Equality of norm groups of subextensions of \( S_n(n \leq 5) \) extensions of algebraic number fields

Leonid Stern

Department of Mathematics, Towson University, Baltimore, MD 21252, USA

Received 30 April 2002; revised 7 February 2003
Communicated by J.S. Hsia

Abstract

Let \( E/k \) be a Galois extension of algebraic number fields with the Galois group isomorphic to the symmetric group \( S_n \) on \( n \leq 5 \) letters. For any field extensions \( k \subseteq K, L \subseteq E \) a necessary and a sufficient condition is given for the equality \( N_{K/k}K^* = N_{L/k}L^* \) to hold, where \( N_{K/k}K^* \) is the group of norms from \( K \) to \( k \) of the elements of the multiplicative group \( K^* \) of \( K \).

\( \odot \) 2003 Elsevier Inc. All rights reserved.

Let \( k \) be an algebraic number field. The main theorem in [9] states that for any finite Galois extensions \( K \) and \( L \) of \( k \)

\[ N_{K/k}K^* \subseteq N_{L/k}L^* \text{ iff } L \subseteq K. \]

In particular, the equality of norm groups of finite Galois extensions of \( k \) is equivalent to the equality of the extensions. For finite non-Galois extensions \( K \) and \( L \) of \( k \) the equality of norm groups holds provided that \( K \) and \( L \) are conjugate over \( k \). The converse, however, is false in general. To investigate the equality of norm groups in the case of non-Galois extensions, we defined in [10] a “weaker” equality of norm groups which is called almost equal norm groups. This relation is equivalent to the equality of certain subsets of a finite group that are defined as follows. Let \( H \) be a subgroup of a finite group \( G \). We define a subset of \( G \) by

\[ \mathcal{P}_G(H) = \{ g^{-1}hg/h \in H \text{ of prime power order, } g \in G \}. \]

We note that in [6,7] the relation of almost equal norm groups was characterized in terms of a decomposition type of ideals in finite extensions of algebraic number fields.
fields. In [11, Theorem 3, p. 343] we proved that the relation of almost equal norm groups is equivalent to the equality of norm groups of idele groups. More specifically, for any algebraic number field \( k \) we denote by \( J_k \) the idele group of \( k \). Also, for any finite extension of algebraic number fields \( L/k \) we set \( N(L/k) = k^* \cap N_{L/k}J_L \), where \( N_{L/k} \) is the norm operator. It follows that \( N(L/k) = \bigcap_v (k^* \cap [N_{L/k}L^*]_v) \) (see for instance [10, Proposition (1.3), p. 113]), where \( v \) ranges over all primes of \( k \), and \([N_{L/k}L^*]_v\) is the topological closure of \( N_{L/k}L^* \) in \( k_v^* \) (the multiplicative group of the completion of \( k \) at \( v \)). So if \( N_{K/k}K^* = N_{L/k}L^* \) for two finite extensions \( K/k \) and \( L/k \) of algebraic number fields, then \( N(K/k) = N(L/k) \).

Let \( K/k \) and \( L/k \) be finite extensions of algebraic number fields. Let \( E \) be a finite Galois extension of \( k \) containing \( K \) and \( L \). Suppose that \( G = G(E/k) \) and \( H_L = G(E/L) \). In [11] we proved that the inclusion \( \mathcal{P}_G(H_K) \subseteq \mathcal{P}_G(H_L) \) is equivalent to each of the inclusions

\[
N_{K/k}J_K \subseteq N_{L/k}J_L \quad \text{and} \quad N(K/k) \subseteq N(L/k).
\]

We thus obtain a necessary group theoretic condition for the equality of norm groups,

\[
N_{K/k}K^* = N_{L/k}L^* \quad \text{imply} \quad \mathcal{P}_G(H_K) = \mathcal{P}_G(H_L).
\]

We wish to determine sets of extensions with the same norm group that are not pairwise conjugate over the base field. The necessary condition (2) leads us to make the following definitions.

**Definition 1.** Let \( G \) be a finite group. A sequence of subgroups \( \{H_i\}_{i=1}^m \) of \( G \) is called a full system of subgroups if for any \( 1 \leq i, j \leq m \) the following conditions are satisfied:

(a) \( H_i \) and \( H_j \) are not conjugate in \( G \) for \( i \neq j \);
(b) \( \mathcal{P}_G(H_i) = \mathcal{P}_G(H_j) \);
(c) for any subgroup \( H \) of \( G \), if \( \mathcal{P}_G(H) = \mathcal{P}_G(H_s) \) for some \( 1 \leq s \leq m \), then \( H \) is conjugate to \( H_i \) in \( G \) for some \( 1 \leq t \leq m \).

We will write \( \mathcal{E}(H_1, \ldots, H_m) \), if \( H_1, \ldots, H_m \) is a full system of subgroups. The length of a full system of subgroups \( \mathcal{E}(H_1, \ldots, H_m) \) is the number \( m \) of subgroups in the sequence.

Two full systems of subgroups \( \mathcal{E}(H_1, \ldots, H_n) \) and \( \mathcal{E}(N_1, \ldots, N_m) \) of a finite group \( G \) are equal, if they are of the same length, and the subgroups in the systems can be reordered, if necessary, in such a way that \( H_i \) and \( N_i \) are conjugate in \( G \) for all \( 1 \leq i \leq m \).

**Definition 2.** Let \( G \) be a finite group. We define \( \mathcal{S}(G) \) to be the set of all distinct nontrivial full systems of subgroups of \( G \), i.e. the set of all distinct full systems of length greater than or equal to two.
The symmetric group $S_2$ has only two conjugacy classes of subgroups, and $\mathcal{S}(S_2) = \emptyset$. There are four conjugacy classes of subgroups of $S_3$ with representatives: the two trivial subgroups, and Sylow 2 and 3-subgroups of $S_3$. It follows that $\mathcal{S}(S_3) = \emptyset$. By (2) we therefore obtain the following theorem.

**Theorem 3.** Let $E/k$ be a finite Galois extension of algebraic number fields with the Galois group $G$. Let $k \subseteq K, L \subseteq E$ be subfields of $E$. If $G$ is isomorphic to $S_2$ or $S_3$, then $N_{K/k}K^* = N_{L/k}L^*$ if and only if $K$ and $L$ are conjugate over $k$.

The symmetric group $S_4$ has 11 conjugacy classes of subgroups, and $\mathcal{S}(S_4) = \{ \Xi(\mathbb{Z}/2\mathbb{Z}, V_4) \}$, where $V_4$ is the Klein 4-group, and $\mathbb{Z}/2\mathbb{Z}$ is an arbitrary subgroup of $V_4$ of order two. If $E/k$ is a Galois extension with the Galois group isomorphic to $S_4$, and $k \subseteq K \subseteq L \subseteq E$ are the fixed fields of $V_4 \subseteq \mathbb{Z}/2\mathbb{Z}$, then by (1) the equality $N(K/k) = N(L/k)$ holds. We will show that the Hasse Norm Principle (HNP) holds for $K/k$, i.e. $N(K/k) = N_{K/k}K^*$.

In general, for any finite extension $X/Y$ of algebraic number fields, the factor group of $N(X/Y)$ by $N_{X/Y}X^*$ is finite, and it is called the total obstruction to HNP for $X/Y$. The order of this factor group is denoted by $i(X/Y)$. If $i(X/Y) = 1$, then we say that HNP holds for $X/Y$. It is well known that HNP holds for cyclic finite Galois extensions. Also, HNP holds for any extension of prime degree [1, Lemma 4][8, Proposition 10.11].

To prove the above equality $N(K/k) = N_{K/k}K^*$, we note that $K$ is the compositum of a quadratic extension of $k$ (the fixed field of $A_4$) with a cubic extension of $k$ (the fixed field of a Sylow 2-subgroup of $S_4$). By Proposition 2 [5, p. 315] HNP holds for $K/k$. So the equality $N_{K/k}K^* = N_{L/k}L^*$ holds if and only if HNP holds for $L/k$. We will determine in this article when HNP holds for $L/k$.

