow[d, "\mathrm{Res}^G_{G'}"] & \mathrm{H}^{i+1}(G,\mathbb{Z}) \arrow[d, "\mathrm{Res}^G_{G'}"] \\
\mathrm{H}^i(G',\mathbb{Z}) \arrow[r, "\eta^*"] & \mathrm{H}^i(G',\mathbb{Z}[G/H]) \arrow[r, "\pi^*"] & \mathrm{H}^i(G',J_{G/H}) \arrow[r, "\delta_i"] & \mathrm{H}^{i+1}(G',\mathbb{Z})
\end{tikzcd} \tag{1.6.2}$$

commutes.

Proof. It is well-known that the restriction map commutes with the connecting homomorphisms δ_i, see [18, end of p. 103] for example. Moreover, as $\mathrm{Res}^G_{G'}$ corresponds to restricting a cocycle defined on G to the subgroup G', it is clear that it commutes with the map π^* given by composing a cocyle with π. By a similar reasoning one checks that $\mathrm{Res}^G_{G'}$ commutes with the map η^* given by composing a cocycle with η. □

The next result shows how the Tate–Shafarevich group of the norm one torus completely controls the local-global principle for norms of K/k, an interpretation that will be essential in later applications.

Proposition 1.6.7. *If K/k is an extension of global fields, then*

$$Ш(R^1_{K/k}\mathbb{G}_m) = (k^* \cap N_{K/k}(\mathbb{A}_K^*))/N_{K/k}(K^*).$$

Proof. See [75, p. 307]. □

We finish this chapter with two results that describe the Tate-Shafarevich group and the birational invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ (via Theorem 1.5.12) for the norm one torus of a Galois extension:

Theorem 1.6.8. *If $T = R^1_{L/k}\mathbb{G}_m$ is the norm one torus of a Galois extension L/k of number fields with Galois group G, we have*

$$Ш^2_\omega(G,\widehat{T}) = \mathrm{H}^2(G,\widehat{T}) = \mathrm{H}^3(G,\mathbb{Z}). \tag{1.6.3}$$

Proof. Taking character groups in the defining sequence of T

$$1 \to T \to R_{L/k}\mathbb{G}_m \xrightarrow{N_{L/k}} \mathbb{G}_m \to 1$$

and using Lemmas 1.4.4 and 1.4.5 gives the exact sequence of G-modules

$$0 \to \mathbb{Z} \to \mathbb{Z}[G] \to \widehat{T} \to 0.$$

Taking the group cohomology of the above sequence and using Lemma 1.6.6 gives the following commutative diagram of abelian groups with exact lines:

$$\begin{tikzcd}
\mathrm{H}^2(G, \mathbb{Z}[G]) \arrow[r] \arrow[d, "\mathrm{Res}"] & \mathrm{H}^2(G, \widehat{T}) \arrow[r] \arrow[d, "\mathrm{Res}"] & \mathrm{H}^3(G, \mathbb{Z}) \arrow[r] \arrow[d, "\mathrm{Res}"] & \mathrm{H}^3(G, \mathbb{Z}[G]) \arrow[d, "\mathrm{Res}"] \\
\prod_{g \in G} \mathrm{H}^2(\langle g \rangle, \mathbb{Z}[G]) \arrow[r] & \prod_{g \in G} \mathrm{H}^2(\langle g \rangle, \widehat{T}) \arrow[r] & \prod_{g \in G} \mathrm{H}^3(\langle g \rangle, \mathbb{Z}) \arrow[r] & \prod_{g \in G} \mathrm{H}^3(\langle g \rangle, \mathbb{Z}[G])
\end{tikzcd} \tag{1.6.4}$$

where the vertical arrows are the products of the restriction maps. By Lemma 1.1.9 we have $\mathrm{H}^i(G, \mathbb{Z}[G]) = \mathrm{H}^i(\langle g \rangle, \mathbb{Z}[G]) = 0$ for $i = 2, 3$. Additionally, by the 2-periodicity of group cohomology of cyclic groups, we have $\mathrm{H}^3(\langle g \rangle, \mathbb{Z}) = \mathrm{H}^1(\langle g \rangle, \mathbb{Z}) = \mathrm{Hom}(\langle g \rangle, \mathbb{Z}) = 0$. Therefore diagram (1.6.4) shows that $\mathrm{H}^3(G, \mathbb{Z}) = \mathrm{H}^2(G, \widehat{T}) = Ш^2_\omega(G, \widehat{T})$, as desired. □

Theorem 1.6.9 (Tate). *If $T = R^1_{L/k}\mathbb{G}_m$ is the norm one torus of a Galois extension L/k of number fields with Galois group G, we have*

$$Ш(T)^\sim = \mathrm{Ker}\left(\mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\mathrm{Res}} \prod_{v \in \Omega_k} \mathrm{H}^3(D_v, \mathbb{Z})\right), \tag{1.6.5}$$

where $D_v = \mathrm{Gal}(L_v/k_v)$ is the decomposition group at v.

Proof. See [18, p. 198]. □

Part I

The Hasse norm principle

Chapter 2

Introduction

In this part of the thesis we study a local-global principle for norms known as the *Hasse norm principle*. Let K/k be an extension of number fields with associated idèle groups $\mathbb{A}_K^*$ and $\mathbb{A}_k^*$. One can naturally define a norm map $N_{K/k} : \mathbb{A}_K^* \to \mathbb{A}_k^*$ by

$$N_{K/k}((x_w)_w) = \left(\prod_{w|v} N_{K_w/k_v}(x_w) \right)_{v \in \Omega_k}$$

where the product runs over all places $w \in \Omega_K$ above v. Since $N_{K/k}(x) = \prod\limits_{w|v} N_{K_w/k_v}(x)$ for any $x \in K^*$ (see, for example, [72, II, Corollary 8.4]), this idèlic norm map extends the usual norm map $N_{K/k} : K^* \to k^*$ of K/k, i.e. the diagram

$$\begin{tikzcd}
K^* \arrow[r, hook] \arrow[d, "N_{K/k}"] & \mathbb{A}_K^* \arrow[d, "N_{K/k}"] \\
k^* \arrow[r, hook] & \mathbb{A}_k^*
\end{tikzcd}$$

commutes.

Definition 2.0.1. The *Hasse norm principle* (often abbreviated to HNP) is said to hold for K/k if the so-called *knot group*

$$\mathfrak{K}(K/k) := (k^* \cap N_{K/k}(\mathbb{A}_K^*))/N_{K/k}(K^*)$$

is trivial, i.e. if being a norm everywhere locally is equivalent to being a global norm from K/k.

This principle was formally introduced and first investigated in [43] by Hasse, who proved the following result:

Theorem 2.0.2 (The Hasse norm theorem, [43])**.** *The HNP holds if K/k is a cyclic extension.*

Hasse also showed that this principle can fail in general, with biquadratic extensions providing the simplest setting where failures are possible.

Theorem 2.0.3. *The HNP fails for the extension $\mathbb{Q}(\sqrt{-3},\sqrt{13})/\mathbb{Q}$. Indeed, 3 is not a global norm, despite being the norm of an idèle.*

Proof. See [43, §2]. □

In general, the HNP fails for a biquadratic extension if and only if all its decomposition groups are cyclic, see [18, p. 199]. Since this principle was first introduced, multiple cases have been analyzed in the literature. For instance, if K/k is Galois, there is an explicit description of the knot group due to Tate[1]

$$\mathfrak{K}(K/k)^{\sim} = \operatorname{Ker}\left(\mathrm{H}^3(G,\mathbb{Z}) \xrightarrow{\text{Res}} \prod_{v\in\Omega_k} \mathrm{H}^3(D_v,\mathbb{Z})\right), \tag{2.0.1}$$

as it follows from Proposition 1.6.7 and Theorem 1.6.9. Using this characterization, many results on the validity of the HNP were obtained in the Galois setting, with a particular emphasis on the abelian case, see e.g. the works of Gerth ([39], [40]), Gurak ([41], [42]) and Razar ([79]).

Nevertheless, results for the non-abelian and non-Galois cases are still limited. For example, if N/k is the normal closure of K/k, the following instances of the HNP are known:

Theorem 2.0.4 (Bartels)**.** *If $[K:k]$ is prime, then the HNP holds for K/k.*

Proof. See [3, Lemma 4]. □

Theorem 2.0.5 (Bartels)**.** *If $[K:k]=n$ and $\mathrm{Gal}(N/k)\cong D_n$ is the dihedral group of order $2n$, then the HNP holds for K/k.*

Proof. See [4, Satz 1]. □

[1] Part of this characterization also appeared in earlier work of Scholz, see [83, II, Satz 3].

Theorem 2.0.6 (Voskresenskiĭ and Kunyavskiĭ)**.** *If* $[K : k] = n$ *and* $\mathrm{Gal}(N/k) \cong S_n$*, then the HNP holds for* K/k*.*

Proof. See [92] or [93]. □

The main underlying theoretical tool used to derive these results is the geometric interpretation of the HNP: by Proposition 1.6.7 the knot group $\mathfrak{K}(K/k)$ is identified with the Tate–Shafarevich group $\text{Ш}(T)$ of the norm one torus $T = R^1_{K/k}\mathbb{G}_m$ and thus by Lemma 1.5.4 the HNP holds for K/k if and only if the Hasse principle holds for all principal homogeneous spaces

$$T_c : N_{K/k}(\Xi) = c \tag{2.0.2}$$

(where Ξ is a variable) under T. In this way, one can explore techniques from the arithmetic of algebraic tori (as presented in Section 1.5) to investigate the group $\text{Ш}(T)$ and thus deduce results on the validity of the HNP.

Over the next four chapters, we exploit this toric interpretation of the Hasse norm principle and related tools in order to do a comprehensive study of this principle in several families of extensions. In Chapter 3 we add to the above list of non-Galois cases where the HNP is known to hold by establishing this principle for any degree $n \geq 5$ extension K/k of number fields such that $\mathrm{Gal}(N/k)$ is isomorphic to A_n.

We subsequently give theoretical results and explicit methods for the computation of the obstructions to the Hasse principle and weak approximation for norm one tori of non-Galois extensions in Chapter 4. We start by applying techniques from the arithmetic of algebraic tori to provide some comparison isomorphisms between these obstructions for a fixed extension and its subextensions/superextensions (see Theorem 4.1.1 and the results of Section 4.2). We then use certain quotients of the knot group and the birational invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ to derive explicit formulas for the the p-primary part of the obstructions we study for all but finitely many primes p, see Corollary 4.1.3 and the results of Section 4.3. We also utilize generalized representation groups and outline work of Drakokhrust which uses these groups to describe the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ (see Theorem 4.1.4). We end the chapter by describing in detail how to compute some of the obstruction groups using computer algebra systems such as GAP [33], see Section 4.4.

In Chapter 5 we make use of the techniques developed in Chapter 4 to do a broad study of the local-global principles for any extension whose normal closure has symmetric or alternating Galois group, generalizing Theorem 2.0.6 above and the main result of Chapter 3. In this setting, we provide explicit formulas for the knot group and the birational invariant

$\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ of any A_n or S_n-extension (see Theorem 5.1.1) and further determine all possibilities for these groups, showing that each possibility occurs (see Theorem 5.1.3). Finally, we demonstrate how to apply our results to obtain precise local conditions controlling the failure of the local-global principles for small values of n, see Propositions 5.1.7, 5.1.8, 5.1.9 and 5.1.10.

A big motivation for providing explicit conditions for the failure of the HNP as described above is to enable an analysis of the frequency of its failures in families of extensions of number fields (see Part III of this thesis for several results in this direction). Furthermore, in order to obtain asymptotic formulas for the number of extensions satisfying certain conditions, it is often necessary to first show the existence of at least one such extension, see [30, Theorem 1.7] for example. The results of the last chapter of this part of the thesis, Chapter 6, address this issue. In this chapter we prove the existence of field extensions with prescribed Galois group that satisfy or fail the Hasse norm principle (see Theorem 6.1.3) and construct A_n and S_n-extensions (over at most a quadratic extension of $\mathbb{Q}$) that illustrate all cases of Propositions 5.1.7 and 5.1.9 (see Sections 6.2.1 and 6.2.2).

Chapter 3

The Hasse norm principle for A_n-extensions

3.1 Main result

In this chapter we investigate the Hasse norm principle for a degree n extension K/k of number fields with normal closure N/k such that $\mathrm{Gal}(N/k)$ is isomorphic to A_n, the alternating group on n letters. We also look at *weak approximation* – recall that this property is said to hold for a variety X/k if $X(k)$ is dense (for the product topology) in $\prod_{v \in \Omega_k} X(k_v)$. In particular, we examine weak approximation for the norm one torus $R^1_{K/k}\mathbb{G}_m$ associated with a degree n extension K/k of number fields with A_n-normal closure.

The first non-trivial case is $n = 3$. In this case, $K = N$ is a cyclic extension of k and the Hasse norm theorem 2.0.2 implies that the HNP holds for K/k. Moreover, one can show that weak approximation holds for the associated norm one torus by invoking a result of Colliot-Thélène and Sansuc, see Remark 3.1.3 below.

The case $n = 4$ was analyzed by Kunyavskiĭ in his work [57] on the arithmetic of three-dimensional tori:

Theorem 3.1.1 (Kunyavskiĭ)**.** *Let K/k be a quartic extension of number fields and let N/k be its normal closure. If $\mathrm{Gal}(N/k) \cong A_4$, then $\mathfrak{K}(K/k) = 0$ or $\mathbb{Z}/2$ and $\mathfrak{K}(K/k)$ is trivial if and only if there exists $v \in \Omega_k$ such that the decomposition group $D_v = \mathrm{Gal}(N_v/k_v)$ is not cyclic. Moreover, the HNP holds for K/k if and only if weak approximation fails for $R^1_{K/k}\mathbb{G}_m$.*

The main goal of this chapter is to complete the picture for this family of extensions by proving the following theorem.

Theorem 3.1.2. *[62, Theorem 1.1] Let K/k be a degree $n \geq 5$ extension of number fields and let N/k be its normal closure. If $\mathrm{Gal}(N/k) \cong A_n$, then the HNP holds for K/k and weak approximation holds for the norm one torus $R^1_{K/k}\mathbb{G}_m$.*

Our strategy to establish this result is twofold. First, we combine the toric interpretation of the HNP described in Sections 1.5 and 1.6 with several cohomological facts about A_n-modules to prove the aforementioned result for $n \geq 8$. Next, we use a computational method developed by Hoshi and Yamasaki to solve the case $n = 6$. The remaining cases $n = 5$ and 7 follow from the remark below. In Chapter 5 we will also see how to obtain Theorem 3.1.2 and further results on A_n-extensions by using different techniques, see Remark 5.1.11.

Remark 3.1.3. We note that when $n = p$ is a prime number, Theorem 3.1.2 was already known. Indeed, in this case the HNP always holds by Theorem 2.0.4 and a result of Colliot-Thélène and Sansuc on the rationality of the norm one torus of an extension with prime degree also shows the validity of weak approximation (see [21, Proposition 9.1 and Remark 9.3]).

3.2 Cohomology of A_n-modules

In this section we prove Theorem 3.1.2 for $n \geq 8$. We start out by establishing several group-theoretic and cohomological facts about A_n-modules. We then exploit the consequences of these results in the arithmetic of norm one tori associated with A_n-extensions.

Recall that, for $n \geq 5$, A_n is a non-abelian simple group and hence perfect. Moreover, its Schur multiplier $M(A_n) = \hat{\mathrm{H}}^{-3}(A_n, \mathbb{Z})$ is given as follows (see [45, Theorem 2.11]):

$$M(A_n) = \begin{cases} 0 & \text{if } n \leq 3; \\ \mathbb{Z}/2 & \text{if } n \in \{4,5\} \text{ or } n \geq 8; \\ \mathbb{Z}/6 & \text{if } n \in \{6,7\}. \end{cases}$$

Given a copy H of A_{n-1} inside $G = A_n$, we have an induced corestriction map on cohomology

$$\mathrm{Cor}^G_H : M(H) \to M(G).$$

This map will play an important role in the proof of Theorem 3.1.2, so we begin by establishing the following result.

Lemma 3.2.1. *Let $n \geq 8$ and let H be a copy of A_{n-1} inside $G = A_n$. Then the corestriction map Cor_H^G is surjective.*

In order to prove this lemma, we will use multiple results about covering groups of S_n and A_n together with the characterization of the image of Cor_H^G given in Lemma 1.3.9. To put this plan into practice, we will use the following presentation of a *Schur covering group* (as defined in Section 1.3) of S_n due to Schur.

Proposition 3.2.2 (Schur). *Let $n \geq 4$ and let U be the group with generators $z, t_1, \dots, t_{n-1}$ and relations*

1. $z^2 = 1$;
2. $zt_i = t_i z$, for $1 \leq i \leq n-1$;
3. $t_i^2 = z$, for $1 \leq i \leq n-1$;
4. $(t_i t_{i+1})^3 = z$, for $1 \leq i \leq n-2$;
5. $t_i t_j = z t_j t_i$, for $|i-j| \geq 2$ and $1 \leq i, j \leq n-1$.

Then U is a Schur covering group of S_n with base normal subgroup $M = \langle z \rangle$. Moreover, if $\overline{t_i}$ denotes the transposition $(i\ \ i+1)$ in S_n, then the map

$$\begin{aligned} \pi \colon U &\longrightarrow S_n \\ z &\longmapsto 1 \\ t_i &\longmapsto \overline{t_i} \end{aligned}$$

is surjective and has kernel M.

Proof. See Schur's original paper [84] or [45, Chapter 2] for a more modern exposition. □

Remark 3.2.3. By Lemma 1.3.3 and Proposition 3.2.2, we immediately see that the Schur multiplier $M(S_n)$ of S_n is isomorphic to $\mathbb{Z}/2$ for all $n \geq 4$.

Using the Schur cover of S_n given in Proposition 3.2.2, one can also construct a Schur covering group of A_n for $n = 4, 5$ or any $n \geq 8$.

Lemma 3.2.4. *In the notation of Proposition 3.2.2, the group $V := \pi^{-1}(A_n)$ defines a Schur covering group of A_n for $n = 4, 5$ or any $n \geq 8$.*

Proof. It is well-known that A_n is generated by the $n-2$ permutations $\overline{e_i} := \overline{t_1}.\overline{t_{i+1}} = (1\ 2)(i+1\ \ i+2)$ for $1 \leq i \leq n-2$. Hence, $V = \pi^{-1}(A_n)$ is generated by $z, e_1, \ldots, e_{n-2}$, where $e_i := t_1 t_{i+1}$ for $1 \leq i \leq n-2$. Clearly, we have $M \subseteq Z(V)$ and $V/M \cong A_n$. As the Schur multiplier of A_n is also $\mathbb{Z}/2$ for $n = 4, 5$ or $n \geq 8$, in order to show that V defines a Schur covering group of A_n it suffices to prove that $M \subseteq [V, V]$.

Claim: $z = [e_1^{-1} e_2 e_1, e_2]$. (3.2.1)

Proof of claim: This follows from a straightforward (but long) computation using the identities $(e_1 e_2)^3 = z$, $e_1^3 = z$ and $e_i^2 = z$ for $2 \leq i \leq n-2$, which result directly from the relations satisfied by t_i. Alternatively, noticing that it suffices to check the assertion for $n = 4$, one can obtain a proof of the claim by using the following instructions in GAP [33]:

```
G:=SymmetricGroup(4);

pi:=EpimorphismSchurCover(G);
M:=Kernel(pi);

z:=Elements(M)[2];
p1:=(1,2);
p2:=(2,3);
p3:=(3,4);

t1:=PreImagesRepresentative(pi,p1);
t2:=PreImagesRepresentative(pi,p2);
t3:=PreImagesRepresentative(pi,p3);

x:=Inverse(t1*t2)*t1*t3*t1*t2;
y:=t1*t3;

Print(Inverse(x)*Inverse(y)*x*y=z);
```

This last line of code outputs `true`, as desired.

From the claim, it follows that $M = \langle z \rangle$ is contained in $[V, V]$, finishing the proof of the lemma. □

Given a copy H of A_{n-1} inside A_n, one can subsequently repeat the same procedure of this last lemma and further restrict π to $W := \pi^{-1}(H)$ to seek a Schur covering group of H. The same argument works, but with two small caveats.

First, it is necessary to assure that we still have $z \in [W, W]$. To show this we will use the following lemma:

Lemma 3.2.5. *Let $n \geq 7$. Then any subgroup $H \leq A_n$ isomorphic to A_{n-1} is conjugate to the point stabilizer $(A_n)_n$ of the letter n in A_n*

Proof. This is a consequence of [96, Lemma 2.2]. □

By Lemma 3.2.5 we have $H = {(A_n)_n}^y$ for some $y \in S_n$. As π is surjective, $y = \pi(x)$ for some $x \in U$ and hence $z = z^x = [e_1^{-1}e_2e_1, e_2]^x = [(e_1^{-1}e_2e_1)^x, e_2^x]$ is in $[W, W]$, as clearly $\overline{e_1}, \overline{e_2} \in (A_n)_n$.

Second, note that we are making use of the fact that the Schur multipliers of A_{n-1} and S_n coincide, which does not hold for $n = 8$ (recall that $M(A_7) = \mathbb{Z}/6$). However, it is still true that $\pi^{-1}(A_7)$ gives a (non-maximal) stem extension (as defined in Section 1.3) of A_7, by the same reasoning as above. We have thus established the following result.

Lemma 3.2.6. *Let $n \geq 8$ and let H be a copy of A_{n-1} inside A_n. Then the restriction of the Schur cover V of A_n given in Lemma 3.2.4 to the group $W = \pi^{-1}(H)$ defines a stem extension of H.*

We can now prove the surjectivity of Cor_H^G for $n \geq 8$.

Proof of Lemma 3.2.1. Let V be the Schur covering group of G constructed in Lemma 3.2.4. We then have a central extension

$$1 \to M(G) \to V \xrightarrow{\pi} G \to 1,$$

where we identified the base normal subgroup M of V with the Schur multiplier $M(G)$ of G. Since $M(G) \subset [V, V]$, V is a *generalized representation group* (Definition 1.3.6) of G. Therefore, by Lemma 1.3.9 we have an isomorphism $\mathrm{Cor}_H^G(M(H)) \cong M(G) \cap [W, W]$, where $W = \pi^{-1}(H)$. Hence, it is enough to show that $M(G) \cap [W, W] = M(G)$. By Lemma 3.2.6, W defines a stem extension of H for $n \geq 8$, so that we immediately get $M(G) \subset [W, W]$. It follows that $M(G) \cap [W, W] = M(G)$, as desired. □

Using this lemma we show the vanishing of the cohomology group $\mathrm{H}^2(G, J_{G/H})$ (where $J_{G/H}$ is the Chevalley module of G/H, as defined in Section 1.6), which we will then use to prove Theorem 3.1.2 for $n \geq 8$.

Proposition 3.2.7. *Let $n \geq 8$ and H be a copy of A_{n-1} inside $G = A_n$. Then $\mathrm{H}^2(G, J_{G/H}) = 0$.*

Proof. Taking the G-cohomology of the exact sequence defining $J_{G/H}$

$$0 \to \mathbb{Z} \xrightarrow{\eta} \mathbb{Z}[G/H] \to J_{G/H} \to 0$$

(where $\eta : \mathbb{Z} \to \mathbb{Z}[G/H]$ is the norm map defined by $1 \mapsto \sum\limits_{gH \in G/H} gH$) gives an exact sequence of abelian groups

$$\mathrm{H}^2(G, \mathbb{Z}[G/H]) \to \mathrm{H}^2(G, J_{G/H}) \to \mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\eta^*} \mathrm{H}^3(G, \mathbb{Z}[G/H]).$$

Applying Shapiro's Lemma 1.1.7, the fundamental duality Theorem 1.2.5 in the cohomology of finite groups and the fact that $\hat{\mathrm{H}}^{-2}(G', \mathbb{Z}) \cong G'/[G', G']$ for any group G' (see [18, IV, §3, Proposition 1]), we have $\mathrm{H}^2(G, \mathbb{Z}[G/H]) \cong \mathrm{H}^2(H, \mathbb{Z}) \cong \hat{\mathrm{H}}^{-2}(H, \mathbb{Z}) \cong H/[H, H] = 0$, as H is perfect. Therefore, this last exact sequence becomes

$$0 \to \mathrm{H}^2(G, J_{G/H}) \to \mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\eta^*} \mathrm{H}^3(G, \mathbb{Z}[G/H]),$$

which shows that $\mathrm{H}^2(G, J_{G/H}) = 0$ if η^* is injective. Since the composition of the map η^* with the isomorphism of Shapiro's lemma

$$\mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\eta^*} \mathrm{H}^3(G, \mathbb{Z}[G/H]) \xrightarrow{\cong} \mathrm{H}^3(H, \mathbb{Z})$$

gives the restriction map by Lemma 1.1.8, it suffices to prove that the restriction

$$\mathrm{Res}^G_H : \mathrm{H}^3(G, \mathbb{Z}) \to \mathrm{H}^3(H, \mathbb{Z})$$

is injective. By Lemmas 1.2.3 and 1.2.6, this is the same as proving that the corestriction map

$$\mathrm{Cor}^G_H : \hat{\mathrm{H}}^{-3}(H, \mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G, \mathbb{Z})$$

is surjective. But this is the content of Lemma 3.2.1 and so it follows that $\mathrm{H}^2(G, J_{G/H}) = 0$. □

We now prove Theorem 3.1.2 for $n \geq 8$. We will make use of the following auxiliary lemma:

Lemma 3.2.8. *Let $n \geq 5$ and let H be a subgroup of $G = A_n$ with index n. Then $H \cong A_{n-1}$.*

Proof. G acts by multiplication on the set of cosets of H in G and identifying this set with $\{1, \ldots, n\}$ gives a homomorphism $\rho : G \to S_n$. Since A_n is simple, ρ is injective and therefore $\operatorname{Im} \rho = A_n$. Finally, note that $\rho(H)$ is a point stabilizer of a letter in $\{1, \ldots, n\}$ and so $\rho(H) \cong A_{n-1}$. It follows that the restriction of ρ to H gives an isomorphism $H \cong A_{n-1}$. □

Proof of Theorem 3.1.2 for $n \geq 8$. Set $G = \mathrm{Gal}(N/k) \cong A_n$ and $H = \mathrm{Gal}(N/K)$. By Theorems 1.5.8 and 1.5.12, it is enough to show that the group $\mathrm{H}^2(G, \widehat{T})$ is trivial, where $T = R^1_{K/k}\mathbb{G}_m$ is the norm one torus associated with the extension K/k. Recall that $\widehat{T} \cong J_{G/H}$ as G-modules by Proposition 1.6.5, so it suffices to prove that $\mathrm{H}^2(G, J_{G/H}) = 0$. But since $[G : H] = n$, we have $H \cong A_{n-1}$ by Lemma 3.2.8 and so the result follows from Proposition 3.2.7. □

Remark 3.2.9. Note that in the proof of Proposition 3.2.7 we actually showed that

$$\mathrm{H}^2(G, J_{G/H}) \cong \mathrm{Ker}(\mathrm{Res}^G_H : \mathrm{H}^3(G, \mathbb{Z}) \to \mathrm{H}^3(H, \mathbb{Z}))$$

for every $n \geq 6$. Using this fact and an approach similar to the one carried out in the proof of Lemma 3.2.1, one can show that $\mathrm{H}^2(G, J_{G/H}) = \mathbb{Z}/3$ when $n = 6$. Therefore the statement of Proposition 3.2.7 does not hold in this case and hence the proof of Theorem 3.1.2 for $n = 6$ requires a different strategy.

3.3 The case $n = 6$

In this section, we conclude the proof of Theorem 3.1.2 by using the computer algebra system GAP [33] to establish the remaining case $n = 6$. For this, we make use of the algorithms[1] developed by Hoshi and Yamasaki in [47]. In this work, the authors study the rationality of low-dimensional algebraic tori via the properties of the corresponding group modules, which they analyze using various computational methods. In particular, they create the following GAP algorithms:

[1] The code for these algorithms is available in the web page: https://www.math.kyoto-u.ac.jp/~yamasaki/Algorithm/RatProbAlgTori/, accessed December, 2020.

- `Norm1TorusJ(d,m)` (Algorithm N1T in [47, Section 8]), computing the action of G on $J_{G/H}$, where G is the transitive subgroup of S_d with GAP index number m (cf. [17] and [33]) and H is the stabilizer of one of the letters in G;
- `FlabbyResolution(G)` (Algorithm F1 in [47, Section 5.1]), computing a flasque resolution of the G-lattice M_G (see [47, Definition 1.26]);
- `H1(G)` (Algorithm F0 in [47, Section 5.0]), computing the cohomology group $\mathrm{H}^1(G, M_G)$ of the G-lattice M_G.

Using these algorithms, we can easily prove the A_6 case of Theorem 3.1.2 as follows:

Proof of the case $n = 6$ of Theorem 3.1.2. Set $G = \mathrm{Gal}(N/k) \cong A_6, H = \mathrm{Gal}(N/K)$ and $T = R^1_{K/k}\mathbb{G}_m$. Note that $H \cong A_5$ by Lemma 3.2.8 and that $\widehat{T} \cong J_{G/H}$ (as G-modules) by Proposition 1.6.5. Therefore, by Theorems 1.5.8 and 1.5.12 it is enough to prove that $\mathrm{H}^1(G, F_{G/H}) = 0$, where $F_{G/H}$ is a flasque module in a flasque resolution of $J_{G/H}$. Writing $K = N^H = k(\alpha_1)$ and $N = k(\alpha_1, \ldots, \alpha_6)$ for some $\alpha_i \in \overline{k}$, we see that H is the stabilizer of α_1 and so the above algorithm `Norm1TorusJ` to compute $J_{G/H}$ applies. Observing that A_6 is the transitive subgroup of S_6 with GAP index number 15, one can conclude that the desired cohomology group is trivial by running the following code in GAP:

```
gap> Read("FlabbyResolution.gap");
gap> J:=Norm1TorusJ(6,15);
<matrix group with 2 generators>
gap> F:=FlabbyResolution(J).actionF;
<matrix group with 2 generators>
gap> Product(H1(F));
1
```

□

Remark 3.3.1. The computation used for the case $n = 6$ in the previous proof can be reproduced for other small values of n. We have checked that for $n \leq 11$ the algorithm confirms our results, giving the trivial group for $n \neq 4$ and producing the counterexample $\mathrm{H}^1(A_4, F_{G/H}) = \mathbb{Z}/2$ for $n = 4$, as computed by Kunyavskiĭ in [57].

Although the primary goal of this section was to establish the case $n = 6$ of Theorem 3.1.2, the computer algorithms of Hoshi and Yamasaki employed here might be of independent interest. Indeed, this computational method can consistently be used to compute the birational invariant $\mathrm{H}^1(G, F_{G/H})$ for low-degree field extensions. In Section 4.4 we describe Hoshi and Yamasaki's method in greater detail, develop a slight modification of their algorithms and subsequently use it in Section 5.3 to deduce consequences on the validity of the Hasse norm principle and weak approximation for norm one tori in further cases.

Chapter 4

Explicit methods for the Hasse norm principle

4.1 Main results

While results of Colliot-Thélène and Sansuc (Theorem 1.5.12) give concise descriptions of the birational invariant $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ of an algebraic torus T, and a result of Tate (Theorem 1.5.13) does the same for its Tate–Shafarevich group, actually computing these groups in practice can be challenging. In this chapter we address this problem by giving theoretical results and explicit methods for computing the groups $Ш(T)$, $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ and $A(T)$ for the norm one torus $T = R^1_{K/k}\mathbb{G}_m$ of an extension of number fields K/k.

Except where stated otherwise, our assumptions throughout the rest of the chapter will be as follows. Let $T = R^1_{K/k}\mathbb{G}_m$ and let X denote a smooth compactification of T. Let L/k be a Galois extension containing K/k and set $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$.

Let X_0 be a smooth compactification of the torus $T_0 = R^1_{L/k}\mathbb{G}_m$. There is a natural inclusion $j : T \hookrightarrow T_0$, which induces canonical maps $A(T) \to A(T_0), Ш(T) \to Ш(T_0)$. Moreover, j extends to a morphism $j' : X \to X'$ for some *suitably chosen* smooth compactification X' of T_0 (see [13, §1.2.2.]) and so it induces a map $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^\sim \to \mathrm{H}^1(k, \operatorname{Pic} \overline{X'})^\sim$. Since $\mathrm{H}^1(k, \operatorname{Pic} \overline{X_1})$ is canonically isomorphic to $\mathrm{H}^1(k, \operatorname{Pic} \overline{X_2})$ for any two smooth compactifications X_1, X_2 of a torus by Theorem 1.5.9, we also obtain a map $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^\sim \to \mathrm{H}^1(k, \operatorname{Pic} \overline{X_0})^\sim$ compatible with Voskresenskiĭ's exact sequence in Theorem 1.5.8. Our first result utilizes these maps to obtain comparison isomorphisms between the aforementioned arithmetic invariants for the tori $R^1_{K/k}\mathbb{G}_m$ and $R^1_{L/k}\mathbb{G}_m$. In what follows, we write $A_{(p)}$ for the p-primary part of an abelian group A.

Theorem 4.1.1. *Let $L/K/k$ be a tower of finite extensions. Let $T_0 = R^1_{L/k}\mathbb{G}_m$, let $T = R^1_{K/k}\mathbb{G}_m$ and let X_0 and X be smooth compactifications of T_0 and T, respectively. For any prime p such that $p \nmid [L:K]$ there is a commutative diagram with exact rows as follows, where the vertical isomorphisms are induced by the natural inclusion $j : T \hookrightarrow T_0$:*

$$\begin{tikzcd}
0 \arrow[r] & A(T)_{(p)} \arrow[r] \arrow[d, "\cong"'] & \mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim}_{(p)} \arrow[r] \arrow[d, "\cong"'] & Ш(T)_{(p)} \arrow[r] \arrow[d, "\cong"'] & 0 \\
0 \arrow[r] & A(T_0)_{(p)} \arrow[r] & \mathrm{H}^1(k, \operatorname{Pic}\overline{X_0})^{\sim}_{(p)} \arrow[r] & Ш(T_0)_{(p)} \arrow[r] & 0.
\end{tikzcd}$$

Alternatively, the norm map $N_{L/K} : T_0 \twoheadrightarrow T$ can be used to obtain a commutative diagram similar to the one in Theorem 4.1.1 with the direction of the vertical isomorphisms reversed. Let

$$f_{L/K} : \mathrm{H}^1(k, \operatorname{Pic}\overline{X_0})^{\sim} \to \mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim}$$

be the canonical map induced by $N_{L/K}$. In order to study the birational invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$, we introduce an object called the '*unramified cover of the first obstruction to the HNP for K/k corresponding to the tower $L/K/k$*' defined as

$$\mathfrak{F}_{nr}(L/K/k) = \operatorname{Coker}(f_{L/K}).$$

In addition to general techniques from the arithmetic of algebraic tori, our work makes use of a quotient of the knot group called the '*first obstruction to the HNP for K/k corresponding to the tower $L/K/k$*' first defined by Drakokhrust and Platonov in [27] as

$$\mathfrak{F}(L/K/k) = (k^* \cap N_{K/k}(\mathbb{A}_K^*))/N_{K/k}(K^*)(k^* \cap N_{L/k}(\mathbb{A}_L^*)),$$

i.e. as the cokernel of the natural map $\mathfrak{K}(L/k) \to \mathfrak{K}(K/k)$. As shown in [27], the first obstruction to the HNP in a tower of number fields admits a purely group-theoretic description in terms of the relevant local and global Galois groups, see Theorem 4.3.5 below. In similar fashion to the first obstruction to the HNP, its unramified cover $\mathfrak{F}_{nr}(L/K/k)$ also admits an explicit group-theoretic description:

Theorem 4.1.2. *There is a canonical isomorphism*

$$\mathfrak{F}_{nr}(L/K/k) = (H \cap [G,G])/\Phi^G(H),$$

where $\Phi^G(H)$ denotes the focal subgroup of H in G, see Definition 4.3.7.

As a corollary, one can use this object to compute the p-primary parts of the knot group, the invariant $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$, and the defect of weak approximation for all but finitely many primes p. In what follows, let

$$\mathfrak{F}(G,H) = (H \cap [G,G])/\Phi^G(H).$$

Corollary 4.1.3. *If p is a prime such that $\mathrm{H}^3(G,\mathbb{Z})_{(p)} = 0$, then*

(i) $\mathfrak{K}(K/k)_{(p)} = \mathfrak{F}(L/K/k)_{(p)}$*;*

(ii) $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim}_{(p)} = \mathfrak{F}(G,H)_{(p)}$*;*

(iii) $A(T)_{(p)} = \operatorname{Ker}\left(\mathfrak{F}(G,H)_{(p)} \to \mathfrak{F}(L/K/k)_{(p)}\right)$*, where the map* $\mathfrak{F}(G,H) \to \mathfrak{F}(L/K/k)$ *is a natural surjection, see Section 4.3.*

Let $\overline{G}$ be a generalized representation group of G with base normal subgroup M, as defined in Section 1.3. By Theorems 1.5.12 and 1.6.8 the group $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ for $R^1_{L/k}\mathbb{G}_m$ is $\hat{\mathrm{H}}^{-3}(G,\mathbb{Z}) \cong M \cap [\overline{G}, \overline{G}]$, which equals $\mathfrak{F}(\overline{G}, M)$ since M is a central subgroup of $\overline{G}$. Our next main result shows that this is a special case of a more general phenomenon.

Theorem 4.1.4 (Drakokhrust)**.** *Let $\overline{G}$ be a generalized representation group of G with projection map λ. Then there is a canonical isomorphism*

$$\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim} = \mathfrak{F}(\overline{G}, \overline{H}),$$

where $\overline{H} = \lambda^{-1}(H)$.

We remark that the above theorem is a direct consequence of Drakokhrust's work in [26] (see the proof in Section 4.3), although it seems to have never appeared in the literature in the concise form given above. The formula in this theorem also enables the computation of the group $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ using a computer algebra system. We have implemented this formula as an algorithm in GAP [33], presented as Algorithm A2 in the Appendix 4.5.

4.2 Using subextensions and superextensions

In order to study the HNP and weak approximation in non-Galois extensions of k, it is often useful to be able to deduce information about the knot group of an extension K/k from information about its subextensions or superextensions, the latter meaning extensions of k containing K. In this section we collect some results that serve this purpose, proving Theorem 4.1.1 along the way.

Lemma 4.2.1. *Let K/k be a finite extension and let X be a smooth compactification of $T = R^1_{K/k}\mathbb{G}_m$. Then $T \times_k K$ is stably rational. Consequently,* $\mathrm{H}^1(K, \operatorname{Pic} \overline{X}) = 0$ *and* $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ *is killed by* $[K : k]$.

Proof. Write $T_K = T \times_k K$. Applying base change to the exact sequence defining T gives

$$1 \to T_K \to (R_{K/k}\mathbb{G}_m) \times_k K \xrightarrow{N_{K/k}} \mathbb{G}_{m,K} \to 1. \tag{4.2.1}$$

Let L/k be a Galois extension containing K. Let $G = \mathrm{Gal}(L/k)$ and let $H = \mathrm{Gal}(L/K)$. Taking character groups gives an exact sequence of H-modules

$$0 \to \mathbb{Z} \xrightarrow{N_{G/H}} \mathbb{Z}[G/H] \to \widehat{T_K} \to 0 \tag{4.2.2}$$

where $N_{G/H} : 1 \mapsto \sum\limits_{gH \in G/H} gH$. The map $\sum\limits_{gH \in G/H} a_{gH} \cdot gH \mapsto a_H$ defines a left splitting of (4.2.2). Therefore, (4.2.1) splits and consequently

$$T_K \times \mathbb{G}_{m,K} \cong (R_{K/k}\mathbb{G}_m) \times_k K.$$

Hence, T_K is K-stably rational, whereby $\mathrm{H}^1(K, \operatorname{Pic} \overline{X}) = \mathrm{H}^1(H, \operatorname{Pic} X_L) = 0$ by [20, Proposition 6]. Now recall that $\mathrm{Cor}^G_H \circ \mathrm{Res}^G_H$ is multiplication by $[G : H] = [K : k]$ by Lemma 1.1.3 and $\mathrm{Res}^G_H : \mathrm{H}^1(G, \operatorname{Pic} X_L) \to \mathrm{H}^1(H, \operatorname{Pic} X_L) = 0$. This completes the proof that $[K : k]$ kills $\mathrm{H}^1(G, \operatorname{Pic} X_L) = \mathrm{H}^1(k, \operatorname{Pic} \overline{X})$. □

The corollary below is an immediate consequence of Theorem 1.5.8 and Lemma 4.2.1.

Corollary 4.2.2. *Let $T = R^1_{K/k}\mathbb{G}_m$. Then $A(T)$ and $\mathfrak{K}(K/k)$ are killed by $[K : k]$.*

Lemma 4.2.3. *Let $\phi : T_1 \to T_2$ be a morphism of algebraic tori over k, and let X_1 and X_2 be smooth compactifications of T_1 and T_2, respectively. Then we obtain a commutative diagram with exact rows as follows, where the vertical arrows are induced by ϕ:*

$$\begin{tikzcd}
0 \arrow[r] & A(T_1) \arrow[r] \arrow[d] & \mathrm{H}^1(k, \operatorname{Pic} \overline{X_1})^{\sim} \arrow[r] \arrow[d] & Ш(T_1) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A(T_2) \arrow[r] & \mathrm{H}^1(k, \operatorname{Pic} \overline{X_2})^{\sim} \arrow[r] & Ш(T_2) \arrow[r] & 0.
\end{tikzcd}$$

Proof. It suffices to show that the diagram

$$\begin{tikzcd}
\mathrm{H}^1(k, \operatorname{Pic} \overline{X_1})^{\sim} \arrow[r, two heads] \arrow[d] & \text{Ш}(T_1) \arrow[d] \\
\mathrm{H}^1(k, \operatorname{Pic} \overline{X_2})^{\sim} \arrow[r, two heads] & \text{Ш}(T_2)
\end{tikzcd}$$

is commutative. But this follows from Voskresenskiĭ's proof of [91, Theorem 6], since all the cohomology groups involved in the construction of the surjection $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim} \twoheadrightarrow \text{Ш}(T)$ therein (namely $\hat{\mathrm{H}}^0(k, C_k(T)), \mathrm{H}^1(k, T(k))$ and $\mathrm{H}^1(k, C_k(N)) = \mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim}$) are functorial in T. □

Definition 4.2.4. An *isogeny* between two algebraic tori T_1, T_2 is a surjective morphism $\phi : T_1 \to T_2$ with finite kernel.

