THE LOCAL-GLOBAL PRINCIPLE AND A PROJECTIVE TWIST ON THE HASSE NORM THEOREM

ALAN BU

Abstract. A finite extension of global fields L/K satisfies the Hasse norm principle if any nonzero element of K has the property that it is a norm locally if and only if it is a norm globally. In 1931, Hasse proved that any cyclic extension satisfies the Hasse norm principle, providing a novel approach to extending the local-global principle to equations with degree greater than 2. In this paper, we introduce the projective Hasse norm principle, generalizing the Hasse norm principle to multiple number fields and asking whether a projective line that contains a norm locally in every number field must also contain a norm globally in every number field. We show that the projective Hasse norm principle is independent from the conjunction of Hasse norm principles in all of the constituent number fields in the general case, but that the latter implies the former when the fields are all Galois and independent. We also prove an analogue of the Hasse norm theorem for the projective Hasse norm theorem, namely that the projective Hasse norm principle holds in all cyclic extensions.

Contents

Date: April 21, 2024.

1. Introduction

Nearly a century ago, mathematician Helmut Hasse first introduced his concept of the *local-global principle*: the idea that, if a diophantine equation has a solution modulo every positive integer n, i.e. it always has a solution *locally*, then it must have an actual solution *globally* over the integers as well. Since then, the principle has been carefully studied in a variety of spaces, and to great depths. It turns out that in most cases, the principle actually fails: in [Sel51], Selmer's famous counterexample is the equation $3x^3 + 4y^3 + 5z^3 = 0$. It is not hard to show this equation has a solution modulo every integer, and yet it has no solution over the rationals. However, in other instances, the principle holds: for instance, the Hasse-Minkowski theorem proves that the principle is true for all quadratic forms over the rationals: multivariable polynomial expressions whose monomials all have degree two. Selmer's example shows that we cannot extend Hasse-Minkowski's theorem into higher degrees, but there are many approaches to extend the local-global principle into cases involving higher degrees.

One of the most prominent of these approaches is through the use of multiplicative norms. In any field extension, we can assign each element a norm acting as a kind of magnitude. For instance, in the Gaussian rationals over $\mathbb{Q}$, the norm of an element is the same as the square of its complex magnitude. In 1931, Hasse published his acclaimed Hasse norm theorem [Has31]: given a cyclic extension of the rationals $K/\mathbb{Q}$, he proved that the norm of the number field K satisfies the local-global principle: given any rational number q, if the equation $N_{K/\mathbb{Q}}(x) = q$ has a solution locally then it has a solution globally.

In our research, we put a projective twist on the problem. Instead of looking at the local-global principle at specific points, we look at lines through the origin instead. Given a space of several number fields, if a projective line always contains a local solution, when must it also contain a global solution?

To address this question, in §2 we define the p-adic numbers, the Hasse norm principle (HNP), the projective Hasse norm principle (PHNP), as well as our formalized research problem. We fix standardized notations in §3 and introduce algebraic tori and cohomology in §4.

In §5 we show a few preliminary results around simple cases of the projective Hasse norm principle and its connection to the Hasse norm principle that do not require cohomology. In §6 we derive a closed form for the character lattices of tori closely related to the projective Hasse norm principle, which we use extensively to analyze our research problem in later section.

In §7, we show that PHNP does not imply HNP by giving an explicit counterexample with a composite quadratic extension. On the other hand, it is often true that when HNP is true in all of the constituent number fields, then PHNP holds as well. To concretely show this, we derive a simple sufficient condition for HNP $\Longrightarrow$ PHNP in §8 dependent solely on the Galois group of the composite field extension. We also derive an explicit construction isomorphic to the Tate-Shafarevich group that encodes the PHNP condition in terms of the decomposition groups of the composite field extension, which allows us to completely reframe the problem of PHNP in terms of discrete group theory. Using these tools, we show that when all of the consituent number fields are Galois and independent, then HNP $\Longrightarrow$ PHNP.

Using these techniques, in §9 we construct an explicit counterexample to HNP $\Longrightarrow$ PHNP using a non-Galois constituent number field. In §10 we further study the implication HNP $\longrightarrow$ PHNP in the Galois case, and show that regardless of the choice of the constituent number fields, when the Galois group of the composite group is abelian, dihedral, or of order p^3 for some prime p, then it follows that HNP $\longrightarrow$ PHNP. We hope that the sufficient conditions for this implication and the methods used in this section will shed light on whether HNP implies PHNP in the general Galois case.

2. Background and Statement of the Problem

In this section, we list a few background concepts in number theory leading up to the Hasse norm theorem. We also define the projective norm and introduce our research problem.

Definition 2.1 (Norm)**.** Let L/K be a field extension. Then the *norm* of an element $x \in L$ is defined to be $N_{L/K}(x) = \prod_{\sigma \in \mathrm{Gal}(L^\sharp/K)} \sigma(x)$ where $L^\sharp$ is the Galois closure of L. Note that $N_{L/K}(x)$ is Galois invariant, and therefore always in K.

Example 2.2. Consider the number field $\mathbb{Q}(i)/\mathbb{Q}$. The norm of an element is given by $N_{\mathbb{Q}(i)/\mathbb{Q}}(a+bi) = (a+bi)(a-bi) = a^2+b^2$, which in this case happens to be equivalent to the square of the complex magnitude of the element, and lies in $\mathbb{Q}$.

Our research revolves around analyzing the local-global properties of these norm functions in the projective setting. Generally, for any equation to be true locally, it must have at least one solution under taking arbitrarily high prime powers as moduli. We introduce p-adics as a way to quantify this idea.

Definition 2.3 (p-adic integers)**.** Let p be a fixed prime number. A *p-adic integer* is a formal infinite series $a_0 + a_1p + a_2p^2 + a_3p^3 + \cdots$ with integers $0 \le a_i < p$ for all $i \in \mathbb{N}_0$. We denote the ring of p-adic integers as $\mathbb{Z}_p$.

In our project we also work with rational numbers: in particular, the first k terms of the p-adic expansion gives us all of the information regarding the residue of any rational number modulo p^k. Since any rational number whose reduced denominator is not a multiple of p has a p-adic expansion, p-adic integers provide a convenient way to encode this information. We can further extend the p-adic integers to include all rational numbers by allowing for a finite division by a power of p.

Definition 2.4 (p-adic numbers, [Neu99, p. 102])**.** Let p be a fixed prime number. A *p-adic number* is a formal infinite series $a_0p^k + a_1p^{k+1} + a_2p^{k+2} + a_3p^{k+3} + \cdots$ with integers $0 \leq a_i < p$ for all $i \in \mathbb{N}_0$ and integer k.The p-adic numbers form a field $\mathbb{Q}_p$ with ring of integers $\mathbb{Z}_p$.

Up to isomorphism, the only completions of $\mathbb{Q}$ are $\mathbb{R}$ and the p-adic field $\mathbb{Q}_p$ for each prime p. To rigorously define the local-global principle, we are interested in a smaller subring of the product of these completions that contains an embedding of $\mathbb{Q}$.

Definition 2.5 (Adèles)**.** We define the *ring of Adèles* $\mathbb{A}$ to be the subring of $\mathbb{R} \times \prod \mathbb{Q}_p$ consisting of elements $(r, a_2, a_3, a_5, \ldots)$ for which there exists a positive integer N such that for all $p > N$, we have $a_p \in \mathbb{Z}_p$.

Notice that having a solution to an equation over $\mathbb{A}$ is equivalent to both having a solution in rational numbers modulo every positive integer and having a real solution. Introducing the Adèle allows us to quantify the local-global principle. We can now reintroduce our research problem in full rigor.

Definition 2.6 (Hasse norm principle)**.** Let K be any number field. We define the boolean $\mathrm{HNP}(K)$ to be the truth of the following statement: for any $y \in \mathbb{Q}$, if there exists $x_1 \in K \otimes \mathbb{A}$ such that $N_{K/\mathbb{Q}}(x_1) = y \otimes 1$, then there exists $x_2 \in K$ such that $N_{K/\mathbb{Q}}(x_2) = y$.

Theorem 2.7 (Hasse norm theorem, [Neu99, Corollary 4.5. p. 384])**.** *Let K be a cyclic extension of $\mathbb{Q}$. Then* $\mathrm{HNP}(K)$ *is true.*

The Hasse norm theorem is a classic theorem in class field theory and stands as one of the strongest examples of extending the Hasse norm principle beyond degree 2 polynomials. We now introduce a more general version of this principle, extending it to projective spaces.

Definition 2.8 (Projective norm)**.** Let $K_1, K_2, \ldots, K_n$ be number fields. Let $x \in \mathbb{Q}^\times$ and $k_i \in K_i^\times$ for all $1 \leq i \leq n$. We define the *projective norm* $\mathrm{PN}(x, k_1, k_2, \ldots, k_n) = (x^{-1}N_{K_1/\mathbb{Q}}(k_1), x^{-1}N_{K_2/\mathbb{Q}}(k_2), \ldots, x^{-1}N_{K_n/\mathbb{Q}}(k_n)) \in (\mathbb{Q}^\times)^n$.

Now that the projective norm is defined, we can express the projective Hasse norm principle in terms of Adèles.

Definition 2.9 (Projective Hasse norm principle)**.** Let $K_1, K_2, \ldots, K_n$ be number fields, and let $\tilde{K} = K_1 \oplus K_2 \oplus \cdots \oplus K_n$. We define the boolean $\mathrm{PHNP}(K_1, K_2, \ldots, K_n)$ to be the truth of the following statement: for any $y \in \mathbb{Q}^n$, if there exists $x_1 \in (\mathbb{Q} \times \tilde{K}) \otimes \mathbb{A}$ such that $\mathrm{PN}(x_1) = y \otimes 1$, then there exists $x_2 \in \mathbb{Q} \times \tilde{K}$ such that $\mathrm{PN}(x_2) = y$.

Remark 2.10. Consider the canonical projection $\pi : \mathbb{Q}^n \to \mathbb{P}^{n-1}_{\mathbb{Q}}$ onto the $(n-1)$-dimensional projective space over $\mathbb{Q}$. We can restate PHNP as follows: if $x \in \mathbb{P}^{n-1}_{\mathbb{Q}}$ has nonzero coordinates and is in the image of $\pi \circ (N_{K_1/\mathbb{Q}}, \ldots, N_{K_n/\mathbb{Q}})$ over every completion, then it lies in the image of $\pi \circ (N_{K_1/\mathbb{Q}}, \cdots, N_{K_n/\mathbb{Q}})$. In other words, if a line locally contains an element in the image of the product of norms, then it also contains one globally.

Note the assumption that x has nonzero coordinates is necessary for x to lie in the image of the map $(\mathbb{Q}^\times)^n \to \mathbb{P}^{n-1}_{\mathbb{Q}}$. In practice, we always assume this holds, since if any coordinate is zero, the problem reduces to a lower dimension.

