Abstract. Let $K/F$ be a cyclic extension of odd prime degree $l$ over a number field $F$. If $F$ has class number coprime to $l$, we study the structure of the $l$-Sylow subgroup of the class group of $K$. In particular, when $F$ contains the $l$-th roots of unity, we obtain bounds for the $\mathbb{F}_l$-rank of the $l$-Sylow subgroup of $K$ using genus theory. We obtain some results valid for general $l$. Following that, we obtain more complete, explicit results for $l=5$ and $F=\mathbb{Q}(\sqrt[5]{5})$. The rank of the 5-class group of $K$ is expressed in terms of power residue symbols. We compare our results with tables obtained using SAGE (the latter is under GRH). We obtain explicit results in several cases. These results have a number of potential applications. For instance, some of them like Theorem 5.16 could be useful in the arithmetic of elliptic curves over towers of the form $\mathbb{Q}(\sqrt[5]{5^n}, x^{1/5})$. Using the results on the class groups of the fields of the form $\mathbb{Q}(\sqrt[5]{5^n}, x^{1/5})$, and using Kummer duality theory, we deduce results on the 5-class numbers of fields of the form $\mathbb{Q}(x^{1/5})$.

Mathematics Subject Classification: 11R29, 13C20.

1. Introduction

We study the $l$-class group of $K$, where $K$ is a cyclic extension of degree $l$ over a number field $F$ which contains the $l$-th roots of unity and has trivial
manisha kulkarni, et al.

l-class group, where l is an odd prime. Denote by τ a generator of \( \text{Gal}(K/F) \). The l-class group \( S_K \) is a \( \mathbb{Z}_l[\zeta_l] \)-module since

\[
\mathbb{Z}_l[\zeta_l] \cong \mathbb{Z}_l[\text{Gal}(K/F)]/(1 + \tau + \cdots + \tau^{l-1})
\]

where \( \zeta_l \) corresponds to \( \tau \). As a module over the discrete valuation ring \( \mathbb{Z}_l[\zeta_l] \) whose maximal ideal is generated by \( \lambda = 1 - \zeta_l \), the l-class group \( S_K \) of \( K \) decomposes as

\[
S_K \cong \mathbb{Z}_l[\zeta_l]/(\lambda^{e_1}) \oplus \mathbb{Z}_l[\zeta_l]/(\lambda^{e_2}) \oplus \cdots \oplus \mathbb{Z}_l[\zeta_l]/(\lambda^{e_t})
\]

for some \( 1 \leq e_1 \leq e_2 \leq \cdots \leq e_t \). Our goal is to compute the rank of \( S_K \) which is the dimension of the \( \mathbb{F}_l \)-vector space \( S_K \otimes \mathbb{F}_l \). To find the \( e_i \)’s, one looks at

\[
s_i = |\{ e_j : e_j = i \}|.
\]

Then, the rank of the \( \mathbb{Z}_l[\zeta_l] \)-module \( \lambda^{i-1}S_K/\lambda^i S_K \) is \( t - s_1 - \cdots - s_{i-1} \) - this is also called the \( \lambda^i \)-rank of \( S_K \). To compute these numbers, we consider the decreasing filtration

\[
S_K \supset \lambda S_K \supset \lambda^2 S_K \supset \cdots
\]

and construct ideal classes generating the pieces \( \lambda^{i-1}S_K/\lambda^i S_K \) and construct genus fields corresponding to them. This is difficult to carry out explicitly in general. However, the general analysis does lead to expressions and bounds for the rank of \( S_K \) such as the following proposition:

\( S_K \) is isomorphic to the direct product of an elementary abelian l-group of rank \( s_1 \) and an abelian \( l \)-group of rank

\[
(\ell - 1)(t - s_1) - (\ell - 3)s_2 - (\ell - 4)s_3 - \cdots - s_{\ell-2}.
\]

In particular,

\[
\text{rank} S_K = (\ell - 1)t - (\ell - 2)s_1 - (\ell - 3)s_2 - \cdots - s_{\ell-2}
\]

satisfies the bounds

\[
2t - s_1 \leq \text{rank} S_K \leq (\ell - 1)t - (\ell - 2)s_1
\]

both of which are attainable.

This is proved in section 3; the expression for the rank is almost immediate but some components of proof of the proposition are used while constructing the genus fields explicitly later.

In section 4, we assume that \( F \) contains the l-th roots of unity and construct genus fields corresponding to the pieces of the class group as above. These fields are of the form \( K(x_1^{1/l}, x_2^{1/l}, \ldots, x_t^{1/l}) \). For a basis \( \{ P_j \} \) of ideal classes for a piece, using Kummer theory to map the Galois group of the
corresponding genus field to \( \mathbb{F}_l \), one writes down a matrix with entries in \( \mathbb{F}_l \) from that part of the class group. This allows us to express the rank of that piece of the class group in terms of the rank of a matrix of Artin symbols of the form \( (\mathbb{F}_{l^i}/\mathbb{F}) \) (see theorems 4.1, 4.2).

In section 5, we specialize to \( l = 5 \) and \( F = \mathbb{Q}(\zeta) \) which allows us to precisely work out the previous results. The major part of the paper is contained in sections 5 and 6. In section 5, we use ideles to rewrite the earlier computations of the \( s_i \)'s in terms of Artin symbols in a more explicit form in terms of local Hilbert symbols. One of the results in section 5 is:

Let \( K = F(x^{5}) \), \( x = u \lambda^{e_1} \pi_1^{e_1} \cdots \pi_g^{e_g} \) and \( F = \mathbb{Q}(\zeta) \) where each \( \pi_i \) is a prime element congruent to a rational integer modulo \( 5 \mathbb{Z}[\zeta] \) and \( u \) is a unit in \( F \). Let \( M_1 = K(x_1^{1/5}, \ldots, x_t^{1/5}) \) denote the genus field of \( K/F \), where \( [M_1 : K] = 5^t \), \( x_i \in F \) for \( 1 \leq i \leq t \), and \( x_i \equiv \pm 1, \pm 7 \) (mod \( 5^2 \)). For \( 1 \leq i \leq t, 1 \leq j \leq g \), let \( v_{ij} \) denote the degree 5 Hilbert symbol \( \left(x_i, \lambda^{j}\right)_{5} \) in the local field \( K_{\pi_j} \). Further, suppose

\[
v_{i, g+1} = \left(\frac{x_i, \lambda}{\lambda}\right) \text{ for } 1 \leq i \leq t, \text{ if the ideal } (\lambda) \text{ of } F \text{ ramifies in } K.
\]

If \( \gamma_{ij} \in \mathbb{F}_l \) are defined by the power symbol \( \zeta^{\gamma_{ij}} = (x_i^{1/5})^{-1} \), and \( C_1 \) is the matrix \( (\gamma_{ij}) \), \( 1 \leq i \leq t, 1 \leq j \leq u = g + 1 \), we have

\[
s_1 = \text{rank}C_1.
\]

The above result is under the assumption that ambiguous ideals are strongly ambiguous; in the contrary case, we have a very similar statement with a slightly bigger matrix (see Theorem 5.9).

A similar result is proved for computing \( s_i \)'s for \( i > 1 \) (see Theorem 5.10). Thus, we have some results on the \( \lambda^2 \)-rank of the 5-class group for general \( i \) and the results on \( \lambda^2 \)-rank are easily computable in many situations.

We give tables of class groups obtained by using the SAGE program and compare our results in its light. Interestingly, after a close inspection of the tables, we were able to guess the following general results which we prove (Theorems 5.12, 5.13, 5.14, 5.15, 5.16, 5.18).

**Theorem.** Let \( p \) be a prime number congruent to \(-1 \pmod{5} \). Let \( F = \mathbb{Q}(\zeta_5) \) and \( K = F(p^{1/5}) \). Assuming that each ambiguous ideal class is strongly ambiguous, we have that 25 divides the class number of \( K \). More precisely, the \( \lambda^2 \)-rank (to be defined below) of the 5-class group \( S_K \) is 1 and, \( 2 \leq \text{rank}S_K \leq 4 \).

The following theorem may be useful in studying the arithmetic of elliptic curves over towers of the form \( \mathbb{Q}(e^{\frac{2\pi i}{5}}, x^{1/5}) \). It is motivated by a comment of
John Coates that I wasawa theory implies the triviality of 5-class group of the above fields for all \( n \) in the cases of \( x \) considered in the theorem.

**Theorem.** Let \( F = \mathbb{Q}(\zeta_5) \) and let \( K = \mathbb{Q}(\zeta_5, x^{1/5}) \) where \( x \) is a positive integer which is not divisible by the 5\(^{th}\) power of any prime in \( F \). Suppose that the prime \( \lambda = 1 - \zeta_5^a \) over 5 in \( F \), ramifies in \( K \). Then \( S_K = \{1\} \) if, and only if, \( x = p^a \), where \( p \) is a prime number such that \( p \equiv \pm 2 \pmod{5} \), but \( p \not\equiv \pm 7 \pmod{25} \) and \( 1 \leq a \leq 4 \). Further, for all \( x \) as above, the prime 5 ramifies totally in \( \mathbb{Q}(\zeta_{25}, x^{1/5}) \).

If we remove the assumption that \( \lambda \) ramifies in \( K/F \), then the 5-class group is trivial if, and only if, \( x = p^a \) with \( p \equiv \pm 2 \pmod{5} \) or \( x = p^a q^b \), where \( p, q \equiv \pm 2 \pmod{5} \) but \( p, q \not\equiv \pm 7 \pmod{25} \) and \( x \equiv \pm 1, \pm 7 \pmod{25} \). All these results are exemplified in Table 1.

**Theorem.** Let \( p \) be a prime number congruent to \( \pm 7 \pmod{25} \) and \( q \) be a prime number congruent to \( -1 \pmod{5} \). Let \( F = \mathbb{Q}(\zeta_5) \) and \( K = F((pq)^{1/5}) \). [Assuming that each ambiguous ideal class is strongly ambiguous,] we have that 125 divides the class number of \( K \). More precisely, \( \lambda^2 \)-rank of \( S_K \) is 1 and we have, \( 3 \leq \text{rank} S_K \leq 5 \).

**Theorem.** Let \( p_i \equiv \pm 7 \pmod{25} \) for \( 1 \leq i \leq r \) be primes and \( r \geq 2 \). Let \( n = p_1^{a_1} \cdots p_r^{a_r} \), where \( 1 \leq a_i \leq 4 \) for \( 1 \leq i \leq r \). Let \( F = \mathbb{Q}(\zeta_5) \) and \( K = F(n^{1/5}) \).

(i) If all ambiguous ideal classes of \( K/F \) are strongly ambiguous, then the \( \lambda^2 \)-rank of \( S_K \) is \( r - 1 \) and \( 2r - 2 \leq \text{rank} S_K \leq 4r - 4 \).

(ii) If there are ambiguous ideal classes which are not strongly ambiguous, then \( s_1 \leq 2 \), \( \lambda^2 \)-rank of \( S_K \) is greater than or equal to \( r - 3 \) and \( \max(2r - 4, r - 1) \leq \text{rank} S_K \leq 4r - 4 \).

**Theorem.** Let \( p_i \equiv \pm 7 \pmod{25} \) for \( 1 \leq i \leq r \) be primes and let \( q_j \) be primes such that \( q_j \equiv \pm 2 \pmod{5} \) but \( q_j \not\equiv \pm 7 \pmod{25} \) for \( 1 \leq j \leq s \). Let \( n = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} \), where \( 1 \leq a_i, b_j \leq 4 \) for \( 1 \leq i \leq r \) and \( 1 \leq j \leq s \). Let \( n \equiv \pm 1, \pm 7 \pmod{25} \). Let \( F = \mathbb{Q}(\zeta_5) \) and \( K = F(n^{1/5}) \).

(i) If all ambiguous ideal classes of \( K/F \) are strongly ambiguous, then the \( \lambda^2 \)-rank of \( S_K \) is \( r + s - 1 \) and \( 2r + 2s - 2 \leq \text{rank} S_K \leq 4r + 4s - 4 \).

(ii) If there are ambiguous ideal classes which are not strongly ambiguous, then \( s_1 \leq 1 \), \( \lambda^2 \)-rank of \( S_K \) is greater than or equal to \( r + s - 2 \) and \( \max(2r + 2s - 3, r + s - 1) \leq \text{rank} S_K \leq 4r + 4s - 4 \).

**Theorem.** Let \( p_i \equiv \pm 7 \pmod{25} \) for \( 1 \leq i \leq r \) be primes and let \( q_j \) be primes such that \( q_j \equiv \pm 2 \pmod{5} \) but \( q_j \not\equiv \pm 7 \pmod{25} \) for \( 1 \leq j \leq s \) with \( s \geq 2 \). Let \( n = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s} \), where \( 1 \leq a_i, b_j \leq 4 \) for
Let $N$ be a positive integer of one of the following forms. Then, the $\lambda$-class group of $L$ is either trivial or cyclic:

- Let $N = p^a$, where $p \equiv \mp 2 \pmod{5}$ is a prime, $1 \leq a \leq 4$.
- Let $N = q_1^{a_1}q_2^{a_2}$ where $q_i \equiv \mp 2 \pmod{5}$ but $q_i \not\equiv \pm 7 \pmod{25}$, $1 \leq a_i \leq 4$ for $i = 1, 2$ such that $N \equiv \mp 1, \pm 7 \pmod{25}$.
- Let $N = p^a$ where $p \equiv -1 \pmod{5}$ is a prime, $1 \leq a \leq 4$.
- Let $N = p_1^{a_1}p_2^{a_2}$ where $p_i \equiv \pm 7 \pmod{25}$, $1 \leq a_i \leq 4$ for $i = 1, 2$ such that $N \equiv \mp 1, \pm 7 \pmod{25}$.
- $N = q_1^{a_1}q_2^{a_2}$ where $q_i \equiv \pm 2 \pmod{5}$ but $q_i \not\equiv \pm 7 \pmod{25}$, $1 \leq a_i \leq 4$ for $i = 1, 2$ such that $N \equiv \mp 1, \pm 7 \pmod{25}$.
- $N = p^aq^b$ where $p \equiv \pm 7 \pmod{25}$, $q \equiv \pm 2 \pmod{5}$ but $q \not\equiv \pm 7 \pmod{25}$ and $1 \leq a, b \leq 4$ such that $N \not\equiv \mp 1, \pm 7 \pmod{25}$.
- $N = q_1^{a_1}q_2^{a_2}$ where $q_i \equiv \pm 2 \pmod{5}$ but $q_i \not\equiv \pm 7 \pmod{25}$, $1 \leq a_i \leq 4$ for $i = 1, 2$ such that $N \not\equiv \mp 1, \pm 7 \pmod{25}$.
- $N = p_1^{a_1}p_2^{a_2}q^b$ where $p_i \equiv \pm 7 \pmod{25}$, $q \equiv \pm 2 \pmod{5}$ but $q \not\equiv \pm 7 \pmod{25}$, $1 \leq a_i, b \leq 4$ for $i = 1, 2$ such that $N \not\equiv \mp 1, \pm 7 \pmod{25}$.
- $N = p^aq_1^{a_1}q_2^{a_2}$ where $p \equiv \pm 7 \pmod{25}$, $q_i \equiv \pm 2 \pmod{5}$ but $q_i \not\equiv \pm 7 \pmod{25}$, $1 \leq a_i \leq 4$ for $i = 1, 2, 3$ such that $N \not\equiv \mp 1, \pm 7 \pmod{25}$.
- $N = p^a$, where $p \equiv -1 \pmod{5}$ and $q \equiv \pm 7 \pmod{25}$ are primes, $1 \leq a, b \leq 4$.

The above corollary is proved in section 6 where we consider quintic fields $L = \mathbb{Q}(n^{1/5})$. If $F = \mathbb{Q}(\zeta)$ as before, then $K = L(\zeta_5) = \mathbb{Q}(n^{1/5}, \zeta_5)$ has Galois group over $L$ to be cyclic of order 4, generated by $\sigma : \zeta \mapsto \zeta^3$. If $\tau : n^{1/5} \mapsto \zeta n^{1/5}$ in Gal($K/F$), then Gal($K/\mathbb{Q}$) is the affine group on $\mathbb{F}_5$; viz., $<\sigma> \times <\tau>$ where $\sigma\tau\sigma^{-1} = \tau^3$. The group $S_K$ is a $\mathbb{Z}_5[G]$-module where $G = \text{Gal}(K/L)$. Denoting by $\omega : G \rightarrow \mathbb{Z}_5^2$ the character sending $\sigma$ to 3 modulo 5, we have for any $\mathbb{Z}_5[G]$-module $C$, one has a decomposition $C = \oplus_{i=0}^{3}C(\omega^i)$ where $C(\omega^i) = \{a \in C : \sigma a = \omega(\sigma)^i a\}$. Using this module structure and Kummer theory, we prove in section 6 the following theorem whose corollary is stated above.
Theorem. If \( L = \mathbb{Q}(n^{1/5}) \) where \( n \) is 5-th power free, then
\[
\text{rank} S_L \leq \min(t, t - s_1 + \text{rank}(S_K/(1 - \zeta)S_K)(\omega_0^0)).
\]
Further, if \( n = p_1^{a_1} \cdots p_m^{a_m} \) where the primes \( p_i \equiv \pm 2 \) or \( \equiv -1 \) modulo 5, then
\[
\text{rank} (S_K/(1 - \zeta)S_K)(\omega_0^0).
\]
Our results along with computation using SAGE, sometimes allows us to deduce the existence of ambiguous ideal classes which are not strongly ambiguous. For example, let \( K = \mathbb{Q}(\zeta_5, \sqrt{301}), L = \mathbb{Q}(\sqrt{301}) \). By Theorem 5.12, if all ambiguous ideal classes are strongly ambiguous, then, \( 2 \leq \text{rank} S_K \leq 4 \). The same theorem tells us that if there are ambiguous ideal classes which are not strongly ambiguous, then \( 1 \leq \text{rank} S_K \leq 4 \). But, SAGE shows \( S_K = C_5 \). Thus, it is likely that we have ambiguous ideal classes which are not strongly ambiguous in this case and that \( t = s_1 = 1 \). By Corollary 6.4 and Theorem 6.6, we see that \( S_L = \{1\} \), which is confirmed by SAGE.