Corollary 4.2.5. *Let $\phi : T_1 \to T_2$ be an isogeny of algebraic tori over k with kernel μ. Let X_1 and X_2 be smooth compactifications of T_1 and T_2, respectively. Then for any prime p such that $p \nmid |\mu(\overline{k})|$, we obtain a commutative diagram with exact rows as follows, where the vertical isomorphisms are induced by ϕ:*

$$\begin{tikzcd}
0 \arrow[r] & A(T_1)_{(p)} \arrow[r] \arrow[d, "\cong"'] & \mathrm{H}^1(k, \operatorname{Pic} \overline{X_1})^{\sim}_{(p)} \arrow[r] \arrow[d, "\cong"'] & \text{Ш}(T_1)_{(p)} \arrow[r] \arrow[d, "\cong"'] & 0 \\
0 \arrow[r] & A(T_2)_{(p)} \arrow[r] & \mathrm{H}^1(k, \operatorname{Pic} \overline{X_2})^{\sim}_{(p)} \arrow[r] & \text{Ш}(T_2)_{(p)} \arrow[r] & 0.
\end{tikzcd}$$

Proof. There exists an isogeny $\psi : T_2 \to T_1$ (called the *dual isogeny*) such that $\psi \circ \phi$ is multiplication by $|\mu(\overline{k})|$ on T_1 (see [73, Proposition 1.3.1.]). Now apply Lemma 4.2.3. □

Using Corollary 4.2.5, we can now prove Theorem 4.1.1:

Proof of Theorem 4.1.1. Let S be the kernel of $N_{L/K} : R_{L/k}\mathbb{G}_m \to R_{K/k}\mathbb{G}_m$ and let $i : S \to R_{L/k}\mathbb{G}_m$ be the inclusion. Then the following diagram with exact rows commutes:

$$\begin{tikzcd}
1 \arrow[r] & S \arrow[r, "i"] \arrow[d, equal] & R^1_{L/k}\mathbb{G}_m \arrow[r, "N_{L/K}"] \arrow[d, hook] & R^1_{K/k}\mathbb{G}_m \arrow[r] \arrow[d, hook] & 1 \\
1 \arrow[r] & S \arrow[r, "i"] & R_{L/k}\mathbb{G}_m \arrow[r, "N_{L/K}"] & R_{K/k}\mathbb{G}_m \arrow[r] & 1.
\end{tikzcd}$$

Let $d = [L : K]$ and let $[d]$ denote the map $x \mapsto x^d$. The natural inclusion $j : R_{K/k}\mathbb{G}_m \to R_{L/k}\mathbb{G}_m$ satisfies $N_{L/K} \circ j = [d]$. Using i and j, we obtain a morphism of algebraic tori

$$\begin{aligned} \alpha\colon S \times R_{K/k}\mathbb{G}_m &\longrightarrow R_{L/k}\mathbb{G}_m \\ (x, y) &\longmapsto i(x)j(y) \end{aligned}$$

Note that if $(x, y) \in \operatorname{Ker}\alpha$, i.e. $i(x)j(y) = 1$, then $j(y) \in S$ and therefore $1 = N_{L/K}(j(y)) = y^d$. We thus see that $\operatorname{Ker}\alpha = \{(i^{-1}(j(x)), x^{-1}) \mid x \in R_{K/k}\mu_d\}$ (where μ_d is the group of d-th roots of unity) is finite. Moreover, α is surjective: given $z \in R_{L/k}\mathbb{G}_m(\overline{k})$, we have $N_{L/K}(z) = y^d$ for some $y \in R_{K/k}\mathbb{G}_m(\overline{k})$, and thus $N_{L/K}(z) = N_{L/K}(j(y))$, which gives $z = \alpha(x, y)$ for some $x \in S$. We conclude that α is an isogeny with kernel killed by d.

Let Z, W and W_0 be smooth compactifications of S, $R_{K/k}\mathbb{G}_m$ and $R_{L/k}\mathbb{G}_m$, respectively. By [91, Lemma 3], $\operatorname{Pic}(\overline{Z \times W}) = \operatorname{Pic}\overline{Z} \oplus \operatorname{Pic}\overline{W}$. Thus, Corollary 4.2.5 yields

$$\mathrm{H}^1(k, \operatorname{Pic}\overline{Z})_{(p)} \oplus \mathrm{H}^1(k, \operatorname{Pic}\overline{W})_{(p)} \cong \mathrm{H}^1(k, \operatorname{Pic}\overline{W_0})_{(p)}.$$

Furthermore, $R_{K/k}\mathbb{G}_m$ and $R_{L/k}\mathbb{G}_m$ are k-rational so $\mathrm{H}^1(k, \operatorname{Pic}\overline{W}) = \mathrm{H}^1(k, \operatorname{Pic}\overline{W_0}) = 0$ by [20, Proposition 6] and hence $\mathrm{H}^1(k, \operatorname{Pic}\overline{Z})_{(p)} = 0$. Therefore, $Ш(S)_{(p)} = A(S)_{(p)} = 0$ by Theorem 1.5.8. The result now follows from an application of Corollary 4.2.5 similar to the one done above, but to the surjective morphism

$$S \times R^1_{K/k}\mathbb{G}_m \to R^1_{L/k}\mathbb{G}_m$$

whose finite kernel is killed by d. □

The following special case of Theorem 4.1.1 reduces the calculation of $A(T)$, $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ and $Ш(T)$ to the case where K/k is the fixed field of a p-group.

Corollary 4.2.6. *Let $L/K/k$ be a tower of finite extensions with L/k Galois. Let $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$. For p prime, let H_p denote a Sylow p-subgroup of H and let K_p denote its fixed field. Let X and X_p be smooth compactifications of $T = R^1_{K/k}\mathbb{G}_m$ and $T_p = R^1_{K_p/k}\mathbb{G}_m$, respectively. Then we obtain a commutative diagram with exact rows as follows, where the vertical isomorphisms are induced by the natural inclusion $T \hookrightarrow T_p$:*

$$\begin{tikzcd} 0 \arrow[r] & A(T)_{(p)} \arrow[r] \arrow[d, "\cong"'] & \mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim}_{(p)} \arrow[r] \arrow[d, "\cong"'] & Ш(T)_{(p)} \arrow[r] \arrow[d, "\cong"'] & 0 \\ 0 \arrow[r] & A(T_p)_{(p)} \arrow[r] & \mathrm{H}^1(k, \operatorname{Pic}\overline{X_p})^{\sim}_{(p)} \arrow[r] & Ш(T_p)_{(p)} \arrow[r] & 0. \end{tikzcd}$$

Alternatively, the norm map $N_{K_p/K} : T_p \twoheadrightarrow T$ can be used to obtain a similar commutative diagram with the direction of the vertical isomorphisms reversed.

As a consequence of Corollary 4.2.6, we obtain the following result which deals with the two extremes in terms of the power of p dividing $|H|$.

Corollary 4.2.7. *Retain the notation of Corollary 4.2.6.*

(i) If $p \nmid |H|$*, then* $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})_{(p)} \cong \mathrm{H}^3(G, \mathbb{Z})_{(p)}$.

(ii) If H *contains a Sylow* p*-subgroup of* G*, then* $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})_{(p)} = 0$.

Proof. (i) Follows from Theorems 1.5.12 and 1.6.8 and Corollary 4.2.6.

(ii) Follows from Lemma 4.2.1. □

We additionally obtain the following result when H is a *Hall subgroup* of G, i.e. a subgroup such that $\gcd(|H|, [G : H]) = 1$.

Corollary 4.2.8. *Retain the notation of Corollary 4.2.6. If* H *is a Hall subgroup of* G*, then*

$$\begin{aligned}\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) &\cong \prod_{p \nmid |H|} \mathrm{H}^3(G, \mathbb{Z})_{(p)},\\ \mathfrak{K}(K/k) &\cong \prod_{p \nmid |H|} \mathfrak{K}(L/k)_{(p)}, \quad \textit{and}\\ A(T) &\cong \prod_{p \nmid |H|} A(T_0)_{(p)},\end{aligned}$$

where $T = R^1_{K/k}\mathbb{G}_m$ *and* $T_0 = R^1_{L/k}\mathbb{G}_m$.

Proof. Follows from Lemma 4.2.1 and Corollaries 4.2.2, 4.2.6, 4.2.7. □

We now drop the assumption that L/k is Galois and return to the more general setting of Theorem 4.1.1.

Corollary 4.2.9. *Retain the notation of Theorem 4.1.1. Then:*

(i) $A(T)$ *is killed by* $[L : K] \cdot \exp(A(T_0))$*;*

(ii) $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ *is killed by* $[L : K] \cdot \exp(\mathrm{H}^1(k, \operatorname{Pic} \overline{X_0}))$*;*

(iii) $Ш(T)$ *is killed by* $[L : K] \cdot \exp(Ш(T_0))$.

Proof. We give the proof for $A(T)$ – the other proofs are analogous. Let $d = [L : K]$, $e = \exp(A(T_0))$ and let $x \in A(T)$. Since $N_{L/K} \circ j = [d]$, we have $x^{de} = N_{L/K}(j(x)^e) = 1$, as $j(x) \in A(T_0)$. □

Corollary 4.2.10. *Retain the notation of Theorem 4.1.1.*

(i) If $\exp(A(T_0)) \cdot [L : K]$ *is coprime to* $[K : k]$*, then weak approximation holds for* K/k*.*

(ii) If $\exp(Ш(T_0)) \cdot [L : K]$ *is coprime to* $[K : k]$*, then the HNP holds for* K/k*.*

Proof. This follows immediately from Corollaries 4.2.2 and 4.2.9. □

The following result is a slight generalization of [42, Proposition 1].

Proposition 4.2.11. *Let* $L/K/k$ *be a tower of finite extensions and let* $d = [L : K]$*. Then the map* $x \mapsto x^d$ *induces a group homomorphism*

$$\varphi : \mathfrak{K}(K/k) \to \mathfrak{K}(L/k)$$

with $\operatorname{Ker}\varphi \subset \mathfrak{K}(K/k)[d]$ *and* $\{x^d \mid x \in \mathfrak{K}(L/k)\} \subset \operatorname{Im}\varphi$*. In particular, if* $|\mathfrak{K}(K/k)|$ *is coprime to* d*, then* φ *induces an isomorphism* $\mathfrak{K}(K/k) \cong \{x^d \mid x \in \mathfrak{K}(L/k)\}$*.*

Proof. The proposition follows from the inclusions $N_{L/k}(\mathbb{A}_L^*) \subset N_{K/k}(\mathbb{A}_K^*)$, $N_{L/k}(L^*) \subset N_{K/k}(K^*)$, $(N_{K/k}(\mathbb{A}_K^*))^d \subset N_{L/k}(\mathbb{A}_L^*)$ and $(N_{K/k}(K^*))^d \subset N_{L/k}(L^*)$. If $|\mathfrak{K}(K/k)|$ is coprime to d, then $\operatorname{Im}\varphi \subset \{x^d \mid x \in \mathfrak{K}(L/k)\}$. □

Next, we establish a generalization of Gurak's criterion (see [42, Proposition 2]) for the validity of the HNP in a compositum of two subextensions with coprime degrees.

Proposition 4.2.12. *Let* L/k *be a finite extension with subextensions* K/k *and* M/k *such that* $L = KM$*. Let* $T = R^1_{L/k}\mathbb{G}_m$*,* $T_1 = R^1_{K/k}\mathbb{G}_m$ *and* $T_2 = R^1_{M/k}\mathbb{G}_m$ *and let* X, X_1 *and* X_2 *be their respective smooth compactifications. Then we obtain a commutative diagram with exact rows as follows, where the vertical homomorphisms are induced by the natural inclusions* $T_1 \hookrightarrow T$ *and* $T_2 \hookrightarrow T$*:*

$$\begin{tikzcd}
0 \arrow[r] & A(T_1) \oplus A(T_2) \arrow[r] \arrow[d] & \mathrm{H}^1(k, \operatorname{Pic}\overline{X_1})^\sim \oplus \mathrm{H}^1(k, \operatorname{Pic}\overline{X_2})^\sim \arrow[r] \arrow[d] & Ш(T_1) \oplus Ш(T_2) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & A(T) \arrow[r] & \mathrm{H}^1(k, \operatorname{Pic}\overline{X})^\sim \arrow[r] & Ш(T) \arrow[r] & 0.
\end{tikzcd}$$

If $[K : k]$ *and* $[M : k]$ *are coprime, then the vertical maps in the diagram are isomorphisms.*

Proof. The commutative diagram comes from Lemma 4.2.3. If $[K : k]$ and $[M : k]$ are coprime, then any prime number divides at most one of $[L : K]$ and $[L : M]$, whence Lemma 4.2.1 and Theorem 4.1.1 show that the vertical maps in the diagram are isomorphisms. □

Proposition 4.2.13. *In the notation of Proposition 4.2.12, the map* $Ш(T_1) \oplus Ш(T_2) \to Ш(T)$ *induces the following homomorphism on the relevant knot groups*

$$\begin{aligned} \varphi : \mathfrak{K}(K/k) \times \mathfrak{K}(M/k) &\to \mathfrak{K}(L/k) \\ (x, y) &\mapsto x^n y^m \end{aligned}$$

where $m = [L : M]$ *and* $n = [L : K]$*. Moreover, if* $a = \exp(\mathfrak{K}(K/k))$*,* $b = \exp(\mathfrak{K}(M/k))$*, and* $h = \gcd(m, n)$*, then* φ *satisfies* $\operatorname{Ker}\varphi \subset \mathfrak{K}(K/k)[bn] \times \mathfrak{K}(M/k)[am]$ *and* $\{z^h \mid z \in \mathfrak{K}(L/k)\} \subset \operatorname{Im}\varphi$*.*

Proof. This follows from the argument in the proof of Proposition 4.2.11. □

We end this section by proving a version of [42, Theorem 1] for weak approximation in nilpotent Galois extensions. We require the following description of the defect of weak approximation:

Proposition 4.2.14. *Let* T *be a torus defined over a number field* k *and split by a finite Galois extension* L/k *with* $G = \operatorname{Gal}(L/k)$*. Then*

$$A(T)^{\sim} = \operatorname{Im}\left(Ш^2_\omega(G, \widehat{T}) \xrightarrow{\text{Res}} \prod_{v \in \Omega_k} \mathrm{H}^2(D_v, \widehat{T}) \right) \tag{4.2.3}$$

where $D_v = \operatorname{Gal}(L_v/k_v)$ *is the decomposition group at* v*. If* $T = R^1_{L/k}\mathbb{G}_m$ *then*

$$A(T)^{\sim} = \operatorname{Im}\left(\mathrm{H}^3(G, \mathbb{Z}) \xrightarrow{\text{Res}} \prod_{v \in \Omega_k} \mathrm{H}^3(D_v, \mathbb{Z}) \right). \tag{4.2.4}$$

Proof. The equality in (4.2.3) follows from Proposition 1.5.14. Then (4.2.4) follows from Theorem 1.6.8 and the analogous result that $\mathrm{H}^2(D_v, \widehat{T}) = \mathrm{H}^3(D_v, \mathbb{Z})$ in this setting. □

We make use of the following weak approximation version of [41, Lemma 2.3]:

Lemma 4.2.15. *Let K/k and M/k be finite subextensions of L/k such that $[K:k]$ and $[M:k]$ are coprime. If weak approximation holds for $R^1_{KM/M}\mathbb{G}_m$, then it holds for $R^1_{K/k}\mathbb{G}_m$. Under the additional assumption that K/k is Galois, weak approximation for $R^1_{K/k}\mathbb{G}_m$ implies weak approximation for $R^1_{KM/M}\mathbb{G}_m$.*

Proof. Let $T = R^1_{K/k}\mathbb{G}_m$, $T_M = T \times_k M$ and $T_K = T \times_k K$. Suppose first that weak approximation holds for $R^1_{KM/M}\mathbb{G}_m = T_M$. By Lemma 4.2.1 and Theorem 1.5.8, weak approximation holds for T_K. To complete the proof, observe that weak approximation for T_K and T_M implies weak approximation for $R_{K/k}T_K$ and $R_{M/k}T_M$. Since $[K:k]$ and $[M:k]$ are coprime, the surjective morphism of algebraic groups

$$\begin{aligned} R_{K/k}T_K \times R_{M/k}T_M &\to T \\ (x,y) &\mapsto N_{K/k}(x)N_{M/k}(y) \end{aligned}$$

has a section. Therefore, weak approximation for T follows from weak approximation for $R_{K/k}T_K$ and $R_{M/k}T_M$.

Now suppose that K/k is Galois and that weak approximation holds for $R^1_{K/k}\mathbb{G}_m$. Then KM/M is Galois with Galois group isomorphic to $\mathrm{Gal}(K/k)$. Let w be a place of M and let v be the place of k lying below w. The various restriction maps give a commutative diagram

$$\begin{tikzcd}
\mathrm{H}^3(\mathrm{Gal}(K/k),\mathbb{Z}) \arrow[r, "\cong"] \arrow[d, "\mathrm{Res}_v"] & \mathrm{H}^3(\mathrm{Gal}(KM/M),\mathbb{Z}) \arrow[d, "\mathrm{Res}_w"] \\
\mathrm{H}^3(D_v,\mathbb{Z}) \arrow[r] & \mathrm{H}^3(D_w,\mathbb{Z}).
\end{tikzcd}$$

Since weak approximation holds for $R^1_{K/k}\mathbb{G}_m$, isomorphism (4.2.4) of Proposition 4.2.14 shows that Res_v is trivial, and hence Res_w is also trivial. As w was arbitrary, weak approximation for $R^1_{KM/M}\mathbb{G}_m$ follows from (4.2.4). □

Remark 4.2.16. The hypothesis that K/k is Galois in the second implication of Lemma 4.2.15 is necessary. To see this, consider a Galois extension L/k with Galois group $G = C_3 \times S_3$ and with a decomposition group D_v containing the Sylow 3-subgroup of G for some place v of k (such an extension always exists, see Chapter 6). Let K/k and M/k be subextensions of L/k of degree 9 and 2, respectively. One can verify that the invariant $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ vanishes for K/k (see the example in Algorithm A1 of the Appendix 4.5) and thus weak approximation holds for $R^1_{K/k}\mathbb{G}_m$ by Theorem 1.5.8. On the other hand, $KM/M = L/M$ is Galois with Galois group $C_3 \times C_3$ and decomposition group $C_3 \times C_3$ for a prime of M

above v. It follows that weak approximation fails for $R^1_{KM/M}\mathbb{G}_m$ by isomorphism (4.2.4) of Proposition 4.2.14. See [60] for some other examples of varieties over number fields that satisfy weak approximation over the base field but not over a quadratic extension.

Proposition 4.2.17. *Let L/k be a Galois extension such that $G = \mathrm{Gal}(L/k)$ is nilpotent. For every prime p, let G_p be a Sylow p-subgroup of G. Let k_p and L_p be the fixed fields of the subgroups G_p and $\prod\limits_{q \neq p} G_q$, respectively. The following assertions are equivalent:*

(i) Weak approximation holds for $R^1_{L/k}\mathbb{G}_m$.

(ii) Weak approximation holds for each $R^1_{L_p/k}\mathbb{G}_m$.

(iii) Weak approximation holds for each $R^1_{L/k_p}\mathbb{G}_m$.

Proof. (i) $\implies$ (ii): Follows from Corollary 4.2.10.

(ii) $\implies$ (iii): Follows from Lemma 4.2.15.

(iii) $\implies$ (i): We prove $A(R^1_{L/k}\mathbb{G}_m)_{(p)} = 0$ for every prime p. Let v be a place of k and let w be a place of k_p above v. The various restriction maps give a commutative diagram

$$\begin{tikzcd}
\mathrm{H}^3(G, \mathbb{Z})_{(p)} \arrow[r, "\mathrm{Res}_1"] \arrow[d, "\mathrm{Res}_4"] & \mathrm{H}^3(D_v, \mathbb{Z})_{(p)} \arrow[d, "\mathrm{Res}_2"] \\
\mathrm{H}^3(G_p, \mathbb{Z}) \arrow[r, "\mathrm{Res}_3"] & \mathrm{H}^3(D_w, \mathbb{Z})
\end{tikzcd}$$

As weak approximation holds for $R^1_{L/k_p}\mathbb{G}_m$, isomorphism (4.2.4) of Proposition 4.2.14 yields $\mathrm{Im}\,\mathrm{Res}_3 = 0$. Furthermore, Lemma 1.1.4 shows that Res_2 is injective. It follows that $\mathrm{Im}\,\mathrm{Res}_1 = 0$ and, since v was arbitrary, we conclude that $A(R^1_{L/k}\mathbb{G}_m)_{(p)} = 0$ by (4.2.4). □

Remark 4.2.18. We note that the implication (iii) $\implies$ (i) in Proposition 4.2.17 does not require the hypothesis that G is nilpotent. This is analogous to the corresponding result for the HNP – see Gurak's remarks preceding [42, Theorem 2].

4.3 The first obstruction to the Hasse norm principle

In this section, we give some background concerning the first obstruction to the Hasse norm principle and then go on to prove Theorems 4.1.2 and 4.1.4 and Corollary 4.1.3. We remark that several results presented below will later be generalized in Section 8.1 for the *multinorm principle*.

We again fix a tower of number fields $L/K/k$ such that L/k is Galois and let X and X_0 be smooth compactifications of the tori $R^1_{K/k}\mathbb{G}_m$ and $R^1_{L/k}\mathbb{G}_m$, respectively. Applying Lemma 4.2.3 to the norm map $N_{L/K} : R^1_{L/k}\mathbb{G}_m \to R^1_{K/k}\mathbb{G}_m$ gives a commutative diagram with exact rows as follows, where the vertical arrows are induced by $N_{L/K}$:

$$\begin{tikzcd}
0 \arrow[r] & A(R^1_{L/k}\mathbb{G}_m) \arrow[r] \arrow[d] & \mathrm{H}^1(k, \operatorname{Pic} \overline{X_0})^{\sim} \arrow[r] \arrow[d, "f_{L/K}"] & Ш(R^1_{L/k}\mathbb{G}_m) \arrow[r] \arrow[d, "g_{L/K}"] & 0 \\
0 \arrow[r] & A(R^1_{K/k}\mathbb{G}_m) \arrow[r] & \mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim} \arrow[r] & Ш(R^1_{K/k}\mathbb{G}_m) \arrow[r] & 0.
\end{tikzcd} \tag{4.3.1}$$

Definition 4.3.1. In the notation of diagram (4.3.1), we define

1. $\mathfrak{F}(L/K/k) := \operatorname{Coker}(g_{L/K}) = (k^* \cap N_{K/k}(\mathbb{A}^*_K))/N_{K/k}(K^*)(k^* \cap N_{L/k}(\mathbb{A}^*_L))$, called the *first obstruction to the HNP for K/k corresponding to the tower $L/K/k$*, see [27, Definition 1];
2. $\mathfrak{F}_{nr}(L/K/k) := \operatorname{Coker}(f_{L/K})$, called the *unramified cover of* $\mathfrak{F}(L/K/k)$.

Clearly the knot group $\mathfrak{K}(K/k)$ (which is sometimes called the total obstruction to the HNP) surjects onto $\mathfrak{F}(L/K/k)$ and $\mathfrak{F}(L/K/k)$ equals $\mathfrak{K}(K/k)$ if the HNP holds for L/k. In [27], Drakokhrust and Platonov give another very useful sufficient criterion for this equality to hold, as follows:

Theorem 4.3.2. *[27, Theorem 3] Set $G = \operatorname{Gal}(L/k), H = \operatorname{Gal}(L/K)$. Let $G_1, \dots, G_r$ be subgroups of G and let $H_1, \dots, H_r$ be subgroups of H such that $H_i \subset H \cap G_i$ for each i. Let $K_i = L^{H_i}$ and $k_i = L^{G_i}$. Suppose that the HNP holds for the extensions K_i/k_i and that the map*

$$\bigoplus_{i=1}^{r} \operatorname{Cor}^G_{G_i} : \bigoplus_{i=1}^{r} \hat{\mathrm{H}}^{-3}(G_i, \mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G, \mathbb{Z})$$

is surjective. Then $\mathfrak{F}(L/K/k) = \mathfrak{K}(K/k)$.

In order to compute $\mathfrak{F}(L/K/k)$, Drakokhrust and Platonov give some explicit results relating this object to the local and global Galois groups of the tower $L/K/k$. We present their results here in a slightly more general setting. Let G be a finite group, let $H \leq G$, and let S be a set of subgroups of G. Consider the following commutative diagram:

$$\begin{tikzcd}
H/[H,H] \arrow[r, "\psi_1"] & G/[G,G] \\
\bigoplus_{D\in S}\left(\bigoplus_{Hx_iD\in H\backslash G/D} H_i/[H_i,H_i]\right) \arrow[u, "\varphi_1"] \arrow[r, "\psi_2"] & \bigoplus_{D\in S} D/[D,D] \arrow[u, "\varphi_2"']
\end{tikzcd} \tag{4.3.2}$$

where the x_i's are a set of representatives of the H–D double cosets of G, the sum over D is a sum over all subgroups in S, and $H_i := H \cap x_iDx_i^{-1}$. The maps ψ_1, φ_1 and φ_2 are induced by the natural inclusions $H \hookrightarrow G$, $H_i \hookrightarrow H$ and $D \hookrightarrow G$, respectively. If $h \in H_i$, then

$$\psi_2(h[H_i,H_i]) = x_i^{-1}hx_i[D,D] \in D/[D,D].$$

Given a subgroup $D \in S$, we denote by ψ_2^D the restriction of the map ψ_2 in diagram (4.3.2) to the subgroup $\bigoplus_{Hx_iD\in H\backslash G/D} H_i/[H_i,H_i]$.

Lemma 4.3.3. *In diagram* (4.3.2), $\varphi_1(\operatorname{Ker}\psi_2^D) \subset \varphi_1(\operatorname{Ker}\psi_2^{D'})$ *whenever* $D \subset D'$.

Proof. The proof proceeds in the same manner as the proof of [27, Lemma 2]. □

Lemma 4.3.4. *([27, Lemma 1] or [72, I, §9]) Set* $G = \mathrm{Gal}(L/k)$ *and* $H = \mathrm{Gal}(L/K)$. *Given a place* v *of* k, *the set of places* w *of* K *above* v *is in one-to-one correspondence with the set of double cosets in the decomposition* $G = \bigcup_{i=1}^{r_v} Hx_iD_v$. *If* w *corresponds to* Hx_iD_v, *then the decomposition group* H_w *of the extension* L/K *at* w *equals* $H \cap x_iD_vx_i^{-1}$.

Set $G = \mathrm{Gal}(L/k)$, $H = \mathrm{Gal}(L/K)$ and $S = \{D_v \mid v \in \Omega_k\}$. Lemma 4.3.4 shows that, with these choices, diagram (4.3.2) takes the form

$$\begin{tikzcd}
H/[H,H] \arrow[r, "\psi_1"] & G/[G,G] \\
\bigoplus_{v\in\Omega_k}\left(\bigoplus_{w\mid v} H_w/[H_w,H_w]\right) \arrow[u, "\varphi_1"] \arrow[r, "\psi_2"] & \bigoplus_{v\in\Omega_k} D_v/[D_v,D_v] \arrow[u, "\varphi_2"']
\end{tikzcd} \tag{4.3.3}$$

where the sum over $w \mid v$ is a sum over all places w of K above v and H_w is the decomposition group of L/K at w.

Theorem 4.3.5. *[27, Theorem 1] With the notation of diagram (4.3.3), there is a canonical isomorphism*

$$\mathfrak{F}(L/K/k) = \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2).$$

We write ψ_2^{nr} for the restriction of the map ψ_2 to the subgroup

$$\bigoplus_{v \text{ unramified in } L/k} \Big(\bigoplus_{w|v} H_w/[H_w, H_w]\Big)$$

and define ψ_2^r similarly using the ramified places.

Lemma 4.3.6. *Set $G = \operatorname{Gal}(L/k)$ and $H = \operatorname{Gal}(L/K)$. Let C be the set of all cyclic subgroups of G and let φ_1^C and ψ_2^C denote the relevant maps in diagram (4.3.2) with $S = C$. Then*

$$\varphi_1(\operatorname{Ker}\psi_2^{nr}) = \varphi_1^C(\operatorname{Ker}\psi_2^C)$$

where the maps in the expression on the left are the ones in diagram (4.3.3).

Proof. This follows from the Chebotarev density theorem and Lemma 4.3.3. □

Definition 4.3.7. Let H be a subgroup of a finite group G. The *focal subgroup of H in G* is

$$\begin{aligned}\Phi^G(H) &= \langle h_1^{-1}h_2 \mid h_1, h_2 \in H \text{ and } h_2 \text{ is } G\text{-conjugate to } h_1\rangle \\ &= \langle [h, x] \mid h \in H \cap xHx^{-1}, x \in G\rangle \trianglelefteq H.\end{aligned}$$

Theorem 4.3.8. *[27, Theorem 2] In the notation of diagram (4.3.3), we have*

$$\varphi_1(\operatorname{Ker}\psi_2^{nr}) = \Phi^G(H)/[H, H].$$

Theorem 4.3.8 is very useful – quite often one can show that $\Phi^G(H) = H \cap [G, G]$ and hence the first obstruction $\mathfrak{F}(L/K/k)$ is trivial. In fact, since $[N_G(H), H] \subset \Phi^G(H)$, if one can show that $[N_G(H), H] = H \cap [G, G]$, then $\mathfrak{F}(L/K/k) = 1$. This criterion generalizes [42, Theorem 3].

Remark 4.3.9. The group $\operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2)$ featured in Theorem 4.3.5 can be computed in finite time. Indeed, $\operatorname{Ker}\psi_1$ is given in terms of the relevant Galois groups, and by [27, p. 307] we have

$$\varphi_1(\operatorname{Ker}\psi_2) = \varphi_1(\operatorname{Ker}\psi_2^{nr})\varphi_1(\operatorname{Ker}\psi_2^r). \tag{4.3.4}$$

Hence, Theorem 4.3.8 and the fact that only finitely many places of k ramify in L/k show that $\varphi_1(\operatorname{Ker}\psi_2)$ can be obtained by a finite computation. We combined these facts to assemble a function `1obs(G,H,l)` in GAP [33] that, given the groups $G = \operatorname{Gal}(L/k)$, $H = \operatorname{Gal}(L/K)$ and the list l of decomposition groups D_v at the ramified places v, returns the group $\operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2)$ isomorphic to the first obstruction $\mathfrak{F}(L/K/k)$. This function will be used in Chapter 5 and we present its code in Algorithm A4 of the Appendix 4.5 together with an example.

Our next task is to prove Theorem 4.1.2, which gives a purely group-theoretic description of $\mathfrak{F}_{nr}(L/K/k)$. First, recall the definition of the group $\mathfrak{F}(G,H)$:

Definition 4.3.10. Let G be a finite group and let $H \leq G$. We define the group $\mathfrak{F}(G,H)$ as

$$\mathfrak{F}(G,H) = (H \cap [G,G])/\Phi^G(H).$$

Returning to the situation of a tower of number fields $L/K/k$ with L/k Galois, $G = \operatorname{Gal}(L/k)$ and $H = \operatorname{Gal}(L/K)$ and letting ψ_1, φ_1^C and ψ_2^C denote the relevant maps in diagram (4.3.2) with $S = C$, the set of all cyclic subgroups of G, we have

$$\mathfrak{F}(G,H) = \operatorname{Ker}\psi_1/\varphi_1^C(\operatorname{Ker}\psi_2^C). \tag{4.3.5}$$

We now prove the following strengthening of Theorem 4.1.2:

Theorem 4.3.11. *There is a canonical isomorphism $\mathfrak{F}_{nr}(L/K/k) = \mathfrak{F}(G,H)$ under which the natural surjection $\mathfrak{F}_{nr}(L/K/k) \twoheadrightarrow \mathfrak{F}(L/K/k)$ coincides with the natural surjection $\mathfrak{F}(G,H) \twoheadrightarrow \mathfrak{F}(L/K/k)$ induced by Theorem 4.3.5.*

Proof. The norm map $N_{L/K}$ induces a commutative diagram of k-tori with exact lines:

$$\begin{tikzcd}
1 \arrow[r] & R^1_{L/k}\mathbb{G}_m \arrow[r] \arrow[d, "N_{L/K}"] & R_{L/k}\mathbb{G}_m \arrow[r] \arrow[d, "N_{L/K}"] & \mathbb{G}_m \arrow[r] \arrow[d, "="] & 1 \\
1 \arrow[r] & R^1_{K/k}\mathbb{G}_m \arrow[r] & R_{K/k}\mathbb{G}_m \arrow[r] & \mathbb{G}_m \arrow[r] & 1
\end{tikzcd} \tag{4.3.6}$$

Taking character groups in (4.3.6) and then taking G-cohomology gives the following commutative diagram of abelian groups with exact lines:

$$\begin{tikzcd}
\mathrm{H}^2(G,\mathbb{Z}) \arrow[r, "\theta_1"] \arrow[d, "="] & \mathrm{H}^2(G,\mathbb{Z}[G/H]) \arrow[r, "\theta_2"] \arrow[d] & \mathrm{H}^2(G,\widehat{T}) \arrow[r, "\theta_3"] \arrow[d, "f^*_{L/K}"] & \mathrm{H}^3(G,\mathbb{Z}) \arrow[d, "="] \\
\mathrm{H}^2(G,\mathbb{Z}) \arrow[r] & \mathrm{H}^2(G,\mathbb{Z}[G]) = 0 \arrow[r] & \mathrm{H}^2(G,\widehat{T_0}) \arrow[r] & \mathrm{H}^3(G,\mathbb{Z})
\end{tikzcd} \tag{4.3.7}$$

By Theorem 1.5.12 and Lemma 1.2.3, the unramified cover

$$\mathfrak{F}_{nr}(L/K/k) = \operatorname{Coker}\left(f_{L/K} : \mathrm{H}^1(k, \operatorname{Pic}\overline{X_0})^{\sim} \to \mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim}\right)$$

is dual to

$$\operatorname{Ker}\left(f^*_{L/K}|_{Ш^2_\omega(G,\widehat{T})} : Ш^2_\omega(G,\widehat{T}) \to Ш^2_\omega(G,\widehat{T_0})\right).$$

As the first line of diagram (4.3.7) is exact, we have

$$\operatorname{Ker}\left(f^*_{L/K}|_{Ш^2_\omega(G,\widehat{T})}\right) = \operatorname{Im}\theta_2 \cap Ш^2_\omega(G,\widehat{T}).$$

Furthermore, by Lemma 1.6.6, taking character groups in the second line of (4.3.6) and then taking both G-cohomology and $\langle g\rangle$-cohomology, we obtain the following commutative diagram with exact lines

$$\begin{tikzcd}
\mathrm{H}^2(G,\mathbb{Z}) \arrow[r, "\theta_1"] \arrow[d] & \mathrm{H}^2(G,\mathbb{Z}[G/H]) \arrow[r, "\theta_2"] \arrow[d, "\theta_4"] & \mathrm{H}^2(G,\widehat{T}) \arrow[d] \\
\prod_{g\in G}\mathrm{H}^2(\langle g\rangle,\mathbb{Z}) \arrow[r, "\theta_5"] & \prod_{g\in G}\mathrm{H}^2(\langle g\rangle,\mathbb{Z}[G/H]) \arrow[r] & \prod_{g\in G}\mathrm{H}^2(\langle g\rangle,\widehat{T})
\end{tikzcd} \tag{4.3.8}$$

(where the vertical arrows are products of restriction maps) and a straightforward diagram chase shows that θ_2 induces an isomorphism

$$\theta_4^{-1}(\operatorname{Im}\theta_5)/\operatorname{Im}\theta_1 \cong \operatorname{Im}\theta_2 \cap Ш^2_\omega(G,\widehat{T}).$$

In [75, Theorem 6.12] and pages leading to it, the authors show that the first square in diagram (4.3.8) is dual to diagram (4.3.2) with $S = C = \{\text{cyclic subgroups of } G\}$, reproduced below:

$$\begin{tikzcd}
H/[H,H] \arrow[rr, "\psi_1"] & & G/[G,G] \\
\bigoplus_{g\in G}\Big(\bigoplus_{Hx_i\langle g\rangle\in H\backslash G/\langle g\rangle}\langle x_i g x_i^{-1}\rangle \cap H\Big) \arrow[u, "\varphi_1^C"] \arrow[rr, "\psi_2^C"] & & \bigoplus_{g\in G}\langle g\rangle \arrow[u]
\end{tikzcd} \tag{4.3.9}$$

In particular, $\theta_4^{-1}(\operatorname{Im}\theta_5)/\operatorname{Im}\theta_1$ is dual to $\operatorname{Ker}\psi_1/\varphi_1^C(\operatorname{Ker}\psi_2^C)$ and the existence of a canonical isomorphism $\mathfrak{F}_{nr}(L/K/k) = \mathfrak{F}(G,H)$ follows from (4.3.5). Theorem 4.3.5 can be proved in an analogous way by considering a version of diagram (4.3.8) with all decomposition groups in place of all cyclic subgroups of G and recalling from Theorem 1.5.13 that $Ш(T)$ is dual to $Ш^2(G,\widehat{T})$. Proposition 1.5.14 now yields the desired compatibility. □

Proof of Corollary 4.1.3. This is a direct consequence of diagram (4.3.1) and Theorems 1.5.12, 1.6.8 and 4.3.11. □

Corollary 4.3.12. *If H is a Hall subgroup of G, then $\mathfrak{F}_{nr}(L/K/k) = \mathfrak{F}(L/K/k) = 1$.*

Proof. The focal subgroup theorem [44] asserts that for a Hall subgroup H of G, we have $\mathfrak{F}(G, H) = 1$. The result therefore follows from Theorem 4.1.2 and the surjection $\mathfrak{F}_{nr}(L/K/k) \twoheadrightarrow \mathfrak{F}(L/K/k)$. □

We end this chapter by giving a proof of Theorem 4.1.4 and presenting a lemma to be used alongside this theorem in Chapter 5.

Proof of Theorem 4.1.4. For any $v \in \Omega_k$, define

$$S_v = \begin{cases} \lambda^{-1}(D_v) \text{ if } v \text{ is ramified in } L/k; \\ \text{a cyclic subgroup of } \lambda^{-1}(D_v) \text{ with } \lambda(S_v) = D_v \text{ otherwise.} \end{cases}$$

Consider the version of diagram (4.3.2) with respect to the groups $\overline{G}$, $\overline{H}$ and $S = \{S_v \mid v \in \Omega_k\}$. In this setting, Drakokhrust shows in [26, Theorem 2] that

$$\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim} = \operatorname{Ker} \psi_1 / \varphi_1(\operatorname{Ker} \psi_2^{nr}),$$

where ψ_2^{nr} denotes the restriction of ψ_2 to the subgroup

$$\bigoplus_{v \text{ unramified in } L/k} \Big(\bigoplus_{i=1}^{r_v} \overline{H} \cap x_i S_v x_i^{-1} \Big)$$

and the x_i's are a set of representatives for the double coset decomposition $\overline{G} = \bigcup_{i=1}^{r_v} \overline{H} x_i S_v$.

By the Chebotarev density theorem we can choose the subgroups S_v for v unramified in such a way that every cyclic subgroup of $\overline{G}$ is in S. For this choice, we obtain

$$\operatorname{Ker} \psi_1 / \varphi_1(\operatorname{Ker} \psi_2^{nr}) = \mathfrak{F}(\overline{G}, \overline{H}).$$

Indeed, we clearly have $\operatorname{Ker} \psi_1 = (\overline{H} \cap [\overline{G}, \overline{G}])/[\overline{H}, \overline{H}]$ and the equality $\varphi_1(\operatorname{Ker} \psi_2^{nr}) = \Phi^{\overline{G}}(\overline{H})/[\overline{H}, \overline{H}]$ follows from Lemma 4.3.6 and an argument similar to the proof of [27, Theorem 2]. □

Lemma 4.3.13. *We have* $\mathfrak{F}(\overline{G},\overline{H}) \cong \mathfrak{F}(G,H)$ *if and only if* $\operatorname{Ker}\lambda \cap [\overline{G},\overline{G}] \subset \Phi^{\overline{G}}(\overline{H})$, *where the notation is as in Theorem 4.1.4.*

Proof. Let $\Lambda : \mathfrak{F}(\overline{G},\overline{H}) \to \mathfrak{F}(G,H)$ be the homomorphism induced by the projection map λ. It is clear that Λ is surjective. We prove that Λ is injective if and only if $\operatorname{Ker}\lambda \cap [\overline{G},\overline{G}] \subset \Phi^{\overline{G}}(\overline{H})$.