Let $L/k$ and $T/k$ be finite extensions of algebraic number fields. In [12] we defined the first obstruction to HNP for $L/k$ corresponding to $T/k$ as the factor group of $k^* \cap N_{L/k}J_L N_{T/k}J_T$ by $N(T/k)N_{L/k}L^*$. We note that if $T$ is a finite Galois extension of $k$ containing $L$, then the first obstruction to HNP for $L/k$ corresponding to $T/k$ is equal to $k^* \cap N_{L/k}J_L N(T/k)N_{L/k}L^*$. This factor group, called the first obstruction to HNP for $L/k$ corresponding to the tower $k \subseteq L \subseteq T$, was introduced and investigated in [4]. Let $E/k$ be a finite Galois extension containing $L$ and $T$, and suppose that $G = G(E/k)$, $H = G(E/L)$, and $N = G(E/T)$. For each prime $v$ of $k$ we fix a $k$-embedding of $E$ into the algebraic closure $\bar{k}_v$ of the completion $k_v$ of $v$ at $k_v$. This will also fix a decomposition group $G_v = \mathrm{res}_{E/E}([G(E_v/k_v)]$ of $v$ in $E$. There is a one-to-one correspondence between the primes $\omega$ of $L$ above $v$ and the distinct double cosets $Hx_0G_v$ of $H$ and $G_v$ in $G$. Furthermore, $H_{\omega} = H \cap x_0 G_v x_0^{-1}$ is a decomposition group of $\omega$ in $E$. Similarly, there is a one-to-one correspondence between the primes $v$ of $T$ above $v$ and the distinct double cosets $Ny_vG_v$ of $N$ and $G_v$ in $G$, and $N_v = N \cap y_v G_v y_v^{-1}$ is a decomposition group of $v$ in $E$. Let $v$ be an arbitrary prime of $k$. Suppose that $G = \bigcup_{\omega \mid \omega} Hx_0 G_v = \bigcup_{v \mid v} Ny_v G_v$ are decompositions of $G$ into the unions of distinct double cosets of $H$, $G_v$ and $N$, $G_v$ in $G$, respectively. From now on in this article, unless stated otherwise, we will denote by $X'$ the commutator subgroup...
For each prime $v$ of $k$ we define a group homomorphism $\lambda_v : \prod_{\omega | v} H_{\omega} / H_{\omega'} \to H / H'$ by the rule

$$\lambda_v([h_\omega H_{\omega'})_{\omega | v}] = \left( \prod_{\omega | v} h_\omega \right) H',$$

and a group homomorphism $\psi_v : \prod_{\omega | v} H_{\omega} / H_{\omega'} \to G_v / \prod_{v | \nu} (N_v^g G_v')$ by the rule

$$\psi_v([h_\omega H_{\omega'})_{\omega | v}] = \left( \prod_{\omega | v} x_\omega^{-1} h_\omega x_\omega \right) \prod_{v | \nu} (N_v^g G_v'),$$

where $N_v^g = y_v^{-1} N_v y_v$. It follows that the diagram

$$\begin{array}{ccc}
\prod_{\omega | v} H_{\omega} / H_{\omega'} & \xrightarrow{\lambda_v} & H / H' \\
\downarrow \psi_v & & \downarrow \pi \\
G_v / \prod_{v | \nu} (N_v^g G_v') & \xrightarrow{\pi_v} & G / N G',
\end{array}$$

is commutative for each prime $v$ of $k$, where $\pi$ and $\pi_v$ are canonical homomorphisms. This commutative diagram can be extended to a commutative diagram in a natural way

$$\begin{array}{ccc}
\prod_v \left( \prod_{\omega | v} H_{\omega} / H_{\omega'} \right) & \xrightarrow{\prod \lambda_v} & H / H' \\
\downarrow \prod \psi_v & & \downarrow \pi \\
\prod_v G_v / \prod_{v | \nu} (N_v^g G_v') & \xrightarrow{\prod \pi_v} & G / N G'.
\end{array}$$

By Theorem 1.7 of [12] the first obstruction to HNP for $L/k$ corresponding to the extension $T/k$ is isomorphic to $\ker \pi / (\prod \lambda_v)[\ker \prod \psi_v]$. We note that $\ker \pi = (H \cap NG') / H'$, and $(\prod \lambda_v)[\ker \prod \psi_v]$ is a subgroup of this factor group generated by subgroups $\lambda_v[\ker \psi_v]$, where $v$ ranges over all primes of $k$. In order to describe the group $(\prod \lambda_v)[\ker \prod \psi_v]$ we will use a subgroup of $G$ that was introduced in [4] to investigate first obstructions to HNP corresponding to towers of field extensions.

$$\Phi^G(H) = \langle \{ [h,g] / h \in H \cap g H g^{-1}, g \in G \} \rangle,$$

where $\langle X \rangle$ denotes the subgroup of $G$ generated by a subset $X$ of $G$, and $[h,g] = h^{-1} g^{-1} h g$. The group $\Phi^G(H)$ contains $H'$, and is a subgroup of $H \cap G'$. Finally, let $S$ be the (finite) set of primes of $k$ whose decomposition groups in $E$ are not cyclic. We
define a subgroup $H' \subseteq X_{L/k}(T, E) \subseteq H \cap NG'$ by
\[ X_{L/k}(T, E)/H' = \prod_{\psi \in S} \lambda_{\psi}[\text{Ker } \psi]. \] (4)

By [12] \((\prod \lambda_{\psi})[\text{Ker } \prod \psi_{\alpha}]\) coincides with the factor group of \(\Phi^G(H) \cdot (H \cap NG(N)) X_{L/k}(T, E)\) by \(H'\). It follows that
\[ \frac{k^* \cap N_{L/k} J_{L/k} J_{k^*/T}}{N_{T/k} N_{L/k} L^*} \cong \Phi^G(H) \cdot (H \cap NG(N)) X_{L/k}(T, E)\] (5)

[12, Theorem 1.11]. We wish now to establish a group theoretic property of \(X_{L/k}(T, E)\).

Let \(H\) and \(N\) be subgroups of a finite group \(G\). For any subgroup \(X\) of \(G\) we define a subgroup of \(H - NG_0\) as follows. Suppose that \(G = \bigcup_{i=1}^n H x_i X = \bigcup_{j=1}^m N y_j X\) are decompositions of \(G\) into the unions of distinct double cosets of \(H, X\) and \(N, X\), respectively. We define \(H_i = H \cap x_i x_i X^{-1}\) for all \(1 \leq i \leq n\), and \(N_j = N \cap y_j y_j X^{-1}\) for all \(1 \leq j \leq m\). The following mapping \(\psi_X : \prod_{i=1}^n H_i / H_i' \to X / \prod_{j=1}^m (N_j y_j X')\) given by
\[ \psi_X(h_1 H_1', \ldots, h_n H_n') = \left(\prod_{i=1}^n x_i^{-1} h_i x_i\right) \prod_{j=1}^m (N_j y_j X') \]
is a group homomorphism. We have a commutative diagram of group homomorphisms similar to diagram (3)
\[ \prod_{i=1}^n H_i / H_i' \xrightarrow{\lambda_X} H / H' \]
\[ \downarrow \psi_X \quad \downarrow \pi \] (6)
\[ X / \prod_{j=1}^m (N_j y_j X') \xrightarrow{\pi_X} G / NG', \]
where \(\lambda_X\) is given by \(\lambda_X(h_1 H_1', \ldots, h_n H_n') = (\prod_{i=1}^n h_i) H',\) and \(\pi, \pi_X\) are canonical homomorphisms. It follows that \(\lambda_X[\text{Ker } \psi_X] \subseteq \text{Ker } \pi = H \cap NG'/H'.\) We will show that \(\lambda_X[\text{Ker } \psi_X]\) does not depend on the choice of representatives \(\{x_i\}\) and \(\{y_j\}\) of double cosets \(H, X\) and \(N, X\) in \(G\), respectively.

**Lemma 4.** Let
be a commutative diagram of group homomorphisms, i.e. \( g \alpha = \tilde{\alpha} f \) and \( \tilde{\gamma} f = \gamma \). Then \( \gamma | \text{Ker} \alpha \subseteq \tilde{\gamma} | \text{Ker} \tilde{\alpha} \).

The proof of the lemma is a straightforward verification of the inclusion.

**Proposition 5.** In the notation of diagram (6) the group \( \lambda_X | \text{Ker} \psi_X \) is independent of the choice of representatives of double cosets \( H, X \) and \( N, X \) in \( G \). Moreover, for any \( g \in G \) the equality \( \lambda_X | \text{Ker} \psi_X = \lambda_X | \text{Ker} \psi_X \) holds.

**Proof.** Suppose that \( G = \bigcup_{i=1}^{n} H_iX = \bigcup_{i=1}^{n} H \alpha_iX \) and \( G = \bigcup_{j=1}^{m} N_jX = \bigcup_{j=1}^{m} N \beta_jX \) are decompositions of \( G \) into the unions of distinct double cosets. Let \( a_i = h_iXz_i \) \((1 \leq i \leq n)\) and \( b_j = n_jX\beta_j \) \((1 \leq j \leq m)\) for some \( h_i \in H \), \( n_j \in N \), and \( z_i, \beta_j \in X \).