Historically, when \( K = \mathbb{Q}(\sqrt{D}) \) is a quadratic field of discriminant \( D \), Gauss’s genus theory of quadratic forms determines the rank of the 2-Sylow subgroup of the ideal class group of \( K \). C. S. Herz ([12]) proved that this rank is \( d - 1 \) or \( d - 2 \) where \( d = \omega(D) \), the number of distinct prime divisors of \( D \). In a series of papers (see [3], [4], [5]), Frank Gerth III proved several results on pure cubic extensions of \( \mathbb{Q} \) and on cyclic cubic extensions of \( \mathbb{Q} \) and also obtained a generalization of Herz’s result for the 3-Sylow subgroup of the ideal class group of a cyclic extension of \( \mathbb{Q}(\omega) \) where \( \omega \) is a primitive 3-rd root of unity. In two papers, G. Gras ([6], [7]) introduced and studied an increasing filtration to obtain results on the narrow ideal class group. Our results are proved using a decreasing filtration and generalize some of Gerth’s results to the case of an odd prime \( l \); they are more complete and explicit when \( l = 5 \).

In the 1930’s, Rédei and Reichardt proved certain results on class groups of some abelian extensions of \( \mathbb{Q} \) ([18]). Curiously, the series of papers by Gerth do not refer to the old work of Rédei and Reichardt. Conversely, the newer papers which refer to Rédei-Reichardt while addressing similar questions (see, for instance, Greither-Kučera’s paper on the lifted root number conjecture [9]), do not seem to be aware of Gerth’s work.

Rédei matrices are square matrices which appeared classically (see [17]) and have been studied by others (see [21],[13],[15]) since then. In our discussion, we construct similar matrices which are rectangular in general.

Our results have some potential applications. One possible application of our results on the \( l \)-class group of certain number fields is towards the existence of \( p \)-descent for certain elliptic curves.

Indeed, assuming that the \( \mathbb{F}_2 \)-rank of the 4-class group of \( K = \mathbb{Q}(\sqrt{-2n}) \) - where \( n = p_0p_1 \cdots p_k \) is a product of distinct odd primes with \( p_i \equiv 1 \) (mod 8) for \( 1 \leq i \leq k \) - is 0 if \( n \equiv \pm3 \) (mod 8) and 1 otherwise, Ye Tian showed ([20]) that the elliptic curves \( E^{(m)}/\mathbb{Q} \) defined by \( my^2 = x^3 - x \), where
Let \( m = n \) or \( 2n \) such that \( m \equiv 5, 6, \) or \( 7 \) modulo \( 8 \), have first \( 2 \)-descent and deduced the BSD conjecture holds for these elliptic curves.

From our results on 5-class numbers of fields of the form \( \mathbb{Q}(\zeta_5, n^{1/5}) \), we use duality theory to deduce results on the 5-class number of the fields \( \mathbb{Q}(n^{1/5}) \) for some \( n \). These have potential applications to the following work of Calegari-Emerton on modular forms. Calegari and Emerton showed ([1]) that if the class group of \( \mathbb{Q}(N^{1/5}) \) is cyclic for a prime \( N \), certain local extensions of \( \mathbb{Q}_5 \) coming from normalized cuspidal Hecke eigenforms are trivial. More precisely:

Let \( f \) be a normalized cuspidal Hecke eigenform of level \( N \). Let \( K_f \) denote the extension of \( \mathbb{Q}_5 \) generated by the \( q \)-expansion coefficients \( a_n(f) \) of \( f \).

If \( N \) is a prime and \( 5 \parallel (N - 1) \), it is known due to Mazur that there exists a unique (upto conjugation) weight 2 normalized cuspidal Hecke eigenform defined over \( \mathbb{Q}_5 \), satisfying the congruence

\[
a_l(f) \equiv 1 + l \pmod{p}
\]

where \( p \) is the maximal ideal of the ring of integer of \( K_f \). It is known that \( K_f \) is a totally ramified extension of \( \mathbb{Q}_5 \). Calegari and Emerton showed that if the class group of \( \mathbb{Q}(N^{1/5}) \) is cyclic, then \( K_f = \mathbb{Q}_5 \).

2. Notations

Let \( \ell \) be an odd prime number. Let \( F \) be a number field and \( K/F \) be a cyclic extension of degree \( \ell \) over \( F \). Let \( C_K \) and \( C_F \) denote the ideal class groups of \( K \) and \( F \) respectively. Let \( S_K \) and \( S_F \) denote their respective Sylow \( \ell \)-subgroups which we sometimes refer to as the \( \ell \)-class groups. The rank of \( S_K \) is defined to be the \( \mathbb{F}_\ell \)-dimension of \( S_K \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell \).

We have a natural action of \( \text{Gal}(K/F) \) on \( C_K \) and on \( S_K \).

We assume throughout that \( S_F \) is trivial. It is convenient to use additive notation. Denote by \( \tau \) a generator of \( \text{Gal}(K/F) \). Let \( \zeta \) be a fixed primitive \( \ell \)-th root of unity. The \( \ell \)-class group \( S_K \) is a \( \mathbb{Z}_\ell \)-module since

\[
\mathbb{Z}_\ell[\zeta] \cong \mathbb{Z}_\ell[\text{Gal}(K/F)]/(1 + \tau + \cdots + \tau^{\ell-1})
\]

as the norm \( 1 + \tau + \cdots + \tau^{\ell-1} \) acts trivially on \( S_K \). Denote the discrete valuation ring \( \mathbb{Z}_\ell[\zeta] \) by \( R \); its maximal ideal is generated by \( \lambda = 1 - \zeta \). As an \( R \)-module, the \( \ell \)-class group \( S_K \) of \( K \) decomposes as

\[
S_K \cong \mathbb{Z}_\ell[\zeta]/(\lambda^{e_1}) \oplus \mathbb{Z}_\ell[\zeta]/(\lambda^{e_2}) \oplus \cdots \oplus \mathbb{Z}_\ell[\zeta]/(\lambda^{e_t})
\]

for some \( 1 \leq e_1 \leq e_2 \leq \cdots \leq e_t \). Let

\[
s_i := \{|e_j : e_j = i\}|
\]
so that \( t = s_1 + s_2 + \cdots + s_{l-2} \) and \( s_k = 0 \) for \( k > l - 2 \) since \((\lambda^{l-1}) = (l)\).

We have a decreasing filtration

\[ S_K \supset \lambda S_K \supset \lambda^2 S_K \supset \cdots \]

Denote by \( S_K[\lambda] \), the kernel of multiplication by \( \lambda \) on \( S_K \); note that \( t = \text{rank} S_K[\lambda] \). Similarly, it is easy to see that

\[ s_i = \text{rank} ((S_K[\lambda] \cap \lambda^{i-1} S_K + \lambda^i S_K) / \lambda^i S_K) \]

Also, the rank of the \( \mathbb{Z}[\lambda] \)-module \( \lambda^{i-1} S_K / \lambda^i S_K \) is \( t - s_1 - \cdots - s_{i-1} \) which is called the \( \lambda^i \)-rank of \( S_K \).

By class field theory, the maximal abelian unramified extension \( M_0 \) of \( K \) satisfies \( C_K \cong \text{Gal}(M_0/K) \). The genus field of \( K / F \) is the maximal abelian extension \( M \) of \( F \) which is contained in \( M_0 \); then \( \text{Gal}(M/F) \) is the abelianization of \( \text{Gal}(M_0/F) \). Moreover, \( C_K / \lambda C_K \cong \text{Gal}(M/K) \) and is called the group of genera.

An ideal class \( c \) in \( C_K \) is said to be ambiguous if \( \tau c = c \); that is, if \( c \in C_K[\lambda] \). Thus, the subgroup \( S_K[\lambda] \) of ambiguous ideal \( l \)-classes is an elementary abelian \( l \)-group whose rank is that of \( S_K / \lambda S_K \) (which we have denoted by \( t \) above). The rank \( t \) is computed using Hasse’s famous formula ([10] and [14]):

\[ t = d + q^* - (r + 1 + o) \]

where

- \( d \) = number of ramified primes in \( K / F \),
- \( r \) = rank of the free abelian part of the group of units \( E_F \) of \( F \),
- \( o = 1 \) or \( 0 \) according as to whether \( F \) contains primitive \( \ell \)th root of unity or not,
- \( q^* \) is defined by \([N_{K/F}(K^*) \cap E_F : N_{K/F}(E_F)] = \ell^{q^*}\).

More generally, let us define for each \( i \leq \ell \), \( S_{iK}^l \) to be the subgroup of ambiguous ideal classes in \( \lambda^{i-1} S_K \). Thus, \( \text{rank} S_{iK} = \text{rank} \lambda^{i-1} S_K / \lambda^i S_K \) which is the \( \lambda^i \)-rank of \( S_K \) (which we observed above to be \( t - s_1 - \cdots - s_{i-1} \)).

There is a subtler notion of strongly ambiguous ideals. An ambiguous ideal \( I \) is said to be strongly ambiguous if the principal ideal \((1 - \tau)I\) is actually \((1)\). There is also a related notion for ideal classes. An ideal class \( a \in C_K \) is said to be a strongly ambiguous ideal class if there exist a representative \( a \in I_K \) for \( a \) such that \((1 - \tau)a = (1)\).

The subgroup \( S_{iK,s} \) of strongly ambiguous ideal classes in \( S_K \) has rank given by a similar formula as above:

\[ \text{rank} S_{iK,s} = d + q - (r + 1 + o) \]

where \( q \) is given by \([N_{K/F}(E_K) \cap E_F : N_{K/F}(E_F)] = \ell^q\).
3. Cyclic extensions of degree $\ell$

In this section we give a formula for the rank of $S_K$, where $K/F$ is a Galois extension of odd prime degree $\ell$.

Throughout, we assume $S_F = \{1\}$.

The proof is an easy generalization of Theorems 3.1 and 4.1 of [3].

**Proposition 3.1.** Let $K$ be a cyclic extension of degree $\ell$ of a number field $F$ for which the $l$-class group $S_F = \{1\}$. Let us denote by $t$ the rank of the group of ambiguous ideal classes $S_K[\lambda]$ in $S_K$, and by $s_i$, the rank of $(\lambda^{i-1}S_K[\lambda] + \lambda^i S_K)/\lambda^i S$. Then

$$\text{rank} S_K = (\ell - 1)t - (\ell - 2)s_1 - \cdots - s_{\ell-2}.$$

Further, $S_K$ is isomorphic to the direct product of an elementary abelian $\ell$-groups of rank $s_1$ and an abelian $\ell$-group of rank

$$(\ell - 1)(t - s_1) - (\ell - 3)s_2 - \cdots - s_{\ell-2}.$$

**Proof.** For $R = \mathbb{Z}[\zeta]$, the $R$-module decomposition

$$S_K = \bigoplus_{i=1}^{l} R/\lambda^i R = \bigoplus (R/\lambda^i R)^{s_i}$$

where $1 \leq e_1 \leq \cdots \leq e_t$ and

$$s_i = |\{j : e_j = i\}|,$$

it follows that

$$\text{rank} S_K = \sum_i |\{j : e_j \geq i\}|$$

$$= t + (t - s_1) + (t - s_1 - s_2) + \cdots + (t - s_1 - s_2 - \cdots - s_{\ell-2})$$

$$= (\ell - 1)t - (\ell - 2)s_1 - (\ell - 3)s_2 - \cdots - s_{\ell-2}.$$

In order to get the direct sum decomposition, we consider the filtration

$$S_K \supset \lambda S_K \supset \cdots \supset \lambda^{l-1} S_K = lS_K$$

and the homomorphism

$$\lambda^i_* : \lambda^{i-1} S_K/\lambda^i S_K \to \lambda^i S_K/\lambda^{i+1} S_K$$

induced by multiplication by $\lambda$.

As $\lambda^{i-1} S_K/\lambda^i S_K$ are elementary abelian $\ell$-groups, they can be viewed as vector spaces over $\mathbb{F}_l$. Then $\lambda^i_*$ is a surjective, vector space homomorphism. Hence there exists groups $R_i, W_i$ such that

$$\lambda^i S_K \subset R_i, W_i \subset \lambda^{i-1} S_K$$
and so that $\lambda_i^*$ gives an isomorphism between $R_i/\lambda^i S_K$ and $\lambda^i S_K/\lambda^{i+1} S_K$.

Therefore, 

$$R_i + W_i = \lambda^{i-1} S_K$$

and $R_i \cap W_i = \lambda^i S_K$.

Clearly $W_i = (\lambda^{i-1} S_K)[\lambda] + \lambda^i S_K$ from the definition of $\lambda_i^*$.

So, there exists a subgroup $H_i \subset (\lambda^{i-1} S_K)[\lambda]$, such that

$$W_i = H_i \oplus \lambda^i S_K,$$

with $H_i \cong (\lambda^{i-1} S_K)[\lambda] + \lambda^i S_K / \lambda^i S_K$. Then

$$\lambda^{i-1} S_K = R_i + W_i = R_i + (H_i \oplus \lambda^i S_K) \cong R_i \oplus H_i$$

since $R_i \cap W_i = \lambda^i S_K$. In particular, for $i = 1$, we get,

$$S_K \cong R_1 \oplus H_1.$$

Recall that $s_i = \text{rank}(\lambda^{i-1} S_K[\lambda] + \lambda^i S_K) / \lambda^i S_K$; thus

$$s_i = \text{rank}H_i = \text{rank}W_i / \lambda^i S_K.$$

Thus, the proposition will follow if we can prove:

$$\text{rank}R_1 = (\ell - 1)(t - s_1) - (\ell - 3)s_2 - (\ell - 4)s_3 - \cdots - s_{\ell-2}.$$  

Since $\ell H_1 = \{1\}$ and $\ell S_K = \lambda^{\ell-1} S_K$, we have:

$$\text{rank}R_1 = \text{rank}R_1 / \ell R_1 = \text{rank}R_1 / \ell S_K = \text{rank}R_1 / \lambda^{\ell-1} S_K$$

$$= \text{rank}R_1 / \lambda S_K + \text{rank}\lambda S_K / \lambda^2 S_K + \cdots + \text{rank}\lambda^{\ell-2} S_K / \lambda^{\ell-1} S_K$$

$$= 2 \cdot \text{rank}R_1 / \lambda S_K + \text{rank}R_2 / \lambda^2 S_K + \cdots + \text{rank}R_{\ell-2} / \lambda^{\ell-2} S_K,$$

since $R_i / \lambda^i S_K \cong \lambda^i S_K / \lambda^{i+1} S_K$.

Now,

$$\text{rank}R_1 / \lambda S_K = \text{rank}S_K / \lambda S_K - \text{rank}W_1 / \lambda S_K = t - s_1.$$

Similarly,

$$\text{rank}R_1 / \lambda^i S_K = \text{rank}\lambda^{i-1} S_K / \lambda^i S_K - \text{rank}W_i / \lambda^i S_K$$

$$= \text{rank}R_{i-1} / \lambda^{i-1} S_K - s_i = t - s_1 - s_2 - \cdots - s_i.$$

Putting all of these together, we get

$$\text{rank}R_1 = (\ell - 1)(t - s_1) - (\ell - 3)s_2 - (\ell - 4)s_3 - \cdots - s_{\ell-2}$$

and

$$\text{rank}S_K = (\ell - 1)t - (\ell - 2)s_1 - (\ell - 3)s_2 - \cdots - s_{\ell-2}. \quad \square$$
Remark. We saw in the beginning of the proof above that from the decomposition $S_K \cong R/\lambda R \times \cdots \times R/\lambda R$, where $R = \mathbb{Z}[\zeta]$ and $\lambda = 1 - \zeta$, one can easily find the formula of the rank by simple counting. We have given the above proof as some ingredients of the proof like the subgroups $R_i$ and $W_i$ will be used later in the construction of genus fields.

We point out the following special cases of interest; the first corollary below is immediate:

**Corollary 3.2.** If $t = s_1$, then $S_K$ is an elementary abelian $\ell$ group of rank $t$.

**Corollary 3.3.** For $i \geq 1$, we have

$$\text{rank} \lambda^i S_K / \lambda^{i+1} S_K = t - s_1 - \cdots - s_i.$$  

In particular, $t - s_1 - \cdots - s_i \geq 0$ for all $i$ and so, we observe

$$0 \leq s_i \leq t - s_1 - \cdots - s_{i-1}.$$  

*Proof.* The proof of this corollary is contained in the proof of the Proposition 3.1.

**Corollary 3.4.** For some $1 \leq i \leq (\ell - 2)$, if we have $\lambda^i S_K = lS_K$, then $s_j = 0$ for $j \geq i + 1$ and $t = s_1 + \cdots + s_i$.