If $\operatorname{Ker}\lambda \cap [\overline{G},\overline{G}] \not\subset \Phi^{\overline{G}}(\overline{H})$, then taking any element $k \in \operatorname{Ker}\lambda \cap [\overline{G},\overline{G}]$ that is not in $\Phi^{\overline{G}}(\overline{H})$ would produce a non-trivial element in $\operatorname{Ker}\Lambda$. Conversely, suppose that $\operatorname{Ker}\lambda \cap [\overline{G},\overline{G}] \subset \Phi^{\overline{G}}(\overline{H})$ and let $x \in \operatorname{Ker}\Lambda$ so that $\lambda(x) \in \Phi^{G}(H)$. For simplicity we assume that $\lambda(x)$ is a commutator (the general case follows along the same line), i.e. $\lambda(x) = [h,g] = h^{-1}g^{-1}hg$ for some $g \in G, h \in H$ such that $g^{-1}hg \in H$. Let $\overline{h} \in \overline{H}$ and $\overline{g} \in \overline{G}$ be such that $\lambda(\overline{h}) = h$ and $\lambda(\overline{g}) = g$. Then $\lambda(\overline{g}^{-1}\overline{h}\overline{g}) = g^{-1}hg \in H$ and hence $[\overline{h},\overline{g}] \in \Phi^{\overline{G}}(\overline{H})$. Since $\lambda([\overline{h},\overline{g}]) = \lambda(x)$, we have $x = [\overline{h},\overline{g}]k$ for some $k \in \operatorname{Ker}\lambda$. As both x and $[\overline{h},\overline{g}]$ are in $[\overline{G},\overline{G}]$, we see that $k \in \operatorname{Ker}\lambda \cap [\overline{G},\overline{G}]$. Since $\operatorname{Ker}\lambda \cap [\overline{G},\overline{G}] \subset \Phi^{\overline{G}}(\overline{H})$, we deduce that k (and thus also x) is in $\Phi^{\overline{G}}(\overline{H})$ so that Λ is injective. □

4.4 Computational methods

In this section we present some computational methods to compute the groups $\text{Ш}(T)$ and $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$, where X is a smooth compactification of the norm one torus $T = R^1_{K/k}\mathbb{G}_m$ of an extension of number fields K/k.

We begin by outlining the computational method in GAP developed by Hoshi and Yamasaki (already used in Section 3.3) to compute the birational invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ by means of the identification $\mathrm{H}^1(k, \operatorname{Pic}\overline{X}) = \mathrm{H}^1(G, F_{G/H})$ of Theorem 1.5.12, where $F_{G/H}$ is a flasque module in a flasque resolution of $\widehat{T} \cong J_{G/H}$. This algorithm starts by computing the Chevalley module $J_{G/H}$ via the function `Norm1TorusJ` (Algorithm N1T in [47, Section 8]) with inputs d and m, giving the action of G on $J_{G/H}$, where G is the transitive subgroup of S_d with GAP index number m (cf. [17] and [33]) and H is the stabilizer of one of the letters in G. It then computes (via the function `FlabbyResolution`, Algorithm F1 in [47, Section 5.1]) all the relevant group modules (namely, the flasque and the permutation module) involved in a flasque resolution of $J_{G/H}$, as defined in Section 1.5. For instance, using this function one can access the flasque module in a flasque resolution of $J_{G/H}$ by invoking the command `FlabbyResolution(Norm1TorusJ(d,m)).actionF`. Finally, Hoshi and Yamasaki's method outputs the desired group $\mathrm{H}^1(G, F_{G/H})$ by using the algorithm `H1` (Algorithm F0 in [47, Section 5.0]).

Example 4.4.1. Since A_4 is the fourth transitive subgroup of S_4 in the GAP library `TransitiveGroups`, the command

```
gap> Product(H1(FlabbyResolution(Norm1TorusJ(4,4)).actionF));
2
```

computes the order of the group $\mathrm{H}^1(G, F_{G/H})$ for $G = A_4$ and $H = A_3$, i.e. the size of the invariant $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ for an A_4-quartic, confirming Kunyavskiĭ's result in [57] that this group is isomorphic to $\mathbb{Z}/2$.

As noted above, Hoshi and Yamasaki's algorithm `Norm1TorusJ` requires one to embed the Galois group G as a transitive subgroup of S_n, whereupon one quickly reaches the limit of the databases of such groups stored in computational algebra systems such as GAP. This would be a problem if one were to use this function to compute the invariant $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ for some of the groups we will analyze later on (namely, in Propositions 5.1.7 and 5.1.9). To overcome this issue, we have employed a small modification of Hoshi and Yamasaki's function `Norm1TorusJ` that does not require one to view the Galois group G as a transitive subgroup of S_d. Instead, our function simply takes as input a pair of finite groups (G, H) where H is a subgroup of G and computes the G-module $J_{G/H}$. Analogously to the `Norm1TorusJ` algorithm, our routine will output the module $J_{G/H}$ as a M_G*-module*, defined as follows:

Definition 4.4.2. [47, Definition 1.26] *Let n be a positive integer and let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Z})$. The G-lattice M_G of rank n is defined to be the G-module with $\mathbb{Z}$-basis $\{u_1, \ldots, u_n\}$ equipped with the right action of G given by $u_i.g = \sum_{j=1}^{n} a_{i,j} u_j$ for any $g = [a_{i,j}] \in G$.*

We now detail our method. Set $d = |G/H|$ and fix a set of right coset representatives $\{Hg_1, \ldots, Hg_d\}$ of H in G. In this way, we have $\mathbb{Z}[G/H] = \sum_{i=1}^{d} Hg_i\mathbb{Z}$ and $N_{G/H}(1) = \sum_{i=1}^{d} Hg_i \in \mathbb{Z}[G/H]$. Let $B = \{Hg_1 + N_{G/H}(1)\mathbb{Z}, \ldots, Hg_{d-1} + N_{G/H}(1)\mathbb{Z}\}$ be a $\mathbb{Z}$-basis of $J_{G/H}$. As the submodule $N_{G/H}(1)\mathbb{Z}$ is fixed by the action of any element of G, we will omit it when working with elements of B.

Given $g \in G$, we build a matrix $R_g \in \mathrm{GL}_{d-1}(\mathbb{Z})$ as follows. For any $Hg_i \in B$, we have $(Hg_i).g = Hg_{\sigma(i)}$ for some $1 \leq \sigma(i) \leq d$. There are two cases:

1. If $\sigma(i) < d$, then the k-th entry of the i-th row of R_g is set to be equal to 1 if $k = \sigma(i)$ and 0 otherwise.

2. If $\sigma(i) = d$, i.e. $(Hg_i).g = Hg_d = -\sum_{i=1}^{d-1} Hg_i$ inside $J_{G/H}$, then the k-th entry of the i-th row of R_g is set to be equal to -1 for every k.

Let R_G be the group $\langle R_g \mid g \in G\rangle \leq \mathrm{GL}_{d-1}(\mathbb{Z})$. It is then clear that the Chevalley module $J_{G/H}$ is isomorphic to the G-module M_{R_G}, which is the output of our function. The code for this function is presented in Algorithm A1 in the Appendix 4.5 and it consists of two routines:

- `row(s,d)` (an auxiliary routine to `action`), constructing the i-th row of the matrix R_g as explained above;
- `action(G,H)`, assembling the matrices R_g for $g \in G$ and returning the group R_G.

These GAP functions can then be combined with Hoshi and Yamasaki's algorithms `FlabbyResolution` and `H1` to compute $\mathrm{H}^1(G, F_{G/H})$ as described above and we present an example of such a computation in the Appendix 4.5.

For some of our future computational applications, we do not employ the algorithms of Hoshi and Yamasaki and instead use the formula of Theorem 4.1.4 which expresses $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ in terms of generalized representation groups of G. We also implemented this formula, along with the simplification afforded by Corollary 4.2.6, as an algorithm in GAP (see Algorithm A2 in the Appendix 4.5, where we also include an example).

Remark 4.4.3. It is noteworthy to compare the method of computing $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ via Theorem 4.1.4 with Hoshi and Yamasaki's algorithm. The approach based on Theorem 4.1.4 involves the computation of the focal subgroup $\Phi^G(H)$, which is generally fast for small subgroups H but impractical for large ones. On the contrary, Hoshi and Yamasaki's method using flasque resolutions deals only with the G-module $J_{G/H}$, whose $\mathbb{Z}$-rank $\frac{|G|}{|H|} - 1$ decreases as $|H|$ grows. Therefore this technique (or the modified version presented as Algorithm A1 in the Appendix 4.5) is usually preferable when H is large. In general, a combination of the two algorithms is the most convenient way to compute $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ for all subgroups of a fixed group G.

The knot group of any Galois extension L/k can also be computed in a computer algebra system by combining the isomorphism (1.6.5) of Theorem 1.6.9 and Lemma 1.3.9. We used these two results to implement an algorithm (presented as Algorithm A3 in the Appendix 4.5 together with an example) in GAP that, given the group $\mathrm{Gal}(L/k)$ and the list l of decomposition groups D_v at the ramified places, returns the knot group $\mathfrak{K}(L/k)$.

4.5 Appendix: Algorithms for the Hasse norm principle

In the following algorithms, we add a few comments in gray (marked with a #, which is also the GAP command for a comment and treated as white space by this program) explaining the goal of several selected lines of code.

4.5.1 A1: computing the Chevalley module $J_{G/H}$

```
row:=function(s,d)
   local r,k;

   r:=[]; # i-th row of $R_g$

   if s = d then # Case (2) of p. 50
      r:=List([1..d-1],x->-1);
   else # Case (1) of p. 49
      for k in [1..d-1] do
         if k = s then
            r:=Concatenation(r,[1]);
         else
            r:=Concatenation(r,[0]);
         fi;
      od;
   fi;

   return r;
end;


action:=function(G,H)
   local d,gens,RT,LT,S,j,Rg,i,s;

   d:=Order(G)/Order(H);
   gens:=GeneratorsOfGroup(G);
   RT:=RightTransversal(G,H);
   LT:=List(RT,i->CanonicalRightCosetElement(H,i)); # List of right coset
```

```
representatives of $H$ in $G$
   S:=[]; # List of matrices $R_g$ for $g \in$ gens

   for j in [1..Size(gens)] do
      Rg:=List([1..d-1],x->0); # Creating a matrix with $d-1$ lines
      for i in [1..d-1] do
         s:=PositionCanonical(RT,LT[i]*gens[j]);
# Obtaining the index s $=\sigma(i)$ of the right coset $(H.L[i])$.gens[j] in RT
         Rg[i]:=row(s,d); # Producing the $i$-th row of $R_{\texttt{gens}[j]}$
      od;
      S:=Concatenation(S,[Rg]); # Appending the matrix $R_{\texttt{gens}[j]}$ to S
   od;

   return GroupByGenerators(S); # Returning the group $R_G$
end;


H1Flasque:=function(G,H)
   local J,FR,FM;

   J:=action(G,H); # Matrix group $R_G$
   FR:=FlabbyResolution(J); # Flasque resolution of $R_G$
   FM:=FR.actionF; # Flasque module in FR

   return Product(H1(FM)); # Returning the cohomology group $\mathrm{H}^1(G,\texttt{FM})$
end;
```

Example: Computation of $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ for the extension K/k of Remark 4.2.16, a degree 9 extension with $C_3 \times S_3$ normal closure:

```
   G:=SmallGroup(18,3);
   StructureDescription(G);
   » "C3 x S3"
   H:=SylowSubgroup(G,2);
   StructureDescription(H);
   » "C2"
   H1Flasque(G,H);
   » 1
```

4.5.2 A2: computing $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ via Theorem 4.1.4

```
Fquot:=function(G,H)
# Function that computes the group $\frac{H\cap[G,G]}{\Phi^G(H)}$

   local l,h1,h2,U,V;

   l:=[];

   for h1 in H do
   for h2 in H do
      if IsConjugate(G,h1,h2) then Append(l,[Inverse(h1)*h2]);fi; # Note that $\Phi^G(H) = \langle h_1^{-1}h_2 \mid h_1, h_2 \in H$ are G-conjugate$\rangle$, see Definition 4.3.7
   od;
   od;

   U:=Intersection(H,DerivedSubgroup(G));
   V:=Subgroup(U,l);
   return U/V;
end;

H1:=function(G,H)
   local GG,lambda,M,HH,res,p,FHp;

   GG:=SchurCover(G);
   lambda:=EpimorphismSchurCover(G); # Projection map $\lambda : \overline{G} \to G$, where $\overline{G}$ is a Schur covering group of $G$
   M:=Kernel(lambda);
   HH:=PreImagesSet(lambda,H); # HH = $\lambda^{-1}(H)$

   res:=Subgroup(HH,[]);

   if Size(HH)=1 then return res;
   else # We compute the $p$-part $\mathfrak{F}(\overline{G},\overline{H})_{(p)}$ for all primes $p \mid |\overline{H}|$ and then take their direct product below
      for p in Set(Factors(Size(HH))) do
         FHp:=Fquot(GG,SylowSubgroup(HH,p)); # Here we use the fact that $\mathfrak{F}(\overline{G},\overline{H})_{(p)} = \mathfrak{F}(\overline{G},\overline{H_p})_{(p)}$ as follows from Theorem 4.1.4 and Corollary 4.2.6
      res:=DirectProduct(res,SylowSubgroup(FHp,p));
    od;

  return res;
  fi;
end;
```

Example: Computation of $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ for an extension K/k with degree 1260 and A_7-normal closure (note that $|A_7| = 2520 = 2 \times 1260$):

```
  G:=AlternatingGroup(7);
  H:=Subgroup(G,[(1,2)(3,4)]);
  StructureDescription(H);
  » "C2"
  Size(H1(G,H));
  » 6
```

4.5.3 A3: computing $\mathfrak{K}(L/k)$ via Theorem 1.6.9

```
Sha:=function(G,l)
  local lambda,M,ImDecGps,D,ImGen,i;

  lambda:=EpimorphismSchurCover(G); # Projection map $\lambda : \overline{G} \to G$, where $\overline{G}$
is a Schur covering group of $G$
  M:=Kernel(lambda);

  if Size(l)=0 then return M;
  else
    ImDecGps:=List(l,D->Intersection(M,DerivedSubgroup(PreImagesSet(lambda,D))));
# Collecting all the groups $\mathrm{Cor}_{D_v}^{G}(\hat{\mathrm{H}}^{-3}(D_v,\mathbb{Z})) \cong M \cap [\lambda^{-1}(D_v), \lambda^{-1}(D_v)]$ by Lemma 1.3.9
    ImGen:=[];
    for i in ImDecGps do
      Append(ImGen,GeneratorsOfGroup(i));
    od;
    return M/Subgroup(M,ImGen); # Returning the group $\text{Ш}(T)$, which is isomorphic
to $\mathrm{Coker}\left(\prod_{v \in \Omega_k} \hat{\mathrm{H}}^{-3}(D_v,\mathbb{Z}) \xrightarrow{\mathrm{Cor}} \hat{\mathrm{H}}^{-3}(G,\mathbb{Z})\right)$ by Theorem 1.6.9
  fi;
```

```
end;
```

Example: Computation of $\mathfrak{K}(L/k)$ for an octic D_4-extension L/k with decomposition group V_4 at all ramified places and for an octic D_4-extension with cyclic decomposition group C_2 at all ramified places:

```
   G:=SmallGroup(8,3);
   StructureDescription(G);
   » "D8"
   l1:=Filtered(AllSubgroups(G),x->StructureDescription(x)="C2 x C2");
   l2:=Filtered(AllSubgroups(G),x->StructureDescription(x)="C2");
   Size(Sha(G,l1));
   » 1
   Size(Sha(G,l2));
   » 2
```

4.5.4 A4: computing $\mathfrak{F}(L/K/k)$ via Theorem 4.3.5

```
directprod:=function(l)
# Auxiliary function computing the direct product of a list of lists as the
following example illustrates:  directprod([[1,2],[3],[4,5]]) outputs the list
[[1,3,4],[1,3,5],[2,3,4],[2,3,5]]

   local res,i,j,t,T,s;

   res:=[];;

# Base cases |l| = 1 or 2
   if Size(l)=1 then return List(l[1],x->[x]); fi;
   if Size(l)=2 then
      for i in l[1] do
         for j in l[2] do
            res:=Concatenation(res,[[i,j]]);;
         od;
      od;
   return res;
   else
      t:=List([2..Size(l)],x->l[x]);;
      T:=directprod(t);; # Recursive step

      for i in l[1] do
         s:=[];;
         for j in T do
            s:=Concatenation([i],j);;
            res:=Concatenation(res,[s]);;
         od;
      od;
   fi;
   return res;
end;

obsv:=function(G,H,Gv)
# Function that computes the group $\varphi_1(\operatorname{Ker}\psi_2^v)$ in the notation of Diagram (4.3.3)

   local K,S,l,Hv,w,Li,Sx,res,i,t,j,f,im;

   K:=Intersection(H,DerivedSubgroup(G));;
   S:=DoubleCosetRepsAndSizes(G,H,Gv);;
   l:=List(S,x->x[1]);;
   Hv:=[];;

   for w in l do # Constructing the groups $H_w$ of Diagram 4.3.3
      if Size(Intersection(H,ConjugateGroup(Gv,Inverse(w)))) <> 1 then
         Hv:=Concatenation(Hv,[[Intersection(H,ConjugateGroup(Gv,Inverse(w))),w]]);;
      fi;
   od;

   Li:=List(Hv,x->(Elements(x[1])));;
   if Size(Li)=0 then return Subgroup(K/DerivedSubgroup(H),[]);
   else
      Sx:=directprod(Li);; # Accessing all the elements of the group $\bigoplus_{w|v} H_w$ in
Diagram 4.3.3
      res:=[];;
      for i in Sx do # Looping over all elements of $\bigoplus_{w|v} H_w$:
         t:=1;;
         for j in [1..Size(i)] do
            t:=t*Inverse(Hv[j][2])*i[j]*Hv[j][2];;
         od;
# Verifying and registering all elements of $\bigoplus_{w|v} H_w$ that are in $\operatorname{Ker}\psi_2^v$:
         if t in DerivedSubgroup(Gv) then res:=Concatenation(res,[i]);fi;
      od;

      f:=NaturalHomomorphismByNormalSubgroup(K,DerivedSubgroup(H));;
      im:=List(res,x->Image(f,Product(x)));; # Computing the image via $\varphi_1$ of
every element in $\operatorname{Ker}\psi_2^v$

      return Subgroup(K/DerivedSubgroup(H),im); # Returning the group $\varphi_1(\operatorname{Ker}\psi_2^v)$
   fi;
end;

obsram:=function(G,H,l)
# Function that computes the group $\varphi_1(\operatorname{Ker}\psi_2^r)$ (in the notation of p. 44) by using
the previous function obsv

   local K,li,x;

   K:=Intersection(H,DerivedSubgroup(G));;
   li:=[];;
   for x in l do
      Append(li,Elements(obsv(G,H,x)));; # Collecting all the elements of the
groups $\operatorname{Ker}\psi_2^v$ for $v$ ramified
   od;

   return Subgroup(K/DerivedSubgroup(H),li); # Outputting the group
$\prod_{v \text{ ramified}} \varphi_1(\operatorname{Ker}\psi_2^v) = \varphi_1(\operatorname{Ker}\psi_2^r)$

end;
```

```
obsunr:=function(G,H)
   local K,l,h1,h2,f,im;
# Function that computes the group $\varphi_1(\operatorname{Ker}\psi_2^{nr})$ (in the notation of p. 44), which
equals $\Phi^G(H)/[H,H]$ by Theorem 4.3.8

   K:=Intersection(H,DerivedSubgroup(G));;
   l:=[];;
   for h1 in H do
   for h2 in H do
      if IsConjugate(G,h1,h2) then Append(l,[Inverse(h1)*h2]);fi; # Again recall
that $\Phi^G(H) = \langle h_1^{-1}h_2 \mid h_1, h_2 \in H$ are G-conjugate$\rangle$ (Definition 4.3.7)
   od;
   od;

   f:=NaturalHomomorphismByNormalSubgroup(K,DerivedSubgroup(H));;
   im:=List(l,x->Image(f,x));;

   return Subgroup(K/DerivedSubgroup(H),im); # Outputting $\varphi_1(\operatorname{Ker}\psi_2^{nr})$
end;

1obs:=function(G,H,l)
# Function that computes the group $\mathfrak{F}(L/K/k) = \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2)$ (Theorem 4.3.5)
by invoking all the previous functions

   local K,Elts,J;

   K:=Intersection(H,DerivedSubgroup(G)); # Note that $H \cap [G,G] = \operatorname{Ker}\psi_1$
   Elts:=Concatenation(Elements(obsunr(G,H)),Elements(obsram(G,H,l)));
# Concatenation of the elements in $\varphi_1(\operatorname{Ker}\psi_2^{nr})$ and $\varphi_1(\operatorname{Ker}\psi_2^{r})$
   J:=Subgroup(K/DerivedSubgroup(H),Elts); # Computing the group $\varphi_1(\operatorname{Ker}\psi_2) =$
$\varphi_1(\operatorname{Ker}\psi_2^{nr})\varphi_1(\operatorname{Ker}\psi_2^{r})$

   return K/J; # Outputting the group $\operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2)$
end;
```

Example: Computation of $\mathfrak{F}(L/K/k)$ for a degree 20 extension K/k with A_6-normal closure and decomposition group D_4 at all ramified places:

```
G:=AlternatingGroup(6);
H:=Filtered(AllSubgroups(G),x->Size(x)=18)[1];
StructureDescription(H);
» "(C3 x C3) :  C2"
Size(G)/Size(H);
» 20
D:=Subgroup(G,[(1,2,3,4)(5,6),(1,3)(5,6)]);
StructureDescription(D);
» "D8"
Size(1obs(G,H,[D]));
» 1
```

Chapter 5

Applications to A_n and S_n-extensions

5.1 Main results

Let K/k be an extension of number fields. In this chapter we apply the techniques developed in Chapter 4 to analyze the obstruction to the Hasse norm principle for K/k and the defect of weak approximation for $R^1_{K/k}\mathbb{G}_m$ when the normal closure of K/k has alternating A_n or symmetric S_n Galois group.

The set-up throughout this chapter is as follows: $L/K/k$ is a tower of number fields such that L/k is Galois and $G = \operatorname{Gal}(L/k)$ is isomorphic to A_n or S_n with $n \geq 4$. We set $H = \operatorname{Gal}(L/K)$, $T = R^1_{K/k}\mathbb{G}_m$ and we let X denote a smooth compactification of T.

Our first theorem gives explicit and computable formulas for the knot group and the birational invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$:

Theorem 5.1.1. *Suppose that G is isomorphic to A_n or S_n for some $n \geq 4$ and $G \not\cong A_6, A_7$. Then*

$$\mathfrak{K}(K/k) = \begin{cases} \mathfrak{F}(L/K/k), \text{ if } |H| \text{ is even;} \\ \mathfrak{F}(L/K/k) \times \mathfrak{K}(L/k), \text{ if } |H| \text{ is odd,} \end{cases}$$

and

$$\mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim} = \begin{cases} \mathfrak{F}_{nr}(L/K/k), \text{if } |H| \text{ is even;} \\ \mathfrak{F}_{nr}(L/K/k) \times \mathbb{Z}/2, \text{ if } |H| \text{ is odd.} \end{cases}$$

Remark 5.1.2. The defect of weak approximation $A(T)$ can also be obtained from Theorem 5.1.1 and the fact that the surjection $\mathrm{H}^1(k, \operatorname{Pic}\overline{X}) \twoheadrightarrow Ш(T)$ in Voskresenskiĭ's exact sequence (Theorem 1.5.8) coincides with the natural surjection $\mathfrak{F}_{nr}(L/K/k) \twoheadrightarrow \mathfrak{F}(L/K/k)$.

Recall that Theorem 1.6.9, due to Tate, shows that the knot group of the Galois extension L/k is dual to $\operatorname{Ker}(\mathrm{H}^3(G,\mathbb{Z}) \to \prod_v \mathrm{H}^3(D_v,\mathbb{Z}))$, where D_v denotes the decomposition group at a place v of k. Note that this kernel only depends on the decomposition groups at the ramified places, since if v is unramified then D_v is cyclic and hence $\mathrm{H}^3(D_v,\mathbb{Z}) = 0$. In the setting of Theorem 5.1.1 we are therefore able to obtain an algorithm (enabled by the earlier algorithms described in Section 4.4) that takes as inputs G, H and the decomposition groups at the ramified places of L/k and gives as its outputs the knot group $\mathfrak{K}(K/k)$, the invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$, and the defect of weak approximation $A(T)$ for $T = R^1_{K/k}\mathbb{G}_m$.

Using Theorem 5.1.1 we also characterize the possible isomorphism classes of the group $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$:

Theorem 5.1.3. *(i) For $G \cong S_n$ the invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ is an elementary abelian 2-group. Moreover, every possibility for $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ is realised: given an elementary abelian 2-group A, there exists $n \in \mathbb{N}$ and an extension of number fields K/k whose normal closure has Galois group S_n such that $\mathrm{H}^1(k, \operatorname{Pic}\overline{X}) \cong A$, where X is a smooth compactification of $R^1_{K/k}\mathbb{G}_m$.*

(ii) For $G \cong A_n$ the invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ is either isomorphic to C_3, C_6 or an elementary abelian 2-group. Again, every possibility for $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ is realised.

Remark 5.1.4. The statement of Theorem 5.1.3 also holds if one replaces $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ by $\mathfrak{K}(K/k)$ or $A(T)$, see Proposition 6.2.1.

Theorems 5.1.1 and 5.1.3 can be combined to obtain more precise information, as demonstrated in Corollary 5.1.5 and Example 5.1.6 below.

Corollary 5.1.5. *Retain the assumptions of Theorem 5.1.1 and, for p prime, let H_p denote a Sylow p-subgroup of H. Then $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})_{(p)} = 0$ for all primes $p > 3$, $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})_{(3)} = 0$ if $G \cong S_n$,*

$$\mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim}_{(2)} = \begin{cases} \mathfrak{F}(G,H)[2] \cong \mathfrak{F}(G,H_2) & \text{if } |H| \text{ is even;} \\ \mathbb{Z}/2 & \text{if } |H| \text{ is odd,} \end{cases}$$

and if $G \cong A_n$ then

$$\mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim}_{(3)} = \mathfrak{F}(G,H)[3] \cong \mathfrak{F}(G,H_3).$$

In particular, if $3 \nmid |H|$ then $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ is 2-torsion.

Example 5.1.6. Suppose that $G \cong S_n$ and $|H|$ is odd. Then $\mathrm{H}^1(k, \operatorname{Pic}\overline{X}) = \mathbb{Z}/2$ and $\mathfrak{K}(K/k) = \mathfrak{K}(L/k)$. The same conclusion holds for $G \cong A_n$ under the stronger assumption that $|H|$ is coprime to 6.

As a further application of Theorem 5.1.1, one can obtain conditions on the decomposition groups determining whether the HNP and weak approximation hold in A_n and S_n extensions. In Propositions 5.1.7 and 5.1.8, we exhibit such a characterization for $n = 4$ or 5, when these local conditions are particularly simple.

Proposition 5.1.7. *Suppose that G is isomorphic to A_4, A_5, S_4 or S_5. Then $\mathfrak{K}(K/k) \hookrightarrow C_2$ and*

(i) if $|H|$ is odd, then $\mathfrak{K}(K/k) = 1 \iff \exists\, v$ such that $V_4 \hookrightarrow D_v$;

(ii) if $\exists\, C \leq H$ generated by a double transposition with $[H : C]$ odd, then $\mathfrak{K}(K/k) = 1 \iff \exists\, v$ such that D_v contains a copy of V_4 generated by two double transpositions;

(iii) in all other cases, $\mathfrak{K}(K/k) = 1$.

Proposition 5.1.8. *Retain the assumptions of Proposition 5.1.7. Then*

$$\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) = \begin{cases} \mathbb{Z}/2 & \text{in cases (i) and (ii) of Proposition 5.1.7;} \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, in cases (i) and (ii) of Proposition 5.1.7, weak approximation holds for $R^1_{K/k}\mathbb{G}_m$ if and only if the HNP fails for K/k. In all other cases, weak approximation holds for $R^1_{K/k}\mathbb{G}_m$.

For the sake of completeness, we also provide criteria for the validity of the HNP when $G \cong A_6$ or A_7 (the two groups not addressed by Theorem 5.1.1), see Propositions 5.1.9 below. The proof uses the first obstruction to the HNP, along with various tricks involving moving between subextensions as detailed in Section 4.2.

Proposition 5.1.9. *Suppose that G is isomorphic to A_6 or A_7. Then $\mathfrak{K}(K/k) \hookrightarrow C_6$ and*

- $$\mathfrak{K}(K/k)_{(2)} = 1 \iff \begin{cases} V_4 \hookrightarrow H; \text{ or} \\ C_4 \hookrightarrow H \text{ and } \exists\, v \text{ such that } D_4 \hookrightarrow D_v; \text{ or} \\ 4 \nmid |H| \text{ and } \exists\, v \text{ such that } V_4 \hookrightarrow D_v. \end{cases}$$

- $$\mathfrak{K}(K/k)_{(3)} = 1 \iff \begin{cases} C_3 \hookrightarrow H; \text{ or} \\ \exists\, v \text{ such that } C_3 \times C_3 \hookrightarrow D_v. \end{cases}$$

Proposition 5.1.10 below addresses weak approximation in the A_6 and A_7 cases. The local conditions controlling weak approximation are given in detail in Proposition 5.3.6; they are a direct consequence of Propositions 5.1.9 and 5.1.10 and Voskresenskiĭ's exact sequence (1.5.1) of Theorem 1.5.8.

Proposition 5.1.10. *Retain the assumptions of Proposition 5.1.9. Then* $\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) \hookrightarrow \mathbb{Z}/6$ *and*

- $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})_{(2)} = 0$ *if and only if* $V_4 \hookrightarrow H$*;*
- $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})_{(3)} = 0$ *if and only if* $C_3 \hookrightarrow H$*.*

Remark 5.1.11. Proposition 5.1.10 and Voskresenskiĭ's exact sequence in Theorem 1.5.8 immediately give the validity of the HNP and weak approximation for the norm one torus of a degree 6 (respectively, degree 7) extension K/k with normal closure having Galois group A_6 (respectively, A_7). Moreover, one can use Theorems 4.1.2 and 5.1.1 to prove that both the HNP and weak approximation for the norm one torus hold for a degree n extension with A_n-normal closure, if $n \geq 5$ and $n \neq 6, 7$. We thus obtain a new proof of the main theorem of Chapter 3. Similarly, our techniques can be used to reprove Voskresenskiĭ and Kunyavskiĭ's Theorem 2.0.6 and Bartels results in Theorems 2.0.4 and 2.0.5.

5.2 Proof of the main theorems

In this section we prove the main theorems of this chapter, namely Theorems 5.1.1 and 5.1.3. We also show Corollary 5.1.5. For any subgroup G' of G, we denote by $F_{G/G'}$ a flasque module in a flasque resolution of the Chevalley module $J_{G/G'}$, see Section 1.5. We use the isomorphism (1.5.2) in Theorem 1.5.12 to identify $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ with $\mathrm{H}^1(G, F_{G/H})$ to make clear that this group only depends on the pair (G, H).

First, we complete the proof of Theorem 5.1.1. For $G \cong A_n$ or S_n, we have $\mathrm{H}^3(G, \mathbb{Z}) \cong \mathbb{Z}/2$, unless $G \cong A_6$ or A_7 in which case $\mathrm{H}^3(G, \mathbb{Z}) \cong \mathbb{Z}/6$. Therefore, in our proof of Theorem 5.1.1, we can apply Corollary 4.1.3 to deal with the odd order torsion. It remains to analyze the 2-primary parts of $\mathfrak{K}(K/k)$ and $\mathrm{H}^1(G, F_{G/H})$. We start with the simpler case where $|H|$ is odd.

Proposition 5.2.1. *If* $|H|$ *is odd, then*

(i) $\mathrm{H}^1(G, F_{G/H})_{(2)} = \mathbb{Z}/2$*, and*

(ii) $\mathfrak{K}(K/k)_{(2)} = \mathfrak{K}(L/k)_{(2)}$ *and* $\mathfrak{K}(K/k)_{(2)}$ *has size at most 2.*

Proof. (i) This follows from Corollary 4.2.7(i).

(ii) This is a consequence of Theorem 4.1.1 and isomorphism (1.6.5) of Theorem 1.6.9. □

Proof of Theorem 5.1.1 for $|H|$ *odd.* We analyze the p-primary parts of the groups in Theorem 5.1.1 for each prime p. For p odd, apply Corollary 4.1.3 and use the fact that $\mathfrak{K}(L/k)^{\sim} \hookrightarrow \mathrm{H}^3(G, \mathbb{Z}) = \mathbb{Z}/2$ (Theorem 1.6.9). For $p = 2$, use Proposition 5.2.1. By Theorem 4.1.2, $\mathfrak{F}_{nr}(L/K/k) = \mathfrak{F}(G, H)$ is a subquotient of $H \cap [G, G]$, whereby $\mathfrak{F}_{nr}(L/K/k)_{(2)} = 1$, since $|H|$ is odd. As $\mathfrak{F}_{nr}(L/K/k)$ surjects onto $\mathfrak{F}(L/K/k)$, we also have $\mathfrak{F}(L/K/k)_{(2)} = 1$. □

We now solve the case where $|H|$ is even. For this, we will use the generalized representation group $\overline{G}$ of G, the projection map λ and the base normal subgroup $M = \langle z \rangle$ presented in Proposition 5.2.2 below.

Proposition 5.2.2. *Let* $n \geq 4$ *and let* U *be the group with generators* $z, \overline{t_1}, \ldots, \overline{t_{n-1}}$ *and relations*

(i) $z^2 = 1$;

(ii) $z\overline{t_i} = \overline{t_i}z$, for $1 \leq i \leq n-1$;

(iii) $\overline{t_i}^2 = z$, for $1 \leq i \leq n-1$;

(iv) $(\overline{t_i}.\overline{t_{i+1}})^3 = z$, for $1 \leq i \leq n-2$;

(v) $\overline{t_i}.\overline{t_j} = z\overline{t_j}.\overline{t_i}$, for $|i - j| \geq 2$ and $1 \leq i, j \leq n-1$.

Then U *is a Schur covering group of* S_n *with base normal subgroup* $M = \langle z \rangle$*. Moreover, if* t_i *denotes the transposition* $(i\ \ i+1)$ *in* S_n*, then the map*

$$\begin{aligned} \lambda\colon U &\longrightarrow S_n \\ z &\longmapsto 1 \\ \overline{t_i} &\longmapsto t_i \end{aligned}$$

is surjective and has kernel M*. Additionally, if* $n \neq 6, 7$*, then a generalized representation group of* A_n *is given by* $V = \lambda^{-1}(A_n) = \langle z, \overline{t_1}.\overline{t_2}, \overline{t_1}.\overline{t_3}, \ldots, \overline{t_1}.\overline{t_{n-1}} \rangle \leq U$*.*

Proof. See Schur's original paper [84] or [45, Chapter 2] for a proof that U has the desired properties. The final assertion concerning A_n was dealt with in Lemma 3.2.4. □

Lemma 5.2.3. *Suppose that G is not isomorphic to A_6 or A_7 and that $|H|$ is even. Let $h \in H$ be any element of order 2. Then there exists a copy A of V_4 inside G such that*

- *$h \in A$;*
- *$z \in [\lambda^{-1}(A), \lambda^{-1}(A)]$.*

Proof. **Case 1) h comprises a single transposition.** Relabeling if necessary, we can assume that $h = (1\ 2)$. Take $A = \langle (1\ 2), (3\ 4) \rangle$ and note that $[\lambda^{-1}((1\ 2)), \lambda^{-1}((3\ 4))] = [\overline{t_1}, \overline{t_3}]$ in the notation of Proposition 5.2.2. Using the relations satisfied by the elements $\overline{t_i} \in \overline{G}$ given in Proposition 5.2.2, it is clear that this commutator is equal to z, as desired.

Case 2) h comprises more than one transposition. Relabeling if necessary, we can assume that $h = (1\ 2)(3\ 4) \cdots (n-1\ n)$ for some even $n \geq 4$. Take $A = \langle h, x \rangle$, where $x = (1\ 3)(2\ 4)$ and let us prove by induction that $z = [\lambda^{-1}(h), \lambda^{-1}(x)]$. Note that, in the notation of Proposition 5.2.2, we have $h = t_1.t_3.\cdots.t_{n-1}$ and $x = t_2.t_1.t_2.t_3.t_2.t_3$.

Base case $n = 4$: A straightforward (but long) computation using the relations satisfied by the elements $\overline{t_i}$ given in Proposition 5.2.2 shows that

$$[\lambda^{-1}(h), \lambda^{-1}(x)] = [\overline{t_1}.\overline{t_3}, \overline{t_2}.\overline{t_1}.\overline{t_2}.\overline{t_3}.\overline{t_2}.\overline{t_3}] = z.$$

Alternatively, this can be verified using the following instructions in GAP [33]:

```
G:=SymmetricGroup(4);

lambda:=EpimorphismSchurCover(G);
M:=Kernel(lambda);

z:=Elements(M)[2];
p1:=(1,2);
p2:=(2,3);
p3:=(3,4);

t1:=PreImagesRepresentative(lambda,p1);
t2:=PreImagesRepresentative(lambda,p2);
t3:=PreImagesRepresentative(lambda,p3);
```

```
x:=t1*t3;
y:=t2*t1*t2*t3*t2*t3;

Print(Inverse(x)*Inverse(y)*x*y=z);
```

This last line of code outputs `true`, as desired.

Inductive step: Suppose that $h = (1\ 2)(3\ 4)\cdots(n-1\ n)(n+1\ n+2)$. Denoting the permutation $(1\ 2)(3\ 4)\cdots(n-1\ n)$ by $\tilde{h}$, write $h = \tilde{h}.t_{n+1}$. Now

$$[\lambda^{-1}(h), \lambda^{-1}(x)] = [\lambda^{-1}(\tilde{h})\overline{t_{n+1}}, \lambda^{-1}(x)] = [\lambda^{-1}(\tilde{h}), \lambda^{-1}(x)]^{\overline{t_{n+1}}}[\overline{t_{n+1}}, \lambda^{-1}(x)].$$

By the inductive hypothesis and the relations of Proposition 5.2.2, $[\lambda^{-1}(\tilde{h}), \lambda^{-1}(x)]^{\overline{t_{n+1}}} = z^{\overline{t_{n+1}}} = z$ and $[\overline{t_{n+1}}, \lambda^{-1}(x)] = [\overline{t_{n+1}}, \overline{t_2}.\overline{t_1}.\overline{t_2}.\overline{t_3}.\overline{t_2}.\overline{t_3}] = 1$, as desired. □

The next proposition completes the proof of Theorem 5.1.1.

Proposition 5.2.4. *Suppose that G is not isomorphic to A_6 or A_7 and that $|H|$ is even. Then*

(i) $\mathrm{H}^1(G, F_{G/H})^{\sim} = \mathfrak{F}_{nr}(L/K/k)$;

(ii) $\mathfrak{K}(K/k) = \mathfrak{F}(L/K/k)$.

Proof. (i) By Theorems 4.1.2, 4.1.4 and isomorphism (1.5.2) of Theorem 1.5.12, if we can show that $\mathfrak{F}(\overline{G}, \overline{H}) \cong \mathfrak{F}(G, H)$ then it will follow that the natural surjection $\mathrm{H}^1(G, F_{G/H})^{\sim} \twoheadrightarrow \mathfrak{F}_{nr}(L/K/k)$ is an isomorphism. By Lemma 4.3.13, it suffices to check that $\operatorname{Ker}\lambda \subset \Phi^{\overline{G}}(\overline{H})$, i.e. that $z \in \Phi^{\overline{G}}(\overline{H})$. Let $A = \langle h, x\rangle$ be the copy of V_4 constructed in the proof of Lemma 5.2.3. Then $h \in H \cap xHx^{-1}$ and therefore $z = [\lambda^{-1}(h), \lambda^{-1}(x)] \in \Phi^{\overline{G}}(\overline{H})$, as desired.

(ii) By the isomorphism (1.5.2) of Theorem 1.5.12, the statement in (i) implies that the map $f_{L/K}$ in diagram (4.3.1) is trivial. As this diagram is commutative, it follows that $g_{L/K}$ is also trivial and thus $\mathfrak{K}(K/k) = Ш(T) = \mathrm{Coker}(g_{L/K}) = \mathfrak{F}(L/K/k)$. □

Now that we have proved Theorem 5.1.1, we have reduced the study of the HNP and weak approximation for norm one tori of A_n and S_n extensions to a purely computational problem (except in the cases of A_6 and A_7). The groups $\mathfrak{F}(L/K/k)$ and $\mathfrak{K}(L/k)$ can be computed using the GAP algorithms described in Remark 4.3.9 and Section 4.4. The calculations of the knot group and of $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ in the remaining cases where $G \cong A_6, A_7$ are done in Section 5.3.

Remark 5.2.5. The method employed in this section to provide explicit and computable formulas for the knot group and the invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$ in A_n and S_n extensions works for other families of extensions. For example, let G' be any finite group such that $\mathrm{H}^3(G', \mathbb{Z}) = \mathbb{Z}/2$. Embed G' into S_n for some n and suppose that G' contains a copy of V_4 conjugate to $\langle(1,2)(3,4),(1,3)(2,4)\rangle$. For such a group G', analogues of Lemma 5.2.3 and Propositions 5.2.1 and 5.2.4 yield a systematic approach to the study of the HNP and weak approximation for G'-extensions.

We proceed by investigating the possible isomorphism classes of the finite abelian group $\mathfrak{F}(G, H)$ (and thus, by Theorems 4.1.2, 5.1.1 and isomorphism (1.5.2), of the invariant $\mathrm{H}^1(G, F_{G/H})$ as well).

