The Hasse Norm Principle

Lectures by: Rachel Newton
Notes by: Ross Paterson

These notes were taken live during lectures at the CMI-HIMR Computational Number Theory summer school held at the University of Bristol in June 2019. In particular, any mistakes are the fault of the transcriber and not of the lecturer. Remarks in red were not written on the board, and were often added later by the transcriber.

Lecture List

Contents

Lecture 1

1 The Hasse Principle

Let k be a number field throughout, X/k a variety. Note that $X(k) \subset \prod_{v \in M_k} X(k_v)$, so that $X(k) \neq \emptyset \Rightarrow X(k_v) \neq \emptyset$. If the reverse implication holds in some family of varieties we say that "the Hasse principle holds" for that family.

Theorem 1.1 (Hasse-Minkowski)**.** *The Hasse principle holds for quadratic forms.*

Example 1 (Selmer)**.** *Let* $X : 3x^3 + 4y^3 + 5z^3 = 0 \subset \mathbb{P}^2$*. Then* $X(\mathbb{R}) \neq \emptyset$ *and* $X(\mathbb{Q}_p) \neq \emptyset$ *for all* p*, but* $X(\mathbb{Q}) = \emptyset$ *so the Hasse principle fails here.*

1.1 The Hasse Norm Principle

If L/k is a finite extension we have a commutative diagram

$$\begin{tikzcd} L^\times \arrow[r] \arrow[d, "N_{L/k}"] & \mathbb{A}_L^\times \arrow[d, "N_{L/k}"] \\ k^\times \arrow[r] & \mathbb{A}_L^\times \end{tikzcd}$$

where the norm map on the ideles is $(x_w)_w \mapsto \prod_{w|v} N_{L_w/k_v}(x_w)$.

Definition 1.2. *The Knot Group the* ***Knot group*** *is*

$$\kappa(L/k) := \frac{k^\times \cap N_{L/k}\mathbb{A}_L^\times}{N_{L/k}L^\times}$$

i.e. this is the group of local norms modulo the global ones. If $\kappa(L/k) = 1$ *then we say that the Hasse norm principle (HNP) holds.*

Example 2. *Let* N/k *be the normal closure of* L/k*, the Hasse norm principle holds for* L/k *if*

(i) $N = L$ *and* $\mathrm{Gal}(L/K)$ *is cyclic (Hasse's norm theorem)*

(ii) $[L : k]$ *is prime (Bartels)*

(iii) $[L : k] = n$ *and* $\mathrm{Gal}(N/k) = \begin{cases} D_n & \text{(Bartels)} \\ S_n & \text{(Kunyavskii \& Voskrensenski)} \\ A_n & \text{Macedo} \end{cases}$

Example 3 (Hasse)**.** $L = \mathbb{Q}(\sqrt{13}, \sqrt{-3})/\mathbb{Q}$*. Then* $3 \in N_{L/\mathbb{Q}}\mathbb{A}_L^\times \backslash N_{L/\mathbb{Q}}L^\times$ *and the HNP fails.*

Theorem 1.3 (6, Tate)**.** *Let* L/k *be Galois with* $\mathrm{Gal}(L/k) = G$ *then*

$$\kappa(L/k)^\vee := \mathrm{Hom}(\kappa(L/k), \mathbb{Q}/\mathbb{Z}) = \ker(H^3(G, \mathbb{Z}) \to \prod_v H^3(G_v, \mathbb{Z}))$$

where $G_v = \mathrm{Gal}(L_v/k_v)$

Proof. POSTPONED $\square$

Corollary 1.4 (Hasse's Norm Theorem)**.** *If* L/k *is cyclic then the HNP holds.*

Proof. G is finite cyclic means that $H^3(G, \mathbb{Z}) = H^1(G, \mathbb{Z}) = \mathrm{Hom}(G, \mathbb{Z}) = 0$. $\square$

2 Connections to Geometry: Arithmetic of Tori

Let $\overline{k}$ be a fixed algebraic closure of k.

Definition 2.1. *An **algebraic torus** T/k is an algebraic group over k such that*

$$T \times_k \overline{k} \cong_{\overline{k}} (\mathbb{G}_m, \overline{k})^n$$

for some $n \in \mathbb{Z}_{>0}$, where $\mathbb{G}_m = \operatorname{spec}(k[t, t^{-1}])$ is the general multiplicative group, an algebraic group in $\mathbb{A}^2$ with defining equation $xy = 1$.

*Note that $T \times_k \overline{k} \cong_{\overline{k}} (\mathbb{G}_{m,\overline{k}})^n$ means that $T(\overline{k}) \cong (\overline{k}^{\times})^n$. We call T **split** if $T \cong_k (\mathbb{G}_{m,k})^n$ for some $n \in \mathbb{Z}_{>0}$.*

Example 4. *$S := R_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m$ (Weil restriction) is a torus, which is an exercise on the exercise sheet. S is a variety over $\mathbb{R}$ defined by*

$$(x_0 + x_1 i)(y_0 + y_1 i) = 1$$

i.e.

$$\begin{cases} x_0 y_0 - x_1 y_1 & = 1 \\ x_0 y_1 + x_1 y_0 & = 0 \end{cases}$$

so $S(\mathbb{R}) = \mathbb{G}_m(\mathbb{C}) = \mathbb{C}^{\times}$.