We define \( H_i, N_j \) as above, and \( \tilde{H}_i = H \cap a_iX \alpha_i^{-1}, \tilde{N}_j = N \cap b_jX \beta_j^{-1} \). Then

\[
\tilde{H}_i = H \cap X^{a_i^{-1}} = H \cap X^{a_iXz_i^{-1}} = H \cap X^{X^{b_j^{-1}}X^{-1}} = H \cap X^{b_j^{-1}}X^{-1} = (H \cap X^{b_j^{-1}})^{X^{-1}} = H_i^{b_j^{-1}}.
\]

Similarly, \( \tilde{N}_j = n_jX \eta_j^{-1} \) \((1 \leq j \leq m)\). We define

\[
\varphi : \prod_{i=1}^{n} H_i/H_i' \rightarrow \prod_{i=1}^{n} \tilde{H}_i/\tilde{H}_i'
\]

by the rule \( \varphi[(z_iH_i')] = (h_iXz_iX^{-1}H_i') \). Since \( \tilde{H}_i = h_iX \alpha_i^{-1}X^{-1}H_i' \) \((1 \leq i \leq n)\), it is easy to show that \( \varphi \) is a well-defined group homomorphism. The equalities \( \tilde{N}_j = n_jX \eta_j^{-1} \) \((1 \leq j \leq m)\) imply that

\[
\tilde{N}_j^b \tilde{X}^b = \tilde{N}_j^{n_j^{-1}b_j} \tilde{X}^b = \tilde{N}_j^{n_j^{-1}b_j} \tilde{X}^b = \tilde{N}_j X^b
\]

(since \( \beta_j \in X \)) for each \( 1 \leq j \leq m \). Let \( Y = \prod_{j=1}^{m} (N_jX^b) = \prod_{j=1}^{m} (N_jX^b) \).

\[
\begin{array}{cccc}
\Pi_n^{n_i} H_i/H_i' & \overset{\varphi}{\longrightarrow} & \Pi_n^{n_i} \tilde{H}_i/\tilde{H}_i' & \overset{\lambda_X}{\longrightarrow} \\
\Pi_n^{n_i} H_i/H_i' & \overset{\tilde{\gamma}_X}{\longrightarrow} & \Pi_n^{n_i} H_i/H_i' & \overset{\psi_X}{\longrightarrow} \\
\text{X/Y} & \overset{\pi_X}{\longrightarrow} & \text{G/NG'} & \overset{\pi}{\longrightarrow}
\end{array}
\]

where \( \tilde{\lambda}_X \) and \( \tilde{\psi}_X \) are defined similarly to \( \lambda_X \) and \( \psi_X \), respectively. It is easy to see that \( \tilde{\lambda}_X \varphi = \lambda_X \). To prove \( \tilde{\psi}_X \varphi = \psi_X \) we choose an arbitrary element
\((z_iH_i') = \prod_{i=1}^{n} H_i/H_i'\). Then
\[
\tilde{\psi}_X \varphi([z_iH_i']) = \tilde{\psi}_X [(z_i^{h_{i'}} H_i')] = \left( \prod_{i=1}^{n} z_i^{h_{i'a_i}} \right) Y.
\]

Since \(a_i = h_i x_i a_i (1 \leq i \leq n)\) and \(X' \subseteq Y\), it follows that
\[
z_i^{h_{i'a_i}} Y = z_i^{x_{a_i}} Y = (z_i^{x_i})^a Y = z_i^X Y.
\]

So \(\tilde{\psi}_X \varphi([z_iH_i']) = (\prod_{i=1}^{n} z_i^{x_{a_i}}) Y = \psi_X ([z_iH_i'])\). By Lemma 4 \(\lambda_X [\text{Ker} \psi_X] \subseteq \tilde{\lambda}_X [\text{Ker} \tilde{\psi}_X]\). By symmetry the opposite inclusion holds. So \(\lambda_X [\text{Ker} \psi_X] = \tilde{\lambda}_X [\text{Ker} \tilde{\psi}_X]\).

We will now prove that the equality \(G \cap x_i X x_i^{-1} = H \cap x_i g X^g (x_i g)^{-1}\) holds for any \(g \in G\). Since \(G = \bigcup_{i=1}^{m} H x_i X\) is the decomposition of \(G\) into the union of distinct double cosets of \(H, X\) in \(G\), it follows that \(G = \bigcup_{j=1}^{m} H x_j g X^g\) is the decomposition of \(G\) into the union of distinct double cosets of \(H, X^g\) in \(G\). For each \(1 \leq i \leq n\)
\[
H_i = H \cap x_i X x_i^{-1} = H \cap x_i g X^g (x_i g)^{-1}.
\]

Similarly, \(G = \bigcup_{j=1}^{m} N y_j X = \bigcup_{j=1}^{m} N y_j g X^g\). For each \(1 \leq j \leq m\)
\[
N \cap y_j g X^g (y_j g)^{-1} = N \cap y_j X y_j^{-1} = N_j.
\]

We define \(\chi : X/\prod_{j=1}^{m} (N_j^{y_j} X^g) \to X^g/\prod_{j=1}^{m} (N_j^{y_j} (X^g)^g)\) in a natural way by conjugation by \(g\).

\[
\begin{array}{c}
\Pi_{i=1}^{n} H_i/H_i' \\
\Pi_{i=1}^{n} H_i/H_i'
\end{array} \xrightarrow{\psi_X} \begin{array}{c}
H/H' \\
H/H'
\end{array} \xrightarrow{\lambda_X} \begin{array}{c}
\Pi_{i=1}^{n} H_i/H_i' \\
\Pi_{i=1}^{n} H_i/H_i'
\end{array} \xrightarrow{\psi_X} \begin{array}{c}
X/\prod_{j=1}^{m} (N_j^{y_j} X^g) \\
X/\prod_{j=1}^{m} (N_j^{y_j} X^g)
\end{array} \xrightarrow{\pi_{Xg}} \begin{array}{c}
G/NG^g \\
G/NG^g
\end{array}
\]

It is easy to verify that \(\lambda_X = \lambda_X^g\) and \(\chi \psi_X = \psi_X^g\). So by Lemma 4 \(\lambda_X [\text{Ker} \psi_X] \subseteq \lambda_X^g [\text{Ker} \psi_X^g]\). By symmetry the opposite inclusion holds. So \(\lambda_X [\text{Ker} \psi_X] = \lambda_X^g [\text{Ker} \psi_X^g]\). □

By Proposition 5 in the notation of diagram (3) \(\lambda_X [\text{Ker} \psi_X]\) is determined by a decomposition group \(G_v\) of a prime \(v\) of \(k\) in \(E\), and it is independent of the choice of a decomposition group of \(v\) in \(E\). The following proposition shows that \(X_{L/k}(T, E)\) can be determined in certain cases by fewer decomposition groups \(G_v\) than it was stated in definition (4).
Proposition 6. Let $H$ and $N$ be subgroups of a finite group $G$. Then for any subgroups $X \subseteq Y$ of $G$ in the notation of diagram (6) the inclusion $\lambda_X[\ker \psi] \subseteq \lambda_Y[\ker \psi]$ holds.

Proof. Let $G = \bigcup_{i=1}^n Ha_iY = \bigcup_{j=1}^m N\alpha_jY$ be decompositions of $G$, respectively, into the unions of distinct double cosets of $H$, $Y$ and $N$, $Y$ in $G$. Since $X$ is a subgroup of $Y$, it follows that $Ha_iY = \bigcup_{r=1}^n Hb_{ir}X$ ($1 \leq i \leq n$) and $N\alpha_jY = \bigcup_{r=1}^m N\beta_{jr}X$ ($1 \leq j \leq m$) are the unions of distinct double cosets of $H$, $X$ and $N$, $X$, respectively. It follows that $\bigcup_{r=1}^n(\bigcup_{i=1}^n Hb_{ir}X) = \bigcup_{r=1}^m(\bigcup_{j=1}^m N\beta_{jr}X)$ are decompositions of $G$, respectively, into the unions of distinct double cosets of $H$, $X$ and $N$, $X$ in $G$. Let

$$H_i = H \cap a_iYa_i^{-1} \quad \text{and} \quad H_{ir} = H \cap b_{ir}Xb_{ir}^{-1} \quad (1 \leq i \leq n, \; 1 \leq r \leq s_i),$$

and

$$N_j = N \cap \alpha_jYa_j^{-1} \quad \text{and} \quad N_{jr} = N \cap \beta_{jr}X\beta_{jr}^{-1} \quad (1 \leq j \leq m, \; 1 \leq r \leq t_j).$$

Since $b_{ir} \in Ha_iY$, it follows that there are $h_{ir} \in H$ and $y_{ir} \in Y$ such that

$$b_{ir} = h_{ir}a_{iy_{ir}}$$

for all $1 \leq i \leq n, 1 \leq r \leq s_i$. Then for any $1 \leq i \leq n, 1 \leq r \leq s_i$

$$H_{ir}^{h_{ir}} = (H \cap X^{a_i^{-1}})_{h_{ir}} = H \cap X^{a_i^{-1}h_{ir}} = H \cap X^{a_i^{-1}a_{ir}^{-1}} \subseteq H \cap Y^{a_i^{-1}} = H_i.$$  \hspace{1cm} (8)

Furthermore, for any $1 \leq j \leq m, 1 \leq r \leq t_j$, $\beta_{jr} \in N\alpha_jY$. Suppose that $\beta_{jr} = u_{jr}x_{jr}v_{jr}$ for some $u_{jr} \in N$ and $v_{jr} \in Y$ ($1 \leq j \leq m, \; 1 \leq r \leq t_j$). Then

$$N_{jr}^{\beta_{jr}}X' = (N \cap X^{\beta_{jr}})_{\beta_{jr}}X' = (N^{\beta_{jr}} \cap X)X' = (N^{\beta_{jr}} \cap Y^{\beta_{jr}})Y' \subseteq (N^{\alpha_j} \cap Y^{\alpha_j})Y' \subseteq (N^{\alpha_j} \cap Y^{\alpha_j})Y' \subseteq N_{jr}^{\alpha_j}Y'.$$