Proposition 5.2.6. *The group $\mathfrak{F}(S_n, H)$ is an elementary abelian 2-group. Moreover, every elementary abelian 2-group occurs as $\mathfrak{F}(S_n, H)$ for some n and some $H \leq S_n$.*

Proof. It suffices to prove that for every element $h \in H \cap [S_n, S_n]$, we have $h^2 \in \Phi^{S_n}(H)$. This is clear from the definition of $\Phi^{S_n}(H)$ because h is conjugate to its inverse in S_n. The statement on the occurrence of every elementary abelian 2-group is shown in Proposition 5.2.8 below. □

Proposition 5.2.7. *The group $\mathfrak{F}(A_n, H)$ is either isomorphic to C_3 or an elementary abelian 2-group. Moreover, every such possibility is realised for some choice of n and H.*

Proof. First, we claim that any element of even order in $\mathfrak{F}(A_n, H)$ is 2-torsion. Let $h \in H$ have even order. By [37], h is A_n-conjugate to h^{-1}. Therefore $h^2 \in \Phi^{A_n}(H)$, which proves the claim.

Next, we claim that any element of odd order in $\mathfrak{F}(A_n, H)$ is 3-torsion. Let $h \in H$ be such that its image in $\mathfrak{F}(A_n, H)$ has odd order. Replacing h by a suitable power, we may assume that h itself has odd order, whereby h is S_n-conjugate to h^2. By the pigeonhole principle, at least two of the three S_n-conjugate elements h, h^{-1}, h^2 are A_n-conjugate. Therefore, at least one of h^{-2}, h, h^3 is in $\Phi^{A_n}(H)$. Since h has odd order, we conclude that in all cases $h^3 \in \Phi^{A_n}(H)$, whence the claim.

Next, we show that $\mathfrak{F}(A_n, H)_{(3)}$ is cyclic. Suppose for contradiction that the images in $\mathfrak{F}(A_n, H)$ of $h_1, h_2 \in H$ generate a copy of $C_3 \times C_3$. Replacing h_1 and h_2 by suitable powers if necessary, we may assume that the lengths of the cycles making up h_1 and h_2 are powers of 3, say $3^{r_1} \leq 3^{r_2} \leq \cdots \leq 3^{r_k}$ for h_1 and $3^{s_1} \leq 3^{s_2} \leq \cdots \leq 3^{s_l}$ for h_2, where $k, l \geq 1$ and $r_i, s_j \in \mathbb{Z}_{\geq 0}$. Note that h_1 and h_1^{-1} cannot be A_n-conjugate, or else we would have $h_1^2 \in \Phi^{A_n}(H)$, and similarly for h_2. The criterion [37] for an element of A_n to be conjugate to its inverse yields $3^{r_i} \neq 3^{r_j}$ and $3^{s_i} \neq 3^{s_j}$ for $i \neq j$. Since $n = \sum_{i=1}^{k} 3^{r_i} = \sum_{i=1}^{l} 3^{s_i}$, the uniqueness of the representation of n in base 3 implies that $k = l$ and $r_i = s_i$ for every i. Thus the cycle structures of h_1 and h_2 are identical and hence h_1, h_2 and h_2^2 are conjugate in S_n. Therefore, at least two of these elements are A_n-conjugate, whereby at least one of $h_1^{-1}h_2, h_1^{-1}h_2^2, h_2$ is in $\Phi^{A_n}(H)$. This contradicts the assumption that the images of h_1 and h_2 generate a non-cyclic subgroup of $\mathfrak{F}(A_n, H)$. One can compute that $\mathfrak{F}(A_{12}, H) \cong C_3$ for $H = \langle(1, 2, 3)(4, 5, 6, 7, 8, 9, 10, 11, 12)\rangle$ using GAP, for example. The statement on the occurrence of every elementary abelian 2-group is shown in Proposition 5.2.8 below. □

Proposition 5.2.8. *For every $k \geq 0$, there exist n and a subgroup H of A_n such that*

$$\mathfrak{F}(A_n, H)_{(2)} \cong \mathfrak{F}(S_n, H)_{(2)} \cong C_2^k.$$

Proof. The case $k = 0$ is realised by letting $H = 1$. From now on, assume that $k \geq 1$. Let H be generated by k commuting and even permutations of order 2 such that, for any $x, y \in H$ with $x \neq y$, the permutations x and y have distinct cycle structures. We define such a group recursively as $H = H_k$, starting from $H_1 = \langle(1, 2)(3, 4)\rangle$, $H_2 = \langle(1, 2)(3, 4),(5, 6)(7, 8)(9, 10)(11, 12)\rangle$ and adding, at step i, a new generator h_i such that:

- h_i is an even permutation of order 2;
- h_i is disjoint to the previous generators $h_1, \dots, h_{i-1}$;
- h_i moves enough points so that its product with any element of H_{i-1} has cycle structure different from that of any element of H_{i-1}.

Let n be large enough so that $H \subset A_n$. It is straightforward to check that one then has $\Phi^{A_n}(H) = \Phi^{S_n}(H) = 1$. Therefore, $\mathfrak{F}(A_n, H) = H \cap [A_n, A_n] = H \cong C_2^k$ and similarly for $\mathfrak{F}(S_n, H)$. □

As a consequence of the work done so far, we can now establish Theorem 5.1.3 and Corollary 5.1.5.

Proof of Theorem 5.1.3. For $G \ncong A_6$ or A_7 the results follow from Theorems 4.1.2 and 5.1.1 and Propositions 5.2.6 and 5.2.7. For the A_6 and A_7 cases, we describe how to compute $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ in Section 5.3 – the results of these computations are in Tables 5 and 6 of the Appendix 5.4 and the C_3 and C_6 cases occur therein. □

Proof of Corollary 5.1.5. Theorem 5.1.3 shows that $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})_{(p)} = 0$ for a prime $p > 3$ and that $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})_{(3)} = 0$ if $G \cong S_n$. Theorem 4.1.2 gives $\mathfrak{F}_{nr}(L/K/k) = \mathfrak{F}(G, H)$. By Theorem 5.1.3, $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim}_{(3)}$ is 3-torsion, so Theorem 5.1.1 gives $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim}_{(3)} = \mathfrak{F}(G, H)[3]$. Let $K_3 = L^{H_3}$ and let X_3 be a smooth compactification of $R^1_{K_3/k}\mathbb{G}_m$. Now Corollary 4.2.6 and Theorem 5.1.1 give $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim}_{(3)} \cong \mathrm{H}^1(k, \operatorname{Pic} \overline{X_3})^{\sim}_{(3)} = \mathfrak{F}(G, H_3)$. If $|H|$ is odd then $\mathfrak{F}(G, H)_{(2)}$ is trivial and hence $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim}_{(2)} = \mathbb{Z}/2$ by Theorem 5.1.1. The result for $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim}_{(2)}$ when $|H|$ is even is obtained in a similar way to the result for the 3-primary part. □

The following corollary of Theorem 5.1.3 and Corollary 4.2.6 gives a useful shortcut when analyzing the HNP and weak approximation for S_n extensions, enabling one to reduce to the case where H is a 2-group.

Corollary 5.2.9. *Suppose that $G \cong S_n$, let H_2 be a Sylow 2-subgroup of H and let K_2 denote its fixed field. Let X_2 be a smooth compactification of $T_2 = R^1_{K_2/k}\mathbb{G}_m$. Then we obtain a commutative diagram with exact rows as follows, where the vertical isomorphisms are induced by the natural inclusion $T \hookrightarrow T_2$:*

$$\begin{tikzcd}
0 \arrow[r] & A(T) \arrow[r] \arrow[d, "\cong"'] & \mathrm{H}^1(k, \operatorname{Pic} \overline{X})^{\sim} \arrow[r] \arrow[d, "\cong"'] & Ш(T) \arrow[r] \arrow[d, "\cong"'] & 0 \\
0 \arrow[r] & A(T_2) \arrow[r] & \mathrm{H}^1(k, \operatorname{Pic} \overline{X_2})^{\sim} \arrow[r] & Ш(T_2) \arrow[r] & 0.
\end{tikzcd}$$

Alternatively, the norm map $N_{K_2/K} : T_2 \twoheadrightarrow T$ can be used to obtain a similar commutative diagram with the direction of the vertical isomorphisms reversed.

Remark 5.2.10. Corollary 5.2.9 also holds in the case $G \cong A_n$ provided $n \neq 6, 7$ and $\mathfrak{F}(G, H)_{(3)} = 1$. In Proposition 5.2.12 we show that for most n we have $\mathfrak{F}(A_n, H)_{(3)} = 1$ for all subgroups H.

The next lemma will aid our characterization of the existence of elements of order 3 in $\mathfrak{F}(A_n, H)$.

Lemma 5.2.11. *Let $n = 3^l$ for some $l \geq 0$ and let $\rho = (a_1 \cdots a_{3^l})$ be a 3^l-cycle in S_n. Let $j \in \mathbb{Z}$ with $j \equiv -1 \pmod 3$. Then ρ^j is A_n-conjugate to ρ if and only if l is even.*

Proof. Observe that $\rho^j(a_i) = a_{i+j}$, where the subscripts are considered modulo 3^l. Therefore, the permutation $x \in S_n$ defined by $x(a_i) = a_{1+(i-1)j}$ satisfies $x\rho x^{-1} = \rho^j$. Let C be the A_n-conjugacy class of ρ. Since the S_n-conjugacy class of ρ splits as a disjoint union $C \sqcup gCg^{-1}$ for any $g \in S_n \setminus A_n$, it is enough to show that $x \in A_n$ if and only if l is even. We study the cycle structure of x by analyzing the fixed points of its powers. Observe that $x^t(a_i) = a_{1+(i-1)j^t}$ for every $t \geq 0$ and so

$$x^t(a_i) = a_i \Leftrightarrow 1 + (i-1)j^t \equiv i \pmod{3^l} \Leftrightarrow (i-1)(j^t - 1) \equiv 0 \pmod{3^l}.$$

Therefore, the number of fixed points of x^t is $\gcd(3^l, j^t - 1)$. Using this fact, we note two useful properties of the cycles occurring in a disjoint cycle decomposition of x:

(i) **The only cycle of $\boldsymbol{x}$ with odd length corresponds to the fixed point $\boldsymbol{a_1}$:** It suffices to show that, for odd $t \geq 1$, the only fixed point of x^t is a_1. As $j \equiv -1 \pmod 3$, it is easy to see that $j^t - 1 \not\equiv 0 \pmod 3$ for odd t and thus $\gcd(3^l, j^t - 1) = 1$.

(ii) **$\boldsymbol{x}$ does not contain a cycle with length divisible by 4:** It is enough to prove that, for any $m \geq 1$, the number of fixed points of x^{4m} and x^{2m} coincide, i.e. that $\gcd(3^l, j^{4m} - 1) = \gcd(3^l, j^{2m} - 1)$. This is clear since $j^{4m} - 1 = (j^{2m} - 1)(j^{2m} + 1)$ and $j^{2m} + 1 \not\equiv 0 \pmod 3$.

Let $c_1 \cdot \ldots \cdot c_k$ be a disjoint cycle decomposition of x where the cycle c_i has length $|c_i|$. By (i) and (ii), we may assume that $|c_1| = 1$ and $|c_i| \equiv 2 \pmod 4$ for all $i \geq 2$. Note that $x \in A_n$ if and only if k is odd. Now $3^l = \sum_i |c_i| \equiv 1 + \sum\limits_{i \geq 2} 2 \pmod 4$. Thus, $x \in A_n$ if and only if $3^l \equiv 1 \pmod 4$. □

Proposition 5.2.12. *There exists $H \leq A_n$ such that $\mathfrak{F}(A_n, H)_{(3)} \cong C_3$ if and only if $n \geq 5$ and $n = \sum\limits_{i=1}^{k} 3^{r_i}$ with $0 \leq r_1 < \cdots < r_k$ and $|\{i \mid r_i \text{ is odd}\}|$ is odd.*

Proof. Suppose that $\mathfrak{F}(A_n, H)_{(3)} \cong C_3$. It is easy to check that $\mathfrak{F}(A_4, H)_{(3)} = 1$ for all $H \leq A_4$ so $n \geq 5$. Let h be an element of H such that its image in $\mathfrak{F}(A_n, H)$ generates $\mathfrak{F}(A_n, H)_{(3)}$. Replacing h by a suitable power if necessary, we may assume that the lengths of the cycles making up h are powers of 3, say $3^{r_1} \leq 3^{r_2} \leq \cdots \leq 3^{r_k}$ with $r_i \in \mathbb{Z}_{\geq 0}$. If h were A_n-conjugate to h^{-1} then we would obtain $h \in \Phi^{A_n}(H)$, a contradiction. Therefore, by criterion [37] we have $3^{r_i} \neq 3^{r_j}$ for $i \neq j$ and $\sum\limits_{i=1}^{k} \frac{3^{r_i} - 1}{2}$ is odd, i.e. the number of odd r_i is odd.

Conversely, assume that $n \geq 5$ is equal to $\sum\limits_{i=1}^{k} 3^{r_i}$ with $r_1 < r_2 < \cdots < r_k$ and $|\{i \mid r_i \text{ is odd}\}|$ odd and let H be the cyclic group of order 3^{r_k} generated by h, where

$$h = \underbrace{(1 \ \cdots \ 3^{r_1})}_{c_1} \underbrace{(3^{r_1}+1 \ \cdots \ 3^{r_1}+3^{r_2})}_{c_2} \dots \underbrace{(\sum_{i=1}^{k-1} 3^{r_i}+1 \ \cdots \ n)}_{c_k}.$$

We will prove that $\mathfrak{F}(A_n, H)_{(3)} \cong C_3$. By Proposition 5.2.7, it is enough to show that $h \notin \Phi^{A_n}(H)$. Observe that $\Phi^{A_n}(H)$ is generated by elements of the form h^{s-t} where h^s is A_n-conjugate to h^t. We complete the proof by showing that $\Phi^{A_n}(H) \subset \langle h^3 \rangle$. Suppose that h^s is A_n-conjugate to h^t. We claim that $s \equiv t \pmod 3$. Since conjugate elements have the same order, $3 \mid s$ if and only if $3 \mid t$. Now assume that $3 \nmid s$. Then h^s generates H and has the same cycle type as h so, relabelling if necessary, we may assume that $s = 1$. Suppose for contradiction that $t \equiv -1 \pmod 3$. For every $1 \leq i \leq k$, let $x_i \in S_n$ be such that x_i only moves points appearing in c_i and $x_i c_i x_i^{-1} = c_i^t$. Then $x = x_1 \cdot \ldots \cdot x_k$ satisfies $xhx^{-1} = h^t$. Lemma 5.2.11 shows that $x_i \in A_n$ if and only if r_i is even. Since $|\{i \mid r_i \text{ is odd}\}|$ is odd, $x \in S_n \setminus A_n$. This gives the desired contradiction as the S_n-conjugacy class of h splits as a disjoint union $C \sqcup xCx^{-1}$ where C denotes the A_n-conjugacy class of h. □

5.3 Explicit results for small values of n

In this section we prove all the results presented in Section 5.1 on the obstructions to the HNP and weak approximation for norm one tori of A_n and S_n-extensions for small values of n.

We start by establishing Propositions 5.1.7 and 5.1.8. Using Hoshi and Yamasaki's method (Algorithm A1, Appendix 4.5) and Drakokhrust's formula (Algorithm A2, Appendix 4.5), we can compute the groups $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ where X is a smooth compactification of the norm one torus $R^1_{K/k}\mathbb{G}_m$ and K/k is contained in a Galois extension L/k with $\mathrm{Gal}(L/k) = G \cong S_4, S_5, A_4, A_5, A_6, A_7$. We remark that our calculations were further simplified thanks to the formulas in Theorem 5.1.1. The outcome of our computations appears in Tables 1 – 6 of the Appendix 5.4 and Proposition 5.1.8 follows immediately.

We now prove Proposition 5.1.7. We use Theorem 5.1.1 to reduce our task to the calculation of the first obstruction $\mathfrak{F}(L/K/k)$ and the knot group $\mathfrak{K}(L/k)$ for the Galois extension L/k. The former is achieved using the algorithm described in Remark 4.3.9 and presented as Algorithm A4 in the Appendix 4.5. The computation of $\mathfrak{K}(L/k)$ follows from a simple application of isomorphism (1.6.5) of Theorem 1.6.9 together with Lemma 1.1.4 and Lemma 5.3.1 below. Note that if $G = A_4, S_4, A_5$ or S_5 then $\mathrm{H}^3(G, \mathbb{Z}) \cong \mathbb{Z}/2$.

Lemma 5.3.1. *Let $G = A_4, S_4, A_5, S_5, A_6$ or A_7 and let A be a copy of V_4 inside G. Then*

$$\mathrm{Res}^G_A : \mathrm{H}^3(G, \mathbb{Z})_{(2)} \to \mathrm{H}^3(A, \mathbb{Z})$$

is an isomorphism.

Proof. Let G_2 be a Sylow 2-subgroup of G containing A. First, we claim that the restriction map $\mathrm{Res}^G_{G_2} : \mathrm{H}^3(G, \mathbb{Z})_{(2)} \to \mathrm{H}^3(G_2, \mathbb{Z})$ is an isomorphism. To see this, recall that $\mathrm{Cor}^G_{G_2} \circ \mathrm{Res}^G_{G_2}$ is multiplication by $[G : G_2]$ by Lemma 1.1.3. Moreover, as $G_2 \cong V_4$ or $G_2 \cong D_4$, we have $\mathrm{H}^3(G, \mathbb{Z})_{(2)} \cong \mathrm{H}^3(G_2, \mathbb{Z}) \cong \mathbb{Z}/2$. Hence, multiplication by the odd integer $[G : G_2]$ is an isomorphism and thus so is $\mathrm{Res}^G_{G_2}$. If $G_2 = A$, we are done. The other possibility is $G_2 \cong D_4$. In this case, an easy exercise using dimension shifting and the Hochschild–Serre spectral sequence $E_2^{i,j} = \mathrm{H}^i(G_2/A, \mathrm{H}^j(A, \mathbb{Q}/\mathbb{Z})) \implies \mathrm{H}^{i+j}(G_2, \mathbb{Q}/\mathbb{Z})$ shows that $\mathrm{Res}^{G_2}_A : \mathrm{H}^3(G_2, \mathbb{Z}) \to \mathrm{H}^3(A, \mathbb{Z})$ is injective and hence an isomorphism as $\mathrm{H}^3(G_2, \mathbb{Z}) \cong \mathbb{Z}/2 \cong \mathrm{H}^3(A, \mathbb{Z})$. □

We now move on to the proving Propositions 5.1.9 and 5.1.10 as well as giving a complete characterization of weak approximation for the norm one tori associated with A_6 and A_7 extensions, see Proposition 5.3.6 below. Various subgroups of A_6 and A_7 are given by semidirect products of smaller subgroups. For brevity, we omit the precise construction of these semidirect products from the main text and refer the reader to Tables 5 and 6 of the Appendix 5.4 containing the generators of these subgroups. We start by settling the Galois case of Proposition 5.1.9.

Proposition 5.3.2. *If L/k is Galois with Galois group A_6 or A_7, then $\mathfrak{K}(L/k) \hookrightarrow C_6$ and*

- $\mathfrak{K}(L/k)_{(2)} = 1$ *if and only if there exists a place v of k such that $V_4 \hookrightarrow D_v$;*
- $\mathfrak{K}(L/k)_{(3)} = 1$ *if and only if there exists a place v of k such that $C_3 \times C_3 \hookrightarrow D_v$.*

Proof. This follows from isomorphism (1.6.5) of Theorem 1.6.9 and Lemmas 1.1.4 and 5.3.1. □

We now solve the non-Galois case. Once again, we compute the invariant $\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) = \mathrm{H}^1(G, F_{G/H})$ for every possibility of $H = \operatorname{Gal}(L/K)$ by using the methods detailed in Section 4.4. The result of this computation is given in Tables 5 and 6 of the Appendix 5.4 and proves Proposition 5.1.10. Building upon the outcome of this computation, we establish multiple results on the knot group $\mathfrak{K}(K/k)$. Looking at Tables 5 and 6, we immediately see that the invariant $\mathrm{H}^1(G, F_{G/H})$ is trivial if H is isomorphic to A_4, $C_2 \times C_6$, D_6, $(C_6 \times C_2) \rtimes C_2$, S_4, $A_4 \times C_3$, A_5, $(A_4 \times C_3) \rtimes C_2$, S_5, $\mathrm{PSL}(3, 2)$ or A_6. Thus, by Theorems 1.5.8 and 1.5.12, both groups $A(T)$ and $\mathfrak{K}(K/k)$ are trivial in all these cases.

Next, we investigate the cases where the first obstruction to the HNP for the tower $L/K/k$ coincides with the total obstruction (the knot group).

Proposition 5.3.3. *If 6 divides $|H|$, then $\mathfrak{K}(K/k) = \mathfrak{F}(L/K/k)$.*

Proof. Let G_1 be a copy of V_4 inside G such that $H \cap G_1 \neq 1$ and G_2 a copy of $C_3 \times C_3$ inside G such that $H \cap G_2 \neq 1$. Set $H_i = H \cap G_i$ for $i = 1, 2$ and notice that the HNP holds for the extensions L^{H_i}/L^{G_i} as they are of degree at most 3. Using Lemmas 1.1.4, 5.3.1 and the duality Lemmas 1.2.3 and 1.2.6, we find that the maps $\operatorname{Cor}^G_{G_1} : \hat{\mathrm{H}}^{-3}(G_1, \mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G, \mathbb{Z})_{(2)}$ and $\operatorname{Cor}^G_{G_2} : \hat{\mathrm{H}}^{-3}(G_2, \mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G, \mathbb{Z})_{(3)}$ are surjective. Hence

$$\operatorname{Cor}^G_{G_1} \oplus \operatorname{Cor}^G_{G_2} : \hat{\mathrm{H}}^{-3}(G_1, \mathbb{Z}) \oplus \hat{\mathrm{H}}^{-3}(G_2, \mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G, \mathbb{Z})$$

is surjective (recall that $\hat{\mathrm{H}}^{-3}(G, \mathbb{Z}) \cong \mathbb{Z}/6$) and therefore $\mathfrak{F}(L/K/k) = \mathfrak{K}(K/k)$ by Theorem 4.3.2. □

As a consequence of this result, one can use the GAP function `1obs` described in Remark 4.3.9 to computationally solve the cases where $6 \mid |H|$ and $\mathrm{H}^1(G, F_{G/H}) \neq 0$. The remaining possibilities for H are dealt with in the two following results.

Proposition 5.3.4. *(i) If $H \cong V_4$ or D_4, then $\mathfrak{K}(K/k) \cong \mathfrak{K}(L/k)_{(3)}$;*

(ii) If $H \cong C_5$ or C_7, then $\mathfrak{K}(K/k) \cong \mathfrak{K}(L/k)$;

(iii) If $H \cong C_3, C_3 \times C_3$ or $C_7 \rtimes C_3$, then $\mathfrak{K}(K/k) \cong \mathfrak{K}(L/k)_{(2)}$.

Proof. We prove only (i) ((ii) and (iii) follow analogously). In this case $\mathrm{H}^1(G, F_{G/H}) = \mathbb{Z}/3$ (see Tables 5 and 6 of the Appendix 5.4) and thus $\mathbb{Z}/3 \twoheadrightarrow \mathfrak{K}(K/k)$ by Theorem 1.5.8 and isomorphism (1.5.2). The result now follows by Theorem 4.1.1, noting that $d = [L : K] = 4$ or 8 is coprime to 3. □

Proposition 5.3.5. *(i) If $H \cong C_2$ or D_5, then $\mathfrak{K}(K/k) \cong \mathfrak{K}(L/k)$;*

(ii) If $H \cong C_4$ or $C_5 \rtimes C_4$, then

$$\mathfrak{K}(K/k) \cong \mathfrak{K}(L/k)_{(3)} \times \mathfrak{K}(M/k) \cong \mathfrak{K}(L/k)_{(3)} \times \mathfrak{F}(L/M/k),$$

where M is the fixed field of a copy of $(C_3 \times C_3) \rtimes C_4$ inside G containing $H_2 \cong C_4$.

Proof. First, note that in all cases $\mathfrak{K}(K/k)_{(3)} \cong \mathfrak{K}(L/k)_{(3)}$, by Theorem 4.1.1. By Proposition 5.1.10 and Theorem 1.5.8, it only remains to compute $\mathfrak{K}(K/k)_{(2)}$. For case (i), let A be a copy of S_3 inside G such that $A \cap H = H_2 \cong C_2$ and let $F = L^A$ and $K_2 = L^{H_2}$. Now Theorem 4.1.1 shows that $\mathfrak{K}(K/k)_{(2)} \cong \mathfrak{K}(K_2/k)_{(2)} \cong \mathfrak{K}(F/k)_{(2)}$. Computing $\mathfrak{K}(F/k)_{(2)}$ using Proposition 5.3.3 and the GAP function `1obs` described in Remark 4.3.9 gives $\mathfrak{K}(F/k)_{(2)} \cong \mathfrak{K}(L/k)_{(2)}$, as required. For case (ii), again let $K_2 = L^{H_2}$. Then $\mathfrak{K}(K/k)_{(2)} \cong \mathfrak{K}(K_2/k)_{(2)} \cong \mathfrak{K}(M/k)_{(2)}$, by Theorem 4.1.1. Now Proposition 5.3.3 gives $\mathfrak{K}(M/k) \cong \mathfrak{F}(L/M/k)$. Furthermore, Theorem 1.5.8 and isomorphism (1.5.2) combined with the results for $(C_3 \times C_3) \rtimes C_4$ in Tables 5 and 6 of the Appendix 5.4 show that $\mathfrak{K}(M/k)$ is 2-torsion. □

We have thus completely proved the characterization of the HNP for an A_6 or A_7 extension given in Proposition 5.1.9. Using Proposition 5.1.10, we can also give a full description of weak approximation. The local conditions controlling the validity of this principle are given in detail in the next result; they are a direct consequence of Propositions 5.1.9 and 5.1.10 and Voskresenskiĭ's exact sequence (1.5.1) of Theorem 1.5.8.

Proposition 5.3.6. *Let K/k be an extension of number fields contained in a Galois extension L/k such that $G = \mathrm{Gal}(L/k) \cong A_6$ or A_7. Let $H = \mathrm{Gal}(L/K)$ and $T = R^1_{K/k}\mathbb{G}_m$.*

- *If $V_4 \hookrightarrow H$ and $C_3 \hookrightarrow H$, then weak approximation holds for T.*
- *If $H \cong 1, C_2, C_5, C_7$ or D_5, then weak approximation holds for T if and only if $V_4 \not\hookrightarrow D_v$ and $C_3 \times C_3 \not\hookrightarrow D_v$ for every place v of k.*
- *If $H \cong C_4$ or $C_5 \rtimes C_4$, then weak approximation holds for T if and only if $D_4 \not\hookrightarrow D_v$ and $C_3 \times C_3 \not\hookrightarrow D_v$ for every place v of k.*
- *In all other cases, weak approximation holds for T if and only if the HNP fails for K/k.*

5.4 Appendix: Computation of $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ for small values of n

We present the results of the computer calculations outlined in Section 5.3. In the following tables, we distinguish non-conjugate but isomorphic groups with a letter in front of the isomorphism class.

Table 1

$\boldsymbol{G = A_4}$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
12	1	$\mathbb{Z}/2$
6	$C_2 = \langle(1,2)(3,4)\rangle$	$\mathbb{Z}/2$
4	$C_3 = \langle(1,2,3)\rangle$	$\mathbb{Z}/2$
3	$V_4 = \langle(1,2)(3,4),(1,3)(2,4)\rangle$	0

Table 2

$\boldsymbol{G = S_4}$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
24	1	$\mathbb{Z}/2$
12	$C_2a = \langle(1,2)\rangle$	0
12	$C_2b = \langle(1,2)(3,4)\rangle$	$\mathbb{Z}/2$
8	$C_3 = \langle(1,2,3)\rangle$	$\mathbb{Z}/2$
6	$C_4 = \langle(1,2,3,4)\rangle$	0
6	$V_4 = \langle(1,2),(3,4)\rangle$	0
6	$V_4 = \langle(1,2)(3,4),(1,3)(2,4)\rangle$	0
4	$S_3 = \langle(1,2,3),(1,2)\rangle$	0
3	$D_4 = \langle(1,2,3,4),(1,3)\rangle$	0
2	$A_4 = \langle(1,2)(3,4),(1,2,3)\rangle$	0

Table 3

$\boldsymbol{G = A_5}$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
60	1	$\mathbb{Z}/2$
30	$C_2 = \langle (1,2)(3,4) \rangle$	$\mathbb{Z}/2$
20	$C_3 = \langle (1,2,3) \rangle$	$\mathbb{Z}/2$
15	$V_4 = \langle (1,2)(3,4), (1,3)(2,4) \rangle$	0
12	$C_5 = \langle (1,2,3,4,5) \rangle$	$\mathbb{Z}/2$
10	$S_3 = \langle (1,2,3), (1,2)(4,5) \rangle$	$\mathbb{Z}/2$
6	$D_5 = \langle (1,2,3,4,5), (2,5)(3,4) \rangle$	$\mathbb{Z}/2$
5	$A_4 = \langle (1,2)(3,4), (1,2,3) \rangle$	0

Table 4

$\boldsymbol{G = S_5}$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
120	1	$\mathbb{Z}/2$
60	$C_2a = \langle (1,2) \rangle$	0
60	$C_2b = \langle (1,2)(3,4) \rangle$	$\mathbb{Z}/2$
40	$C_3 = \langle (1,2,3) \rangle$	$\mathbb{Z}/2$
30	$C_4 = \langle (1,2,3,4) \rangle$	0
30	$V_4a = \langle (1,2), (3,4) \rangle$	0
30	$V_4b = \langle (1,2)(3,4), (1,3)(2,4) \rangle$	0
24	$C_5 = \langle (1,2,3,4,5) \rangle$	$\mathbb{Z}/2$
20	$C_6 = \langle (1,2,3), (4,5) \rangle$	0
20	$S_3a = \langle (1,2,3), (1,2) \rangle$	0
20	$S_3b = \langle (1,2,3), (1,2)(4,5) \rangle$	$\mathbb{Z}/2$
15	$D_4 = \langle (1,2,3,4), (1,3) \rangle$	0
12	$D_5 = \langle (1,2,3,4,5), (2,5)(3,4) \rangle$	$\mathbb{Z}/2$
10	$A_4 = \langle (1,2)(3,4), (1,2,3) \rangle$	0
10	$S_3 \times C_2 = \langle (1,2,3), (1,2), (4,5) \rangle$	0
6	$C_5 \rtimes C_4 = \langle (1,2,3,4,5), (2,3,5,4) \rangle$	0
5	$S_4 = \langle (1,2,3,4), (1,2) \rangle$	0
2	$A_5 = \langle (1,2,3,4,5), (1,2,3) \rangle$	0

Table 5

$\boldsymbol{G = A_6}$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
360	1	$\mathbb{Z}/6$
180	$C_2 = \langle(1,2)(3,4)\rangle$	$\mathbb{Z}/6$
120	$C_3 = \langle(1,2,3)\rangle$	$\mathbb{Z}/2$
120	$C_3 = \langle(1,2,3)(4,5,6)\rangle$	$\mathbb{Z}/2$
90	$C_4 = \langle(1,2,3,4)(5,6)\rangle$	$\mathbb{Z}/6$
90	$V_4a = \langle(1,2)(3,4),(1,3)(2,4)\rangle$	$\mathbb{Z}/3$
90	$V_4b = \langle(1,2)(5,6),(1,2)(3,4)\rangle$	$\mathbb{Z}/3$
72	$C_5 = \langle(1,2,3,4,5)\rangle$	$\mathbb{Z}/6$
60	$S_3a = \langle(1,2,3)(4,5,6),(1,2)(4,5)\rangle$	$\mathbb{Z}/2$
60	$S_3b = \langle(1,2,3),(1,2)(4,5)\rangle$	$\mathbb{Z}/2$
45	$D_4 = \langle(1,2,3,4)(5,6),(1,3)(5,6)\rangle$	$\mathbb{Z}/3$
40	$C_3 \times C_3 = \langle(1,2,3),(4,5,6)\rangle$	$\mathbb{Z}/2$
36	$D_5 = \langle(1,2,3,4,5),(2,5)(3,4)\rangle$	$\mathbb{Z}/6$
30	$A_4a = \langle(1,2)(3,4),(1,2,3)\rangle$	0
30	$A_4b = \langle(1,2,3)(4,5,6),(1,4)(2,5)\rangle$	0
20	$(C_3 \times C_3) \rtimes C_2 = \langle(1,2,3),(4,5,6),(1,2)(4,5)\rangle$	$\mathbb{Z}/2$
15	$S_4a = \langle(1,2,3,4)(5,6),(1,2)(5,6)\rangle$	0
15	$S_4b = \langle(1,3,5)(2,4,6),(1,6)(2,5)\rangle$	0
10	$(C_3 \times C_3) \rtimes C_4 = \langle(1,2,3),(4,5,6),(1,4)(2,5,3,6)\rangle$	$\mathbb{Z}/2$
6	$A_5a = \langle(1,2,3,4,5),(1,2,3)\rangle$	0
6	$A_5b = \langle(1,2,3,4,5),(1,4)(5,6)\rangle$	0

Table 6

$\boldsymbol{G = A_7}$		
$[K : k]$	H	$\mathrm{H}^1(G, F_{G/H})$
2520	1	$\mathbb{Z}/6$
1260	$C_2 = \langle (1,2)(3,4) \rangle$	$\mathbb{Z}/6$
840	$C_3a = \langle (1,2,3) \rangle$	$\mathbb{Z}/2$
840	$C_3b = \langle (1,2,3)(4,5,6) \rangle$	$\mathbb{Z}/2$
630	$C_4 = \langle (1,2,3,4)(5,6) \rangle$	$\mathbb{Z}/6$
630	$V_4a = \langle (1,2)(3,4), (1,3)(2,4) \rangle$	$\mathbb{Z}/3$
630	$V_4b = \langle (1,2)(5,6), (1,2)(3,4) \rangle$	$\mathbb{Z}/3$
504	$C_5 = \langle (1,2,3,4,5) \rangle$	$\mathbb{Z}/6$
420	$C_6 = \langle (1,2)(3,4)(5,6,7) \rangle$	$\mathbb{Z}/2$
420	$S_3a = \langle (1,2,3)(4,5,6), (1,2)(4,5) \rangle$	$\mathbb{Z}/2$
420	$S_3b = \langle (1,2,3), (1,2)(4,5) \rangle$	$\mathbb{Z}/2$
360	$C_7 = \langle (1,2,3,4,5,6,7) \rangle$	$\mathbb{Z}/6$
315	$D_4 = \langle (1,2,3,4)(5,6), (1,3)(5,6) \rangle$	$\mathbb{Z}/3$
280	$C_3 \times C_3 = \langle (1,2,3), (4,5,6) \rangle$	$\mathbb{Z}/2$
252	$D_5 = \langle (1,2,3,4,5), (2,5)(3,4) \rangle$	$\mathbb{Z}/6$
210	$A_4a = \langle (1,2)(3,4), (1,2,3) \rangle$	0
210	$A_4b = \langle (1,2,3)(4,5,6), (1,4)(2,5) \rangle$	0
210	$A_4c = \langle (1,5,3)(4,7,6), (2,6)(4,7) \rangle$	0
210	$A_4d = \langle (1,2,5)(4,6,7), (3,4)(6,7) \rangle$	0
210	$C_2 \times C_6 = \langle (1,2)(3,5)(4,6,7), (1,3)(2,5) \rangle$	0
210	$D_6 = \langle (1,2)(3,5)(4,6,7), (1,2)(6,7) \rangle$	0
210	$C_3 \rtimes C_4 = \langle (2,3,6), (1,4,7,5)(3,6) \rangle$	$\mathbb{Z}/2$
140	$(C_3 \times C_3) \rtimes C_2 = \langle (1,2,3), (4,5,6), (1,2)(4,5) \rangle$	$\mathbb{Z}/2$
126	$C_5 \rtimes C_4 = \langle (1,2)(4,5,7,6), (3,6,7,4,5) \rangle$	$\mathbb{Z}/6$
120	$C_7 \rtimes C_3 = \langle (1,7,4,2,6,5,3), (2,3,5)(4,6,7) \rangle$	$\mathbb{Z}/2$
105	$(C_6 \times C_2) \rtimes C_2 = \langle (1,2)(3,5)(4,6,7), (1,3)(2,5), (1,2)(6,7) \rangle$	0
105	$S_4a = \langle (1,2,3,4)(5,6), (1,2)(5,6) \rangle$	0
105	$S_4b = \langle (1,3,5)(2,4,6), (1,6)(2,5) \rangle$	0
105	$S_4c = \langle (1,2,3)(5,6,7), (2,3)(4,5,6,7) \rangle$	0
105	$S_4d = \langle (1,3,2)(5,6,7), (2,3)(4,5,6,7) \rangle$	0
70	$A_4 \times C_3 = \langle (1,3,5)(4,6,7), (1,2,3) \rangle$	0
70	$(C_3 \times C_3) \rtimes C_4 = \langle (1,2,3), (4,5,6), (1,4)(2,5,3,6) \rangle$	$\mathbb{Z}/2$
42	$A_5a = \langle (1,2,3,4,5), (1,2,3) \rangle$	0
42	$A_5b = \langle (1,2,3,4,5), (1,4)(5,6) \rangle$	0
35	$(A_4 \times C_3) \rtimes C_2 = \langle (2,3)(5,7), (1,2)(4,5,6,7), (2,3)(5,6) \rangle$	0
21	$S_5 = \langle (1,2)(3,7), (2,6,5,4)(3,7) \rangle$	0
15	$\mathrm{PSL}(3,2)a = \langle (1,4)(2,3), (2,4,6)(3,5,7) \rangle$	0
15	$\mathrm{PSL}(3,2)b = \langle (1,3)(2,7), (1,5,7)(3,4,6) \rangle$	0
7	$A_6 = \langle (1,2,3,4,5), (4,5,6) \rangle$	0

Chapter 6

Examples

6.1 (G, H)-extensions

This section concerns the existence of number fields with prescribed Galois group for which the HNP holds, and the existence of those for which it fails. The main result is Theorem 6.1.3 below, which generalizes [41, Corollary 3.3] to non-normal extensions. To prove it, we will use the notion of k-adequate extensions, as introduced by Schacher in [82].

Definition 6.1.1. An extension K/k of number fields is said to be *k-adequate* if K is a maximal subfield of a finite dimensional k-central division algebra.

A conjecture of Bartels (see [3, p. 198]) predicted that the HNP would hold for any k-adequate extension. This was proved by Gurak (see [41, Theorem 3.1]) for Galois extensions, but disproved in general by Drakokhrust and Platonov (see [27, §9, §11]). Given a Galois extension L/k, a result of Schacher (see [82, Proposition 2.6]) shows that L is k-adequate if and only if for every prime $p \mid [L : k]$ there are at least two places v_1 and v_2 of k such that $D_{v_i} = \mathrm{Gal}(L_{v_i}/k_{v_i})$ contains a Sylow p-subgroup of $\mathrm{Gal}(L/k)$. This led Schacher to establish the following result:

Theorem 6.1.2. *[82, Theorem 9.1] For any finite group G there exists a number field k and a k-adequate Galois extension L/k with $\mathrm{Gal}(L/k) \cong G$.*

Let G be a finite group and H a subgroup of G. We define a (G, H)-extension of a number field k to be an extension K/k for which there exists a Galois extension L/k containing K/k such that $\mathrm{Gal}(L/k) \cong G$ and $\mathrm{Gal}(L/K) \cong H$. We write $F_{G/H}$ for a flasque module in a flasque resolution of the Chevalley module $J_{G/H}$.

Theorem 6.1.3. *Let G be a finite group and H a subgroup of G. Then*

(i) there exist a number field k and a (G, H)-extension of k satisfying the HNP and, furthermore, if $\mathrm{H}^1(G, F_{G/H}) \neq 0$ then weak approximation fails for the norm one torus associated with this extension;

(ii) there exist a number field k and a (G, H)-extension of k whose norm one torus satisfies weak approximation and, furthermore, if $\mathrm{H}^1(G, F_{G/H}) \neq 0$ then this extension fails the HNP.

Proof. (i) Let L/k be a k-adequate Galois extension with Galois group G as given in Theorem 6.1.2. Let $K = L^H$ and $T = R^1_{K/k}\mathbb{G}_m$. Recall that, by Theorem 1.5.13,

$$Ш(T)^{\sim} = \operatorname{Ker}\left(\mathrm{H}^2(G, J_{G/H}) \xrightarrow{\text{Res}} \prod_{v\in\Omega_k} \mathrm{H}^2(D_v, J_{G/H})\right).$$

Let p be a prime dividing $|G|$ and let D_v be a decomposition group containing a Sylow p-subgroup of G. Then Lemmas 1.1.2 and 1.1.4 show that the map

$$\mathrm{H}^2(G, J_{G/H})_{(p)} \xrightarrow{\text{Res}} \prod_{v\in\Omega_k} \mathrm{H}^2(D_v, J_{G/H})$$

is injective. It follows that $Ш(T) = 0$ and so $\mathfrak{K}(K/k)$ is trivial. The statement regarding weak approximation follows from Theorem 1.5.8 and isomorphism (1.5.2) of Theorem 1.5.12.

(ii) By [32] there exists a Galois extension L/k of number fields with $\mathrm{Gal}(L/k) \cong G$ such that every decomposition group is cyclic. Let $K = L^H$, $T = R^1_{K/k}\mathbb{G}_m$ and let X be a smooth compactification of T. By [91, §3, Theorem 6 and Corollary 2], we have $A(T) = 0$ and $Ш(T) \cong \mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim}$. The result now follows from isomorphism (1.5.2) of Theorem 1.5.12 and the fact that $\mathfrak{K}(K/k) = Ш(T)$. □

The condition $\mathrm{H}^1(G, F_{G/H}) \neq 0$ in Theorem 6.1.3 is necessary because for a (G, H)-extension K/k with X a smooth compactification of $R^1_{K/k}\mathbb{G}_m$, one has $\mathrm{H}^1(k, \operatorname{Pic}\overline{X}) = \mathrm{H}^1(G, F_{G/H})$ (see Theorem 1.5.12).