Definition 2.2 (Highbrow definition of Weil Restriction)**.** *L/k a finite extension and X/L a variety. $R_{L/k}X$ is the variety over k representing the functor*

$$\begin{aligned} (k\text{-schemes})^{\mathrm{op}} &\to \text{sets} \\ S &\mapsto X(S \times_k L) \end{aligned}$$

i.e. $R_{L/k}X(S) = X(S \times_k L)$

Definition 2.3 (Lowbrow definition of Weil Restriction)**.** *X/L is definted by*

$$f(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0$$

choose a basis $\alpha_1, \ldots, \alpha_d$ for L/k and write $x_i := \sum_{j=1}^{d} y_{i,j}\alpha_j$ and then plug into the f_i to get equations for the variety $R_{L/k}X$ over k.

Example 5. *L/k finite. Then the norm one torus $R^1_{L/k}\mathbb{G}_m$ is defined by the exact sequence*

$$1 \longrightarrow R^1_{L/k}\mathbb{G}_m \longrightarrow R_{L/k}\mathbb{G}_m \xrightarrow{N_{L/k}} \mathbb{G}_m \longrightarrow 1. \tag{1}$$

Explicitly, if $\alpha_1, \ldots, \alpha_d$ is a k basis for L, then $T := R^1_{L/k}\mathbb{G}_m$ is the affine variety defined by

$$N_{L/k}\left(\sum_{i=1}^{d} x_i \alpha_i\right) = 1.$$

Definition 2.4. *A **principal homogeneous space** X for T/k is a variety X/k such that T acts simply transitively on X. If $X(k) \neq \emptyset$ then $X \cong_k T$. Thus*

$$X \times_k \overline{k} \cong_{\overline{k}} T \times_k \overline{k}$$

X represents a class in $H^1(k, T)$.

(We are about to use Galois cohomology, so it is worth mentioning that when we do we are taking the $\overline{k}$-rational points of the sheaves. Further, it is NOT true that $H^1(k,T) = 0$ by Hilbert 90 for a torus T. This is because, although $T(\overline{k}) = \overline{k}^{\times}$ as groups, the Galois action is different because the isomorphism is not necessarily over k but in fact some splitting extension L.)

Taking Galois cohomology of (1) gives

$$1 \longrightarrow T(k) \longrightarrow L^{\times} \xrightarrow{N_{L/k}} k^{\times} \longrightarrow H^1(k,T) \longrightarrow H^1(k, R_{L/k}\mathbb{G}_m)$$

but the right hand side term is 0 by Hilbert 90 (Not quite obviously, so $\mathbb{R}_{L/k}\mathbb{G}_m(\overline{k}) \cong L \otimes \overline{k} \cong \overline{k}^{[L:k]}$ with Galois action on the right hand side component only. Thus $H^1(k, R_{L/K}\mathbb{G}_m) = H^1(k, \overline{k}^{[L:k]}) = 0$ by Hilbert 90.). So

$$H^1(k,T) = \frac{k^{\times}}{N_{L/k}L^{\times}}$$

(Note that $T = R^1_{L/k}\mathbb{G}_m$ here)

Exercise 1. *Let $c \in k^{\times}$. Then if $T = R^1_{L/k}\mathbb{G}_m$, define*

$$T_c : N_{L/k}\left(\sum_{i=1}^{d} x_i \alpha_i\right) = c.$$

Show that this is a principal homogeneous space for T and its class in $H^1(k,T)$ is given by c.

Definition 2.5. *The **Tate-Shaferevich group** of a group scheme A/k is*

$$\text{Ш}(A) = \text{Ш}^1(A) := \ker\left(H^1(k,A) \to \prod_v H^1(k_v, A)\right)$$

Exercise 2. *Show that $\text{Ш}^1(R^1_{L/k}\mathbb{G}_m) = \kappa(L/k)$, so that the HNP holds for L/k if and only if the Hasse principle holds for all principal homogeneous spaces for $R^1\mathbb{G}_m$.*

Definition 2.6. *Let T/k be a torus, then we define the **Galois module of characters** to be*

$$\widehat{T} := \mathrm{Hom}(T_{\overline{k}}, \mathbb{G}_{m,\overline{k}})$$

*which is a Galois module via the natural action of $\mathrm{Gal}(\overline{k}, k)$. We also have the **Galois module of cocharacters***

$$\widehat{T}^0 := \mathrm{Hom}(\mathbb{G}_{m,\overline{k}}, T_{\overline{k}}).$$

(Note these are homomorphisms of algebraic groups, so must be algebraic homs). These are both $\mathbb{Z}$-free modules of finite rank with continuous Galois action.

