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

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

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 $\mathrm{Spec}(K[t,t^{-1}])$ 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
$\mathrm{Pic}\, X$	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
$\hat{T}$	the character group $\mathrm{Hom}(\overline{T}, \mathbb{G}_{m,\overline{K}})$ 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 $h \in H, g \in G$
${}^{G}(H)$	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
$\hat{G}$	the $\mathbb{Q}/\mathbb{Z}$-dual $\mathrm{Hom}(G,\mathbb{Q}/\mathbb{Z})$ of G
G_p	a Sylow p-subgroup of G
$H_i(G,A)$	the i-th homology group
$H^i(G,A)$	the i-th cohomology group

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

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 '$\simeq$' to indicate a canonical isomorphism between two objects.

[1] Since $\hat{H}^q(G;A) = H^q(G;A)$ 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

Lemma 1.1.2. Let $K \quad H \quad G$ be a tower of groups with $[G : K]$ nite. Then

$$\mathrm{Res}^G_K = \mathrm{Res}^H_K \quad \mathrm{Res}^G_H \text{ and } \mathrm{Cor}^G_K = \mathrm{Cor}^G_H \quad \mathrm{Cor}^H_K :$$

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

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

$$\mathrm{Cor}^G_H \quad \mathrm{Res}^G_H : \hat{H}^i(G; A) \,!\, \quad \hat{H}^i(G; A)$$

equals the multiplication by1082 Td3Td [(i)]TJ 8213.759 0 Td [([)]TJ/F43 11.9552 Tf 3.252 0 Td [(G)]

Proof. See [15, III, Proposition 9.55(i)].

$(G; A($

Lem09

i

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

$$H^i(G;\mathrm{Ind}_H^G(A)) \cong H^i(H;A)$$

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

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

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 $H^i(H;\mathbb{Z}[G]) = 0$ 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

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

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

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

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

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

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

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

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

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)

$$\begin{aligned} \cup : H^i(G; A) \otimes H^j(G; B) &\to H^{i+j}(G; A \otimes B) \\ (a; b) &\mapsto a \cup b \end{aligned}$$

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

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

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

2552 Tf 10.036 0 Td [(l5 d913ules)-350(c)50(omm,[(0)]TJ/F436-2.les]0 d 124.9.015 1 Tf 6.587 0 T
$a \cup b$

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

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

where the map δ on the left denotes the connecting homomorphism

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

and δ on the right denotes the connecting homomorphism

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

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

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

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

Proof. See [71, II, Proposition 1.38]. $\square$

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

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

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

Proof. See [15, VI, Theorem 7.4]. $\square$

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 $\mathrm{Res}^G_H : \hat{H}^i(G;\mathbb{Z}) \to \hat{H}^i(H;\mathbb{Z})$ is the corestriction map $\mathrm{Cor}^G_H : \hat{H}^{-i}(H;\mathbb{Z}) \to \hat{H}^{-i}(G;\mathbb{Z})$.

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

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

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

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

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

We thus have a commutative diagram

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

Definition 1.3.2. The homology group $\hat{H}^{3}(G;\mathbb{Z})$ 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 $\hat{H}^{3}(G;\mathbb{Z})$ 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

1.4 Algebraic tori

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

Definition 1.4.1. An algebraic torus T (or torus, for simplicity) over k is a k-algebraic group such that, over $\bar{k}$, T becomes isomorphic to

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 $(R_{K/k}X)(S) = X(S\otimes_k K)$ 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 $\hat{T} \cong \mathbb{Z}[G/H]$ 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

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

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 $x\in T(\bar{k})$ as $x = \bigoplus_{gH\in G/H} x_{gH}$ for uniquely determined $x_{gH}\in \bar{k}^\times$. Define $\chi_{gH} : T_{\bar{k}} \to \mathbb{G}_{m,\bar{k}}$ 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

$$\varphi : \mathbb{Z}[G/H] \to \hat{T}, \qquad gH \mapsto \chi_{gH}$$

is an isomorphism. We prove that φ is G-equivariant, finishing the proof of the lemma. Note that the action of $G_k = \mathrm{Gal}(\bar{k}/k)$ 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 $\hat{T}$ is induced by the action of G_k on $\hat{T}$ and π. It thus suffices to check that φ is G_k-equivariant. Since the G_k-action on $T(\bar{k})$ is given by $(\sigma x)_{gH} = \sigma(x_{\pi(\sigma)^{-1}gH})$, we have

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

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

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

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*

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

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*

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

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

Proof. Voskresenskiĭ showed (see [91, Theorem 1]) that there exists a canonical isomorphism of G_k-modules $\operatorname{Pic}(\overline{X_1}) \oplus P_1 \cong \operatorname{Pic}(\overline{X_2}) \oplus P_2$ 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 $H^1(k, \mathbb{Z}[G_k/H]) = H^1(H, \mathbb{Z}) = \operatorname{Hom}(H, \mathbb{Z}) = 0$ by Shapiro's lemma 1.1.7, we deduce that $H^1(k, \operatorname{Pic} \overline{X_1}) = H^1(k, \operatorname{Pic} \overline{X}$

Voskresenski proved Theorem 1.5.8 by working with a asque resolution of $\hat{T}$, 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 nite 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 asque if $\hat{H}$if G

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

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*

$$Ш(T) \cong Ш^2(G;\hat{T}); \tag{1.5.4}$$

where $Ш^2(G;\hat{T}) = \mathrm{Ker}\ H^2(G;\hat{T}) \xrightarrow{\mathrm{Res}} \prod_{v \in k} H^2(D_v$

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

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

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:

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

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

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

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

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

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]

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

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 $\text{Gal}(N/k) = D_n$ 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 $\mathrm{Gal}(N/k) = S_n$, 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 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

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

(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 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 $H^1(k, \mathrm{Pic}\,\overline{X})$ 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 $H^1(k, \mathrm{Pic}\,\overline{X})$ (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

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 Kunyavski in his work [57] on the arithmetic of three-dimensional tori:

Theorem 3.1.1 (Kunyavski)**.** *Let K/k be a quartic extension of number fields and let N/k be its normal closure. If $\mathrm{Gal}(N/k) = A_4$, 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 5 extension of number elds and let $N=k$ be its normal closure. If $\mathrm{Gal}(N=k) = A_n$, then the HNP holds for $K=k$ and weak approximation holds for the norm one torus $R^1_{K=k}\,G_m$.

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 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 di erent 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-

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

[redacted]

Lemma 3.2.4. In the notation of Proposition 3.2.2, the group $V := {}^{1}(A_n)$ de nes a [redacted] Schur covering group of A_n for $n = 4; 5$ or any $n \quad 8$.

Proof. It is well-known that A_n is generated by the $n \quad 2$ permutations $\overline{e_i} := \overline{t_1} \cdot \overline{t_{i+1}} =$ $(1\ 2)(i+1\ \ i+2)$ for [illegible]

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 to $W := {}^{-1}(H)$ 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 is surjective, $y = (x)$ for some $x \in U$ and hence $z = z^x = [e_1^{-1} e_2 e_1; e_2]^x = [(e_1^{-1} e_2 e_1)^x; e_2^x]$ 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} S

Using this lemma we show the vanishing of the cohomology group $H^2(G; J_{G/H})$ (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 $H^2(G; J_{G/H}) = 0$.*

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

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

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

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

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

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

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

$$H^3(G; \mathbb{Z}) \xrightarrow{\epsilon^*} H^3(G; \mathbb{Z}[G/H]) \xrightarrow{\cong} H^3(H; \mathbb{Z})$$

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

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

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

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

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

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 $\{1, \dots, n\}$ gives a homomorphism $\phi : G \to S_n$. Since A_n is simple, ϕ is injective and therefore $\operatorname{Im} \phi = A_n$. Finally, note that $\phi(H)$ is a point stabilizer of a letter in $\{1, \dots, n\}$ and so $\phi(H) = A_{n-1}$. It follows that the restriction of ϕ to H gives an isomorphism $H \cong A_{n-1}$. □

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

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

for every $n \geq 6$

- 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 $H^1(G; M_G)$ 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 $G = \mathrm{Gal}(N/k) = A_6; H = \mathrm{Gal}(N/K)$ and $T = R^1_{K/k}\mathbb{G}_m$. Note that $H = A_5$ by Lemma 3.2.8 and that $\hat{T} = J_{G/H}$ (as G-modules) by Proposition 1.6.5. Therefore, by Theorems 1.5.8 and 1.5.12 it is enough to prove that $H^1(G; F_{G/H}) = 0$, 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 Norm1TorusJ59lhm

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 $H^1(k, \operatorname{Pic} \overline{X})$ 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 $Ш(T)$, $H^1(k, \operatorname{Pic} \overline{X})$ 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

Theorem 4.1.1. Let $L=K=k$ be a tower of nite extensions. Let $T_0 = R^1_{L=k} G_m$, let $T = R^1_{K=k} G_m$

As a corollary, one can use this object to compute the p-primary parts of the knot group, the invariant $H^1(k; \mathrm{Pic}$

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 $T \; _k K$ is stably rational. Consequently, $H^1(K; \operatorname{Pic} \overline{X}) = 0$ and $H^1(k; \operatorname{Pic} \overline{X})$ is killed by $[K : k]$.

[illegible] $: K]$ and let $[d]$ denote the map $x \mapsto x^d$. The natural inclusion j [illegible] s es $N_{L/K} \circ j = [d]$. Using i and j, we obtain a morphism of [illegible]

$$\phi : S \times R_{K/k} G_m \to R_{L/k} G_m$$
$$(x; y) \mapsto i(x) j(y)$$

No[illegible] Ker ϕ, i.e. $i(x)j(y) = 1$, then $j(y) \in S$ and the[illegible] $y)) = y^d$. W[illegible] Ker $\phi = \{(i^{-1}(j(x)); x^{-1}) \mid x \in R_{K/k}\,\mu_d\}$ [illegible] group of d-th ro[illegible]ite. Moreover, ϕ is surjective: give[illegible], we have $N_{L/K}(z)$ [illegible] $\in R_{K/k} G_m(\bar{k})$, and thus $N_{L/K}(z)$ [illegible] which gives $z = \phi(x; y)$ [illegible] We conclude that ϕ is an iso[illegible] killed by d.