By (8) we can define a homomorphism

$$\varphi_i : \prod_{r=1}^{s_i} H_{ir}/H_{ir}' \to H_{i}/H_{i}'$$

by the rule $\varphi_i[(x_{ir}H_{ir}')_{1 \leq r \leq s_i}] = (\prod_{r=1}^{s_i} h_{ir}^{-1}x_{ir}h_{ir})H_{i}'$ for each $1 \leq i \leq n$. By (9) we have a canonical homomorphism

$$\chi : X/\prod_{j=1}^m (N_{jr}^{\beta_{jr}}X') \to Y/\prod_{j=1}^m (N_{jr}^{\alpha_j}Y').$$
The above-defined homomorphisms yield a commutative diagram
\[
\begin{array}{c}
\xymatrix{X/\prod_{j=1}^{m}(\Pi_{r=1}^{i}N_{jr}X') \ar[r]^\psi_{X} & \prod_{i=1}^{n}(\Pi_{r=1}^{i}H_i/H_i') \ar[dl]_{\lambda_X} \\
Y/\prod_{j=1}^{m}(N_{j}X') \ar[r]_{\psi_{Y}} & \prod_{i=1}^{n}H_i/H_i' \ar[ul]_{\lambda_Y} } 
\end{array}
\]
(10)
where \(\psi_{X}, \psi_{Y}\) and \(\lambda_X, \lambda_Y\) are defined similarly to \(\psi_{X}\) and \(\lambda_X\), respectively, in diagram (6).

To prove that diagram (10) is commutative we will first prove the equality
\[
\chi \psi_{X} = \psi_{Y}(\prod_{r} \varphi_{r}).
\]
Let \(x_{ir} \in H_i\) \((1 \leq i \leq n, 1 \leq r \leq s_i)\) be arbitrary elements. By (8) \(h_{ir}^{-1}x_{ir}h_{ir} \in H_i\), and therefore \(a_{ir}^{-1}h_{ir}^{-1}x_{ir}h_{ir}a_{i} \in Y\). In (7) we defined \(y_{ir} \in Y\) \((1 \leq i \leq n, 1 \leq r \leq s_i)\). Now using the fact that the commutator \([a_{ir}^{-1}h_{ir}^{-1}x_{ir}h_{ir}a_{i}, y_{ir}]\) is an element of \(Y'\) we obtain
\[
b_{ir}^{-1}x_{ir}b_{ir}' = a_{ir}^{-1}h_{ir}^{-1}x_{ir}h_{ir}a_{i}Y'
\]
for any \(1 \leq i \leq n, 1 \leq r \leq s_i\). It follows now by (11) that
\[
\chi \psi_{X}([((x_{i1}H_{i1}', \ldots, x_{is}H_{is}')_{1 \leq i \leq n}])
\]
\[
= \chi \left( \prod_{1 \leq i \leq n, 1 \leq r \leq s_i} b_{ir}^{-1}x_{ir}b_{ir} \right) \prod_{1 \leq j \leq m, 1 \leq r \leq t_j} (N_{jr}^{\beta_{jr}}X')
\]
\[
= \left( \prod_{1 \leq i \leq n, 1 \leq r \leq s_i} b_{ir}^{-1}x_{ir}b_{ir} \right) \prod_{j=1}^{m} (N_{jr}^{\beta_{jr}}X')
\]
\[
= \left( \prod_{1 \leq i \leq n, 1 \leq r \leq s_i} a_{ir}^{-1}h_{ir}^{-1}x_{ir}h_{ir}a_{i} \right) \prod_{j=1}^{m} (N_{jr}^{\beta_{jr}}X').
\]
(12)
On the other hand
\[
\psi_{Y}(\prod_{r} \varphi_{r})[(((x_{i1}H_{i1}', \ldots, x_{is}H_{is}')_{1 \leq i \leq n}])
\]
\[
= \psi_{Y} \left( \prod_{r=1}^{s_1} h_{ir}^{-1}x_{ir}h_{ir}H_{i1}', \ldots, \prod_{r=1}^{s_n} h_{ir}^{-1}x_{ir}h_{ir}H_{in}' \right)
\]
\[
= \left( \prod_{1 \leq i \leq n, 1 \leq r \leq s_i} a_{ir}^{-1}h_{ir}^{-1}x_{ir}h_{ir}a_{i} \right) \prod_{j=1}^{m} (N_{jr}^{\beta_{jr}}Y').
\]
(13)
By (12) and (13) we obtain the desired equality \( \chi \psi_X = \psi_Y (\prod \varphi_i) \). To complete the proof that diagram (10) is commutative it remains to show that the equality \( \lambda_Y (\prod \varphi_i) = \lambda_X \) holds. Let \( x_{ir} \in H_{ir} \) \( (1 \leq i \leq n, 1 \leq r \leq s_i) \) be arbitrary elements. Since \( x_{ir} \in H_{ir} \subseteq H \), it follows that \( h_{ir}^{-1} x_{ir} h_{ir} H' = x_{ir} H' \). Then

\[
\lambda_Y (\prod \varphi_i) \left[ \left( x_{i1} H_{i1}' , \ldots , x_{is_i} H_{is_i}' \right) \right]_{1 \leq i \leq n} \\
= \lambda_Y \left[ \left( \prod_{r=1}^{s_i} h_{ir}^{-1} x_{ir} h_{ir} H' \right) \right]_{1 \leq i \leq n} \\
= \left( \prod_{1 \leq i \leq n} h_{ir}^{-1} x_{ir} h_{ir} \right) H' \\
= \left( \prod_{1 \leq i \leq n} x_{ir} \right) H' = \lambda_X \left[ \left( x_{i1} H_{i1}' , \ldots , x_{is_i} H_{is_i}' \right) \right]_{1 \leq i \leq n}.
\]

Since diagram (10) is commutative, it follows by Lemma 4 that \( \lambda_X [\text{Ker } \psi_X] \subseteq \lambda_Y [\text{Ker } \psi_Y] \). \( \Box \)

We wish now to generalize Proposition 6.

**Proposition 7.** Let \( G \) be a subgroup of a finite group \( \tilde{G} \), and let \( H, N \) be a subgroups of \( G \). In the notation of diagram (6) for any subgroup \( Y \) of \( \tilde{G} \) we obtain two subgroups of \( H/H' : \lambda_Y [\text{Ker } \psi_Y] \) is defined by \( \tilde{G}, H, N, \) and \( Y; \lambda_X [\text{Ker } \psi_X] \) is defined by \( G, H, N, \) and \( X = G \cap Y \). Then \( \lambda_X [\text{Ker } \psi_X] \subseteq \lambda_Y [\text{Ker } \psi_Y] \).

**Proof.** Suppose that \( \tilde{G} = \bigcup_{i=1}^{m} D_i(H) \) and \( \tilde{G} = \bigcup_{j=1}^{s} D_j(N) \) be decompositions of \( \tilde{G} \) into the unions of distinct double cosets of \( H, Y \) and \( N, Y \), respectively. Let \( \{ D_i(H) \}_{1 \leq i \leq m} \) and \( \{ D_j(N) \}_{1 \leq j \leq s} \) be all double cosets for which \( D_i(H) \cap G \neq \emptyset \) and \( D_j(N) \cap G \neq \emptyset \). Suppose that \( D_i(H) = H x_i Y \) for \( 1 \leq i \leq n \) and \( D_j(N) = N y_j Y \) for \( 1 \leq j \leq r \), and \( x_i, y_j \in G \) for \( 1 \leq i \leq m \) and \( 1 \leq j \leq s \). It follows that \( G = \bigcup_{i=1}^{m} H x_i X = \bigcup_{j=1}^{s} N y_j X \) are decompositions of \( G \) into the unions of distinct double cosets of \( H, X \) and \( N, X \) in \( G \), respectively. We define

\[
\tilde{H}_i = H \cap x_i Y x_i^{-1} \quad (1 \leq i \leq n) \quad \text{and} \quad H_i = H \cap x_i X x_i^{-1} \quad (1 \leq i \leq m),
\]

\[
\tilde{N}_j = N \cap y_j Y y_j^{-1} \quad (1 \leq j \leq r) \quad \text{and} \quad N_j = N \cap y_j X y_j^{-1} \quad (1 \leq j \leq s)
\]
Diagram (6) yields the following diagram of group homomorphisms.

\[
\begin{array}{cccc}
\Pi_{i=1}^{n} H_i/H'_i & \xrightarrow{\lambda_X} & H/H' \\
\Pi_{i=1}^{n} \tilde{H}_i/\tilde{H}'_i & \xrightarrow{\lambda_Y} & \tilde{H}/\tilde{H}' \\
\psi_Y & & & \pi \\
X/\Pi_{j=1}^{r} (N_j' Y') & \xrightarrow{\pi_X} & G/NG', \\
Y/\Pi_{j=1}^{r} (N_j' Y') & \xrightarrow{\pi_Y} & \tilde{G}/NG',
\end{array}
\]

where \(\phi, \eta, \chi\) are the canonical homomorphisms. The remaining homomorphisms in the above diagram are defined similarly to the corresponding homomorphisms in diagram (6). It is easy to show that the equalities \(\lambda_X = \lambda_Y \phi\) and \(\psi_Y \phi = \eta \psi_X\) hold. It follows by Lemma 4 that \(\lambda_X[Ker \psi_X] \subseteq \lambda_Y[Ker \psi_Y].\)

By Propositions 6 and 7 we immediately obtain the following theorem.