Remark 6.1.4. It is interesting to compare Theorem 6.1.3 with [30, Theorem 1.3], where the authors prove existence of Galois extensions failing the HNP with prescribed solvable Galois group G and base field k. Here we avoid the restriction on G but lose control of the base field which, in both cases of Theorem 6.1.3, may be of quite large degree over $\mathbb{Q}$.

6.2 Successes and failures for A_n and S_n-extensions

As a consequence of Theorem 6.1.3, we can also obtain a version of Theorem 5.1.3 for the knot group and the defect of weak approximation. In what follows, let $L/K/k$ be a tower of number fields where L/k is Galois with Galois group G and let $T = R^1_{K/k}\mathbb{G}_m$.

Proposition 6.2.1. *(i) For $G \cong S_n$ the groups $\mathfrak{K}(K/k)$ and $A(T)$ are elementary abelian 2-groups. Moreover, every possibility for $\mathfrak{K}(K/k)$ is realised: given an elementary abelian 2-group A, there exists $n \in \mathbb{N}$ and an extension of number fields K/k whose normal closure has Galois group S_n such that $\mathfrak{K}(K/k) \cong A$. Likewise, every possibility for $A(T)$ is realised.*

(ii) For $G \cong A_n$ the groups $\mathfrak{K}(K/k)$ and $A(T)$ are elementary abelian 2-groups or isomorphic to C_3 or C_6. Again, every possibility for $\mathfrak{K}(K/k)$ is realised, and likewise for $A(T)$.

Proof. This follows from Theorems 1.5.8, 5.1.3 and the proof of Theorem 6.1.3. □

We now provide examples of number fields over $\mathbb{Q}$ illustrating that in every case addressed by Propositions 5.1.7 and 5.1.9, there exists an extension of the desired type satisfying the HNP. Furthermore, in the cases where failure of the HNP is theoretically possible, we construct examples showing that failures actually occur (over at most a quadratic extension of $\mathbb{Q}$). When looking for such examples, [88, Lemmas 18 and 20] give useful practical conditions to test the local properties of Proposition 5.1.7. Some of these extensions were found using the LMFBD database [61] and all assertions below concerning Galois groups and ramification properties were verified using the computer algebra system MAGMA [14].

6.2.1 Successes

- First consider $G = A_4$ or S_4. Let $L/\mathbb{Q}$ be the splitting field of the polynomial $f(x)$ defined as

$$f(x) = \begin{cases} x^4 - 2x^3 + 2x^2 + 2 & \text{if } G = A_4, \\ x^4 - 2x^3 - 4x^2 - 6x - 2 & \text{if } G = S_4. \end{cases}$$

  In both cases $L/\mathbb{Q}$ is a Galois extension with Galois group G such that the decomposition group at the prime 2 is the full Galois group. Applying Proposition 5.1.7 we thus conclude that the HNP holds for $L/\mathbb{Q}$ as well as for any subextension $K/\mathbb{Q}$ contained in $L/\mathbb{Q}$.

- For $G = A_5$, let $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^5 - x^4 + 2x^2 - 2x + 2$, and let $L/\mathbb{Q}$ be the normal closure of $K/\mathbb{Q}$. We have $\mathrm{Gal}(L/\mathbb{Q}) \cong A_5$ and there exists a prime $\mathfrak{p}$ of K above 2 with ramification index 4, so it follows that $4 \mid |D_2|$. Since any subgroup of A_5 with order divisible by 4 contains a copy of V_4 generated by two double transpositions, Proposition 5.1.7 shows that the HNP holds for any subextension of $L/\mathbb{Q}$.

- For $G = S_5$, take $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^{10} - 4x^9 - 24x^8 + 80x^7 + 174x^6 - 416x^5 - 372x^4 + 400x^3 + 370x^2 + 32x - 16$, and let $L/\mathbb{Q}$ be the normal closure of $K/\mathbb{Q}$. One can verify that $\mathrm{Gal}(L/\mathbb{Q}) \cong S_5$ and that there is a prime $\mathfrak{p}$ of K above 2 with ramification index 8. By the same reasoning as in the A_5 case, D_2 contains a copy of V_4 generated by two double transpositions, and thus the HNP holds for any subextension of $L/\mathbb{Q}$ by Proposition 5.1.7.

- For $G = A_6$, let $K = \mathbb{Q}(\alpha)$, where α is a root of the polynomial $x^{15} - 3x^{13} - 2x^{12} + 12x^{10} + 50x^9 - 54x^7 + 68x^6 - 162x^5 + 30x^4 - 67x^3 + 15x + 4$, and let $L/\mathbb{Q}$ be the normal closure of $K/\mathbb{Q}$. We have $\mathrm{Gal}(L/\mathbb{Q}) \cong A_6$ and there are primes $\mathfrak{p}$ and $\mathfrak{q}$ of K above 2 and 3, respectively, such that $[K_{\mathfrak{p}} : \mathbb{Q}_2] = 8$ and $[K_{\mathfrak{q}} : \mathbb{Q}_3] = 9$. Since every subgroup of A_6 with order divisible by 8 contains a copy of D_4, it follows that $D_4 \hookrightarrow D_2$. Analogously, we have $C_3 \times C_3 \hookrightarrow D_3$. Proposition 5.1.9 then shows that the HNP holds for any subextension of $L/\mathbb{Q}$.

- For $G = A_7$, let $L/\mathbb{Q}$ be the splitting field of the polynomial $x^7 - 3x^6 - 3x^5 - x^4 + 12x^3 + 24x^2 + 16x + 24$. We have $\mathrm{Gal}(L/\mathbb{Q}) \cong A_7$ and the primes 2 and 3 ramify in $L/\mathbb{Q}$. Let M be the fixed field of the subgroup $\langle (2,3)(5,7), (1,2)(4,5,6,7), (2,3)(5,6)\rangle \cong (A_4 \times C_3) \rtimes C_2$ of A_7, a degree 35 extension of $\mathbb{Q}$. Given a prime p, let $e = e(p)$ denote its ramification index and $f = f(p)$ its inertial degree in L. Note that if the decomposition $\mathcal{O}_M/p\mathcal{O}_M \cong \bigoplus_i \mathbb{F}_{p^{f_i}}[t_i]/(t_i^{e_i})$ holds for some $e_i, f_i \in \mathbb{Z}_{\geq 0}$, then $\mathrm{lcm}(e_i) \mid e$, $\mathrm{lcm}(f_i) \mid f$ and hence $\mathrm{lcm}(e_i) \cdot \mathrm{lcm}(f_i) \mid ef = |D_p|$. Factoring the prime $p = 2$ in $\mathcal{O}_M$ gives $\mathrm{lcm}(e_i) = 12$ and $\mathrm{lcm}(f_i) = 2$, so $24 \mid |D_2|$. Since any subgroup of A_7 with order divisible by 24 contains a copy of D_4, we conclude that $D_4 \hookrightarrow D_2$. Using the same reasoning with the prime $p = 3$, we find $18 \mid |D_3|$ and consequently D_3 contains a copy of $C_3 \times C_3$. By Proposition 5.1.9, it follows that the HNP holds for any subextension of $L/\mathbb{Q}$.

Remark 6.2.2. An alternative approach to finding examples of number fields satisfying the HNP and with Galois groups as in Propositions 5.1.7 and 5.1.9 is to use $\mathbb{Q}$-adequate extensions. Indeed, examining the local conditions of Propositions 5.1.7 and 5.1.9, it is clear that the HNP holds for any subextension of a $\mathbb{Q}$-adequate Galois extension with Galois group $G = A_4, S_4, A_5, S_5, A_6, A_7$. The existence of $\mathbb{Q}$-adequate extensions with prescribed Galois group G has been studied by Schacher and others. For $G = A_4, S_4, A_5, S_5, A_6, A_7$, there exist $\mathbb{Q}$-adequate Galois extensions $L/\mathbb{Q}$ with $\mathrm{Gal}(L/\mathbb{Q}) \cong G$. We give some references for the interested reader. For $G = A_4, A_5$ see [35], [36], respectively. In fact, for these two groups stronger results hold. For $G = A_4$ there exist k-adequate Galois extensions with Galois group A_4 for *any* global field k of characteristic not equal to 2 or 3 (see [35, Corollary 2.2]). For $G = A_5$, [36, Theorem 1] constructs k-adequate Galois extensions with Galois group A_5 for any number field k such that $\sqrt{-1} \notin k$. For $G = S_4, S_5$ see [82, Theorem 7.1]. The cases $G = A_6, A_7$ are treated in [29]. We chose not to pursue this approach because the polynomials defining the field extensions were rather cumbersome, particularly for A_6 and A_7.

6.2.2 Failures

- We start with the cases where G is A_4 or S_4. Let $L/\mathbb{Q}$ be the splitting field of $f(x)$, where
$$f(x) = \begin{cases} x^4 + 3x^2 - 7x + 4 & \text{if } G = A_4, \\ x^4 - x^3 - 4x^2 + x + 2 & \text{if } G = S_4. \end{cases}$$

  In both cases $L/\mathbb{Q}$ is a Galois extension with Galois group G such that every decomposition group is cyclic. Therefore, Proposition 5.1.7 shows that the HNP fails for any subextension of L/k falling under case (i) or (ii) of Proposition 5.1.7, i.e. an extension where the HNP can theoretically fail.

- We now find examples for the A_5 and S_5 cases using work of Uchida [90]. Examples for the A_6 and A_7 cases can be obtained in a manner analogous to the construction for A_5. Let $F/\mathbb{Q}$ be the splitting field of $f(x) = x^5 - x + 1$ and set $D = \mathrm{Disc}(f) = 19 \cdot 151$. By [90, Corollary and Theorem 2], $F/\mathbb{Q}(\sqrt{D})$ is an unramified Galois extension with Galois group A_5, while $F(\sqrt{2})/\mathbb{Q}(\sqrt{2D})$ is an unramified Galois extension with Galois group S_5. If $G = A_5$ then set $L = F, k = \mathbb{Q}(\sqrt{D})$. If $G = S_5$ then set $L = F(\sqrt{2}), k = \mathbb{Q}(\sqrt{2D})$. Let K/k be a subextension of L/k falling under case (i) or (ii) of Proposition 5.1.7. Since L/k is unramified, all its decomposition groups are cyclic, whereby the HNP fails for K/k by the criterion of Proposition 5.1.7.

  A similar construction allows us to provide examples of unramified Galois A_6 and A_7 extensions. By Proposition 5.1.9, these extensions have knot groups isomorphic to C_6 and therefore the HNP fails for them. It is also possible to construct failures with knot group C_2 or C_3. Indeed, if $G = A_6$ or A_7, one can set $S = C_3 \times C_3$ in [27, Lemma 6] in order to get a Galois extension of number fields with decomposition group $D_v = C_3 \times C_3$ for every ramified place v. Since the remaining places have cyclic decomposition groups, it follows from Proposition 5.1.9 that the knot group of this extension is C_2. An analogous construction choosing $S = D_4$ gives a Galois extension of number fields with knot group equal to C_3.

Part II

The multinorm principle

Chapter 7

Introduction

Let $K = (K_1, \ldots, K_n)$ be an n-tuple ($n \geq 1$) of finite extensions of a number field k. In this part of the thesis, we study the so-called *multinorm principle* for K, which is said to hold if, for any $c \in k^*$, the affine k-variety

$$T_c : \prod_{i=1}^{n} N_{K_i/k}(\Xi_i) = c \tag{7.0.1}$$

(where Ξ_i is a variable) satisfies the Hasse principle. In other words, K satisfies the multinorm principle if, for all $c \in k^*$, the existence of points on T_c over every completion of k implies the existence of a k-point.

From a geometric viewpoint, T_c defines a principal homogenous space under the *multinorm one torus* T, defined by the exact sequence of k-algebraic groups

$$1 \to T \to \prod_{i=1}^{n} R_{K_i/k}\mathbb{G}_m \xrightarrow{\prod_i N_{K_i/k}} \mathbb{G}_m \to 1.$$

In this way, the Tate–Shafarevich group $Ш(T)$ of T is naturally identified with the *obstruction to the multinorm principle* for K

$$\mathfrak{K}(K, k) = k^* \cap \prod_{i=1}^{n} N_{K_i/k}(\mathbb{A}^*_{K_i}) / \prod_{i=1}^{n} N_{K_i/k}(K_i^*),$$

and the multinorm principle holds if and only if $\mathfrak{K}(K, k) = 1$.

Setting $n = 1$ one recovers the *Hasse norm principle* (HNP), studied in Part I of this thesis. Recall that if K/k is Galois, then Tate's theorem 1.6.9 gives an explicit description of the obstruction to the HNP in terms of the group cohomology of its local and global Galois groups. Later work of Drakokhrust allows one to obtain a more general description of this obstruction for an arbitrary extension K/k in terms of generalized representation groups, see [26, Theorem 2].

It is natural to look for a similar description when $n > 1$. This is the main objective of this part of the thesis and we provide explicit formulas for the obstructions to the multinorm principle and weak approximation for the multinorm one torus of n arbitrary extensions. In order to achieve this, we generalize the concept (due to Drakokhrust and Platonov in [27] and described in detail in Section 4.3) of the first obstruction to the Hasse norm principle (see Section 8.1). By then adapting work of Drakokhrust ([26]), we obtain our main result (Theorem 8.2.6), describing the obstructions to the multinorm principle and weak approximation in terms of generalized representation groups of the relevant local and global Galois groups. The formulas given in Theorem 8.2.6 are effectively computable and we also provide algorithms in GAP [33] for this effect (see Remark 8.2.7).

Multiple other questions on the multinorm principle have been analyzed in the literature. For example, if $n = 2$ it is known that the multinorm principle holds if

1. K_1 or K_2 is a cyclic extension of k ([50, Proposition 3.3]);
2. K_1/k is abelian, satisfies the HNP and K_2 is linearly disjoint from K_1 ([78, Proposition 4.2]);
3. the Galois closures of K_1/k and K_2/k are linearly disjoint over k ([77]).

Subsequent work of Demarche and Wei provided a generalization of the result in (3) to n extensions ([25, Theorems 1 and 6]), while also addressing weak approximation for the associated multinorm one torus. In [76], Pollio computed the obstruction to the multinorm principle for a pair of abelian extensions and, in [5], Bayer-Fluckiger, Lee and Parimala provided an explicit combinatorial description of $\mathfrak{K}(K, k)$ as well as necessary and sufficient conditions for the variety T_c to have a k-rational point, assuming that one of the extensions K_i/k is cyclic.

We will also apply our techniques to describe the validity of the local-global principles in three concrete examples (see Chapter 9) motivated by the aforementioned results of Demarche–Wei, Pollio and Bayer-Fluckiger–Lee–Parimala. To obtain these results, we use comparison maps between the obstructions to the local-global principles in the multinorm and the Hasse norm principle setting. We start by proving a result inspired by [25, Theorem 6] that compares the birational invariants $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ and $\mathrm{H}^1(k, \operatorname{Pic} \overline{Y})$, where X is a smooth compactification of the multinorm one torus T and Y is a smooth compactification of the norm one torus $S = R^1_{F/k}\mathbb{G}_m$ of the extension $F = \bigcap\limits_{i=1}^{n} K_i$. In particular, we show (Theorem 9.2.1) that under certain conditions there is an isomorphism

$$\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) \xrightarrow{\simeq} \mathrm{H}^1(k, \operatorname{Pic} \overline{Y}).$$

This result further allows us to compare the defect of weak approximation for T with the defect of weak approximation for S (Corollary 9.2.3).

Under the same assumptions, we also show (Theorem 9.3.1) the existence of isomorphisms

$$\mathfrak{K}(K, k) \cong \mathfrak{K}(F/k) \text{ and } A(T) \cong A(S)$$

when all the extensions K_i/k are abelian. This theorem generalizes Pollio's main result in [76] on the obstruction to the multinorm principle for a pair of abelian extensions.

In Section 9.4 we complement [5, Theorem 8.3] by providing a characterization (Theorem 9.4.1) of weak approximation for the multinorm one torus of n non-isomorphic cyclic extensions of prime degree p. More precisely, we show that both the multinorm principle and weak approximation for T hold if $[K_1 \dots K_n : k] > p^2$. Otherwise, weak approximation holds if and only if the multinorm principle fails (a property that can be detected by precise local conditions, see Remark 9.4.3).

In recent (and independent) work, Lee [59] extends results of [5, §8] to provide a description of the multinorm principle and weak approximation for the multinorm one torus of n non-isomorphic cyclic extensions (and, in this way, obtains a result more general than Theorem 9.4.1). Similarly, Bayer-Fluckiger and Parimala [6] have recently extended arithmetical results of [5] to determine the unramified Brauer groups of torsors over some norm one tori and have also proved Theorem 9.4.1 (see [6, Corollary 9.10]).

Chapter 8

Explicit methods for the multinorm principle

In this chapter we define the concept of the first obstruction to the multinorm principle and present several of its properties. We fix a number field k, an n-tuple $K = (K_1, \ldots, K_n)$ of finite extensions of k and a finite Galois extension L/k containing all the fields $K_1, \ldots, K_n$. We denote $G = \mathrm{Gal}(L/k)$, $H_i = \mathrm{Gal}(L/K_i)$ for $i = 1, \ldots, n$ and $H = \langle H_1, \ldots, H_n \rangle$, the subgroup of G generated by all the H_i. Note that $H = \mathrm{Gal}(L/F)$, where $F = \bigcap\limits_{i=1}^{n} K_i$.

8.1 The first obstruction to the multinorm principle

Definition 8.1.1. We define the *first obstruction to the multinorm principle for K corresponding to (L, K, k)* as

$$\mathfrak{F}(L, K, k) = k^* \cap \prod_{i=1}^{n} N_{K_i/k}(\mathbb{A}^*_{K_i}) / \prod_{i=1}^{n} N_{K_i/k}(K_i^*)(k^* \cap N_{L/k}(\mathbb{A}^*_L)).$$

Remark 8.1.2. This notion generalizes the concept (introduced by Drakokhrust and Platonov in [27]) of the *first obstruction to the Hasse norm principle for K/k corresponding to a tower of fields $L/K/k$*, defined in Section 4.3.

The first obstruction to the multinorm principle has various useful properties – for example, it is clear from the definition that the total obstruction to the multinorm principle

$\mathfrak{K}(K,k)$ surjects onto $\mathfrak{F}(L,K,k)$ with equality if the Hasse norm principle holds for L/k. Moreover, this equality also happens if the first obstruction to the Hasse norm principle for some extension K_i/k corresponding to the tower $L/K_i/k$ coincides with the knot group $\mathfrak{K}(K_i/k) = k^* \cap N_{K_i/k}(\mathbb{A}^*_{K_i})/N_{K_i/k}(K_i^*)$:

Lemma 8.1.3. *If $\mathfrak{K}(K_i/k) = \mathfrak{F}(L/K_i/k)$ for some $i = 1, \dots, n$, then $\mathfrak{K}(K,k) = \mathfrak{F}(L,K,k)$.*

Proof. The assumption translates into $k^* \cap N_{L/k}(\mathbb{A}^*_L) \subset N_{K_i/k}(K_i^*)$. This implies that $\prod_{i=1}^{n} N_{K_i/k}(K_i^*)(k^* \cap N_{L/k}(\mathbb{A}^*_L)) = \prod_{i=1}^{n} N_{K_i/k}(K_i^*)$ and hence $\mathfrak{K}(K,k) = \mathfrak{F}(L,K,k)$. □

Corollary 8.1.4. *If $[K_i : k]$ is square-free for some $i = 1, \dots, n$, then $\mathfrak{K}(K,k) = \mathfrak{F}(L,K,k)$.*

Proof. By [27, Corollary 1], if $[K_i : k]$ is square-free, then $\mathfrak{K}(K_i/k) = \mathfrak{F}(L/K_i/k)$. Now apply Lemma 8.1.3. □

More generally, one has the following criterion (extending [27, Theorem 3]) for the equality $\mathfrak{K}(K,k) = \mathfrak{F}(L,K,k)$.

Proposition 8.1.5. *Let $1 \le t \le n$ and $n_1, \dots, n_t$ be positive integers. For each $i = 1, \dots, t$, choose a collection of n_i subgroups $G_{i,1}, \dots, G_{i,n_i}$ of G and n_i subgroups $H_{i,1}, \dots, H_{i,n_i}$ such that $H_{i,j} \subset H_i \cap G_{i,j}$ for any $j = 1, \dots, n_i$. Set $K_{i,j} = L^{H_{i,j}}$ and $k_{i,j} = L^{G_{i,j}}$ for all i, j. Suppose that the Hasse norm principle holds for all the extensions $K_{i,j}/k_{i,j}$ and that the map*

$$\bigoplus_{i=1}^{t}\bigoplus_{j=1}^{n_i} \mathrm{Cor}^G_{G_{i,j}} : \bigoplus_{i=1}^{t}\bigoplus_{j=1}^{n_i} \hat{\mathrm{H}}^{-3}(G_{i,j},\mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G,\mathbb{Z})$$

is surjective. Then $\mathfrak{K}(K,k) = \mathfrak{F}(L,K,k)$.

Proof. By Tate's theorem on class formations (see [18, p. 197]), the following diagram commutes for any subgroup G' of G

$$\begin{tikzcd}
\hat{\mathrm{H}}^{-3}(G',\mathbb{Z}) \arrow[r, "\simeq"] \arrow[d, "\mathrm{Cor}^G_{G'}"] & \hat{\mathrm{H}}^{-1}(G',C_L) \arrow[d, "\mathrm{Cor}^G_{G'}"'] \\
\hat{\mathrm{H}}^{-3}(G,\mathbb{Z}) \arrow[r, "\simeq"] & \hat{\mathrm{H}}^{-1}(G,C_L)
\end{tikzcd} \tag{8.1.1}$$

where C_L denotes the idèle class group of L/k and the horizontal isomorphisms are given by cup product with the canonical generator of $\hat{\mathrm{H}}^2(G, C_L)$. The hypothesis is thus equivalent to the map

$$\bigoplus_{i=1}^{t}\bigoplus_{j=1}^{n_i}\mathrm{Cor}_{G_{i,j}}^{G} : \bigoplus_{i=1}^{t}\bigoplus_{j=1}^{n_i}\hat{\mathrm{H}}^{-1}(G_{i,j}, C_L) \to \hat{\mathrm{H}}^{-1}(G, C_L) \tag{8.1.2}$$

being surjective. Using the definition of the Tate cohomology group $\hat{\mathrm{H}}^{-1}$, (8.1.2) is equivalent to the surjectivity of the map induced by the natural embeddings

$$\bigoplus_{i=1}^{t}\bigoplus_{j=1}^{n_i} N_{L/k_{i,j}}^{-1}(k_{i,j}^*)/I_{G_{i,j}}\mathbb{A}_L^* \cdot L^* \to N_{L/k}^{-1}(k^*)/I_G\mathbb{A}_L^* \cdot L^* \tag{8.1.3}$$

Here $N_{L/k}^{-1}(k^*) = \{a \in \mathbb{A}_L^* \mid N_{L/k}(a) \in k^*\}$, $I_G\mathbb{A}_L^* = \langle \sigma(a)a^{-1} \mid \sigma \in G, a \in \mathbb{A}_L^*\rangle$ and the corresponding notions for $k_{i,j}$ and $G_{i,j}$ are defined similarly.

We now prove that $\mathfrak{K}(K, k) = \mathfrak{F}(L, K, k)$. It suffices to show that $k^* \cap N_{L/k}(\mathbb{A}_L^*) \subset \prod\limits_{i=1}^{t} N_{K_i/k}(K_i^*)$. Let $\alpha = N_{L/k}(a) \in k^* \cap N_{L/k}(\mathbb{A}_L^*)$ for some $a \in \mathbb{A}_L^*$. From the surjectivity of (8.1.3) it follows that there exist $a_{i,j} \in N_{L/k_{i,j}}^{-1}(k_{i,j}^*) \subset \mathbb{A}_L^*$ such that $a = \prod\limits_{i=1}^{t}\prod\limits_{j=1}^{n_i} a_{i,j}$, and thus $\alpha = \prod\limits_{i=1}^{t}\prod\limits_{j=1}^{n_i} N_{L/k}(a_{i,j})$. Since by hypothesis the Hasse norm principle holds for $K_{i,j}/k_{i,j}$, there exist $\gamma_{i,j} \in K_{i,j}^*$ such that $N_{L/k_{i,j}}(a_{i,j}) = N_{K_{i,j}/k_{i,j}}(\gamma_{i,j})$. Moreover, as $K_i \subset K_{i,j}$ for any $i = 1, \dots, t$ and $j = 1, \dots, n_i$, we have

$$\alpha = \prod_{i=1}^{t}\prod_{j=1}^{n_i} N_{L/k}(a_{i,j}) = \prod_{i=1}^{t}\prod_{j=1}^{n_i} N_{k_{i,j}/k}(N_{L/k_{i,j}}(a_{i,j})) = \prod_{i=1}^{t}\prod_{j=1}^{n_i} N_{k_{i,j}/k}(N_{K_{i,j}/k_{i,j}}(\gamma_{i,j})) =$$

$$= \prod_{i=1}^{t}\prod_{j=1}^{n_i} N_{K_{i,j}/k}(\gamma_{i,j}) = \prod_{i=1}^{t} N_{K_i/k}(\prod_{j=1}^{n_i} N_{K_{i,j}/K_i}(\gamma_{i,j})) \in \prod_{i=1}^{t} N_{K_i/k}(K_i^*).$$

□

A further trait of the first obstruction to the multinorm principle $\mathfrak{F}(L, K, k)$ is that it can be expressed in terms of the local and global Galois groups of the towers $L/K_i/k$ (in similar fashion to the first obstruction to the Hasse norm principle). In order to prove this, we will make use of Lemma 4.3.4, which for convenience we restate below:

Lemma 8.1.6. *(Lemma 4.3.4) Let $L/K/k$ be a tower of number fields with L/k Galois. Set $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Gal}(L/K)$. Then, given a place v of k, the set of places w of K above v is in bijection with the set of double cosets in the decomposition $G = \bigcup_{i=1}^{r_v} Hx_iD_v$. If w corresponds to Hx_iD_v, then the decomposition group H_w of the extension L/k at w equals $H \cap x_iD_vx_i^{-1}$.*

In our situation, for any $v \in \Omega_k$ and $i = 1, \ldots, n$, let $G = \bigcup_{t=1}^{r_{v,i}} H_ix_{i,t}D_v$ be a double coset decomposition. By the above lemma, $H_{i,w} := H_i \cap x_{i,t}D_vx_{i,t}^{-1}$ is the decomposition group of L/K_i at a place w of K_i above v corresponding to the double coset $H_ix_{i,t}D_v$. Now consider the commutative diagram:

$$\begin{tikzcd}
\bigoplus_{i=1}^{n} H_i^{\mathrm{ab}} \arrow[r, "\psi_1"] & G^{\mathrm{ab}} \\
\bigoplus_{i=1}^{n}\Big(\bigoplus_{v\in\Omega_k}\big(\bigoplus_{w|v} H_{i,w}^{\mathrm{ab}}\big)\Big) \arrow[u, "\varphi_1"] \arrow[r, "\psi_2"] & \bigoplus_{v\in\Omega_k} D_v^{\mathrm{ab}} \arrow[u, "\varphi_2"']
\end{tikzcd} \tag{8.1.4}$$

Here the superscript ${}^{\mathrm{ab}}$ above a group denotes its abelianization and the inside sum over $w|v$ runs over all the places w of K_i above v. Additionally, the maps φ_1, ψ_1 and φ_2 are induced by the inclusions $H_{i,w} \hookrightarrow H_i, H_i \hookrightarrow G$ and $D_v \hookrightarrow G$, respectively, while ψ_2 is obtained from the product of all conjugation maps $H_{i,w}^{ab} \to D_v^{ab}$ sending $h_{i,t}[H_{i,w}, H_{i,w}]$ to $x_{i,t}^{-1}h_{i,t}x_{i,t}[D_v, D_v]$. We denote by ψ_2^v (respectively, ψ_2^{nr}) the restriction of the map ψ_2 to the subgroup $\bigoplus_{i=1}^{n}(\bigoplus_{w|v} H_{i,w}^{\mathrm{ab}})$ (respectively, $\bigoplus_{i=1}^{n}(\bigoplus_{\substack{v\in\Omega_k\\ v \text{ unramified}}}(\bigoplus_{w|v} H_{i,w}^{\mathrm{ab}})))$. With this notation set, we can now establish the main result of this section (generalizing Theorem 4.3.5):

Theorem 8.1.7. *In the notation of diagram (8.1.4), we have*

$$\mathfrak{F}(L, K, k) \cong \mathrm{Ker}\,\psi_1/\varphi_1(\mathrm{Ker}\,\psi_2).$$

Proof. Diagram (8.1.4) can be written as

$$\begin{tikzcd}
\bigoplus_{i=1}^{n} \hat{\mathrm{H}}^{-2}(H_i, \mathbb{Z}) \arrow[r, "\psi_1"] & \hat{\mathrm{H}}^{-2}(G, \mathbb{Z}) \\
\bigoplus_{i=1}^{n}\Big(\bigoplus_{v \in \Omega_k} \big(\bigoplus_{w|v} \hat{\mathrm{H}}^{-2}(H_{i,w}, \mathbb{Z})\big)\Big) \arrow[r, "\psi_2"] \arrow[u, "\varphi_1"] & \bigoplus_{v \in \Omega_k} \hat{\mathrm{H}}^{-2}(D_v, \mathbb{Z}) \arrow[u, "\varphi_2"']
\end{tikzcd} \tag{8.1.5}$$

By the local (respectively, global) Artin isomorphism, we have $\hat{\mathrm{H}}^{-2}(H_{i,w}, \mathbb{Z}) \cong \hat{\mathrm{H}}^{0}(H_{i,w}, L_w^*)$ and $\hat{\mathrm{H}}^{-2}(D_v, \mathbb{Z}) \cong \hat{\mathrm{H}}^{0}(D_v, L_v^*)$ (respectively, $\hat{\mathrm{H}}^{-2}(H_i, \mathbb{Z}) \cong \hat{\mathrm{H}}^{0}(H_i, C_L)$ and $\hat{\mathrm{H}}^{-2}(G, \mathbb{Z}) \cong \hat{\mathrm{H}}^{0}(G, C_L)$, where C_L is the idèle class group of L/k). Additionally, by [18, Proposition 7.3(b)] there are identifications $\bigoplus_{v \in \Omega_k} (\bigoplus_{w|v} \hat{\mathrm{H}}^{0}(H_{i,w}, L_w^*)) \cong \hat{\mathrm{H}}^{0}(H_i, \mathbb{A}_L^*)$ and $\bigoplus_{v \in \Omega_k} \hat{\mathrm{H}}^{0}(D_v, L_v^*) \cong \hat{\mathrm{H}}^{0}(G, \mathbb{A}_L^*)$. Since all these isomorphisms are compatible with the maps in diagram (8.1.5), this diagram induces the commutative diagram

$$\begin{tikzcd}
\bigoplus_{i=1}^{n} \hat{\mathrm{H}}^{0}(H_i, C_L) \arrow[r, "\psi_1"] & \hat{\mathrm{H}}^{0}(G, C_L) \\
\bigoplus_{i=1}^{n} \hat{\mathrm{H}}^{0}(H_i, \mathbb{A}_L^*) \arrow[r, "\psi_2"] \arrow[u, "\varphi_1"] & \hat{\mathrm{H}}^{0}(G, \mathbb{A}_L^*) \arrow[u, "\varphi_2"']
\end{tikzcd} \tag{8.1.6}$$

where φ_1, φ_2 are the natural projections and ψ_1, ψ_2 are induced by the product of the norm maps $N_{K_i/k}$. Using the definition of the cohomology group $\hat{\mathrm{H}}^{0}$, this diagram is equal to

$$\begin{tikzcd}
\bigoplus_{i=1}^{n} \frac{\mathbb{A}_{K_i}^*}{K_i^* N_{L/K_i}(\mathbb{A}_L^*)} \arrow[r, "\psi_1"] & \frac{\mathbb{A}_k^*}{k^* N_{L/k}(\mathbb{A}_L^*)} \\
\bigoplus_{i=1}^{n} \frac{\mathbb{A}_{K_i}^*}{N_{L/K_i}(\mathbb{A}_L^*)} \arrow[r, "\psi_2"] \arrow[u, "\varphi_1"] & \frac{\mathbb{A}_k^*}{N_{L/k}(\mathbb{A}_L^*)} \arrow[u, "\varphi_2"']
\end{tikzcd} \tag{8.1.7}$$

From diagram (8.1.7), it is clear that

$$\operatorname{Ker} \psi_1 = \{(x_i K_i^* N_{L/K_i}(\mathbb{A}_L^*))_{i=1}^n \mid \prod_{i=1}^{n} N_{K_i/k}(x_i) \in k^* N_{L/k}(\mathbb{A}_L^*)\}$$

and

$$\varphi_1(\operatorname{Ker}\psi_2) = \{(x_i K_i^* N_{L/K_i}(\mathbb{A}_L^*))_{i=1}^n \mid \prod_{i=1}^n N_{K_i/k}(x_i) \in N_{L/k}(\mathbb{A}_L^*)\}.$$

Now define

$$\begin{aligned} f\colon\ \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2) &\longrightarrow \mathfrak{F}(L,K,k) \\ (x_i K_i^* N_{L/K_i}(\mathbb{A}_L^*))_{i=1}^n &\longmapsto x\prod_{i=1}^n N_{K_i/k}({K_i}^*)(k^* \cap N_{L/k}(\mathbb{A}_L^*)) \end{aligned}$$

where x is any element of $k^* \cap \prod_{i=1}^n N_{K_i/k}(\mathbb{A}_{K_i}^*)$ such that $\prod_{i=1}^n N_{K_i/k}(x_i) \in xN_{L/k}(\mathbb{A}_L^*)$. It is straightforward to check that f is well defined and an isomorphism. □

Remark 8.1.8. Given the knowledge of the local and global Galois groups of the towers $L/K_i/k$, the first obstruction to the multinorm principle can be computed in finite time by employing Theorem 8.1.7. First, it is clear that the computation of the groups $\operatorname{Ker}\psi_1$ and $\varphi_1(\operatorname{Ker}\psi_2^v)$ for the ramified places v of L/k is finite. Moreover, from the definition of the maps in diagram (8.1.4), it is clear that if $v_1, v_2 \in \Omega_k$ are such that $D_{v_1} = D_{v_2}$, then $\varphi_1(\operatorname{Ker}\psi_2^{v_1}) = \varphi_1(\operatorname{Ker}\psi_2^{v_2})$. This shows that the computation of $\varphi_1(\operatorname{Ker}\psi_2^{nr})$ is also finite. On this account, we designed a function in GAP [33] (whose code is available in [63]) that takes as input the Galois groups G, H_i and the decomposition groups D_v at the ramified places of L/k and outputs the group $\mathfrak{F}(L,K,k)$.

8.2 The total obstruction to the multinorm principle

In this section we prove that the total obstruction to the multinorm principle $\mathfrak{K}(K,k)$ can always be expressed in terms of the arithmetic of the extensions K_i/k by using generalized representation groups (as defined in Section 1.3) of $G = \operatorname{Gal}(L/k)$. The link between this group-theoretic tool and our goal of computing the arithmetic obstruction $\mathfrak{K}(K,k)$ comes from the following result:

Proposition 8.2.1. *There exists a Galois extension P/k containing L and such that*

$$\mathfrak{F}(P,K,k) = \mathfrak{K}(K,k).$$

Furthermore, this extension has the property that $\overline{G} = \operatorname{Gal}(P/k)$ is a generalized representation group of G with base normal subgroup $\overline{M} = \operatorname{Gal}(P/L)$ and if $\overline{\lambda} : \overline{G} \to G$ is the associated projection map, we have $\operatorname{Gal}(P/K_i) = \overline{\lambda}^{-1}(H_i)$.

Proof. In [74, Satz 3], Opolka established that, given any Galois extension L/k, there exists a Galois extension P/k containing L and such that

$$N_{P/k}(\mathbb{A}_P^*) \cap k^* \subset N_{L/k}(L^*). \tag{8.2.1}$$

From (8.2.1) it follows that the first obstruction to the Hasse norm principle $\mathfrak{F}(P/K_i/k)$ coincides with the knot group $\mathfrak{K}(K_i/k)$ for any K_i and thus $\mathfrak{F}(P,K,k) = \mathfrak{K}(K,k)$ by Lemma 8.1.3. Furthermore, setting $\overline{M} := \mathrm{Gal}(P/L)$ and $\overline{G} := \mathrm{Gal}(P/k)$, Opolka observed in the proof of [74, Satz 3] that $\overline{M} \subset Z(\overline{G})$ and that the *deflation* map (see [58, §1]) $\mathrm{def} : \hat{\mathrm{H}}^{-3}(\overline{G},\mathbb{Z}) \to \hat{\mathrm{H}}^{-3}(G,\mathbb{Z})$ is trivial. From the long sequence of cohomology of the extension

$$1 \to \overline{M} \to \overline{G} \to G \to 1$$

we obtain the exact sequence

$$\hat{\mathrm{H}}^{-3}(\overline{G},\mathbb{Z}) \xrightarrow{\mathrm{def}} \hat{\mathrm{H}}^{-3}(G,\mathbb{Z}) \to \overline{M} \to \overline{G}/[\overline{G},\overline{G}],$$

from which it follows that $\overline{M} \cap [\overline{G},\overline{G}] \cong \hat{\mathrm{H}}^{-3}(G,\mathbb{Z})$ and thus $\overline{G}$ is a generalized representation group of G. □

As remarked in [26], the extension P/k is not uniquely determined and the computation of its arithmetic is not always easy. Nonetheless, one can still compute $\mathfrak{F}(P,K,k)$ by commencing with an arbitrary generalized representation group of G.

Let $\widetilde{G}$ be any generalized representation group of G with projection map $\widetilde{\lambda}$ and base normal subgroup $\widetilde{M}$. For any subgroup B of G, define $\widetilde{B} = \widetilde{\lambda}^{-1}(B)$ and $\overline{B} = \overline{\lambda}^{-1}(B)$. We will use of Lemma 1.3.8 of Section 1.3, which for convenience we restate below:

Lemma 8.2.2 (Lemma 1.3.8)**.** *There exists an isomorphism*

$$\tau : [\widetilde{G},\widetilde{G}] \xrightarrow{\sim} [\overline{G},\overline{G}]$$

with the following properties:

(i) $\overline{\lambda}(\tau(a)) = \widetilde{\lambda}(a)$ *for every* $a \in [\widetilde{G},\widetilde{G}]$*;*

(ii) $\tau([\widetilde{g}_1,\widetilde{g}_2]) = [\overline{g}_1,\overline{g}_2]$ *for all* $\widetilde{g}_1,\widetilde{g}_2 \in \widetilde{G}$ *and* $\overline{g}_1,\overline{g}_2 \in \overline{G}$ *such that* $\widetilde{\lambda}(\widetilde{g}_i) = \overline{\lambda}(\overline{g}_i)$*.*

For any subgroup B *of* G*,* τ *further identifies*

- $[\widetilde{B}, \widetilde{B}] \cong [\overline{B}, \overline{B}]$ *and*
- $\widetilde{M} \cap [\widetilde{B}, \widetilde{B}] \cong \overline{M} \cap [\overline{B}, \overline{B}]$.

Let R be the set of ramified places of L/k. For any $v \in \Omega_k$, set

$$\widetilde{S}_v = \begin{cases} \widetilde{D_v}, \text{ if } v \in R, \\ \text{a cyclic subgroup of } \widetilde{D_v} \text{ such that } \widetilde{\lambda}(\widetilde{S}_v) = D_v, \text{ otherwise.} \end{cases}$$

Furthermore, by the Chebotarev density theorem we can (and do) choose the subgroups $\widetilde{S}_v$ for $v \notin R$ in such a way that all the cyclic subgroups of $\widetilde{D_v}$ such that $\widetilde{\lambda}(\widetilde{S}_v) = D_v$ occur.

Remark 8.2.3. As pointed out in [26, p. 31], a double coset decomposition $\overline{G} = \bigcup_{t=1}^{r_{v,i}} \overline{H_i}\overline{x}_{i,t}\overline{D_v}$ corresponds to a double coset decomposition $\widetilde{G} = \bigcup_{t=1}^{r_{v,i}} \widetilde{H_i}\widetilde{x}_{i,t}\widetilde{S}_v$, where $\widetilde{x}_{i,t}$ is any element of $\widetilde{G}$ such that $\widetilde{\lambda}(\widetilde{x}_{i,t}) = \overline{\lambda}(\overline{x}_{i,t})$.

Consider the following diagram analogous to (8.1.4):

$$\begin{tikzcd}
\bigoplus_{i=1}^{n} \widetilde{H_i}^{\mathrm{ab}} \arrow[r, "\widetilde{\psi}_1"] & \widetilde{G}^{\mathrm{ab}} \\
\bigoplus_{i=1}^{n}\Big(\bigoplus_{v\in\Omega_k}\Big(\bigoplus_{w|v} \widetilde{H}_{i,w}^{\mathrm{ab}}\Big)\Big) \arrow[u, "\widetilde{\varphi}_1"] \arrow[r, "\widetilde{\psi}_2"] & \bigoplus_{v\in\Omega_k} \widetilde{S}_v^{\mathrm{ab}} \arrow[u, "\widetilde{\varphi}_2"']
\end{tikzcd} \tag{8.2.2}$$

where $\widetilde{H}_{i,w} = \widetilde{H_i} \cap \widetilde{x}_{i,t}\widetilde{S}_v\widetilde{x}_{i,t}^{-1}$ and all the maps are defined as in diagram (8.1.4).