Proposition 2.11. *If $n = 1$, $\mathrm{PHNP}(K_1)$ is trivially true.*

Remark 2.12. If $n = 2$, $\mathrm{PHNP}(K_1, K_2)$ can be reformulated as the following statement: for any fixed $y \in \mathbb{Q}$, the equation $y = \frac{N_{K_1/\mathbb{Q}}(x_1)}{N_{K_2/\mathbb{Q}}(x_2)}$ has a global solution if and only if it has a local solution. In particular, if $K_1 = K_2$, the equation reduces to $y = N_{K_1/\mathbb{Q}}(\frac{x_1}{x_2})$, so it is equivalent to $\mathrm{HNP}(K_1)$. Thus, the projective Hasse norm principle is a strict generalization of the Hasse norm principle.

In this paper, we compare PHNP and HNP across many settings, mainly studying whether it is true that $\mathrm{PHNP}(K_1, K_2, \ldots, K_n)$ implies or is implied by $\bigwedge_i \mathrm{HNP}(K_i)$ in each setting of the problem. In particular, we show in Theorem 10.3 that $\bigwedge_i \mathrm{HNP}(K_i)$ implies $\mathrm{PHNP}(K_1, K_2, \ldots, K_n)$ when each of the field extensions $K_i/\mathbb{Q}$ is Galois and abelian, which in turn implies a projective analogue of the Hasse norm theorem. We also show that this result holds when $\mathrm{Gal}((K_1K_2 \cdots K_n)^\sharp)$ is dihedral or has order p^3 for some prime p. We also demonstrate in Proposition 8.9 that when $K_1, K_2, \ldots, K_n$ are each Galois extensions of $\mathbb{Q}$ and have independent Galois groups, it is also true that $\bigwedge_i \mathrm{HNP}(K_i) \implies \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$. We furthermore give counterexamples to each direction of implication in the most general case without restrictions on $K_1, K_2, \ldots, K_n$.

Remark 2.13. In this paper, all of the methodology used is purely algebraic. Thus the results of the paper also hold for any global base field in place of $\mathbb{Q}$. One reason we use $\mathbb{Q}$ in place of a general base field is to avoid introducing unnecessary complexity. Furthermore, the original Hasse norm Theorem was introduced exclusively with the rational numbers as its setting, and our use of $\mathbb{Q}$ is more in line with the historical notation.

3. Notations

Let $K_1, K_2, \ldots, K_n$ be number fields. Let $K = (K_1K_2 \cdots K_n)^\sharp$ be the Galois closure of the composite field $K_1K_2 \cdots K_n$. Let $\tilde{K}$ denote the étale algebra $K_1 \oplus K_2 \oplus \cdots \oplus K_n$, and let G denote $\mathrm{Gal}(K/\mathbb{Q})$. For simplicity, we let $H^i(M)$ denote $H^i(G, M)$ for any $\mathbb{Z}[G]$-module M. For any finite group A, we let $A^\vee = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ denote the Pontryagin dual of A and let $A^{\mathrm{ab}} = (A^\vee)^\vee$ denote the abelianization of A. We furthermore let A^{der} denote the derived or commutator subgroup of A.

For each i, we define $G^{(i)} = \mathrm{Gal}(K/K_i)$. If $K_i/\mathbb{Q}$ is a Galois extension, we define $G_i = \mathrm{Gal}(K_i/\mathbb{Q})$ so that $G_i \cong G/G^{(i)}$. If $K_1, K_2, \ldots, K_n$ are all independent and Galois, then we have $G \cong \prod_i G_i$ and $G^{(i)} \cong \prod_{j \neq i} G_j$ for all i.

Lemma 3.1. *We have that* $\bigcap_i G^{(i)} = 0$.

Proof. Suppose a nontrivial element g exists such that $g \in G^{(i)}$ for all i, then let $G' = \langle g \rangle$. Since $|G/G'| < |G|$ is an automorphism group of K fixing each of the subfields $K_1, K_2, \ldots, K_n$ and strictly smaller than $\mathrm{Gal}(K/\mathbb{Q})$, it follows that K is not the minimal Galois closure of $K_1, K_2, \ldots, K_n$, giving contradiction. $\square$

4. Methodology

Classically, the Hasse norm theorem is related to the cohomology of specific algebraic tori. We introduce the definition of algebraic tori alongside those of a few basic tori which we use extensively in our research.

Definition 4.1 (Multiplicative Group)**.** Let R be any unital ring. We define the *multiplicative group* $\mathbb{G}_m(R)$ to be the group of invertible elements in R.

Example 4.2. For $K = \mathbb{Q}(i)/\mathbb{Q}$, we have that $\mathbb{G}_m(\mathbb{Q}(i)) = \mathbb{Q}(i)^\times$. This group is a torus defined over $\mathbb{Q}(i)$. We later show in Example 4.5 that the same torus can be defined over $\mathbb{Q}$ in a way that preserves its rational points. More generally for any ring R, it is true that $\mathbb{G}_m(R) = R^\times$.

Definition 4.3 (Algebraic Torus)**.** Let K be a field with separable closure $\overline{K}$. Let $\mathbf{G}$ be an algebraic group over K. We say $\mathbf{G}$ is an *algebraic torus* if $\mathbf{G}(\overline{K}) \cong \mathbb{G}_m(\overline{K})^n$ for some $n \in \mathbb{N}$. The integer n is called the *rank* of the torus.

One important method central to reformulating the Hasse norm principle and the projective Hasse norm principle into the language of Galois cohomology is the Weil restriction of scalars. Generally, a norm is a function endowed on a number field K. However, since K can be viewed as a finite-dimensional vector space over $\mathbb{Q}$, it is reasonable that algebraic expression of K such as the norm could be reparameterized as algebraic expressions over $\mathbb{Q}$.

Definition 4.4 (Weil restriction of scalars, [PR94, p. 49])**.** Let K be a number field. Since K can be written as a vector space over $\mathbb{Q}$, it follows that $\mathbb{G}_m$ can be written as an algebraic torus $R_{K/\mathbb{Q}}\mathbb{G}_m$ over $\mathbb{Q}$ such that $R_{K/\mathbb{Q}}\mathbb{G}_m(\mathbb{Q}) = \mathbb{G}_m(K)$. This torus has rank $[K : \mathbb{Q}]$. In particular if $K/\mathbb{Q}$ is Galois then $R_{K/\mathbb{Q}}\mathbb{G}_m(K) \cong (K^\times)^{[K:\mathbb{Q}]}$. We call this algebraic torus the *Weil restriction of scalars* of the multiplicative group.

Below, we give an explicit example deriving the Weil restriction of scalars for a simple number field, continuing the extension in Example 4.2.

Example 4.5. For $K = \mathbb{Q}(i)/\mathbb{Q}$, notice that $\mathbb{G}_m(\mathbb{Q}(i))$ can be described by the solutions in z_1 to the equation $z_1z_2 = 1$. Substituting $z_1 = a+bi$ and $z_2 = c+di$ for $a, b, c, d \in \mathbb{Q}$, the set of solutions can be described as an algebraic group over $\mathbb{Q}$ obeying $ac - bd = 1$ and $ad + bc = 0$. Now plugging in $\mathbb{Q}(i)$ instead of $\mathbb{Q}$ for each variable, the space of solutions are solutions to $(a+bi)(c+di) = 1$ where a, b, c, d are in $\mathbb{Q}(i)$. We must have $(a^2+b^2)(c^2+d^2) = 1$ so $(a+bi)(a-bi)u = 1$ for $u = c^2+d^2$ determined by a, b. Letting $z_1 = a + bi$ and $z_2 = a - bi$ makes this equivalent to $z_1z_2u = 1$, which is the same as the condition $z_1, z_2 \neq 0$. Thus, this space is isomorphic to $\mathbb{Q}(i)^\times \times \mathbb{Q}(i)^\times$, so it is an algebraic torus. Notably, the Galois action on this space maps $(z_1, z_2) = (a+bi, a-bi)$ to $(\overline{a} + \overline{b}i, \overline{a} - \overline{b}i) = (\overline{a-bi}, \overline{a+bi}) = (\overline{z_2}, \overline{z_1})$. Notably, the fixed points of this action can be represented as $(z, \overline{z})$, where $z \in \mathbb{Q}(i)^\times$. In particular, the norm map on $\mathbb{Q}(i)^\times$ can be viewed as the restriction of the map $(z_1, z_2) \to z_1z_2$ to the set of fixed points.

Notice that $N_{K/\mathbb{Q}}$ gives an algebraic map from the torus $R_{K/\mathbb{Q}}\mathbb{G}_m$ to $\mathbb{G}_m$. Using the kernel of this map, we can construct another algebraic torus, whose cohomology is central to the study of the Hasse norm principle.

Definition 4.6 (Norm 1 torus)**.** Let K be a number field. The *norm 1 torus* $R^{(1)}_{K/\mathbb{Q}}\mathbb{G}_m$ is the kernel of the norm map $N_{K/\mathbb{Q}}$ from $R_{K/\mathbb{Q}}\mathbb{G}_m$ to $\mathbb{G}_m$.

Example 4.7. For $K = \mathbb{Q}(i)/\mathbb{Q}$, the norm 1 torus is the set of rational points satisfying $x^2 + y^2 = 1$. More generally, for a number field K, we have $R^{(1)}_{K/\mathbb{Q}}\mathbb{G}_m(\mathbb{Q}) = \{x \in K^\times | N_{K/\mathbb{Q}}(x) = 1\}$.

Notice that we have an exact sequence between abelian groups with $\mathrm{Gal}(K/\mathbb{Q})$-action.

$$1 \longrightarrow R^{(1)}_{K/\mathbb{Q}}\mathbb{G}_m(K) \longrightarrow R_{K/\mathbb{Q}}\mathbb{G}_m(K) \xrightarrow{N_{K/\mathbb{Q}}} \mathbb{G}_m(K) \longrightarrow 1.$$

One can use this sequence to relate $\mathrm{HNP}(K)$ to a problem on the Galois cohomology of $R^{(1)}_{K/\mathbb{Q}}\mathbb{G}_m$.