**Theorem 8.** Let \(G\) be a subgroup of a finite group \(\tilde{G}\), and let \(H, N\) be subgroups of \(G\). In the notation of diagram (6) for any subgroup \(Y\) of \(G\) and for any subgroup \(X\) of \(G\) that is contained in \(Y\) we obtain two subgroups of \(H/H'\): \(\lambda_Y[Ker \psi_Y]\) is defined by \(\tilde{G}, H, N,\) and \(Y\); \(\lambda_X[Ker \psi_X]\) is defined by \(G, H, N,\) and \(X\). Then \(\lambda_X[Ker \psi_X] \subseteq \lambda_Y[Ker \psi_Y]\).

**Definition 9.** Let \(\mathcal{A}\) be a set of subgroups of a finite group \(G\). We define \(M(\mathcal{A})\) to be a subset of \(\mathcal{A}\) such that

(a) for any \(X \in \mathcal{A}\) there are \(Y \in M(\mathcal{A})\) and \(g \in G\) such that \(X^g \subseteq Y\);

(b) for any \(X, Y \in M(\mathcal{A})\) and \(g \in G\), \(X^g \neq Y\).

By Theorem 8 we obtain the following corollary.

**Corollary 10.** Let \(H\) and \(N\) be subgroups of a finite group \(G\). Let \(\mathcal{A}\) be a set of subgroups of \(G\). Then in the notation of diagram (6) we have equality of subgroups of \(H \cap NG'/H'\)

\[
\prod_{X \in \mathcal{A}} \lambda_X[Ker \psi_X] = \prod_{X \in M(\mathcal{A})} \lambda_X[Ker \psi_X].
\]

The set \(\mathcal{S}(S_4)\) of distinct nontrivial full systems of subgroups of \(S_4\) is \(\{\mathcal{E}(\mathbb{Z}/2\mathbb{Z}, V_4)\}\), where \(\mathbb{Z}/2\mathbb{Z} = \langle (1,2)(3,4) \rangle\) and \(V_4 = \langle (1,2)(3,4), (1,3)(4,2) \rangle\) is the Klein 4-group.
Lemma 11. Let \( E/k \) be a Galois extension with the Galois group \( G = G(E/k) \) isomorphic to \( S_4 \). Let \( k \subset K \subset L \subset E \) be the fixed fields of \( V_4 \supseteq \mathbb{Z}/2\mathbb{Z} \). If there is a prime \( v \) of \( k \) whose decomposition group in \( E \) contains the Sylow 2-subgroup of \( A_4 \), then \( N_{k/k}K^* = N_{L/k}L^* \).

**Proof.** Let \( v \) be a prime of \( k \) whose decomposition group \( G_v \) in \( E \) contains the Sylow 2-subgroup \( V_4 \) of \( A_4 \). Let \( F \) be the fixed field of \( A_4 \). Then there is a prime \( \omega \) of \( F \) above \( v \) whose decomposition group \( A_4 \supset G_v \) in \( E \) contains \( V_4 \). By Proposition 1.1 [10, p. 111] \( N_{K/F}K^* = N_{L/F}L^* \). It follows that
\[
N_{k/k}K^* = N_{F/k}(N_{K/F}K^*) = N_{F/k}(N_{L/F}L^*) = N_{L/k}L^*. \]

The set of distinct nontrivial full systems of subgroups of \( S_5 \) is \( \mathcal{S}(S_5) = \{ \Xi(H_1, H_2), \Xi(N_1, N_2), \Xi(R_1, R_2) \} \), where
\[
H_1 = \langle (1, 2, 3)(4, 5) \rangle \cong \mathbb{Z}/6\mathbb{Z} \quad \text{and} \quad H_2 = \langle (3, 4, 5), (4, 5) \rangle \cong S_3
\]
\[
N_1 = \langle (2, 3)(4, 5) \rangle \cong \mathbb{Z}/2\mathbb{Z} \quad \text{and} \quad N_2 = \langle (2, 3)(4, 5), (2, 4)(3, 5) \rangle \cong V_4
\]
\[
R_1 = \langle (1, 2)(4, 5), (3, 4, 5) \rangle \cong S_3 \quad \text{and} \quad R_2 = \langle (2, 3)(4, 5), (2, 4)(3, 5), (3, 4, 5) \rangle \cong A_4.
\]

![Fig. 1](image-url)

Fig. 1.
Let $E/k$ be a Galois extension with the Galois group isomorphic to $S_5$. Suppose that $K_i, L_i$ and $M_i$ ($i = 1, 2$) are the fixed fields of $H_i, N_i$ and $R_i$, respectively. The compositum $K_1K_2$ is fixed by $H_1 \cap H_2 = \langle (4,5) \rangle$. We identify $S_4$ with the symmetric group on the set $\{2, 3, 4, 5\}$, and $A_4$ with $R_2$. Let $F, T$ be the fixed fields of $A_5$ and $S_4$, respectively. Field extensions of $k$ contained in $E$ are shown above in Fig. 1.

The proof of the following lemma is similar to the proof of Lemma 11.

**Lemma 12.** In the notation of Fig. 1 if there is a prime $v$ of $k$ whose decomposition group in $E$ contains a Sylow 2-subgroup of $A_5$, then $N_{L_1/k}L_1^* = N_{L_2/k}L_2^*$ and $N_{M_1/k}M_1^* = N_{M_2/k}M_2^*$.

**Proof.** We first note that $N_2$ is a Sylow 2-subgroup of $A_5$. Let $v$ be a prime of $k$ whose decomposition group $G_v$ in $E$ contains a Sylow 2-subgroup of $A_5$, say $N_2^g$ for some $g \in A_5$. There is a prime of $F$ and there is a prime of $T$ above $v$ whose decomposition groups in $E$ are $A_5 \cap G_v$ and $S_4 \cap gG_gg^{-1}$, respectively. The first decomposition group contains the Sylow 2-subgroup $N_2^g$ of $A_5$. By Proposition 2.4 of [12, p. 258] $N_{M_1/F}M_1^* = N_{M_2/F}M_2^*$. It follows as in the proof of Lemma 11 that $N_{M_1/k}M_1^* = N_{M_2/k}M_2^*$. The second decomposition group contains the Sylow 2-subgroup $N_2$ of $A_4$. By Lemma 11 $N_{L_1/T}L_1^* = N_{L_2/T}L_2^*$. So $N_{L_1/k}L_1^* = N_{L_2/k}L_2^*$.

To prove the next proposition we will use a theorem that was proved in [4]. We will include the statement of the theorem here for the convenience of the reader.

**Theorem 13.** Let $k \subseteq T \subseteq F$ be a tower of finite extensions of an algebraic number field $k$ with $F$ Galois over $k$. Let $G = G(F/k)$ and $H = G(F/T)$. If $G$ contains subgroups $G_1, \ldots, G_n$, and subgroups $H_s \subseteq G_s \cap H(s = 1, \ldots, n)$ such that

$$\prod_{s=1}^{n} \text{Cot}_{G}^{G_s} : \prod_{s=1}^{n} \hat{H}^{-3}(G_s, \mathbb{Z}) \to \hat{H}^{-3}(G, \mathbb{Z})$$

is a surjective homomorphism, and

$$i(T_s/k_s) = 1 \quad \text{for each } s = 1, \ldots, n,$$

where $G(F/k_s) = G_s$ and $G(F/T_s) = H_s$ ($s = 1, \ldots, n$), then $N(F/K) \subseteq N_{T/k}T^*$.

In the above theorem $\hat{H}^{-3}(G_s, \mathbb{Z})$ is a Tate cohomology group, and $\hat{H}^{-3}(G_s, \mathbb{Z}) = H_2(G_s, \mathbb{Z})$. Similarly, $\hat{H}^{-3}(S_5, \mathbb{Z}) = H_2(S_5, \mathbb{Z})$. We will show in the following proposition that the equality $N_{K_1/k}K_1^* = N_{K_2/k}K_2^*$ (see Fig. 1) holds for any Galois extension $E/k$ with the Galois group isomorphic to $S_5$.

**Proposition 14.** In the notation of Fig. 1, HNP holds for both extensions $K_1/k$, $K_2/k$, and $N_{K_1/k}K_1^* = N_{K_2/k}K_2^*$. 