*Proof.* Since $\lambda^i S_K^\lambda = lS_K$, we see that

$$\lambda^i S_K = \lambda^{i+1} S_K = \cdots = \lambda^l S_K = lS_K.$$  

So, the quotients $\lambda^i S_K / \lambda^{i+1} S_K$ are trivial for all $j \geq i$. The previous corollary implies the assertion now.

**Corollary 3.5.** The rank of $S_K$ satisfies the bounds

$$2t - s_1 \leq \text{rank} S_K \leq (\ell - 1)t - (\ell - 2)s_1.$$  

Moreover, if $s_2 = t - s_1$, then the lower bound is achieved; that is, rank of $S_K$ equals $2t - s_1$. Further, if $s_2 = s_3 = \cdots = s_{\ell - 2} = 0$, then the upper bound is achieved, that is, rank of $S_K$ is $(\ell - 1)t - (\ell - 2)s_1$.

*Proof.* The upper bound of rank $S_K$ is immediate from the proposition because $\text{rank} S_K = (l - 1)t - (l - 2)s_1 - \cdots - s_{l-2}$. The lower bound follows since $\text{rank} S_K = t + \sum_{i=1}^{l-2} (t - s_1 - \cdots - s_i) \geq 2t - s_1$ (since $t - s_1 - \cdots - s_i \geq 0$). Combining these two facts we obtain the bound for rank of $S_K$.

Since $t - s_1 - s_2 = 0$, we see that $s_3 = s_4 = \cdots = s_{l-2} = 0$ (follows from Corollary 3.3). Substituting these values of $s_i$ in the formula for the rank of $S_K$ in Theorem 3.1, we obtain that, $\text{rank} S_K = 2t - s_1$.  

$\square$
Remark. The above bounds constitute an improvement of the bounds obtained in Gerth’s paper [3][Corollary 2.5]; he obtains $t \leq \text{rank} S_K \leq (\ell - 1)t$.

4. When $F$ contains $\zeta_\ell$ and has class number coprime to $\ell$

We recall the earlier notations:

$K$ is a cyclic extension of degree $\ell$ (an odd prime) over a number field $F$ with trivial $\ell$-class group which, we now assume, contains a primitive $\ell$-th roots of unity $\zeta$. By class field theory, the maximal abelian unramified extension $M_0$ of $K$ satisfies $C_K \cong \text{Gal}(M_0/K)$. The genus field of $K/F$ is the maximal abelian extension $M$ of $F$ which is contained in $M_0$; then $\text{Gal}(M/F)$ is the abelianization of $\text{Gal}(M_0/F)$ (see [8]). Moreover, $C_K/\lambda C_K \cong \text{Gal}(M/K)$ and is called the group of genera. By Kummer theory, $K = F(x^{1/\ell})$ for some $x \in F^* - (F^*)^\ell$. Being the $\ell$-Sylow subgroup of the group $C_K/\lambda C_K$, the group $S_K/\lambda S_K$ is a direct summand of it. Thus, there is a unique subfield $M_1$ of $M$ which contains $K$ and satisfies $S_K/\lambda S_K \cong \text{Gal}(M_1/K)$; thus, note that $\text{Gal}(M_1/K)$ is elementary abelian of rank $t$.

Recall also from the proof of 3.1 that for $i \geq 1$, there is a subgroup $H_i \subset (\lambda^{i-1}S_k)[\lambda]$ such that $H_i \cap \lambda^i S_K = (0)$ and $H_i \cong ((\lambda^{i-1}S_k)[\lambda] + \lambda^i S_K)/\lambda^i S_K$. Note that $s_i = \text{rank} H_i$ for $i \geq 1$.

The first theorem below computes the rank $s_1$ of $H_1$ in terms of the rank of a certain matrix with entries in $\mathbb{F}_l$.

Firstly, by Kummer theory, there exist $x_1, \ldots, x_t \in K^* - (K^*)^\ell$ such that $M_1 = K(x_1^{1/\ell}, \ldots, x_t^{1/\ell})$. In the following theorem, we obtain a $t \times t$ matrix over $\mathbb{F}_l$ whose rank equals $s_1$. The entries of this matrix involve the Artin symbols of the generators $x_i$’s.

Note that the Artin symbols $\left(\frac{K(x_i^{1/\ell})}{K}\right)$ are defined for any ideal $I$ of $K$ since the conductor of the field $M_1$ is trivial.

**Theorem 4.1.** Let $F, K, M, M_1$ be as above. Fix representative ideals $\alpha_1, \ldots, \alpha_t$ whose ideal classes form a basis for the group $S_K[\lambda]$. Denote by $\mu_{ij}$, the Artin symbol $\left(\frac{K(x_i^{1/\ell})}{\alpha_j}\right)$. Write $\alpha_{ij} \in \mathbb{F}_l$ for which $\zeta^{\alpha_{ij}}$ is the power residue symbol $(x_i^{1/\ell})^{\mu_{ij} - 1}$. If $A_1$ is the matrix $(\alpha_{ij}) \in M_t(\mathbb{F}_l)$, then

$$\text{rank} A_1 = \text{rank} H_1 = s_1.$$

**Proof.** As noted above, since $M$ is an unramified extension of $K$ and $K \subset M_1 \subset M$, the conductor of $M_1/K$ is trivial and hence, the Artin symbol $\left(\frac{M_1/K}{\alpha}\right) \in \text{Gal}(M_1/K)$ is well defined for all ideals $\alpha$ of $K$. We define a map
\[ \psi_1 : S_K[\lambda] \to S_K \to S_K/\lambda S_K \cong \text{Gal}(M_1/K) \]

which is the composite of the natural inclusion, the natural surjection and the canonical isomorphism. If \( cl(a) \) denotes the ideal class of an ideal \( a \), and if \( cl(a) \in S_K[\lambda] \), then we see by Artin reciprocity that \( \psi_1(cl(a)) = \left( \frac{M_1}{K} \right) \frac{a}{a} \) and that the kernel of \( \psi_1 \) is \( S_K[\lambda] \cap \lambda S_K \).

Now \( M_1 = K(x_1^{\frac{1}{\ell}}, \ldots, x_t^{\frac{1}{\ell}}) \) and \([M_1 : K] = \ell^t\) imply that there exists an isomorphism

\[ \delta_1 : \text{Gal}(M_1/K) \cong \text{Gal}(K(x_1^{\frac{1}{\ell}})/K) \times \cdots \times \text{Gal}(K(x_t^{\frac{1}{\ell}})/K). \]

For each \( i = 1, \ldots, t \), Kummer theory provides an isomorphism

\[ \theta_i : \text{Gal}(K(x_i^{\frac{1}{\ell}})/K) \to \mathbb{F}_\ell, \mu \mapsto a_\mu \]

where \( \zeta a_\mu = (x_i^{\frac{1}{\ell}})^{\mu-1} \).

Define

\[ \phi_1 := \left( \prod_{i=1}^t \theta_i \right) \circ \delta_1 \circ \psi_1 : S_K[\lambda] \to \mathbb{F}_\ell. \]

Now, \( S_K[\lambda] \) is a vector space over \( \mathbb{F}_\ell \) (as it is an elementary abelian \( \ell \)-group) and \( \phi_1 \) is a vector space homomorphism; also \( \ker \phi_1 = \ker \psi_1 = S_K[\lambda] \cap \lambda S_K \).

Now \( A_1 \) is precisely the matrix of \( \phi_1 \) with respect to basis \([cl(a_1), \ldots, cl(a_t)]\) of \( S_K[\lambda] \). Then

\[ \text{rank}(S_K[\lambda] \cap \lambda S_K) = \text{rank}(\ker(\phi_1)) = t - \text{rank}A_1. \]

Equivalently, \( \text{rank}A_1 = t - \text{rank}(S_K[\lambda] \cap \lambda S_K) \). Since \( S_K[\lambda] \) is an elementary abelian \( \ell \)-group of rank \( t \) and

\[ H_1 \cong (S_K[\lambda] + \lambda S_K)/\lambda S_K \cong S_K[\lambda]/(S_K[\lambda] \cap \lambda S_K), \]

then \( s_1 = \text{rank}H_1 = t - \text{rank}(S_K[\lambda] \cap \lambda S_K) = \text{rank}A_1. \)

The above result for the rank \( s_1 \) of \( H_1 \) can be generalized to a general \( s_i \) in the following manner.

Recall from the proof of Proposition 3.1 that there exists a subgroup \( R_i \) satisfying \( \lambda^i \subset R_i \subset \lambda^{i-1}S_K \) and

\[ R_i/\lambda^i S_K \cong \lambda^{i-1}S_K/W_i \cong \lambda^i S_K/\lambda^{i+1}S_K \]

where the last isomorphism is induced by the multiplication-by-\( \lambda \) map.
Let $\psi$ see that $\lambda$-

\[ K \subset M_{i+1} \subset M_i \subset M_1 \subset M \]

and

\[ \text{Gal}(M_{i+1}/K) \cong R_i/\lambda^i S_K \cong \lambda^i S_K/\lambda^{i+1} S_K. \]

From the above isomorphism, we see that Gal$(M_{i+1}/K)$ is an elementary abelian $\ell$-group. We have

\[ t-s_1-\cdots-s_i = \text{rank}\ \text{Gal}(M_{i+1}/K) = \text{rank}\lambda^i S_K/\lambda^{i+1} S_K. \]

Once again, Kummer theory assures us elements $y_1, \ldots, y_{t-s_1-\cdots-s_i} \in K^{*} - (K^{*})^{1}$ such that

\[ M_{i+1} = K\left(y_1^{\frac{1}{\lambda}}, \ldots, y_{t-s_1-\cdots-s_i}^{\frac{1}{\lambda}}\right). \]

Fix representative ideals $b_1, \ldots, b_{t-s_1-\cdots-s_i}$ whose ideal classes form a basis for the group $(\lambda^i S_K)[\lambda]$. With these notations, we prove the following theorem:

**Theorem 4.2.** Let $\mu_{jk}$ denote the Artin symbol \( \left( \frac{K(y_j^{\frac{1}{\lambda}})/K}{b_k} \right) \), and let $\beta_{jk} \in \mathbb{F}_l$ for which $\zeta^{\beta_{jk}}$ is the power residue symbol $(y_j^{\frac{1}{\lambda}})^{\mu_{jk}^{-1}}$. For $1 \leq i \leq l-3$, if $A_{i+1}$ is the matrix $(\beta_{jk})$, $1 \leq j, k \leq t-s_1-\cdots-s_i$ with entries in $\mathbb{F}_l$, then

\[ s_{i+1} = \text{rank} A_{i+1}. \]

**Proof.** Since $M$ is an unramified extension of $K$ and $K \subset M_{i+1} \subset M$, the conductor of $M_{i+1}/K$ is (1) and hence the Artin symbol \( \left( \frac{M_{i+1}/K}{\alpha} \right) \in \text{Gal}(M_{i+1}/K) \) is well defined for all ideals $\alpha$ of $K$. We define a map

\[ \psi_{i+1} : (\lambda^i S_K)[\lambda] \to \lambda^i S_K \to \lambda^i S_K/\lambda^{i+1} S_K \cong R_i/\lambda^i S_K \cong \text{Gal}(M_{i+1}/K) \]

which is the composite of the natural inclusion, the natural surjection and the canonical isomorphisms. If $c(l)(\alpha) \in (\lambda^i S_K)[\lambda]$, then by Artin reciprocity, we see that $\psi_{i+1}(c(l)(\alpha)) = \left( \frac{M_{i+1}/K}{\alpha} \right)$ and that the kernel of $\psi_{i+1}$ is $(\lambda^i S_K)[\lambda] \cap \lambda^{i+1} S_K$.

Now $M_{i+1} = K(y_1^{\frac{1}{\lambda}}, \ldots, y_{t-s_1-\cdots-s_i}^{\frac{1}{\lambda}})$ and $[M_{i+1} : K] = \ell^{t-s_1-\cdots-s_i}$ imply that there exists an isomorphism

\[ \delta_{i+1} : \text{Gal}(M_{i+1}/K) \cong \text{Gal}(K(y_1^{\frac{1}{\lambda}})/K) \times \cdots \times \text{Gal}(K(y_{t-s_1-\cdots-s_i}^{\frac{1}{\lambda}})/K). \]

Once again, Kummer theory provides for each $j \leq t-s_1-\cdots-s_i$, an isomorphism

\[ \alpha_j : \text{Gal}(M_{i+1}/K) \cong \text{Gal}(K(y_j^{\frac{1}{\lambda}})/K). \]
\[ \theta_j : \text{Gal} \left( K(y_j^{\ell})/K \right) \to \mathbb{F}_\ell \]
\[ \mu \mapsto \alpha_\mu \]

where \( \zeta_\alpha \mu = (y_j^{\ell})^{\mu-1} \).

Define
\[ \phi_{i+1} := \left( \prod_{j=1}^{t-s_1-s_i} \theta_j \right) \circ \delta_{i+1} \circ \psi_{i+1} : (\lambda^i S_K)[\lambda] \to \mathbb{F}_\ell^{t-s_1-s_i} \cdot \]

Since \((\lambda^i S_K)[\lambda]\) is an elementary abelian \( \ell \)-group, it may be viewed as a vector space over \( \mathbb{F}_\ell \), and \( \phi_{i+1} \) is a vector space homomorphism. Since
\[ \ker \phi_{i+1} = \ker \psi_{i+1} = (\lambda^i S_K)[\lambda] \cap \lambda^{i+1} S_K \]
and since \( A_{i+1} \) is precisely the matrix of \( \phi_{i+1} \) with respect to the basis \( \{ cl(b_1), \ldots, cl(b_{t-s_1-s_i}) \} \), we have
\[ \text{rank}((\lambda^i S_K)[\lambda] \cap \lambda^{i+1} S_K) = \text{rank}(\ker(\phi_{i+1})) = (t-s_1-s_i) - \text{rank} A_{i+1} \]

Equivalently, \( \text{rank} A_{i+1} = (t-s_1-s_i) - \text{rank}((\lambda^i S_K)[\lambda] \cap \lambda^{i+1} S_K) \).

Since \((\lambda^i S_K)[\lambda]\) is an elementary abelian \( \ell \)-group of rank \((t-s_1-s_i)\) and
\[ (\lambda^i S_K)[\lambda] \cap \lambda^{i+1} S_K \cong (\lambda^i S_K)[\lambda]/(\lambda^i S_K)[\lambda] \cap \lambda^{i+1} S_K \cong H_{i+1}, \]
we obtain
\[ s_{i+1} = \text{rank} H_{i+1} = (t-s_1-s_i) - \text{rank}((\lambda^i S_K)[\lambda] \cap \lambda^{i+1} S_K) \]
\[ = \text{rank} A_{i+1}. \quad \square \]

5. \( F = \mathbb{Q}(\zeta_5) \) and \( K = F(x^{1/5}) \)

In the last section, we showed that the rank of \( S_K \) can be expressed in terms of the ranks of certain matrices over \( \mathbb{F}_\ell \). The explicit determination of these matrices seems very difficult in general. Gerth had carried this out in the case of \( \ell = 3 \). In this section, we look at the case of \( \ell = 5 \). We assume in this section that \( F \) is the cyclotomic field \( \mathbb{Q}(\zeta) \) generated by the 5-th roots of unity; note that \( F \) has class number 1. We analyze what the earlier theorems give for several examples and compare them with computations obtained by the program SAGE (the latter uses GRH) - a detailed table is given at the end of the paper. After that, we exploit the theorems of the previous section to
prove a number of general results which were guessed at by a close inspection of the tables.

Consider any cyclic extension $K = F(x^{1/5})$ of degree 5 over $F$. We may assume that $x$ is an integer in $F$ which is not divisible by the $5^{th}$ power of any prime element of $F$.

The ring of integers $\mathbb{Z}[\zeta]$ of $F$ is a principal ideal domain. Consider those nonzero elements $x$ which can be written as

$$x = u\lambda^{e_1} \pi_1^{e_1} \cdots \pi_g^{e_g},$$

where $u$ is a unit in $\mathbb{Z}[\zeta]$, $\lambda = 1 - \zeta$ is the unique prime over 5 (so, $\lambda^4 \mid 5$), and $\pi_1, \ldots, \pi_g$ are prime elements in $F$ not associated to $\lambda$, where $e_i \in \{1, \ldots, 4\}$ for $1 \leq i \leq g$, and $e_\lambda \in \{0, 1, \ldots, 4\}$.

5.1 Unwinding Hasse’s formula for $\mathbb{Q}(\zeta, x^{1/5})$

Let us see how the rank $t$ of the group of ambiguous ideal classes in the 5-class group $\Delta_K$ is computed using Hasse’s famous formula ([10]) in our case:

$$t = d + q^* - (r + 1 + o).$$

For our fields $F$ and $K$, we have

$$r = \frac{\ell - 3}{2} = 1,$$

$$o = 1,$$

$$d = \begin{cases} g & \text{if } (\lambda) \text{ does not ramify in } K/F, \\
    g + 1 & \text{if } (\lambda) \text{ ramifies in } K/F, \end{cases}$$

$$q^* \leq \frac{\ell - 1}{2} = 2, \quad \text{(since the order of } [E_F : E_F^\ell] = \ell^2 = 5^2)$$

In $F$, the group of units is generated by $\zeta$ and $1 + \zeta$ where $\zeta$ is a primitive 5-th root of unity. We see from the definition of $q^*$ that

$$q^* = \begin{cases} 2 & \text{if } \zeta, 1 + \zeta \in N_{K/F}(K^*), \\
    1 & \text{if some, but not all } \zeta^i(1 + \zeta)^j \in N_{K/F}(K^*), \\
    0 & \text{if } \zeta^i(1 + \zeta)^j \notin N_{K/F}(K^*), \text{ for } 0 \leq i, j \leq 4, i + j \neq 0. \end{cases}$$

We have $t = d - 3 + q^*$ with $d, q^*$ determined as above.