Definition 4.8 (Galois cohomology, [GS17, Definition 3.1. p. 50])**.** For all abelian groups A equipped with a left-action from G, let A^G denote the elements of A fixed by G. We can define abelian groups $H^i(G, A)$ for all $i \geq 0$ such that $H^0(G, A) = A^G$ and for any short exact sequence:

$$1 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 1.$$

We have the long exact sequence:

$$1 \longrightarrow H^0(G, A) \longrightarrow H^0(G, B) \longrightarrow H^0(G, C) \longrightarrow H^1(G, A) \longrightarrow H^1(G, B) \longrightarrow \cdots.$$

For the Hasse norm theorem, Galois cohomology is applied to obtain the following commutative diagram:

$$\begin{tikzcd}
1 \arrow[r] \arrow[d] & R^{(1)}_{K/\mathbb{Q}}\mathbb{G}_m(\mathbb{Q}) \arrow[r] \arrow[d] & K^\times \arrow[r, "N_{K/\mathbb{Q}}"] \arrow[d] & \mathbb{Q}^\times \arrow[r] \arrow[d] & H^1(K/\mathbb{Q}, R^{(1)}_{K/\mathbb{Q}}\mathbb{G}_m(K)) \arrow[d, "r"] \\
1 \arrow[r] & \prod_p R^{(1)}_{K/\mathbb{Q}}\mathbb{G}_m(\mathbb{Q}_p) \arrow[r] & \prod_{v|p} K_v^\times \arrow[r] & \prod_p \mathbb{Q}_p^\times \arrow[r] & \prod_{v|p} H^1(K_v/\mathbb{Q}_p, R^{(1)}_{K/\mathbb{Q}}\mathbb{G}_m(K_v)),
\end{tikzcd}$$

where v is taken over all primes in K dividing p. In the diagram, the Hasse norm theorem is equivalent to injectivity of the map r. We can do something analogous for the projective norm. Recall that the projective norm can be extended to a map between algebraic tori $\mathbb{G}_m \times \prod R_{K_i/\mathbb{Q}}\mathbb{G}_m \to (\mathbb{G}_m)^n$. Let torus $\mathbf{T}$ be the kernel of this map. The Galois cohomology of $\mathbf{T}(K)$ yields

$$1 \longrightarrow \mathbf{T}(\mathbb{Q}) \longrightarrow \mathbb{Q}^\times \times \bigoplus_{i=1}^n K_i^\times \xrightarrow{PN} (\mathbb{Q}^\times)^n \longrightarrow H^1(K/\mathbb{Q}, \mathbf{T}(K)).$$

In particular, $\mathbf{T}(\mathbb{Q})$ represents the set of elements $(q, k_1, k_2, \dots, k_n) \in \mathbb{Q}^\times \times \tilde{K}^\times$ such that $q = N_{K_1/\mathbb{Q}}(k_1) = N_{K_2/\mathbb{Q}}(k_2) = \cdots = N_{K_n/\mathbb{Q}}(k_n)$. Now, taking the injections $\mathbb{Q} \to \mathbb{Q}_p$ yields the commutative diagram

$$\begin{tikzcd}
1 \arrow[r] \arrow[d] & \mathbf{T}(\mathbb{Q}) \arrow[r] \arrow[d] & \mathbb{Q}^\times \times \bigoplus_{i=1}^n K_i^\times \arrow[r, "PN"] \arrow[d] & (\mathbb{Q}^\times)^n \arrow[r, "\delta"] \arrow[d, "\pi"] & H^1(K/\mathbb{Q}, \mathbf{T}(K)) \arrow[d] \\
1 \arrow[r] & \prod_p \mathbf{T}(\mathbb{Q}_p) \arrow[r] & \prod_{v|p} \mathbb{Q}_p^\times \times \bigoplus_{i=1}^n K_{i,v}^\times \arrow[r, "\gamma"] & \prod_p (\mathbb{Q}_p^\times)^n \arrow[r, "\eta"] & \prod_{v|p} H^1(K_v/\mathbb{Q}_p, \mathbf{T}(K_v))
\end{tikzcd}$$

where the maps $H^1(K/\mathbb{Q}, \mathbf{T}(K)) \to H^1(K_v/\mathbb{Q}_p, \mathbf{T}(K_v))$ are restriction maps.

Proposition 4.9. PHNP$(K_1, K_2, \dots, K_n)$ *is true if and only if* $H^1(K/\mathbb{Q}, \mathbf{T}(K)) \to \prod H^1(K_v/\mathbb{Q}_p, \mathbf{T}(K_v))$ *is injective.*

Proof. One can note that PHNP is equivalent to the statement: for all $\alpha \in (\mathbb{Q}^\times)^n$, $\alpha \in \mathrm{im}(PN) \iff \pi(\alpha) \in \mathrm{im}(\gamma)$. Using the exact sequences, this is equivalent to the statement $\delta(\alpha) = 1 \iff \alpha \in \mathrm{Ker}(\delta) \iff \pi(\alpha) \in \mathrm{Ker}(\eta) \iff \eta(\pi(\alpha)) = 1$ for all $\alpha \in (\mathbb{Q}^\times)^n$. Since the diagram is commutative, this is equivalent to the kernel of the map $H^1(K/\mathbb{Q}, \mathbf{T}(K)) \to \prod H^1(K_v/\mathbb{Q}_p, \mathbf{T}(K_v))$ being trivial, as desired. □

The map $H^1(K/\mathbb{Q}, \mathbf{T}(K)) \to \prod H^1(K_v/\mathbb{Q}_p, \mathbf{T}(K_v))$ represents a localization from a cohomology group to a product of all its p-adic completions. In general, the kernel of such a localization is known as a Tate-Shafarevich group, and represents the failure of the local-global principle over a space. A variety of tools have been developed to analyze these Tate-Shafarevich groups, some of which we use.

Definition 4.10 (Tate-Shafarevich group)**.** Let A be an abelian group with an action of $\mathrm{Gal}(K/\mathbb{Q})$. We define the *Tate-Shafarevich groups* for each $i \geq 0$ to be $Ш^i(K/\mathbb{Q}, A) = \mathrm{Ker}(H^i(K/\mathbb{Q}, A) \to \prod H^i(K_v/\mathbb{Q}_p, A))$.

Therefore, the PHNP is true if and only if the Tate-Shafarevich group $Ш^1(K/\mathbb{Q}, \mathbf{T}(K))$ is trivial. It is known that this group is finite, but it is hard to compute the cohomology of $\mathbf{T}(K)$ directly, so we make use of *Tate-Nakayama duality*.

Definition 4.11 (Character Lattice)**.** Let K be a number field, and let $\mathbf{T}$ be an Algebraic torus defined over K. We define the *character lattice* of $\mathbf{T}$ as $\mathbf{X}^*(\mathbf{T}) = \mathrm{Hom}(\mathbf{T}, \mathbb{G}_m)$. We define a group action for each $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ mapping each element α of the character lattice to the map $(\sigma \cdot \alpha)(x) = \sigma(\alpha(\sigma^{-1}(x)))$.

The character lattice provides us an easier way to compute, both mathematically and programmatically, the Tate-Shafarevich group of an algebraic tori thanks to the Tate-Nakayama Theorem. The structure of these lattices are closely linked to the Galois group of the field extension, and oftentimes can easily be expressed in a closed form in terms of this Galois group. To demonstrate, we introduce the following example of a character lattice, where the field extension is quadratic (and thus Galois).

Example 4.12. Suppose $K = \mathbb{Q}(\sqrt{d})$ is a quadratic field extension of $\mathbb{Q}$. Then the character lattice of $\mathbb{G}_m$ is isomorphic to $\mathbb{Z}$, corresponding to the maps $x \to x^n$ for integer n. The character lattice of $R_{K/\mathbb{Q}}\mathbb{G}_m$ is isomorphic to the group ring $\mathbb{Z}[\mathbb{Z}/2\mathbb{Z}]$, corresponding to the maps $x + y\sqrt{d}$ to $(x + y\sqrt{d})^m(x - y\sqrt{d})^n$ for $m, n \in \mathbb{Z}$. Notice that the Galois-invariant elements of this character lattice are exactly the powers of the norm map: $(x + y\sqrt{d})^m(x - y\sqrt{d})^m = (x^2 - dy^2)^m$. Finally, the character lattice of $R^{(1)}_{K/\mathbb{Q}}\mathbb{G}_m$ is isomorphic to $\mathbb{Z}$, corresponding to the maps $x \to x^n$. The only map here which is Galois invariant is $x \to 1$. More generally, it is well known that the character lattice of $R_{K/\mathbb{Q}}\mathbb{G}_m$ is isomorphic to the group ring $\mathbb{Z}[\mathrm{Gal}(K/\mathbb{Q})]$, where the element $\sum_{g \in \mathrm{Gal}(K/\mathbb{Q})} \lambda_g g$ corresponds to the homomorphism $x \to \prod_g g(x)^{\lambda_g}$ from [PR94, p. 54].

Theorem 4.13 (Tate-Nakayama theorem, [PR94, Theorem 6.2])**.** *Let K be a number field, let $\mathbf{T}$ be an algebraic torus defined over K, and let $\mathbf{X}^*(\mathbf{T})$ be its character lattice. Then $Ш^1(K/\mathbb{Q}, \mathbf{T}) \cong Ш^2(K/\mathbb{Q}, \mathbf{X}^*(\mathbf{T}))$.*

The Tate-Nakayama theorem allows us to evaluate the Tate-Shafarevich group of an algebraic tori, such as the ones relevant to the HNP and PHNP, by instead analyzing the finite character lattice over these respective tori. It will be invaluable to us to have a closed form for the character lattice of the tori representing the PHNP. In the following proposition, we give an example of such a closed form when $K_1, K_2, \ldots, K_n$ are each Galois number fields.

Proposition 4.14. *Suppose $K_1, K_2, \ldots, K_n$ are all Galois number fields. Let $d_i = \sum_{g \in G_i} g \in \mathbb{Z}[G_i]$ for all i. Then $\mathbf{X}^*(\mathbf{T}) \cong (\prod_i \mathbb{Z}[G_i])/\{(\lambda_1 d_1, \lambda_2 d_2, \ldots, \lambda_n d_n) : \lambda_i \in \mathbb{Z}, \sum_i \lambda_i = 0\}$.*

Proof. Notice that the space of homomorphisms from $\mathbf{T}$ to $\mathbb{G}_m$ is a quotient of the space of homomorphisms from $\prod_i \mathrm{R}_{K_i/\mathbb{Q}}\mathbb{G}_m$ to $\mathbb{G}_m$. Furthermore, $\mathrm{Hom}(\prod_i \mathrm{R}_{K_i/\mathbb{Q}}\mathbb{G}_m, \mathbb{G}_m) = \prod_i \mathrm{Hom}(\mathrm{R}_{K_i/\mathbb{Q}}\mathbb{G}_m, \mathbb{G}_m) = \prod_i \mathbb{Z}[G_i]$. Each of these homomorphisms corresponds to an element of the character lattice of $\mathbf{T}$ since we can restrict the domain of the homomorphism from $\prod_i \mathrm{R}_{K_i/\mathbb{Q}}\mathbb{G}_m$ to $\mathbf{T}$, but it is possible for multiple homomorphisms to correspond to the same element of the character lattice. Hence it suffices to determine the kernel of the restriction map. Suppose a map χ is in this kernel. Thus χ is fixed under each element of $\mathrm{Gal}(K_i/\mathbb{Q})$, so it follows that $\chi = (\lambda_1 d_1, \lambda_2 d_2, \ldots, \lambda_n d_n)$ for integers λ_i. Then χ corresponds to the homomorphism $(k_1, k_2, \ldots, k_n) \to \prod_i \prod_{g \in \mathrm{Gal}(K_i/\mathbb{Q})} g(k_i)^{\lambda_i} = \prod_i N_{K_i/\mathbb{Q}}(k_i)^{\lambda_i}$. By definition there exists $q = N_{K_1/\mathbb{Q}}(k_1) = N_{K_2/\mathbb{Q}}(k_2) = \cdots = N_{K_n/\mathbb{Q}}(k_n)$, so as long as q is not $-1, 0, 1$, this implies that $\sum \lambda_i = 0$. To show such an element exists, simply take $k_i = 2^{\frac{\mathrm{lcm}([K_1:\mathbb{Q}],[K_2:\mathbb{Q}],\ldots,[K_n:\mathbb{Q}])}{[K_i:\mathbb{Q}]}} \in \mathbb{Z} \subseteq K_i$ for every i to finish. Furthermore, any such homomorphism constructed with $\sum \lambda_i = 0$ is in the kernel since $\prod_i N_{K_i/\mathbb{Q}}(k_i)^{\lambda_i} = q^{\sum_i \lambda_i} = q^0 = 1$, so the kernel of this restriction from $\mathbf{X}^*(\prod_i \mathrm{R}_{K_i/\mathbb{Q}}\mathbb{G}_m)$ to $\mathbf{X}^*(\mathbf{T})$ is exactly the set $\{(\lambda_1 d_1, \lambda_2 d_2, \ldots, \lambda_n d_n) : \lambda_i \in \mathbb{Z}, \sum_i \lambda_i = 0\}$. The result follows. □