Let Z, W a[illegible] compactifications of S, [illegible] G_m, respectively. By [91, Lemma [illegible] Pic $\bar{Z} \oplus$ Pic $\bar{W}$. Th[illegible] yields

$$[illegible]\ H^1(k; \mathrm{Pic}\,\bar{W})_{(p)}\ [illegible]_{(p)}:$$

Furthermore, $R_{K/k} G_m$ [illegible] k-ration[illegible] $) = H^1(k; \mathrm{Pic}\,\bar{W}_0) = 0$ by [20, Proposition 6] and [illegible]$_{(p)}$ [illegible] $X(S)_{(p)} = A(S)_{(p)} = 0$ by Theorem 1.5.8. The resu[illegible]n of Corollary 4.2.5 similar to the one done above, but to [illegible]

$$[illegible]_m$$

whose finite kernel is killed by d. □

The following special case [illegible]he calculation of $A(T)$, $H^1(k; \mathrm{Pic}\,\bar{X})$ and $X(T)$ to the case whe[illegible]up.

Corollary 4.2.6. Let L[illegible] of [illegible] with L/k Galois. Let $G = \mathrm{Gal}(L/k)$ and $H = \mathrm{Ga}$[illegible]rime, le[illegible]ylow p-sub[illegible]

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 $H^1(k; \operatorname{Pic} \overline{X})_{(p)} = H^3(G; \mathbb{Z})_{(p)}$.

(ii) If H contains a Sylow p

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

$$\varphi : K(K/k) \to K(L/k)$$

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

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.

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

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

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 $H^1(k, \mathrm{Pic}\,\overline{X})$ 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 $\prod_{q\neq p} G_q$, 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) $\Rightarrow$ (ii): Follows from Corollary 4.2.10.

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

(iii) $\Rightarrow$ (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 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 $N_{L/K}$:

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

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 their results here in a slightly more general setting. Let G be a finite group, let $H \subseteq G$, and let S be a set of subgroups of G. Consider the following commutative diagram:

$$\begin{tikzcd} H/[H,H] \arrow[rr, "\alpha_1"] & & G/[G,G] \\ \bigoplus_{D\in S} \bigoplus_{Hx_iD \in H\backslash G/D} H_i/[H_i,H_i] \arrow[u, "\varphi_1"] \arrow[rr, "\alpha_2"] & & \bigoplus_{D \in S} D/[D,D] \arrow[u, "\varphi_2"'] \end{tikzcd} \tag{4.3.2}$$

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 $\alpha_1; \varphi_1$ 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

$$\alpha_2(h[H_i;H_i]) = x_i^{-1}hx_i[D;D] \in D/[D;D]:$$

Given a subgroup $D \in S$, we denote by α_2^D the restriction of the map α_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), $\varphi_1(\mathrm{Ker}\,\alpha_2^D) \subseteq \varphi_1(\mathrm{Ker}\,\alpha_2^{D'})$ whenever $D \subseteq D'$.

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

[r5]TJ/F79 11.9552 Tf 11.9552 552 Tf 9.528 0 Td [(he)-363(de)50(c)50(52 55

the set of double cosets in the decomposition $G =$

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

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

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

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

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 $\mathcal{C}$ be the set of all cyclic subgroups of G and let $\varphi_1^{\mathcal{C}}$ and $\psi_2^{\mathcal{C}}$ denote the relevant maps in diagram (4.3.2) with $\mathcal{S} = \mathcal{C}$. Then

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

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 $F(L/K/k)$ is trivial. In fact, since $[N_G(H), H] \subseteq \Phi^G(H)$, if one can show that $[N_G(H), H] = H \cap [G, G]$, then $F(L/K/k) = 1$. 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

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

By Theorem 1.5.12 and Lemmam

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 $F_{nr}(L/K/k) = F(L/K/k) = 1$.*

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

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

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

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

$$H^1(k, \operatorname{Pic} \overline{X}) \cong \operatorname{Ker} {}_1/\varphi_1(\operatorname{Ker} {}^{nr}_2 {}_1/\varphi$$

Lemma 4.3.13. We have $F(\overline{G};\overline{H}) = F(G;H)$ if and only if Ker \ $[\overline{G};\overline{G}]$ $^{\overline{G}}(\overline{H})$, where the notation is as in Theorem 4.1.4.

Proof. Let : $F(\overline{G};\overline{H})$! $F(G;H)$

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

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 $H^1(k; \mathrm{Pic}\,\overline{X})$ 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 modi cation 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 nite 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, de ned as follows:

De nition 4.4.2. [47, De nition 1.26] Let n be a positive integer and let G be a nite subgroup of $GL_n(Z)$. The G-lattice M_G of rank n is de ned to be the G-module with

Z-basis f u/F40 211.95582 Tfsrm10 211.95582 Tfs21.95582 Tf44 7.9701Td [(J)]T Tf44 u(M)]TJ/F44 7.9701 Tf 39.889 -1.793 Td [(n)]TJ/630 11.955

2. If $(i) = d$, 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 $h R_g$ j $g \in G i$ $GL_{d\ 1}(\mathbb{Z})$. 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 $H^1(G; F_{G=H})$ 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 $H^1(k; \mathrm{Pic}\,\overline{X})$ in terms of generalized representation groups of G. We also implemented this formula, along with the simpli cation a orded 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 $H^1(k; \mathrm{Pic}\,\overline{X})$ 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 $^G(H)$, which is generally fast for small subgroups H but impractical for large ones. On the contrary, Hoshi and Yamasaki's method using asque resolutions deals only with the G-module $J_{G=H}$, whose $\mathbb{Z}$-rank $\frac{jGj}{jHj}$ 1 decreases as j(the8.88 0 Td9=o)-27[(j)]0(fast)-260(f)-1(o)1(frne2f 8.45i's)-5 44.628 (A2)-9w7s3 44.628

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 Rg

   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
```

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

```
Fquot:=function(G,H)
# Function that computes the group (H ∩ [G,G]) / Φ^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
  Φ^G(H) = ⟨h1^-1 h2 | h1,h2 ∈ H are G-conjugate⟩, 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 λ : Ḡ → G, where Ḡ
is a Schur covering group of G
    M:=Kernel(lambda);
    HH:=PreImagesSet(lambda,H); # HH = λ^-1(H)

    res:=Subgroup(HH,[]);

    if Size(HH)=1 then return res;
    else # We compute the p-part F(Ḡ,H̄)_(p) for all primes p | |H̄| 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
F(Ḡ,H̄)_(p) = F(Ḡ,H̄_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 $H^1(k,\operatorname{Pic}\overline{X})$ for an extension K/k with degree 1260 and A_7-normal closure (note that $|A_7| = 2520 = 2\cdot 1260$):

```
    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 λ : Ḡ → G, where Ḡ 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 Cor^G_{D_v}(Ĥ^{-3}(D_v,Z)) = M ∩ [λ^{-1}(D_v), λ^{-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 Ш(T)
```

```
end;
```

Example: Computation of $K(L=k)$ for an octic D_4-extension $L=k$ with decomposition group V_4 at all rami ed places and for an octic D_4-extension with cyclic decomposition group C_2 at all rami ed 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 $F(L=K=k)$ 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]]
```

```
    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 ' 1(Ker v 2) 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 Hw 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 L wjv Hw in
Diagram 4.3.3
        res:=[];;
```

```
        for i in Sx do # Looping over all elements of  ⊕_{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 ⊕_{w|v} H_w that are in Ker ψ_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 φ_1 of
every element in Ker ψ_2^v

        return Subgroup(K/DerivedSubgroup(H),im); # Returning the group φ_1(Ker ψ_2^v)
    fi;
end;

obsram:=function(G,H,l)
# Function that computes the group φ_1(Ker ψ_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 Ker ψ_2^v for v ramified
    od;

    return Subgroup(K/DerivedSubgroup(H),li); # Outputting the group
∏_{v ramified} φ_1(Ker ψ_2^v) = φ_1(Ker ψ_2^r)

end;
```

```
obsunr:=function(G,H)
    local K,l,h1,h2,f,im;
# Function that computes the group ' 1(Ker nr 2) (in the notation of p. 44), which
equals 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 G(H) = hh1 1h2 j h1; h2 2 H are G-conjugate i (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 ' 1(Ker nr 2)
end;

1obs:=function(G,H,l)
# Function that computes the group F(L=K=k) = Ker 1=' 1(Ker 2) (Theorem 4.3.5)
by invoking all the previous functions

    local K,Elts,J;

    K:=Intersection(H,DerivedSubgroup(G)); # Note that H \ [G;G] = Ker 1
    Elts:=Concatenation(Elements(obsunr(G,H)),Elements(obsram(G,H,l)));
# Concatenation of the elements in ' 1(Ker nr 2) and ' 1(Ker r 2)
    J:=Subgroup(K/DerivedSubgroup(H),Elts); # Computing the group ' 1(Ker 2) =
' 1(Ker nr 2)' 1(Ker r 2)

    return K/J; # Outputting the group Ker 1=' 1(Ker 2)
end;
```

Example: Computation of 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

Recall that Theorem 1.6.9, due to Tate, shows that the knot group of the Galois extension L/k is dual to $\mathrm{Ker}(H^3(G,\mathbb{Z}) \to \prod_v H^3(D_v,\mathbb{Z}))$, 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 $H^3(D_v,\mathbb{Z}) = 0$. 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 $H^1(k,\mathrm{Pic}\,\overline{X})$

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 K

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 Voskresenski's exact sequence (1.5.1) of Theorem 1.5.8.

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

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

Remark 5.1.11. Proposition 5.1.10 and Voskresenski'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 Voskresenski and Kunyavski'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 $H^1(k, \operatorname{Pic} \overline{X})$ with $H^1(G, F_{G/H})$ to make clear that this group only depends on the pair (G, H).

First, we complete the proof of Theorem 5.1.1

(ii) $K(K{=}k)_{(2)} = K(L{=}k)_{(2)}$ and $K(K{=}k)_{(2)}$ 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. See Schur's original paper [84] or [45

```
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 $h = (1\ 2)(3\ 4)\quad(n\quad 1\ n)(n+1\ \ n+2)$. Denoting the permutation $(1\ 2)(3\ 4)\quad(n\quad 1\ n)$ by $\tilde{h}$, write $h = \tilde{h}{:}t_{n+1}$. Now

$$[\quad{}^{1}(h);\quad{}^{1}(x)] = [\quad{}^{1}(\tilde{h})\overline{t_{n+1}};\quad{}^{1}(x)] = [\quad{}^{1}(\tilde{h});\quad{}^{1}(x)]^{\overline{t_{n+1}}}[\overline{t_{n+1}};\quad{}^{1}(x)]:$$

By the inductive hypothesis and the relations of Proposition 5.2.2, $[\quad{}^{1}(\tilde{h});\quad{}^{1}(x)]^{\overline{t_{n+1}}} = z^{\overline{t_{n+1}}} =$

Remark 5.2.5. The method employed in this section to provide explicit and computable formulas for the knot group and the invariant $H^1(k, \operatorname{Pic} \overline{X})$ in A_n and S_n extensions works for other families of extensions. For example, let G' be any finite group such that $H^3(G', \mathbb{Z}) = \mathbb{Z}/2$. 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 $F(G, H)$ (and thus, by Theorems 4.1.2, 5.1.1 and isomorphism (1.5.2), of the invariant $H^1(G, F_{G/H})$ as well).