---

Theorem. To prove the equality of norm groups we will use Theorem 13 to show that $N(E/k) \subseteq N_{K_i/k}K_i^*$ for each $i = 1, 2$. Let $G_i$ be a Sylow 2-subgroup of $S_5$ containing $H_1 \cap H_2 = \langle (4,5) \rangle$. Let $G_2$ and $G_3$ be a Sylow 3-subgroup and a Sylow 5-subgroup of $S_5$, respectively. By Proposition 3.1.15 of [13, p. 92]

$$
\prod_{i=1}^{3} \text{Cor} G_i : \prod_{i=1}^{3} \hat{H}^{-3}(G_i, \mathbb{Z}) \to \hat{H}^{-3}(S_5, \mathbb{Z})
$$

is a surjective homomorphism. Let $H_{ij} = G_j \cap H_i$ $(1 \leq i \leq 2, 1 \leq j \leq 3)$, and let $k_j$ and $T_{ij}$ be the fixed fields of $G_j$ and $H_{ij}$, respectively. For $j \neq 1$, $T_{ij}/k_j$ is a cyclic extension of degree 1, 3, or 5 for any $1 \leq i \leq 2$. So HNP holds for all extensions $T_{ij}/k_j$ for which $i = 1, 2$ and $j \neq 1$. The group $G_1$ is isomorphic to the dihedral group $D_8$ of order 8. Since $D_8$ contains only one nontrivial central element, which is the square of an element of order four, it follows that the nontrivial central element of $G_1$ is an even permutation in $S_5$. So the cyclic group $\langle (4,5) \rangle$ is not normal in $G_1$. Since $H_{ii} = \langle (4,5) \rangle$ for $i = 1, 2$, it follows by Satz 1 [2] that HNP holds for $T_{ii}/k_1$ for $i = 1, 2$. So by Theorem 13, $N(E/k) \subseteq N_{K_i/k}K_i^*$ for each $i = 1, 2$. By (1) the equality $\mathcal{P}_{S_5}(H_1) = \mathcal{P}_{S_5}(H_2)$ implies $N(K_1/k) = N(K_2/k)$. By (5) the first obstruction $N(K_i/k)/N(E/k)N_{K_i/k}K_i^*$ $(i = 1, 2)$ to HNP for $K_i/k$ corresponding to $E/k$ is a homomorphic image of $H_i \cap S_5'/\Phi^{S_5}(H_i)$, where $S_5' = A_5$ is the commutator subgroup of $S_5$. Since $H_i \cap A_5 = \Phi^{S_5}(H_i)$ is the cyclic subgroup of order 3 of $H_i$, it follows that the obstruction $N(K_i/k)/N(E/k)N_{K_i/k}K_i^*$ is trivial for each $i = 1, 2$. So for each $i = 1, 2$

$$
N(K_i/k) = N(E/k)N_{K_i/k}K_i^* = N_{K_i/k}K_i^*.
$$

It follows that HNP holds for both extensions $K_1/k$ and $K_2/k$, and therefore the equality $N_{K_1/k}K_1^* = N_{K_2/k}K_2^*$ holds. \qed

In Lemmas 11 and 12 we discussed the equality of norm groups of certain extensions in the case when there is a prime of the base field whose decomposition group in an extension contains a Sylow 2-subgroup of $A_4$ or $A_5$. We wish now to consider the case when a decomposition group of an arbitrary prime does not contain a Sylow 2-subgroup of $A_4$ or $A_5$. Since $A_4 = R_2$, the Sylow 2-subgroup $V_4$ of $A_4$ is also a Sylow 2-subgroup of $A_5$.

Lemma 15. Let $E/k$ be a finite Galois extension of an algebraic number field $k$ with the Galois group $G \cong S_5$. In the notation of Fig. 1, if for any prime of $k$ its decomposition group in $E$ does not contain Sylow 2-subgroups of $A_5$, then $N_{L_1/k}L_1^* \neq N_{L_2/k}L_2^*$ and $N_{M_1/k}M_1^* \neq N_{M_2/k}M_2^*$.
Proof. The commutator subgroup of $S_5$ is $A_5$. So for each $i = 1, 2$ the first obstructions to HNP for $L_i/k$ and $M_i/k$ corresponding to $E/k$ are isomorphic to

$$N_i \cap A_5 / \Phi^G(N_i)X_{L_i/k}(E, E) \quad \text{and} \quad R_i \cap A_5 / \Phi^G(R_i)X_{M_i/k}(E, E),$$

respectively. It follows that $\Phi^G(N_1) = 1, \Phi^G(N_2) = N_2$, and $\Phi^G(R_1) = R_1' = \langle (3, 4, 5) \rangle, \Phi^G(R_2) = R_2$. Since all four groups $N_i, R_i (i = 1, 2)$ are subgroups of $A_5$, it follows that

$$N(L_1/k) / N(E/k)N_{L_1/k}L_1^* \cong N_1 / X_{L_1/k}(E, E) \quad \text{and}$$

$$N(L_2/k) = N(E/k)N_{L_2/k}L_2^*, \quad (14)$$

and

$$N(M_1/k) / N(E/k)N_{M_1/k}M_1^* \cong R_1 / X_{M_1/k}(E, E) \quad \text{and}$$

$$N(M_2/k) = N(E/k)N_{M_2/k}M_2^*. \quad (15)$$

We will prove that

$$X_{L_1/k}(E, E) = N_1' (= 1) \quad (16)$$

and

$$X_{M_1/k}(E, E) = R_1' (= \langle (3, 4, 5) \rangle). \quad (17)$$

If equalities (16) and (17) hold, then by (14) and (15)

$$N_{L_1/k}L_1^* \neq N_{L_2/k}L_2^* \quad \text{and} \quad N_{M_1/k}M_1^* \neq N_{M_2/k}M_2^*.$$  

If the decompositions groups $G_v$ of all primes $v$ of $k$ in $E$ are cyclic, then by the definition of the group $X_{L_1/k}(E, E)$ equality (16) holds. Similarly, equality (17) holds if $G_v$ is cyclic for all primes $v$ of $k$. We assume, therefore, that there is a prime $v$ of $k$ for which $G_v$ is not cyclic. Let $S$ be the (finite) set of all primes $v$ of $k$ for which $G_v$ is not cyclic. We will show that $\lambda_v[\ker \psi_v]$ is the trivial subgroup of order one of $N_1/N_1' (R_1/R_1')$ for each prime $v \in S$. We note that for each prime $v \in S$, $G_v$ is a noncyclic solvable subgroup of $G = S_5$, and by the assumption $G_v$ does not contain a Sylow 2-subgroup of $A_5$. Let $\mathcal{A}$ be the set of all decomposition groups of primes from $S$ in $E$, and let $\mathcal{A} \subseteq \mathcal{B}$ be the set of all solvable noncyclic subgroups of $G$ that do not contain a Sylow 2-subgroup of $A_5$. We will show that $\lambda_X[\ker \psi_X]$ is trivial for all $X \in M(\mathcal{B})$. By Theorem 8 this will imply that $\lambda_v[\ker \psi_v]$ is the trivial subgroup of order one of $N_1/N_1' (R_1/R_1')$ for each prime $v \in S$. The set $M(\mathcal{B})$ contains two groups: a semidirect product of two cyclic groups $C_6 \cdot C_2 = \langle (1, 2, 3)(4, 5), (2, 3) \rangle = \langle a, b \rangle$ with $a^6 = b^2 = 1$, $b^{-1}ab = a^{-1}$, and a semidirect product of cyclic groups $C_5 \cdot C_4 = \langle (1, 2, 3, 4, 5), (2, 4, 5, 3) \rangle = \langle a, \beta \rangle$ with $a_5 = \beta^4 = 1, \beta^{-1}ax = a^3$. 


\[ 271 \]
We first consider the case when $X = C_6 \cdot C_2$. The group $G$ is the union of six distinct double cosets of $N_1$ and $X$ in $G$ with representatives \{1, (3, 4), (3, 4, 5), (2, 4)(3, 5), (1, 4, 3, 2), (1, 4, 2)(3, 5)\}. In the notation of diagram (6) the corresponding subgroups of $N_1$ are $(N_1)_1 = (N_1)_4 = N_1$, and the remaining four subgroups are trivial. So $\lambda_X[\text{Ker } \psi_X]$ is the trivial subgroup of order one of $N_1/N_1'$.

Suppose now that $X$ is equal to the second group $C_5 \cdot C_4$ in $M(\emptyset)$. Then $G$ is the union of four distinct double cosets of $N_1$ and $X$ in $G$ with representatives \{1, (4, 5), (3, 5, 4), (3, 5)\}. In the notation of diagram (6) the corresponding subgroups of $N_1$ are $(N_1)_1 = (N_1)_2 = 1$, and $(N_1)_3 = (N_1)_4 = N_1$. The kernel of

$$\psi_X : \prod_{i=1}^{6} (N_1)_i/(N_1)_i' \to X/X'$$

is the cyclic group of order 2 generated by the 6-tuple in which the first and the fourth components are $(2, 3)(4, 5)$, and the remaining components are trivial. So $\lambda_X[\text{Ker } \psi_X]$ is the trivial subgroup of order one of $N_1/N_1'$.

It follows that $\lambda_X[\text{Ker } \psi_X]$ is the trivial subgroup of order one of $N_1/N_1'$. This completes the proof of the equality $X_{L_1/k}(E, E) = N_1'$. So $N_{L_1/k}L_1^* \neq N_{L_2/k}L_2^*$.

