A NOTE ON HILBERT'S THEOREM 90

BAO-PING JIA AND LARRY SANTONI

(Communicated by Maurice Auslander)

Abstract. In this paper we extend "up to powers" Hilbert's Theorem 90 to arbitrary finite Galois extensions. In the case of algebraic number fields with class number equal to 1, we completely determine the kernel and image of the norm map.

Let $L/K$ be a finite Galois extension with Galois group $G$. Hilbert's Theorem 90 gives us a characterization of the kernel of the norm map in the case where $L$ is a cyclic extension, i.e., if $G$ is a cyclic group. In this paper, we investigate the module structure of the multiplicative group of field extensions as $ZG$-modules and their associated norm functions. We obtain some partial results about the image and the kernel of these norm functions. For example, by using a theorem from [J] (see (1.6) in §1 below), we find the kernel and image of $1_Q \otimes_z N$, where $N : L^* \to K^*$ is the norm map $1_Q \otimes_z L^* \to Q \otimes_z K^*$ (where $L^*$ denotes the nonzero elements of $L$). We will omit the subscript $Z$ in the tensor product notation as is conventional. We have completely determined the kernel and image of the norm map in the situation of algebraic number fields with class number equal to 1. We also obtain a partial generalization of Hilbert's Theorem 90 to arbitrary finite Galois field extension, not necessarily cyclic.

1. Hilbert's Theorem 90

Let $L/K$ be a finite Galois extension with Galois group $G$, and let $ZG$ be the group ring. If $\alpha \in L^*$ and $g \in G$, we write $\alpha^g$ instead of $g(\alpha)$. Since $\alpha^n$ is the $n$th power of $\alpha$ as usual, in this way $L^*$ becomes a right $ZG$-module in the obvious way. For example, if $r = 3g + 5 \in ZG$, then $\alpha^r = (\alpha^3)^g(\alpha^5)$. For any $\omega \in L^*$, the norm of $\omega$ is defined to be $N(\omega) = N_{L/K}(\omega) = \prod\{\omega^g | g \in G\}$. If we let $c = \sum\{g | g \in G\}$, then $N(\omega) = \omega^c$.

Before going further we first quote some results from [J].

1.1. Theorem. Let $L/K$ be a finite Galois extension with Galois group $G$, and assume that $K$ is not an algebraic extension of a finite field. Then $Q \otimes L^*$ is a free $QG$-module of rank $\text{card}(K)$.
1.2. **Corollary.** \( L^* \) is a \( \mathbb{Z}G \)-module, and there is a free \( \mathbb{Z}G \)-module \( F \) contained in \( L^* \) such that:

(1.2.1) \( L^*/F \) is a torsion abelian group;
(1.2.2) \( \alpha \in F \cap K \Leftrightarrow \alpha = N(\beta) \) for some \( \beta \in F \); i.e., \( \text{image}(N|_F) = F \cap K \) and \( \ker(N|_F) = \{ F(1 - g)| g \in G \} \);
(1.2.3) For each \( \alpha \in L^* \), there exists an integer \( m \) such that \( \alpha^m \in K \Leftrightarrow \alpha = N(\beta) \) for some \( \beta \in L^* \).

**Proof.** If \( K \) is algebraic over a finite field, then \( L^* \) is torsion and we let \( F = 1 \). If \( K \) is not algebraic over any finite field, then, by (1.1), \( \mathbb{Q} \otimes L^* \) is a free \( \mathbb{Q}G \)-module of rank \( \text{card}(K) \). One checks that if \( b = \sum r_i \otimes g_i \) is a basis element for \( \mathbb{Q} \otimes L^* \), then it may be rewritten as \( b = \frac{1}{n} \gamma \) for a suitable choice of \( d \in \mathbb{Q} \) and \( \gamma \in L^* \). Then let \( F \) be the free \( \mathbb{Z}G \)-module generated by the \( \gamma \)'s and (1.2.1) follows. For (1.2.2), let \( c = \sum \{ g| g \in G \} \). If \( \alpha = N(\beta) \) for some \( \beta \in F \), then \( \alpha = \beta^c \in F \cap K \). If \( 1 \neq \alpha \in F \cap K \), then \( \alpha^c = \alpha^n \) where \( n = [L : K] \). Since \( F \) is free, we may assume that \( \alpha = \prod \{ g^d \}| g \in G \} \) where \( \gamma \) is a basis element of \( F \) and \( a_{g, \gamma} \) is an integer for each \( g \) and each \( \gamma \). Then for each fixed \( \gamma \), \( na_g, \gamma = \sum \{ a_{g, \gamma}| h \in G \} \) for each \( g \), and we let \( a_g = a_{g, \gamma} a_{h, \gamma} \) for all \( g \) and \( h \). Let \( \beta = \sum \{ \gamma^d \} \). Then \( \alpha = \text{res}(\beta) = \beta^c \). The theorem follows.