To create the aforementioned lattice in the SageMath environment, we use the following function:

```
def MakeLattice(G, H1, H2):
    L1 = GLattice(H1, 1)
    G = KleinFourGroup()
    H1, H2 = [G.subgroups()[1], G.subgroups()[2]]
    IL1 = GLattice(H1, 1).induced_lattice(G)
    IL2 = GLattice(H2, 1).induced_lattice(G)
    IL = IL1.direct_sum(IL2)
    a, b = IL.fixed_sublattice().basis()
    HNPLattice = IL.quotient_lattice(IL.fixed_sublattice())
    PHNPLattice = IL.quotient_lattice(IL.sublattice([a-b]))
    return [PHNPLattice, HNPLattice]
```

5. Preliminary Results

Thought closely related, neither HNP nor PHNP directly imply one another, so current results do not extend to the PHNP condition easily. Thus, we aim to draw connections between the conditions. It turns out that in some cases, we can directly construct a global solution from the local solutions of PHNP when HNP holds.

Definition 5.1. For a given n-tuple of rational numbers $q_1, q_2, \ldots, q_n \in \mathbb{Q}^n$, if there exists $x_i \in K_i \otimes \mathbb{Q}_p$ and a constant $s_p \in \mathbb{Q}_p$ such that $N_{K_i/\mathbb{Q}}(x_i) = s_p \cdot q_i$. Without loss of generality, let us assume $q_1, q_2, \ldots, q_n$ are integers. We call the n-tuple $(x_1, x_2, \ldots, x_n; s_p)$ a p-local solution with *scale factor* s_p.

Note that the PHNP is equivalent to the assertion that if there exists a p-local solution for every p, then there exists a global solution.

Proposition 5.2. *If there exists a rational number s such that s is a scale factor of some p-local solution for every p, then we have that* $\mathrm{HNP}(K_1) \wedge \mathrm{HNP}(K_2) \wedge \cdots \wedge \mathrm{HNP}(K_n) \implies \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$

Proof. Suppose such an s exists, then we have that sq_i is a norm in every $\mathbb{Q}_p$. Thus HNP implies that there exists $x_i \in \mathbb{Q}$ such that $N_{K_i/\mathbb{Q}}(x_i) = sq_i$, so taking $(sq_1, sq_2, \ldots, sq_n)$ gives a global norm for the PHNP condition. □

The proposition below further shows that we can always reduce the projective Hasse norm principle to the case where all of $K_1, K_2, \ldots, K_n$ are number fields with degree greater than 1.

Proposition 5.3. *Given number fields $K_1, K_2, \ldots K_n$, we have that:*

$$\mathrm{PHNP}(K_1, K_2, \ldots, K_n, \mathbb{Q}) = \mathrm{PHNP}(K_1, K_2, \ldots, K_n).$$

Proof. Notice that a p-local solution $(x_1, x_2, \ldots, x_n; s_p)$ for the rationals $q_1, q_2, \ldots, q_n$ taking elements from $K_1, K_2, \ldots, K_n$ can be extended to a particular p-local solution for $q_1, q_2, \ldots, q_{n+1}$ over $K_1, K_2, \ldots, K_n, \mathbb{Q}$ simply by choosing $(x_1, x_2, \ldots, x_n, q_{n+1}s_p; s_p)$, since $N_{\mathbb{Q}/\mathbb{Q}}(q_{n+1}s_p) = q_{n+1}s_p$. Furthermore, we can restrict a p-local solution over $K_1, K_2, \ldots, K_n, \mathbb{Q}$ to $K_1, K_2, \ldots, K_n$ by simply removing x_{n+1} without changing the value of s_p, so there exists a p-local solution over $K_1, K_2, \ldots, K_n$ if and only if there exists a p-local solution over $K_1, K_2, \ldots, K_n, \mathbb{Q}$. The same logic applies to taking a global solution, so it follows that there exists a global solution to PHNP over $K_1, K_2, \ldots, K_n$ if and only if there exists a global solution to $K_1, K_2, \ldots, K_n, \mathbb{Q}$. This finishes. □

Next, we introduce another reduction of PHNP to HNP when all of the number fields $K_1, K_2, \ldots, K_n$ are identical.

Proposition 5.4. *More generally, if $K_1 = K_2 = \cdots = K_n$ for $n \geq 2$, then we must have* $\mathrm{PHNP}(K_1, K_2, \ldots, K_n) = \mathrm{HNP}(K_1)$.

Proof. Suppose $\mathrm{PHNP}(K_1, K_2, \ldots, K_n)$ is true. We know from PHNP, for any $x \in \mathbb{Q}$, there exists a global solution to $\mathrm{PN}(q, k_1, k_2, \ldots, k_n) = (x, 1, 1, \ldots, 1)$ if and only if it has a local solution. Thus for k_1, k_2 ranging in K_1 the equation $x = \frac{N_{K_1/\mathbb{Q}}(k_1)}{N_{K_1/\mathbb{Q}}(k_2)} = N_{K_1/\mathbb{Q}}(\frac{k_1}{k_2})$ has local solutions if and only it has global solutions. Since $\frac{k_1}{k_2}$ ranges freely over all elements of K_1, it follows that $\mathrm{HNP}(K_1)$ is true. For the other direction, if $\mathrm{HNP}(K_1)$ is true, then I claim that an element $(a_1, a_2, \ldots, a_n) \in (\mathbb{Q}^\times)^n$ is a projective norm if and only if every $\frac{a_i}{a_1}$ is a norm in K_1. Clearly, if $\mathrm{PN}(x, k_1, k_2, \ldots, k_n) = (a_1, a_2, \ldots, a_n)$ such that $k_i \in K_1$ for all i, then each $\frac{k_i}{k_1}$ has norm $\frac{a_i}{a_1}$, proving the implication. As for the other direction, suppose we have $x_i \in K_1$ such that the $N_{K_1/\mathbb{Q}}(x_i)$ is $\frac{a_i}{a_1}$ for all i. Then we have that $\mathrm{PN}(a_1^{-1}, 1, x_2, x_3, \ldots, x_n) = (a_1, a_2, \ldots, a_n)$ is a global solution to the PHNP equation. Notice that this construction remains valid if we instead choose $(a_1, a_2, \ldots, a_n) \in (\mathbb{Q}_p^\times)^n$ from a completion $\mathbb{Q}_p$ of $\mathbb{Q}$.

Thus, in this example, over each completion of $\mathbb{Q}$ and over $\mathbb{Q}$, PHNP can be reduced to a condition on whether a tuple of numbers satisfies the HNP condition. Since HNP(K_1) implies that an element satisfies the HNP condition if and only if it satisfies the condition over all completions of $\mathbb{Q}$, it follows that an element satisfies the PHNP condition if and only if it satisfies the condition over all completions of $\mathbb{Q}$ as desired. Hence we are done. □

Proposition 5.5. *If K_1, K_2 are quadratic extensions, then* PHNP(K_1, K_2) *holds.*

Proof. For the case where $K_1 \neq K_2$, we run the following SageMath code:

```
sage: G = KleinFourGroup()
sage: H1, H2 = [G.subgroups()[1], G.subgroups()[2]]
sage: PHNP = MakeLattice(G, H1, H2)[0]
sage: PHNP.Tate_Shafarevich_lattice(2)
[]
```

This demonstrates that PHNP holds for any pair of distinct quadratic extensions. We also know from Proposition 5.4 that both PHNP and HNP hold if both quadratic extensions are the same. □

Notably in the above proposition, all quadratic extensions are Galois and have abelian Galois groups. In later sections, we generalize this result.

Remark 5.6. Although the previous proposition examines a very restricted setting, it provides us with a very interesting application. In [AAG+22], the authors establish a mass formula to count the size of isogeny classes of principally polarized abelian varieties over finite fields, weighted by the size of their respective automorphism groups. This extends to yield a similar formula for elliptic curves. The formula is very concrete, except one constant: the Tamagawa number of a specific global torus, which can be seen locally as the centralizer of the Frobenius element acting on the dual of Tate groups.

This Tamagawa number can be written $\tau(\mathbf{T}) = \frac{|H^1(\mathbb{Q}, \mathbf{X}^*(\mathbf{T}))|}{|\text{Ш}^1(\mathbf{T})|}$, and the real difficulty in its calculation is to determine the denominator.

One can apply the work done in [AAG+22] and apply it to a product of elliptic curves, and count either isogenous abelian surfaces, or modify the formula to restrict the count to other products of elliptic curves. In both cases, the same Tamagawa number computation arises. For one elliptic curve, the torus is a maximal torus of $\mathrm{GL}_2(\mathbb{Q})$ which is either split or a restriction of scalars and has a trivial Tamagawa number. For two elliptic curves, however, we get a maximal torus of $(\mathrm{GL}_2 \times \mathrm{GL}_2)^0(\mathbb{Q}) \subset \mathrm{GSp}_4(\mathbb{Q})$ where $(\mathrm{GL}_2 \times \mathrm{GL}_2)^0$ is the group of pairs of matrices $(g_1, g_2) \in \mathrm{GL}_2$ with matching determinants. The most interesting case is when the torus is compact modulo center (the *elliptic* case), and the corresponding Tate-Shafarevich group is exactly the obstruction to PHNP(K_1, K_2) where K_i is generated by eigenvalues of g_i.

