PROBLEMS ON THE HASSE NORM PRINCIPLE (HNP)

RACHEL NEWTON

k is a number field throughout. All field extensions are finite.

1. Knot groups

Let L/k be an extension of number fields. The knot group $\mathfrak{K}(L/k)$ is defined as

$$\mathfrak{K}(L/k) = \frac{N_{L/k}\mathbb{A}_L^* \cap k^*}{N_{L/k}L^*}.$$

(1) Let L/k be an extension of number fields. Show that $\mathfrak{K}(L/k)$ is killed by $[L:k]$.

(2) Let $F/L/k$ be a tower of number fields and let $d = [F : L]$. Show that $x \mapsto x^d$ induces a homomorphism $\varphi : \mathfrak{K}(L/k) \to \mathfrak{K}(F/k)$ such that $\ker \varphi \subset \mathfrak{K}(L/k)[d]$ and $\{y^d \mid y \in \mathfrak{K}(F/k)\} \subset \operatorname{Im} \varphi$. Show that if $|\mathfrak{K}(L/k)|$ is coprime to d then φ induces an isomorphism $\mathfrak{K}(L/k) \to \{y^d \mid y \in \mathfrak{K}(F/k)\}$.

(3) Let L/k be a Galois extension such that every decomposition group is cyclic. Show that weak approximation holds for $R^1_{L/k}\mathbb{G}_m$.

(4) Let $a, b \in \mathbb{Z} \setminus \{1, 0\}$ be coprime, squarefree and congruent to 1 modulo 4. Show that the HNP fails for $\mathbb{Q}(\sqrt{a}, \sqrt{b})/\mathbb{Q}$ if and only if $\left(\frac{a}{p}\right) = 1$ for all primes p dividing b and $\left(\frac{b}{p}\right) = 1$ for all primes p dividing a.

(5) Let L/k be biquadratic. Show that the HNP holds for L/k if and only if weak approximation fails for $R^1_{L/k}\mathbb{G}_m$.

(6) Let F/k be a Galois extension with Galois group A_4 and let L/k be a quartic subextension of F/k. Let K/k be the fixed field of V_4 in F/k. Show that

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

(7) Show that the HNP holds for any Galois extension of degree 6.

(8) Show that the HNP holds for an extension of prime degree.

(9) Let G be a finite abelian group. Show that $H^3(G, \mathbb{Z}) = 0$ iff G is cyclic. Let k be a number field. Shafarevich's resolution of the inverse Galois problem for soluble groups produces a Galois extension L/k with $\mathrm{Gal}(L/k) \cong G$ with all decomposition groups

cyclic. Hence conclude that there exists a Galois extension L/k with $\mathrm{Gal}(L/k) \cong G$ for which the HNP fails iff G is non-cyclic.

2. Tori

(10) Show that $R_{\mathbb{C}/\mathbb{R}}\mathbb{G}_m$ is a torus.
(11) Let L/k be a finite extension. Let $T = R^1_{L/k}\mathbb{G}_m$. Show that $Ш^1(T) = \mathfrak{K}(L/k)$.
(12) Show that the module of characters of $\mathbb{G}_m$ is $\mathbb{Z}$.
(13) Let L/k be a Galois extension with Galois group G. Show that the module of characters of $R_{L/k}\mathbb{G}_m$ is $\mathbb{Z}[G]$.
(14) Let $F/L/k$ be a tower of number fields with F/k Galois, $\mathrm{Gal}(F/k) = G$, $\mathrm{Gal}(F/L) = H$. Show that the module of characters of $R_{L/k}\mathbb{G}_m$ is $\mathbb{Z}[G/H]$.
(15) Let L/k be a Galois extension. Let $T = R^1_{L/k}\mathbb{G}_m$. Show that $Ш^2_\omega(G, \hat{T}) = H^3(G, \mathbb{Z})$.
(16) Let T be a torus, let $\hat{T}$ be its module of characters and let $\hat{T}^\circ$ be its module of co-characters. Show that there is a perfect pairing $\hat{T} \otimes \hat{T}^\circ \to \mathbb{Z}$.
(17) Let L/k be a Galois extension. Let $T = R^1_{L/k}\mathbb{G}_m$. Let $A(T) = \prod_v T(k_v)/\overline{T(k)}$, where $\overline{T(k)}$ denotes the closure of $T(k)$ in $\prod_v T(k_v)$. Let S be the set of places of k that ramifiy in L/k. Show that

$$A(T) = \prod_{v \in S} T(k_v)/\overline{T(k)} = \prod_{v \in S} T(k_v)/T(k) \prod_{v \in S} N_{L_w/k_v} T(L_w) = T(\mathbb{A}_k)/T(k)N_{L/k}T(\mathbb{A}_L)$$

where for each $v \in S$, we have chosen one place w of L above v.