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

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 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 $F(A_n; H)$. One can compute that $F(A_{12}; H) = C_3$ 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

$$F(A_n; H)_{(2)} = F(S_n; H)_{(2)} = C_2^k.$$

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 $h_1; \ldots; h_{i-1}$;
- 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 $H \subseteq A_n$. It is straightforward to check that one then has $\Phi^{A_n}(H) = \Phi^{S_n}(H) = 1$. Therefore, $F(A_n; H) = H \cap [A_n; A_n] = H = C_2^k$ and similarly for $F(S_n; H)$. □

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 $G \not\cong A_6$ 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 $H^1(k; \operatorname{Pic} \overline{X})$ 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 $H^1(k, \operatorname{Pic} \overline{X})_{(p)} = 0$ for a prime $p > 3$ and that $H^1(k, \operatorname{Pic} \overline{X})_{(3)} = 0$ if $G = S_n$. Theorem 4.1.2 gives $\mathcal{F}_{nr}(L/K/k) = F(G, H)$. By Theorem 5.1.3, $H^1(k, \operatorname{Pic} \overline{X})_{(3)}$ is 3-torsion, so Theorem 5.1.1 gives $H^1(k, \operatorname{Pic} \overline{X})_{(3)} = F(G, H)[3]$. Let $K_3 = L^{H_3}$ and let X_3

the A_n-conjugacy class of . Since the S_n-conjugacy class of splits as a disjoint union C t gCg ^{1} for any g 2 S_n n A_n, it is enough to show that x 2 A_n if and only if l is even. We study the cycle structure of x by analyzing the xed points of its powers. Ob9a0hy of

Conversely, assume that $n \geq 5$ is equal to $\sum_{i=1}^{k} 3^{r_i}$ 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

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

We will prove that $F(A_n;H)_{(3)} = C_3$. 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 $\Phi^{A_n}(H) \leq \langle h^3 \rangle$. 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

presented as Algorithm A4 in the Appendix 4.5. The computation of $K(L=k)$ 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 $H^3(G;$ then

We now solve the non-Galois case. Once again, we compute the invariant $H^1(k, \operatorname{Pic} \overline{X}) = H^1(G, F_{G/H})$ 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 $\mathfrak{K}(K/k)$ on

Proposition 5.3.5. (i) If $H = C_2$ or D_5, then $K(K=k) = K(L=k)$;

(ii) If $H = C_4$ or C_5 o C_4, then

$$K(K=k) = K(L=k)_{(3)} \quad K(M=k) = K(L=k)_{(3)} \quad F(L=M=k);$$

where M is the xed eld of a copy of $(C_3 \quad C_3)$ o C_4 inside G containing $H_2 = C_4$.

Proof. First, note that in all cases $K(K=k)_{(3)} = K(L=k)_{(3)}$, by Theorem 4.1.1. By Proposition 5.1.10 and Theorem 1.5.8, it only remains to compute $K(K=k)_{(2)}$. For case (i), let A be a copy of S_3 inside G such that $A \setminus H$ Now 4.1 Tdk 7.970 5.0 ...

C_2 7.970130 11.9552 Tf 7.307 00 0 03(7.970...

5.4 Appendix: Computation of $H^1(k; \mathrm{Pic}\,\overline{X})$ 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

$G = A_4$		
[K : k]	H	$H^1(G; F_{G=H})$
12	1	Z=2
6	C_2 = h(1; 2)(3; 4)i	Z=2
4	C_3 = h(1; 2; 3)i	Z=2
3	V_4 = h(1; 2)(3; 4); (1; 3)(2; 4)i	0

Table 2

$G = S_4$		
[K : k]	H	$H^1(G; F_{G=H})$
24	1	Z=2
12	C_2a = h(1; 2)i	0
12	C_2b = h(1; 2)(3; 4)i	Z=2
8	C_3 = h(1; 2; 3)i	Z=2
6	C_4 = h(1; 2; 3; 4)i	0
6	V_4 = h(1; 2); (3; 4)i	0
6	V_4 = h(1; 2)(3; 4); (1; 3)(2; 4)i	0
4	S_3 = h(1; 2; 3); (1; 2)i	0
3	D_4 = h(1; 2; 3; 4); (1; 3)i	0
2	A_4 = h(1; 2)(3; 4); (1; 2; 3)i	0

Table 3

$G = A_5$		
$[K : k]$	H	$H^1(G; F_{G=H})$
60	1	$Z=2$
30	$C_2 = h(1; 2)(3; 4)i$	$Z=2$
20	$C_3 = h(1; 2; 3)i$	$Z=2$
15	$V_4 = h(1; 2)(3; 4); (1; 3)(2; 4)i$	0
12	$C_5 = h(1; 2; 3; 4; 5)i$	$Z=2$
10	$S_3 = h(1; 2; 3); (1; 2)(4; 5)i$	$Z=2$
6	$D_5 = h(1; 2; 3; 4; 5); (2; 5)(3; 4)i$	$Z=2$
5	$A_4 = h(1; 2)(3; 4); (1; 2; 3)i$	0

Table 4

$G = S_5$		
$[K : k]$	H	$H^1(G; F_{G=H})$
120	1	$Z=2$
60	$C_2a = h(1; 2)i$	0
60	$C_2b = h(1; 2)(3; 4)i$	$Z=2$
40	$C_3 = h(1; 2; 3)i$	$Z=2$
30	$C_4 = h(1; 2; 3; 4)i$	0
30	$V_4a = h(1; 2); (3; 4)i$	0
30	$V_4b = h(1; 2)(3; 4); (1; 3)(2; 4)i$	0
24	$C_5 = h(1; 2; 3; 4; 5)i$	$Z=2$
20	$C_6 = h(1; 2; 3); (4; 5)i$	0
20	$S_3a = h(1; 2; 3); (1; 2)i$	0
20	$S_3b = h(1; 2; 3); (1; 2)(4; 5)i$	$Z=2$
15	$D_4 = h(1; 2; 3; 4); (1; 3)i$	0
12	$D_5 = h(1; 2; 3; 4; 5); (2; 5)(3; 4)i$	$Z=2$
10	$A_4 = h(1; 2)(3; 4); (1; 2; 3)i$	0
10	$S_3 \quad C_2 = h(1; 2; 3); (1; 2); (4; 5)i$	0
6	C_5 o $C_4 = h(1; 2; 3; 4; 5); (2; 3; 5; 4)i$	0
5	$S_4 = h(1; 2; 3; 4); (1; 2)i$	0
2	$A_5 = h(1; 2; 3; 4; 5); (1; 2; 3)i$	0

Table 5

$G = A_6$		
$[K : k]$	H	$H^1(G; F_{G=H})$
360	1	$Z{=}6$
180	$C_2 =$	

Table 6

$G = A_7$		
$[K : k]$	H	$H^1(G; F_{G=H})$
2520	1	$Z=$

Chapter 6

Examples

6.1 $(G; H)$-extensions

This section concerns the existence of number elds 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].

De nition 6.1.1. An extension $K=k$ of number elds is said to be k-adequate if K is a maximal sub eld of a nite 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, Ÿ9, Ÿ11]). 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 nite group G there exists a number eld k and a k-adequate Galois extension $L=k$ with $\mathrm{Gal}(L=k) = G$.

Let G be a nite group and H a subgroup of G. We de ne a $(G; H)$-extension of a number eld k to be an extension $K=k$ for which there exists a Galois extension $L=k$ containing $K=k$ such that $\mathrm{Gal}(L=k) = G$ and $\mathrm{Gal}(L=K) = H$. We write $F_{G=H}$ for a asque module in a asque 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 $H^1(G, F_{G/H}) \neq 0$ 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 $H^1(G, F_{G/H}) \neq 0$ 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,

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

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

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

is injective. It follows that $X(T) = 0$ and so $K(K/k)$ 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 Gal(1.5.12) and $(F_{G/H}) = 0$ then t

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 $G = S_n$ the groups $\mathfrak{K}(K/k)$ and A

- For $G = A_5$, let $K = Q(\ )$, where is a root of the polynomial $x^5 \quad x^4 + 2x^2 \quad 2x + 2$, and let $L{=}Q$ be the normal closure of $K{=}Q$. We have $\mathrm{Gal}(L{=}Q) = A_5$ and there exists a prime p of K above 2 with rami cation 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 $L{=}Q$.

- For $G = S_5$, take $K = Q(\ )$, where is a root of the polynomial $x^{10} \quad 4x^9 \quad 24x^8 + 80x^7 + 174x^6 \quad 416x^5 \quad 372x^4 + 400x^3 + 370x^2 + 32x \quad 16$, and let $L{=}Q$ be the normal closure of $K{=}Q$. One can verify that $\mathrm{Gal}(L{=}Q) = S_5$ and that there is a prime p of K above 2 with rami cation index 8. By the same reasoning as in the A_5

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 $\mathrm{Gal}(L/\mathbb{Q}) = G$. 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 AG

A s29n]TJ/F43 1.95

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 $K = (K_1, \dots, K_n)$ 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

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

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 $K(K; k)$ 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 $H^1(k, \operatorname{Pic} \overline{X})$ and $H^1(k, \operatorname{Pic} \overline{Y})$, 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 $F = \bigcap_{i=1}^{n} K_i$. In particular, we show (Theorem 9.2.1) that under certain conditions there is an isomorphism

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

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

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

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 Sec 10.655 0 eC0 0f7 0fin[

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 $K = (K_1, \dots, K_n)$ of finite extensions of k and a finite Galois extension L/k containing all the fields $K_1, \dots, K_n$. We denote $G = \mathrm{Gal}(L/k)$, $H_i = \mathrm{Gal}(L/K_i)$ for $i = 1, \dots, n$ and $H = \langle H_1, \dots, H_n \rangle$, the subgroup of G generated by all the H_i. Note that $H = \mathrm{Gal}(L/F)$, where $F = \bigcap_{i=1}^{n} K_i$.