We wish now to prove that $N_{M_1/k}M_1^* \neq N_{M_2/k}M_2^*$. The group $G$ is the union of three distinct double cosets of $R_1$ and $X = C_6 \cdot C_2$ in $G$ with representatives \{1, (2, 4, 3), (1, 4, 2, 5, 3)\}. In the notation of diagram (6) the corresponding subgroups of $R_1$ are $(R_1)_1 = \langle (1, 2)(4, 5) \rangle$, $(R_1)_2 = 1$, and $(R_1)_3 = R_1$. The kernel of

$$\psi_X : \prod_{i=1}^{3} (R_1)_i/(R_1)_i' \to X/X'$$

is the cyclic group of order 2 generated by the ordered triple in which the second component is trivial, and the remaining two components contain $(1, 2)(4, 5)$. It follows that $\lambda_X[\text{Ker } \psi_X]$ is the trivial subgroup of order one of $R_1/R_1'$. Finally, we assume that $X = C_5 \cdot C_4$. Then $G$ is the union of two distinct double cosets of $R_1$ and $X$ in $G$ with representatives \{1, (4, 5)\}. In the notation of diagram (6) the corresponding subgroups of $R_1$ are $(R_1)_1 = \langle (1, 2)(3, 5) \rangle$, and $(R_1)_2 = \langle (1, 2)(3, 4) \rangle$. The kernel of

$$\psi_X : (R_1)_1 \times (R_1)_2 \to X/X'$$
is the cyclic group of order 2 generated by \((1, 2)(3, 5), (1, 2)(3, 4)\). So \(\lambda_X[\text{Ker } \psi_X]\) is the subgroup of \(R_1/R'_1\) generated by
\[ (1, 2)(3, 5)(1, 2)(3, 4)R'_1 = (3, 5)(3, 4)R'_1 = (3, 5, 4)R'_1 = R'_1. \]

This completes the proof of the inequality \(N_{M_1/k}M'_1 \neq N_{M_2/k}M'_2\).

**Corollary 16.** Let \(E/k\) be a finite Galois extension of an algebraic number field \(k\) with the Galois group isomorphic to \(S_4\). Suppose that \(k < K < L \subseteq E\) are the fixed fields of \(V_4 \supseteq \mathbb{Z}/2\mathbb{Z}\), where \(\mathbb{Z}/2\mathbb{Z}\) is an arbitrary subgroup of order two of the Klein 4-group \(V_4\). If for any prime of \(k\) its decomposition group in \(E\) does not contain the Sylow 2-subgroup \((V_4)\) of \(A_4\), then \(N_{K/k}K^* \neq N_{L/k}L^*\).

**Proof.** We already observed that HNP holds for \(K/k\). By (1) \(N(K/k) = N(L/k)\). So to prove that \(N_{K/k}K^* \neq N_{L/k}L^*\) it suffices to show that HNP does not hold for \(L/k\), i.e. \(N_{L/k}L^*\) is a proper subgroup of \(N(L/k)\). We set \(H = \mathbb{Z}/2\mathbb{Z}\), and note that the commutator subgroup of \(S_4\) is equal to \(A_4\). Also, \(\Phi^S(H) = 1\). So by (5) the first obstruction to HNP for \(L/k\) corresponding to \(E/k\) is isomorphic to \(H/X_{L/k}(E, E)\).

We assume that \(S_4\) is a subgroup of \(S_5\). Let \(\mathcal{A}(\mathcal{B})\) be the set of all solvable noncyclic subgroups of \(S_4\) (\(S_5\)) that do not contain a Sylow 2-subgroup of \(A_4\) (\(A_5\)). It follows that \(\mathcal{B} \subseteq \mathcal{A}\). In the proof of Lemma 15 we showed that in the notation of diagram (6) with \(G = S_5\) and \(N = 1, \lambda_X[\text{Ker } \psi_X]\) is trivial for all \(X \in M(\mathcal{B})\). By Theorem 8 \(\lambda_X[\text{Ker } \psi_X]\) is trivial for all \(X \in \mathcal{B}\). So in the notation of diagram (6) with \(G = S_4\) and \(N = 1\) we obtain by Theorem 8 that \(\lambda_X[\text{Ker } \psi_X]\) is trivial for all \(X \in \mathcal{B}\). By the assumption on the primes of \(k\), and by (4) we obtain that \(X_{L/k}(E, E) = H' = 1\). So for the first obstruction to HNP for \(L/k\) corresponding to \(E/k\) we have
\[ N(L/k)/N(E/k)N_{L/k}L^* \cong H. \]

In particular, \(N(L/k) \neq N_{L/k}L^*\).

The set of the distinct nontrivial full systems of subgroups of \(S_4\) is \(\mathcal{S}(S_4) = \{\mathfrak{A}(\mathbb{Z}/2\mathbb{Z}, V_4)\}\). So by Lemma 11 and Corollary 16 we obtain a criterion for the equality of norm groups corresponding to extensions contained in a Galois extension with the Galois group isomorphic to \(S_4\).

**Theorem 17.** Let \(E/k\) be a finite Galois extension of an algebraic number field \(k\) with the Galois group \(S_4\). Suppose that \(k \subseteq K \subseteq E\) is the fixed field of the Klein 4-group \(V_4\) (the only Sylow 2-subgroup of \(A_4\)), and \(L\) is a quadratic extension of \(K\) contained in \(E\). Let \(k \subseteq X, Y \subseteq E\) be two fields. If there is a prime of \(k\) whose decomposition group in \(E\) contains the Sylow 2-subgroup \((V_4)\) of \(A_4\), then \(N_{X/k}X^* = N_{Y/k}Y^*\) if and only if either \(X\) and \(Y\) are conjugate over \(k\), or \(X\) and \(Y\) are conjugate over \(k\) to \(K\) and \(L\). Otherwise, \(N_{X/k}X^* = N_{Y/k}Y^*\) if and only if \(X\) and \(Y\) are conjugate over \(k\).
There are up to conjugation five transitive subgroups of $S_4$: a cyclic subgroup $\langle (1,2,3,4) \rangle$ of order four, Sylow 2-subgroups of $A_4$ and $S_4$, $A_4$, and $S_4$ [3, p. 871]. Each of these groups with the exception of the cyclic group contains the Sylow 2-subgroup of $A_4$. Since the Galois group of a reducible polynomial of degree four with coefficients in a completion of an algebraic number field does not contain the Sylow 2-subgroup of $A_4$, we obtain the following lemma.

**Lemma 18.** Let $k_v$ be the completion of an algebraic number field $k$ at a prime $v$ of $k$. Suppose that $G_v$ is the Galois group over $k_v$ of the splitting field of a polynomial $f(x) \in k_v[x]$ of degree four. Then $G_v$ contains the Sylow 2-subgroup of $A_4$ if and only if $f(x)$ is irreducible over $k_v$, and $G_v$ is not cyclic of order four.

Let

$$f(x) = x^4 - x^3 - 4x^2 + x + 2$$

be a polynomial with rational coefficients. The discriminant of $f(x)$ is a prime integer 2777. Let $F$ be the splitting field of $f(x)$. Since $f(x)$ is irreducible over GF(3), and $\sqrt{2777} \notin \mathbb{Q}$, it follows that $G(F/\mathbb{Q})$ is a transitive subgroup of $S_4$, and it is not contained in $A_4$. Since $f(x)$ factors into two irreducible factors $(x+6)(x^3+4x^2+5x+4)$ over GF(11), it follows by Hensel's Lemma [14, p. 45] that the local extension $F_{11}$ (the completion of $F$ at a prime above 11) is the unramified cubic extension of $\mathbb{Q}_{11}$. So 3 divides the order of $G(F/\mathbb{Q})$, and therefore $G(F/\mathbb{Q})$ is isomorphic to $S_4$. For each prime $p \neq 2777$ the extension $F_p/\mathbb{Q}_p$ is unramified cyclic extension. Since $f(x)$ factors into irreducible factors $(x+310)(x+1422)(x+522)^2$ over GF(2777), it follows by Hensel's Lemma that $F_p = \mathbb{Q}_p(\sqrt{2777})$ is a totally ramified quadratic extension of $\mathbb{Q}_p$ at the prime $p = 2777$. So all local extensions are cyclic. It follows that the decomposition groups of all primes of $\mathbb{Q}$ in $F$ are cyclic, and therefore they do not contain the Sylow 2-subgroup of $A_4$. So by Theorem 17 for any fields $\mathbb{Q} \subseteq X, Y \subseteq F$ the equality $N_{X/\mathbb{Q}}X^* = N_{Y/\mathbb{Q}}Y^*$ holds if and only if $X$ and $Y$ are conjugate over $\mathbb{Q}$, i.e. $X$ and $Y$ are isomorphic.