Since $q^*$ depends on whether $\zeta^i(1 + \zeta)^j$ is a norm from $K$ or not, its value can be determined in terms of the local Hilbert symbols in completions of $F$ as in the following lemma.
Lemma 5.1. Let $F = \mathbb{Q}(\zeta)$ and let $K = F(x^{1/5})$ where $x = u\lambda^{e_1}\pi_1^{e_1}\cdots\pi_g^{e_g}$, with $u$ a unit in $\mathbb{Z}[\zeta]$, $\lambda = 1 - \zeta$ is the unique prime over $\ell$ (so, $\lambda^5|5$), and $\pi_1, \ldots, \pi_g$ prime elements in $\mathbb{Z}[\zeta]$. Then

(a) $\zeta \in N_{K/F}(K^*) \iff N_{F/\mathbb{Q}}((\pi_i)) \equiv 1 \pmod{25}$ for all $i$;
(b) if $\zeta^i((1 + \zeta)^j) \in N_{K/F}(K^*)$, if and only if, every $\pi_j | x$ above has the property that $\zeta^i((1 + \zeta)^j)$ is a 5-th power modulo $(\pi_j)$ in $\mathbb{Z}[\zeta]$ for all $i, j$;
(c) $(\lambda)$ ramifies in $K/F$ $\iff x \not\equiv \pm 1, \pm 7 \pmod{\lambda^5}$.

Proof. Now $\zeta^i((1 + \zeta)^j) \in N_{K/F}(K^*) \iff \left(\frac{x_\zeta^i((1 + \zeta)^j)}{\pi_j}\right) = 1$ for all prime ideals $\pi$ of $F$.

Since $\zeta^i((1 + \zeta)^j)$ is a unit, $\left(\frac{x_\zeta^i((1 + \zeta)^j)}{p}\right) = 1$ if $p$ does not ramify in $K/F$.

We will now look at the prime ideals $(\lambda)$ and the $(\pi_k)$'s.

Firstly, look at $p = (\pi_k)$, where $\pi_k | x$. Then

\[
\left(\frac{x_\zeta^i((1 + \zeta)^j)}{(\pi_k)}\right) = \left(\frac{u\lambda^{e_1}\pi_1^{e_1}\cdots\pi_g^{e_g}}{(\pi_k)}\right) \left(\frac{\zeta^i((1 + \zeta)^j)}{(\pi_k)}\right) \times \cdots \times \left(\frac{\pi_k^{e_k}}{(\pi_k)}\right) = \left(\frac{\pi_k, \zeta^i((1 + \zeta)^j)}{(\pi_k)}\right)^{e_k} = 1 \iff \left(\frac{\pi_k, \zeta^i((1 + \zeta)^j)}{(\pi_k)}\right) = 1 \iff \left(\frac{\zeta^i((1 + \zeta)^j)}{(\pi_k)}\right) = 1.
\]

The last equality is equivalent to the conditions

$\pi_k$ splits completely in $F((\zeta^i((1 + \zeta)^j)/5)/F$.

Since the last condition holds if and only if $\zeta^i((1 + \zeta)^j) \equiv a^5 \pmod{(\pi_k)}$ for some $a \in \mathbb{Z}[\zeta]$ ([11][Theorem 118]), the necessity assertion in (b) for $\zeta^i((1 + \zeta)^j)$ to be a norm follows.

The converse assertion follows by the product law since $\left(\frac{x_\zeta^i((1 + \zeta)^j)}{\pi_k}\right) = 1$ for all $\pi_k | x$ implies $\left(\frac{x_\zeta^i((1 + \zeta)^j)}{(\pi_k)}\right) = 1$ and hence, $\zeta^i((1 + \zeta)^j) \in N_{K/F}(K^*)$.

To deduce (a) from (b), we note that, in particular, $\zeta \in N_{K/F}(K^*)$ if and only if, all $\pi_j$ splits completely in $F((\zeta^i)/F$, which is equivalent to the condition, $N_{F/\mathbb{Q}}((\pi_i)) \equiv 1 \pmod{25}$, for all $i$. 

---

I-Class groups of cyclic extensions of prime degree $l$
Finally (c) follows from ([11][Theorem 119]) which shows that \((\lambda)\) ramifies in \(K/F\) iff \(x \not\equiv \pm 1, \pm 7 \pmod{\lambda^5}\).

From the above lemma, we may immediately formulate the following proposition.

**Proposition 5.2.** Let \(F = \mathbb{Q}(\zeta)\) and \(K = F(x^{\frac{1}{5}})\) of degree 5 as above. Write \(x = u\lambda^{e_1}\pi_1^{e_1}\cdots\pi_g^{e_g}\), \(\lambda = 1 - \zeta\), each \(\pi_i \in F\) is a prime element, \(e_i \in \{1, 2, 3, 4\}\) for \(1 \leq i \leq g\). Let \(d \in \{0, 1, 2, 3\}\) as before. Let \(d\) denote the number of primes that ramify in \(K/F\). Then the rank \(t\) of the group of ambiguous ideal classes in \(S_K\) is given by:

\[-d + 1, -d + 2, -d + 3\]

respective as to the following three situations:

I: each \(\pi_k\) divides \(x\) has the property that both \(\zeta\) and \(1 + \zeta\) are 5-th powers modulo \((\pi_k)\) in \(\mathbb{Z}[\zeta]\);

II: each \(\pi_k\) divides \(x\) has the property that some, but not all \(\zeta^i(1 + \zeta)^j\) is a 5-th power modulo \((\pi_k)\) in \(\mathbb{Z}[\zeta]\);

III: some \(\pi_k\) divides \(x\) has the property that none of the \(\zeta^i(1 + \zeta)^j\) is a 5-th power modulo \((\pi_k)\) in \(\mathbb{Z}[\zeta]\).

These are further simplified to the expressions \(t = g, g - 1, g - 2\) according as to the respective conditions A, B, C, D:

A: \(x \not\equiv \pm 1, \pm 7 \pmod{\lambda^5}\) and each \(\pi_k\) divides \(x\) has the property that both \(\zeta\) and \(1 + \zeta\) are 5-th powers modulo \((\pi_k)\) in \(\mathbb{Z}[\zeta]\);

B: \(x \equiv \pm 1, \pm 7 \pmod{\lambda^5}\) and each \(\pi_k\) divides \(x\) has the property that both \(\zeta\) and \(1 + \zeta\) are 5-th powers modulo \((\pi_k)\) in \(\mathbb{Z}[\zeta]\);

OR

C: \(x \not\equiv \pm 1, \pm 7 \pmod{\lambda^5}\) and some \(\pi_k\) divides \(x\) has the property that none of the \(\zeta^i(1 + \zeta)^j\) is a 5-th power modulo \((\pi_k)\) in \(\mathbb{Z}[\zeta]\);

OR

D: \(x \equiv \pm 1, \pm 7 \pmod{\lambda^5}\) and some \(\pi_k\) divides \(x\) has the property that none of the \(\zeta^i(1 + \zeta)^j\) is a 5-th power modulo \((\pi_k)\) in \(\mathbb{Z}[\zeta]\).

5.2 Examples

We demonstrate the above results by means of some examples. In each case, the conclusion is confirmed by a SAGE program (which is known to be valid under GRH); see table 1 compiled in section 5.5.
Example 5.3. We consider $K = \mathbb{Q}(\zeta, 7^\frac{1}{4})$. We observe that $\zeta \in N_{K/F}(K^*)$, and $(1 + \zeta) \equiv (2 + 4\zeta^3)^3 \pmod{7}$. Hence $q^* = 2$, and $t = g - 1 = 0$. Thus, $S_K$ must be trivial by our result.

Example 5.4. Let $K = \mathbb{Q}(\zeta, 18^\frac{1}{4})$. Notice that in this case $\zeta \notin N_{K/F}(K^*)$. We observe that,

$$\zeta^2(1 + \zeta) \equiv (1 + \zeta^2)^5 \pmod{2},$$

$$\zeta^2(1 + \zeta) \equiv (-1 - \zeta)^5 \pmod{3}.$$ 

Hence $q^* = 1$ and $t = g - 2 = 0$. Thus, $S_K = \{1\}$ from our result.

Example 5.5. Let $K = \mathbb{Q}(\zeta, 11^\frac{1}{4})$. Note that in $F = \mathbb{Q}(\zeta_5)$, $11 = \pi_1\pi_2\pi_3\pi_4$, with $\pi_1 = (\zeta^3 + 2\zeta^2 + \zeta + 2) = (\zeta + 2), \pi_2 = (-\zeta^2 + \zeta + 1), \pi_3 = (\zeta^3 - \zeta + 1), \pi_4 = (-2\zeta^3 - \zeta^2 - \zeta) = (2\zeta^2 + \zeta + 1)$. Thus in this case, $g = 4$.

Next, we note that $\zeta \equiv -2 \pmod{(\zeta + 2)}$ is not a $5^{th}$ power in $\mathbb{Z}[\zeta]$, because if it is a $5^{th}$ power modulo $(\zeta + 2)$, then $11|(n^5 + 2)$, for some integer $n \in \mathbb{Z}$, which is not true.

We also notice that $\zeta \equiv x^5 \pmod{(-\zeta^2 + \zeta + 1)}$, because if so, then we have modulo $-\zeta^2 + \zeta + 1$,

$$\zeta \equiv (a + b\zeta)^5 \equiv (a^5 + b^5 + 10a^3b^2 + 10a^2b^3 + 10ab^4) + 5ab(a^3 + 2a^2b + 4ab^2 + 3b^3)\zeta.$$ 

Next we note that, for $1 \leq i \leq 4$, we have,

$$(1 + \zeta)^i \equiv \zeta^{2i} \pmod{(-\zeta^2 + \zeta + 1)}.$$ 

Hence $(1 + \zeta)^i$ is not a $5^{th}$ power modulo $(-\zeta^2 + \zeta + 1)$.

Next for $1 \leq i \leq 4, 0 \leq j \leq 4$, we see that,

$$\zeta^i(1 + \zeta)^j \equiv (-1)^i\zeta^{i} \pmod{(\zeta + 2)}.$$ 

Hence, $\zeta^i(1 + \zeta)^j$ is not a $5^{th}$ power modulo $(\zeta + 2)$.

So in this case we have $q^* = 0$ and $t = g - 2 = 2$. So rank $S_K \geq 2$ by our result.

Example 5.6. Let $K = \mathbb{Q}(\zeta, 19^\frac{1}{4})$. Note that in $F = \mathbb{Q}(\zeta_5)$, $19 = \pi_1\pi_2$, with $\pi_1 = (3 + 4\zeta^2 + 4\zeta^3), \pi_2 = (-1 - 4\zeta^2 - 4\zeta^3)$. Notice that in this case, $\zeta \notin N_{K/F}(K^*)$. We observe that,

$$-\zeta^2(1 + \zeta) \equiv 3^5 \pmod{\pi_1},$$

$$-\zeta^2(1 + \zeta) \equiv 6^5 \pmod{\pi_2}.$$ 

Hence $q^* = 1$ and $t = g - 1 = 1$. So $1 \leq \text{rank } S_K \leq 4$ by our result.
Example 5.7. Let $K = \mathbb{Q}(\zeta, 42^{\frac{1}{5}})$. Notice that in this case $\zeta \notin N_{K/F}(K^*)$.

From Examples 5.2 and 5.3, we see that $\zeta^2(1 + \zeta) \in N_{K/F}(K^*)$.

Hence $q = 1$ and $t = g - 1 = 2$. Thus, $2 \leq \text{rank} S_K \leq 8$ from our result.

5.3 Constructing genus fields

We want to find elements $x_1, \ldots, x_t \in K$ such that the genus field $M_1 = K(x_1^{\frac{1}{5}}, \ldots, x_t^{\frac{1}{5}})$.

In the following proposition, we restrict our attention only to those elements $x$ for which each $\pi$ that divides $x$ is of the form $\pi \equiv a \pmod{5\mathbb{Z}[\zeta]}$ for some $a \in \{1, 2, 3, 4\}$.

Proposition 5.8. Let $F = \mathbb{Q}(\zeta)$, and let $K = F(x^{\frac{1}{5}})$ be cyclic of degree 5 as above. Writing $x = u^{\lambda^e_1} \pi_1^{e_1} \cdots \pi_f^{e_f} \pi_{f+1}^{e_{f+1}} \cdots \pi_g^{e_g}$,

where each $\pi_i \equiv \pm 1, \pm 7 \pmod{\lambda^5}$, for $1 \leq i \leq f$, and $\pi_j \not\equiv \pm 1, \pm 7 \pmod{\lambda^5}$, for $f + 1 \leq j \leq g$.

Then, we have:

(i) there exist $h_i \in \{1, 2, 3, 4\}$ such that $\pi_{f+1}^{h_i} \equiv \pm 1, \pm 7 \pmod{\lambda^5}$, for $f + 2 \leq i \leq g$;

(ii) if $\lambda$ ramifies in $K/F$ and each $\pi_k | x$ has the property that some, but not all $\zeta^i(1 + \zeta)^j$ are 5-th powers modulo $(\pi_k)$ in $\mathbb{Z}[\zeta]$, then the genus field $M_1$ is given as

$$M_1 = K(\pi_1^{\frac{1}{5}}, \ldots, \pi_f^{\frac{1}{5}}, (\pi_{f+1}^{h_{f+1}})^{\frac{1}{5}}, \ldots, (\pi_g^{h_g})^{\frac{1}{5}})$$ (1)

where $h_i \in \{1, 2, 3, 4\}$ is chosen as in (i);

(iii) in the other cases, the the genus field $M_1$ is given similarly by deleting an appropriate number of 5th roots from the right-hand side of the equation (1).

Proof. The proof of (i) is straightforward and we proceed to prove (ii).

Suppose first that $\lambda$ ramifies in $K/F$ and that for each $\pi_k | x$, some (but not all) $\zeta^i(1 + \zeta)^j$ are 5-th powers modulo $(\pi_k)$ in $\mathbb{Z}[\zeta]$. Let $M_1'$ denote the field given on the right-hand side of equation (1); we shall prove that $M_1'$ is the genus field $M_1$ of degree 5' over $K$ which corresponds to $S_K / \lambda S_K$. Note that, by the previous proposition, the number of 5th roots in this expression is $t$. Next, we note that only $\pi_i$ ramifies in $F(\pi_i^{\frac{1}{5}})/F$ for $1 \leq i \leq f$, and that
only the primes \( \pi_i \) and \( \pi_{f+1} \) ramify in \( F((\pi_{f+1}\pi_i^{h_i})^{\frac{1}{5}}) / F \) for \( f+2 \leq i \leq g \). Hence, each of the fields

\[
F(\pi_1^{\frac{1}{5}}), \ldots, F(\pi_f^{\frac{1}{5}}), F((\pi_{f+1}\pi_1^{h_1})^{\frac{1}{5}}), \ldots, F((\pi_{f+1}\pi_g^{h_g})^{\frac{1}{5}}), F(x^{\frac{1}{5}})
\]
is linearly disjoint from the composite of the other fields. Thus,

\[
[F(\pi_1^{\frac{1}{5}}, \ldots, \pi_f^{\frac{1}{5}}, (\pi_{f+1}\pi_1^{h_1})^{\frac{1}{5}}, \ldots, (\pi_{f+1}\pi_g^{h_g})^{\frac{1}{5}}, x^{\frac{1}{5}}) : F] = S_f^{l+1}.
\]

This implies \([M'_1 : K] = S_f \). As \([M_1 : K] = S_f \), we will have \( M'_1 = M_1 \) if we can show that \( M'_1 \subseteq M_1 \). Now, by definition, \( M_1 \) is the maximal abelian extension of \( F \) contained in the Hilbert class field of \( K \). Since \( M'_1 \) is a composite of linearly disjoint abelian extensions, it is an abelian extension of \( F \). Therefore, to show \( M'_1 = M_1 \), it suffices to show that \( M'_1 \) is unramified over \( K \). But, this is true because each \( (\pi_i) \) is \( 5^{th} \) power of an ideal in \( K \), \( \pi_i \equiv \pm 1, \pm 7 \pmod{\lambda^3} \) for \( 1 \leq i \leq f \) and \( \pi_{f+1}\pi_i^{h_i} \equiv \pm 1, \pm 7 \pmod{\lambda^3} \) for \( f+2 \leq i \leq g \).

Thus, we have proved (ii).

The remaining case (iii) is handled completely similarly; we just need to delete an appropriate number of any \( 5^{th} \) roots from the right-hand side of the equation (1).

\[ \square \]

**Corollary 5.9.** Let \( F, K, x \) be as in the proposition. Further, suppose the genus field \( M_1 \) of \( K / F \) is described as in the proposition. Then, for \( i = 1, 2 \), the genus fields \( M_{i+1} \) are obtained recursively by deleting \( s_i \) generators of the field \( M_i \).