8.1 The first obstruction to the multinorm principle

Definition 8.1.1. We define the first obstruction to the multinorm principle for K corre-

K(K; k

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 $\hat{H}^2(G; C_L)$. The hypothesis is thus equivalent to the map

$$\bigoplus_{i=1}^{t} \bigoplus_{j=1}^{r_i} \mathrm{Cor}_{G_{i,j}}^{G} : \bigoplus_{i=1}^{t} \bigoplus_{j=1}^{r_i} \hat{H}^{-1}(G_{i,j}; C_L) \to \hat{H}^{-1}(G; C_L) \tag{8.1.2}$$

being surjective. Using the definition of the Tate cohomology group $\hat{H}^{-1}$

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 $G = \bigcup_{i=1}^{s} Hx_iD_v$. 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 $i = 1, \dots, n$, let $G = \bigcup_{t=1}^{r_i} H_ix_{i,t}D_v$ 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:

$$\begin{tikzcd} \bigoplus_{i=1}^{n} H_i^{ab} \arrow[r, "\psi_1"] & G^{ab} \\ \bigoplus_{i=1}^{n}\Big(\bigoplus_{v\in\Omega_k}\Big(\bigoplus_{w|v} H_{i,w}^{ab}\Big)\Big) \arrow[u, "\varphi_1"] \arrow[r, "\psi_2"] & \bigoplus_{v\in\Omega_k} D_v^{ab} \arrow[u, "\varphi_2"'] \end{tikzcd} \tag{8.1.4}$$

Here the superscript ^{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 $\bigoplus_{i=1}^{n}\big(\bigoplus_{w|v} H_{i,w}^{ab}\big)$ (respectively, $\bigoplus_{i=1}^{n}\big(\bigoplus_{\substack{v\in\Omega_k \\ v \text{ unramified}}}\big(\bigoplus_{w|v} H_{i,w}^{ab}\big)\big)$). 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*

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

Proof. Diagram (8.1.4) can be written as

$$\begin{tikzcd} \bigoplus_{i=1}^{n} \hat{H}^{-2}(H_i; \mathbb{Z}) \arrow[r, "\psi_1"] & \hat{H}^{-2}(G; \mathbb{Z}) \\ \bigoplus_{i=1}^{n} \Big(\bigoplus_{v \in S_k} \Big(\bigoplus_{w|v} \hat{H}^{-2}(H_{i,w}; \mathbb{Z})\Big)\Big) \arrow[r, "\psi_2"] \arrow[u, "\varphi_1"] & \bigoplus_{v \in S_k} \hat{H}^{-2}(D_v; \mathbb{Z}) \arrow[u, "\varphi_2"'] \end{tikzcd} \tag{8.1.5}$$

By the local (respectively, global) Artin isomorphism, we have $\hat{H}^{-2}(H_{i,w}; \mathbb{Z}) = \hat{H}^{0}(H_{i,w}; L_w)$ and $\hat{H}^{-2}(D_v; \mathbb{Z}) = \hat{H}^{0}(D_v; L_v)$ (respectively, $\hat{H}^{-2}(H_i; \mathbb{Z}) = \hat{H}^{0}(H_i; C_L)$ and $\hat{H}^{-2}(G; \mathbb{Z}) = \hat{H}^{0}(G; C_L)$, where C_L is the idèle class group of L/k). Additionally, by [18, Proposition 7.3(b)] there are identifications $\bigoplus_{v \in S_k} (\bigoplus_{w|v} \hat{H}^{0}(H_{i,w}; L_w)) = \hat{H}^{0}(H_i; A_L)$ and $\bigoplus_{v \in S_k} \hat{H}^{0}(D_v; L_v) = \hat{H}^{0}(G; A_L)$. Since all these isomorphisms are compatible with the maps in diagram (8.1.5), this diagram induces the commutative diagram

$$\begin{tikzcd} \bigoplus_{i=1}^{n} \hat{H}^{0}(H_i; C_L) \arrow[r, "\psi_1"] & \hat{H}^{0}(G; C_L) \\ \bigoplus_{i=1}^{n} \hat{H}^{0}(H_i; A_L) \arrow[r, "\psi_2"] \arrow[u, "\varphi_1"] & \hat{H}^{0}(G; A_L) \arrow[u, "\varphi_2"'] \end{tikzcd} \tag{8.1.6}$$

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 $\hat{H}^0$, this diagram is equal to

$$\begin{tikzcd} \bigoplus_{i=1}^{n} \dfrac{A_{K_i}}{K_i^{\times} N_{L/K_i}(A_L)} \arrow[r, "\psi_1"] & \dfrac{A_k}{k^{\times} N_{L/k}(A_L)} \\ \bigoplus_{i=1}^{n} \dfrac{A_{K_i}}{N_{L/K_i}(A_L)} \arrow[r, "\psi_2"] \arrow[u, "\varphi_1"] & \dfrac{A_k}{N_{L/k}(A_L)} \arrow[u, "\varphi_2"'] \end{tikzcd} \tag{8.1.7}$$

From diagram (8.1.7), it is clear that

$$\mathrm{Ker}\, \psi_1 = \{(x_i K_i^{\times} N_{L/K_i}(A_L))_{i=1}^{n} \mid \prod_{i=1}^{n} N_{K_i/k}(x_i) \in k^{\times} N_{L/k}(A_L)\}$$

and

$$\varphi_1(\operatorname{Ker}\psi_2) = \{(x_i K_i^* \cap N_{L/K_i}(A_L^*))_{i=1}^n \mid \prod_{i=1}^n N_{K_i/k}(x_i) \in N_{L/k}(A_L^*)\}.$$

Now define

$$f : \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2) \to F(L, K, k)$$
$$(x_i K_i^* \cap N_{L/K_i}(A_L^*))_{i=1}^n \mapsto x \prod_{i=1}^n N_{K_i/k}(K_i^*)(k^* \cap N_{L/k}(A_L^*))$$

where x is any element of $k^* \cap \prod_{i=1}^n N_{K_i/k}(A_{K_i}^*)$ such that $\prod_{i=1}^n N_{K_i/k}(x_i) \in x N_{L/k}(A_L^*)$. 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.

Proof. We construct a vector $\alpha \in \bigoplus_{i=1}^{n}(\bigoplus_{\substack{v \in \Sigma_k \\ v \text{ unramified}}}(\bigoplus_{w|v} \widetilde{H}^{ab}_{i,w}))$ 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 $w_1 \in \Sigma_{K_{i_1}}$ (respectively, $w_2 \in \Sigma_{K_{i_2}}$) 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 $\widetilde{\varphi}_1(\alpha) = h$. $\square$

Theorem 8.2.5. In the notation of diagram (8.2.2), we have

$$K(K/k) = \operatorname{Ker} \widetilde{\psi}_1 / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2).$$

Proof. By Theorem 8.1.7 and Proposition 8.2.1, we have $K(K/k) = \operatorname{Ker} \overline{\psi}_1 / \overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)$, where the $\overline{}$ 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

$$\begin{aligned} f : \operatorname{Ker} \widetilde{\psi}_1 / \widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2) &\to \operatorname{Ker} \overline{\psi}_1 / \overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2) \\ (\widetilde{h}_1, \ldots, \widetilde{h}_n) &\mapsto (\overline{h}_1, \ldots, \overline{h}_n) \end{aligned}$$

where, for each $i = 1, \ldots, n$, the element $\overline{h}_i \in \overline{H}_i$ is selected as follows: take $\overline{h}_i \in \overline{H}_i$ such that $\overline{\pi}(\overline{h}_i) = \widetilde{\pi}(\widetilde{h}_i)$ (note that $\overline{h}_i$ is only defined modulo $\overline{M} = \operatorname{Ker} \overline{\pi}$). In this way, we have $\overline{\pi}(\overline{h}_1 \cdots \overline{h}_n) = \widetilde{\pi}(\widetilde{h}_1 \cdots \widetilde{h}_n)$. Additionally, by Lemma 8.2.2(i), $\overline{\pi}(\lambda(\widetilde{h}_1 \cdots \widetilde{h}_n)) = \widetilde{\pi}(\widetilde{h}_1 \cdots \widetilde{h}_n)$ and thus

$$\lambda(\widetilde{h}_1 \cdots \widetilde{h}_n) = \overline{h}_1 \cdots \overline{h}_n m \tag{8.2.3}$$

for some $m \in \overline{M}$. Changing $\overline{h}_n$ if necessary, we assume that $m = 1$ so that $\overline{h}_1 \cdots \overline{h}_n \in [\overline{G}, \overline{G}]$ and therefore $(\overline{h}_1, \ldots, \overline{h}_n) \in \operatorname{Ker} \overline{\psi}_1$.

Claim 1: f is well defined, i.e. it does not depend on the choice of the elements $\overline{h}_i$ and $f(\widetilde{\varphi}_1(\operatorname{Ker} \widetilde{\psi}_2)) \subseteq \overline{\varphi}_1(\operatorname{Ker} \overline{\psi}_2)$.

Proof: We first prove that f does not depend on the choice of $\overline{h}_i$. Suppose that, for each $i = 1, \ldots, n$, we choose elements $\underline{h}_i \in \overline{H}_i$ satisfying $\widetilde{\varphi}(\widetilde{h}_i) = \overline{\psi}(\underline{h}_i)$ and $\varphi(\widetilde{h}_1 \cdots \widetilde{h}_n) = \underline{h}_1 \cdots \underline{h}_n$. We show that $(\underline{h}_1, \ldots, \underline{h}_n) \equiv (\overline{h}_1, \ldots, \overline{h}_n)$ in $\operatorname{Ker} \overline{\alpha}_1 / \pi_1(\operatorname{Ker} \overline{\alpha}_2)$. Writing $\underline{h}_i = \overline{h}_i m_i$ for some $m_i \in \overline{M}$, it suffices to prove that $(m_1, \ldots, m_n) \in \pi_1(\operatorname{Ker} \overline{\alpha}_2)$. Since $\overline{h}_1 \cdots \overline{h}_n = \varphi(\widetilde{h}_1 \cdots \widetilde{h}_n) = \underline{h}_1 \cdots \underline{h}_n$ and the elements m_i are in $\overline{M} \subseteq Z(\overline{G})$, we obtain $m_1 \cdots m_n = 1$. As $\overline{M} \subseteq \bigcap_{i=1}^{n} \overline{H}_i$, multiplying $(m_1, \ldots, m_n)$ by $(m_2, m_2^{-1}, 1, \ldots, 1)$ (which lies in $\pi_1(\operatorname{Ker} \overline{\alpha}_2)$ by Lemma 8.2.4), we have $(m_1, \ldots, m_n) \equiv (m_1 m_2, 1, m_3, \ldots, m_n) \pmod{\pi_1(\operatorname{Ker} \overline{\alpha}_2)}$. Repeating this procedure, we obtain $(m_1, \ldots, m_n) \equiv (m_1 \cdots m_n, \ldots, 1) = (1, \ldots, 1) \pmod{\pi_1(\operatorname{Ker} \overline{\alpha}_2)}$ and therefore $(m_1, \ldots, m_n)$ is in $\pi_1(\operatorname{Ker} \overline{\alpha}_2)$, as desired.