Let $E$ be the splitting field of

$$g(x) = x^4 - 6x^2 - 3x + 3 \in \mathbb{Q}[x]$$

The discriminant of $g(x)$ is 9909 = $3^3 \cdot 367$. Since $g(x)$ is an Eisenstein polynomial over $\mathbb{Q}_3$, it follows by Theorem 3.3.1 of [14, p. 86] that $g(x)$ is irreducible over $\mathbb{Q}_3$, and that $\mathbb{Q}_3(\alpha)/\mathbb{Q}_3$ is a totally ramified extension of degree four, where $\alpha \in E_3$ is a root of $g(x)$. We wish to show that $G(E_3/\mathbb{Q}_3)$ contains the Sylow 2-subgroup of $A_4$. Indeed, by Lemma 18 it suffices to show that $G(E_3/\mathbb{Q}_3)$ is not cyclic of order four. Suppose the Galois group is cyclic of order four. Then $E_3 = \mathbb{Q}_3(\alpha)$, and $E_3/\mathbb{Q}_3$ is a totally and tamely ramified extension of degree four. By Proposition 3.4.3 of [14, p. 89] $E_3 = \mathbb{Q}_3(\sqrt[4]{\pi})$ for some prime element $\pi \in \mathbb{Q}_3$. It follows that $E_3$ contains a primitive 4th root of unity, since $E_3$ is a Galois extension of $\mathbb{Q}_3$. This, however, is impossible. We thus obtain that a decomposition group of 3 in $E$ contains the Sylow
2-subgroup of $A_4$. The polynomial $g(x)$ is irreducible over $\mathbb{Q}$, and $\sqrt{9909} \notin \mathbb{Q}$. So $G(E/\mathbb{Q})$ is a transitive subgroup of $S_4$, and it is not contained in $A_4$. Since $g(x)$ factors into two irreducible factors $(x + 4)(x^3 + x^2 + 2)$ over $GF(5)$, it follows by Hensel’s Lemma that $E_5/\mathbb{Q}_5$ is unramified cubic extension. So 3 divides the order of $G(E/\mathbb{Q})$, and therefore $G(E/\mathbb{Q})$ is isomorphic to $S_4$. In the notation of Theorem 17 we thus obtain that for any fields $\mathbb{Q} \subseteq X, Y \subseteq E$ the equality $N_{X/\mathbb{Q}}X^* = N_{Y/\mathbb{Q}}Y^*$ holds if and only if either $X$ and $Y$ are isomorphic, or $X$ and $Y$ are isomorphic to $K$ and $L$.

The set of the distinct nontrivial full systems of subgroups of $S_5$ is $\mathcal{F}(S_5) = \{\mathcal{E}(H_1, H_2), \mathcal{E}(N_1, N_2), \mathcal{E}(R_1, R_2)\}$. So by Lemma 12, Proposition 14, and Lemma 15 we obtain a criterion for the equality of norm groups corresponding to extensions contained in a Galois extension with the Galois group isomorphic to $S_5$.

**Theorem 19.** Let $E/k$ be a finite Galois extension of an algebraic number field $k$ with the Galois group isomorphic to $S_5$. Let $k \subseteq X, Y \subseteq E$ be two fields. In the notation of Fig. 1, if there is a prime of $k$ whose decomposition group in $E$ contains a Sylow 2-subgroup of $A_5$, then $N_{X/k}X^* = N_{Y/k}Y^*$ if and only if either $X$ and $Y$ are conjugate over $k$, or $X$ and $Y$ are conjugate over $k$ to one of the pairs: $K_1$ and $K_2$, $L_1$ and $L_2$, or $M_1$ and $M_2$. Otherwise, $N_{X/k}X^* = N_{Y/k}Y^*$ if and only if either $X$ and $Y$ are conjugate over $k$, or $X$ and $Y$ are conjugate over $k$ to $K_1$ and $K_2$.

**Lemma 20.** Let $k_v$ be the completion of an algebraic number field $k$ at a prime $v$ of $k$. Suppose that $G_v$ is the Galois group over $k_v$ of the splitting field of a polynomial $f(x) \in k_v[x]$ of degree five. Then $G_v$ contains a Sylow 2-subgroup of $A_5$ if and only if $f(x)$ factors into a linear and an irreducible polynomial of degree four over $k_v$, and $G_v$ is not cyclic of order four.

**Proof.** Suppose $G_v$ contains a Sylow 2-subgroup of $A_5$. We wish to show that $f(x)$ is reducible over $k_v$. Indeed, if $f(x)$ is irreducible over $k_v$, then $G_v$ is conjugate to one of five transitive subgroups of $S_5$ [3, p. 872]. Only two of these subgroups $A_5$ and $S_5$ contain a Sylow 2-subgroup of $A_5$. Since $G_v$ is a solvable group, $G_v$ cannot be $A_5$ or $S_5$. So $f(x)$ is reducible over $k_v$. If the highest degree of an irreducible factor of $f(x)$ is at most three, then $G_v$ does not contain a Sylow 2-subgroup of $A_5$. It follows that $f(x)$ factors over $k_v$ into a product of a linear and an irreducible polynomial of degree four.

Conversely, suppose that $f(x)$ factors into a linear and an irreducible polynomial of degree four over $k_v$. Then $G_v$ is the Galois group over $k_v$ of the splitting field of an irreducible polynomial of degree four, and $G_v$ is not cyclic of order four by assumption. So by Lemma 18 $G_v$ contains the Sylow 2-subgroup of $A_5$. It follows that $G_v$ as a permutation group on the roots of $f(x)$ contains a Sylow 2-subgroup of $A_5$. □

The discriminant of the polynomial

$$f(x) = x^5 - x^4 - x^3 + x^2 - 1 \in \mathbb{Q}[x]$$
is a prime number 1609. Let $E$ be the splitting field of $f(x)$, and let $G$ be the Galois group of the extension $E/\mathbb{Q}$. Since $f(x)$ is irreducible over $\text{GF}(3)$, and factors into a product of irreducible polynomials $(x^2 + x + 4)(x^3 + 5x^2 + 4x + 5)$ over $\text{GF}(7)$, it follows that $G$ contains a 5-cycle and a transposition. So $G$ is isomorphic to $S_5$. The factorization $(x + 621)(x + 704)(x^2 + 1271x + 1113)$ of $f(x)$ over $\text{GF}(1609)$ shows by Lemma 20 that the Galois group of the local extension $E_p/\mathbb{Q}_p$ at the prime $p = 1609$ does not contain a Sylow 2-subgroup of $A_5$. Also, for any prime $p \neq 1609$ the extension $E_p/\mathbb{Q}_p$ is cyclic. So by Theorem 19 for any fields $\mathbb{Q} \subseteq X, Y \subseteq E$ the equality $N_{X/\mathbb{Q}}X^* = N_{Y/\mathbb{Q}}Y^*$ holds if and only if, in the notation of Fig. 1, either $X$ and $Y$ are isomorphic, or $X$ and $Y$ are isomorphic to $K_1$ and $K_2$.

Let $F$ be the splitting field of

$$g(x) = x^5 - 11x^4 + 42x^3 - 63x^2 + 27x + 3 \in \mathbb{Q}[x].$$

Since $g(x)$ factors into a product of irreducible polynomials $(x^2 + 2x + 3)(x^3 + 2x^2 + 1)$ over $\text{GF}(5)$, and is irreducible over $\text{GF}(13)$, it follows that $G(F/\mathbb{Q})$ is isomorphic to $S_5$. The discriminant of $g(x)$ is $310257 = 3^3 \cdot 11491$, and $g(x)$ factors into a product of irreducible factors $x^4(x + 1)$ over $\text{GF}(3)$. By Hensel’s Lemma

$$g(x) = (x^4 + ax^3 + bx^2 + cx + d)(x + \theta)$$

(18)

over the ring of integers $\mathcal{O}$ of $\mathbb{Q}_3$. Let $\mathfrak{m}$ be the maximal ideal of $\mathcal{O}$. Then $a, b, c, d$ belong to $\mathfrak{m}$, and $\theta \in 1 + \mathfrak{m}$. Since 3 is a generator of $\mathfrak{m}$, it follows that $\lambda = v3^m$ for some unit $v \in \mathcal{O}$ and $m \geq 1$. By (18) $\lambda \theta = 3$. On the other hand $\lambda \theta = u3^m$ for some unit $u \in \mathcal{O}$, since $\theta$ is a unit in $\mathcal{O}$. So $\lambda = v3$, and therefore $x^4 + ax^3 + bx^2 + cx + d$ is an Eisenstein polynomial over $\mathbb{Q}_3$. It follows that this polynomial is irreducible over $\mathbb{Q}_3$, and the completion $F_3$ contains $\mathbb{Q}_3(\sqrt[3]{\pi})$ for some prime element $\pi \in \mathbb{Q}_3$. If $G(F_3/\mathbb{Q}_3)$ were cyclic of order four, then $F_3 = \mathbb{Q}_3(\sqrt[3]{\pi})$ and, therefore, $\mathbb{Q}_3$ would contain a primitive 4th root of unity. This, however, is impossible. So by Lemma 20 $G(F_3/\mathbb{Q}_3)$ contains a Sylow 2-subgroup of $A_5$. So by Theorem 19 in the notation of Fig. 1 for any fields $\mathbb{Q} \subseteq X, Y \subseteq F$ the equality $N_{X/\mathbb{Q}}X^* = N_{Y/\mathbb{Q}}Y^*$ holds if and only if either $X$ and $Y$ are isomorphic, or $X$ and $Y$ are isomorphic to one of the pairs: $K_1$ and $K_2$, $L_1$ and $L_2$, or $M_1$ and $M_2$.

References