**Proof.** We have \([M_i : K] = S_f^{l-s_1-\cdots-s_{1-i}} \) and \([M_{i+1} : K] = S_f^{l-s_1-\cdots-s_i} \).

Since each of the fields \( F(\pi_1^{\frac{1}{5}}), \ldots, F(\pi_f^{\frac{1}{5}}), F((\pi_{f+1}\pi_1^{h_1})^{\frac{1}{5}}), \ldots, F((\pi_{f+1}\pi_g^{h_g})^{\frac{1}{5}}), F(x^{\frac{1}{5}}) \) is linearly disjoint from the composite of the other fields, the result follows. \[ \square \]

Now, we look for representative ideals \( a_1, \ldots, a_i \) whose classes form a basis of the ambiguous ideal class group \( S_K[\lambda] \). Similarly, we also look for representative ideals \( b_1, \ldots, b_{-s_1-\cdots-s_i} \) whose classes form a basis of \((\lambda^i S_K)[\lambda] \) for \( i = 1, 2 \). For this purpose, we find ideals whose classes generate \( S_K[\lambda,i] \) for \( i = 1, 2, 3 \).

We observe that the ambiguous ideal class group \( S_K[\lambda] \) may be identified with the group \( S_{K,s} \) of strongly ambiguous ideal classes, excepting the case when at least one of \( \zeta^i(1+\zeta)^j \in N_{K/F}(K^*) \), and \( \zeta \notin N_{K/F}(E_K) \), where \( E_K \) is the group of units of \( K \).

We note that a necessary condition for the exceptional case to occur is that for any \( \pi_k|x \), one has \( \zeta^i(1+\zeta)^j \equiv a^5 \pmod{\pi_k} \) for some \( a \in \mathbb{Z}[\zeta] \) and
434
Manisha Kulkarni, et al.

Some i, j. There are two possible situations when the exceptional case occurs. 
Namely, if both \( \zeta, 1 + \zeta \) are norms of elements from \( K^* \), but neither of them 
is a norm from \( E_k \), then \( S_K[\lambda] \) is the direct product of \( S_{K,s} \) and two cyclic 
groups of order 5. In other exceptional cases, \( S_K[\lambda] \) is the direct product of 
\( S_{K,s} \) and a cyclic group of order 5.

5.4 Using ideles to express in terms of Hilbert symbols

We saw in section 4 how to obtain matrices with entries in \( F_l \) whose ranks are 
equal to the \( s_i \)'s. In this section, where \( l = 5 \) and the genus fields are chosen 
as above, we explain what these matrices simplify to.

Using the notation of Proposition 5.8, we choose prime ideals \( \mathfrak{B}_i \) in \( K \) 
such that \( \mathfrak{B}_i \otimes (\pi_i) \) for \( 1 \leq i \leq g \). If \( (\lambda) \) ramifies in \( K/F \), we let \( \mathfrak{I} \) denote 
the prime ideal in \( K \) such that \( 5 \mathfrak{I} = (\lambda) \). If there exists ambiguous ideal 
classes of \( K/F \) which are not strongly-ambiguous, we let \( \mathfrak{B} \) be a prime ideal 
which is contained in one such class and is relatively prime to \( x_1, \ldots, x_t \), 
where \( M_1 = K(x_1^{\frac{1}{5}}, \ldots, x_t^{\frac{1}{5}}) \) and \( x_1, \ldots, x_t \in F \). If \( q^r = 2 \) and \( q = 0 \), 
we choose \( \mathfrak{B}' \) to be a prime ideal contained in another class (from \( \mathfrak{B} \) of ideal 
which is ambiguous but not strongly-ambiguous, and is relatively prime to 
\( \mathfrak{B}, x_1, \ldots, x_t \).

Let \( I_{K}^{(r)} \) denote the free abelian group generated by these prime ideals. 
In other words, \( I_{K}^{(r)} \) is generated by \( \mathfrak{B}_1, \ldots, \mathfrak{B}_g, \) and \( \mathfrak{I} \) (in case \( (\lambda) \) 
ramifies in \( K/F \)), and \( \mathfrak{B} \) (in the case when there exist ambiguous ideal 
classes which are not strong-ambiguous), and also \( \mathfrak{B}' \) (in case \( q^r = 2 \) and \( q = 0 \)).

Let \( D_K^{(r)} = I_{K}^{(r)}/5I_{K}^{(r)} \). Viewed as a vector space over \( F_5 \), let \( D_K^{(r)} \) have 
dimension \( u \). Then \( u = g, g + 1, g + 2 \) or \( g + 3 \) in the four possibilities 
mentioned above respectively. Now, the map \( I_{K}^{(r)} \rightarrow S_K[\lambda] \) sending each 
ideal to its ideal class induces surjective homomorphisms

\[ \omega_1 : D_K^{(r)} = I_{K}^{(r)}/5I_{K}^{(r)} \rightarrow S_K[\lambda]. \]

Recall the map \( \phi_1 : S_K[\lambda] \rightarrow F_5^2 \) constructed in the proof of Theorem 4.1. 
Define \( \eta_1 := \phi_1 \circ \omega_1 : D_K^{(r)} \rightarrow F_5^2. \)

For \( 1 \leq i \leq t, 1 \leq j \leq g \), let \( \mu_{ij} \) denote the Artin symbol \( (K(x_i^{\frac{1}{5}})K^{\mathfrak{B}_j^{\mathfrak{I}}}) \).

Further, suppose

\[ \mu_{i(s+1)} = \left(\frac{K(x_i^{\frac{1}{5}})}{\mathfrak{B}_j^{\mathfrak{I}}} \right) \text{ for } 1 \leq i \leq t, \text{ if } (\lambda) \text{ ramifies in } K/F, \]
and

$$\mu_{i(g+2)} = \left( \frac{K(x_i^g)/K}{\mathcal{B}} \right)$$

for $1 \leq i \leq t$, if $S_K[\lambda] \setminus S_{K,s} \neq \emptyset$.

and

$$\mu_{iu} = \left( \frac{K(x_i^g)/K}{\mathcal{B}'} \right)$$

for $1 \leq i \leq t$, if $|S_K[\lambda]/S_{K,s}| > 5$.

If $\gamma_{ij} \in \mathbb{F}_e$ are defined by the power symbol $\zeta^\gamma_{ij} = (x_i^g)^{-1}$, let $C_1$ be the matrix of $\eta_1$ with respect to the ordered basis $\{\mathcal{B}_{e1}, \ldots, \mathcal{B}_{eg}, \mathcal{I} \}$ (if included), $\mathcal{B}$ (if included), and $\mathcal{B}'$ (if included). Since $\omega_1$ is surjective, $\text{rank} C_1 = \text{rank} A_1 = s_1$ (see Theorem 4.1).

We next construct ideles $a_{2g_1}, \ldots, a_{2g_1}, a_2, a_2, a_{2g_1} \in J_K$, the idele group of $K$, such that

$$(a_{2g_1}, K(x_i^g)/K) = \left( \frac{K(x_i^g)/K}{\mathcal{B}_{j'}} \right)$$

for $1 \leq i \leq t, 1 \leq j \leq g$.

$$(a_2, K(x_i^g)/K) = \left( \frac{K(x_i^g)/K}{\mathcal{I}} \right)$$

for $1 \leq i \leq t, (a_{2g_1}, K(x_i^g)/K) = \left( \frac{K(x_i^g)/K}{\mathcal{B}} \right)$$

for $1 \leq i \leq t$.

$$(a_{2g_1}, K(x_i^g)/K) = \left( \frac{K(x_i^g)/K}{\mathcal{B}'} \right)$$

for $1 \leq i \leq t$.

This is done as follows. Let

$$a_{2g_1} = (\cdots, 1, x_i^g, 1, \ldots)$$

for $1 \leq j \leq g$,

the idele which is 1 at all places except at the place corresponding to $\mathcal{B}_j$, where it is $x_i^g$. Let

$$a_2 = (\cdots, 1, x_3, 1, \ldots),$$

the idele which is 1 at all places except at the place corresponding to $\mathcal{I}$, where we insert an element $x_3 \in K$, such that $\mathcal{I} | x_3$, but $\mathcal{I}^2 \nmid x_3$. Let

$$a_2 = (\cdots, 1, x_2, 1, \ldots),$$

the idele which is 1 at all places except at the place corresponding to $\mathcal{B}'$, where we insert an element $x_2 \in K$, such that $\mathcal{B}' | x_2$.
the idele which is 1 at all places except at the place corresponding to \( \mathcal{B} \), where we insert an element \( x_{2\mathfrak{q}} \in \mathcal{K} \), such that \( \mathcal{B}|x_{2\mathfrak{q}} \), but \( \mathcal{B}^2 \not\mid x_{2\mathfrak{q}} \). Let

\[ a_{2\mathfrak{q}} = (\cdots, 1, x_{2\mathfrak{q}}, 1, \ldots), \]

the idele which is 1 at all places except at the place corresponding to \( \mathcal{B} \), where we insert an element \( x_{2\mathfrak{y}} \in \mathcal{K} \), such that \( \mathcal{B}'|x_{2\mathfrak{y}} \), but \( \mathcal{B}'^2 \not\mid x_{2\mathfrak{y}} \).

Now

\[ (a_{2\mathfrak{y}}, K(x_{2\mathfrak{y}})^{1}/K)|F(x_{2\mathfrak{y}}) = (N_{K/F}(a_{2\mathfrak{y}}), F(x_{2\mathfrak{y}}))/F, \]

where \( N_{K/F}(a_{2\mathfrak{y}}) \) is the idele \((\ldots, 1, x, 1, \ldots)\) of \( F \) which is 1 at all places except at the place corresponding to \((\pi_j)\), where it is \( x \). We denote \( N_{K/F}(a_{2\mathfrak{y}}) \) by \( a_{\pi_j} \). Similarly,

\[ (a_{2\mathfrak{y}}, K(x_{2\mathfrak{y}})^{1}/K)|F(x_{2\mathfrak{y}}) = (a_{\pi}, F(x_{2\mathfrak{y}}))/F, \]

where \( a_{\pi} = N_{K/F}(a_{2\mathfrak{y}}) = (\ldots, 1, x_{\pi}, 1, \ldots) \) with \( x_{\pi} = N_{K/F}(x_{2\mathfrak{y}}) \). Also,

\[ (a_{2\mathfrak{y}}, K(x_{2\mathfrak{y}})^{1}/K)|F(x_{2\mathfrak{y}}) = (a_{\pi'}, F(x_{2\mathfrak{y}}))/F, \]

where \( a_{\pi'} = N_{K/F}(a_{2\mathfrak{y}}) = (\ldots, 1, x_{\pi'}, 1, \ldots) \), where \( \pi' = N_{K/F}(\mathcal{B}') \), with \( x_{\pi'} = N_{K/F}(x_{2\mathfrak{y}}) \).

We now consider \( \zeta^{\gamma_{ij}} = (x_{i}^{1})^{\mu_{ij}} \). From our calculation we can replace

\[ \mu_{ij} \text{ by } v_{ij} = (a_{\pi_j}, F(x_{i}^{1})/F) \text{ for } 0 \leq i \leq t, 1 \leq j \leq g, \]

\[ \mu_{i(g+1)} \text{ by } v_{i(g+1)} = (a_{\pi}, F(x_{i}^{1})/F) \text{ for } 0 \leq i \leq t, \]

\[ \mu_{i(g+2)} \text{ by } v_{i(g+2)} = (a_{\pi'}, F(x_{i}^{1})/F) \text{ for } 0 \leq i \leq t, \]

\[ \mu_{i(g+3)} \text{ by } v_{i(g+3)} = (a_{\pi'}, F(x_{i}^{1})/F) \text{ for } 0 \leq i \leq t. \]

So we have,

\[ \zeta^{\gamma_{ij}} = (x_{i}^{1})^{v_{ij}} \text{ for all } i, j. \]

Since the ideles \( a_{\pi_j}(1 \leq j \leq g), a_{\pi}, a_{\pi'} \) are local ideles, we may identify the expressions \( (x_{i}^{1})^{v_{ij}} \) with the degree 5 Hilbert symbols.
Let $M = \pm \alpha$. Now, we write $\pm \alpha$ to was chosen relatively prime to $x_i$. Hence we have, $x_i \equiv \pm 1, \pm 7 \pmod{\lambda}$. Since $x_i \equiv \pm 1, \pm 7 \pmod{\lambda}$, let $x_i = x_i$, and write $\alpha = \pm1 + \lambda y$ or $\alpha = \pm2 + \lambda y$ (respectively). Since $y$ is a root of a polynomial $f(Y) \in \mathcal{O}_K[Y]$, such that $f(Y) = Y^5 - Y - c \pmod{\lambda}$, we have $f'(y) \equiv -1 \neq 0 \pmod{\lambda}$. Thus $F_{\lambda}(y) = F_{\lambda}(x_1^t)$ is unramified over $F_{\lambda}$. Thus we have, $(\frac{x_i \cdot x_i}{\lambda}) = 1$ (See, [19][page 209, Exercise 5]). So,

$$
\left( \frac{x_i, z_i}{\lambda} \right) = \left( \frac{x_i, \lambda}{\lambda} \right) \left( \frac{x_i, z_i}{\lambda} \right)^{-1} \left( \frac{x_i, \lambda}{\lambda} \right), \text{ for } 1 \leq i \leq t.
$$

Now, we write $x_\pi = \pi y_\pi$, where $y_\pi$ is relatively prime to $\pi$. Since $\mathfrak{B}$ was chosen relatively prime to $x_1, \ldots, x_t$, then $\pi$ is relatively prime to $x_i$ for all $i$. Hence

$$
\left( \frac{x_i, x_\pi}{\pi} \right) = \left( \frac{x_i, \pi}{\pi} \right) \left( \frac{x_i, y_\pi}{\pi} \right) = \left( \frac{x_i, \pi}{\pi} \right), \text{ for } 1 \leq i \leq t.
$$

Finally, let us write $x_\pi' = \pi' y_\pi'$, where $y_\pi'$ is relatively prime to $\pi'$. Since $\mathfrak{B}'$ was chosen relatively prime to $x_1, \ldots, x_t$, then $\pi'$ is relatively prime to $x_i$ for all $i$. Hence

$$
\left( \frac{x_i, x_\pi'}{\pi'} \right) = \left( \frac{x_i, \pi'}{\pi'} \right) \left( \frac{x_i, y_\pi'}{\pi'} \right) = \left( \frac{x_i, \pi'}{\pi'} \right), \text{ for } 1 \leq i \leq t.
$$

With these notations, we may describe the matrix whose entries are power residue symbols and, whose rank gives us the rank of the piece $H_1$ (see 3.1) of the $l$-class group.

**Theorem 5.10.** Let $F = \mathbb{Q}(\zeta)$, $K = F(\sqrt{5})$, $x = u \lambda^{c_1} \pi_1^{c_1} \cdots \pi_g^{c_g}$ as above. Let $M_1 = K(x_1^t, \ldots, x_t^t)$ denote the genus field of $K/F$, where $[M_1 : K] = 5^t$, $x_i \in F$ for $1 \leq i \leq t$, and $x_i \equiv \pm1, \pm7 \pmod{\lambda^5}$. Let $\mathfrak{B}, \mathfrak{B}'$ be ideals as above defined respectively when there exist ambiguous ideal classes which are not strongly-ambiguous, and when $q^* = 2, q = 0$. Let $(\pi) = N_{K/F}(\mathfrak{B})$ and $(\pi') = N_{K/F}(\mathfrak{B}')$, where $N_{K/F}$ is the norm map from $K$ to $F$. For $1 \leq i \leq t$, $1 \leq j \leq g$, let $v_{ij}$ denote the degree 5 Hilbert symbol $(\frac{x_i \cdot x_j}{\pi_{ij}})$. Further, suppose

$$
v_{i(g+1)} = \left( \frac{x_i, \lambda}{\lambda} \right) \text{ for } 1 \leq i \leq t, \text{ if } (\lambda) \text{ ramifies in } K/F,
$$
and
\[ v_{i(g+2)} = \left( \frac{x_i, \pi}{(\pi)} \right) \text{ for } 1 \leq i \leq t, \text{ if } S_K^{(r)} \backslash S_K^{(s)} \neq \emptyset, \]
and
\[ v_{iu} = \left( \frac{x_i, \pi'}{(\pi')} \right) \text{ for } 1 \leq i \leq t, \text{ if } |S_K^{(r)} / S_K^{(s)}| > 5. \]

If \( \gamma_{ij} \in \mathbb{F}_5 \) are defined by the power symbol \( \zeta_{\gamma_{ij}} = (x_1^5)^{\gamma_{ij} - 1} \), and \( C_i \) is the matrix \((\gamma_{ij})\), \( 1 \leq i \leq t, 1 \leq j \leq u \), we have
\[ s_1 = \text{rank} H_1 = \text{rank} C_1. \]

Finally, we discuss how the above theorem can be generalized to determine the ranks \( s_i \)'s for \( i > 1 \). Observe that
\[ S_K[\lambda] \supset (\lambda S_K)[\lambda] \supset (\lambda^2 S_K)[\lambda]. \]

Since \( cl(\mathfrak{B}_1), \ldots, cl(\mathfrak{B}_g), cl(\mathfrak{I}) \) (if included), \( cl(\mathfrak{B}) \) (if included), and \( \mathfrak{B}' \) (if included) generate \( S_K[\lambda] \), there exists a basis of \( (\lambda^{i-1} S_K)[\lambda] \), \( cl(\Gamma_{i,1}), \ldots, cl(\Gamma_{i,t-s_1-\cdots-s_{i-1}}) \) consisting of elements which are \( \mathbb{F}_5 \)-linear combinations of \( cl(\mathfrak{B}_1), \ldots, cl(\mathfrak{B}_g), cl(\mathfrak{I}), cl(\mathfrak{B}), cl(\mathfrak{B}') \), for \( i = 2, 3. \)