We now show that $f(\varphi e$

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 $f(\tilde{h}_1, \dots, \tilde{h}_n) = (\overline{h}_1, \dots, \overline{h}_n)$. As $(\overline{h}_1, \dots, \overline{h}_n)$ is in $\pi_1(\mathrm{Ker}\,\overline{\psi}_2)$, this proves the claim.

Note that

$$\prod_{i=1}^{n} \prod_{t=1}^{r_{v,i}} \tilde{h}_{i,t} = \Big(\prod_{i=1}^{n} \prod_{t=1}^{r_{v,i}} \tilde{h}_{i,t}\Big)\Big(\prod_{i=n}^{1} \prod_{t=r_{v,i}}^{1} \tilde{x}_{i,t}^{-1} \tilde{h}_{i,t}^{-1} \tilde{x}_{i,t}\Big) \in \tilde{\psi}_2(\gamma).$$

Denote $\big(\prod_{i=1}^{n} \prod_{t=1}^{r_{v,i}} \tilde{h}_{i,t}\big)\big(\prod_{i=n}^{1} \prod_{t=r_{v,i}}^{1} \tilde{x}_{i,t}^{-1} \tilde{h}_{i,t}^{-1} \tilde{x}_{i,t}\big)$ by τ. Then $\tau \in [\tilde{G}, \tilde{G}]$ and using an explicit description of τ as a product of commutators and Lemma 8.2.2(ii), we deduce that $\psi(\tau) = \tau'$, where $\tau' = \big(\prod_{i=1}^{n} \prod_{t=1}^{r_{v,i}} \overline{h}_{i,t}\big)\big(\prod_{i=n}^{1} \prod_{t=r_{v,i}}^{1} \overline{x}_{i,t}^{-1} \overline{h}_{i,t}^{-1} \overline{x}_{i,t}\big)$. Therefore, we have

$$\prod_{i=1}^{n} \overline{h}_i = \prod_{i=1}^{n} \prod_{t=1}^{r_{v,i}} \overline{h}_{i,t} \equiv \tau' = \psi(\tau) \equiv \psi\Big(\prod_{i=1}^{n} \tilde{h}_i\Big) \pmod{[\overline{D_v}, \overline{D_v}]};$$

and thus $m \in [\overline{D_v}, \overline{D_v}]$, as desired.

Claim 2: f is a homomorphism.

Proof: Let $h = (\tilde{h}_1, \dots, \tilde{h}_n), h' = (\tilde{h}'_1, \dots, \tilde{h}'_n) \in \mathrm{Ker}\,\tilde{\psi}_1$ 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, $hh' = (\tilde{h}_1\tilde{h}'_1, \dots, \tilde{h}_n\tilde{h}'_n)$ and

$$\psi(\tilde{h}_1\tilde{h}'_1 \cdots \tilde{h}_n\tilde{h}'_n) \equiv \psi((\tilde{h}_1 \cdots \tilde{h}_n)(\tilde{h}'_1 \cdots \tilde{h}'_n)) = (\overline{h}_1 \cdots \overline{h}_n)(\overline{h}'_1 \cdots \overline{h}'_n) \equiv \overline{h}_1\overline{h}'_1 \cdots \overline{h}_n\overline{h}'_n \pmod{[\overline{G}, \overline{G}]}.$$

Since $\tilde{\psi}(\tilde{h}_i\tilde{h}'_i) = \overline{\psi}(\overline{h}_i\overline{h}'_i)$ for all $i = 1, \dots, n$ and $(\overline{h}_1 \cdots \overline{h}_n)(\overline{h}'_1 \cdots \overline{h}'_n) \in [\overline{G}, \overline{G}]$, 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 $\overline{h}_1 \cdots \overline{h}_n \in [\overline{G}, \overline{G}]$. Take any elements $\tilde{h}_i \in \tilde{H}_i$ satisfying $\tilde{\psi}(\tilde{h}_i) = \overline{\psi}(\overline{h}_i)$. As above, by Lemma 8.2.2(i) this implies that there exists $m \in \overline{M}$ such that

$$\psi(\tilde{h}_1 \cdots \tilde{h}_n) = \overline{h}_1 \cdots \overline{h}_n m \in [\overline{G}, \overline{G}].$$

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 $\overline{M} \cap [\overline{G},\overline{G}] = \phi(\widetilde{M} \cap [\widetilde{G},\widetilde{G}])$ by Lemma 8.2.2. Therefore $m = \phi(m')$ for some $m' \in \widetilde{M} \cap [\widetilde{G},\widetilde{G}]$ and thus $\psi(\overline{h}_1,\dots,\overline{h}_n) = f(\widetilde{h}_1,\dots,\widetilde{h}_n m'^{-1})$.

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. $\square$

Using this theorem, one can also obtain descriptions of the birational invariant $H^1(k,\operatorname{Pic}\overline{X})$ 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 $\mathbf{K}$ and let X be a smooth compactification of T. In the notation of diagram (8.2.2), we have

$$Ш(T) \cong \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2);$$

$$H^1(k,\operatorname{Pic}\overline{X})^\vee \cong \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{\mathrm{nr}});$$

$$A(T) \cong \widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2)/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{\mathrm{nr}}).$$

Proof. The first isomorphism is the statement of Theorem 8.2.5 (recall that $Ш(T)$ is isomorphic to $\mathfrak{K}(\mathbf{K},k)$). 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 $\mathbf{K}' = (K_1',\dots,K_n')$. Let T' be the multinorm one torus over k' associated with $\mathbf{K}'$ and let X' be a smooth compactification of T'. Note that $H^1(k,\operatorname{Pic}\overline{X}) = H^1(k',\operatorname{Pic}\overline{X'})$ since $\widehat{T} = \widehat{T'}$ 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 $H^1(k',\operatorname{Pic}\overline{X'})^\vee \cong Ш(T')$. The result follows since $Ш(T') \cong \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{\mathrm{nr}})$ 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 $H^1(k,\operatorname{Pic}\overline{X})^\vee \to Ш(T)$ given in this theorem corresponds to the natural surjection $\operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{\mathrm{nr}}) \to \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2)$ (this fact follows from an argument analogous to the one given in the Hasse norm principle case, see Theorem 4.3.11). $\square$

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 $\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{\mathrm{nr}})$ 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

Proposition 8.2.9. *Suppose that there exists $j \in \{1, \dots, n\}$ such that, for every prime p dividing $|\hat{H}^{-3}(G, \mathbb{Z})|$, p^2 does not divide $[K_j : k]$. Then, in the notation of diagram* (8.1.4), *we have*

$$X(T) \cong \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2);$$
$$H^1(k, \operatorname{Pic}\overline{X}) \cong \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2^{\mathrm{nr}});$$
$$A(T) \cong \varphi_1(\operatorname{Ker}\psi_2)/\varphi_1(\operatorname{Ker}\psi_2^{\mathrm{nr}}).$$

Proof. We prove only that $H^1(k, \operatorname{Pic}\overline{X}) \cong \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2^{\mathrm{nr}})$ (the other two isomorphisms can be obtained by a similar argument). Assume, without loss of generality, that $j = 1$ and $\tilde{G}$ is a Schur covering group of G so that $\widetilde{M}$ is contained in $[\tilde{G}, \tilde{G}]$ and $\widetilde{M} \cong \hat{H}^{-3}(G, \mathbb{Z})$. We show that the map

$$\begin{aligned} \lambda : \operatorname{Ker}\tilde{\psi}_1/\tilde{\varphi}_1(\operatorname{Ker}\tilde{\psi}_2^{\mathrm{nr}}) &\to \operatorname{Ker}\psi_1/\varphi_1(\operatorname{Ker}\psi_2^{\mathrm{nr}}) \\ h = (\tilde{h}_1, \dots, \tilde{h}_n) &\mapsto (\tilde{\pi}(\tilde{h}_1), \dots, \tilde{\pi}(\tilde{h}_n)) \end{aligned}$$

is an isomorphism, which proves the desired statement by Theorem 8.2.6.

We first verify that λ is well defined. It is enough to check that $\lambda(\tilde{\varphi}_1(\operatorname{Ker}\tilde{\psi}_2^{v})) \subseteq \varphi_1(\operatorname{Ker}\psi_2^{v})$ for an unramified place v of L/k. Note that if $\tilde{G} = \bigcup_{t=1}^{r_{v,i}} \widetilde{H}_i \tilde{x}_{i,t} \tilde{D}_v$ is a double coset decomposition of $\tilde{G}$, then $G = \bigcup_{t=1}^{r_{v,i}} H_i x_{i,t} D_v$ is a double coset decomposition of G, where $x_{i,t} = \tilde{\pi}(\tilde{x}_{i,t})$. From this observation, it is straightforward to verify that $\lambda(\tilde{\varphi}_1(\operatorname{Ker}\tilde{\psi}_2^{v})) \subseteq \varphi_1(\operatorname{Ker}\psi_2^{v})$.

We now prove that λ is surjective. Suppose that we are given, for $i = 1, \dots, n$, elements $h_i \in H_i$ such that $h_1 \cdots h_n \in [G, G]$. Since $\widetilde{M} \subseteq [\tilde{G}, \tilde{G}]$, any choice of elements $\tilde{h}_i \in \widetilde{H}_i$ such that $\tilde{\pi}(\tilde{h}_i) = h_i$ will satisfy $\tilde{h}_1 \cdots \tilde{h}_n \in [\tilde{G}, \tilde{G}]$ and thus $(h_1, \dots, h_n) = \lambda(\tilde{h}_1, \dots, \tilde{h}_n)$.

We finally show that λ is injective. Suppose that $(h_1, \dots, h_n) = \lambda(h) \in \varphi_1(\operatorname{Ker}\psi_2^{v})$ 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 $\tilde{h}_{i,t} \in \tilde{\pi}^{-1}(h_{i,t})$ and $\tilde{x}_{i,t} \in \tilde{\pi}^{-1}(x_{i,t})$ for all possible i, t, we obtain $\prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} \tilde{x}_{i,t}^{-1} \tilde{h}_{i,t} \tilde{x}_{i,t} = m$ for some $m \in \widetilde{M} = \operatorname{Ker}\tilde{\pi}$. As $m \in Z(\tilde{G}) \cap \bigcap_{i=1}^{n} \widetilde{H}_i$, we have $(\tilde{h}_1 m^{-1}, \tilde{h}_2, \dots, \tilde{h}_n) \in \tilde{\varphi}_1(\operatorname{Ker}\tilde{\psi}_2^{\mathrm{nr}})$.