Example 6. *It is an exercise to show that:*

(a) $\widehat{\mathbb{G}_{m,k}} = \mathbb{Z}$,

(b) If $F/L/k$ is a tower of number fields with F/k Galois and $\mathrm{Gal}(F/k) = G \geq H = \mathrm{Gal}(F/L)$ then

$$\widehat{R_{L/k}\mathbb{G}_m} = \mathbb{Z}[G/H]$$

Now taking characters in the sequence defining $R^1_{L/k}\mathbb{G}_m$, namely (1), gives

$$0 \longrightarrow \mathbb{Z} \xrightarrow{N_{L/k}} \mathbb{Z}[G/H] \longrightarrow \widehat{R^1_{L/k}\mathbb{G}_m} \longrightarrow 0$$

where the $N_{L/k}$ is given by $1 \mapsto \sum_{g \in G/H} g$

We have one more exercise, in response to the question about why $R^1_{L/k}\mathbb{G}_m$ is even a torus:

Exercise 3. *(a) Show that if T/L is a torus then $R_{L/k}T$ is a torus.*

(b) Show that $R^1_{L/k}\mathbb{G}_m$ is a torus.

Lecture 2

Aside: Let $L = \frac{k[X]}{f(X)}$ be a separable field extension. Note that

$$L \otimes_k k_v = \frac{k_v[X]}{f_1(X) \dots f_r(X)} = \prod_{i=1}^{r} \frac{k_v[X]}{f_i(X)} = \prod_{w|v} L_w$$

and we have an injection $L \to L_w$, which has a dense subset. Applying the norm map on $L \otimes_k k_v$ we get a commutative diagram

$$\begin{tikzcd} L \otimes_k k_v \arrow[r, "N_{L/k}"] \arrow[d, equal] & k \otimes_k k_v \arrow[d, equal] \\ \prod_{w|v} L_w \arrow[r, "\prod N_{L_w/K_v}"] & k_v \end{tikzcd}$$

Now, from last time take $c \in k^\times$ and recall the associated norm torus $T_c : N_{L/k}(\sum_i x_i \alpha_i) = c$ for α_i forming a k basis of L. Then

$$\begin{aligned} [T_c] = 0 \in H^1(k, T) &\iff T_c(k) \neq \emptyset \\ &\iff c \in N_{L/k}L^\times \\ [T_c] = 0 \in H^1(k_v, T) &\iff T_c(k_v) \neq \emptyset \\ &\iff c \in N_{L/k}(L \otimes_k k_v) \\ &\iff c \in \prod_{w|v} N_{L_w/k_v} L_w^\times \end{aligned}$$

The New Lecture: Continuing the lecture proper, recall from last the the modules of characters and cocharacters:

$$\widehat{T} = \mathrm{Hom}(T_{\overline{k}}, \mathbb{G}_{m,\overline{k}})$$
$$\widehat{T}^\circ = \mathrm{Hom}(\mathbb{G}_{m,\overline{k}}, T_{\overline{k}})$$

where Hom is the homomorphisms that are regular maps of varieties that are also group homomorphisms. Note that $\mathrm{Gal}(\overline{k}/k)$ acts on $\widehat{T}$ and $\widehat{T}^\circ$ by

$$(g \cdot \varphi)(x) = g\varphi(g^{-1}x)$$

Exercise 4 (17)**.** *Show that there is a* ***perfect pairing*** *of Galois modules*

$$\widehat{T} \otimes \widehat{T}^{\circ} \xrightarrow{\theta} \mathbb{Z}.$$

and hence $\widehat{T}^{\circ} = \mathrm{Hom}(\widehat{T}, \mathbb{Z})$ *as Galois modules.*

Lemma 2.7 (18)**.** *Let T/k be split by a finite Galois extension L/k (i.e. under base change to L it becomes $\mathbb{G}_m^n$ for some n), denote $G := \mathrm{Gal}(L/k)$. Then*

$$\widehat{T}^{\circ} \otimes L^{\times} \cong T(L)$$

as G-modules.

Proof. L/k splits T means that $T_L = \mathbb{G}_{m,L}^n$ for some $n \in \mathbb{Z}_{>0}$. This in turn tells us that $\mathrm{Gal}(\overline{k}/L)$ acts trivially on $\widehat{T}$ and on $\widehat{T}^{\circ}$, so all cocharacters are defined over L. Then

$$\widehat{T}^{\circ} \otimes L^{\times} \to^{f} T(L)$$
$$\varphi \otimes \alpha \mapsto \varphi(\alpha)$$

is a G-homomorphism. $\widehat{T}^{\circ} \cong \mathbb{Z}^n$ as a group and $T(L) \cong (L^{\times})^n$ as a group. Therefore f is an isomorphism. □

Definition 2.8 (19)**.** *Let T/k be a torus, split by L/k finite Galois with $G = \mathrm{Gal}(L/k)$. Define more Sha's by*

$$Ш^2(G, \widehat{T}) := \ker\left(H^2(G, \widehat{T}) \to \prod_v H^2(G_v, \widehat{T})\right)$$

$$Ш^2_w(G, \widehat{T}) := \ker\left(H^2(G, \widehat{T}) \to \prod_{g \in G} H^2(\langle g \rangle, \widehat{T})\right)$$

Theorem 2.9 (20)**.** *Let T be as in definition 2.8. Then there is a canonical isomorphism*

$$Ш^1(T) \cong \mathrm{Hom}(Ш^2(G, \widehat{T}), \mathbb{Q}/\mathbb{Z})$$

Recall Theorem 1.3, which tells us a similar thing. In fact, Theorem 1.3 follows from Theorem 2.9 once you have shown that for $T = R^1_{L/k}\mathbb{G}_m$ and L/k Galois,

$$Ш^2(G, \widehat{T}) = \ker\left(H^3(G, \mathbb{Z}) \to \prod_v H^3(G, \mathbb{Z})\right).$$

This is an exercise.