6. Description of Character Lattices

Recall that we have the following exact sequence between algebraic tori by mapping each element of $\mathbf{T}$ to its shared norm under $\prod_i N_{K_i/\mathbb{Q}}$:

$$1 \longrightarrow \prod_i R^{(1)}_{K_i/\mathbb{Q}}\mathbb{G}_m \longrightarrow \mathbf{T} \longrightarrow \mathbb{G}_m \longrightarrow 1.$$

Let $\Lambda := \mathbf{X}^*(\mathbf{T})$ and $\Lambda^1 := \mathbf{X}^*(\prod_i R^{(1)}_{K_i/\mathbb{Q}}\mathbb{G}_m)$. From this, we can obtain a short exact sequence on the character lattice of each tori as in Example 5.1 by taking the dual of the previous exact sequence:

$$0 \longrightarrow \mathbb{Z} \longrightarrow \Lambda \longrightarrow \Lambda^1 \longrightarrow 0. \tag{1}$$

We proceed to generalize Proposition 4.14 to arbitrary number fields $K_1, K_2, \ldots, K_n$ without the Galois condition.

Proposition 6.1. *Let $K_1, K_2, \ldots, K_n$ be arbitrary number fields. For each i, let S_i denote the left coset space $G/G^{(i)}$ equipped with a left G-action. Let $d_i = \sum_{g\in S_i} g \in \mathbb{Z}[S_i]$ for each i. Then it follows that*

$$\mathbf{X}^*(\mathbf{T}) \cong \left(\prod_i \mathbb{Z}[S_i]\right)/\{(\lambda_1 d_1, \lambda_2 d_2, \ldots, \lambda_n d_n) : \lambda_i \in \mathbb{Z}, \sum_i \lambda_i = 0\}.$$

Proof. Recall that the space of homomorphisms from $\mathbf{T}$ to $\mathbb{G}_m$ is a quotient of the space of homomorphisms from $\prod_i R_{K_i/\mathbb{Q}}\mathbb{G}_m$ to $\mathbb{G}_m$. More generally, the homomorphism can be obtained from the space of homomorphisms from $\prod_i R_{K/\mathbb{Q}}\mathbb{G}_m$ to $\mathbb{G}_m$ by restricting to the subfield K_i. Now, proceeding analogously to the proof of Proposition 4.14, we have that $\mathrm{Hom}(\prod_i R_{K/\mathbb{Q}}\mathbb{G}_m, \mathbb{G}_m) = \prod_i \mathrm{Hom}(R_{K/\mathbb{Q}}\mathbb{G}_m, \mathbb{G}_m) = \prod_i \mathbb{Z}[G]$, where the action of $\sigma \in G$ is determined by

$$\sigma\left(\sum_{g\in G} a_g g\right) = \sum_{g\in G} a_g \sigma(g)$$

where $a_g \in \mathbb{Z}$ for each $g \in G$. The image of the restriction map from $\mathrm{Hom}(R_{K/\mathbb{Q}}\mathbb{G}_m, \mathbb{G}_m)$ to $\mathrm{Hom}(R_{K_i/\mathbb{Q}}\mathbb{G}_m, \mathbb{G}_m)$ depends solely on the action of the map on K_i, hence the kernel of the restriction map is $\mathbb{Z}[G^{(i)}]$, the set of elements which fix the subfield K_i entirely. Taking the quotient, we obtain

$$\mathrm{Hom}\left(\prod_i R_{K_i/\mathbb{Q}}\mathbb{G}_m, \mathbb{G}_m\right) \cong \prod_i \mathbb{Z}[G]/\mathbb{Z}[G^{(i)}] = \prod_i \mathbb{Z}[S_i].$$

Each of these homomorphisms corresponds to an element of the character lattice of $\mathbf{T}$ by restricting the domain of the homomorphism from $\prod_i R_{K_i/\mathbb{Q}}\mathbb{G}_m$ to $\mathbf{T}$, but multiple homomorphisms may map to the same element of $\mathbf{X}^*(\mathbf{T})$, so it suffices to determine the kernel of this restriction map. If a map χ is in this kernel, then the ith element of χ is fixed under all elements of S_i. It follows that $\chi = (\lambda_1 d_1, \lambda_2 d_2, \dots, \lambda_n d_n)$ for some integers λ_i. Furthermore, χ corresponds to the homomorphism $(k_1, k_2, \dots, k_n) \to \prod_i \prod_{g \in S_i} g(k_i)^{\lambda_i} = \prod_i N_{K_i/\mathbb{Q}}(k_i)^{\lambda_i}$ for $k_i \in K_i$.

To finish, if there exists some rational $q = N_{K_1/\mathbb{Q}}(k_1) = \cdots = N_{K_n/\mathbb{Q}}(k_i)$ such that $q \neq -1, 0, 1$, then this implies that $\sum_i \lambda_i = 0$. We can construct such a q by taking $k_i = 2^{\frac{\operatorname{lcm}([K_1:\mathbb{Q}],[K_2:\mathbb{Q}],\dots,[K_n:\mathbb{Q}])}{[K_i:\mathbb{Q}]}} \in \mathbb{Z} \subseteq K_i$ for every i to finish. Furthermore, any such homomorphism satisfying $\sum_i \lambda_i = 0$ must lie in the kernel since $\prod_i N_{K_i/\mathbb{Q}}(k_i)^{\lambda_i} = q^{\sum_i \lambda_i} = 1$, so it follows that the desired kernel is exactly the set $\{(\lambda_1 d_1, \lambda_2 d_2, \dots, \lambda_n d_n) : \lambda_i \in \mathbb{Z}, \sum_i \lambda_i = 0\}$. The result follows. $\square$

7. Counterexample to PHNP $\implies$ HNP

Though the two conditions may appear equivalent for lower degree choices of K_i, once we choose extensions of degree 4 or higher, counterexamples appear quite often. To find our counterexamples as well as calculate cohomology groups, we used SageMath to compute the results using the code shown in Appendix A.

In this section, we assert that K_1, K_2 are Galois. Using our result and notations from 4.14 and denoting the character lattice $\mathbf{X}^*(\mathbf{T})$ as Λ and the lattice $\{(\lambda_i d_i) \mid \lambda_i \in \mathbb{Z}, \sum_i \lambda_i = 0\}$ as L, we have the following short exact sequence:

$$1 \longrightarrow L \longrightarrow \prod_i \mathbb{Z}[G_i] \longrightarrow \Lambda \longrightarrow 1.$$

Using Galois cohomology, we can obtain the long exact sequence

$$1 \to H^0(G, L) \to H^0(G, \prod_i \mathbb{Z}[G_i]) \to H^0(G, \Lambda) \to H^1(G, L) \to \cdots .$$

Example 7.1. In particular, we investigate the case where $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, choosing $n = 2$, $G_1 = \mathbb{Z}/2\mathbb{Z}$, and $G_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Furthermore, define $G = G_2$ and $N = \mathrm{Gal}(K_2/K_1)$. We have that that $L \cong \mathbb{Z}$, and $\prod_i \mathbb{Z}[G_i] = \mathbb{Z}[G] \times \mathbb{Z}[N]$. We can then compute the cohomology groups in the sequence near $H^2(G, \Lambda)$ using Shapiro's lemma (see [Mil97], p.62):

$$H^i(G, \mathbb{Z}[G] \times \mathbb{Z}[N]) = H^i(G, \mathbb{Z}[G]) \times H^i(G, \mathbb{Z}[N]) = H^i(G/N, \mathbb{Z}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} & 2 \mid i \\ 1 & 2 \nmid i. \end{cases}$$

It is well known that $H^2(G, \mathbb{Z}) \cong G^{\mathrm{ab}}$ and $H^3(G, \mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$ by Lyndon's formula (see [Lyn48]), giving us the following exact sequence:

$$1 \to H^1(G, \Lambda) \to (\mathbb{Z}/2\mathbb{Z})^2 \to \mathbb{Z}/2\mathbb{Z} \to H^2(G, \Lambda) \to \mathbb{Z}/2\mathbb{Z} \to 1.$$

From this sequence, we know that we must have $H^1(G,\Lambda) \in \{\mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2\}$ and $H^2(G,\Lambda) \in \{\mathbb{Z}/2\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z})^2, \mathbb{Z}/4\mathbb{Z}\}$. By computing these cohomology groups explicitly in SageMath, we obtain that $H^1(G,\Lambda) \cong H^2(G,\Lambda) \cong \mathbb{Z}/2\mathbb{Z}$.

We can now repeat the same process to compute these cohomology groups for two nontrivial subgroups N, H where H is a complement of N in G. For N, we obtain

$$1 \longrightarrow H^1(N,\Lambda) \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 1 \longrightarrow H^2(N,\Lambda) \longrightarrow 1 \longrightarrow 1.$$

So we have that $H^1(N,\Lambda) \cong \mathbb{Z}/2\mathbb{Z}$ and $H^2(N,\Lambda) \cong 1$. Similarly, for H, we obtain

$$1 \longrightarrow H^1(H,\Lambda) \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^2 \longrightarrow H^2(H,\Lambda) \longrightarrow 1 \longrightarrow 1.$$

Computing these cohomology groups in SageMath gives $H^1(H,\Lambda) \cong 1, H^2(H,\Lambda) \cong \mathbb{Z}/2\mathbb{Z}$. Furthermore, the program tell us that $\mathrm{Ker}(H^2(G,\Lambda) \to H^2(H,\Lambda)) \cong 1$. Hence $Ш^2(G,\Lambda) \cong 1$, so $Ш^1(\mathbf{T})$ is trivial in this example if none of the decomposition groups are equal to G. (It is well known that this can only happen over ramified primes in K.)

Now, choosing $K_1 = \mathbb{Q}(\sqrt{-3}), K_2 = \mathbb{Q}(\sqrt{-3}, \sqrt{13})$ gives exactly the desired selection of Galois groups, so it follows that $\mathrm{PHNP}(K_1, K_2)$ holds in this case. However, it is shown in [Has31] that $\mathbb{Q}(\sqrt{-3}, \sqrt{13})$ does not satisfy the Hasse norm principle, hence this example demonstrates that PHNP does not imply HNP in each of the constituent fields.

Similarly, we can take $K_1 = \mathbb{Q}(\sqrt{p})$ and $K = K_2 = \mathbb{Q}(\sqrt{p}, \sqrt{q})$, where p, q are prime numbers such that $\left(\frac{p}{q}\right) = 1$ and $p, q \equiv 1 \pmod 4$, which ensures that the decomposition groups of $\mathrm{Gal}(K/\mathbb{Q})$ are always cyclic. Such a pair verifies $\mathrm{PHNP}(K_1, K_2)$ however it is well known that $Ш^1(K_2/\mathbb{Q}, \mathrm{R}^{(1)}_{K_2/\mathbb{Q}}\mathbb{G}_m)) \cong \mathbb{Z}/2\mathbb{Z}$ hence $\mathrm{HNP}(K_2)$, and by extension $\mathrm{HNP}(K_1) \wedge \mathrm{HNP}(K_2)$, does not hold.

8. A Condition for HNP $\Longrightarrow$ PHNP

In contrast to PHNP $\Longrightarrow$ HNP, counterexamples to HNP $\Longrightarrow$ PHNP are far more sparse. In this section, we find sufficient conditions for identifying cases where HNP in all of the constituent fields implies PHNP based off work in [Rüd22] and [LOYY22].