Let \( \Gamma_{i,1}, \ldots, \Gamma_{i,t-s_1-\cdots-s_{i-1}} \) be some representative ideals for the respective classes. With these choices, we have the following theorem expressing the ranks \( s_i \) in terms of matrices over \( \mathbb{F}_5 \):

**Theorem 5.11.** Let \( F = \mathbb{Q}(\zeta), K = F(x^{\frac{1}{t}}) \), where \( x = u^{\lambda e_1} \pi^{e_1} \cdots \pi^{e_g} \) as above. Let \( M_1 \) be the genus field of \( K/F \) and, for \( i = 1, 2, \) let \( M_{i+1} = K(y^{\frac{1}{t}}_1, \ldots, y^{\frac{1}{t}}_{t-s_1-\cdots-s_i}) \) as in Theorem 4.2. Let \( \Gamma_{i+1,1}, \ldots, \Gamma_{i+1,t-s_1-\cdots-s_i} \) be as in the previous paragraph. Denote
\[ \mu_{jk} = \left( \frac{K(y^{\frac{1}{t}}_j)/K}{\Gamma_{i+1,k}} \right) \text{ for } 1 \leq j, k \leq t - s_1 - \cdots - s_i. \]

If \( \gamma_{jk} \) are defined by \( \zeta_{\gamma_{jk}} = (y^{\frac{1}{t}}_j)^{\mu_{jk} - 1} \), and \( C_{i+1} = (\gamma_{jk}), 1 \leq j, k \leq t - s_1 - \cdots - s_i \), then
\[ s_{i+1} = \text{rank} H_{i+1} = \text{rank} C_{i+1}. \]

**Proof.** We have the map
\[ \phi_{i+1} : (\lambda^i S_K)[\lambda] \to \mathbb{F}_5^{t-s_1-\cdots-s_i}. \]
constructed in the proof of Theorem 4.2. Clearly, \( C_{i+1} \) is the matrix of \( \phi_{i+1} \) with respect to the ordered basis 

\[ \{ \Gamma_{i+1,1}, \ldots, \Gamma_{i+1,\tau-s_1-\cdots-s_1} \} \]

Thus, from Theorem 4.2,

\[ s_{i+1} = \text{rank}C_{i+1}. \]

**Remarks.** In conclusion, the above theorems show in principle how to compute \( t, s_1, s_2, s_3 \). We can use them to find the rank of \( S_K \) using the formula obtained from Proposition 3.1; namely,

\[ \text{rank}S_K = 4t - 3s_1 - 2s_2 - s_3. \]

However, concrete determination of \( s_2, s_3 \) seems to be difficult. In particular, it would be useful to find explicit generators for the groups \( (\lambda^iS_K)[\lambda] \) for \( i \geq 1 \). We also obtain a bound for the rank of \( S_K \) in terms of \( t \) and \( s_1 \) as follows,

\[ 2t - s_1 \leq \text{rank}S_K \leq 4t - 3s_1. \]

### 5.5 Applications – explicit results

We apply our result in various situations to give sharp bounds for the rank of the 5-class group.

**Theorem 5.12.** Let \( p_i \equiv \pm7 \pmod{25} \) for \( 1 \leq i \leq r \) be primes and \( r \geq 2 \). Let \( n = p_1^{a_1} \cdots p_r^{a_r} \), where \( 1 \leq a_i \leq 4 \) for \( 1 \leq i \leq r \). Let \( F = \mathbb{Q}(...\mathbb{Q}(\zeta_5)) \) and \( K = F(n^\frac{1}{5}) \). Assume that all ambiguous ideal classes of \( K/F \) are strongly ambiguous. Then, the \( \lambda^2 \)-rank of \( S_K \) is \( r - 1 \) and \( 2r - 2 \leq \text{rank}S_K \leq 4r - 4 \).

If there are ambiguous ideal classes which are not strongly ambiguous, then \( s_1 \leq 2 \), and the \( \lambda^2 \)-rank of \( S_K \) is greater than or equal to \( r - 3 \) and \( \max(2r - 4, r - 1) \leq \text{rank}S_K \leq 4r - 4 \).

**Proof.** Firstly we notice that \( n \equiv \pm1, \pm7 \pmod{25} \). So \( \lambda \) does not ramify in \( K/F \). Looking at the fields \( K_i = F(p_i^{\frac{1}{5}}) \), one can easily see that \( \zeta \) and \( 1 + \zeta \) are fifth powers modulo \( p_i \) for all \( i = 1, \ldots, r \). Thus \( q^* = q = 2 \) and \( t = d - 3 + q^* = r - 1 \).

To compute \( s_1 \), let \( x_i = p_i \) where \( 1 \leq i \leq r - 1 \). Using [19][Chapter 14, Section 3] one can easily check that \( (\frac{5}{p_i}) = 1 \) for \( 1 \leq i \leq r - 1 \) and \( 1 \leq j \leq r \). That is the \( (r - 1) \times r \) matrix \( C_1 \) is the zero matrix. So, \( s_1 = 0 \).

Thus, we get \( \lambda^2 \)-rank of \( S_K \) is \( t - s_1 = r - 1 \). Since \( 2t - s_1 \leq \text{rank}S_K \leq 4r - 3s_1 \), we obtain that \( 2r - 2 \leq \text{rank}S_K \leq 4r - 4 \).
The second part of the statement follows from the fact that $0 \leq q \leq 1$, and then the matrix $C_1$ is of size $(r - 1) \times (r + q^s - q)$, which can have rank at most 2.

\[ \text{Theorem 5.13.} \] Let $p_i \equiv \pm 7 \pmod{25}$ for $1 \leq i \leq r$ be primes and let $q_j$ be primes such that $q_j \equiv \pm 2 \pmod{5}$ but $q_j \not\equiv \pm 7 \pmod{25}$ for $1 \leq j \leq s$. Let $n = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$, where $1 \leq a_i, b_j \leq 4$ for $1 \leq i \leq r$ and $1 \leq j \leq s$. Let $n \not\equiv \pm 1, \pm 7 \pmod{25}$. Let $F = \mathbb{Q}(\zeta_5)$ and $K = F(n^\frac{1}{5})$. Assume that all ambiguous ideal classes of $K/F$ are strongly ambiguous. Then, the $\lambda^2$-rank of $SK$ is $r + s - 1$ and $2r + 2s - 2 \leq \text{rank}SK \leq 4r + 4s - 4$.

If there are ambiguous ideal classes which are not strongly ambiguous, then $s_1 \leq 1$, and the $\lambda^2$-rank of $SK$ is greater than or equal to $r + s - 2$ and $\max(2r + 2s - 3, r + s - 1) \leq \text{rank}SK \leq 4r + 4s - 4$.

\[ \text{Proof.} \] Firstly we notice that $\lambda$ ramifies in $K/F$. Since $N(q) \not\equiv 1 \pmod{25}$, $\zeta \not\equiv N_K/F(K^*)$. Looking at the fields $K_i = F(p_i^\frac{1}{5})$ and $L_j = F((q_j^{h_j})^\frac{1}{5})$, where $1 \leq h_j \leq 4$ are chosen such that $q_j^{h_j} \equiv \pm 1, \pm 7 \pmod{25}$, $j \neq 1$, one can easily see that some $\zeta^t(1 + \zeta)^j$ is fifth power modulo $p_i$ for all $i = 1, \ldots, r$ and $q_j$ for $1 \leq j \leq s$. Thus $q^* = q = 1$ and $t = d - 3 + q^* = r + s - 1$.

To compute $s_1$, let $x_i = p_i$ where $1 \leq i \leq r$ and $y_{j-1} = q_j^{h_j}$ where $2 \leq j \leq s$. Using [19][Chapter 14, Section 3] one can easily check that $(\frac{\alpha_{ij}}{p_i}) = 1$ for $1 \leq i, j \leq r$, $(\frac{\alpha_{ij}}{q_j}) = 1$ for $1 \leq i \leq r, 1 \leq j \leq s$, $(\frac{\alpha_{ij}}{n}) = 1$ for $1 \leq i \leq s - 1, 1 \leq j \leq r$ and $(\frac{\alpha_{ij}}{q_j}) = 1$ for $1 \leq i \leq s - 1, 1 \leq j \leq s$. That is, the $(r + s - 1) \times r + s$ sub matrix of $C_1$ is zero matrix. Since $x_i, y_j \equiv \pm 7 \pmod{25}$, using [2][Exercise 2.12, pg. 353–354] one can easily check that $(\frac{\alpha_{ij}}{p_i})(\frac{\alpha_{ij}}{q_j}) = 1$. Therefore, $s_1 = 0$.

So, we see that the $\lambda^2$-rank of $SK$ is $t - s_1 = r + s - 1$. Since $2t - s_1 \leq \text{rank}SK \leq 4r + 3s_1$, we obtain that $2r + 2s - 2 \leq \text{rank}SK \leq 4r + 4s - 4$.

The second part of the statement follows from the fact that $q = 0$, as, then the matrix $C_1$ is of size $(r + s - 1) \times (r + s + 2)$, which can have rank at most 2.

\[ \text{Theorem 5.14.} \] Let $p_i \equiv \pm 7 \pmod{25}$ for $1 \leq i \leq r$ be primes and let $q_j$ be primes such that $q_j \equiv \pm 2 \pmod{5}$ but $q_j \not\equiv \pm 7 \pmod{25}$ for $1 \leq j \leq s$ with $s \geq 2$. Let $n = p_1^{a_1} \cdots p_r^{a_r} q_1^{b_1} \cdots q_s^{b_s}$, where $1 \leq a_i, b_j \leq 4$ for $1 \leq i \leq r$ and $1 \leq j \leq s$. Let $n \equiv \pm 1, \pm 7 \pmod{25}$. Let $F = \mathbb{Q}(\zeta_5)$ and $K = F(n^\frac{1}{5})$. Assume that all ambiguous ideal classes of $K/F$ are strongly ambiguous. Then, the $\lambda^2$-rank of $SK$ is $r + s - 2$ and $2r + 2s - 2 \leq \text{rank}SK \leq 4r + 4s - 8$.\]
If there are ambiguous ideal classes which are not strongly ambiguous, then \( s_1 \leq 1 \). \( \lambda^2 \)-rank of \( S_K \) is greater than or equal to \( r + s - 3 \) and \( \max(2r + 2s - 5, r + s - 2) \leq \text{rank} S_K \leq 4r + 4s - 8 \).

Proof. Firstly, we notice that \( \lambda \) does not ramify in \( K/F \). Since \( N(q) \not\equiv 1 \) \((\bmod 25)\), \( \zeta \not\equiv N_{K/F}(\zeta)^1 \). Looking at the fields \( K_i = F(p_i^{\frac{1}{2}}) \) and \( L_j = F(q_j^{h_j}) \), where \( 1 \leq h_j \leq 4 \) are chosen such that \( q_jq_j^{1 \equiv \pm 1, \pm 7} \) \((\bmod 25)\), \( j \neq 1 \), one can easily see that some \( \zeta^u(1 + \zeta)^v \) is a fifth power modulo \( p_i \) for all \( i = 1, \ldots, r \) and a fifth power modulo \( q_j \) for \( 1 \leq j \leq s \). Thus \( q^u = q = 1 \) and \( t = d - 3 + q^n = r + s - 2 \).

To compute \( s_1 \), let \( x_i = p_i \) where \( 1 \leq i \leq r \) and \( y_j = q_j^{h_i} \) where \( 2 \leq j \leq s - 1 \). Using [19][Chapter 14, Section 3] one can easily check that \( \left( \frac{w_i}{w_j} \right) = 1 \) if \( 1 \leq i \leq j, r \leq 1 \leq j \leq s \), \( \left( \frac{w_i}{w_j} \right) = 1 \) for \( 1 \leq i \leq j \leq s - 2, 1 \leq j \leq r \) and \( \left( \frac{w_i}{w_j} \right) = 1 \) if \( 1 \leq i \leq s - 2, 1 \leq j \leq s \). That is, the \((r + s - 2) \times (r + s)\) matrix \( C_i \) is the zero matrix. So \( s_1 = 0 \).

We obtain that the \( \lambda^2 \)-rank of \( S_K \) is \( r - s_1 = r + s - 2 \). Since \( 2r - s_1 \leq \text{rank} S_K \leq 4r + 4s - 8 \), we get \( 2r + 2s - 4 \leq \text{rank} S_K \leq 4r + 4s - 8 \).

The second part of the statement follows from the fact that \( q = 0 \), and then

**Table 1.** Number fields and their class groups.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( n(F) )</th>
<th>( S_K )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2,3,4,7,9,16,17,23,27</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>43,47,49,53,73,81,97</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>13,37,67,83</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>18,24,26,51,68,74</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>6,12,14,21,28,36,39,48,52</td>
<td>2</td>
<td>( C_5 )</td>
</tr>
<tr>
<td>54,56,69,72,91,92,94,98</td>
<td>2</td>
<td>( C_5 )</td>
</tr>
<tr>
<td>34,46,63,86</td>
<td>2</td>
<td>( C_5 )</td>
</tr>
<tr>
<td>301</td>
<td>2</td>
<td>( C_5 )</td>
</tr>
<tr>
<td>19,29,59,79,89</td>
<td>2</td>
<td>( C_5 \times C_5 )</td>
</tr>
<tr>
<td>57,76</td>
<td>3</td>
<td>( C_5 \times C_5 )</td>
</tr>
<tr>
<td>38,58,87,133</td>
<td>3</td>
<td>( C_5 \times C_5 \times C_5 )</td>
</tr>
<tr>
<td>42,78,84</td>
<td>3</td>
<td>( C_5 \times C_5 \times C_5 \times C_5 \times C_5 )</td>
</tr>
<tr>
<td>11,41,61,71</td>
<td>4</td>
<td>( C_5 \times C_5 )</td>
</tr>
<tr>
<td>31</td>
<td>4</td>
<td>( C_5 \times C_5 \times C_5 \times C_5 \times C_5 )</td>
</tr>
<tr>
<td>82,93,99</td>
<td>5</td>
<td>( C_5 \times C_5 )</td>
</tr>
<tr>
<td>22,44,62,77</td>
<td>5</td>
<td>( C_5 \times C_5 \times C_5 \times C_5 \times C_5 )</td>
</tr>
<tr>
<td>33,88</td>
<td>5</td>
<td>( C_5 \times C_5 \times C_5 \times C_5 \times C_5 )</td>
</tr>
<tr>
<td>66</td>
<td>6</td>
<td>( C_5 \times C_5 \times C_5 \times C_5 \times C_5 \times C_5 )</td>
</tr>
<tr>
<td>5,25</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>10,15,20,45,75,80</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>40,50,65,85</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>35</td>
<td>2</td>
<td>( C_5 )</td>
</tr>
<tr>
<td>30,60,70,90</td>
<td>3</td>
<td>( C_5 )</td>
</tr>
<tr>
<td>55,95</td>
<td>3</td>
<td>( C_5 \times C_5 )</td>
</tr>
</tbody>
</table>
The matrix $C_1$ is of size $(r + s - 2) \times (r + s + 1)$, which can have rank at most 1.

The following table provided by SAGE gives the computation of various class groups. We have $F = \mathbb{Q}(\zeta_5)$, $K = F(p^{\frac{1}{5}})$. We denote by $n(F)$ the number of distinct prime divisors of $n$ in $F$ and $S_K$ the 5-class group of $K$ respectively.

We observe from Table 1 that, if $p \equiv -1 \pmod{5}$, then rank of class group is at least 2. That motivated us to prove the following result (see also Table 2 below). The table is obtained using SAGE with $K = \mathbb{Q}(\zeta_5)(p^{\frac{1}{5}})$, where $p \equiv -1 \pmod{5}$ and $R = \mathbb{Z}[\zeta_5]$. The second column describes the $R$-module structure of the 5-class group $S_K$.

**Theorem 5.15.** Let $p$ be a prime congruent to $-1 \pmod{5}$. Let $F = \mathbb{Q}(\zeta_5)$ and $K = F(p^{\frac{1}{5}})$. Assume that all ambiguous ideal classes are strongly ambiguous. Then 25 divides the class number of $K$. More precisely, the $\lambda^2$-rank of $S_K$ is 1 and we have, $2 \leq \text{rank} S_K \leq 4$.

**Proof.** It is known that any prime of the form $p \equiv -1 \pmod{5}$ can be written as

$$p = a^2 + ab - b^2$$

with $a, b \in \mathbb{Z}$, non-zero with $(a, b) = 1$. Note that this implies that $(a, p) = (b, p) = 1$.

Let $c = a - b$, define

$$\pi_1 = a_3 + a\zeta^2 + b \quad \text{and} \quad \pi_2 = a_3 + a\zeta^2 + c.$$
Now we observe the following two identities:

\[ a^2 + bc = a^2 + b(a - b) = p \quad \text{and} \quad a^2 - ab - ac = a^2 - a(b + c) = 0. \]

Thus,

\[
\begin{align*}
\pi_1 \pi_2 &= (a_1^b + a_1^c)(a_2^b + a_2^c) \\
&= (2a^2 + bc) + a^2(\zeta + \zeta^4) + (ab + ac)(\zeta^2 + \zeta^3) \\
&= (a^2 + bc) + (a^2 - ab - ac)(1 + \zeta + \zeta^4) \\
&= p.
\end{align*}
\]

This gives us prime decomposition of \( p \) in \( F \). Now to compute the \( \lambda^2 \)-rank of \( S_K \), we compute \( t \) and \( s_1 \).