3 Tate Cohomology of Finite Groups

G a finite group, A a G-module. The Tate Cohomology groups are

$$\widehat{H}^n(G, A) = \begin{cases} H^n(G, A) & n \geq 1 \\ \frac{A^G}{N_G A} & n = 0 \\ \frac{\{a \in A \mid N_G a = 0\}}{\langle g \cdot a - a \mid a \in A, g \in G\rangle} & n = -1 \\ H_{-n-1}(G, A) & n < -1 \end{cases}$$

where $N_G = \sum_{g \in G} g$.

Definition 3.1 (Cup Products)**.** *for all $m, n \in \mathbb{Z}$ and all G-modules A, B we have a* ***cup product*** *map*

$$\cup : \widehat{H}^m(G,A) \otimes \widehat{H}^n(G,B) \to \widehat{H}^{m+n}(G, A \otimes B)$$

which for $m = n = 0$ is given by the natural map $A^G \otimes B^G \to (A \otimes B)^G$ induced by tensor product.

Theorem 3.2 (Duality)**.** *Let A be a G-module which is $\mathbb{Z}$-free. Then*

$$\begin{tikzcd}
\widehat{H}^n(G,A) \otimes \widehat{H}^{-n}(G, \mathrm{Hom}(A,\mathbb{Z})) \arrow[d, "\cup"] \\
\widehat{H}^0(G, A \otimes \mathrm{Hom}(A,\mathbb{Z})) \arrow[d, "(a\otimes\varphi \mapsto \varphi(a))"] \\
\widehat{H}^0(G,\mathbb{Z}) \arrow[d, equal] \\
\mathbb{Z}/\left|G\right|\mathbb{Z}
\end{tikzcd}$$

is a perfect pairing. Hence

$$\begin{aligned}
\widehat{H}^{-n}(G, \mathrm{Hom}(A,\mathbb{Z})) &\cong \mathrm{Hom}(\widehat{H}^n(G,A), \mathbb{Z}/\left|G\right|\mathbb{Z}) \\
&\cong \mathrm{Hom}(\widehat{H}^n(G,A), \mathbb{Q}/\mathbb{Z})
\end{aligned}$$

where the last step is because cohomology is $|G|$-torsion anyways.

Proof of Theorem 2.9.

$$\begin{tikzcd}
1 \arrow[r] & L^\times \arrow[r] & \mathbb{A}_L^\times \arrow[r] & C_L \arrow[r] & 1
\end{tikzcd}$$

is an exact sequence, and taking $\mathrm{Tor}^{\mathbb{Z}}$ gives us

$$\begin{tikzcd}
\mathrm{Tor}_1^{\mathbb{Z}}(C_L, \widehat{T^\circ}) \arrow[r] & \widehat{T}^\circ \otimes L^\times \arrow[r] & \widehat{T}^\circ \otimes \mathbb{A}_L^\times \arrow[r] & \widehat{T}^\circ \otimes C_L \arrow[r] & 0
\end{tikzcd}$$

So in particular

$$\widehat{T}^\circ \otimes C_L = \frac{T(\mathbb{A}_L)}{T(L)} =: C_L(T).$$

Then we take Tate cohomology

$$\begin{tikzcd}
\dots \arrow[r] & \widehat{H}^0(G, T(L)) \arrow[r, "\alpha"] & \widehat{H}^0(G, T(\mathbb{A}_L)) \arrow[r, "\beta"] & \widehat{H}^0(G, C_L(T)) \arrow[dll, "\gamma"] \\
\widehat{H}^1(G, T(L)) \arrow[r, "\delta"] & \widehat{H}^1(G, T(\mathbb{A}_L))
\end{tikzcd}$$

Now, it is an exercise to show that $H^1(G, T(L)) = H^1(k, T)$.

Furthermore, for all $r \in \mathbb{Z}$, $\widehat{H}^r(G, T(\mathbb{A}_L)) \cong \oplus_v \widehat{H}^r(G_v, T(L_v))$ via the restriction and corestriction maps (and the surjections/injections between $L_v^\times$ and $\mathbb{A}_L^\times$). So $\text{Ш}^1(T) = \ker(\delta) = \mathrm{im}(\gamma) \cong \mathrm{coker}(\beta)$.

Global Class Field Theory: $H^2(G, C_L) = \mathbb{Z}/\left|G\right|\mathbb{Z}$ with a canonical generator $u_{L/k}$ and for all $r \in \mathbb{Z}$, and all $\mathbb{Z}$-free modules M

$$\widehat{H}^r(G, M) \cong \widehat{H}^{r+2}(G, M \otimes C_L)$$
$$\chi \mapsto \chi \cup u_{L/k}$$

(This is just Tates theorem for class formations).