Proposition 8.1. *Suppose $\bigwedge_i \mathrm{HNP}(K_i)$ holds. Let x be any element of $Ш^2(\Lambda) \subseteq H^2(\Lambda)$, and let ι be the canonical map from $H^2(\Lambda)$ to $H^2(\Lambda^1)$ defined from equation 1. Then $x \in Ker(\phi)$.*

Proof. We begin by taking the cohomology of the exact sequence in equation 1. At H^2, we have

$$\cdots \longrightarrow H^2(\mathbb{Z}) \longrightarrow H^2(\Lambda) \longrightarrow H^2(\Lambda^1) \longrightarrow \cdots.$$

Now from Definition 4.10, it follows that for any abelian group A with an action of G,

$$0 \longrightarrow Ш^2(G,A) \longrightarrow H^2(G,A) \longrightarrow \prod_D H^2(D,A)$$

is an exact sequence, where the product is taken over all decomposition groups D. We can then combine these sequences into a commutative diagram, labelling maps a,b,c,d,e in the diagram.

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
 & Ш^2(\mathbb{Z}) \arrow[d] & Ш^2(\Lambda) \arrow[d, "\iota"] & Ш^2(\Lambda^1) \arrow[d] & \\
\cdots \arrow[r] & H^2(\mathbb{Z}) \arrow[r, "e"] \arrow[d] & H^2(\Lambda) \arrow[r, "\phi"] \arrow[d, "a"] & H^2(\Lambda^1) \arrow[r] \arrow[d, "d"] & \cdots \\
\cdots \arrow[r] & \prod H^2(D,\mathbb{Z}) \arrow[r] & \prod H^2(D,\Lambda) \arrow[r, "b"] & \prod H^2(D,\Lambda^1) \arrow[r] & \cdots
\end{tikzcd}$$

Now, since we suppose that $\bigwedge_i \mathrm{HNP}(K_i)$ holds, it follows that $Ш^2(\Lambda^1) = 0$. Hence d is injective. Since Ker a = Im ι, we have $b(a(\iota(x))) = 0$, so $d(c(\iota(x))) = 0$. Since ι, d are both injective, it follows that $\iota(x) \in$ Ker ϕ as desired. □

Notice furthermore that Im e = Ker ϕ. Therefore if HNP holds, equivalently if d is injective, we have that Im $\iota \subseteq$ Im e. Note that if e is trivial, it follows that $Ш^2(\Lambda)$ is trivial, so PHNP must hold with the assumption that $\bigwedge_i \mathrm{HNP}(K_i)$ is true. Following the notations of [LOYY22], let $H^2(\mathbb{Z})' := \{x \in H^2(\mathbb{Z}) : e(x) \in \text{Im } \iota\}$. We can now extract a set of sufficient conditions for when HNP implies PHNP using decomposition groups.

Proposition 8.2. *Suppose $\bigwedge_i \mathrm{HNP}(K_i)$ holds. Let ψ be the map from $\prod H^1(D,\Lambda^1)$ to $\prod H^2(D,\mathbb{Z})$ in the commutative diagram from Proposition 8.1. Then $|Ш^2(\Lambda)| = \frac{|H^2(\mathbb{Z})'|}{|\text{Ker } e|}$. In particular, if $|\text{Im } \psi| = |\text{Ker } e|$ then* PHNP *holds.*

Proof. First, we show that $Ш^2(\mathbb{Z}) = 0$. Suppose otherwise, then there exists a nonzero map $f \in H^2(G,\mathbb{Z}) \cong G^\vee$ in $Ш^2(\mathbb{Z})$. In particular, there exists some $g \in G$ such that $f(g) \neq 0$. Then $\langle g \rangle \subset G$ is a cyclic subgroup of G, so by the Chebotarev density theorem (see [Mil97], p.164), it follows that $\langle g \rangle$ is a decomposition group. However $f|_{\langle g \rangle} \neq 0$, giving contradiction.

Now, we can redraw the commutative diagram from Proposition 8.1, shifting the sequence one term to the left and labeling functions e, f, g, a, ξ as shown.

$$\begin{tikzcd}
 & 0 \arrow[d] & & 0 \arrow[d] & \\
 & Ш^1(\Lambda^1) \arrow[d] & 0 \arrow[d] & Ш^2(\Lambda) \arrow[d, "\iota"] & \\
\cdots \arrow[r] & H^1(\Lambda^1) \arrow[r, "\xi"] \arrow[d] & H^2(\mathbb{Z}) \arrow[r, "e"] \arrow[d, "f"] & H^2(\Lambda) \arrow[r] \arrow[d, "a"] & \cdots \\
\cdots \arrow[r] & \prod H^1(D,\Lambda^1) \arrow[r, "\psi"] & \prod H^2(D,\mathbb{Z}) \arrow[r, "g"] & \prod H^2(D,\Lambda) \arrow[r] & \cdots
\end{tikzcd}$$

In particular, since ι is injective, the image of $H^2(\mathbb{Z})'$ under e is exactly Im ι. Thus $|Ш^2(\Lambda)| = |\text{Im } \iota| = \frac{|H^2(\mathbb{Z})'|}{|\ker e|}$.

Furthermore, for any element x of $H^2(\mathbb{Z})'$, $e(x) \in$ Im ι so $a(e(x)) = 0$. Thus $f(x) \in$ Ker g so $f(x) \in$ Im ψ. Thus since f is injective, it follows that $|H^2(\mathbb{Z})'| \leq |\text{Im } \psi$ so if $|\text{Im } \psi| = |\text{Ker } e|$ then $1 = \frac{|\text{Im } \psi|}{|\text{Ker } e|} \geq \frac{|H^2(\mathbb{Z})'|}{|\text{Ker } e|} = |Ш^2(\Lambda)|$ as desired. $\square$

Corollary 8.3. *If* Ker $e = H^2(\mathbb{Z}) \cong G^\vee$, *then* $\bigwedge_i \text{HNP}(K_i) \implies \text{PHNP}(K_1, K_2, \dots, K_n)$.

Proof. It follows from Proposition 8.2 that $1 \geq \frac{|H^2(\mathbb{Z})'|}{H^2(\mathbb{Z})} = |Ш^2(\Lambda)|$, so $Ш^2(\Lambda) = 0$ as desired. $\square$

Now that we have a path to determining when PHNP holds in a given collection of number fields, we hope to understand the map e so that we can explicitly compute its kernel and $H^2(\mathbb{Z})'$. We proceed by analyzing the map ξ.

Proposition 8.4. *Let* $\Lambda_i^1 = Ind_{G^{(i)}}^G \mathbb{Z}/\langle d_i\rangle$ *for any* i. *It follows that* $H^1(G, \Lambda_i^1) \cong \{f : G \to \mathbb{Q}/\mathbb{Z} : f|_{G^{(i)}} \equiv 0\}$.

Proof. Recall from Proposition 6.1 that

$$\begin{aligned}
\Lambda^1 &= \bigoplus_{i=1}^n \text{Ind}_{G^{(i)}}^G \mathbb{Z}/\langle d_i\rangle \\
&\cong \bigoplus_{i=1}^n \mathbb{Z}[G/G^{(i)}]/\langle \sum_{g \in G/G^{(i)}} g\rangle.
\end{aligned}$$

Thus we have $H^i(G, \Lambda^1) = \bigoplus_i H^i(G, \Lambda_i^1)$.

Letting diag$_i$ denote the map from $k \in \mathbb{Z}$ to kd_i, we obtain the following short exact sequence:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\text{diag}_i} \text{Ind}_{G^{(i)}}^G \mathbb{Z} \longrightarrow \Lambda_i^1 \longrightarrow 0.$$

Computing the cohomology, we obtain:

$$\cdots \longrightarrow H^1(G, \mathrm{Ind}_{G^{(i)}}^G \mathbb{Z}) \longrightarrow H^1(G, \Lambda_i^1) \longrightarrow H^2(G, \mathbb{Z}) \longrightarrow H^2(G, \mathrm{Ind}_{G^{(i)}}^G \mathbb{Z}) \longrightarrow \cdots .$$

Note that $H^1(G, \mathrm{Ind}_{G^{(i)}}^G \mathbb{Z}) \cong H^1(G^{(i)}, \mathbb{Z}) = 0$ by Shapiro's Lemma and Hilbert 90 (see [Mil97], p.67), $H^2(G, \mathbb{Z}) = G^\vee$, and $H^2(G, \mathrm{Ind}_{G^{(i)}}^G \mathbb{Z}) \cong H^2(G^{(i)}, \mathbb{Z}) = (G^{(i)})^\vee$. Rewriting the cohomology, we have

$$0 \longrightarrow H^1(G, \Lambda_i^1) \longrightarrow G^\vee \xrightarrow{r_i} (G^{(i)})^\vee \longrightarrow \cdots .$$

It follows that $H^1(G, \Lambda_i^1) \cong \mathrm{Ker}\ r_i = \{f : G \to \mathbb{Q}/\mathbb{Z} : f|_{G^{(i)}} \equiv 0\}$ as desired. $\square$

In particular, analogously to [LOYY22], it follows the map ξ is the sum map, obtained by taking the f_i such that $H^1(\Lambda^1) = \bigoplus_i H^1(\Lambda_i^1) = (f_1, f_2, \ldots, f_n)$ and summing them to obtain $f = f_1 + f_2 + \cdots + f_n \in G^\vee = H^2(G, \mathbb{Z})$. Hence we obtain the following proposition.

Proposition 8.5. *We have*

$$\mathrm{Ker}\ e = \mathrm{Im}\ \xi = \{f \in G^\vee : \forall i, \exists f_i \in G^\vee, f_i|_{G^{(i)}} \equiv 0, f = \sum_i f_i\}$$

where $f_1, f_2, \ldots, f_n \in G^\vee$.

Remark 8.6. Both of Propositions 8.4 and 8.5 can be adapted for a different choice of Galois group $D \subseteq G$. It suffices to replace $G^{(i)}$ with $D^{(i)} = G^{(i)} \cap D$ and redefine $\Lambda_i^1 = \mathrm{Ind}_{D^{(i)}}^D$ throughout the proof. These changes yield the following proposition.

Proposition 8.7. *Let e_D denote the map $H^2(D, \mathbb{Z}) \to H^2(D, \Lambda)$ given in the commutative diagram. We have*

$$\mathrm{Ker}\ e_D = \{f \in D^\vee : \forall i, \exists f_i \in D^\vee, f_i|_{D^{(i)}} \equiv 0, f = \sum_i f_i\}$$

where $f_1, f_2, \ldots, f_n \in D^\vee$.

Using the above result, we can also deduce an explicit formulation for $H^2(\mathbb{Z})'$ analogous to that of Proposition 8.5 for Ker e.