1.3. **Theorem.** Let \( L/K \) be a finite Galois extension with Galois group \( G \), and assume that \( K \) is not an algebraic extension of a finite field (otherwise \( \mathbb{Q} \otimes L^* = 0 \)). Let \( H \) be any subgroup of \( G \), and let \( L_H = \{ \alpha \in L|\alpha^h = \alpha \text{ for all } h \in H\} \) be the fixed field of \( H \) and \( c_H = \sum \{ h| h \in H \} \). Then \( \mathbb{Q} \otimes L_H^* \cong (\mathbb{Q}G)^{c_H} = (\mathbb{Q}(Gc_H)^{c_H} \text{ card}(K)) \).

**Proof.** Since \( \mathbb{Q} \otimes L^* \cong (\mathbb{Q}G)^{c_H} \), with some abuse of notation, we may identify \( 1 \otimes \alpha \) with its image in \( \mathbb{Q}G \). For any \( \alpha \in L_H^* \), \( (1 \otimes \alpha)h = (1 \otimes \alpha^h) = (1 \otimes \alpha) \). Without loss of generality, we may assume \( 1 \otimes \alpha \in \mathbb{Q}G \). Then \( 1 \otimes \alpha = \sum \{ a_g h| g \in G \text{ and } a_g \in \mathbb{Q} \} \). Write \( G = \bigcup \{ g_i H| 1 \leq i \leq r \} \), where \( r = [G : H] \). Then \( 1 \otimes \alpha = \sum \{ a_{ih} g_i h| h \in H \}, 1 \leq i \leq r \text{ and } a_{ih} \in \mathbb{Q} \). Since \( (1 \otimes \alpha)h = (1 \otimes \alpha) \), for each \( i \), there exists \( a_i \in \mathbb{Q}G \) such that \( a_i = a_{ih} \) for any \( h \in H \). Therefore \( 1 \otimes \alpha \in \mathbb{Q}Gc_H \) and \( \mathbb{Q} \otimes L^*_H \subseteq (\mathbb{Q}Gc_H)^{c_H} \). Conversely, we choose \( F = (\mathbb{Q}G)^{c_H} \) as in (1.2) such that \( \mathbb{Q} \otimes L^* = (\mathbb{Q}G)^{c_H} = \mathbb{Q} \otimes F \). Then \( F \subseteq \mathbb{Q} \otimes F = \mathbb{Q} \otimes L^* = (\mathbb{Q}G)^{c_H} \). If \( \beta \in \mathbb{Q}Gc_H \subseteq \mathbb{Q}G \), then \( \beta = 1 \otimes \alpha \) for some \( \alpha \in F \). Now \( \beta h = \beta \) implies that \( \alpha h = \alpha \) since \( F \) is free. Therefore \( \alpha \in L_H^* \), and \( (\mathbb{Q}Gc_H)^{c_H} \subseteq L^*_H \). The theorem follows.

1.4. **Corollary.** Let \( K/k \) be a finite separable extension. Suppose \( k \) is not algebraic over a finite field. Let \( L \) be the normal closure of \( K \) and let \( G = \text{Gal}(L/k) \). Then \( K = L_H \) is the fixed field of \( H \) for some subgroup \( H \) of \( G \) and \( \mathbb{Q} \otimes K^* \cong ((\mathbb{Q}G)^{c_H}) = (\mathbb{Q}Gc_H)^{c_H} \text{ card}(K), \text{ where } c_H = \sum \{ h| h \in H \} \).