Local Class Field Theory: $H^2(G_v, L_v^\times) = \mathbb{Z}/\left|G_v\right|\mathbb{Z}$ with canonical generator, and for all $r \in \mathbb{Z}$ and all $\mathbb{Z}$-free modules M we again have

$$\widehat{H}^r(G_v, M) \cong \widehat{H}^{r+2}(G_v, M \otimes L_v)$$
$$\chi \mapsto \chi \cup \text{canonical generator}$$

(again this is just Tates theorem for class formations.)

Continuing with the Proof: Putting this together gives us

$$Ш^1(T) = \operatorname{coker}(\oplus_v H^{-2}(G_v, \widehat{T}^\circ) \to^{``\beta''} \widehat{H}^{-2}(G, \widehat{T}^\circ))$$

(This is using all of the above, in particular we are using the cup product isomorphism in reverse.)

and duality for Tate cohomology gives

$$\operatorname{Hom}(Ш^1(T), \mathbb{Q}/\mathbb{Z}) = \ker(H^2(G, \widehat{T}) \to \oplus_v H^2(G_v, \widehat{T}))$$

□

Lecture 3

We will start by defining weak approximation.

Definition 3.3. *We say that **weak approximation** holds for a variety X if the rational points $X(k)$ are dense in $\prod_v A(k_v)$ (the topology on the product is the product topology)*

Definition 3.4. *Let T/k be a torus. The **defect of weak approximation** for T is*

$$A(T) := \frac{\prod_v T(k_v)}{\overline{T(k)}}$$

where $\overline{T(k)}$ is the closure in the product topology.

Exercise 5 (23)**.** *Let $T = R^1_{L/k}\mathbb{G}_m$ with L/k Galois. Show that*

$$A(T) = \frac{T(\mathbb{A}_k)}{T(k)N_{L/k}T(\mathbb{A}_L)}$$

Theorem 3.5 (24, Voskresenski)**.** *Let T be as in Ex 5 and $G = \operatorname{Gal}(L/k)$. Then we have an exact sequence*

$$0 \longrightarrow A(T) \longrightarrow \operatorname{Hom}(H^3(G, \mathbb{Z}), \mathbb{Q}/\mathbb{Z}) \longrightarrow Ш^1(T) \longrightarrow 0$$

Corollary 3.6 (25)**.** *If T is as above and $H^3(G, \mathbb{Z}) = 0$ then the HNP holds for L/k and weak approximation holds for T.*

Proof. Recall the exact sequence from the proof of Theorem 2.9:

$$\begin{tikzcd}[column sep=small]
 & \dots \arrow[r] & \widehat{H}^0(G,T(L)) \arrow[r, "\alpha"] & \widehat{H}^0(G,T(\mathbb{A}_L)) \arrow[r, "\beta"] & \widehat{H}^0(G,C_L(T)) \arrow[dlll, "\gamma"] \\
\widehat{H}^1(G,T(L)) \arrow[r, "\delta"] & \widehat{H}^1(G,T(\mathbb{A}_L)) & & &
\end{tikzcd}$$

In the proof of Theorem 2.9 we showed that $Ш^1(T) = \mathrm{im}(\gamma)$. Consider

$$\begin{tikzcd}
\widehat{H}^0(G,T(L)) \arrow[r, "\alpha"] \arrow[d, equal] & \widehat{H}^0(G,T(\mathbb{A}_L)) \arrow[d, equal] \\
T(k)/N_{L/k}T(L) & T(\mathbb{A}_k)/N_{L/k}T(\mathbb{A}_L)
\end{tikzcd}$$

We obtain a short exact sequence

$$\begin{tikzcd}
0 \arrow[r] & \frac{T(\mathbb{A}_k)}{T(k)N_{L/k}T(\mathbb{A}_L)} \arrow[r, "\beta"] & \widehat{H}^0(G,C_L(T)) \arrow[r] & Ш^1(T) \arrow[r] & 0
\end{tikzcd}$$

By exercise 5 the injective term is $A(T)$. Further we see that the middle term is, as in the proof of Theorem 2.9, is $\mathrm{Hom}(\widehat{H}^2(G,\widehat{T}),\mathbb{Q}/\mathbb{Z})$ Now it remains to show that $\widehat{H}^2(G,\widehat{T}) = H^3(G,\mathbb{Z})$ (an easy exercise) $\square$

Theorem 3.7 (Colliot-Thélène & Sansuc, 26)**.** *T/k split by a finite Galois extension L/k with $\mathrm{Gal}(L/k) = G$ then*

$$\begin{tikzcd}
0 \arrow[r] & A(T) \arrow[r] & \mathrm{Hom}(Ш^2_w(G,\widehat{T}),\mathbb{Q}/\mathbb{Z}) \arrow[r] & Ш^1(T) \arrow[r] & 0
\end{tikzcd}$$

is exact.