We now prove the main result of this section, namely that the object $\operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2)$ does not depend on the choice of generalized representation group (and thus, by Theorem 8.1.7 and Proposition 8.2.1, it always coincides with $\mathfrak{K}(K, k)$). Before we show this, we need a lemma. To ease the notation, we often omit the cosets $\widetilde{H_i}'$ and $\overline{H_i}'$ when working with elements of $\operatorname{Ker}\widetilde{\psi}_1$ or $\operatorname{Ker}\overline{\psi}_1$.

Lemma 8.2.4. *For any indices* $1 \le i_1 < i_2 \le n$ *and any* $m \in \widetilde{H_{i_1}} \cap \widetilde{H_{i_2}}$, *we have*

$$h = (1, \ldots, \underbrace{m}_{i_1\text{-th entry}}, 1, \ldots, 1, \underbrace{m^{-1}}_{i_2\text{-th entry}}, 1, \ldots, 1) \in \widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}).$$

Proof. We construct a vector $\alpha \in \bigoplus_{i=1}^{n}\Big(\bigoplus_{\substack{v\in\Omega_k \\ v \text{ unramified}}}\big(\bigoplus_{w|v}\widetilde{H}_{i,w}^{\mathrm{ab}}\big)\Big)$ such that $\widetilde{\psi}_2(\alpha) = 1$ and $\widetilde{\varphi}_1(\alpha) = h$. Let v be an unramified place of k such that $\widetilde{S}_v = \langle m \rangle$. By definition, if $\widetilde{G} = \bigcup_{t=1}^{r_{v,i}} \widetilde{H_i}\widetilde{x}_{i,t}\widetilde{S}_v$ is a double coset decomposition of $\widetilde{G}$, then $\widetilde{H}_{i,w} = \widetilde{H_i} \cap \widetilde{x}_{i,t}\widetilde{S}_v\widetilde{x}_{i,t}^{-1}$. Let us suppose, without loss of generality, that $\widetilde{x}_{i_1,n_1} = 1 = \widetilde{x}_{i_2,n_2}$ for some index $1 \leq n_1 \leq r_{v,i_1}$ (respectively, $1 \leq n_2 \leq r_{v,i_2}$) corresponding to a place $w_1 \in \Omega_{K_{i_1}}$ (respectively, $w_2 \in \Omega_{K_{i_2}}$) via Lemma 8.1.6. In this way, we have $m \in \widetilde{H}_{i_1,w_1}$ and $m^{-1} \in \widetilde{H}_{i_2,w_2}$. Setting the (i_1, v, w_1)-th (respectively, (i_2, v, w_2)-th) entry of α to be equal to m (respectively, m^{-1}) and all other entries equal to 1, we obtain $\widetilde{\psi}_2(\alpha) = 1$ and $\widetilde{\varphi}_1(\alpha) = h$. □

Theorem 8.2.5. *In the notation of diagram* (8.2.2), *we have*

$$\mathfrak{K}(K, k) \cong \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2).$$

Proof. By Theorem 8.1.7 and Proposition 8.2.1, we have $\mathfrak{K}(K, k) \cong \operatorname{Ker}\overline{\psi}_1/\overline{\varphi}_1(\operatorname{Ker}\overline{\psi}_2)$, where the $^{-}$ notation is as in diagram (8.2.2) with respect to the groups of Proposition 8.2.1. Therefore, it suffices to prove that

$$\operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2) \cong \operatorname{Ker}\overline{\psi}_1/\overline{\varphi}_1(\operatorname{Ker}\overline{\psi}_2).$$

Define

$$\begin{aligned} f\colon\ \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2) &\longrightarrow \operatorname{Ker}\overline{\psi}_1/\overline{\varphi}_1(\operatorname{Ker}\overline{\psi}_2) \\ (\widetilde{h}_1, \dots, \widetilde{h}_n) &\longmapsto (\overline{h}_1, \dots, \overline{h}_n) \end{aligned}$$

where, for each $i = 1, \dots, n$, the element $\overline{h}_i \in \overline{H_i}$ is selected as follows: take $\overline{h}_i \in \overline{H_i}$ such that $\overline{\lambda}(\overline{h}_i) = \widetilde{\lambda}(\widetilde{h}_i)$ (note that $\overline{h}_i$ is only defined modulo $\overline{M} = \operatorname{Ker}\overline{\lambda}$). In this way, we have $\overline{\lambda}(\overline{h}_1 \dots \overline{h}_n) = \widetilde{\lambda}(\widetilde{h}_1 \dots \widetilde{h}_n)$. Additionally, by Lemma 8.2.2(i), $\overline{\lambda}(\tau(\widetilde{h}_1 \dots \widetilde{h}_n)) = \widetilde{\lambda}(\widetilde{h}_1 \dots \widetilde{h}_n)$ and thus

$$\tau(\widetilde{h}_1 \dots \widetilde{h}_n) = \overline{h}_1 \dots \overline{h}_n m \tag{8.2.3}$$

for some $m \in \overline{M}$. Changing $\overline{h}_n$ if necessary, we assume that $m = 1$ so that $\overline{h}_1 \dots \overline{h}_n \in [\overline{G}, \overline{G}]$ and therefore $(\overline{h}_1, \dots, \overline{h}_n) \in \operatorname{Ker}\overline{\psi}_1$.

Claim 1: f is well defined, i.e. it does not depend on the choice of the elements $\overline{h}_i$ and $f(\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2)) \subset \overline{\varphi}_1(\operatorname{Ker}\overline{\psi}_2)$.

Proof: We first prove that f does not depend on the choice of $\overline{h}_i$. Suppose that, for each $i = 1, \dots, n$, we choose elements $\underline{h}_i \in \overline{H_i}$ satisfying $\widetilde{\lambda}(\widetilde{h}_i) = \overline{\lambda}(\underline{h}_i)$ and $\tau(\widetilde{h}_1 \dots \widetilde{h}_n) = \underline{h}_1 \dots \underline{h}_n$. We show that $(\underline{h}_1, \dots, \underline{h}_n) = (\overline{h}_1, \dots, \overline{h}_n)$ in $\operatorname{Ker} \overline{\psi}_1 / \overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)$. Writing $\underline{h}_i = \overline{h}_i m_i$ for some $m_i \in \overline{M}$, it suffices to prove that $(m_1, \dots, m_n) \in \overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)$. Since $\overline{h}_1 \dots \overline{h}_n = \tau(\widetilde{h}_1 \dots \widetilde{h}_n) = \underline{h}_1 \dots \underline{h}_n$ and the elements m_i are in $\overline{M} \subset Z(\overline{G})$, we obtain $m_1 \dots m_n = 1$. As $\overline{M} \subset \bigcap_{i=1}^{n} \overline{H_i}$, multiplying $(m_1, \dots, m_n)$ by $(m_2, m_2^{-1}, 1, \dots, 1)$ (which lies in $\overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)$ by Lemma 8.2.4), we have $(m_1, \dots, m_n) \equiv (m_1 m_2, 1, m_3, \dots, m_n) \pmod{\overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)}$. Repeating this procedure, we obtain $(m_1, \dots, m_n) \equiv (m_1 \dots m_n, \dots, 1) = (1, \dots, 1) \pmod{\overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)}$ and therefore $(m_1, \dots, m_n)$ is in $\overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)$, as desired.

We now show that $f(\widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2)) \subset \overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)$. It suffices to check that $f(\widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^v)) \subset \overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2^v)$ for any $v \in \Omega_k$. For $i = 1, \dots, n$, let $\widetilde{G} = \bigcup_{t=1}^{r_{v,i}} \widetilde{H_i} \widetilde{x}_{i,t} \widetilde{S}_v$ be a double coset decomposition of $\widetilde{G}$ and recall that, by definition, the group $\widetilde{H}_{i,w}$ equals $\widetilde{H_i} \cap \widetilde{x}_{i,t} \widetilde{S}_v \widetilde{x}_{i,t}^{-1}$ if $w \in \Omega_{K_i}$ corresponds to the double coset $\widetilde{H_i} \widetilde{x}_{i,t} \widetilde{S}_v$. Let $\alpha = \bigoplus_{i=1}^{n} \bigoplus_{t=1}^{r_{v,i}} \widetilde{h}_{i,t} \in \operatorname{Ker} \widetilde{\psi}_2^v$, where $\widetilde{h}_{i,t} \in \widetilde{H}_{i,w}$ for all possible i, t. We thus have

$$\widetilde{\psi}_2(\alpha) = \prod_{i=1}^{n} \prod_{t=1}^{r_{v,i}} \widetilde{x}_{i,t}^{-1} \widetilde{h}_{i,t} \widetilde{x}_{i,t} \in [\widetilde{S}_v, \widetilde{S}_v]. \tag{8.2.4}$$

For any $i = 1, \dots, n$ define $\widetilde{h}_i = \prod_{t=1}^{r_{v,i}} \widetilde{h}_{i,t}$. We need to show that $f(\widetilde{h}_1, \dots, \widetilde{h}_n)$ is in $\overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2^v)$.

Set $x_{i,t} := \widetilde{\lambda}(\widetilde{x}_{i,t}) \in G$ and $h_{i,t} := \widetilde{\lambda}(\widetilde{h}_{i,t}) \in H_i \cap x_{i,t} D_v x_{i,t}^{-1}$ for all possible i, t. We have $\prod_{i=1}^{n} \prod_{t=1}^{r_{v,i}} x_{i,t}^{-1} h_{i,t} x_{i,t} \in [D_v, D_v]$. Let $\overline{x}_{i,t} \in \overline{G}$ be such that $\overline{\lambda}(\overline{x}_{i,t}) = x_{i,t}$ and $\overline{h}_{i,t} \in \overline{H}_i \cap \overline{x}_{i,t} \overline{D_v} \overline{x}_{i,t}^{-1}$ satisfying $\overline{\lambda}(\overline{h}_{i,t}) = h_{i,t}$. Multiplying one of the $\overline{h}_{1,t}$ by an element of $\overline{M}$ if necessary, we can assure that

$$\prod_{i=1}^{n} \prod_{t=1}^{r_{v,i}} \overline{x}_{i,t}^{-1} \overline{h}_{i,t} \overline{x}_{i,t} \in [\overline{D_v}, \overline{D_v}]. \tag{8.2.5}$$

In particular, $\alpha' := \bigoplus_{i=1}^{n} \bigoplus_{t=1}^{r_{v,i}} \overline{h}_{i,t}$ is in $\operatorname{Ker} \overline{\psi}_2^v$. Defining $\overline{h}_i := \prod_{t=1}^{r_{v,i}} \overline{h}_{i,t}$ for $i = 1, \dots, n$, we get $\overline{\varphi_1}(\alpha') = (\overline{h}_1, \dots, \overline{h}_n)$. We have $\widetilde{\lambda}(\widetilde{h}_i) = \overline{\lambda}(\overline{h}_i)$ by construction and therefore

$$\tau(\widetilde{h}_1 \dots \widetilde{h}_n) = \overline{h}_1 \dots \overline{h}_n m$$

for some $m \in \overline{M}$. We prove that m is also in $[\overline{D_v}, \overline{D_v}]$ so that, by multiplying one of the elements $\overline{h}_{1,t}$ by $m^{-1} \in \overline{M} \cap [\overline{D_v}, \overline{D_v}]$ if necessary (note that doing so does not change condition (8.2.5)), we obtain $f(\widetilde{h}_1, \dots, \widetilde{h}_n) = (\overline{h}_1, \dots, \overline{h}_n)$. As $(\overline{h}_1, \dots, \overline{h}_n)$ is in $\overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2^{v})$, this proves the claim.

Note that

$$\prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} \widetilde{h}_{i,t} = (\prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} \widetilde{h}_{i,t})(\prod_{i=n}^{1}\prod_{t=r_{v,i}}^{1} \widetilde{x}_{i,t}^{-1}\widetilde{h}_{i,t}^{-1}\widetilde{x}_{i,t})\widetilde{\psi}_2(\alpha).$$

Denote $(\prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} \widetilde{h}_{i,t})(\prod_{i=n}^{1}\prod_{t=r_{v,i}}^{1} \widetilde{x}_{i,t}^{-1}\widetilde{h}_{i,t}^{-1}\widetilde{x}_{i,t})$ by β. Then $\beta \in [\widetilde{G}, \widetilde{G}]$ and using an explicit description of β as a product of commutators and Lemma 8.2.2(ii), we deduce that $\tau(\beta) = \beta'$, where $\beta' = (\prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} \overline{h}_{i,t})(\prod_{i=n}^{1}\prod_{t=r_{v,i}}^{1} \overline{x}_{i,t}^{-1}\overline{h}_{i,t}^{-1}\overline{x}_{i,t})$. Therefore, we have

$$\prod_{i=1}^{n} \overline{h}_i = \prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} \overline{h}_{i,t} \equiv \beta' = \tau(\beta) \equiv \tau(\prod_{i=1}^{n} \widetilde{h}_i) \pmod{[\overline{D_v}, \overline{D_v}]},$$

and thus $m \in [\overline{D_v}, \overline{D_v}]$, as desired.

Claim 2: f is a homomorphism.

Proof: Let $h = (\widetilde{h}_1, \dots, \widetilde{h}_n), h' = (\widetilde{h}'_1, \dots, \widetilde{h}'_n) \in \operatorname{Ker} \widetilde{\psi}_1$ and write $f(h) = (\overline{h}_1, \dots, \overline{h}_n)$ and $f(h') = (\overline{h}'_1, \dots, \overline{h}'_n)$ for some elements $\overline{h}_i, \overline{h}'_i \in \overline{H_i}$. We have $f(h)f(h') = (\overline{h}_1\overline{h}'_1, \dots, \overline{h}_n\overline{h}'_n)$. On the other hand, $hh' = (\widetilde{h}_1\widetilde{h}'_1, \dots, \widetilde{h}_n\widetilde{h}'_n)$ and

$$\tau(\widetilde{h}_1\widetilde{h}'_1 \dots \widetilde{h}_n\widetilde{h}'_n) \equiv \tau((\widetilde{h}_1 \dots \widetilde{h}_n)(\widetilde{h}'_1 \dots \widetilde{h}'_n)) = (\overline{h}_1 \dots \overline{h}_n)(\overline{h}'_1 \dots \overline{h}'_n) \equiv \overline{h}_1\overline{h}'_1 \dots \overline{h}_n\overline{h}'_n \pmod{[\overline{G}, \overline{G}]}.$$

Since $\widetilde{\lambda}(\widetilde{h}_i\widetilde{h}'_i) = \overline{\lambda}(\overline{h}_i\overline{h}'_i)$ for all $i = 1, \dots, n$ and $(\overline{h}_1 \dots \overline{h}_n)(\overline{h}'_1 \dots \overline{h}'_n) \in [\overline{G}, \overline{G}]$, by the definition of f it follows that $f(hh') = (\overline{h}_1\overline{h}'_1, \dots, \overline{h}_n\overline{h}'_n) = f(h)f(h')$.

Claim 3: f is surjective.

Proof: For $i = 1, \dots, n$, let $\overline{h}_i \in \overline{H_i}$ be such that $\overline{h}_1 \dots \overline{h}_n \in [\overline{G}, \overline{G}]$. Take any elements $\widetilde{h}_i \in \widetilde{H_i}$ satisfying $\widetilde{\lambda}(\widetilde{h}_i) = \overline{\lambda}(\overline{h}_i)$. As above, by Lemma 8.2.2(i) this implies that there exists $m \in \overline{M}$ such that

$$\tau(\widetilde{h}_1 \dots \widetilde{h}_n) = \overline{h}_1 \dots \overline{h}_n m \in [\overline{G}, \overline{G}].$$

Since $\overline{h}_1 \dots \overline{h}_n \in [\overline{G}, \overline{G}]$, we have $m \in \overline{M} \cap [\overline{G}, \overline{G}]$. But $\overline{M} \cap [\overline{G}, \overline{G}] = \tau(\widetilde{M} \cap [\widetilde{G}, \widetilde{G}])$ by Lemma 8.2.2. Therefore $m = \tau(m')$ for some $m' \in \widetilde{M} \cap [\widetilde{G}, \widetilde{G}]$ and thus $(\overline{h}_1, \dots, \overline{h}_n) = f(\widetilde{h}_1, \dots, \widetilde{h}_n m'^{-1})$.

Claim 4: f is an isomorphism.

Proof: We have seen that f is surjective. Now we can analogously define a surjective map from $\operatorname{Ker} \overline{\psi}_1 / \overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)$ to $\operatorname{Ker} \widetilde{\psi}_1 / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2)$. It follows that the finite groups $\operatorname{Ker} \widetilde{\psi}_1 / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2)$ and $\operatorname{Ker} \overline{\psi}_1 / \overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)$ have the same size and so f is an isomorphism. □

Using this theorem, one can also obtain descriptions of the birational invariant $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ and the defect of weak approximation $A(T)$ for the multinorm one torus T:

Theorem 8.2.6. *Let T be the multinorm one torus associated with K and let X be a smooth compactification of T. In the notation of diagram (8.2.2), we have*

$$Ш(T) \cong \operatorname{Ker} \widetilde{\psi}_1 / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2),$$

$$\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^\sim \cong \operatorname{Ker} \widetilde{\psi}_1 / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^{nr}),$$

$$A(T) \cong \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2) / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^{nr}).$$

Proof. The first isomorphism is the statement of Theorem 8.2.5 (recall that $Ш(T)$ is isomorphic to $\mathfrak{K}(K, k)$). In order to show the second isomorphism, let L'/k' be an unramified Galois extension with Galois group G (such an extension always exists by [32]), let $K'_i = L'^{H_i}$ for $i = 1, \dots, n$ and let $K' = (K'_1, \dots, K'_n)$. Let T' be the multinorm one torus over k' associated with K' and let X' be a smooth compactification of T'. Note that $\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) \cong \mathrm{H}^1(k', \operatorname{Pic} \overline{X'})$ since $\widehat{T} \cong \widehat{T'}$ as G-modules. As L'/k' is unramified, by [91, Corollary 2] we have $A(T') = 0$ and thus Voskresenskiĭ's exact sequence of Theorem 1.5.8 gives $\mathrm{H}^1(k', \operatorname{Pic} \overline{X'})^\sim \cong Ш(T')$. The result follows since $Ш(T') \cong \operatorname{Ker} \widetilde{\psi}_1 / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^{nr})$ by the first isomorphism. Finally, in order to obtain the third isomorphism apply again Voskresenskiĭ's Theorem 1.5.8 and note that the surjection $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^\sim \twoheadrightarrow Ш(T)$ given in this theorem corresponds to the natural surjection $\operatorname{Ker} \widetilde{\psi}_1 / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^{nr}) \twoheadrightarrow \operatorname{Ker} \widetilde{\psi}_1 / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2)$ (this fact follows from an argument analogous to the one given in the Hasse norm principle case, see Theorem 4.3.11). □

Remark 8.2.7. As explained in Remark 8.1.8, all the groups $\operatorname{Ker} \widetilde{\psi}_1, \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2)$ and $\widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^{nr})$ in Theorem 8.2.6 can be computed in finite time. To this extent, we assembled a function in GAP [33] (whose code is available in [63]) that, given the relevant local and global Galois groups, outputs the obstructions to the multinorm principle and weak approximation for the multinorm one torus of a finite number of extensions by means of Theorem 8.2.6.

We end this section by generalizing Corollary 8.1.4 and proving a result (Proposition 8.2.9 below) showing that, in many situations, one can actually circumvent the use of generalized representation groups when computing the obstructions to the local-global principles.

For a moment, let G be any finite group and let H be a subgroup of G. Recall that the *focal subgroup of H in G* is defined as $\Phi^G(H) = \langle [h,x] \mid h \in H \cap xHx^{-1}, x \in G \rangle$. In [27, Theorem 2] (Theorem 4.3.8 of Chapter 4), we saw that

$$\varphi_1(\operatorname{Ker} \psi_2^{nr}) = \Phi^G(H)/[H,H]$$

in the setting of the first obstruction to the Hasse norm principle (case $n = 1$). Returning to the multinorm context, this fact promptly implies that, in the notation of diagram (8.2.2), we have

$$(1, \dots, \underbrace{\Phi^{\widetilde{G}}(\widetilde{H_i})}_{i\text{-th entry}}, 1, \dots, 1) \subset \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^{nr}). \tag{8.2.6}$$

for every $i = 1, \dots, n$.

Lemma 8.2.8. *Let G be a finite group and let G_p be a Sylow p-subgroup of G. Then $G_p \cap [G,G] \cap Z(G) \subset [G_p, G_p]$.*

Proof. To prove this lemma we will use the transfer homomorphism $v : G \to G_p/[G_p, G_p]$. This map has the property (see [51, Lemma 5.5]) that

$$v(g) = \prod_{i=1}^{r} t_i^{-1} g^{n_i} t_i [G_p, G_p], \tag{8.2.7}$$

for all $g \in G$, where t_i are elements of G such that $t_i^{-1} g^{n_i} t_i \in G_p$ for all i and n_i are integers such that $\sum_{i=1}^{r} n_i = [G : G_p]$.

Let $x \in G_p \cap [G,G] \cap Z(G)$. Since $\operatorname{Im}(v) \leq G_p/[G_p, G_p]$ is abelian, we have $[G,G] \leq \operatorname{Ker}(v)$ and thus $x \in \operatorname{Ker}(v)$, i.e. $v(x) \in [G_p, G_p]$. Since $x \in Z(G)$, by (8.2.7) we have $v(x) = x^{\sum_i n_i} = x^{[G:G_p]} \in [G_p, G_p]$. Finally, as the order of x is a power of p, we conclude that $x \in [G_p, G_p]$. □

Proposition 8.2.9. *Suppose that there exists $j \in \{1, \dots, n\}$ such that, for every prime p dividing $|\hat{\mathrm{H}}^{-3}(G, \mathbb{Z})|$, p^2 does not divide $[K_j : k]$. Then, in the notation of diagram (8.1.4), we have*

$$\text{Ш}(T) \cong \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2),$$
$$\mathrm{H}^1(k, \operatorname{Pic}\overline{X})^\sim \cong \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2^{nr}),$$
$$A(T) \cong \varphi_1(\operatorname{Ker}\psi_2)/\varphi_1(\operatorname{Ker}\psi_2^{nr}).$$

Proof. We prove only that $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})^\sim \cong \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2^{nr})$ (the other two isomorphisms can be obtained by a similar argument). Assume, without loss of generality, that $j = 1$ and $\widetilde{G}$ is a Schur covering group of G so that $\widetilde{M}$ is contained in $[\widetilde{G}, \widetilde{G}]$ and $\widetilde{M} \cong \hat{\mathrm{H}}^{-3}(G, \mathbb{Z})$. We show that the map

$$\begin{aligned} \rho\colon \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) &\longrightarrow \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2^{nr}) \\ h = (\widetilde{h}_1, \dots, \widetilde{h}_n) &\longmapsto (\widetilde{\lambda}(\widetilde{h}_1), \dots, \widetilde{\lambda}(\widetilde{h}_n)) \end{aligned}$$

is an isomorphism, which proves the desired statement by Theorem 8.2.6.

We first verify that ρ is well defined. It is enough to check that $\rho(\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^v)) \subset \varphi_1(\operatorname{Ker}\psi_2^v)$ for an unramified place v of L/k. Note that if $\widetilde{G} = \bigcup_{t=1}^{r_{v,i}} \widetilde{H}_i \widetilde{x}_{i,t} \widetilde{S}_v$ is a double coset decomposition of $\widetilde{G}$, then $G = \bigcup_{t=1}^{r_{v,i}} H_i x_{i,t} D_v$ is a double coset decomposition of G, where $x_{i,t} = \widetilde{\lambda}(\widetilde{x}_{i,t})$. From this observation, it is straightforward to verify that $\rho(\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^v)) \subset \varphi_1(\operatorname{Ker}\psi_2^v)$.

We now prove that ρ is surjective. Suppose that we are given, for $i = 1, \dots, n$, elements $h_i \in H_i$ such that $h_1 \dots h_n \in [G, G]$. Since $\widetilde{M} \subset [\widetilde{G}, \widetilde{G}]$, any choice of elements $\widetilde{h}_i \in \widetilde{H}_i$ such that $\widetilde{\lambda}(\widetilde{h}_i) = h_i$ will satisfy $\widetilde{h}_1 \dots \widetilde{h}_n \in [\widetilde{G}, \widetilde{G}]$ and thus $(h_1, \dots, h_n) = \rho(\widetilde{h}_1, \dots, \widetilde{h}_n)$.

We finally show that ρ is injective. Suppose that $(h_1, \dots, h_n) = \rho(h) \in \varphi_1(\operatorname{Ker}\psi_2^v)$ for some unramified place v of L/k. Write $h_i = \varphi_1(\bigoplus_{t=1}^{r_{v,i}} h_{i,t})$ for some elements $h_{i,t} \in H_i \cap x_{i,t} D_v x_{i,t}^{-1}$. As $(h_1, \dots, h_n) \in \varphi_1(\operatorname{Ker}\psi_2^v)$, we have $\prod_{i=1}^n \prod_{t=1}^{r_{v,i}} x_{i,t}^{-1} h_{i,t} x_{i,t} = 1$. Picking elements $\widetilde{h}_{i,t} \in \widetilde{\lambda}^{-1}(h_{i,t})$ and $\widetilde{x}_{i,t} \in \widetilde{\lambda}^{-1}(x_{i,t})$ for all possible i, t, we obtain $\prod_{i=1}^n \prod_{t=1}^{r_{v,i}} \widetilde{x}_{i,t}^{-1} \widetilde{h}_{i,t} \widetilde{x}_{i,t} = m$ for some $m \in \widetilde{M} = \operatorname{Ker}\widetilde{\lambda}$. As $m \in Z(\widetilde{G}) \cap \bigcap_{i=1}^n \widetilde{H}_i$, we have $(\widetilde{h}_1 m^{-1}, \widetilde{h}_2, , \dots, \widetilde{h}_n) \in \widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr})$.

Therefore, in order to prove that $h \in \widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr})$ it suffices to show that $(m^{-1}, 1, \ldots, 1) \in \widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr})$. We prove that $m \in \Phi^{\widetilde{G}}(\widetilde{H_1})$, which completes the proof by (8.2.6).

Claim: If p^2 does not divide $[K_1 : k]$ for every prime p dividing $|\widetilde{M}|$, then $\widetilde{M} \subset \Phi^{\widetilde{G}}(\widetilde{H_1})$.

Proof: We show that $\widetilde{M_{(p)}} \subset \Phi^{\widetilde{G}}(\widetilde{H_1})$. We have $[K_1 : k] = [G : H_1]$ and therefore $[G_p : (H_1)_p] = [\widetilde{G}_p : (\widetilde{H_1})_p] = 1$ or p. In any case, $(\widetilde{H_1})_p \trianglelefteq \widetilde{G}_p$ and we can write $\widetilde{G}_p = \langle x_p \rangle.(\widetilde{H_1})_p$ for some $x_p \in \widetilde{G}_p$. Since $\widetilde{M_{(p)}} \subset \widetilde{G}_p \cap [\widetilde{G}, \widetilde{G}] \cap Z(\widetilde{G})$ and $\widetilde{G}_p \cap [\widetilde{G}, \widetilde{G}] \cap Z(\widetilde{G}) \subset [\widetilde{G}_p, \widetilde{G}_p]$ by Lemma 8.2.8, we have $\widetilde{M_{(p)}} \subset [\widetilde{G}_p, \widetilde{G}_p]$ and so it suffices to prove that $[\widetilde{G}_p, \widetilde{G}_p] \subset \Phi^{\widetilde{G}}(\widetilde{H_1})$. Let $z = [x_p^a h_1, x_p^b h_1']$ for some $a, b \in \mathbb{Z}$ and $h_1, h_1' \in (\widetilde{H_1})_p$. Using the commutator properties, we have $z = [x_p^a, h_1']^{h_1}[h_1, h_1'][h_1, x_p^b]^{h_1'}$. As $(\widetilde{H_1})_p \trianglelefteq \widetilde{G}_p$ and $\Phi^{\widetilde{G}}(\widetilde{H_1}) \trianglelefteq \widetilde{H_1}$, it follows that each one of the commutators above is in $\Phi^{\widetilde{G}}(\widetilde{H_1})$. □

As a consequence we obtain the following result, which can be thought of as an analog of [27, Corollary 1] for the birational invariant $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})$.

Corollary 8.2.10. *Let K/k be an extension of number fields and suppose that $[K : k]$ is square-free. Let X be a smooth compactification of the norm one torus $R^1_{K/k}\mathbb{G}_m$. Then*

$$\mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim} \cong \frac{H \cap [G, G]}{\Phi^G(H)}.$$

Proof. The conditions of Proposition 8.2.9 are satisfied and therefore $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim} \cong \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2^{nr})$. The result then follows from the fact that $\operatorname{Ker}\psi_1 = (H \cap [G, G])/[H, H]$ and $\varphi_1(\operatorname{Ker}\psi_2^{nr}) = \Phi^G(H)/[H, H]$ (Theorem 4.3.8 of Chapter 4). □

Chapter 9

Applications

In this chapter we illustrate the scope of the techniques developed in Chapter 8 by investigating the multinorm principle and weak approximation for the multinorm one torus in three different situations. Namely, we extend results of Demarche–Wei [25], Pollio [76] and Bayer-Fluckiger–Lee–Parimala [5]. The notation used throughout this section is as in Chapter 8, except we now assume L/k to be the minimal Galois extension containing all the fields $K_1, \dots, K_n$. Additionally, we will make use of the norm one torus $S = R^1_{F/k}\mathbb{G}_m$ of the extension $F = \bigcap\limits_{i=1}^{n} K_i$ and we let Y denote a smooth compactification of S. We start by establishing two auxiliary lemmas to be used in later sections.

9.1 Two useful lemmas

Lemma 9.1.1. *In the notation of diagram (8.2.2), we have*

$$\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) \subseteq \{(h_1\widetilde{H_1}', \dots, h_n\widetilde{H_n}') \in \operatorname{Ker}\widetilde{\psi}_1 \mid h_1 \dots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})\}.$$

A proof of this lemma can be obtained by following the same strategy as in the proof of the analogous result for the Hasse norm principle (case $n = 1$) in [27, Theorem 2]. Nonetheless, as the details are slightly intricate, we include a proof here for the benefit of the reader.

Proof. Since $\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) = \prod_{\substack{v \in \Omega_k \\ v \text{ unramified}}} \widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{v})$, it suffices to prove that

$$\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{v}) \subseteq \{(h_1\widetilde{H_1}', \dots, h_n\widetilde{H_n}') \mid h_1 \dots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})\}$$

for any unramified place v of L/k. Let $\alpha \in \operatorname{Ker}\widetilde{\psi}_2^{v}$ and fix a double coset decomposition $\widetilde{G} = \bigcup_{t=1}^{r_{v,i}} \widetilde{H_i}\widetilde{x}_{i,t}\widetilde{S}_v$. Write $\widetilde{S}_v = \langle g \rangle$ and $\alpha = \bigoplus_{i=1}^{n}\bigoplus_{t=1}^{r_{v,i}} \widetilde{h}_{i,t}$ for some $g \in \widetilde{G}$, $\widetilde{h}_{i,t} = \widetilde{x}_{i,t}g^{e_{i,t}}\widetilde{x}_{i,t}^{-1} \in \widetilde{H_i} \cap \widetilde{x}_{i,t}\langle g \rangle \widetilde{x}_{i,t}^{-1}$ and some $e_{i,t} \in \mathbb{Z}$. By hypothesis, we have $1 = \widetilde{\psi}_2(\alpha) = g^{\sum_{i,t} e_{i,t}}$ and therefore

$$\sum_{i,t} e_{i,t} \equiv 0 \pmod{m},$$

where m is the order of g. Since $g^m = 1$, by changing some of the $e_{i,t}$ if necessary, we can (and do) assume that

$$\sum_{i,t} e_{i,t} = 0. \tag{9.1.1}$$

Letting $h_i = \prod_{t=1}^{r_{v,i}} \widetilde{h}_{i,t}$ for any $1 \leq i \leq n$, we have $\widetilde{\varphi}_1(\alpha) = (h_1\widetilde{H_1}, \dots, h_n\widetilde{H_n}) \in \operatorname{Ker}\widetilde{\psi}_1$. We prove that

$$\prod_{i=1}^{n} h_i = \prod_{i=1}^{n}(\prod_{t=1}^{r_{v,i}} \widetilde{h}_{i,t}) = \prod_{i=1}^{n}(\prod_{t=1}^{r_{v,i}} \widetilde{x}_{i,t}g^{e_{i,t}}\widetilde{x}_{i,t}^{-1}) \in \Phi^{\widetilde{G}}(\widetilde{H})$$

by induction on $s := \sum_{i=1}^{n} r_{v,i}$. The case $s = 1$ is trivial and the case $s = 2$ is solved as in the analogous result for the Hasse norm principle setting, see [27, p. 308]. Now let $s > 2$ and set $d = \gcd(e_{i,t} \mid 1 \leq i \leq n, 1 \leq t \leq r_{v,i})$ and $f_{i,t} = \frac{e_{i,t}}{d}$. It follows that $\gcd(f_{i,t} \mid 1 \leq i \leq n, 1 \leq t \leq r_{v,i}) = 1$ and, since $\sum_{i,t} f_{i,t} = 0$ by (9.1.1), we have $\gcd(f_{i,t} \mid 1 \leq i \leq n, 1 \leq t \leq r_{v,i} \text{ and } (i,t) \neq (n, r_{v,n})) = 1$. Hence there exist $a_{i,t} \in \mathbb{Z}$ such that $\sum_{\substack{i,t \\ (i,t) \neq (n,r_{v,n})}} f_{i,t}a_{i,t} = 1$. Consider the element

$$\beta = \Big(\bigoplus_{\substack{i,t \\ (i,t) \neq (n,r_{v,n})}} \widetilde{x}_{i,t}g^{e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{i,t}^{-1} \Big) \oplus \widetilde{x}_{n,r_{v,n}}g^{-e_{n,r_{v,n}}}\widetilde{x}_{n,r_{v,n}}^{-1} \in \bigoplus_{i=1}^{n} \Big(\bigoplus_{t=1}^{r_{v,i}} \widetilde{H}_{i,w} \Big).$$

Since $e_{i,t}f_{n,r_{v,n}} = e_{n,r_{v,n}}f_{i,t}$, we have

$$\widetilde{\psi}_2(\beta) = g^{\left(\sum\limits_{\substack{i,t\\(i,t)\neq(n,r_{v,n})}} e_{i,t}f_{n,r_{v,n}}a_{i,t}\right)-e_{n,r_{v,n}}} = g^{\left(\sum\limits_{\substack{i,t\\(i,t)\neq(n,r_{v,n})}} e_{n,r_{v,n}}f_{i,t}a_{i,t}\right)-e_{n,r_{v,n}}} = 1$$

and so $\beta \in \operatorname{Ker}\widetilde{\psi}_2^v$.

Additionally, if $\widetilde{\varphi}_1(\beta) = (\widetilde{h}_1, \dots, \widetilde{h}_n)$, we have

$$\begin{aligned}\prod_{i=1}^{n}\widetilde{h}_i &= \left(\prod_{\substack{i,t\\(i,t)\neq(n,r_{v,n})}} \widetilde{x}_{i,t}g^{e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{i,t}^{-1}\right)\widetilde{x}_{n,r_{v,n}}g^{-e_{n,r_{v,n}}}\widetilde{x}_{n,r_{v,n}}^{-1} = \\ &= \left(\prod_{\substack{i,t\\(i,t)\neq(n,r_{v,n})}} \widetilde{x}_{i,t}g^{e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{i,t}^{-1}\right)\widetilde{x}_{n,r_{v,n}}g^{-e_{n,r_{v,n}}\sum\limits_{\substack{i,t\\(i,t)\neq(n,r_{v,n})}} f_{i,t}a_{i,t}}\widetilde{x}_{n,r_{v,n}}^{-1} \equiv \\ &\equiv \left(\prod_{\substack{i,t\\(i,t)\neq(n,r_{v,n})}} \widetilde{x}_{i,t}g^{e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{i,t}^{-1}\widetilde{x}_{n,r_{v,n}}g^{-e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{n,r_{v,n}}^{-1}\right) \pmod{[\widetilde{H},\widetilde{H}]}\end{aligned} \tag{9.1.2}$$

since the elements $\widetilde{x}_{i,t}g^{e_{i,t}}\widetilde{x}_{i,t}^{-1}$ (for all possible i,t) are in $\widetilde{H}$.

We claim that $\prod_{i=1}^{n}\widetilde{h}_i \in \Phi^{\widetilde{G}}(\widetilde{H})$. To show this note that the elements $\widetilde{x}_{i,t}g^{e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{i,t}^{-1}$ and $\widetilde{x}_{n,r_{v,n}}g^{-e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{n,r_{v,n}}^{-1}$ are in $\widetilde{H}$ and so $\widetilde{x}_{i,t}g^{e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{i,t}^{-1} \in \widetilde{H}\cap(\widetilde{x}_{i,t}\widetilde{x}_{n,r_{v,n}}^{-1})\widetilde{H}(\widetilde{x}_{n,r_{v,n}}\widetilde{x}_{i,t}^{-1})$. We thus see that $\widetilde{x}_{i,t}g^{e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{i,t}^{-1}\widetilde{x}_{n,r_{v,n}}g^{-e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{n,r_{v,n}}^{-1} = [\widetilde{x}_{i,t}g^{-e_{i,t}f_{n,r_{v,n}}a_{i,t}}\widetilde{x}_{i,t}^{-1}, \widetilde{x}_{i,t}\widetilde{x}_{n,r_{v,n}}^{-1}]$ is in $\Phi^{\widetilde{G}}(\widetilde{H})$ for all i,t such that $(i,t) \neq (n, r_{v,n})$ and from (9.1.2) we deduce that $\prod_{i=1}^{n}\widetilde{h}_i \in \Phi^{\widetilde{G}}(\widetilde{H})$.

Finally, we prove that $h_1 \dots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})$ as well. Consider the element

$$\alpha' = \alpha\beta = \bigoplus_{\substack{i,t\\(i,t)\neq(n,r_{v,n})}} \widetilde{x}_{i,t}g^{e_{i,t}(1+f_{n,r_{v,n}}a_{i,t})}\widetilde{x}_{i,t}^{-1} \in \bigoplus_{i=1}^{n}\Big(\bigoplus_{t=1}^{r_{v,i}}\widetilde{H}_{i,w}\Big).$$

It is clear that α', being the product of two elements in $\operatorname{Ker}\widetilde{\psi}_2^v$, is also in this set. By the induction hypothesis, if $\widetilde{\varphi}_1(\alpha') = (\widehat{h}_1, \dots, \widehat{h}_n)$ we have $\widehat{h}_1 \dots \widehat{h}_n \in \Phi^{\widetilde{G}}(\widetilde{H})$. Since $\widehat{h}_i \equiv h_i\widetilde{h}_i$ $(\mathrm{mod}\ [\widetilde{H}, \widetilde{H}])$ for all $i = 1, \dots, n$, we conclude that $h_1 \dots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})$. □

Lemma 9.1.2. *(i) There exists a surjection* $f : \mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim} \to \mathrm{H}^1(k, \operatorname{Pic}\overline{Y})^{\sim}$. *If in addition*

$$\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) \supseteq \{(h_1\widetilde{H_1}', \dots, h_n\widetilde{H_n}') \mid h_1 \dots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})\}$$

(in the notation of diagram (8.2.2)), then f is an isomorphism.

(ii) If F/k is Galois, f induces a surjection $\text{Ш}(T) \twoheadrightarrow \text{Ш}(S)$.

Proof. Consider the analog of diagram (8.2.2) for the extension F/k (note that this is the fixed field of the group H inside L/k):

$$\begin{tikzcd}
\widetilde{H}^{\mathrm{ab}} \arrow[r, "\widehat{\psi}_1"] & \widetilde{G}^{\mathrm{ab}} \\
\bigoplus_{v \in \Omega_k} \Big(\bigoplus_{w|v} \widetilde{H}_w^{\mathrm{ab}}\Big) \arrow[u, "\widehat{\varphi}_1"] \arrow[r, "\widehat{\psi}_2"] & \bigoplus_{v \in \Omega_k} \widetilde{S}_v^{\mathrm{ab}} \arrow[u, "\widehat{\varphi}_2"']
\end{tikzcd}$$

(9.1.3)

Here all the maps with the $\widehat{\ }$ notation are defined as in diagram (8.2.2) with respect to the extension F/k. Now define

$$\begin{aligned} f\colon\ \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) &\longrightarrow \operatorname{Ker}\widehat{\psi}_1/\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr}) \\ (\widetilde{h}_1\widetilde{H_1}', \dots, \widetilde{h}_n\widetilde{H_n}')\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) &\longmapsto (\widetilde{h}_1 \dots \widetilde{h}_n[\widetilde{H}, \widetilde{H}])\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr}) \end{aligned}$$

Since $\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr}) = \Phi^{\widetilde{G}}(\widetilde{H})/[\widetilde{H}, \widetilde{H}]$ (see [27, Theorem 2] or Theorem 4.3.8), the map f is well defined by Lemma 9.1.1. Additionally, as the target group is abelian, it is easy to check that f is a homomorphism and surjective. By Theorem 8.2.6 we have $\mathrm{H}^1(k, \operatorname{Pic}\overline{X})^{\sim} \cong \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr})$ and $\mathrm{H}^1(k, \operatorname{Pic}\overline{Y})^{\sim} \cong \operatorname{Ker}\widehat{\psi}_1/\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr})$. The statement in the first sentence follows. Finally, if we assume $\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) \supseteq \{(h_1\widetilde{H_1}', \dots, h_n\widetilde{H_n}') \mid h_1 \dots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})\}$, then it is clear that f is injective.