If \( G \) is generated by elements \( g_1, \ldots, g_m \), then, in the group ring \( \mathbb{Z}G \), for any \( g \in G \), \( 1 - g \in \sum \{ \mathbb{Z}G(1 - g_i)| 1 \leq i \leq m \} \)—the left ideal of \( \mathbb{Z}G \) generated by the \( g_i \)'s. The reason is that any element of \( G \) is a product of powers of the \( g_i \)'s. For example,

\[
1 - g_i^e = (1 + g_i + \cdots + g_i^{e-1})(1 - g_i) \in \sum \{ \mathbb{Z}G(1 - g_i)| 1 \leq i \leq m \}.
\]
Therefore
\[ 1 - g_1^e g_2^e g_3^e = 1 - g_1^e + g_1^e g_2^e + g_1^e g_2^e g_3^e = (1 - g_1^e) + g_1^e (1 - g_2^e) + g_1^e g_2^e (1 - g_3^e) \in \sum \{ ZG(1 - g_i) | 1 \leq i \leq m \}. \]

The following corollary is an easy consequence of (1.2).2.

1.5. **Corollary.** If \( G \) is generated by elements \( g_1, \ldots, g_m \), then, in the group ring \( ZG \), \( \sum \{ ZG(1 - g_i) | 1 \leq i \leq m \} \) is a left ideal of \( ZG \) generated by the elements \( g_i \)'s. For each \( g \in G \), \( 1 - g \in \sum \{ ZG(1 - g_i) | 1 \leq i \leq m \} \). Let \( F \) be as in (1.2). Then \( \ker(\text{N}|_F) = \sum \{ F(1 - g_i) | 1 \leq i \leq m \} \).

1.6. **Theorem.** Let \( L/K \) and \( G \) be as in (1.1). Suppose \( G \) is generated by elements \( g_1, \ldots, g_m \). If \( \eta \in L^* \) and \( \text{N}(\eta) = 1 \), then \( \eta^n = \prod \{ \beta_i^{1-g_i} | 1 \leq i \leq m \} \) for some \( \beta_i \in L^* \) and \( n = [L : K] \).

**Proof.** Suppose \( 1 = \text{N}(\eta) = \eta^c \). Therefore \( \eta = \prod \{ \eta^{1-g} | 1 \neq g \in G \} \) and \( \eta^n = \prod \{ \eta^{1-g} | g \in G \} \). The result follows from (1.5).

1.7. **Theorem (Hilbert's Satz 90).** Let \( L/K \) be a cyclic extension, and let \( \eta \) be a generator of the Galois group of \( L/K \). Let \( N = NL/K \). Then \( \text{N}(u) = 1 \) for \( u \in L \) if and only if there exists a \( v \in L \) such that \( u = v/v^n \) (sometimes written as \( v^{1-n} \)).

1.8. **Corollary.** Let \( L/K \) be a Galois extension with Galois group \( G \). Suppose \( G \) is generated by elements \( g_1, \ldots, g_m \). Then

(1.8.1) \( Q \otimes \ker(\text{N}) \cong I^{\text{card}(L)} \), where \( I \) is the left ideal of \( QG \) generated by \( 1 - g_i, 1 \leq i \leq m \);

(1.8.2) \( Q \otimes N(L^*) \cong c(QG)^{\text{card}(L)} = (Qc)^{\text{card}(L)} \), where \( c = \sum \{ g | g \in G \} \);

(1.8.3) \( Q \otimes (L^*/K^*) \cong R^{\text{card}(L)} \), where \( R = QG/Qc \).

**Proof.** (1.8.1) follows from (1.6), and (1.8.2) is trivial since \( QGc = Qc \). (1.8.3) follows from the fact that if \( \alpha \in K \), then \( \alpha^n = \text{N}(\alpha) \) with \( n = [L : K] \), hence \( \frac{1}{n} \otimes \alpha = 1 \otimes \alpha^n = 1 \otimes \text{N}(\alpha) \) and \( Q \otimes \text{N}(L^*) \supset Q \otimes K^* \).}

2. **Some results in algebraic number theory**

In this section we discuss some problems in algebraic number theory. A number of well-known results, which are quoted here, can be found in [K] or [M].