If \( p \equiv -1 \pmod{25} \), then \( N(\pi_i) = p^2 \equiv 1 \pmod{25} \) for \( i = 1, 2 \).

So \( \zeta \in N_{K/F}(K^*) \).

If \( p \not\equiv -1 \pmod{25} \), then \( N(\pi_i) = p^2 \not\equiv 1 \pmod{25} \) for \( i = 1, 2 \).

So \( \zeta \not\in N_{K/F}(K^*) \).

In both cases,

\[-\zeta^2(1 + \zeta) \equiv \frac{b}{a} \pmod{\pi_1} \quad \text{and} \quad -\zeta^2(1 + \zeta) \equiv \frac{c}{a} \pmod{\pi_2}.
\]

Note that \( \frac{b}{a} \) and \( \frac{c}{a} \) are in \( \mathbb{F}_p^* \). Since \( 5 \nmid p - 1 \), \( x \mapsto x^5 \) is an isomorphism of \( \mathbb{F}_p^* \). Hence \( \frac{b}{a} \) and \( \frac{c}{a} \) are fifth power modulo \( \pi_1 \) and \( \pi_2 \) respectively. Thus in both cases we see that, \(-\zeta^2(1 + \zeta) \in N_{K/F}(K^*)\).

Combining these facts, we see that in both cases, \( t = g - 1 = 1 \).

In the case, \( p \not\equiv -1 \pmod{25} \), we have \( q^* = q = 1 \). In the case \( p \equiv -1 \pmod{25} \), we have \( q^* = q = 2 \) and \( \lambda \) does not ramify in \( K/F \).

Let \( M_1 \) denote the genus field of \( K/F \). It is of the form \( M_1 = K(x_1^{\frac{1}{5}}) \). Since \( M_1 \) is unramified over \( K \), only the primes that ramify in \( K \) can divide \( x_1 \).

Suppose \( p \equiv -1 \pmod{25} \). Then, only \( \pi_1 \) and \( \pi_2 \) ramify in \( K \). So \( x_1 \) is of the form \( x_1 = \pi_1^a \pi_2^b \). To compute \( s_1 \), we need to compute \( \frac{(\zeta_1^i \pi_1)}{(\zeta_2^i \pi_2)} \). Let \( c_1 = (-1)^{a_1} p^{1/5} = (-1)^{a_1} \pi_2^{a_2 - a_1} \). Since \( \pi_2 = c - b \pmod{\pi_1} \), with \( c - b \in \mathbb{F}_p^* \), we see on using [19][Chapter 14, Section 3] that, \( (\zeta_1^i \pi_1)^{(c_1)}(p^2 - 1)/5 = 1 \). This was because the residue field is \( \mathbb{F}_{p^2} \) and \( (p^2 - 1)/5 \) is a multiple of \( p - 1 \). Similarly we find that, \( (\zeta_2^i \pi_2)^{(c_2)} = 1 \). So in this case the \((1 \times 2)\) matrix \( C_1 \) is the zero matrix. Hence \( s_1 = 0 \).

Now suppose the \( p \not\equiv -1 \pmod{25} \), then \( \lambda \) also ramifies in \( K \). So in this case, \( x_1 \) is of the form \( x_1 = \lambda^a \pi_1^a \pi_2^b \). To compute \( s_1 \), we need to compute \( \frac{(\zeta_1^i \pi_1)}{\pi_2} \). Let \( c_1 = (-1)^{a_2} \lambda \pi_2 = (-1)^{a_1} \pi_2^{a_2 - a_1} \lambda \). Since \( \pi_2 = c - b \pmod{\pi_1} \), with \( c - b \in \mathbb{F}_p^* \) and \( (\lambda)^4 = 5 \pmod{\pi_1} \), we see that...
(\bar{c}_1)^{4(p-1)} = 1. That is \((\frac{\bar{c}_1}{\pi_1}) = (\bar{c}_1)^{(p^2-1)/5} = \pm 1. Since it is a fifth root of unity in \mathbb{F}_p[\zeta]^*, it can not be \(-1. Thus, (\frac{\bar{c}_1}{\pi_1}) = 1. Similarly we see that, (\frac{\bar{c}_1}{\pi_2}) = 1. To compute (\frac{\bar{c}_2}{\pi_1}), we compute (\frac{\bar{c}_2}{\pi_2}) and use the product formula. We compute (\frac{\bar{c}_2}{\pi_1}) similarly to get, (\frac{\bar{c}_2}{\pi_1}) = 1 for i = 1, 2. Thus (\frac{\bar{c}_2}{\pi_1}) = 1. So in this case the 1 \times 3 matrix \(C_1\) is the zero matrix. Hence \(s_1 = 0\).

Thus \(s_1 = 0\) in either case which means that the \(\lambda^2\)-rank of \(S_K\) is \(t - s_1 = 1\).

Lastly, we observe that,

\[2 = 2t - s_1 \leq \text{rank} S_K \leq 4t - 3s_1 = 4,\]

that is 25 divides the class number of \(K\). \hfill \Box

The following theorem may be useful in studying elliptic curves over towers of the form \(K_n := \mathbb{Q}(e^{2\pi i/5^n}, x^{1/5})\). It is motivated by a comment of John Coates that Iwasawa theory implies the triviality of \(S_{K_n}\) for all \(n\) for all \(x\) considered in the theorem.

**Theorem 5.16.** Let \(F = \mathbb{Q}(\zeta_5)\) and let \(K = \mathbb{Q}(\zeta_5, x^{1/5})\) where \(x\) is a positive integer which is not divisible by the 5\(^{th}\) power of any prime in \(F\). Suppose that the prime \(\lambda = 1 - \zeta_5\) ramifies in \(K\). Then \(S_K = \{1\}\) if, and only if, \(x = p^a\), where \(p\) is a prime number such that \(p \equiv \pm 2 \pmod{5}\), but \(p \not\equiv \pm 7 \pmod{25}\) and \(1 \leq a \leq 4\). Further, 5 is totally ramified in \(\mathbb{Q}(\zeta_{25}, x^{1/5})\) for \(x\) as above.

**Proof.** Suppose that \(x = p^a\), where \(p\) is as described above. Then, clearly \(\lambda\) ramifies in \(K/F\) from Lemma 5.1(c), since \(x \not\equiv \pm 1, \pm 7 \pmod{25}\). Furthermore, \(\zeta\) is not in \(N_{K/F}(K^*)\) once again by Lemma 5.1, since \(N_{F/Q}(p) \equiv 1 \pmod{25}\); so \(q^* \leq 1\). Thus \(t = d - 3 + q^* = q^* - 1\). It follows that \(q^* = 1\) and \(t = 0\). Since, \(t = 0\), we see that \(S_K = \{1\}\).

Conversely, suppose that \(\lambda\) ramifies in \(K/F\) and \(S_K = \{1\}\). Then we must have \(t = 0\) (since, rank \(S_K \geq t\)). We also note that, in this situation \(x \not\equiv \pm 1, \pm 7 \pmod{25}\). Let \(g\) be the number of distinct primes of \(F\), which divides \(x\). Then \(d = g + 1\) (since \(\lambda\) ramifies in \(K/F\)). Thus \(0 = t = d - 3 + q^* = g + q^* - 2\), or in other words, \(g + q^* = 2\).

If \(g = 2\), there are three possible cases.

(i) \(x \equiv -1 \pmod{5}\) is a prime. Then as in Theorem 5.16, we see that, \(t = 1\).

(ii) \(x = p^aq^b\), where \(p \equiv \pm 7 \pmod{25}\) and \(q \equiv \pm 2 \pmod{5}\) but \(q \not\equiv \pm 7 \pmod{25}\). By Theorem 5.13 with \(r = s = 1\), we see that \(t = 1\).

(iii) \(x = p^aq^b\), where \(p, q \equiv \pm 2 \pmod{5}\) but \(p, q \not\equiv \pm 7 \pmod{25}\) and \(x \not\equiv \pm 1, \pm 7 \pmod{25}\). By Theorem 5.13 with \(r = 0\) and \(s = 2\), we see that \(t = 1\).
Table 3. Structure of 5-class group of $K$.

<table>
<thead>
<tr>
<th>$n = p \times q$</th>
<th>Structure of $S_K$ as $R$ module</th>
</tr>
</thead>
<tbody>
<tr>
<td>$7 \times 19$</td>
<td>$R/(\lambda) \times R/(\lambda^2)$</td>
</tr>
<tr>
<td>$7 \times 29$</td>
<td>$R/(\lambda) \times R/(\lambda^3)$</td>
</tr>
<tr>
<td>$7 \times 59$</td>
<td>$R/(\lambda) \times R/(\lambda^2)$</td>
</tr>
<tr>
<td>$7 \times 79$</td>
<td>$R/(\lambda) \times R/(\lambda^3)$</td>
</tr>
<tr>
<td>$7 \times 89$</td>
<td>$R/(\lambda) \times R/(\lambda^2)$</td>
</tr>
<tr>
<td>$7 \times 149$</td>
<td>$R/(\lambda) \times R/(\lambda^2)$</td>
</tr>
<tr>
<td>$43 \times 149$</td>
<td>$R/(\lambda) \times R/(\lambda^3)$</td>
</tr>
<tr>
<td>$107 \times 149$</td>
<td>$R/(\lambda) \times R/(\lambda^2)$</td>
</tr>
<tr>
<td>$7 \times 199$</td>
<td>$R/(\lambda) \times R/(\lambda^2)$</td>
</tr>
<tr>
<td>$43 \times 199$</td>
<td>$R/(\lambda) \times R/(\lambda^3)$</td>
</tr>
<tr>
<td>$107 \times 199$</td>
<td>$R/(\lambda) \times R/(\lambda^2)$</td>
</tr>
</tbody>
</table>

Thus, we must have $g = 1$; that is, $x = p^a$ with $p \equiv \pm 2 \pmod{5}$. If $p \equiv \pm 7 \pmod{25}$, then $x \equiv \pm 1, \pm 7 \pmod{25}$, contradicting the assumption that $\lambda$ ramifies in $K/F$. So we obtain that, $x = p^a$, where $p$ is a rational prime such that $p \equiv \pm 2 \pmod{5}$, but $p \not\equiv \pm 7 \pmod{25}$ and $1 \leq a \leq 4$. This completes the proof excepting the last assertion which is checked easily using a finite computation.

**Remark 5.17.** If we remove the assumption that $\lambda$ ramifies in $K/F$, then $S_K$ is trivial if and only if $x = p^a$ with $p \equiv \pm 2 \pmod{5}$ or $x = p^a q^b$, where $p, q \equiv \pm 2 \pmod{5}$ but $p, q \not\equiv \pm 7 \pmod{5}$ and $x \equiv \pm 1, \pm 7 \pmod{25}$. By Theorem 5.12, with $r = 1$, it follows that, if $g = 1$, then $x = p^a$, with $p \equiv \pm 2 \pmod{5}$ has $t = 0$. On the other hand, in case $g = 2$, we see from Theorem 5.14 (with $r = 0$ and $s = 2$) that in the case mentioned, $t = 0$. Compare with Table 1.

The following theorem is similar in flavor to that of Theorem 5.15 (see also Table 3 below). The table is obtained using SAGE with $K = \mathbb{Q}(\zeta_5)(n^*)$, where $n = pq$ with $p \equiv \pm 7 \pmod{25}$, $q \equiv -1 \pmod{5}$ and $R = \mathbb{Z}[\zeta_5]$. The second column describes the $R$-module structure of the 5-class group $S_K$.

**Theorem 5.18.** Let $p$ be a prime congruent to $\pm 7 \pmod{25}$ and $q$ be a prime congruent to $-1 \pmod{5}$. Let $F = \mathbb{Q}(\zeta_5)$ and $K = F((pq)^*)$. Assume that all ambiguous ideal classes are strongly ambiguous. Then, 125 divides the class number of $K$. More precisely, the $\lambda^2$-rank of $S_K$ is 1, and $3 \leq \text{rank}S_K \leq 5$.

**Proof.** Suppose firstly that $q \equiv -1 \pmod{25}$. Then, $q$ factors as $\pi_1 \pi_2$ in $F$ as in Theorem 5.15. Since $p \equiv \pm 7 \pmod{25}$, $p$ is prime in $F$. We have $N(p) = p^4 \equiv 1 \pmod{25}$ and $N(\pi_i) = q^2 \equiv 1 \pmod{25}$ for $i = 1, 2$. Thus $\zeta \in N_{K/F}(K^*)$. 


As in Theorem 5.15, we see that \( 1 + \zeta \) is a fifth power modulo \( \pi_1 \) and modulo \( \pi_2 \). Considering the intermediate field \( K_1 = F(p^{\frac{1}{5}}) \), we see that the Hasse formula from section 5.1 for this situation gives \( t_1 = d_1 - 3 + q_1^* = q_1^* - 2 \). Thus \( q_1^* = 2 \), that is, \( 1 + \zeta \) is a fifth power modulo \( p \). Thus \( 1 + \zeta \in N_{K_1/F}(K^*) \). We note that in this case \( \lambda \) does not ramify.

If \( q \not\equiv -1 \pmod{25} \), then \( N(\pi_i) = q^2 \not\equiv 1 \pmod{25} \) for \( i = 1, 2 \). But in this situation, \(-\zeta^2(1+\zeta) \in N_{K_1/F}(K^*) \). So \( q^* = 1 \) and \( \lambda \) ramifies. Combining these facts, we immediately see that, in both cases, \( t = q - 1 = 3 - 1 = 2 \).

Next we want to compute \( s_1 \). Let \( x_1 = \pi \) and \( x_2 = \pi^{a_1} \pi^{a_2} \) as in the proof of Theorem 5.15. When \( q \equiv -1 \pmod{25} \), to compute the matrix \( C_1 \), we need to compute the Hilbert symbols, \((\frac{x_1}{p})_p\), \((\frac{x_1}{\pi_1})_{\pi_1}\), \((\frac{x_1}{\pi_2})_{\pi_2}\), \((\frac{x_2}{\pi_1})_{\pi_1}\), \((\frac{x_2}{\pi_2})_{\pi_2}\). Using the formula given in [19][Chapter 14, Section 3], we can see as in Theorem 5.15, that

\[
\begin{pmatrix}
\frac{x_1, pq}{p} \\
\frac{x_1, pq}{\pi_1} \\
\frac{x_1, pq}{\pi_2}
\end{pmatrix}
= \begin{pmatrix}
\frac{x_1, pq}{\pi_1} \\
\frac{x_1, pq}{\pi_2}
\end{pmatrix}
= \begin{pmatrix}
\frac{x_2, pq}{\pi_1} \\
\frac{x_2, pq}{\pi_2}
\end{pmatrix} = 1,
\]

and \( \frac{x_2, pq}{\pi_1} \) \( \not\equiv 1 \). Thus, the \( 2 \times 3 \) matrix \( C_1 \) has only one nonzero entry. So \( s_1 = 1 \).

When \( q \not\equiv -1 \pmod{25} \), \( C_1 \) has one more column consisting of \( \frac{x_1, \lambda}{(\pi)} \) and \( \frac{x_2, \lambda}{(\pi)} \). We see as in 5.15, \( \frac{x_1, \lambda}{(\pi)} = 1 \) and since \( x_1 = \pm 7 \pmod{25} \), \( \frac{x_2, \lambda}{(\pi)} = 1 \) as well. Then. the \( 2 \times 4 \) matrix \( C_1 \) in this case also has only one nonzero entry. So \( s_1 = 1 \).

Thus we see that in both cases, the \( \lambda^2 \)-rank of \( S_K \) is \( t - s_1 = 1 \). Lastly, we observe that

\[
3 = 2t - s_1 \leq \text{rank} S_K \leq 4t - 3s_1 = 5.
\]

**Remarks.** If there are ambiguous ideal classes which are not strongly ambiguous, then in Theorem 5.15, \( s_1 \) can possibly be equal to 1; in that case, the rank of \( S_K \) would be 1. Similarly, in Theorem 5.18, \( s_1 \) can possibly be 2; in that case, the rank of \( S_K \) would be 2. But, we have not been able to find any example for either of these situations; perhaps, under the hypotheses of Theorem 5.16 or of Theorem 5.17, all ambiguous ideal classes are strongly ambiguous.

### 6. 5-class group of pure quintic fields

In this final section, we apply the results of the last section (especially Theorems 5.12, 5.13 and 5.14) to deduce results on some quintic extensions of \( \mathbb{Q} \). Let \( L \) be a degree 5 extension of \( \mathbb{Q} \) such that \( [L(\zeta_5) : L] = 4 \) and \( \text{Gal}(L(\zeta_5)/L) \cong \mathbb{Z}/4\mathbb{Z} = G \). Let \( K = L(\zeta_5) \). Write \( G = < \sigma > \).

Let \( \omega \) be the character \( G \to \mathbb{Z}_5^* \) which maps \( \sigma \) to 3 modulo 5. Note that \( \omega^2(\sigma) = -1 \).
Lemma 6.1. Let $C$ be a $\mathbb{Z}_5[G]$ module. Let $C(\omega^i) = \{ a \in C : \sigma a = \omega^i (\sigma a) \}$ for $i = 0, 1, 2, 3$. Then $C \cong C^+ \oplus C(\omega) \oplus C(\omega^2) \oplus C(\omega^3)$ where we have written $C^+$ for $C(\omega^0) = \{ a \in C | \sigma a = a \}$.

Proof. We omit the easy proof. \qed

Lemma 6.2. Let $S_K$ and $S_L$ denotes the 5-class group of $K$ and $L$ respectively. Then, $S_L \cong S_K^+ \oplus SL \cong (S_K/5S_K)^+$.