4 The First Obstruction to the HNP

Definition 4.1. *Let $F/L/k$ be a tower of number fields where F/k is Galois. The* ***first obstruction*** *to the HNP corresponding to this tower is*

$$\mathscr{F}(F/L/k) = \frac{N_{L/k}\mathbb{A}_L^\times \cap k^\times}{(N_{F/k}\mathbb{A}_F^\times \cap k^\times)N_{L/k L^\times}}$$

Remark 4.2.
1. *The knot group $\kappa(L/k)$ surjects onto $\mathscr{F}(F/L/k)$, so if this first obstruction is nontrivial then so is the knot group and L/k does not satisfy HNP.*
2. *If HNP holds for F/k then $N_{F/k}\mathbb{A}_F^\times \cap k^\times = N_{F/k}F^\times$, and so $\mathscr{F}(F/L/k) = \kappa(L/k)$.*

Proposition 4.3 (29, Drakonkhurst & Platonov)**.** *For $F/L/k$ as above, let $G = \mathrm{Gal}(F/k)$ and $H = \mathrm{Gal}(F/L)$. Consider the commutative diagram*

$$\begin{tikzcd}
\widehat{H}^0(H,C_F) \arrow[r, "\psi_1"] & \widehat{H}^0(G,C_F) \\
\widehat{H}^0(H,\mathbb{A}_F^\times) \arrow[r, "\psi_2"] \arrow[u, "\varphi"', "1"] & \widehat{H}^0(G,\mathbb{A}_F^\times) \arrow[u, "\varphi_2"']
\end{tikzcd}$$

where the φ_i are induced by the natural surjection $\mathbb{A}_F^\times C_F$ and the ψ_i are $\mathrm{Cor}_H^G = N_{L/k}$, then

$$\frac{\ker \psi_1}{\varphi_1(\ker \psi_2)} \cong \mathscr{F}(F/L/k)$$

Recall that class field theory gives isomorphisms

$$\frac{C_k}{N_{F/k} C_F} = \widehat{H}^0(G, C_F) \cong \widehat{H}^{-2}(G, \mathbb{Z}) = H_1(G, \mathbb{Z}) = G^{\mathrm{ab}}$$

and

$$\widehat{H}^0(G, \mathbb{A}_F^\times) = \bigoplus_{v \in M_k} \widehat{H}^0(G_v, F_v^\times) \cong \bigoplus_{v \in M_k} \widehat{H}^{-2}(G_v, \mathbb{Z}) \cong \bigoplus_{v \in M_k} \frac{G_v}{[G_v, G_v]}$$

and similarly for H. Now the diagram of Proposition 4.3 looks like

$$\begin{tikzcd} \frac{H}{[H,H]} \arrow[r, "\psi_1"] & \frac{G}{[G,G]} \\ \bigoplus_{v \in M_k} \bigoplus_{M_L \ni w | v} \frac{H_w}{[H_w, H_w]} \arrow[u, "\varphi_1"] \arrow[r, "\psi_2"] & \bigoplus_{v \in M_k} \frac{G_v}{[G_v, G_v]} \arrow[u, "\varphi_2"'] \end{tikzcd} \tag{2}$$

There is something subtle going on with the bottom map, note that separate places above a fixed place are conjugate. We give a concrete description: Write G as a disjoint union of its $H - G_v$ double cosets: $G = \bigcup_{i=1}^{r_v} H x_i G_v$ where x_i are the double coset representatives. Then

$$\{x_1, \ldots x_{r_v}\} \leftrightarrow \{w \mid v\}$$

is a 1:1 correspondence. Now, $H_w = x_i G_v x_i^{-1} \cap H$. If $h \in H_w = x_i G_v x_i^{-1} \cap H$ then $\psi_2(h) = x_i^{-1} h x_i \in \frac{G_v}{[G_v, G_v]}$. Hence

$$\mathscr{F}(F/L/k) = \frac{\ker \psi_1}{\varphi_1 \ker \psi_2}$$

is looking far more computable! The top part is easy, $\ker \psi_1 = H \cap [G, G]$, so if $H \cap [G, G] = [H, H]$ then the first obstruction $\mathscr{F}(F/L/k) = 1$.

Let ψ_2^v denote the restriction of ψ_2 to $\bigoplus_{w|v} \frac{H_w}{[H_w, H_w]}$.

Lemma 4.4 (Drakokhurst & Platonov, 30)**.** *If $G_{v_2} \subset G_{v_1}$ then $\varphi_1(\ker \psi_2^{v_2}) \subset \varphi_1(\ker \psi_2^{v_1})$.*

Proof. This is an exercise, a hint is: Let $G = \bigcup_{i=1}^r H x_i G_{v_1}$. Now write $H x_i G_{v_1} = \bigcup_{j=1}^{s_i} H x_i \gamma_{ij} G_{v_2}$ for $\gamma_{ij} \in G_{v_1}$. So $G = \bigcup_{i=1}^r \bigcup_{j=1}^{s_i} H x_i \gamma_{ij} G_{v_2}$ □

Let ψ_2^{nr} denote the restriction of ψ_2 to $\bigoplus_{v \text{ unram} \in F/k} \bigoplus_{w|v} \frac{H_w}{[H_w, H_w]}$. Let ψ_2^r denote the restriction to the remaining (ramified) places $\bigoplus_{v \text{ ram} \in F/k} \bigoplus_{w|v} \frac{H_w}{[H_w, H_w]}$.

Note that $\varphi_1(\ker \psi_2) = \varphi_1(\ker \psi_2^r) \varphi_1(\ker \psi_2^{\mathrm{nr}})$.