Let \( L/K \) be a Galois extension with Galois group \( G \). It is clear that the restriction of the norm function \( N = NL/K \) to the multiplicative group \( L^* \) of nonzero elements of \( L \) defines a homomorphism of \( L^* \) to \( K^* \). It is natural to seek information on the image \( \text{N}(L^*) \) and kernel of \( \text{N}: L^* \to K^* \). This information is usually not easy to obtain. In the case where the class number of \( L \) is equal to 1, we are able to answer this question. We also have some partial results in the general case.

2.1. **Notation.** Let \( K \) be a number field, and let \( A \) be the integral closure of \( Z \) in \( K \). Then \( A \) is a Dedekind domain. Let \( L/K \) be a finite Galois extension with Galois group \( G \). Let \( B \) be the integral closure of \( A \) in \( L \). Then \( L \) is the quotient field of \( B \). For each nonzero prime ideal \( p \) in \( A \), we can choose
just one nonzero prime ideal $P$ of $B$ such that $P \cap A = p$. Let $\mathcal{P}$ be the set of all such nonzero prime ideals in $B$, and let $v_{L/K} = \{P\text{-adic valuation on } L|P \in \mathcal{P}\}$, and $v_{L/K} = \{p\text{-adic valuation on } K|p = P \cap A \text{ and } P \in \mathcal{P}\}$. Since each nonzero element of $B$ is contained in only finitely many nonzero prime ideals of $B$, the set $v_{L/K}$ has finite character, i.e., for any nonzero element $a \in L$, only finitely many members of $v_{L/K}$ are nonzero at $a$. We also know that card($V$) = card($K$) = card($L$) since both $V$ and $K$ are countable. Let $v \in v_{L/K}$, and let $V \in v_{L/K}$ designate the corresponding extension of $v$. We define valuations $V^g$ for $g \in G$ by the formula $V^g(\alpha) = V(\alpha)$ for all $\alpha \in L^*$. (Equivalently, $V^g(\alpha) = V(\alpha^{-1})$.) Before proceeding to our main results, we first prove the following easy lemma.

2.2. Lemma. Let $K, A, L, B,$ and $G$ be as in (2.1), and let $U$ be the unit group of $B$. Let $\alpha, \beta \in B - \{0\}$. Then $V^g(\alpha) = V^g(\beta)$ for all $g \in G$ and all $V \in v_{L/K} \iff \alpha = u\beta$ for some $u \in U$.

Proof. We let $I = \alpha B$ and $J = \beta B$. Then $V^g(\alpha) = V^g(\beta)$ for all $g \in G$ and all $V \in v_{L/K} \iff I = J \iff \alpha = u\beta$ and $\beta = w\alpha$ for $u, w \in B$. But then $\alpha = u\beta = uw\alpha$, and we have $uw = 1$ and $u \in U$.

2.3. The map $\phi$ induced by $v = v_{L/K}$. For each $v \in v$, we define a homomorphism $\phi_v: L^* \to \mathbb{Z}G$ by

\begin{equation}
\phi_v(\alpha) = \sum \{(V^g(\alpha))g|g \in G\}.
\end{equation}

It is easy to check that $\phi_v$ is a $\mathbb{Z}G$-module homomorphism. Since $v_{L/K}$ has finite character, the $\mathbb{Z}G$-module homomorphisms $\phi_v$ induces a $\mathbb{Z}G$-module homomorphism $\phi = \bigoplus\{\phi_v|v \in v\}$ from $L^*$ to $(\mathbb{Z}G)^{\text{card}(v)}$, the direct sum of card($v$) copies of $\mathbb{Z}G$. We want to find the image and the kernel of $\phi$. Let $c$ be the sum, in $\mathbb{Z}G$, of the elements of $G$. Then $Zc$ is a $\mathbb{Z}G$-submodule of $\mathbb{Z}G$ and is also an ideal of $\mathbb{Z}G$. We note that since $\phi$ is a $\mathbb{Z}G$-module homomorphism from $L^*$ to $(\mathbb{Z}G)^{\text{card}(v)}$, $\phi$ commutes with $c$.