We now prove (ii). By Theorem 8.2.6, it is enough to show that $f(\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2)) \subset \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2)$. Since $\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2) = \prod_{v \in \Omega_k} \widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^v)$, it suffices to verify $f(\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^v)) \subset \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2)$ for all $v \in \Omega_k$. Let $\alpha \in \operatorname{Ker}\widetilde{\psi}_2^v$ and write $\alpha = \bigoplus_{i=1}^{n}\bigoplus_{t=1}^{r_{v,i}} \widetilde{h}_{i,t}$ for some $\widetilde{h}_{i,t} \in$

$\widetilde{H_i} \cap \widetilde{x}_{i,t}\widetilde{S}_v\widetilde{x}_{i,t}^{-1}$. Hence, we obtain $\widetilde{\varphi}_1(\alpha) = (\widetilde{h}_1, \dots, \widetilde{h}_n)$, where $\widetilde{h}_i = \prod_{t=1}^{r_{v,i}} \widetilde{h}_{i,t}$, and we wish to show that $\prod_{i=1}^{n} \widetilde{h}_i \in \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2)$. Since F/k is Galois, $\widetilde{H}$ is a normal subgroup of $\widetilde{G}$ and thus $\Phi^{\widetilde{G}}(\widetilde{H}) = [\widetilde{H}, \widetilde{G}]$. In this way, we have

$$\prod_{i=1}^{n} \widetilde{h}_i = \prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} \widetilde{h}_{i,t} \equiv \prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} \widetilde{x}_{i,t}^{-1}\widetilde{h}_{i,t}\widetilde{x}_{i,t} = \widetilde{\psi}_2(\alpha) \pmod{\Phi^{\widetilde{G}}(\widetilde{H})}.$$

As $\Phi^{\widetilde{G}}(\widetilde{H})/[\widetilde{H}, \widetilde{H}] = \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr})$, it suffices to prove that $\widetilde{\psi}_2(\alpha) \in \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{v})$. For this, let $\widetilde{G} = \bigcup_{j=1}^{r} \widetilde{H}\widetilde{y}_j\widetilde{S}_v$ be a double coset decomposition and suppose, without loss of generality, that $\widetilde{y}_{j_0} = 1$ for some index $1 \leq j_0 \leq r$ corresponding to a place w_0 of F via Lemma 8.1.6. Therefore, we obtain $\widetilde{\psi}_2(\alpha) = \prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} \widetilde{x}_{i,t}^{-1}\widetilde{h}_{i,t}\widetilde{x}_{i,t} \in \widetilde{H} \cap \widetilde{S}_v = \widetilde{H}_{w_0}$ since $\widetilde{x}_{i,t}^{-1}\widetilde{h}_{i,t}\widetilde{x}_{i,t} \in \widetilde{H}$ for all possible i, t. In this way, if $\beta \in \bigoplus_{v \in \Omega_k} (\bigoplus_{w|v} \widetilde{H}_w^{\mathrm{ab}})$ is the vector with the (v, w_0)-th entry equal to $\widetilde{\psi}_2(\alpha)$ and all other entries equal to 1, we have $\widehat{\psi}_2(\beta) = \widetilde{\psi}_2(\alpha) \in [\widetilde{S}_v, \widetilde{S}_v]$ (as $\alpha \in \operatorname{Ker}\widetilde{\psi}_2^{v}$) and so $\widetilde{\psi}_2(\alpha) = \widehat{\varphi}_1(\beta) \in \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{v})$. □

9.2 Linearly disjoint extensions

In this section we prove a theorem similar to the main result of [25], but with a slightly different hypothesis (and in some cases more general, see Remark 9.2.2 below).

Theorem 9.2.1. *For any non-empty subset $I \subset \{1, \dots, n\}$, let $K_I \subseteq L$ be the compositum of the fields K_i $(i \in I)$ and let E_I be the Galois closure of K_I/k. Suppose that there exist indices $i_0, j_0 \in \{1, \dots, n\}$ such that, for every $1 \leq i \leq n$, there is a partition $I_i \sqcup J_i = \{1, \dots, n\}$ with $i_0 \in I_i, j_0 \in J_i$ and $E_{I_i} \cap E_{J_i} \subseteq K_i$. Then*

$$\mathrm{H}^1(k, \operatorname{Pic}\overline{X}) \cong \mathrm{H}^1(k, \operatorname{Pic}\overline{Y}).$$

Proof. If $n = 1$ there is nothing to show, so assume $n \geq 2$. By Lemma 9.1.2(i) it suffices to prove that

$$\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) \supseteq \{(h_1\widetilde{H_1}', \dots, h_n\widetilde{H_n}') \mid h_1 \dots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})\}.$$

Let $\alpha = (h_1\widetilde{H_1}', \ldots, h_n\widetilde{H_n}')$ be such that $h_1 \ldots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})$. Renaming the fields K_i if necessary, we assume that $i_0 = 1$ and $j_0 = 2$. Denoting $B_{I_i} = \mathrm{Gal}(L/E_{I_i}), B_{J_i} = \mathrm{Gal}(L/E_{J_i})$ for all $1 \leq i \leq n$, the hypothesis $E_{I_i} \cap E_{J_i} \subseteq K_i$ is equivalent to $B_{I_i}B_{J_i} \supseteq H_i$ and thus

$$\widetilde{H_i} \subseteq \widetilde{B_{I_i}}\widetilde{B_{J_i}} \tag{9.2.1}$$

with $1 \in I_i$, $2 \in J_i$ and $i \in I_i$ or J_i. If $n \geq 3$, this implies that for any $3 \leq i \leq n$ we can decompose $h_i = h_{1,i}h_{2,i}$ for some $h_{1,i} \in \widetilde{H_1} \cap \widetilde{H_i}$ and $h_{2,i} \in \widetilde{H_2} \cap \widetilde{H_i}$. Using Lemma 8.2.4 as done in Claim 1 of the proof of Theorem 8.2.5, we obtain

$$\alpha \equiv ((\prod_{3\leq i\leq n} h_{1,i})h_1, (\prod_{3\leq i\leq n} h_{2,i})h_2, 1, \ldots, 1)$$

modulo $\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{nr})$. We can thus assume α to be of the form $(h_1', h_2', 1, \ldots, 1)$ for some $h_1' \in \widetilde{H_1}, h_2' \in \widetilde{H_2}$ such that $h_1'h_2' \in \Phi^{\widetilde{G}}(\widetilde{H})$. Note that (9.2.1) implies that $\widetilde{H} = \langle\widetilde{H_i}\rangle \subset \widetilde{B_1}\widetilde{B_2}$, where $B_1 = \mathrm{Gal}(L/E_{\{1\}})$ and $B_2 = \mathrm{Gal}(L/E_{\{2\}})$. It thus follows that $\Phi^{\widetilde{G}}(\widetilde{H}) \subset \Phi^{\widetilde{G}}(\widetilde{B_1}\widetilde{B_2}) = \Phi^{\widetilde{G}}(\widetilde{B_1})\Phi^{\widetilde{G}}(\widetilde{B_2})$ and so $h_1'h_2' \in \Phi^{\widetilde{G}}(\widetilde{B_1})\Phi^{\widetilde{G}}(\widetilde{B_2})$. Since $\Phi^{\widetilde{G}}(\widetilde{B_i}) \subset \Phi^{\widetilde{G}}(\widetilde{H_i})$ and recalling that

$$(1, \ldots, \underbrace{\Phi^{\widetilde{G}}(\widetilde{H_i})}_{i\text{-th entry}}, 1, \ldots, 1) \subset \widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{nr})$$

(see (8.2.6) in Section 8.2), we can multiply h_1' and h_2' by elements of $\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{nr})$ to attain $\alpha \equiv (h_1'', h_2'', 1, \ldots, 1) \pmod{\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{nr})}$ for some $h_1'' \in \widetilde{H_1}, h_2'' \in \widetilde{H_2}$ such that $h_1''h_2'' = 1$. Thus $h_2'' = h_1''^{-1}$ and $\alpha = (h_1'', h_1''^{-1}, 1, \ldots, 1)$, which by Lemma 8.2.4 is in $\widetilde{\varphi}_1(\mathrm{Ker}\,\widetilde{\psi}_2^{nr})$, as desired. □

Remark 9.2.2. It is easy to see that if there exists a partition $I \sqcup J = \{1, \ldots, n\}$ such that $E_I \cap E_J = F$ (the assumption in [25, Theorem 6] when $F_i = E_I$ and $F_j = E_J$ for every $i \in I, j \in J$), the conditions of Theorem 9.2.1 are satisfied. Therefore, our theorem applies to all the cases described in [25, Examples 9(i), (ii) and (iii)]. Moreover, our hypothesis applies for n-tuples of fields for which the assumptions in [25, Theorem 6] might fail. For example, let $K = (\mathbb{Q}(\sqrt{2}, \sqrt{3}), \mathbb{Q}(\sqrt{2}, \sqrt{5}), \mathbb{Q}(\sqrt{3}, \sqrt{5}))$. It is easy to see that the assumptions of Theorem 9.2.1 are satisfied, but [25, Theorem 6] does not apply to this tuple of fields. Indeed, Demarche and Wei's hypothesis imply that there is a partition $I \sqcup J = \{1, \ldots, n\}$ such that $K_I \cap K_J = F$, which does not exist in the example above.

As consequence of Theorem 9.2.1 and Lemma 9.1.2(ii) we also obtain versions of [25, Corollaries 7 and 8]:

Corollary 9.2.3. *Let $c \in k^*$. Assume the hypothesis of Theorem 9.2.1 and that F/k is Galois. Suppose that the k-variety $N_{F/k}(\Xi) = c$ satisfies weak approximation. Then the k-variety $\prod_{i=1}^{n} N_{K_i/k}(\Xi_i) = c$ satisfies weak approximation if and only if it has a k-point.*

Corollary 9.2.4. *Assume the hypothesis of Theorem 9.2.1 and suppose that the Hasse principle and weak approximation hold for all norm equations $N_{F/k}(\Xi) = c$, $c \in k^*$. Then the Hasse principle and weak approximation hold for all multinorm equations $\prod_{i=1}^{n} N_{K_i/k}(\Xi_i) = c$.*

9.3 Abelian extensions

In this subsection we generalize the main theorem of [76] to n abelian extensions under the conditions of Theorem 9.2.1.

Theorem 9.3.1. *Let $K = (K_1, \ldots, K_n)$ be an n-tuple of abelian extensions of k and suppose that the conditions of Theorem 9.2.1 are satisfied for K. Then*

$$Ш(T) \cong Ш(S) \text{ and } A(T) \cong A(S).$$

Proof. Note that if $A(T) \cong A(S)$, then by Theorem 9.2.1 and Voskresenskiĭ's exact sequence of Theorem 1.5.8 we deduce that $|Ш(T)| = |Ш(S)|$. Since $Ш(T)$ surjects onto $Ш(S)$ by Lemma 9.1.2(ii), we conclude that $Ш(T) \cong Ш(S)$. Therefore, it is enough to prove that $A(T) \cong A(S)$.

Let us again consider the analog of diagram (8.2.2) for the extension F/k:

$$\begin{tikzcd}
\widetilde{H}^{\mathrm{ab}} \arrow[r, "\widehat{\psi}_1"] & \widetilde{G}^{\mathrm{ab}} \\
\bigoplus\limits_{v \in \Omega_k} \Big(\bigoplus\limits_{w|v} \widetilde{H}_w^{\mathrm{ab}}\Big) \arrow[u, "\widehat{\varphi}_1"] \arrow[r, "\widehat{\psi}_2"] & \bigoplus\limits_{v \in \Omega_k} \widetilde{S}_v^{\mathrm{ab}} \arrow[u, "\widehat{\varphi}_2"']
\end{tikzcd} \tag{9.3.1}$$

As before, in this diagram all the maps with the $\widehat{}$ superscript are defined as in diagram (8.2.2) with respect to F/k. By Theorem 8.2.6, we have $A(T) \cong \widetilde{\varphi}_1(\mathrm{Ker}\, \widetilde{\psi}_2)/\widetilde{\varphi}_1(\mathrm{Ker}\, \widetilde{\psi}_2^{nr})$ (in the notation of diagram (8.2.2)) and $A(S) \cong \widehat{\varphi}_1(\mathrm{Ker}\, \widehat{\psi}_2)/\widehat{\varphi}_1(\mathrm{Ker}\, \widehat{\psi}_2^{nr})$ (in the notation of diagram (9.3.1)). Therefore it suffices to show that $\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2)/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr})$ is isomorphic to $\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2)/\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr})$. For this, we again consider the natural map

$$\begin{aligned} f\colon \widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2)/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) &\longrightarrow \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2)/\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr}) \\ (\widetilde{h}_1\widetilde{H_1}',\dots,\widetilde{h}_n\widetilde{H_n}')\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) &\longmapsto (\widetilde{h}_1\dots\widetilde{h}_n[\widetilde{H},\widetilde{H}])\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr}) \end{aligned}$$

In the proof of Lemma 9.1.2(ii) it was shown that $f(\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2)) \subset \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2)$. Additionally, recalling that $\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr}) = \Phi^{\widetilde{G}}(\widetilde{H})/[\widetilde{H},\widetilde{H}]$ by Theorem 4.3.8 of Chapter 4, we have $f(\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr})) = \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr})$ by Lemma 9.1.1 and the proof of Theorem 9.2.1. This shows that f is well defined and injective.

Finally, let us check that f is surjective. Fix a place v of k and a double coset decomposition $\widetilde{G} = \bigcup_{j=1}^{r} \widetilde{H}\widetilde{y}_j\widetilde{D}_v$ and let $\alpha \in \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{v})$. We can write $\alpha = \widehat{\varphi}_1(\bigoplus_{j=1}^{r}\widetilde{h}_j) = \prod_{j=1}^{r}\widetilde{h}_j$ for some $\widetilde{h}_j \in \widetilde{H} \cap \widetilde{y}_j\widetilde{S}_v\widetilde{y}_j^{-1}$ such that $\beta := \widehat{\psi}_2(\bigoplus_{j=1}^{r}\widetilde{h}_j) = \prod_{j=1}^{r}\widetilde{y}_j^{-1}\widetilde{h}_j\widetilde{y}_j$ is in $[\widetilde{S}_v,\widetilde{S}_v]$. Note that as G is abelian, we have $[\widetilde{G},\widetilde{G}] \subset \operatorname{Ker}\widetilde{\lambda} = \widetilde{M}$ and therefore $[\widetilde{S}_v,\widetilde{S}_v] \subset \widetilde{M} \subset \widetilde{H}_i$ for every $1 \leq i \leq n$. In particular, we have $\beta \in \widetilde{H}_1 \cap \widetilde{S}_v$ and from this one readily checks that the n-tuple $(\beta,1,\dots,1)$ is in $\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{v})$. Since $\widetilde{H} \trianglelefteq \widetilde{G}$, we have $\Phi^{\widetilde{G}}(\widetilde{H}) = [\widetilde{H},\widetilde{G}]$ and thus $f(\beta,1,\dots,1) = \beta = \prod_j \widetilde{y}_j^{-1}\widetilde{h}_j\widetilde{y}_j \equiv \prod_j \widetilde{h}_j = \alpha \pmod{\Phi^{\widetilde{G}}(\widetilde{H})}$. As $\Phi^{\widetilde{G}}(\widetilde{H})/[\widetilde{H},\widetilde{H}] = \widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr})$, we obtain $\alpha = f(\beta,1,\dots,1)$ inside $\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2)/\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr})$. □

Remark 9.3.2. Note that the conditions of Theorem 9.2.1 are always satisfied if $n = 2$, so that Theorem 9.3.1 generalizes the main theorem of [76].

9.4 Products of cyclic extensions of prime degree

In this subsection we extend the result in [5, Theorem 8.3] to include the weak approximation property for the multinorm one torus of n cyclic extensions of prime degree p.

Theorem 9.4.1. *Let $K_1,\dots,K_n$ be non-isomorphic cyclic extensions of k with prime degree p. Then, we have*

$$\mathrm{H}^1(k,\operatorname{Pic}\overline{X}) = \begin{cases} (\mathbb{Z}/p)^{n-2}, \textit{ if } [K_1\dots K_n : k] = p^2; \\ 0, \textit{ otherwise.} \end{cases}$$

Proof. The case $n = 1$ was proved in [21, Proposition 9.1] and for $n = 2$ the result follows from Theorem 9.2.1, so assume $n \geq 3$.

Suppose first that $[K_1 \ldots K_n : k] > p^2$. Reordering the fields $K_3, \ldots, K_n$ if necessary, we can (and do) assume that each one of the fields $K_1, \ldots, K_{s-1}$ is contained in K_1K_2 (for some $3 \leq s \leq n$), while none of $K_s, \ldots, K_n$ is contained in K_1K_2. We prove two auxiliary claims:

Claim 1: $\widetilde{H_i} \subset (\widetilde{H_1} \cap \widetilde{H_i}).\widetilde{H_s}$ for any $i = 1, \ldots, s-1$.

Proof: Observe that $K_1K_i \cap K_s = k$ as otherwise we would have $K_s \subset K_1K_i \subset K_1K_2$, contradicting the assumption on s. Therefore $K_i \supset k = K_1K_i \cap K_s$ and passing to subgroups this implies that $H_i \subset (H_1 \cap H_i).H_s$, from which the claim follows.

Claim 2: $\widetilde{H_i} \subset (\widetilde{H_1} \cap \widetilde{H_i}).\widetilde{H_2}$ for any $i = s, \ldots, n$.

Proof: Observe that $K_2 \not\subset K_1K_i$ as otherwise we would have $K_i \subset K_1K_i = K_1K_2$, contradicting the assumption on K_i. Therefore $K_i \supset k = K_1K_i \cap K_2$ and passing to subgroups this implies that $H_i \subset (H_1 \cap H_i).H_2$, from which the claim follows.

Let us now prove that $\mathrm{H}^1(k, \operatorname{Pic} \overline{X}) = 0$. Since $\bigcap\limits_i K_i = k$, by Lemma 9.1.2(i) it suffices to show that

$$\widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^{nr}) \supseteq \{(h_1\widetilde{H_1}', \ldots, h_n\widetilde{H_n}') \mid h_1 \ldots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})\}.$$

Let $\alpha = (h_1\widetilde{H_1}', \ldots, h_n\widetilde{H_n}')$ be such that $h_1 \ldots h_n \in \Phi^{\widetilde{G}}(\widetilde{H})$. By Claim 1 above, for $i = 3, \ldots, s-1$ we can write $h_i = h_{1,i}h_{s,i}$, where $h_{1,i} \in \widetilde{H_1} \cap \widetilde{H_i}$ and $h_{s,i} \in \widetilde{H_s} \cap \widetilde{H_i}$. Using this decomposition, we can apply Lemma 8.2.4 as done in the proof of Theorem 9.2.1 in order to simplify α modulo $\widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^{nr})$ and assume it has the form $(h_1', h_2, 1, \ldots, 1, h_s', h_{s+1} \ldots, h_n)$ for some $h_1' \in \widetilde{H_1}, h_s' \in \widetilde{H_s}$. Using Claim 2 and Lemma 8.2.4 in the same way, we further reduce α modulo $\widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2^{nr})$ to a vector of the form $(h_1'', h_2', 1, \ldots, 1)$ for some $h_1'' \in \widetilde{H_1}, h_2' \in \widetilde{H_2}$ such that $h_1''h_2' \in \Phi^{\widetilde{G}}(\widetilde{H})$. Finally, since $K_1 \cap K_2 = k$, we have $\widetilde{H} = \widetilde{H_1}\widetilde{H_2}$ and thus $\Phi^{\widetilde{G}}(\widetilde{H}) \subset \Phi^{\widetilde{G}}(\widetilde{H_1})\Phi^{\widetilde{G}}(\widetilde{H_2})$. The result follows by an argument similar to the one given at the end of the proof of Theorem 9.2.1.

Now assume that $[K_1 \ldots K_n : k] = p^2$ (note that this is only possible if $n \leq p+1$ as a bicyclic field has $p+1$ subfields of degree p) and therefore $G = C_p \times C_p$ is abelian. By Proposition 8.2.9 it suffices to prove that $\operatorname{Ker} \psi_1 / \varphi_1(\operatorname{Ker} \psi_2^{nr}) \cong (\mathbb{Z}/p)^{n-2}$. We first show that $\varphi_1(\operatorname{Ker} \psi_2^{nr}) = 1$. Let $\alpha \in \operatorname{Ker} \psi_2^v$ for some unramified place v of L/k. Write $D_v = \langle g \rangle$

and $\alpha = \bigoplus_{i=1}^{n} \bigoplus_{t=1}^{r_{v,i}} h_{i,t}$ for some $g \in G$ and $h_{i,t} \in H_i \cap x_{i,t}\langle g \rangle x_{i,t}^{-1} = H_i \cap \langle g \rangle$. If $g \notin H_i$ for all $i = 1, \dots, n$, then α is the trivial vector and $\varphi_1(\alpha) = (1, \dots, 1)$. Otherwise, if $g \in H_{i_0} \cong C_p$ for some index i_0, then $g \notin H_i$ for all $i \neq i_0$ and thus $h_{i,t} = 1$ for $i \neq i_0$. In this way, it follows that $1 = \psi_2(\alpha) = \prod_{i=1}^{n} \prod_{t=1}^{r_{v,i}} x_{i,t}^{-1} h_{i,t} x_{i,t} = \prod_{t=1}^{r_{v,i_0}} h_{i_0,k}$. Therefore, if $\varphi_1(\alpha) = (h_1, \dots, h_n)$, we have $h_i = 1$ if $i \neq i_0$ and $h_{i_0} = \prod_{t=1}^{r_{v,i_0}} h_{i_0,k} = 1$. In conclusion, $\varphi_1(\alpha) = (1, \dots, 1)$.

On the other hand, we have $\operatorname{Ker} \psi_1 = \{(h_1, \dots, h_n) \mid h_i \in H_i, \prod_{i=1}^{n} h_i = 1\}$. This group is the kernel of the surjective group homomorphism

$$\begin{aligned} f \colon H_1 \times \cdots \times H_n &\longrightarrow G \\ (h_1, \dots, h_n) &\longmapsto h_1 \dots h_n \end{aligned}$$

and thus $\operatorname{Ker} \psi_1 = \operatorname{Ker} f \cong (\mathbb{Z}/p)^{n-2}$, as desired. □

Corollary 9.4.2. *Let $K = (K_1, \dots, K_n)$ be a tuple of $n \geq 3$ non-isomorphic cyclic extensions of k with prime degree p.*

1. *If $[K_1 \dots K_n : k] = p^2$, then weak approximation for the multinorm one torus T holds if and only if the multinorm principle for K fails.*
2. *Otherwise, both the multinorm principle for K and weak approximation for T hold.*

Proof. Follows from Voskresenskiĭ's exact sequence of Theorem 1.5.8, Theorem 9.4.1 and [5, Theorem 8.3]. □

Remark 9.4.3. In [5, Proposition 8.5] it is shown that, in the case (1) above, the multinorm principle for K fails if and only if all decomposition groups of the bicyclic extension $K_1 \dots K_n$ are cyclic. We thus have a simple criterion to test the validity of weak approximation for the associated multinorm one torus.

Part III

Statistics of local-global principles

Chapter 10

Introduction

A considerable motivation for providing *qualitative* studies of local-global principles (such as the Hasse norm principle or weak approximation) as done in Parts I and II of this thesis is to enable a statistical analysis of these principles in families of algebraic varieties. Such *quantitative* studies of local-global principles have attracted significant interest in the area of Arithmetic Geometry in the past decade, see [16] for a survey of recent developments around this topic. In this last part of the thesis, our goal is to prove several quantitative results on the Hasse norm principle and weak approximation for norm one tori and, in this way, contribute to the ongoing rapid progress in the area of statistics of local-global principles.

In Chapter 11 we start by establishing a result (Theorem 11.0.1) showing that, in a precise sense, the HNP holds for *almost all* degree n extensions of a fixed number field k. This result is conditional on the *weak Malle conjecture* on the distribution of number fields with prescribed Galois group (see (11.0.1) below), a conjecture that has also received significant attention lately and where progress is rapidly being made (see [99] for recent results on this conjecture). We then present two unconditional results (Theorems 11.0.3 and 11.0.6) for degrees $n = 4$ and $n = 6$ and base field $k = \mathbb{Q}$ by exploiting a few cases where Malle's conjecture is known to be true.

If one wishes to obtain more precise results, it is natural to not only fix the degree and the base field of our extensions, but to also specify their Galois group. For instance, using Tate's description of the knot group for Galois extensions in (2.0.1), one can often characterize the validity of the Hasse norm principle in the family of Galois extensions of k with fixed Galois group G (henceforth denominated *G-extensions*), see [39, 40, 46] for some examples. It is also possible to use this description to show that, if G is a finite solvable group, then there exists a G-extension of k failing the Hasse norm principle if and only if $\mathrm{H}^3(G, \mathbb{Z}) \neq 0$ (see [30, Theorem 1.2]). In light of this result it is natural to try to understand how frequently counter-examples to the Hasse norm principle arise in families of G-extensions.

In [52], Jehne provided a result in this direction, showing the existence of *infinitely many* extensions with prescribed Galois group G, knot-group ν and base field k, when G is a finite abelian p-group, ν a quotient group of $\mathrm{H}^3(G, \mathbb{Z})$ and k a number field not containing p-th roots of unity. Recently, Frei–Loughran–Newton have also analyzed this type of question and did a comprehensive study of the distribution of abelian extensions failing the Hasse norm principle, when fields are ordered by discriminant (see [30, Theorems 1.1 and 1.4]) or by conductor (see [31, Corollary 1.10]). For example, their work implies that, when G is the Klein four-group V_4, 100% (but not all) of G-extensions of k satisfy the Hasse norm principle. This result was shortly after refined by Rome [80] to an asymptotic formula for the number of biquadratic extensions of $k = \mathbb{Q}$ failing the Hasse norm principle, when fields are ordered by discriminant.

In the last chapter of this thesis, Chapter 12, we obtain the first density result on the HNP for a family of *non-abelian* extensions. Namely, we investigate this principle for octic extensions of $\mathbb{Q}$ with Galois group D_4 and show (Theorem 12.0.1) that the HNP holds for 100% of such extensions, when fields are ordered by discriminant or by an Artin conductor.

Chapter 11

Statistics of local-global principles for degree n extensions

In this chapter we present some results on the density of degree n extensions of a fixed number field that fail the Hasse norm principle, when extensions are ordered by discriminant. Although counting degree $n > 4$ extensions of number fields with bounded discriminant is an intricate problem and precise asymptotics may be out of reach at present, there are very precise conjectures for the number of such extensions. Namely, the weak Malle conjecture on the distribution of number fields (see [69]) predicts that the number $N(k, G, X)$ of degree n extensions K of a number field k with Galois group G and $|N_{k/\mathbb{Q}}(\mathrm{Disc}_{K/k})| \leq X$ satisfies

$$X^{\frac{1}{\alpha(G)}} \ll N(k, G, X) \ll X^{\frac{1}{\alpha(G)}+\epsilon}, \tag{11.0.1}$$

where $\alpha(G) = \min_{g \in G \setminus \{1\}} \{\mathrm{ind}(g)\}$ and $\mathrm{ind}(g)$ equals n minus the number of orbits of g on $\{1, \ldots, n\}$. Using the computational method developed by Hoshi and Yamasaki to determine $\mathrm{H}^1(k, \mathrm{Pic}\,\overline{X})$ outlined in Section 4.4, we obtain the following consequence of this conjecture:

Theorem 11.0.1. *Fix a number field k and an integer $n \leq 15$ with $n \neq 8, 12$. Suppose that Conjecture (11.0.1) holds for every transitive subgroup $G \leq S_n$. Then*

(i) the HNP holds for 100% of degree n extensions over k, when ordered by discriminant;

(ii) weak approximation holds for 100% of norm one tori of degree n extensions over k, when ordered by discriminant of the associated extension.

Proof. Note that an extension K/k of degree n is a (G, H)-extension (as defined in Section 6.1), where G is a transitive subgroup of S_n and H is an index n subgroup of G. Since there are a finite number of possibilities for G and H, one can compute all possibilities for $\mathrm{H}^1(G, F_{G/H})$ using the aforementioned algorithms of Hoshi and Yamasaki. If $\mathrm{H}^1(G, F_{G/H}) = 0$, then both the HNP for K/k and weak approximation for $R^1_{K/k}\mathbb{G}_m$ hold by Theorem 1.5.8 and the isomorphism (1.5.2) of Theorem 1.5.12. If $\mathrm{H}^1(G, F_{G/H}) \neq 0$, one can compute the integer $\alpha(G)$ of Malle's conjecture and for every such case one verifies that $\alpha(G) > 1$. Thus, if the conjecture holds, then the number of degree n extensions with discriminant bounded by X and for which the HNP or weak approximation fails is $o(X)$. The result then follows by observing that Malle's conjecture also implies that the number of degree n extensions of k with discriminant bounded by X is asymptotically at least $c(k, n)X$ for some positive constant $c(k, n)$. □

Remark 11.0.2. We list a few observations about Theorem 11.0.1 and its proof.

(i) The reason for excluding degrees $n = 8$ and 12 is that in these cases there are pairs (G, H), where $G \leq S_n$ is a transitive subgroup and H is an index n subgroup of G, such that $\mathrm{H}^1(G, F_{G/H})$ is non-trivial and $\alpha(G) = 1$. A more detailed analysis of the proportion of these (G, H)-extensions for which the local-global principles fail is needed in these cases. In the next chapter we give a first result in this direction by investigating the frequency of the HNP for D_4-octics.

(ii) Computing the values of $\alpha(G)$ for all transitive subgroups G of S_n with $\mathrm{H}^1(G, F_{G/H}) \neq 0$ and $[G : H] = n$ yields an upper bound (conditional on Malle's conjecture) on the number of degree n extensions for which the HNP (or weak approximation for the norm one torus) fails. For example, the number of degree 14 extensions of k for which the HNP (or weak approximation for the norm one torus) fails is $\ll_{k,\epsilon} x^{\frac{1}{6}+\epsilon}$, when ordered by discriminant.

(iii) In the statement of Theorem 11.0.1 it suffices to assume Malle's conjecture only for the few transitive subgroups $G \leq S_n$ containing an index n subgroup H such that $\mathrm{H}^1(G, F_{G/H})$ is not trivial. Indeed, the assumption for all $G \leq S_n$ was used solely to show that the number of degree n extensions of k with discriminant bounded by X is $\gg_{k,n} X$. For $n \leq 15$ composite, one can use an argument similar to that of [28, pp. 723–724] for n even and the results of Datskovsky and Wright [24] for cubics and of Bhargava, Shankar and Wang [12] for quintics to prove the aforementioned result. Finally, for n prime we do not need any assumptions as the HNP for K/k and weak approximation for $R^1_{K/k}\mathbb{G}_m$ always hold for extensions of prime degree (see [21, Proposition 9.1 and Remark 9.3]).

(iv) To simplify the statement we only presented results for degree $n \leq 15$ but one can obtain results for higher degrees in a similar way. However, Hoshi and Yamasaki's algorithms require one to embed the Galois group G as a transitive subgroup of S_n, whereupon one quickly reaches the limit of the databases of such groups stored in computational algebra systems such as GAP. To overcome this problem, one may use the modification of Hoshi and Yamasaki's algorithms presented as Algorithm A1 in the Appendix 4.5.

An analysis of the invariant $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ for extensions K/k of degree $n \leq 15$ has also recently been carried out independently by Hoshi, Kanai and Yamasaki in [48] and [49]. In these works, the computation of $\mathrm{H}^1(k, \operatorname{Pic} \overline{X})$ for such extensions (which here happened behind the scenes of the above proof) is made explicit and, additionally, necessary and sufficient conditions for the vanishing of $\mathfrak{K}(K/k)$ are given.

We end this chapter by using results on the distribution of number fields with prescribed Galois group to prove two unconditional theorems on the density of the HNP. The first one concerns the family of quartic extensions of $\mathbb{Q}$:

Theorem 11.0.3. *The HNP holds for 100% of quartic extensions of* $\mathbb{Q}$*, when ordered by discriminant.*

Proof. Since the HNP holds for all C_4, D_4 and S_4-quartics (see Theorems 2.0.2, 2.0.5 and 2.0.6, respectively), the only quartic extensions of number fields for which HNP can fail are those with associated Galois groups V_4 or A_4. By work of Baily [2] and Wong [97], it is known that 0% of quartic extensions of $\mathbb{Q}$ have Galois group V_4 or A_4, when ordered by discriminant. The result follows. □

Similarly to the case of quartics, we also obtain an unconditional density result for the family of sextic extensions of $\mathbb{Q}$, Theorem 11.0.6 below. To prove this result, we will use the following two lemmas:

Lemma 11.0.4. *Let* $K/\mathbb{Q}$ *be a sextic extension. If* $K/\mathbb{Q}$ *fails the HNP, then* $\mathrm{Gal}(N/\mathbb{Q}) \cong A_4$ *or* A_5*, where* N *is the normal closure of* $K/\mathbb{Q}$*.*

Proof. See [27, Lemma 12]. □

Lemma 11.0.5. *Let* $K/\mathbb{Q}$ *be a degree* n *extension, let* p *be a prime that is tamely ramified in* $K/\mathbb{Q}$ *and let* N *denote the normal closure of* $K/\mathbb{Q}$*. Then the exact exponent of* p *dividing* $\mathrm{Disc}(K/\mathbb{Q})$ *equals* $\mathrm{ind}(g)$*, where* g *is any element of the transitive subgroup* $\mathrm{Gal}(N/\mathbb{Q}) \leq S_n$ *that generates the inertia group of* $N/\mathbb{Q}$ *at* p*.*

Proof. See, for example, [94, §2.2]. □

Theorem 11.0.6. *The HNP holds for 100% of sextic extensions of $\mathbb{Q}$, when ordered by discriminant.*

Proof. Since the total number of sextic extensions of $\mathbb{Q}$ with absolute discriminant $< X$ is $\gg X$ (see Remark 11.0.2(iii) above), by Lemma 11.0.4 it suffices to show that the number of A_4-sextics (respectively, A_5-sextics) over $\mathbb{Q}$ is $o(X)$. We present the argument for A_5-sextics – the case of A_4-sextics is analogous.

Let $\mathcal{L}_5(X)$ (respectively, $\mathcal{L}_6(X)$) be the set of isomorphism classes of A_5-quintics (respectively, A_5-sextics) over $\mathbb{Q}$ with absolute discriminant $< X$. Let K_6 be a sextic extension of $\mathbb{Q}$ with A_5-normal closure. Denote the quintic sibling field[1] of K_6 by K_5. We will show that taking the quintic sibling of an A_5-sextic defines an injection

$$\mathcal{L}_6(X) \hookrightarrow \mathcal{L}_5(cX)$$

for some positive constant c and deduce the desired result by invoking the fact that $|\mathcal{L}_5(cX)| = o(X)$ as follows from the work of Bhargava in [11].

We start by comparing the exact power of p dividing $\mathrm{Disc}(K_6/\mathbb{Q})$ and $\mathrm{Disc}(K_5/\mathbb{Q})$ for a tamely ramified prime p. Let G_1 be the copy of A_5 in its regular representation inside S_5 and let G_2 be a copy of the transitive subgroup of S_6 that is isomorphic to A_5 (unique up to conjugacy). A quick computation in GAP [33] shows that $\mathrm{ind}(g) \leq \mathrm{ind}(g')$ for any $g \in G_1, g' \in G_2$ such that g and g' have the same order. Therefore by Lemma 11.0.5 we deduce that $p^k \mid\mid \mathrm{Disc}(K_5/\mathbb{Q})$ implies $p^k \mid \mathrm{Disc}(K_6/\mathbb{Q})$.

For a potentially wildly ramified prime $p = 2, 3$ or 5 of $K_5/\mathbb{Q}$, the exact power of p dividing the discriminant is bounded by a constant independent of the field K_5 (see [72, III, §2, Theorem 2.6]). From this fact and the conclusion of the previous paragraph, we deduce that there exists some positive constant $c > 0$ such that $\mathrm{Disc}(K_5/\mathbb{Q}) < c\,\mathrm{Disc}(K_6/\mathbb{Q})$ for all A_5-siblings K_5 and K_6. Therefore, if $K_6 \in \mathcal{L}_6(X)$, its quintic sibling field K_5 is in $\mathcal{L}_5(cX)$. As there is one and only one isomorphism class of a sibling A_5-quintic field for each A_5-sextic, this association is injective and the result follows. □

[1] Two finite extensions K_1, K_2 of $\mathbb{Q}$ are called *siblings* if they are not isomorphic, but have isomorphic normal closures.

Chapter 12

Statistics of local-global principles for D_4-octics

In this chapter we provide the first density result in the simplest non-abelian setting where failures of the Hasse norm principle are possible, namely for the family of D_4-octics. Note that, since $\mathrm{H}^3(D_4, \mathbb{Z}) = \mathbb{Z}/2$, failures of this principle (over any number field k) always exist by [30, Theorem 1.2]. Nonetheless, our main result shows that such failures are rare:

Theorem 12.0.1. *When ordered by discriminant or by conductor*[1], *100% of D_4-octics over $\mathbb{Q}$ satisfy the Hasse norm principle.*

Remark 12.0.2. We remark that the density result on D_4-octics ordered by discriminant in Theorem 12.0.1 is conditional on the work in progress [85] of Shankar–Varma, outlined below in Section 12.1.2.

While for an abelian group G there are precise asymptotics for the number of G-extensions of bounded discriminant (see [67], [100]), conductor (see [68]) and even more general counting functions (see [98]), the problem of enumerating non-abelian fields is much more complicated and results in this setting are still quite limited (see [99] for a survey of recent developments in this area).

In spite of this, Altuğ–Shankar–Varma–Wilson [1] have recently combined arithmetic invariant theory with techniques from geometry of numbers and the algebraic structure of D_4 in order to determine the asymptotic number of quartic D_4-fields over $\mathbb{Q}$ ordered by conductor. Furthermore, in their upcoming work [85], Shankar and Varma also compute

[1] See Section 12.1.2 for the definition of the conductor of a D_4-octic over $\mathbb{Q}$.

the asymptotic number of octic D_4-fields over $\mathbb{Q}$ ordered by discriminant, verifying the strong form of Malle's conjecture (see (12.1.5) below) for this family of extensions.

In the aforementioned works of Altuğ–Shankar–Varma–Wilson and Shankar–Varma the constants of proportionality in the main term of the asymptotics are shown to satisfy the so-called *Malle–Bhargava principle*. Specifically, this principle predicts that such constants will be given by an Euler product of local masses, obtained from the expectation that the (weighted) number of D_4-extensions ordered by a counting function (like the discriminant or an Artin conductor) equals the product over all places $v \in \Omega_{\mathbb{Q}}$ of the (weighted) number of D_4-compatible extensions of $\mathbb{Q}_v$ consistent with that counting function (see [99, Section 10] for a detailed explanation of the Malle-Bhargava principle). This fact is key in the application of the present chapter as it allows us to count D_4-fields with certain local conditions at a finite number of primes that ensure successes of the Hasse norm principle and, in this way, deduce Theorem 12.0.1.

Remark 12.0.3. If G is a group of order 8, then G is either abelian, isomorphic to the quaternion group $\mathcal{Q}_8$ or isomorphic to D_4. In the first case, work of Frei–Loughran–Newton shows that 100% of G-extensions of $\mathbb{Q}$ satisfy the Hasse norm principle, when ordered by conductor. If $G = \mathcal{Q}_8$, then $\mathrm{H}^3(G, \mathbb{Z}) = 0$ and the Hasse norm principle always holds. Therefore, Theorem 12.0.1 completes the picture on the density of octic G-extensions of $\mathbb{Q}$ satisfying the Hasse norm principle.

Remark 12.0.4. Theorem 12.0.1 and the link between the Hasse principle and weak approximation for algebraic tori also allows us to obtain density results for the number of norm one tori of D_4-octics over $\mathbb{Q}$ that satisfy weak approximation, see Section 12.1.1.

12.1 Preliminaries

Throughout this chapter we fix a presentation of the group of symmetries of a square, $D_4 = \langle r, s \mid r^4 = s^2 = (rs)^2 = 1 \rangle$. We say that an extension M/k of fields is a D_4-*octic* if it is Galois with Galois group isomorphic to D_4. A quartic extension of fields L/k is said to be a D_4-*quartic* if its normal closure is a D_4-octic. If the ground field k of a D_4-octic or D_4-quartic is not specified, it is taken to be $\mathbb{Q}$.

12.1.1 Local-global principles for norms of D_4-fields

Hasse norm principle

In [39], Gerth provided an explicit characterization of the Hasse norm principle for Galois extensions with metacyclic Galois group. In particular, Gerth's work gives us the following description of this principle for D_4-octics:

Proposition 12.1.1. *Let M/k be a D_4-octic. Then the Hasse norm principle holds for M/k if and only if there exists a place v of k such that the decomposition group $D_v = \mathrm{Gal}(M_v/k_v)$ contains a copy of the Klein four-group V_4.*

Proof. Follows from [39, Corollary 2]. □

Remark 12.1.2. Note that a place v satisfying the conditions of Proposition 12.1.1 must ramify. Therefore, one can decide in finite time if a given D_4-octic satisfies the Hasse norm principle.