Proposition 8.8. *The set of $H^2(\mathbb{Z})' \subseteq H^2(\mathbb{Z}) \cong G^\vee$ is exactly $\{f : G \to \mathbb{Q}/\mathbb{Z} : \forall D, f|_D \in \mathrm{Ker}\ e_D\}$ where D is chosen over all decomposition groups of G.*

Proof. Recall the following commutative diagram from the proof of Proposition 8.2.

$$\begin{tikzcd}
 & 0 \arrow[d] & & 0 \arrow[d] & \\
 & Ш^1(\Lambda^1) \arrow[d] & 0 \arrow[d] & Ш^2(\Lambda) \arrow[d, "\iota"] & \\
\cdots \arrow[r] & H^1(\Lambda^1) \arrow[r, "\xi"] \arrow[d] & H^2(\mathbb{Z}) \arrow[r, "e"] \arrow[d, "f"] & H^2(\Lambda) \arrow[r] \arrow[d, "a"] & \cdots \\
\cdots \arrow[r] & \prod H^1(D,\Lambda^1) \arrow[r, "\psi"] & \prod H^2(D,\mathbb{Z}) \arrow[r, "g"] & \prod H^2(D,\Lambda) \arrow[r] & \cdots
\end{tikzcd}$$

By definition, $H^2(\mathbb{Z})'$ is exactly the set of elements x of $H^2(\mathbb{Z})$ such that $a(e(x)) = 0$. Since this diagram is commutative, it follows that $g(f(x)) = 0$. However f is injective and given by the restriction map to each decomposition group D. Thus $H^2(\mathbb{Z})'$ is exactly the set of maps $f \in G^\vee$ such that $f|_D \in \operatorname{Ker} e_D$ for every decomposition group D, since g can be decomposed as a direct product of e_D for each decomposition group D of G. $\square$

These tools gives us an explicit way to prove that PHNP holds in a given choice of $K_1, K_2, \ldots, K_n$ by combining our formulation in Proposition 8.5 and the result in Proposition 8.2. We apply these tools to the simple case when $K_1, K_2, \ldots, K_n$ are all Galois and independent:

Proposition 8.9. *If $K_1, K_2, \ldots, K_n$ are all Galois over $\mathbb{Q}$ and $G \cong \prod_i G_i$, then $\bigwedge_i \mathrm{HNP}(K_i) \implies \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$. Equivalently, $G^\vee \cong \prod_i G_i^\vee$.*

Proof. Since $G = \prod_i G_i$, each element of G can be represented as $(g_1, g_2, \ldots, g_n)$ such that $g_i \in G_i$ for each i and $G_i = \{(g_1, g_2, \ldots, g_n) : \forall j \neq i, g_j = 0\}$. For any choice of $f \in G^\vee$, choosing f_i such that $f_i(g_1, g_2, \ldots, g_n) = f(0, \ldots, 0, g_i, 0, \ldots, 0)$ satisfies the conditions on f_i and $f = \sum_i f_i$ given in Proposition 8.5.

Thus $f \in \operatorname{Ker} e$. Hence $H^2(G, \mathbb{Z}) \subseteq \operatorname{Ker} e \subseteq H^2(G, \mathbb{Z})$, so $\operatorname{Ker} e = H^2(G, \mathbb{Z})$. Applying Proposition 8.2, it follows that PHNP holds. $\square$

9. Counterexample to HNP $\implies$ PHNP

In this section, we construct a counterexample to the claim that $\bigwedge_i \mathrm{HNP}(K_i) \implies \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$, showing that neither PHNP or HNP directly implies the other. We provide an explicit example.

Example 9.1. Let K be the extension of $\mathbb{Q}$ generated by the roots of $x^4 - x + 1$. It is known that that $\mathrm{Gal}(K/\mathbb{Q}) \cong S_4$ (from [LMF24]). Let $H_1 = \langle (12) \rangle$ and $H_2 = \langle (1234) \rangle$ be subgroups of $\mathrm{Gal}(K/\mathbb{Q})$ and let K_1, K_2 be the subfields of K fixed by these two subgroups respectively. From LMFDB, we know that the only ramified prime of K is 229, whose decomposition group is $\mathbb{Z}/2\mathbb{Z}$.

Thus all decomposition groups of $\mathrm{Gal}(K/\mathbb{Q})$ are cyclic. It can be furthermore verified that HNP is satisfied in K_1 and K_2 respectively.

Now, consider Proposition 8.2, which states that $|\text{Ш}^2(\Lambda)| = \frac{|H^2(\mathbb{Z})'|}{|\mathrm{Ker}\ e|}$. The denominator Ker e can be computed through Proposition 8.5: for any $g = aba^{-1}b^{-1} \in G^{\mathrm{der}}$, we have $f(g) = f(a)f(b)f(a^{-1})f(b^{-1}) = 0$ for $f : G \to \mathbb{Q}/\mathbb{Z}$.

Since the commutator subgroup of S_4 is A_4, it follows that the only two maps f in $H^2(\mathbb{Z})$ are $f \equiv 0$ and

$$f = \begin{cases} 0 & g \in A_4 \\ \frac{1}{2} & \text{otherwise.} \end{cases}$$

However, since $G^{(1)} = \mathrm{Gal}(K/K_1) = H_1$ and $G^{(2)} = \mathrm{Gal}(K/K_2) = H_2$, the latter map is nonzero over both H_1 and H_2, so it follows that the only choice for f_1 and f_2 is the trivial map. Thus, Ker e is trivial.

Next, we show that $H^2(\mathbb{Z})'$ contains at least two elements, which would imply that $\text{Ш}^2(\Lambda)$ is nontrivial and thus that $\mathrm{PHNP}(K_1, K_2)$ is false.

It suffices to show that f satisfies the conditions of Proposition 8.8. First, notice that no cyclic subgroup of S_4 intersects both $\langle(1234)\rangle$ and $\langle(12)\rangle$, so for each decomposition group D, it follows that we can solve $f|_D = f_1 + f_2$ by choosing $\{f_1, f_2\} = \{0, f|_D\}$ depending on whether $D^{(1)}$ or $D^{(2)}$ is trivial. Hence $f \in \mathrm{Ker}\ e_D$ for all decomposition groups D so $f \in H^2(\mathbb{Z})'$ as desired.

We now know that HNP $\Longrightarrow$ PHNP holds for independent Galois field extensions but does not hold in the non-Galois case. It remains to be shown whether it is true that HNP implies PHNP when $K_1, K_2, \ldots, K_n$ are non-independent Galois field extensions. We give a few partial results in this direction.

10. Studying HNP $\Longrightarrow$ PHNP in the Galois Case

We proceed to derive a set of sufficient conditions that allow us to prove HNP $\Longrightarrow$ PHNP using only the Galois groups of the fields $K_1, K_2, \ldots, K_n$. In this section, we exclusively consider the case where each $K_i/\mathbb{Q}$ is a Galois extension.

Proposition 10.1. *If for any $f \in G^\vee$, there exists functions $f_i \in G^\vee$ for each i such that $f_i|_{G^{(i)}} \equiv 0$ and such that $f = \sum_i f_i$, then $\bigwedge_i \mathrm{HNP}(K_i) \Longrightarrow \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$.*

Proof. First, recall from Proposition 8.5 that

$$\mathrm{Ker}\ e = \{f \in G^\vee : \forall i, \exists f_i \in G^\vee, f_i|_{G^{(i)}} \equiv 0, f = \sum_i f_i\}.$$

If it is true that Ker $e \cong H^2(\mathbb{Z})$, then Proposition 8.2 implies that $|\text{Ш}^2(\Lambda)| = \frac{|H^2(\mathbb{Z})'|}{|\mathrm{Ker}\ e|} \leq \frac{|H^2(\mathbb{Z})|}{|\mathrm{Ker}\ e|} = 1$, so PHNP holds. □

This weaker condition for PHNP allows us to study HNP $\implies$ PHNP using only the structure of the Galois group G. The following proposition gives us an algorithmic approach to verify the conditions of Proposition 10.1 in G.

Proposition 10.2. *If for any $g \in G$ and $1 \le i \le n$, we have that $gG^{(i)} \subseteq G^{der}G^{(i)} \implies g \in G^{der}$, then it follows that $\bigwedge_i \mathrm{HNP}(K_i) \implies \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$. Equivalently, if $\bigcap_i G^{der}G^{(i)} = G^{der}$, then it follows that $\bigwedge_i \mathrm{HNP}(K_i) \implies \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$.*

Proof. Note that $G^{(i)} \trianglelefteq G$ for every i from the Galois condition. We have the equality $(G/G^{(i)})^{\mathrm{der}} = G^{\mathrm{der}}G^{(i)}/G^{(i)}$ since for any $g_1, g_2, \in G$,

$$g_1G^{(i)}g_2G^{(i)}(g_1G^{(i)})^{-1}(g_2G^{(i)})^{-1} = (g_1g_2g_1^{-1}g_2^{-1})G^{(i)}.$$

Let α be the homomorphism from G^{ab} to $(G/G^{(1)})^{\mathrm{ab}} \times (G/G^{(2)})^{\mathrm{ab}} \times \cdots \times (G/G^{(n)})^{\mathrm{ab}}$ obtained by mapping each $g \in G^{\mathrm{ab}}$ to the coset of $G^{\mathrm{ab}}/G^{(i)} \cong (G/G^{(i)})^{\mathrm{ab}}$ containing it. Here, $G^{\mathrm{der}}G^{(i)}$ is exactly the kernel of the abelianization map from $G/G^{(i)}$ to $(G/G^{(i)})^{\mathrm{ab}}$. Now, α is injective if and only if there does not exist a nonzero element $g \in G^{\mathrm{ab}}$ such that

$$\alpha(g) = 0 \iff \forall i, gG^{(i)} \subseteq G^{\mathrm{der}}G^{(i)}.$$

Note that the existence of such an element is equivalent to the conditions given in the proposition, so α is injective.

Since $(G^{\mathrm{ab}})^\vee \cong ((G^\vee)^\vee)^\vee \cong G^\vee$, consider the dual map $\chi : (G/G^{(1)} \times G/G^{(2)} \times \cdots \times G/G^{(n)})^\vee \cong (G/G^{(1)})^\vee \times (G/G^{(2)})^\vee \times \cdots \times (G/G^{(n)})^\vee \to G^\vee$ of α, where the isomorphism is defined by mapping $f(x_1, x_2, \ldots, x_n) \in (G/G^{(1)} \times G/G^{(2)} \times \cdots \times G/G^{(n)})^\vee$ to $(f_1, f_2, \ldots, f_n)$ such that $f_i = f(1, 1, \ldots, x_i, \ldots, 1, 1) \in (G/G^{(i)})^\vee$ for each i. Since $(G^{\mathrm{ab}})^{\mathrm{der}} = 0$, χ is surjective if and only if α is injective.

Now, it follows for our description of the isomorphism that χ is the sum map, defined by mapping $(f_1, f_2, \ldots, f_n) \in (G/G^{(1)})^\vee \times (G/G^{(2)})^\vee \times \cdots \times (G/G^{(n)})^\vee$ to $f \in G^\vee$ such that for every $g \in G$, we define $f(g) = \sum f_i(g_i)$ where $(g_1, g_2, \ldots, g_n) = \alpha(g)$.