Therefore, in order to prove that $h \in \tilde{\varphi}_1(\operatorname{Ker} \tilde{e}_2^{nr})$ it suffices to show that $(m^{-1}, 1, \ldots, 1) \in \tilde{\varphi}_1(\operatorname{Ker} \tilde{e}_2^{nr})$. We prove that $m \in \Phi(\widetilde{H}_1)$, 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 $\widetilde{M} \subseteq \Phi(\widetilde{H}_1)$.

Proof: We show that $\widetilde{M}_{(p)} \subseteq \Phi(\widetilde{H}_1)$. 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 $\widetilde{M}_{(p)} \subseteq \widetilde{G}_p \cap [\widetilde{G}, \widetilde{G}] \cap Z(\widetilde{G})$ and $\widetilde{G}_p \cap [\widetilde{G}, \widetilde{G}] \cap Z(\widetilde{G}) \subseteq [\widetilde{G}_p, \widetilde{G}_p]$ by Lemma 8.2.8, we have $\widetilde{M}_{(p)} \subseteq [\widetilde{G}_p, \widetilde{G}_p]$ and so it suffices to prove that $[\widetilde{G}_p, \widetilde{G}_p] \subseteq \Phi(\widetilde{H}_1)$. 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 $\Phi(\widetilde{H}_1) \trianglelefteq \widetilde{H}_1$, it follows that each one of the commutators above is in Φ

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 $F = \bigcap_{i=1}^{n} K_i$ 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

$$\tilde{\varphi}_1(\mathrm{Ker}\ \tilde{e}^{nr}_2) \quad f \quad (h_1 \tilde{H}_1(K$$

Proof. Since $\varphi_1(\operatorname{Ker} \tilde{e}_2^{nr}) = \prod_{\substack{v \in \Sigma_k \\ v \text{ unramified}}} \varphi_1(\operatorname{Ker} \tilde{e}_2^{v})$, it suffices to prove that

$$\varphi_1(\operatorname{Ker} \tilde{e}_2^{v}) \subseteq \{(h_1 \tilde{H}_1', \ldots, h_n \tilde{H}_n') \mid h_1 \cdots h_n \in \Phi^{\tilde{G}}(\tilde{H})\}$$

for any unramified place v of L/k. Let $\sigma \in \operatorname{Ker} \tilde{e}_2^{v}$ and fix a double coset decomposition $\tilde{G} = \bigcup_{t=1}^{r_{v,i}} \tilde{H}_i x_{i,t} \tilde{S}_v$. Write $\tilde{S}_v = \langle g \rangle$ and $\sigma = \bigoplus_{i=1}^{n} \bigoplus_{t=1}^{r_{v,i}} \tilde{h}_{i,t}$ for some $g \in \tilde{G}$, $\tilde{h}_{i,t} = x_{i,t} g^{e_{i,t}} x_{i,t}^{-1} \in \tilde{H}_i \cap x_{i,t} \langle g \rangle x_{i,t}^{-1}$ and some $e_{i,t} \in \mathbb{Z}$. By hypothesis, we have $1 = \tilde{e}_2(\sigma) = g^{\sum_{i,t} e_{i,t}}$ 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 $h_i = \prod_{t=1}^{r_{v,i}} \tilde{h}_{i,t}$ for any $1 \leq i \leq n$, we have $\varphi_1(\sigma) = (h_1 \tilde{H}_1', \ldots, h_n \tilde{H}_n') \in \operatorname{Ker} \tilde{e}_1$. We prove that

$$\prod_{i=1}^{n} h_i = \prod_{i=1}^{n} \Big(\prod_{t=1}^{r_{v,i}} \tilde{h}_{i,t}\Big) = \prod_{i=1}^{n} \Big(\prod_{t=1}^{r_{v,i}} x_{i,t} g^{e_{i,t}} x_{i,t}^{-1}\Big) \in \Phi^{\tilde{G}}(\tilde{H})$$

by induction on $s :=$ P.605.(9 11.9552 Tf 9.)]TJ/F41e/F40706 0 Td [(e)]TJ/F445-1.73.25d [(()]TJ/F.

Since $e_{i,t} f_{n,r_{v,n}} = e_{n,r_{v,n}} f_{i,t}$, we have

$$e_2(\sigma) = g^{\sum\limits_{(i,t)\neq(n,r_{v,n})} e_{i,t} f_{n,r_{v,n}} a_{i,t} - e_{n,r_{v,n}} \cdots} = g^{\sum\limits_{(i,t)\neq(n,r_{v,n})} e_{n,r_{v,n}} f_{i,t} a_{i,t} - e_{n,r_{v,n}} \cdots} = 1$$

and so $\sigma \in \operatorname{Ker} \tilde{e}_2^{v}$.

Additionally, if $\varphi_{\tilde{e}_1}(\sigma) = (\tilde{h}_1, \dots, \tilde{h}_n)$, we have

$$\begin{aligned}
\prod_{i=1}^{n} \tilde{h}_i &= \left(\prod_{(i,t)\neq(n,r_{v,n})} \xi_{i,t}\, g^{e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{i,t}^{-1} \right) \xi_{n,r_{v,n}}\, g^{-e_{n,r_{v,n}} \cdots}\, \xi_{n,r_{v,n}}^{-1} = \\
&= \left(\prod_{(i,t)\neq(n,r_{v,n})} \xi_{i,t}\, g^{e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{i,t}^{-1} \right) \xi_{n,r_{v,n}}\, g^{-e_{n,r_{v,n}} \sum\limits_{(i,t)\neq(n,r_{v,n})} f_{i,t} a_{i,t}}\, \xi_{n,r_{v,n}}^{-1} \\
&\equiv \left(\prod_{(i,t)\neq(n,r_{v,n})} \xi_{i,t}\, g^{e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{i,t}^{-1} \xi_{n,r_{v,n}}\, g^{-e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{n,r_{v,n}}^{-1} \right) \pmod{[\tilde{H}, \tilde{H}]}
\end{aligned} \tag{9.1.2}$$

since the elements $\xi_{i,t}\, g^{e_{i,t}}\, \xi_{i,t}^{-1}$ (for all possible i, t) are in $\tilde{H}$.

We claim that $\prod_{i=1}^{n} \tilde{h}_i \in \Phi(\tilde{H})$. To show this note that the elements $\xi_{i,t}\, g^{e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{i,t}^{-1}$ and $\xi_{n,r_{v,n}}\, g^{-e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{n,r_{v,n}}^{-1}$ are in $\tilde{H}$ and so $\xi_{i,t}\, g^{e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{i,t}^{-1} \in \tilde{H} \cap (\xi_{i,t} \xi_{n,r_{v,n}}^{-1}) \tilde{H} (\xi_{n,r_{v,n}} \xi_{i,t}^{-1})$. We thus see that $\xi_{i,t}\, g^{e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{i,t}^{-1} \xi_{n,r_{v,n}}\, g^{-e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{n,r_{v,n}}^{-1} = [\xi_{i,t}\, g^{e_{i,t} f_{n,r_{v,n}} a_{i,t}}\, \xi_{i,t}^{-1}, \xi_{i,t} \xi_{n,r_{v,n}}^{-1}]$ is in $\Phi(\tilde{H})$ for all i, t such that $(i,t) \neq (n, r_{v,n})$ and from (9.1.2) we deduce that $\prod_{i=1}^{n} \tilde{h}_i \in \Phi(\tilde{H})$.

Finally, we prove that h_1

It is clear that σ', being the product of two elements in $\operatorname{Ker}\widetilde{\psi}_2^v$, is also in this set. By the induction hypothesis, if $\widetilde{\varphi}_1(\sigma') = (\widetilde{h}_1, \dots, \widetilde{h}_n)$ we have $\widetilde{h}_1 \cdots \widetilde{h}_n \in \Phi(\widetilde{H})$. Since $\widetilde{h}_i \equiv h_i\widetilde{h}_i$ (mod $[\widetilde{H}, \widetilde{H}]$) for all $i = 1, \dots, n$, we conclude that $h_1 \cdots h_n \in \Phi(\widetilde{H})$. □

Lemma 9.1.2. (i) There exists a surjection $f : H^1(k, \operatorname{Pic}\overline{X}) \to H^1(k, \operatorname{Pic}\overline{Y})$. If in addition

$$\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) \subset \{(h_1\widetilde{H}_1', \dots, h_n\widetilde{H}_n') \mid h_1 \cdots h_n \in \Phi(\widetilde{H})\}$$

(in the notation of diagram (8.2.2)), then f is an isomorphism.

(ii) If F/k is Galois, f induces a surjection $X(T) \twoheadrightarrow X(S)$.

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):

$$\begin{tikzcd}
\widetilde{H}_O^{ab} \arrow[r, "\widehat{\psi}_1"] \arrow[d, "\widehat{\varphi}_1"] & \widetilde{G}_O^{ab} \arrow[d, "\widehat{\varphi}_2"] \\
\bigoplus_{v\in\Omega_k} \bigoplus_{w|v} (\widetilde{H}_w^{ab}) \arrow[r, "\widehat{\psi}_2"] & \bigoplus_{v\in\Omega_k} \widetilde{S}_v^{ab}
\end{tikzcd} \tag{9.1.3}$$

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

$$\begin{aligned}
f : \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) &\to \operatorname{Ker}\widehat{\psi}_1/\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr}) \\
(\widetilde{h}_1\widetilde{H}_1', \dots, \widetilde{h}_n\widetilde{H}_n')\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) &\mapsto (\widetilde{h}_1 \cdots \widetilde{h}_n[\widetilde{H}, \widetilde{H}])\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr})
\end{aligned}$$