3. The first obstruction to the HNP

(18) Let $F/L/k$ be a tower of number fields with F/k Galois, $\mathrm{Gal}(F/k) = G$, $\mathrm{Gal}(F/L) = H$. Consider the commutative diagram

$$\begin{array}{ccc} \hat{H}^0(H, C_F) & \xrightarrow{\psi_1} & \hat{H}^0(G, C_F) \\ \uparrow{\scriptstyle \varphi_1} & & \uparrow{\scriptstyle \varphi_2} \\ \hat{H}^0(H, \mathbb{A}_F^*) & \xrightarrow{\psi_2} & \hat{H}^0(G, \mathbb{A}_F^*) \end{array}$$

where the vertical arrows are induced by $\mathbb{A}_F^* \to \mathbb{A}_F^*/F^* = C_F$ and the horizontal arrows are given by $\mathrm{Cor}_H^G = N_{L/k}$. Show that the norm map $N_{L/k}$ induces an isomorphism

$$\frac{\ker \psi_1}{\varphi_1(\ker \psi_2)} \to \frac{N_{L/k}\mathbb{A}_L^* \cap k^*}{(N_{F/k}\mathbb{A}_F^* \cap k^*)N_{L/k}L^*}.$$

(19) Let $F/L/k$ be a tower of number fields with F/k Galois, $\mathrm{Gal}(F/k) = G$, $\mathrm{Gal}(F/L) = H$. Let Ω_k denote the set of places of k. Consider the commutative diagram

$$\begin{array}{ccc} H/[H,H] & \xrightarrow{\psi_1} & G/[G,G] \\ \uparrow{\scriptstyle \varphi_1} & & \uparrow{\scriptstyle \varphi_2} \\ \oplus_{v\in\Omega_k}\left(\oplus_{w|v} H_w/[H_w,H_w]\right) & \xrightarrow{\psi_2} & \oplus_{v\in\Omega_k} G_v/[G_v,G_v] \end{array}$$

For a place v of k, let ψ_2^v denote the restriction of ψ_2 to $\oplus_{w|v} H_w/[H_w,H_w]$. Show that if v_1, v_2 are places such that the decomposition groups satisfy $G_{v_2} \subset G_{v_1}$ then

$$\varphi_1(\ker\psi_2^{v_2}) \subset \varphi_1(\ker\psi_2^{v_1}).$$

Hint: choose representatives $x_1, \dots x_r$ for the H–G_{v_1} double coset decomposition of G, so $G = \cup_{i=1}^r H x_i G_{v_1}$. Now decompose each double coset as $H x_i G_{v_1} = \cup_{j=1}^{s_i} H x_i y_{ij} G_{v_2}$ and hence obtain the H–G_{v_2} double coset decomposition of G of the form $\cup_{i=1}^r \cup_{j=1}^{s_i} H x_i y_{ij} G_{v_2}$.

(20) Let $F/L/k$ be as above and suppose that $[L:k]$ is squarefree. Show that

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

4. Number fields with prescribed norms

Let k be a number field, G a finite abelian group, and $\alpha \in k^*$. A G-extension of k is a Galois extension L/k with an isomorphism $\mathrm{Gal}(L/k) \to G$. A sub-G-extension of a field F is a Galois extension E/F with an injection $\mathrm{Gal}(E/F) \hookrightarrow G$.

Definition 1. For $d \in \mathbb{N}$, let $k_d = k(\mu_d, \sqrt[d]{\alpha})$. We define

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

where $|g|$ denotes the order of g in G and $\mathrm{id}_G \in G$ is the identity element.

Theorem 2. *Let S be a finite set of places of k. For $v \in S$ let Λ_v be a non-empty set of sub-G-extensions of k_v. For $v \notin S$, let $\Lambda_v = \{$sub-G-extensions $F/k_v \mid \alpha \in N_{F/k_v}F^*\}$. Let $N(k,G,\Lambda,B)$ be the number of G-extensions L/k such that $L_v \in \Lambda_v$ $\forall v \in \Omega_k$ and the norm of the conductor of L/k is at most B. Then*

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

as $B \to \infty$, for some constant $c_{k,G,\alpha}$ which is positive if there exists a sub-G-extension L/k with $L_v \in \Lambda_v$ for all $v \in \Omega_k$.

(21) Let $\alpha \in k^* \setminus k^{*2}$. Show that for 100% of quadratic extensions of k, α is not in the image of the norm map.

(22) Let G be an abelian group of exponent e. Let F be a local field and let $\alpha \in F^{*e}$. Show that for any Galois extension E/F with $\mathrm{Gal}(E/F) \hookrightarrow G$, we have $\alpha \in N_{E/F}E^*$.

Definition 3.
- Let $N(k, G, \alpha, B)$ be the number of G-extensions L/k such that $\alpha \in N_{L_v/k_v} L_v^*$ for all $v \in \Omega_k$ and the norm of the conductor of L/k is at most B.
- Let $N(k, G, B) = N(k, G, 1, B)$ be the number of G-extensions L/k such that the norm of the conductor of L/k is at most B.

(23) Let $e = \exp(G)$. Show that the following are equivalent:
  (a) $\lim_{B\to\infty} \frac{N(k,G,\alpha,B)}{N(k,G,B)} > 0$;
  (b) $\alpha \in k(\mu_d)^{*d}\ \forall d \mid e$;
  (c) $\alpha \in k_v^{*e}$ for all but finitely many v.

(24) Let $e = \exp(G)$. Show that $\lim_{B\to\infty} \frac{N(k,G,\alpha,B)}{N(k,G,B)}$
  (a) is 1 if $\alpha \in k^{*e}$;
  (b) only depends on $\overline{\alpha} \in k^*/k^{*e}$;
  (c) is 0 for all but finitely many $\overline{\alpha} \in k^*/k^{*e}$.