Thus, it follows that $\mathrm{Im}\,\chi$ is exactly Ker e, so since χ is surjective into $G^\vee \cong H^2(\mathbb{Z})$, it follows from Proposition 10.1 that $\bigwedge_i \mathrm{HNP}(K_i) \implies \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$ as desired. $\square$

We use this result to prove that HNP $\implies$ PHNP in several classes of G, including when G is abelian or dihedral.

Theorem 10.3. *If $K_i/\mathbb{Q}$ is Galois and abelian for each i, then $\bigwedge_i \mathrm{HNP}(K_i) \implies \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$.*

Proof. For any abelian group A, we have $A^{\mathrm{der}} = 0$ and $A^{\mathrm{ab}} \cong A$. Since G directly embeds into $\prod_i G/G^{(i)}$, which must be abelian, it follows that G is abelian and thus $G^{\mathrm{der}} = 0$. Therefore by Proposition 10.2, it suffices to show that there is no nontrivial $g \in G$ such that $g \in \bigcap_i G^{(i)}$. This follows from Lemma 3.1. $\square$

This result immediately gives us an analogue of the Hasse norm theorem for the projective Hasse norm principle:

Corollary 10.4. *If $K_1, K_2, \ldots, K_n$ are cyclic Galois number fields, then it follows that* $\mathrm{PHNP}(K_1, K_2, \ldots, K_n)$ *holds.*

Proposition 10.2 can also be used to tackle many nonabelian cases. To demonstrate this, we show below that this proposition is sufficient to address the case where G is dihedral.

Theorem 10.5. *If G is dihedral and $K_i/\mathbb{Q}$ is Galois for each i, then* $\bigwedge_i \mathrm{HNP}(K_i) \Longrightarrow \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$.

Proof. Let $G = D_n = \langle r, s : r^n = s^2 = (sr)^2 = 1\rangle$, then we have that $G^{\mathrm{der}} = \langle r^2\rangle$. By Proposition 10.2, it suffices to show that there does not exist $g \in \bigcap_i G^{\mathrm{der}}G^{(i)}$ such that $g \notin G^{\mathrm{der}}$.

Suppose such a g exists. If $g = r^m$ for some m then n is even and m is odd. Furthermore, it follows that $r = gr^{1-m} \in G^{(i)}$ for all m, however this gives contradiction by Lemma 3.1.

Otherwise, if $g = r^m s$ for some s. Then for each $G^{(i)}$, there exists k such that $r^k s \in G^{(i)}$ Since each $G^{(i)} \trianglelefteq G$, it follows that $r^{k+2}s = rr^k sr^{-1} \in G^{(i)}$, so $r^2 \in G^{(i)}$ for all i. This gives contradiction by Lemma 3.1 for all $n \geq 3$. Otherwise, if $n = 1, 2$ then G is abelian, so the result follows from Theorem 10.3 as desired. □

By running the Oscar code in Appendix B, we found that in the groups we investigated, the conditions of Proposition 10.2 held in all groups G whose order is quarticfree. We prove two theorems supporting this observation:

Theorem 10.6. *If G has order p^3 for some prime p, then we have* $\bigwedge_i \mathrm{HNP}(K_i) \Longrightarrow \mathrm{PHNP}(K_1, K_2, \ldots, K_n)$.

Proof. If G is abelian, then the result follows immediately from Theorem 10.3. Otherwise, it follows that G^{der} is a nontrivial normal subgroup of G. If any of $G^{(i)}$ are trivial, it follows that $K_i = \mathbb{Q}$ and can be removed using Proposition 5.2. Now for each i, we have that $G^{(i)}$ is a normal subgroup of G, so since $|G/G^{(i)}| \in \{1, p, p^2\}$ for all i, so it follows that $G/G^{(i)}$ is an abelian group. However by definition, G^{der} is the minimal subgroup G' of G such that G/G' is abelian. Thus, it follows that $G^{\mathrm{der}} \subseteq G^{(i)}$ for all i. However, since G^{der} is nontrivial, this contradicts Lemma 3.1, finishing. □

Proposition 10.7. *Suppose $G \cong \mathbb{Z}/p\mathbb{Z} \times H$ where H is a nonabelian group of order p^3. Then there exists a choice of $G^{(1)}, G^{(2)}$ such that $G^{der}G^{(1)} \cap G^{der}G^{(2)} \neq G^{der}$.*

Proof. Any p-group has a nontrivial center (by the class equation), so H must have a normal subgroup H' of order p. Since H/H' is abelian, it follows that, $H^{\mathrm{der}} = H' \cong \mathbb{Z}/p\mathbb{Z}$. Suppose G is isomorphic to $H \times \langle\alpha\rangle$ where α has order p, and let β be a generator of H^{der}. Now, choose $G^{(1)} = \langle\alpha\rangle, G^{(2)} = \langle\alpha\beta\rangle$. We have that $G^{(1)} \cap G^{(2)}$ is trivial and $G^{\mathrm{der}}G^{(1)} = G^{\mathrm{der}}G^{(2)} = \langle\alpha, \beta\rangle$. However, $G^{\mathrm{der}} = \langle\beta\rangle \ncong \langle\alpha, \beta\rangle$, as desired. □

The author hopes that determining the exact groups for which the conditions of Proposition 10.2 hold may give further insight on whether HNP implies PHNP in the general Galois case. In addition, a more general set of conditions utilizing Proposition 8.8 and Proposition 8.5 may suffice to show the implication.

11. Acknowledgements

I would like to thank my mentor, Dr. Thomas Rüd, for closely guiding this research project and providing the computational and educational resources essential to making this research possible. His invaluable support throughout the year was essential to the development of our results. Furthermore, I would also like to thank MIT PRIMES for helping to set up this research, as well as Dr. Tanya Khovanova and Dr. Felix Gotti for their suggestions and feedback.

Appendix A. SageMath Code to Test for HNP and PHNP

```
def TestAll(G, check):
    subg = G.normal_subgroups()
    subg.pop()
    for i in range(len(subg)):
        H1 = subg[i]
        if H1.order() == G.order():
            continue
        L1 = GLattice(H1, 1)
        IL1 = L1.induced_lattice(G)
        for j in range(i, len(subg)):
            H2 = subg[j]
            if H2.order() == G.order():
                continue
            L2 = GLattice(H2, 1)
            IL2 = L2.induced_lattice(G)

            if check:
                P1 = False
                P2 = False
                if len(prime_factors(IL1.rank())) <= 1:
                    P1 = True
                if len(prime_factors(IL2.rank())) <= 1:
                    P2 = True
                if P1 and P2:
                    continue

            if H1.group_id() == H2.group_id():
                continue

            IL = IL1.direct_sum(IL2)
            SL = IL.fixed_sublattice()
            a, b = SL.basis()
            SSL = SL.sublattice([a-b])

            QL1 = IL.quotient_lattice(SSL)
            QL2 = IL.quotient_lattice(SL)

            TS1 = QL1.Tate_Shafarevich_lattice(2)
            TS2 = QL2.Tate_Shafarevich_lattice(2)

            if TS1 != TS2:
                print('FOUND!!')
                print(G)
                print(H1)
                print(H2)
                print(TS1)
                print(TS2)
                print('-------------')

def HuntHNP(depth):
    for i in range(1, depth):
        print(i)
        for j in range(1, TransitiveGroups(i).cardinality()+1):
            print(TransitiveGroup(i, j))
            TestAll(TransitiveGroup(i, j), True)
```

Appendix B. Oscar Code to Test for the Galois Case

```
function test(g,h1,h2)
      d = derived_subgroup(g)[1]
      h1d = sub(g,[gens(h1);gens(d)])[1]
      h2d = sub(g,[gens(h2);gens(d)])[1]
      i = intersect([h1d,h2d])[1]
      if order(i)>order(d)
           true
      else
           false
      end
end


function testall(g)
      n = normal_subgroups(g)
      for h1 in n
           for h2 in n
                if order(intersect([h1,h2])[1]) == 1
                     if test(g,h1,h2)
                          print("FOUND")
                     end
                 end
            end
       end
 end



function looptestall(n)
     numb = number_small_groups(n)
     for i in 1:numb
          println(i)
          testall(small_group(n,i))
          println(" ")
     end
end


function testv2(g,h1,h2)
      d = derived_subgroup(g)[1]
      q1, f1 = quo(g,h1)
      q2, f2 = quo(g,h2)
      d1 = derived_subgroup(q1)[1]
      d2 = derived_subgroup(q2)[1]
      for i in g
           if !(i in d)
                if (f1(i) in d1)&(f2(i) in d2)
                     return true
                end
            end
      end
      return false
end

function testallv2(g)
```

```
    n = normal_subgroups(g)
    l = []
    for h1 in n
        for h2 in n
            if order(intersect([h1,h2])[1]) == 1
                if testv2(g,h1,h2)
                    print("FOUND ")
                    append!(l, [[g,h1,h2]])
                end
            end
        end
    end
    return l
end

function looptestallv2(n)
    numb = number_small_groups(n)
    for i in 1:numb
        println(i)
        s = testallv2(small_group(n,i))
        for r in s
            println(r)
        end
        println(" ")
    end
end
```

References

[AAG+22] Jeff Achter, Salim Ali Altug, Luis Garcia, Julia Gordon, Wen-Wei Li, and Thomas Rüd, *Counting abelian varieties over finite fields via frobenius densities*, 2022.

[GS17] Philippe Gille and Tamás Szamuely, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 165, Cambridge University Press, Cambridge, 2017, Second edition of [MR2266528]. MR 3727161

[Has31] Helmut Hasse, *Beweis eines Satzes und Wiederlegung einer Vermutung über das allgemeine Normenrestsymbol*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **85** (1931), 64–69.

[LMF24] The LMFDB Collaboration, *Number field 4.0.229.1*, 2024, [Online; accessed 13 January 2024].

[LOYY22] Pei-Xin Liang, Yasuhiro Oki, Hsin-Yi Yang, and Chia-Fu Yu, *On tamagawa numbers of cm tori*, 2022.

[Lyn48] Roger C. Lyndon, *The cohomology theory of group extensions*, Duke Math. J. **15** (1948), 271–292. MR 25468

[Mil97] James S Milne, *Class field theory*, 1997, pp. 13, 62, 164.

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR 1697859

[PR94] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press, Inc., Boston, MA, 1994, Translated from the 1991 Russian original by Rachel Rowen. MR 1278263

[Rüd22] Thomas Rüd, *Explicit Tamagawa numbers for certain algebraic tori over number fields*, Math. Comp. **91** (2022), no. 338, 2867–2904. MR 4473106

[Sel51] Ernst S. Selmer, *The Diophantine equation $ax^3 + by^3 + cz^3 = 0$*, Acta Math. **85** (1951), 203–362 (1 plate). MR 41871

Phillips Exeter Academy, Exeter, NH, 03833
Email address: abu@exeter.edu