2.4. Theorem. Let $K, A, L, B,$ and $G$ be as in (2.1), and let $U$ be the unit group of $B$. Let $c$ be as in (2.3). Then

\begin{enumerate}
\item[(2.4.1)] $\ker(\phi) = U$ and $\text{image}(\phi)$ is a $\mathbb{Z}G$-submodule of $(\mathbb{Z}G)^{\text{card}(v)}$;
\item[(2.4.2)] $L^* \cong U \oplus \phi(L^*)$ as $\mathbb{Z}$-submodules;
\item[(2.4.3)] $\phi(N(L^*)) = c\phi(L^*) \subseteq c(\mathbb{Z}G)^{\text{card}(v)} = (Zc)^{\text{card}(v)}$.
\end{enumerate}

Proof. For each $x \in L^*$, since $L$ is the quotient field of $B$, we can write $x = \alpha/\beta$ for some $\alpha, \beta \in B - \{0\}$. Then $\phi(x) = 0 \iff \phi_v(x) = 0$ for all $v \in v \iff V^g(\alpha) = V^g(\beta)$ for all $g \in G$ and for all $V \in v \iff \alpha = u\beta$ for some $u \in U$. Since $\phi$ is a $\mathbb{Z}G$-module homomorphism and $\phi(L^*) \subseteq (\mathbb{Z}G)^{\text{card}(v)}$, $\phi(L^*)$ is a free $\mathbb{Z}$-module. Hence $L^* \cong U \oplus \phi(L^*)$ as $\mathbb{Z}$-modules (not as $\mathbb{Z}G$-modules).

2.5. Theorem. Let $K, A, L, B, c, U,$ and $G$ be as in (2.4), and let $n$ be the class number of $L$. Let $S = \{n^i|0 \leq i < \infty\}$, and let $\mathbb{Z}_S = S^{-1}\mathbb{Z}$ be the localization of $\mathbb{Z}$ at $S$. For any subgroup $H$ of $G$, let $c_H = \sum\{h|h \in H\} \in \mathbb{Z}_G$.

Then

\begin{enumerate}
\item[(2.5.1)] $\mathbb{Z}_S \otimes \phi(L^*)$ is a direct sum of cyclic right $\mathbb{Z}_SG$-modules on generators of the form $c_H$, where $H$ is a subgroup of $G$;
\end{enumerate}
(2.5.2) \( \mathbb{Z}_S \otimes \phi(N(L^*)) = \mathbb{Z}_S \otimes c(\phi(L^*)) \) is a direct sum of cyclic \( \mathbb{Z}_SG \)-modules
\( r_H c\mathbb{Z}_S \), where \( r_H = \text{card}(H) \) for the subgroup \( H \) of \( G \) and
\[ \mathbb{Z}_S \otimes \phi(N(L^*)) \subseteq c(\mathbb{Z}G)^{\text{card}(v)} = (\mathbb{Z}c)^{\text{card}(v)}. \]

**Proof.** Since \( n \) is the class number of \( L \), \( P^n \) is a principal ideal of \( B \) for any prime ideal \( P \) of \( B \). Let \( H = \{ g \in G | P^g = P \} \) be the decomposition group of \( P \), and let \( V \) be the \( P \)-adic valuation. Let \( \phi_v \) be defined by (2.3.1). Then \( \mathbb{1}_{\mathbb{Z}_S} \otimes \phi \) is a surjective \( \mathbb{Z}G \)-module homomorphism from \( \mathbb{Z}_S \otimes L^* \) to a sum of cyclic modules of the form \( \mathbb{Z}_H \mathbb{Z}_SG \), and the theorem follows from this.

**2.6. Corollary.** Let \( K, A, L, B, c, U \) be as in (2.4). Suppose the class number of \( L \) is equal to 1. Let \( G \) be generated by \( g_1, \ldots, g_m \). For any \( P \in \mathbb{P} \), let \( H_P = \{ g \in G | P^g = P \} \). Then
\[ (2.6.1) \phi(L^*) = \bigoplus \{ c_{H_P} \mathbb{Z}G | P \in \mathbb{P} \} \text{ and } L^* \cong U \oplus \phi(L^*) \text{ as } \mathbb{Z}G \text{-modules;} \]
\[ (2.6.2) N(L^*) \cong \Lambda \oplus c\phi(L^*), \text{ where } \Lambda \subseteq \{ 1, -1 \}; \]
\[ (2.6.3) c\phi(L^*) = \bigoplus \{ r_{H_P} (c\mathbb{Z}) | P \in \mathbb{P} \}. \]