Since $\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr}) = \Phi(\widetilde{H})/[\widetilde{H}, \widetilde{H}]$ (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 $H^1(k, \operatorname{Pic}\overline{X}) \cong \operatorname{Ker}\widetilde{\psi}_1/\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr})$ and $H^1(k, \operatorname{Pic}\overline{Y}) \cong \operatorname{Ker}\widehat{\psi}_1/\widehat{\varphi}_1(\operatorname{Ker}\widehat{\psi}_2^{nr})$. The statement in the first sentence follows. Finally, if we assume $\widetilde{\varphi}_1(\operatorname{Ker}\widetilde{\psi}_2^{nr}) \subset \{(h_1\widetilde{H}_1', \dots, h_n\widetilde{H}_n') \mid h_1 \cdots h_n \in \Phi(\widetilde{H})\}$, 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 $\sigma \in \operatorname{Ker}\widetilde{\psi}_2^v$ and write $\sigma = \prod_{i=1}^{n} \prod_{t=1}^{l_{v,i}} \widetilde{h}_{i,t}$ 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 $\widetilde{\varphi}_1(\ ) = (\widetilde{h}_1; : : : ; \widetilde{h}_n)$, where $\widetilde{h}_i = \prod_{t=1}^{r_v} \widetilde{h}_{i;t}$, and we wish to show that $\prod_{i=1}^{n} \widetilde{h}_i \in \widehat{\varphi}_1(\mathrm{Ker}\ \widehat{\varphi}_2)$. Since $F = k$ is Galois, $\widetilde{H}$ is a normal subgroup of $\widetilde{G}$ and thus ${}^{\widetilde{G}}(\widetilde{H}) = [\widetilde{H}; \widetilde{G}]$

Let $\sigma = (h_1 \tilde{H}_1^0, \dots, h_n \tilde{H}_n^0)$ be such that $h_1 \cdots h_n \in \tilde{\mathcal{C}}(\tilde{H})$. 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 $1 \le i \le n$, 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

$$\tilde{H}_i \subseteq \tilde{B}_{I_i} \tilde{B}_{J_i} \qquad (9.2.1)$$

Corollary 9.2.3. Let $c \in k^\times$. Assume the hypothesis of Theorem 9.2.1 and that F/k is Galois. Suppose that the k-variety $N_{F/k}(\ ) = c$ satisfies weak approximation. Then the k-variety $\prod_{i=1}^{n} N_{K_i/k}(\ _i) = c$ 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 $N_{F/k}(\ ) = c$, $c \in k^\times$. Then the Hasse principle and weak approximation hold for all multinorm equations $\prod_{i=1}^{n} N_{K_i/k}(\ _i) = c$.

9.3 Abelian extensions

In this subsection we generalize the main theorem of [76] to 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

$$X(T) = X(S) \text{ and } A(T) = A(S).$$

Proof. Note that if $A(T) = A(S)$, then by Theorem 9.2.1 and Voskresenski's exact sequence of Theorem 1.5.8 we deduce that $|X(T)| = |X(S)|$. Since $X(T)$

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 $[K_1 \cdots K_n : k] > p^2$. 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: $\tilde{H}_i \subseteq (\tilde{H}_1 \cap \tilde{H}_i).\tilde{H}_s$ for any $i = 1, \ldots, s-1$.

Proof: Observe that $K_1K_i \cap K_s = k$ as otherwise we would have $K_s \subseteq K_1K_i \subseteq K_1K_2$, contradicting the assumption on s. Therefore $K_i \supseteq k = K_1K_i \cap K_s$ and passing to subgroups this implies that $H_i \subseteq (H_1 \cap H_i).H_s$, from which the claim follows.

Claim 2: $\tilde{H}_i \subseteq (\tilde{H}_1 \cap \tilde{H}_i).\tilde{H}_2$ for any $i = s, \ldots, n$.

Proof: Observe that $K_2 \not\subseteq K_1K_i$ as otherwise we would have $K_i \subseteq K_1K_i = K_1K_2$, contradicting the assumption on K_i. Therefore $K_i \supseteq k = K_1K_i \cap K_2$ and passing to subgroups this implies that $H_i \subseteq (H_1 \cap H_i).H_2$, from which the claim follows.

Let us now prove that $H^1(k, \mathrm{Pic}\,\overline{X}) = 0$. Since $\bigcap_i K_i = k$, by Lemma 9.1.2(i) it suffices to show that

$$\varphi_{e_1}(\mathrm{Ker}\,\tilde{e}_2^{nr}) \supseteq \{(h_1\tilde{H}_1', \ldots, h_n\tilde{H}_n') \mid h_1 \cdots h_n \in \Phi(\tilde{H})\}.$$

Let $\alpha = (h_1\tilde{H}_1', \ldots, h_n\tilde{H}_n')$ be such that $h_1 \cdots h_n \in \Phi(\tilde{H})$. By Claim 1 above, for $i = 3, \ldots, s-1$ we can write $h_i = h_{1,i}h_{s,i}$, where $h_{1,i} \in \tilde{H}_1 \cap \tilde{H}_i$ and $h_{s,i} \in \tilde{H}_s \cap \tilde{H}_i$. 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 $\varphi_{e_1}(\mathrm{Ker}\,\tilde{e}_2^{nr})$ and assume it has the form $(h_1', h_2, 1, \ldots, 1, h_s', h_{s+1}, \ldots, h_n)$ for some $h_1' \in \tilde{H}_1, h_s' \in \tilde{H}_s$. Using Claim 2 and Lemma 8.2.4 in the same way, we further reduce α modulo $\varphi_{e_1}(\mathrm{Ker}\,\tilde{e}_2^{nr})$ to a vector of the form $(h_1'', h_2', 1, \ldots, 1)$ for some $h_1'' \in \tilde{H}_1, h_2' \in \tilde{H}_2$ such that $h_1''h_2' \in \Phi(\tilde{H})$. Finally, since $K_1 \cap K_2 = k$, we have $\tilde{H} = \tilde{H}_1\tilde{H}_2$ and thus $\Phi(\tilde{H}) \subseteq \Phi(\tilde{H}_1)\Phi(\tilde{H}_2)$. 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 $[K_1 \cdots K_n : k] = p^2$ (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 $\mathrm{Ker}\,\psi_1 = \varphi_1(\mathrm{Ker}\ \ (\mathrm{Ker}$

and $\tau = \bigoplus_{i=1}^{n} \bigoplus_{t=1}^{v,i} h_{i,t}$ 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 τ is the trivial vector and $\varphi_1(\tau) = (1,\dots,1)$. Otherwise, if $g \in H_{i_0} = C_p$ 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 $1 = \varphi_2(\tau) = \prod_{i=1}^{n}\prod_{t=1}^{r_{v,i}} x_{i,t}^{-1} h_{i,t} x_{i,t} = \prod_{t=1}^{r_{v,i_0}} h_{i_0,k}$. Therefore, if $\varphi_1(\tau) = (h_1,\dots,h_n)$, 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, $\varphi_1(\tau) = (1,\dots,1)$.

On the other hand, we have $\operatorname{Ker}\varphi_1 = \{(h_1,\dots,h_n) \mid h_i \in H_i, \prod_{i=1}^{n} h_i = 1\}$. This group is the kernel of the surjective group homomorphism

$$\begin{aligned} f : H_1 \times \cdots \times H_n &\to G \\ (h_1,\dots,h_n) &\mapsto h_1\cdots h_n \end{aligned}$$

and thus $\operatorname{Ker}\varphi_1 = \operatorname{Ker} f = (\mathbb{Z}/p)^{n-2}$, as desired. $\square$

Corollary 9.4.2. Let $K = (K_1,\dots,K_n)$ be a tuple of $n \geq 3$ non-isomorphic cyclic extensions n 00;11.8/F30 11.9] Tf 7.528 0 Td [(=)-278((n)]98/0 T.857p0.wo9

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 signi cant 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 xed number eld k. This result is conditional on the *weak Malle conjecture* on the distribution of number elds with prescribed Galois group (see (11.0.1) below), a conjecture that has also received signi cant 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+04sa] forteThisdTd [(p Td [(on49(this69etic)-370(kn0this69eescrib)s69e1.0.6)69ewit solvable group, then there exists a G-extension of k failing the Hasse norm principle if and only if $H^3(G; \mathbb{Z}) \neq 0$ (see [30

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

$$X^{\frac{1}{a(G)}} \ll N(k;G;X) \ll X^{\frac{1}{a(G)}+\epsilon}; \qquad (11.0.1)$$

where $a(G) = \min_{g \in G \setminus \{1\}} \{\mathrm{ind}(g)\}$ 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 H^1 (Disc

Proof. Note that an extension $K=k$ of degree n is a $(G;H)$-extension (as de ned 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 nite number of possibilities for G and H, one can compute all possibilities for $H^1(G;F_{G=H})$ using the aforementioned algorithms of Hoshi and Yamasaki. If $H^1(G;F_{G=H}) = 0$, then both the HNP for $K=k$ and weak approximation for $R^1_{K=k}\,G_m$ hold by Theorem 1.5.8 and the isomorphism (1.5.2) of Theorem 1.5.12. If $H^1(G;F_{G=H}) \neq 0$, one can compute the integer (G) of Malle's conjecture and for every such case one veri es that $(G) > 1$. 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 $G \quad S_n$ is a transitive subgroup and H is an index n subgroup of G, such that $H^1(G;F_{G=H})$ is non-trivial and $(G) = 1$. 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 rst result in this direction by investigating the frequency of the HNP for D_4-octics.

(ii) Computing the values of (G) for all transitive subgroups G of S_n with $H^1(G;F_{G=H}) \neq 0$ 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 $_{k;}\ X^{\frac{1}{6}+}$, when ordered by discriminant.

(iii) In the statement of Theorem 11.0.1 it su ces to assume Malle's conjecture only for the few transitive subgroups $G \quad S_n$ containing an index n $\quad H^1(G;F_{G=H=}$

(iv) To simplify the statement we only presented results for degree n 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 $H^1(k; \mathrm{Pic}\,\overline{X})$ for extensions $K=k$ of degree n 15 has also recently been carried out independently by Hoshi, Kanai and Yamasaki in [48] and [49]. In these works, the computation of $H^1(k; \mathrm{Pic}\,\overline{X})$ for such extensions (which here happened behind the scenes of the above proof) is made explicit and, additionally, necessary and s[illegible]

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 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 $L_5(X)$ (respectively, $L_6(X)$) 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

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 $H^3(D_4;\mathbb{Z}) = \mathbb{Z}/2$, 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-elds over Q ordered by discriminant, verifying the strong form of Malle's conjecture (see (12.1.5) below) for this family of extensions.

12.1.1 Local-global principles for norms of D_4- elds

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

Remark 12.1.4. Ordering norm one tori of D_4-octics over Q by the conductor or discriminant of the associated extension, one gets a one-to-one correspondence between (isomorphism classes of) tori and eld 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 Q satisfy weak approximation, when ordered by conductor or by discriminant of the associated eld extension.

12.1.2 Counting D_4- elds with local speci cations

In this section we recall results of Altu§ Shankar Varma Wilson [1] and describe work in progress of Shankar Varma [85] on the number of D_4- elds over Q satisfying local conditions at nitely many places. Throughout the section, L and M will always denote a D_4-quartic and a D_4-octic over Q, respectively. By an étale algebra over a eld k we mean a k-algebra which is isomorphic to a nite product of nite separable eld extensions of k.