Weak approximation

Proposition 12.1.3. *Let M/k be a D_4-octic. Then weak approximation holds for $R^1_{M/k}\mathbb{G}_\mathrm{m}$ if and only if the Hasse norm principle fails for M/k.*

Proof. By Theorem 1.5.8 there exists an exact sequence

$$0 \to A(T) \to \mathrm{H}^1(k, \operatorname{Pic} \overline{X})^\sim \to Ш(T) \to 0, \tag{12.1.1}$$

where $A(T)$ is the defect of weak approximation for T, $Ш(T)$ is the Tate–Shafarevich group of T and X is a smooth compactification of T. For the norm one torus $T = R^1_{M/k}\mathbb{G}_m$, one has a canonical isomorphism

$$Ш(T) \cong \mathfrak{K}(M/k) \tag{12.1.2}$$

by Proposition 1.6.7 and thus (12.1.1) relates weak approximation for T with the Hasse norm principle for M/k. Moreover, as M/k is Galois with Galois group $G \cong D_4$, Theorems 1.5.12 and 1.6.8 and the fact that $\hat{\mathrm{H}}^{-3}(G, \mathbb{Z}) = \mathbb{Z}/2$ (see [54, Theorem 3.3.6(iii)]) show that

$$\mathrm{H}^1(k, \operatorname{Pic} \overline{X})^\sim \cong \hat{\mathrm{H}}^{-3}(G, \mathbb{Z}) = \mathbb{Z}/2. \tag{12.1.3}$$

The result follows from (12.1.1), (12.1.2) and (12.1.3). □

Remark 12.1.4. Ordering norm one tori of D_4-octics over $\mathbb{Q}$ by the conductor or discriminant of the associated extension, one gets a one-to-one correspondence between (isomorphism classes of) tori and field extensions (see [30, Proposition 6.3]). Therefore, it follows from Theorem 12.0.1 and Proposition 12.1.3 that 0% of norm one tori of D_4-octics over $\mathbb{Q}$ satisfy weak approximation, when ordered by conductor or by discriminant of the associated field extension.

12.1.2 Counting D_4-fields with local specifications

In this section we recall results of Altuğ–Shankar–Varma–Wilson [1] and describe work in progress of Shankar–Varma [85] on the number of D_4-fields over $\mathbb{Q}$ satisfying local conditions at finitely many places. Throughout the section, L and M will always denote a D_4-quartic and a D_4-octic over $\mathbb{Q}$, respectively. By an *étale* algebra over a field k we mean a k-algebra which is isomorphic to a finite product of finite separable field extensions of k.

Counting by conductor

Following [1], we define the *conductor* $\mathfrak{f}(M)$ of M as the Artin conductor of the (unique up to conjugacy) irreducible 2-dimensional Galois representation

$$\rho_M : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C})$$

that factors through $\mathrm{Gal}(M/\mathbb{Q}) \cong D_4$. Similarly, the conductor $\mathfrak{f}(L)$ of L is defined to be the conductor of its normal closure. In [1], the authors determined the asymptotic number of D_4-quartics ordered by conductor with prescribed local specifications, defined as follows:

Definition 12.1.5.

- For each place v of $\mathbb{Q}$, a *quartic local specification* is a set Σ_v consisting of pairs (L_v, K_v), where L_v is (an isomorphism class of) a quartic étale algebra over $\mathbb{Q}_v$ and K_v is (an isomorphism class of) a quadratic subalgebra of L_v.
- A collection of quartic local specifications $\Sigma = (\Sigma_v)_v$ is said to be *acceptable* if, for all but finitely many primes p, the set Σ_p contains all pairs (L_p, K_p) with conductor not divisible by p^2, where the conductor of (L_p, K_p) is defined as $\mathrm{C}(L_p, K_p) = \mathrm{Disc}(L_p)/\mathrm{Disc}(K_p)$.

We now recall the main result of [1]. Let X be a positive real number and Σ an acceptable collection of quartic local specifications. Denote by $\mathcal{L}(\Sigma)$ the set of D_4-quartics L such that $(L \otimes \mathbb{Q}_v, K \otimes \mathbb{Q}_v) \in \Sigma_v$ for all places v (where K is the quadratic subfield of L) and by $N_4(\Sigma, |\mathfrak{f}| < X)$ the number of isomorphism classes of field extensions in $\mathcal{L}(\Sigma)$ whose conductor is bounded by X.

Theorem 12.1.6. *[1, Theorem 3] If $\Sigma = (\Sigma_v)_v$ is an acceptable collection of quartic local specifications such that Σ_2 contains every pair (L_2, K_2), consisting of a quartic étale algebra L_2 over $\mathbb{Q}_2$ containing a quadratic subalgebra K_2, then*

$$N_4(\Sigma, |\mathfrak{f}| < X) \sim \frac{1}{2}\cdot\Bigg(\sum_{(L,K)\in\Sigma_\infty} \frac{1}{\#\operatorname{Aut}(L,K)}\Bigg)\cdot\prod_p\Bigg(\sum_{(L_p,K_p)\in\Sigma_p} \frac{1}{\#\operatorname{Aut}(L_p,K_p)}\frac{1}{\mathrm{C}_p(L_p,K_p)}\Bigg)\Big(1-\frac{1}{p}\Big)^2\cdot X\log X, \tag{12.1.4}$$

where for all places v, $\operatorname{Aut}(L_v, K_v)$ consists of the automorphisms of L_v which send K_v to itself and $\mathrm{C}_p(L_p, K_p) :=$ p-part of $\mathrm{C}(L_p, K_p)$.

In Table 1 of the Appendix we record the values of the invariants $\mathrm{C}_p(L_p, K_p)$ and $\operatorname{Aut}(L_v, K_v)$ for the different isomorphism classes of pairs (L_p, K_p). As a consequence of the data therein (which is given in terms of the *splitting types* of L_p and K_p, see Definition 12.2.1 and the paragraphs preceding Table 1), we obtain the asymptotic number $N_4(D_4, |\mathfrak{f}| < X)$ of D_4-quartics with conductor bounded by X:

Corollary 12.1.7. $N_4(D_4, |\mathfrak{f}| < X) \sim \frac{3}{8}\cdot\prod_p\left(1+\frac{2}{p}+\frac{2}{p^2}\right)\left(1-\frac{1}{p}\right)^2\cdot X\log X.$

Counting by discriminant

The strong form of Malle's conjecture [70] predicts that the number $N(k, G, X)$ of degree n extensions K of a number field k with Galois group G and $|N_{k/\mathbb{Q}}(\mathrm{Disc}_{K/k})| \le X$ satisfies

$$N(k,G,X) \sim c(k,G)X^{\frac{1}{\alpha(G)}}(\log X)^{\beta(k,G)-1}, \tag{12.1.5}$$

where $\alpha(G)$ and $\beta(k, G)$ are explicit positive constants and $c(k, G) > 0$. This prediction has been verified in plenty of cases, for example when G is an abelian group by work of Wright ([100]), for $G = S_n$ when $n = 3$ by Datskovsky–Wright ([24]) and $n = 4, 5$ by Bhargava ([8], [11]), for $G = S_3 \subset S_6$ by Bhargava–Wood ([10]) and for $G = D_4 \subset S_4$ by Cohen–Diaz y Diaz–Olivier ([19]). However, this conjecture is not always true in the form given in (12.1.5), as Klüners ([56]) found the counter-example $G = C_3 \wr C_2 \subset S_6$ for which the constant $\beta(k, G)$ is too small. The number $\alpha(G)$ in (12.1.5) is nonetheless still widely believed to be correct and corrections for the constant $\beta(k, G)$ have also been proposed, see [89].

In [9], Bhargava observed that the constant $c(k, G)$ in the predicted estimate (12.1.5) satisfies a certain local-global compatibility for degree $n \le 5$ S_n-extensions. More precisely, in this case the constant $c(k, G)$ can be realized as an Euler product of local p-adic masses, derived from the heuristic assumption that local behaviors of a random extension at different places of k are independent. In the same paper, Bhargava also conjectures that such a local-global compatibility holds when $n > 5$ and further speculates that a similar phenomenon might hold for any Galois group G and any base field k. Such a compatibility is now called the *Malle–Bhargava* principle and it has only been analyzed in a few cases. For instance, it is also known to hold when G is an abelian group of prime exponent by the work of Mäki [68] and Wright [100] (see also [98]) as well as for sextic S_3-extensions by the work of Bhargava–Wood [10].

Nonetheless, the Malle–Bhargava principle may fail. In [1, Section 3.3], Altuğ–Shankar–Varma–Wilson use the work of Cohen–Diaz y Diaz–Olivier [19] in order to verify that the family of D_4-quartics over $\mathbb{Q}$ does *not* satisfy the Malle–Bhargava principle. Furthermore, in work in progress [85], Shankar and Varma not only establish the strong Malle's conjecture for D_4-*octics* over $\mathbb{Q}$, but also prove that the Malle–Bhargava principle does hold in this family. We now outline their main result.

Definition 12.1.8.

- For any place v of $\mathbb{Q}$, a *D_4-type* at v is a D_4-conjugacy class of continuous group homomorphisms $\rho_v\colon \operatorname{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v) \to D_4$. An octic étale algebra M_v over $\mathbb{Q}_v$ is of *D_4-type* if there exists a continuous group homomorphism $\rho_v\colon \operatorname{Gal}(\overline{\mathbb{Q}}_v/\mathbb{Q}_v) \to D_4$ such that $M_v \cong \operatorname{Ind}_{\operatorname{Im}\rho_v}^{D_4} \overline{\mathbb{Q}}_v^{\operatorname{Ker}\rho_v}$, i.e. M_v is isomorphic to $\#\operatorname{Coker}(\rho_v)$ copies of the fixed field of $\operatorname{Ker}(\rho_v)$ in $\overline{\mathbb{Q}}_v$. In this case, we further say that M_v is of *D_4-type* $[\rho_v]$.
- For a finite place p of $\mathbb{Q}$, an *octic local specification* is a set Σ_p consisting of pairs $(M_p, [\rho_p])$, where M_p is an isomorphism class of an octic étale algebra of $\mathbb{Q}_p$ of D_4-type $[\rho_p]$. For the infinite place ∞ of $\mathbb{Q}$, an octic local specification Σ_∞ is a subset of $\{\mathbb{R}^8, \mathbb{C}^4\}$.
- A collection of octic local specifications $\Sigma = (\Sigma_v)_v$ is said to be *finite* if, for all but finitely many primes p, Σ_p contains all pairs $(M_p, [\rho_p])$, where M_p is an octic étale algebra of $\mathbb{Q}_p$ of D_4-type $[\rho_p]$.

Let X be a positive real number and Σ a finite collection of octic local specifications. Denoting by $\mathcal{F}(\Sigma)$ the set of D_4-octics M such that $(M \otimes \mathbb{Q}_v, [\rho_{M,v}]) \in \Sigma_v$ for all places v of $\mathbb{Q}$ and by $N_8(\Sigma, |\Delta| < X)$ the number of isomorphism classes of D_4-octics in $\mathcal{F}(\Sigma)$ with discriminant Δ bounded by X, we have:

Theorem 12.1.9. *[85, Theorem 2, in preparation] If $\Sigma = (\Sigma_v)_v$ is a finite collection of octic local specifications such that Σ_2 contains all D_4-types, then*

$$N_8(\Sigma, |\Delta| < X) \sim \frac{1}{4}\cdot\Bigg(\sum_{(M,\rho)\in\Sigma_\infty} \frac{1}{\#\operatorname{Aut}_{D_4}(\rho_\infty)}\Bigg)\cdot\prod_p\Bigg(\sum_{(M_p,\rho_p)\in\Sigma_p} \frac{1}{\#\operatorname{Aut}_{D_4}(\rho_p)}\frac{1}{|\Delta(M_p)|^{\frac{1}{4}}}\Bigg)\Bigg(1-\frac{1}{p}\Bigg)^3\cdot X^{\frac{1}{4}}\log^2(X^{\frac{1}{4}}),$$

where for all places v, $\mathrm{Aut}_{D_4}(\rho_v)$ denotes the centralizer of the subgroup $\mathrm{Im}\,\rho_v$ of D_4.

Using the tabulated values of $\Delta(M_p)$ and $\mathrm{Aut}_{D_4}(\rho_p)$ in Table 1, we obtain the following asymptotic formula for the number $N_8(D_4, |\Delta| < X)$ of D_4-octics with discriminant bounded by X:

Corollary 12.1.10. $N_8(D_4, |\Delta| < X) \sim \frac{1}{4}\cdot\frac{3}{4}\cdot\frac{1}{8}(\frac{56+3\sqrt{2}}{16})\cdot\prod_p(1+\frac{3}{p}+\frac{1}{p^{\frac{3}{2}}})(1-\frac{1}{p})^3\cdot X^{\frac{1}{4}}\log^2(X^{\frac{1}{4}})$.

12.2 Proof of the main theorem

In this section we show how to deduce Theorem 12.0.1 from the results of Sections 12.1.1 and 12.1.2. We require the following definition:

Definition 12.2.1. Let p be a prime and M_p an étale algebra over $\mathbb{Q}_p$. Then $M_p = \bigoplus_{i=1}^{g} K_{p,i}$, where $K_{p,i}$ are finite field extensions of $\mathbb{Q}_p$, and we define the *splitting type* $\varsigma(M_p)$ *of* M_p *at* p as the symbol $(f_1^{e_1} f_2^{e_2} \dots f_g^{e_g})$, where e_i (respectively, f_i) is the ramification index (respectively, residue degree) of $K_{p,i}$. Given a number field M, we define the *splitting type* $\varsigma_p(M)$ *of* M *at* p as the splitting type of $M \otimes \mathbb{Q}_p$.

12.2.1 Proof of the conductor result of Theorem 12.0.1

For each $n \geq 1$, we define a collection of quartic local specifications $\Sigma_n^4 = ((\Sigma_n^4)_v)_v$ as follows. Let P_n be the set of the first n odd primes. For a prime $p \in P_n$, we require that $(\Sigma_n^4)_p$ contains all pairs (L_p, K_p) of a quartic étale algebra $L_p/\mathbb{Q}_p$ and a quadratic subalgebra K_p such that the pair of splitting types $(\varsigma(L_p), \varsigma(K_p))$ is not $((2^2), (1^2))$ nor $((1^2 2), (11))$ (highlighted in bold in Table 1). For a place v of $\mathbb{Q}$ not in P_n, we let $(\Sigma_n^4)_v$ contain all pairs (L_v, K_v) of a quartic étale algebra $L_v/\mathbb{Q}_v$ with quadratic subalgebra K_v. It is clear that the collection Σ_n^4 constructed in this way is acceptable.

Note that if a D_4-quartic L with normal closure M is not in $\mathcal{L}(\Sigma_n^4)$ for some $n \geq 1$, then there exists $p \in P_n$ such that the pair of splitting types $(\varsigma_p(L), \varsigma_p(K))$ (where K is the quadratic subfield of L) is $((2^2), (1^2))$ or $((1^2 2), (11))$. In either case, one can see from Table 1 that this implies that the decomposition group D_p of $M/\mathbb{Q}$ at p is isomorphic to V_4 and so the HNP holds for $M/\mathbb{Q}$ by Proposition 12.1.1. Therefore the set $\mathcal{L}_{fail}$ of all

D_4-quartics whose normal closure fails the Hasse norm principle is contained in $\mathcal{L}(\Sigma_n^4)$ for all n. Since, up to isomorphism, each D_4-octic has two distinct quartic subfields which are D_4-quartics, we have

$$\frac{\#\{M \mid M \text{ is a } D_4\text{-octic failing the HNP and } \mathfrak{f}(M) < X\}}{\#\{M \mid M \text{ is a } D_4\text{-octic and } \mathfrak{f}(M) < X\}} = \frac{\frac{1}{2}\#\mathcal{L}_{fail}(|\mathfrak{f}| < X)}{\frac{1}{2}N_4(D_4, |\mathfrak{f}| < X)} \leq \frac{N_4(\Sigma_n^4, |\mathfrak{f}| < X)}{N_4(D_4, |\mathfrak{f}| < X)}$$

for all n and so to prove Theorem 12.0.1 it suffices to show that $\lim\limits_{n\to\infty} \lim\limits_{X\to\infty} \frac{N_4(\Sigma_n^4, |\mathfrak{f}|<X)}{N_4(D_4, |\mathfrak{f}|<X)} = 0$. This follows from the next lemma and a standard criterion for the divergence of an infinite product.

Lemma 12.2.2.

$$\lim_{X\to\infty} \frac{N_4(\Sigma_n^4, |\mathfrak{f}| < X)}{N_4(D_4, |\mathfrak{f}| < X)} = \prod_{p\in P_n} \left(1 - \frac{p}{p^2 + 2p + 2}\right)$$

Proof. Using the data in Table 1, it is easy to compute the Euler factor in (12.1.4) for any quartic local specification Σ_p^4 at an odd prime $p \in P_n$ and one obtains

$$\sum_{\text{all pairs } (L_p, K_p)} \frac{1}{\#\operatorname{Aut}(L_p, K_p)} \frac{1}{\mathrm{C}_p(L_p, K_p)} = 1 + \frac{2}{p} + \frac{2}{p^2}$$

and

$$\sum_{(L_p, K_p)\in(\Sigma_n^4)_p} \frac{1}{\#\operatorname{Aut}(L_p, K_p)} \frac{1}{\mathrm{C}_p(L_p, K_p)} = 1 + \frac{1}{p} + \frac{2}{p^2}.$$

The result follows from an application of Theorem 12.1.6. □

12.2.2 Proof of the discriminant result of Theorem 12.0.1

We proceed similarly as in Section 12.2.1: let $n \geq 1$ and let P_n be the set of the first n odd primes. We define a finite collection of octic local specifications $\Sigma_n^8 = ((\Sigma_n^8)_v)_v$ analogously to Section 12.2.1. Namely, for $p \in P_n$, let $(\Sigma_n^8)_p$ be the set of all octic local specifications $(M_p, [\rho_p])$ such that the pair of splitting types $(\varsigma(L_p), \varsigma(K_p))$ is not $((2^2), (1^2))$ nor $((1^2 2), (11))$, where $L_p = M_p^{\langle s\rangle}$ and $K_p = M_p^{\langle s, r^2\rangle}$. For $v \notin P_n$, we let $(\Sigma_n^8)_v$ contain all octic local specifications at v.

As in Section 12.2.1, we see that if M is an octic D_4-field failing the Hasse norm principle, then $M \otimes \mathbb{Q}_v \in (\Sigma_n^8)_v$ for all v and all n and therefore

$$\frac{\#\{M \mid M \text{ is a } D_4\text{-octic failing the HNP, } |\operatorname{Disc}(M)| < X\}}{N_8(D_4, |\Delta| < X)} \leq \frac{N_8(\Sigma_n^8, |\Delta| < X))}{N_8(D_4, |\Delta| < X)}$$

for every n. Theorem 12.0.1 then follows from the fact that $\lim\limits_{n\to\infty} \lim\limits_{X\to\infty} \frac{N(\Sigma_n^8, |\Delta|<X))}{N_8(D_4,|\Delta|<X)} = 0$, which can be deduced from a standard criterion on the divergence of infinite products and the following lemma.

Lemma 12.2.3.

$$\lim_{X\to\infty} \frac{N_8(\Sigma_n^8, |\Delta| < X))}{N_8(D_4, |\Delta| < X)} = \prod_{p \in P_n} \left(1 - \frac{p}{p^2 + 3p + p^{\frac{1}{2}}}\right)$$

Proof. Analogously to the proof of Lemma 12.2.2, this equality follows from an application of Theorem 12.1.9 and the data in Table 1. □

12.3 Appendix: Local data for D_4-extensions

Let p be a prime and let M_p be (an isomorphism class of) an octic étale algebra of $\mathbb{Q}_p$ of D_4-type $[\rho_p]$ as in Definition 12.1.8. Let L_p be a quartic étale algebra over $\mathbb{Q}_p$ contained in M_p and let K_p be a quadratic subalgebra of L_p. Using a database of local fields (such as [53] or [61]), it is easy to check that the automorphism groups appearing in Theorems 12.1.6 and 12.1.9 coincide[2], i.e. we have

$$\operatorname{Aut}(L_p, K_p) = \operatorname{Aut}_{D_4}(\rho_p).$$

One can additionally verify that these automorphism groups as well as the invariants $\mathrm{C}_p(L_p, K_p), \Delta(M_p)$ and the decomposition group $D_p = \operatorname{Im} \rho_p$ are completely determined by the splitting type of the algebras M_p, L_p and K_p.

In the following table we record all possible splitting types ς (defined in 12.2.1) at an odd prime p of an étale algebra M_p over $\mathbb{Q}_p$ of D_4-type and of the relevant subalgebras, the number of isomorphism classes of such objects as well as the associated decomposition groups D_p and invariants C_p and Δ appearing in Theorems 12.1.6 and 12.1.9, respectively.

[2] A non-computational proof of this fact will also appear in a future version of [85].

Table 1

D_p	$\varsigma(M_p)$	$(\varsigma(L_p), \varsigma(K_p))$	$\#(L_p, K_p)$	$\mathrm{Aut}(L_p, K_p)$	$\mathrm{C}_p(L_p, K_p)$	$\Delta(M_p)$
$\{1\}$	(11111111)	((1111),(11))	1	D_4	1	1
$\langle r^2\rangle$	(2222)	((22), (11))	1	D_4	1	1
$\langle rs\rangle$	(2222)	((22), (2))	1	V_4	1	1
$\langle s\rangle$	(2222)	((112), (11))	1	V_4	1	1
$\langle r\rangle$	(44)	((4), (2))	1	C_4	1	1
$\{s\}$	$(1^21^21^21^2)$	$((1^211), (11))$	2	V_4	p	p^4
$\boldsymbol{\langle s, r^2\rangle}$	$\boldsymbol{(2^22^2)}$	$\boldsymbol{((1^22), (11))}$	**2**	$\boldsymbol{V_4}$	$\boldsymbol{p}$	$\boldsymbol{p^4}$
$\langle rs\rangle$	$(1^21^21^21^2)$	$((1^21^2), (1^2))$	2	V_4	p	p^4
$\boldsymbol{\langle rs, r^2\rangle}$	$\boldsymbol{(2^22^2)}$	$\boldsymbol{((2^2), (1^2))}$	**2**	$\boldsymbol{V_4}$	$\boldsymbol{p}$	$\boldsymbol{p^4}$
$\langle r^2\rangle$	$(1^21^21^21^2)$	$((1^21^2), (11))$	2	D_4	p^2	p^4
$\langle r^2, s\rangle$	(2^22^2)	$((1^21^2), (11))$	1	V_4	p^2	p^4
$\langle rs, r^2\rangle$	(2^22^2)	$((2^2), (2))$	1	V_4	p^2	p^4
$\langle r\rangle$	(2^22^2)	$((2^2), (2))$	1	C_4	p^2	p^4
$\langle r\rangle$	(1^41^4)	$((1^4), (1^2))$	$(4, 0)$	C_4	p^2	p^6
D_4	(2^4)	$((1^4), (1^2))$	$(0, 2)$	C_2	p^2	p^6

In the column of Table 1 containing the number of pairs $\#(L_p, K_p)$, the number (a, b) equals a if $p \equiv 1 \pmod 4$, or b if $p \equiv 3 \pmod 4$. We also present the analogous table for the prime $p = 2$ obtained using databases of local fields [53] and [61]:

Table 2

D_2	$\varsigma(M_2)$	$(\varsigma(L_2), \varsigma(K_2))$	$\#(L_2, K_2)$	$\mathrm{Aut}_{D_4}(\rho_2)$	$\mathrm{C}_2(L_2, K_2)$	$\Delta(M_2)$
$\{1\}$	(11111111)	((1111),(11))	1	D_4	1	1
$\langle r^2\rangle$	(2222)	((22),(11))	1	D_4	1	1
$\langle rs\rangle$	(2222)	((22),(2))	1	V_4	1	1
$\langle s\rangle$	(2222)	((112),(11))	1	V_4	1	1
$\langle r\rangle$	(44)	((4),(2))	1	C_4	1	1
$\{s\}$	$(1^21^21^21^2)$	$((1^211), (11))$	2	V_4	2^2	2^8
$\{s\}$	$(1^21^21^21^2)$	$((1^211), (11))$	4	V_4	2^3	2^{12}
$\langle s, r^2\rangle$	(2^22^2)	$((1^22), (11))$	2	V_4	2^2	2^8
$\langle s, r^2\rangle$	(2^22^2)	$((1^22), (11))$	4	V_4	2^3	2^{12}
$\langle rs\rangle$	$(1^21^21^21^2)$	$((1^21^2), (1^2))$	2	V_4	2^2	2^8
$\langle rs\rangle$	$(1^21^21^21^2)$	$((1^21^2), (1^2))$	4	V_4	2^3	2^{12}
$\langle rs, r^2\rangle$	(2^22^2)	$((2^2), (1^2))$	2	V_4	2^2	2^8
$\langle rs, r^2\rangle$	(2^22^2)	$((2^2), (1^2))$	4	V_4	2^3	2^{12}
$\langle r^2\rangle$	$(1^21^21^21^2)$	$((1^21^2), (11))$	2	D_4	2^4	2^8

$\langle r^2 \rangle$	$(1^2 1^2 1^2 1^2)$	$((1^2 1^2), (11))$	4	D_4	2^6	2^{12}
$\langle r^2, s \rangle$	$(2^2 2^2)$	$((1^2 1^2), (11))$	1	V_4	2^4	2^8
$\langle r^2, s \rangle$	$(2^2 2^2)$	$((1^2 1^2), (11))$	2	V_4	2^6	2^{12}
$\langle r^2, s \rangle$	$(1^4 1^4)$	$((1^2 1^2), (11))$	4	V_4	2^6	2^{16}
$\langle r^2, s \rangle$	$(1^4 1^4)$	$((1^2 1^2), (11))$	8	V_4	2^5	2^{16}
$\langle rs, r^2 \rangle$	$(2^2 2^2)$	$((2^2), (2))$	1	V_4	2^4	2^8
$\langle r \rangle$	$(2^2 2^2)$	$((2^2), (2))$	1	C_4	2^4	2^8
D_4	(2^4)	$((2^2), (2))$	2	C_2	2^4	2^8
$\langle rs, r^2 \rangle$	$(2^2 2^2)$	$((2^2), (2))$	2	V_4	2^6	2^{12}
$\langle r \rangle$	$(2^2 2^2)$	$((2^2), (2))$	2	C_4	2^6	2^{12}
D_4	(2^4)	$((2^2), (2))$	2	C_2	2^6	2^{12}
$\langle rs, r^2 \rangle$	$(1^4 1^4)$	$((1^4), (1^2))$	4	V_4	2^6	2^{16}
$\langle rs, r^2 \rangle$	$(1^4 1^4)$	$((1^4), (1^2))$	8	V_4	2^5	2^{16}
$\langle r \rangle$	$(1^4 1^4)$	$((1^4), (1^2))$	8	C_4	2^8	2^{22}
D_4	(2^4)	$((1^4), (1^2))$	2	C_2	2^4	2^{12}
D_4	(2^4)	$((1^4), (1^2))$	2	C_2	2^6	2^{16}
D_4	(1^8)	$((1^4), (1^2))$	16	C_2	2^7	2^{22}
D_4	(2^4)	$((1^4), (1^2))$	4	C_2	2^8	2^{22}
D_4	(1^8)	$((1^4), (1^2))$	8	C_2	2^8	2^{24}

Bibliography

[1] S. A. Altug, A. Shankar, I. Varma, K. H. Wilson, The number of quartic D_4-fields ordered by conductor. *J. Eur. Math. Soc.*, to appear. Preprint. arXiv:1704.01729.

[2] A. M. Baily, On the density of discriminants of quartic fields. *J. reine angew. Math.* **315** (1980), 190–210.

[3] H.-J. Bartels, Zur Arithmetik von Konjugationsklassen in algebraischen Gruppen. *J. Algebra* **70** (1981), 179–199.

[4] H.-J. Bartels, Zur Arithmetik von Diedergruppenerweiterungen. *Math. Ann.* **256** (1981), 465–473.

[5] E. Bayer-Fluckiger, T.-Y. Lee, R. Parimala, Hasse principles for multinorm equations. *Advances in Math.* **356** (2019), Article 106818.

[6] E. Bayer-Fluckiger, R. Parimala, On unramified Brauer groups of torsors over tori. *Documenta Math.* **25** (2020), 1263–1284.

[7] F. R. Beyl, J. Tappe, *Group Extensions, Representations, and the Schur Multiplicator*. Lecture Notes in Mathematics **958**, Springer-Verlag, 1982.

[8] M. Bhargava, The density of discriminants of quartic rings and fields. *Ann. of Math.* **162**(2) (2005), 1031–1063.

[9] M. Bhargava, Mass Formulae for Extensions of Local Fields, and Conjectures on the Density of Number Field Discriminants. *Int. Math. Res. Notices* Vol. rnm052 (2007).

[10] M. Bhargava, M. M. Wood, The density of discriminants of S_3-sextic number fields. *Proc. Amer. Math. Soc.* **136**(5) (2008), 1581–1587.

[11] M. Bhargava, The density of discriminants of quintic rings and fields. *Ann. of Math.* **172**(3) (2010) 1559–1591.

[12] M. Bhargava, A. Shankar, X. Wang, Geometry-of-numbers methods over global fields I: Prehomogeneous vector spaces. Preprint. arXiv:1512.03035.

[13] M. Borovoi, B. È. Kunyavskiĭ, Formulas for the unramified Brauer group of a principal homogeneous space of a linear algebraic group. *J. Algebra* **225** (2000), 804–821.

[14] W. Bosma, J. Cannon, C. Playoust, The Magma algebra system. I. The user language. J. Symbolic Comput., **24** (1997), 235–265.

[15] K. S. Brown, *Cohomology of groups.* Graduate Texts in Mathematics **87**, Springer-Verlag, 1982.

[16] T.D. Browning, How often does the Hasse principle hold? *Algebraic Geometry: Salt Lake City 2015, Proc. Symposia Pure Math.* **97.2** (2018), AMS, 89–102.

[17] G. Butler, J. McKay, The transitive groups of degree up to eleven. *Comm. Algebra* **11** (1983), 863–911.

[18] J. W. S. Cassels, A. Fröhlich (eds.), *Algebraic Number Theory.* Academic Press (London), 1967.

[19] H. Cohen, F. Diaz y Diaz, M. Olivier, Enumerating quartic dihedral extensions of $\mathbb{Q}$. *Compositio Math.* **133**(1) (2002), 65–93.

[20] J.-L. Colliot-Thélène, J.-J. Sansuc, La R-équivalence sur les tores. *Ann. Sc. E.N.S.* **10** (1977), 175–229.

[21] J.-L. Colliot-Thélène, J.-J. Sansuc, Principal homogeneous spaces under flasque tori: Applications. *J. Algebra* **106** (1987), 148–205.

[22] J.-L. Colliot-Thélène, D. Harari, A. N. Skorobogatov, Compactification équivariante d'un tore (d'après Brylinski et Künnemann). *Expo. Math.* **23** (2005), 161–170.

[23] J.-L. Colliot-Thélène, Groupe de Brauer non ramifié d'espaces homogènes de tores. *J. Théor. Nombres Bordeaux* **26** (2014), 69-83.

[24] B. Datskovsky, D. J. Wright, Density of discriminants of cubic extensions. *J. reine angew. Math.* **386** (1988), 116–138.

[25] C. Demarche, D. Wei, Hasse principle and weak approximation for multinorm equations. *Israel J. Math.* **202** (2014), no.1, 275-293.

[26] Y. A. Drakokhrust, On the complete obstruction to the Hasse principle. *Amer. Math. Soc. Transl.*(2) **143** (1989), 29–34.

[27] Y. A. Drakokhrust, V. P. Platonov, The Hasse norm principle for algebraic number fields. *Math. USSR-Izv.* **29** (1987), 299–322.

[28] J. S. Ellenberg, A. Venkatesh, The number of extensions of a number field with fixed degree and bounded discriminant. *Ann. of Math.* **163**(2) (2006), 723–741.

[29] B. Fein, M. Schacher, $\mathbb{Q}$-Admissibility Questions for Alternating Groups. *J. Algebra* **142** (1991), 360–382.

[30] C. Frei, D. Loughran, R. Newton, The Hasse norm principle for abelian extensions. *Amer. J. Math* **140**(6) (2018), 1639–1685.

[31] C. Frei, D. Loughran, R. Newton, with an appendix by Y. Harpaz, O. Wittenberg, Number fields with prescribed norms. Preprint. arXiv:1810.06024.

[32] A. Fröhlich, On non-ramified extensions with prescribed Galois group. *Mathematika* **9** (1962), 133–134.

[33] GAP Group, GAP – Groups, Algorithms, and Programming, Version 4.8.10 (2018). Available at https://www.gap-system.org.

[34] P. Gille, T. Szamuely, *Central simple algebras and Galois cohomology.* Cambridge University Press, Cambridge, UK, 2006.

[35] B. Gordon, M. Schacher, Quartic coverings of a cubic. In *Number Theory and Algebra*, Academic Press, New York, 1977, 97–101.

[36] B. Gordon, M. Schacher, The admissibility of A_5. *J. Number Theory* **11** (1979), 489–504.

[37] Groupprops, The Group Properties Wiki, Criterion for element of alternating group to be real. Available at https://groupprops.subwiki.org/wiki/Criterion_for_element_of_alternating_group_to_be_real.

[38] K. W. Gruenberg, *Cohomological Topics in Group Theory.* Lecture Notes in Mathematics **143**, Springer-Verlag, 1970.

[39] F. Gerth, The Hasse norm principle in metacyclic extensions of number fields. *J. London Math. Soc.*, (2) **16** (1977), 203–208.

[40] F. Gerth, The Hasse norm principle for abelian extensions of number fields. *Bulletin of the AMS* **83**(2) (1977) 264–266.

[41] S. Gurak, On the Hasse norm principle. *J. reine angew. Math.* **299/300** (1978), 16–27.

[42] S. Gurak, The Hasse norm principle in non-abelian extensions. *J. reine angew. Math.* **303/304** (1978), 314–318.

[43] H. Hasse, Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol. *Nachr. Ges. Wiss. Göttingen Math.-Phys. Kl.* (1931), 64–69.

[44] D. Higman, Focal series in finite groups. *Canad. J. Math.* **5** (1953), 477–497.

[45] P. N. Hoffman, J. F. Humphreys, *Projective representations of the symmetric groups.* Oxford Mathematical Monographs, Clarendon Press, Oxford, 1992.

[46] M. Horie, The Hasse norm principle for elementary abelian extensions. *Proc. Amer. Math. Soc.* 118(1) (1993) 47–56.

[47] A. Hoshi, A. Yamasaki, Rationality problem for algebraic tori. *Mem. Amer. Math. Soc.* **248** (2017), No. 1176.

[48] A. Hoshi, K. Kanai, A. Yamasaki, Norm one tori and Hasse norm principle. Preprint. arXiv:1910.01469.

[49] A. Hoshi, K. Kanai, A. Yamasaki, Norm one tori and Hasse norm principle II: degree 12 case. Preprint. arXiv:2003.08253.

[50] W. Hürlimann, On algebraic tori of norm type. *Comment. Math. Helv.* **59** (1984), 539-549.

[51] I. M. Isaacs, *Finite group theory.* Graduate Studies in Math. **92** AMS Providence (2008).

[52] W. Jehne, On knots in algebraic number theory. *J. reine angew. Math.* **311/312** (1979), 215–254.

[53] J. W. Jones, D. P. Roberts, A database of local fields. *J. Symb. Comp.* **41** (2006), 80–97. Database available at https://math.la.asu.edu/~jj/localfields/.

[54] G. Karpilovsky, *The Schur Multiplier*. Clarendon Press, Oxford, 1987.

[55] G. Karpilovsky, *Group Representations Vol 2*. North-Holland Mathematics Studies **177**, 1993.

[56] J. Klüners, A counter example to Malle's conjecture on the asymptotics of discriminants. *C. R. Math.*, **340**(6) (2005), 411–414.

[57] B. È. Kunyavskiĭ, Arithmetic properties of three-dimensional algebraic tori. *Zap. Nauch. Sem. LOMI Akad. Nauk SSSR* **16** (1982), 102-107.

[58] L. V. Kuz'min, Homology of profinite groups, Schur multipliers, and class field theory. *Izv. Akad. Nauk SSSR Ser. Mat.* **33** (1969), 1220–1254; English translation: *Math. USSR Izv.* **3** (1969).

[59] T.-Y. Lee, The Tate–Shafarevich groups of multinorm-one tori. Preprint. arXiv:1912.09823.

[60] Y. Liang, Non-invariance of weak approximation properties under extension of the ground field. Preprint. arXiv:1805.08851.

[61] The LMFDB Collaboration, *The L-functions and Modular Forms Database*. Available at http://www.lmfdb.org.

[62] A. Macedo, The Hasse norm principle for A_n-extensions. *J. Number Theory* **211** (2020), 500–512.

[63] A. Macedo, GAP code (2019). Available at https://sites.google.com/view/andre-macedo/code.

[64] A. Macedo, R. Newton, Explicit methods for the Hasse norm principle and applications to A_n and S_n extensions. *Math. Proc. Camb. Philos. Soc.*, to appear. Preprint. arXiv:1906.03730.

[65] A. Macedo, On the obstruction to the Hasse principle for multinorm equations. *Israel J. Math.*, to appear. Preprint. arXiv:1912.11941.

[66] A. Macedo, A note on the density of D_4-fields failing the Hasse norm principle. In preparation.

[67] S. Mäki, On the density of abelian number fields. *Ann. Acad. Sci. Fenn. Ser. A I Math. Diss.* **54** (1985).

[68] S. Mäki, The conductor density of abelian number fields. *J. London Math. Soc.* (2) **47** (1993), 18–30.

[69] G. Malle, On the distribution of Galois groups. *J. Number Theory* **92**(2) (2002), 315–329.

[70] G. Malle, On the distribution of Galois groups, II. *Experiment. Math.* **13**(2) (2004), 129–135.

[71] J. S. Milne, Class Field Theory, Version 4.03 (2020). Available at http://www.jmilne.org/math/CourseNotes/CFT.pdf.

[72] J. Neukirch, *Algebraic Number Theory.* Grundlehren der mathematischen Wissenschaften **322**, Springer-Verlag, Berlin, 1999.

[73] T. Ono, Arithmetic of algebraic tori. *Ann. of Math.* **74** (1961), 101–139.

[74] H. Opolka, Zur Auflösung zahlentheoretischer Knoten. *Math. Z.* **173** (1980) 95–103.

[75] V. Platonov, A. Rapinchuk, *Algebraic groups and number theory.* Pure and Applied Mathematics **139**, Academic Press, Inc., Boston, MA, 1994.

[76] T. Pollio, On the multinorm principle for finite abelian extensions. *Pure Appl. Math. Q.* **10** (2014), 547-566.

[77] T. Pollio, A. S. Rapinchuk, The multinorm principle for linearly disjoint Galois extensions. *J. Number Theory* **133** (2013), 802-821.

[78] G. Prasad, A. S. Rapinchuk, Local-global principles for embedding of fields with involution into simple algebras with involution. *Comment. Math. Helv.* **85** (2010), 583-645.

[79] M. J. Razar, Central and genus class fields and the Hasse norm theorem. *Compositio Math.* **35** (1977), 281–298.

[80] N. Rome, The Hasse norm principle for biquadratic extensions. *J. Théor. Nombres Bordeaux* **30** No. 3 (2018), 947–964.

[81] J.-J. Sansuc, Groupe de Brauer et arithmétique des groupes algébriques linéaires sur un corps de nombres. *J. reine angew. Math.* **327** (1981), 12–80.

[82] M. Schacher, Subfields of division rings I. *J. Algebra* **9** (1968) 451–477.

[83] A. Scholz, Totale Normenreste, die keine Normen sind, als Erzeuger nichtabelscher Korpererweiterungen II. *J. reine angew. Math.* **182** (1940), 217–234.

[84] J. Schur, Über die Darstellung der symmetrischen und der alternierenden Gruppe durch gebrochene lineare Substitutionen. *J. reine angew. Math.* **139** (1911), 155–250.

[85] A. Shankar, I. Varma, Malle's Conjecture for Galois octic fields over $\mathbb{Q}$. In preparation.

[86] A. N. Skorobogatov, *Torsors and rational points.* Cambridge Tracts in Mathematics **144**, Cambridge University Press, 2001.

[87] T. A. Springer, *Linear algebraic groups.* Vol **9** of Progress in Mathematics. Birkhauser Boston Inc., Boston, MA., 1998.

[88] L. Stern, Equality of norm groups of subextensions of S_n $(n \leq 5)$ extensions of algebraic number fields. *J. Number Theory* **102**(2) (2003), 257–277.

[89] S. Türkelli, Connected components of Hurwitz schemes and Malle's conjecture. *J. Number Theory* **155** (2015), 163–201.

[90] K. Uchida, Unramified extensions of quadratic number fields I. *Tohoku Math. J.* **22** (1970), 220–224.

[91] V. E. Voskresenskiĭ, Birational properties of linear algebraic groups. *Izv. Akad. Nauk SSSR Ser. Mat.* **34** (1970) 3–19. English translation: *Math. USSR-Izv.* Vol. **4** (1970), 1–17.

[92] V. E. Voskresenskiĭ, Maximal tori without affect in semisimple algebraic groups. Mat. Zametki **44** (1988) 309–318; English transl. in Math. Notes **44** (1989) 651–655.

[93] V. E. Voskresenskiĭ, B. È. Kunyavskiĭ, Maximal tori in semisimple algebraic groups. Manuscript deposited at VINITI 15.03.84, No. 1269-84, 28pp. (in Russian)

[94] J. Wang, Malle's Conjecture for $S_n \times A$ for $n = 3, 4, 5$. *Compositio Math.* **157**(1) (2021), 83–121.

[95] E. Weiss, *Cohomology of Groups.* Pure and Applied Mathematics **34**, Academic Press, 1969.

[96] R. A. Wilson, *The finite simple groups.* Graduate Texts in Mathematics **251**, Springer-Verlag, 2009.

[97] S. Wong, Automorphic forms on $GL(2)$ and the rank of class groups. *J. reine angew. Math.* **515** (1999), 125–153.

[98] M. M. Wood, On the probabilities of local behaviors in abelian field extensions. *Compositio Math.* **146** (2010), 102–128.

[99] M. M. Wood, Asymptotics for number fields and class groups. In *Directions in Number Theory: Proceedings of the 2014 WIN3 Workshop*. Springer, New York, 2016.

[100] D. J. Wright, Distribution of discriminants of abelian extensions. *Proc. London Math. Soc.*, **58**(1) (1989), 17—50.