Corollary 4.5 (31)**.** *Computing $\mathscr{F}(F/L/k)$ is a finite calculation.*

Proof. Lemma 4.4, the fact that finitely many places are ramified in F/k and the fact that G has finitely many cyclic subgroups. □

Lecture 4

We have broken our computation of $\mathscr{F}(F/L/k)$ into finitely many peices. Now we will look at the unramifiec part from the end of the last lecture.

Theorem 4.6 (Drakokhurst & Platonov, 32)**.**

$$\varphi_1(\ker \psi_2^{\mathrm{nr}}) = \Phi^G(H)/[H,H]$$

where

$$\Phi^G(H) = \left\langle h_i^{-1}h_2 \mid h_i \in H \text{ and } h_2 \text{ is } G \text{ -conjugate to } h_1 \right\rangle.$$

Corollary 4.7 (33)**.** *There is a surjection*

$$\frac{H \cap [G,G]}{\Phi^G(H)} \to \mathscr{F}(F/L/k)$$

so if $H \cap [G,G] = \Phi^G(H)$ then $\mathscr{F}(F/L/k) = 1$.

Theorem 4.8 (34, Drakokhurst & Platonov)**.** *$F/L/k$ and G, H as above. For $i = 1, \dots, n$ let $G_i < G$ and $H_i < H \cap G_i$, $L_i = F^{H_i}$ and $k_i = F^{G_i}$.*

Suppose that the HNP holds for each L_i/k_i and that

$$\bigoplus_{i=1}^{m} \mathrm{Cor}_{G_i}^{G} : \bigoplus_{i=1}^{m} \widehat{H}^{-3}(G, \mathbb{Z}) \to \widehat{H}^{-3}(G, \mathbb{Z})$$

is surjective. Then

$$N_{F/k}\mathbb{A}_F^\times \cap k^\times \subset N_{L/k}L^\times$$

and hence $\mathscr{F}(F/L/k) = \kappa(L/k)$.

Proof. Exercise: Use the identifications

$$\widehat{H}^{-3}(G, \mathbb{Z}) = \widehat{H}^{-1}(G, C_F)$$
$$\widehat{H}^{-3}(G_i, \mathbb{Z}) = \widehat{H}^{-1}(G_i, C_F)$$

□

Recall that $\mathrm{Hom}(\kappa(L/k), \mathbb{Q}/\mathbb{Z}) = \ker\left(H^2(G, \widehat{T}) \to \prod_v H^2(G_v, \widehat{T})\right)$ where

$$1 \longrightarrow T = R^1_{L/K}\mathbb{G}_m \longrightarrow R_{L/K}\mathbb{G}_m \longrightarrow \mathbb{G}_m \longrightarrow 1$$

Take characters

$$0 \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}[G/H] \longrightarrow \widehat{T} \longrightarrow 0$$

and we have a commutative diagram:

$$\begin{tikzcd}
H^2(G,\mathbb{Z}) \arrow[r, "\psi_1^\vee"] \arrow[d, "\varphi_2^\vee"] & H^2(G,\mathbb{Z}[G/H]) \arrow[r, "\theta"] \arrow[d, "\varphi_1^\vee"] & H^2(G,\widehat{T}) \arrow[r] \arrow[d, "\varphi_0^\vee"] & H^3(G,\mathbb{Z}) \\
\prod_v H^2(G_v,\mathbb{Z}) \arrow[r, "\psi_2^\vee"] & \prod_v H^2(G_v,\mathbb{Z}[G/H]) \arrow[r] & \prod_v H^2(G_v,\widehat{T}) &
\end{tikzcd} \tag{3}$$

By Shapiro, $H^2(G,\mathbb{Z}[G/H]) = H^2(H,\mathbb{Z})$, and by Mackey & Shapiro

$$\begin{aligned} H^2(G_v,\mathbb{Z}[G/H]) &= H^2(G_v, \operatorname{res}^G_{G_v} \operatorname{Ind}^G_H \mathbb{Z}) \\ &= H^2(G_v, \bigoplus_{w|v} \operatorname{Ind}^{G_v}_{H_w} \mathbb{Z}) \\ &= \bigoplus_{w|v} H^2(H_w,\mathbb{Z}) \end{aligned}$$

So the first square of our diagram is dual to (2): Recall

$$\mathscr{F}(F/L/k) = \frac{\ker\psi_1}{\varphi_1(\ker\psi_2)}$$

so (exercise)

$$\operatorname{Hom}(\mathscr{F}(F/L/k),\mathbb{Q}/\mathbb{Z}) = \frac{(\varphi_1^\vee)^{-1}(\operatorname{im}(\psi_2^\vee))}{\operatorname{im}(\psi_1^\vee)}$$

and so θ induces an injection

$$\operatorname{Hom}(\mathscr{F}(F/L/k),\mathbb{Q}/\mathbb{Z}) \to \ker(\varphi_0^\vee) = \operatorname{Hom}(\kappa(L/k),\mathbb{Q}/\mathbb{Z})$$

Theorem 4.9 (35, Macedo)**.** *Let p be a prime such that $H^2(G,\mathbb{Z})_{(p)} = 0$ (where we denote by $A_{(p)}$ the p-primary part of an abelian group A). Then*

$$\kappa(L/k)_{(p)} = \mathscr{F}(F/L/k)_{(p)}$$

Proof. Exercise. □

Macedo was able to use this to prove:

Theorem 4.10 (36, Macedo)**.** *Let $F/L/k$ and G,H be as above, with $G \cong A_n$ or S_n and $n \geq 4$, $G \neq A_6, A_7$. Then*

$$\kappa(L/k) = \begin{cases} \mathscr{F}(F/L/k) & |H| \in 2\mathbb{Z} \\ \mathscr{F}(F/L/k) \times \kappa(F/k) & |H| \in 2\mathbb{Z}+1 \end{cases}$$

Sketch proof: For $|H|$ even, first show that there is a subgroup $V_4 \subset G$ such that $|V_4 \cap H| \geq 2$ and

$$\operatorname{Cor}^G_{V_4} : \widehat{H}^{-3}(V_4,\mathbb{Z}) \to \widehat{H}^{-3}(G,\mathbb{Z})$$

is surjective. Now use Theorem 4.8. The case $|H|$ odd is an exercise using the result of exercise 2 on the problem sheet □

5 Number Fields with Prescribed Norms

(Joint with C. Frei & D. Loughran) Let k be a number field and G a finite abelian group. Let $\alpha \in k^\times$.

Question 1 (37)**.** *Does there exist L/k Galois with $\operatorname{Gal}(L/k) \cong G$ such that $\alpha \in N_{L/k}L^\times$? It suffices to show that there is some L/k a G-extension such that the HNP holds for L/k and $\alpha \in N_{L/k}\mathbb{A}_L^\times$.*

We gave a positive answer to Question1 by counting. We reduce to local conditions via

Theorem 5.1 (Frei & Loughran & Newton, 38). *HNP holds for* 100% *of G-extensions L/k for which $\alpha \in N_{L/k}\mathbb{A}_L^\times$, ordered by conudctor.*

It is important that we count by conductor here, if we were to instead count by discriminant the result is different.

Corollary 5.2 (39). *HNP holds for* 100% *of G-extensions of k ordered by conductor.*

Proof. Take $\alpha = 1$ □

To prove Theorem 5.1, use Tates result (Theorem 1.3) to give necessary local conditions for the failure of HNP. Count G-extensions L/k satisfying those local conditions and the local conditions given by $\alpha \in N_{L/k}\mathbb{A}_L^\times$. Show that this is 0% of G-extensions L/k such that $\alpha \in N_{L/k}\mathbb{A}_L^\times$.

5.1 Main Technical Result for Counting

At each place $v \in M_k$ we let Λ_v denote a set of "allowed" sub-G-extensions of k_v (i.e. F/k Galois with $\mathrm{Gal}(F_v/k_v) \subset G$). Let $\Lambda = (\Lambda_v)$ be our allowed conditions,

$$N(k, G\,\Lambda, B) = \#\left\{{\scriptstyle G-\text{extensions } L/k \text{ with conductor } \leq B \,:\, L_v \in \Lambda_v \ \forall v}\right\}$$

$$\omega(k, G, \alpha) = \sum_{g \in G \setminus \{1\}} \frac{1}{[k_{|g|} : k]}$$

where $|g|$ is the order of g and $k_d = k(\mu_d, \sqrt[d]{\alpha})$.

Theorem 5.3 (Frei & Loughran & Newton (FLN), 40). *Let S be a finite set of places of k. For $v \in S$ let Λ_v be a nonempty set of sub-G-extensions of k_v. For $v \notin S$ let $\Lambda_v = \left\{F/k_v : \text{sub-}G\text{-extensions s.t. } \alpha \in N_{F/k_v}F^\times\right\}$ Then*

$$N(k, G, \Lambda, B) \sim c_{k,G,\Lambda} B (\log B)^{\omega(k,G,\alpha)-1}$$

as $B \to \infty$. Where $c > 0$ if there is a sub-G-extension L/k with $L_v \in \Lambda_v$ for all v.

Definition 5.4.

$$N_{\mathrm{loc}}(k, G, \alpha, B) = \#\left\{G\text{-extensions } L/k \text{ with conductor } \leq B \text{ s.t. } \alpha \in N_{L/k}\mathbb{A}_L^\times\right\}$$
$$N_{\mathrm{glob}}(k, G, \alpha, B) = \#\left\{G\text{-extensions } L/k \text{ with conductor } \leq B \text{ s.t. } \alpha \in N_{L/k}L^\times\right\}$$

Theorem 5.5 (FLN, 41). $N_{\mathrm{loc}}(k, G, \alpha, B) \sim c \cdot B(\log B)^{\omega(k,G,\alpha)-1}$ *for some $c > 0$.*

Proof. Apply Theorem 5.3 with $S = \emptyset$. To show $c > 0$ need a sub-G-extension with $\alpha \in N_{L/k}\mathbb{A}_L^\times$. But we can take the trivial extension! $L = k$. □

Theorem 5.6 (FLN, 42). $N_{\mathrm{glob}}(k, G, \alpha, B) \sim c \cdot B(\log B)^{\omega(k,G,\alpha)-1}$ *for some $c > 0$.*

Proof. Theorem 5.5 and Theorem 5.1. □

Corollary 5.7 (43). *The answer to Question 1 is YES!*