Counting by conductor

Following [1], we de ne the conductor $f(M)$ of M as the Artin conductor of the (unique up to conjugacy) irreducible 2-dimensional Galois representation

$$_M : \mathrm{Gal}(\overline{Q}=Q) \; ! \; GL_2(C)$$

that factors through $\mathrm{Gal}(M=Q) = D_4$. Similarly, the conductor $f(L)$ of L is de ned 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 speci cations, de ned as follows:

De nition 12.1.5. ˆ For each place v of Q, a quartic local speci cation is a set $_v$ consisting of pairs $(L_v; K_v)$, where L_v is (an isomorphism class of) a quartic étale algebra over Q_v and K_v is (an isomorphism class of) a quadratic subalgebra of L_v.

ˆ A collection of quartic local speci cations $= (\;_v)_v$ is said to be acceptable if, for all but nitely many primes p, the set $_p$ contains all pairs $(L_p; K_p)$ with conductor not divisible by p^2, where the conductor of $(L_p; K_p)$ is de ned as $C(L_p; K_p$the conductor of its. p 7.9701 Tf 15.23e

Theorem 12.1.6. [1, Theorem 3] If $= (\;_v)_v$ is an acceptable collection of quartic local specifications such that $_2$ contains every pair $(L_2; K_2)$, consisting of a quartic étale algebra L_2 over Q_2 containing a quadratic subalgebra K_2, then

$$N_4(\;; |f| < X) \quad \frac{1}{2} \sum_{(L;K)\;2\;_1} \frac{1}{\# \mathrm{Aut}(L;K)} \prod_p \sum_{(L_p;K_p)\;2\;_p} \frac{1}{\# \mathrm{Aut}(L_p;K_p)} \frac{1}{C_p(L_p;K_p)} \quad 1 \quad \frac{1}{p}^{\;2} X \log X; \tag{12.1.4}$$

where for all places v, $\mathrm{Aut}(L_v; K_v)$ consists of the automorphisms of L_v which send K_v to itself and $C_p(L_p; K_p) :=$ p-part of $C(L_p; K_p)$.

In Table 1 of the Appendix we record the values of the invariants $C_p(L_p; K_p)$ and $\mathrm{Aut}(L_v; K_v)$ 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 $N_4(D_4; |f| < X)$ of D_4-quartics with conductor bounded by X:

Corollary 12.1.7. $N_4(D_4; |f| < X) \quad \frac{3}{8} \prod_p \; 1 + \frac{2}{p} + \frac{2}{p^2} \quad 1 \quad \frac{1}{p}^{\;2} \; X \log X.$

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 $|N_{k=Q}(\mathrm{Disc}_{K=k})| \quad X$ satisfies

$$N(k; G; X) \quad c(k; G) X^{\frac{1}{(G)}} (\log X)^{\;(k;G)\;\;1}; \tag{12.1.5}$$

where (G) and $(k; G)$ 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 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].

where for all places v, $\mathrm{Aut}_{D_4}(\ _v)$ denotes the centralizer of the subgroup $\ _v$ of D_4.

Using the tabulated values of $(\ M_p)$ and $\mathrm{Aut}_{D_4}(\ _p)$ in Table 1, we obtain the following asymptotic formula for the number $N_8(D_4; j\ \ j < X)$ of D_4-octics with discriminant bounded by X:

Corollary 12.1.10. $N_8(D_4; j\ \ j < X)\ \ \frac{1}{4}\ \frac{3}{4}\ \frac{1}{8}(\frac{56+3^{p}\bar{2}}{16}) \prod_p (1+\frac{3}{p}+\frac{1}{p^{\frac{3}{2}}})(1\ \ \frac{1}{p})^3 X^{\frac{1}{4}} \log^2(X^{\frac{1}{4}})$.

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 de nition:

De nition 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 nite eld extensions of $\mathbb{Q}_p$, and we de ne the splitting type $\&(M_p)$ of M_p at p as the symbol $(f_1^{e_1} f_2^{e_2} ::: f_g^{e_g})$, where e_i (respectively, f_i) is the rami cation index (respectively, residue degree) of $K_{p;i}$. Given a number eld M, we de ne the splitting type $\&_p(M)$ of M at p as the splitting type of $M\ \ \mathbb{Q}_p$.

12.2.1 Proof of the conductor result of Theorem 12.0.1

For each $n\ \ 1$, we de ne a collection of quartic local speci cations $\ ^4_n = ((\ \ ^4_n)_v)_v$ as follows. Let P_n be the set of the rst n odd primes. For a prime $p \in P_n$, we require that $(\ = ((\ \ ^4_n$

D_4-quartics whose normal closure fails the Hasse norm principle is contained in $L(\ ^{4}_{n})$ for all n. Since, up to isomorphism, each D_4-octic has two distinct quartic subfields which are D_4-quartics, we have

$$\frac{\#\{M \mid M \text{ is a } D_4\text{-octic failing the HNP and } f(M) < X\}}{\#\{M \mid M \text{ is a } D_4\text{-octic and } f(M) < X\}} = \frac{\frac{1}{2}\# L_{fail}(|f| < X)}{\frac{1}{2} N_4(D_4; |f| < X)} \quad \frac{N_4(\ ^{4}_{n}; |f| < X)}{N_4(D_4; |f| < X)}$$

for all n and so to prove Theorem 12.0.1 it suffices to show that $\lim_{n\to\infty} \lim_{X\to\infty} \frac{N_4(\ ^{4}_{n}; |f|<X)}{N_4(D_4; |f|<X)} = 0$

9 !1 4(4 n jf < X)N4

Nt(. g 1 0 0 1 461.45 53 T7(4)29 l 1N)d 0 J 0.478 w 039 m 4.234 00 Tf 0T /F43 1 461.45 53 T9(4)300Td1N T /F43 1 4

Table 1

D_p	&(M_p)	(&(L_p); &(K_p))	#(L_p; K_p)	Aut(L_p; K_p)	C_p(L_p; K_p)	(M_p)
f 1g	(11111111)	((1111),(11))	1	D_4	1	1
hr^{2}i	(2222)	((22); (11))	1	D_4	1	1
hrsi	(2222)	((22); (2))	1	V_4	1	1
hsi	(2222)	((112); (11))	1	V_4	1	1
hr i	(44)	((4); (2))	1	C_4	1	1
f sg	($1^2 1^2 1^2 1^2$)	(($1^2$11); (11))	2	V_4	p	p^4
hs; r^{2}i	**($2^2 2^2$)**	**(($1^2$2); (11))**	**2**	$\boldsymbol{V_4}$	***p***	$\boldsymbol{p^4}$
hrsi	($1^2 1^2 1^2 1^2$)	(($1^2 1^2$); (1^2))	2	V_4	p	p^4
hrs; r^{2}i	**($2^2 2^2$)**	**((2^2); (1^2))**	**2**	$\boldsymbol{V_4}$	***p***	$\boldsymbol{p^4}$
hr^{2}i	($1^2 1^2 1^2 1^2$)	(($1^2 1^2$); (11))	2	D_4	p^2	p^4
hr^2; si	($2^2 2^2$)	(($1^2 1^2$); (11))	1	V_4	p^2	p^4
hrs; r^{2}i	($2^2 2^2$)	((2^2); (2))	1	V_4	p^2	p^4
hr i	($2^2 2^2$)	((2^2); (2))	1	C_4	p^2	p^4
hr i	($1^4 1^4$)	((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

hr^{2}i	$(1^2 1^2 1^2 1^2)$	$((1^2 1^2);(11))$	4	D_4	2^6	2^{12}
hr^2; si	$(2^2 2^2)$	$((1^2 1^2);(11))$	1	V_4	2^4	2^8
hr^2; si	$(2^2 2^2)$	$((1^2 1^2);(11))$	2	V_4	2^6	2^{12}
hr^2; si	$(1^4 1^4)$	$((1^2 1^2);(11))$	4	V_4	2^6	2^{16}
hr^2; si	$(1^4 1^4)$	$((1^2 1^2);(11))$	8	V_4	2^5	2^{16}
hrs; r^{2}i						

Bibliography

[1] S. A. Altug, A. Shankar, I. Varma, K. H. Wilson, The number of quartic D_4- elds ordered by conductor. J. Eur. Math. Soc., to appear. Preprint. arXiv:1704.01729.

[2] A. M. Baily, On the density of discriminants of quartic elds. 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.

70densit22Sts N01(n)27(um)27(b)t22SFi351 Df discrimin elds.

[4] H.-J.H.-ur Arit(H.-ik)-346(v537(Die Tdgn)-346(Gruperwk)-3eiterue)-ppen.

[4]

[11] M. Bhargava, The density of discriminants of quintic rings and eldsAnn. of Math. 172(3) (2010) 1559 1591.

[12] M. Bhargava, A. Shankar, X. Wang, Geometry-of-numbers methods over global elds

[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 principleAmer. Math. Soc. Transl.(2) 143 (1989), 29 34.

[27] Y. A. Drakokhrust, V. P. Platonov, The Hasse norm principle for algebraic number elds. Math. USSR-Izv. 29 (1987), 299 322.

[28] J. S. Ellenberg, A. Venkatesh, The number of extensions of a number eld with xed degree and bounded discriminantAnn. of Math. 163(2) (2006), 723 741.

[29] B. Fein, M. Schacher,

[39] F. Gerth, The Hasse norm principle in metacyclic extensions of number elds. J. London Math. Soc, (2) 16 (1977), 203 208.

[40] F. Gerth, The Hasse norm principle for abelian extensions of number elds. 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 nite groups. Canad. J. Math. 5 (1953), 477 497.

[45] P. N. Ho man, 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 elds. 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. Kunyavski, Arithmetic properties of three-dimensional algebraic tori. Zap. Nauch. Sem. LOMI Akad. Nauk SSSR 116 (1982), 102-107.

[58] L. V. Kuz'min, Homology of pro nite groups, Schur multipliers, and class eld 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 eld. 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- elds failing the Hasse norm principle. In preparation.

[67] S. Mäki, On the density of abelian number elds. 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]

[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 elds 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 5) extensions of algebraic number elds. 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, Unrami ed extensions of quadratic number elds I. Tohoku Math. J. 22 (1970), 220 224.

[91] V. E. Voskresenski, 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. Voskresenski, Maximal tori without a ect in semisimple algebraic groups. Mat. Zametki 44 (1988) 309 318; English transl. in Math. Notes 44 (1989) 651 655.

[93]

[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 eld extensions. Compositio Math. 146 (2010), 102 128.

[99] M. M. Wood, Asymptotics for number elds 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.