Let \( M \) be the subgroup of \( \mathbb{Q} \) generated by \( \{ p^{d(p)} | p \text{ is a positive prime number of } \mathbb{Z} \} \), where \( d(p) = o(H_P) \) is the degree of the prime ideal \( P \) with \( P \cap \mathbb{Z} = p\mathbb{Z} \). Then
\[ (2.6.4) N(L^*) \cong \Lambda \oplus M \text{ and } M \text{ is torsionfree.} \]

Let \( U(1) = \{ u \in U | N(u) = 1 \} \). For each \( P \in \mathbb{P} \), choose \( \pi_P \in P \) such that \( P = \pi_P B \). Let \( D \) be the \( \mathbb{Z}G \)-submodule of \( L^* \) generated by \( \{ \pi_P^k | a = \beta - \beta g_i, \beta \in \mathbb{Z}G \} \), and let \( F \) be the submodule of \( L^* \) generated by all such \( \pi_P \)'s. Then
\[ (2.6.5) F \cong \phi(L^*) = \bigoplus \{ c_{H_P} \mathbb{Z}G | P \in \mathbb{P} \}, \text{ and } L^* = UF \cong U \oplus F \text{ is the direct product of } U \text{ and } F; \]
\[ (2.6.6) \ker(N) = U(1)D \text{ and } D \text{ is torsionfree.} \]

**Proof.** Since the class number of \( L/K \) is 1, \( \phi \) must be surjective and (2.6.1)–(2.6.5) follow. For (2.6.6), we need only check that the annihilator of \( c \) in \( \phi(L^*) \) is \( \phi(D) \). As in the proof of (1.3), write \( G = \bigcup \{ g_i H | 1 \leq i \leq r \} \), where \( r = [G : H] \). If \( 0 = (c_H \sum a_i g_i) c = c_H (\sum a_i - \sum a_i (1 - g_i)) c \), then \( \sum a_i = 0 \) since \( c \) annihilates the \( 1 - g_i \).

Let \( r \) and \( 2s \) denote the number of real and nonreal automorphisms of \( L \). Then the Dirichlet unit theorem tells us that \( U = W \oplus V \), where \( W \) is a finite cyclic group consisting of the roots of 1 in \( L \) and \( V \) is a free abelian group of rank \( r + s - 1 \). Then \( U \) is a finitely generated \( \mathbb{Z} \)-module and every subgroup of \( U \) is finitely generated as an abelian group.

**2.7. Lemma.** Let \( U(1) \) be as in (2.6). Then \( U(1) \cong W(1) \oplus V(1) \), where \( W(1) = \langle \omega \rangle \) is a finite cyclic group generated by some root \( \omega \) of 1 in \( L \) and \( V(1) \cong \bigoplus \{ \langle u_i | 1 \leq i \leq t \} \) is a free abelian group of rank \( t \leq r + s - 1 \).

**2.8. Corollary.** Let \( L \) and \( U \) be as in (2.6). Let \( U(1) \cong \langle \omega \rangle \oplus \bigoplus \{ \mathbb{Z}u_i | 1 \leq i \leq t \} \) be as in (2.7), and let \( D \) be as in (2.6). Then \( \ker(N) = U(1)D \cong \langle \omega \rangle \oplus \bigoplus \{ \mathbb{Z}u_i | 1 \leq i \leq t \} \oplus D \) is a direct sum.

**Remark.** A complete generalization of Hilbert's Theorem 90 can now be obtained in the case where the \( u_i \)'s can be written in the form \( u_i = \beta^{1-g} \). We do not know at this point whether this is always possible.
The results in this paper suggest that a unique factorization is possible even though the field is not the quotient field of a unique factorization domain. For example, (1.2) tells us that for any finite Galois extension $L/K$ with Galois group $G$, there is a free $\mathbb{Z}G$-module $F$ contained in $L^*$ such that $L^*/F$ is a torsion abelian group. It follows that some power of any nonzero element of $L$ can be factored with unique exponents in $\mathbb{Z}G$.

REFERENCES


Department of Mathematical Sciences, University of Alaska Fairbanks, Fairbanks, Alaska 99775