Proof. We have a natural inclusion $S_L \hookrightarrow S_K$ as 5 is relatively prime to $[K : L] = 4$. Moreover, $S_L \hookrightarrow S_K^+$ as $\sigma a = a$ for all $a \in S_L$. Let $a \in S_K^+$, then $a = 4 (\frac{1}{4} a) = (1 + \sigma + \sigma^2 + \sigma^3)(\frac{1}{4} a) = N(\frac{1}{4} a)$. Thus, $a \in S_L$. So $S_L \cong S_K^+$. Now, $S_L/5S_L \cong S_K^+/5(S_K^+ \cong (S_K/5S_K)^+$.

6.1 Decomposing $S_K$ under the affine group of $F_5$

Now let $L$ is a pure quintic field, that is $L = \mathbb{Q}(\sqrt[5]{n})$, where $n$ is a positive integer which does not contain any $5^{th}$ power. Let $F = \mathbb{Q}(\zeta_5)$ and $K = F(\sqrt[5]{n}) = L(\zeta_5)$. Then $K$ is a cyclic extension of degree 5 over $F$ and we can use the theory developed in the previous sections to determine $S_K$. Let $\sigma$ be a generator of $G = \text{Gal}(K/L)$ and $\tau$ be a generator of $\text{Gal}(K/F)$. We observe that, $K/\mathbb{Q}$ is Galois. We fix the generators $\sigma, \tau$ in $\text{Gal}(K/\mathbb{Q})$ satisfying the relations

$$\sigma^4 = \tau^5 = 1, \sigma \tau = \tau^3 \sigma.$$ 

Let $\lambda = 1 - \tau$.

Note that $S_K, 5S_K$ are $\mathbb{Z}_5[G]$-modules. Consider the filtration

$$S_K \supset \lambda S_K \supset \lambda^2 S_K \supset \lambda^3 S_K \supset 5S_K = \lambda^4 S_K.$$ 

Using the relations $\sigma \tau = \tau^3 \sigma$ and $\tau = 1 - \lambda$, we note that

$$\sigma \lambda = \lambda ((\lambda^2 - 3 \lambda + 3) \sigma a) \equiv 3 \lambda \sigma a \pmod{\lambda^2},$$
$$\sigma \lambda^2 a = 5 \lambda \sigma a - 6 \lambda^2 \sigma a + 2 \lambda^3 \sigma a \equiv -\lambda^2 \sigma a \pmod{\lambda^3},$$
$$\sigma \lambda^3 a = 10 \lambda \sigma a - 15 \lambda^2 \sigma a + 7 \lambda^3 \sigma a \equiv 2 \lambda^3 \sigma a \pmod{\lambda^4}.$$ 

Note that $\lambda^i S_K$ for $0 \leq i \leq 4$ are $\mathbb{Z}_5[G]$-modules. Using Lemma 6.1, we get for $0 \leq i \leq 3$,

$$\lambda^i S_K/5S_K \cong (\lambda^i S_K/5S_K)^+ \oplus \bigoplus_{j=1}^3 (\lambda^j S_K/\lambda^{j+1}S_K)(\omega^j),$$

$$\lambda^i S_K/\lambda^{i+1} S_K \cong (\lambda^i S_K/\lambda^{i+1}S_K)^+ \oplus \bigoplus_{j=1}^3 (\lambda^j S_K/\lambda^{j+1}S_K)(\omega^j).$$
The natural projection $ \lambda^i S_K / 5S_K \to \lambda^i S_K / \lambda^{i+1} S_K$ is surjective with kernel $\lambda^{i+1} S_K / 5S_K$. Restricting to the + part, we get the surjective map $(\lambda^i S_K / 5S_K)^+ \to (\lambda^i S_K / \lambda^{i+1} S_K)^+$ with kernel $(\lambda^{i+1} S_K / 5S_K)^+$. Since $(S_K / 5S_K)^+, (\lambda^i S_K / \lambda^{i+1} S_K)^+$ are of exponent 5, we have,

$$\text{rank} S_L = \text{rank}(S_K / 5S_K)^+ = \sum_{i=0}^{3} \text{rank}(\lambda^i S_K / \lambda^{i+1} S_K)^+.$$  

The rank of $(S_K / \lambda S_K)^+$ can be read off from the generators of the genus field, which we will describe at the end. We first determine the rank of $(\lambda^i S_K / \lambda^{i+1} S_K)^+$ for $i \geq 1$.

As before, consider the map induced by multiplication by $\lambda$:

$$\lambda^*: \lambda^i S_K / \lambda^{i+1} S_K \to \lambda^{i+1} S_K / \lambda^{i+2} S_K$$

$$a \pmod{\lambda^{i+1} S_K} \mapsto \lambda a \pmod{\lambda^{i+2} S_K}.$$  

Since $\sigma \lambda a = 3\lambda \sigma a \pmod{\lambda^2}$, we see that $\lambda_0^*$ induces surjective maps

$$\theta_i : (S_K / \lambda S_K)(\omega^i) \to (\lambda S_K / \lambda^2 S_K)(\omega^{i+1}) \text{ for } i = 0, 1, 2, 3.$$  

We note that $\sum_{i=0}^{3} \text{rank Ker} \theta_i = s_1$.

We have,

$$\text{rank}(\lambda S_K / \lambda^2 S_K)^+ = \text{rank}(S_K / \lambda S_K)(\omega^3) - \text{rank Ker} \theta_3.$$  

Similarly, since $\sigma \lambda^2 a = -\lambda^2 \sigma a \pmod{\lambda^3}$, we see that $\lambda_1^*$ induces surjective maps

$$\alpha_i : (\lambda S_K / \lambda^2 S_K)(\omega^i) \to (\lambda^2 S_K / \lambda^3 S_K)(\omega^{i+2}) \text{ for } i = 0, 1, 2, 3.$$  

We note that $\sum_{i=0}^{3} \text{rank Ker} \alpha_i = s_2$.

We have,

$$\text{rank}(\lambda^2 S_K / \lambda^3 S_K)^+ = \text{rank}(\lambda S_K / \lambda^2 S_K)(\omega^2) - \text{rank Ker} \alpha_2$$

$$= \text{rank}(S_K / \lambda S_K)(\omega) - \text{rank Ker} \theta_1 - \text{rank Ker} \alpha_2.$$  

Finally, since $\sigma \lambda^3 a = 2\lambda^3 \sigma a \pmod{\lambda^4}$, we see that $\lambda_2^*$ induces surjective maps

$$\beta_i : (\lambda^2 S_K / \lambda^3 S_K)(\omega^i) \to (\lambda^3 S_K / \lambda^4 S_K)(\omega^{i+3}) \text{ for } i = 0, 1, 2, 3.$$  

We note that $\sum_{i=0}^{3} \text{rank Ker} \beta_i = s_3$. 
We have,

\[
\text{rank} \left( \frac{\lambda^3 S_K}{\lambda^4 S_K} \right)^+ = \text{rank} \left( \frac{\lambda^2 S_K}{\lambda S_K} \right)(\omega) - \text{rank} \ker \beta_1 \\
= \text{rank} \left( \frac{\lambda S_K}{\lambda^2 S_K} \right)(\omega^3) - \text{rank} \ker \alpha_3 - \text{rank} \ker \beta_1 \\
= \text{rank} \left( \frac{S_K}{\lambda S_K} \right)(\omega^2) - \text{rank} \ker \theta_2 \\
- \text{rank} \ker \alpha_3 - \text{rank} \ker \beta_1
\]

Putting these together, we get

\[
\text{rank} S_L = \text{rank} \left( \frac{S_K}{\lambda S_K} \right) - (\text{rank} \ ker \theta_1 + \text{rank} \ ker \theta_2 + \text{rank} \ ker \theta_3 \\
+ \text{rank} \ ker \alpha_2 + \text{rank} \ ker \alpha_3 + \text{rank} \ ker \beta_1).
\]

Observing that \(\text{rank} \left( \frac{S_K}{\lambda S_K} \right) = t\), we see that \(\text{rank} S_L \leq t\). Also, noting that \(\sum_{i=0}^{3} \text{rank} \ ker \theta_i = s_1\), we obtain another upper bound for the rank of \(S_L\) as

\[
\text{rank} S_L \leq t - s_1 + \text{rank} \ ker \theta_0 \leq \text{rank} \left( \frac{S_K}{\lambda S_K} \right)^+ + (t - s_1).
\]

On the other hand, using \(\sum_{i=0}^{3} \text{rank} \ ker \alpha_i = s_2\) and \(\sum_{i=0}^{3} \text{rank} \ ker \beta_i = s_3\), we see that,

\[
\text{rank} S_L \geq t - s_1 - s_2 - s_3.
\]

Thus, we have proved the following theorem.

**Theorem 6.3.** Let \(L = \mathbb{Q}(\sqrt[5]{n})\), where \(n\) is an integer which does not contain any fifth power. Let \(F = \mathbb{Q}(\zeta_5)\) and \(K = F(\sqrt[5]{n}) = L(\zeta_5)\). Then,

\[
t - s_1 - s_2 - s_3 \leq \text{rank} S_L \leq \min (t, (t - s_1) + \text{rank} \left( \frac{S_K}{\lambda S_K} \right)^+).
\]

**Corollary 6.4.** When \(t = s_1\), \(\text{rank} S_L = \text{rank} \left( \frac{S_K}{\lambda S_K} \right)^+\).

**Proof.** Since \(t = s_1\), \(\lambda S_K = 5S_K\) and \(s_2 = s_3 = 0\). Thus \(\ker \alpha_i = \ker \beta_j = 0\) for all \(i, j\). Moreover, \(\lambda S_K / \lambda^2 S_K = 0\). So,

\[
\text{rank} S_L = \text{rank} \left( \frac{S_K}{\lambda S_K} \right)^+ + t - s_1 = \text{rank} \left( \frac{S_K}{\lambda S_K} \right)^+.
\]

6.2 Kummer duality to bound rank of \(\left( \frac{S_K}{\lambda S_K} \right)^+\)

Finally we describe how one can determine \(\text{rank} \left( \frac{S_K}{\lambda S_K} \right)^+\) or give an upper bound for this rank. Let \(M\) be the maximal abelian unramified extension of \(K\) with exponent 5. By class field theory, we have, \(S_K / 5S_K \cong \text{Gal}(M/K)\). By Kummer theory there exists a subgroup \(A\) of \(K^*\),

\[
(K^*)^5 \subset A \subset K^*.
\]
such that $M = K(\sqrt[3]{A})$. We have a bilinear pairing

$$A/(K^*)^5 \times \text{Gal}(M/K) \to \{5^\text{th} \text{ roots of unity}\}$$

$$(x, \mu) \mapsto [x, \mu] = (x^{\frac{1}{5}})^{\mu^{-1}}.$$  

By Kummer theory $A/(K^*)^5$ and $\text{Gal}(M/K)$ are dual groups with respect to this pairing. Thus identifying $S_K/5S_K$ with $\text{Gal}(M/K)$ we see that $A/(K^*)^5$ and $S_K/5S_K$ are dual groups in the bilinear pairing. Let $M_1$ be a field $K \subset M_1 \subset M$ and $M_1/K$ is Galois. By Kummer theory, there is a subgroup $B$ of $A$ such that

$$(K^*)^5 \subset B \subset A \subset K^*$$

and $M_1 = K(\sqrt[5]{B})$. Moreover, there is a group $T$, satisfying $5S_K \subset T \subset S_K$, such that $S_K/T$ is dual of $B/(K^*)^5$ and $S_K/T \cong \text{Gal}(M_1/K)$. One can easily check that $[x^\sigma, \mu^\sigma] = [x, \mu]^\sigma$, where $\sigma$ is the generator of $\text{Gal}(K/L)$.

Writing

$$(B/(K^*)^5)^+ = \{b \in B/(K^*)^5 | b^5 = b\},$$

$$(B/(K^*)^5)(\omega) = \{b \in B/(K^*)^5 | b^5 = b^3\},$$

$$(B/(K^*)^5)(\omega^2) = \{b \in B/(K^*)^5 | b^5 = b^{-1}\},$$

$$(B/(K^*)^5)(\omega^3) = \{b \in B/(K^*)^5 | b^5 = b^2\},$$

we have the following lemma:

**Lemma 6.5.** Let

$$B/(K^*)^5 \times S_K/T \to \{5^\text{th} \text{ roots of unity in } K\}$$

$$(x, \mu) \mapsto [x, \mu]$$

be the bilinear pairing described above. Then $(B/(K^*)^5)^+$ is dual to $(S_K/T)(\omega)$ under the pairing. Similarly, $(B/(K^*)^5)(\omega)$ is dual to $(S_K/T)(\omega^2)$, $(B/(K^*)^5)(\omega^2)$ is dual to $(S_K/T)^+$ and $(B/(K^*)^5)(\omega^3)$ is dual to $(S_K/T)(\omega^2)$ under this pairing.

**Proof.** Let $x \in (B/(K^*)^5)^+$ and $\mu \in (S_K/T)^+$. Then $[x, \mu] = [x^{\sigma}, \mu^{\sigma}]$ $= [x, \mu]^\sigma = [x, \mu]^3$, since $\zeta^3 = \zeta^3$. Thus $[x, \mu]^2 = 1$, hence $[x, \mu] = 1$. Thus $(B/(K^*)^5)^+$ and $(S_K/T)^+$ are orthogonal in this pairing.

Now, let $x \in (B/(K^*)^5)^+$ and $\mu \in (S_K/T)(\omega^2)$. Then $[x, \mu] = [x^{\sigma}, (\mu^{-1})^{\sigma}] = [x, \mu^{-1}]^{\sigma} = ([x, \mu^{-1}]^{\sigma} = [x, \mu]^2$, since $\zeta^3 = \zeta^3$. Thus $[x, \mu] = 1$. We see that, $(B/(K^*)^5)^+$ and $(S_K/T)(\omega^2)$ are orthogonal in this pairing.
Finally, let \( x \in (B/(K^*)^5)^+ \) and \( \mu \in (S_K/T)(\omega^3) \). Then \([x, \mu] = [x^5, (\mu^5)^5] = [x, \mu]^5 = [x, \mu]^{-1}, \) since \( \zeta^5 = \zeta^3 \). Thus \([x, \mu]^2 = 1, \) hence \([x, \mu] = 1. \) Thus \((B/(K^*)^5)^+\) and \((S_K/T)(\omega^3)\) are orthogonal in this pairing.

The other cases are similar and the duality claimed easily follows. \( \square \)

Let \( M_1 = K(x_1^{\frac{1}{5}}, \ldots, x_r^{\frac{1}{5}}) \) be the genus field of \( K/F, \) that is \( S_K/\lambda S_K \cong \text{Gal}(M_1/K). \) Suppose \( x_1, \ldots, x_w \) are the rational numbers among the \( x_i \)'s. Then, \( \text{rank}(B/(K^*)^5)^+ = w. \) Suppose \( x_{w+1}, \ldots, x_r \) are the \( x_i \)'s whose factors only contain rational numbers and primes of the form \( a\zeta^2 + a\zeta^3 + b. \) Noticing that for an element \( \pi = a\zeta^2 + a\zeta^3 + b, \) we get \( \pi^2 = \pi \neq \pi^3, \) we have

\[
\text{rank}(B/(K^*)^5)(\omega^2) = r - w
\]

and

\[
\text{rank}(B/(K^*)^5)(\omega) \oplus (B/(K^*)^5)(\omega^3) = t - r.
\]

Hence

\[
\text{rank}(S_K/\lambda S_K)^+ \leq t - r.
\]

In particular, we obtain the theorem:

**Theorem 6.6.** Let \( L = \mathbb{Q}(n^{\frac{1}{5}}), \) where \( n = p_1^{a_1} \cdots p_m^{a_m} q_1^{b_1} \cdots q_u^{b_u} \) where \( p_i \equiv \pm 2 \pmod{5}, q_j \equiv -1 \pmod{5} \) and \( 1 \leq a_i, b_j \leq 4 \) for \( i \in \{1, \ldots, m\} \) and for \( j \in \{1, \ldots, u\}. \) Let \( F = \mathbb{Q}(\zeta_5) \) and \( K = F(n^{\frac{1}{5}}) = L(\zeta_5). \) Then \( \text{rank}(S_K/\lambda S_K)^+ = 0 \) and

\[
t - s_1 - s_2 = \lambda - \text{rank} S_K \leq \lambda^2 - \text{rank} S_K = t - s_1.
\]

**Proof.** As proved in proposition 5.8 and Theorem 5.15, all the generators of the genus field \( M_1 \) are either rational integers with prime factors \( p_i \) or contains factors of \( q_j \) in \( F. \) But, as we proved in Theorem 5.15, factors of \( q_j \)'s are of the form \( a\zeta^2 + a\zeta^3 + b. \) Hence, with \( r \) as defined before the theorem, we have \( r = t. \) Notice that both \((S_K/\lambda S_K)^+\) and \((S_K/\lambda S_K)(\omega^2)\) are 0 in this case. Therefore, we have

\[
t - s_1 \geq \text{rank} S_L = t - s_1 - \text{rank Ker}_2 = (t - s_1 - s_2) + \text{rank Ker}_0 \geq t - s_1 - s_2. \quad \square
\]

**Remarks.** (i) We would have better results if we can get more information about \( \text{rank} (S_K/\lambda S_K)^+. \)

(ii) Under the assumption that all ambiguous ideal classes are strongly ambiguous, we computed the \( \lambda^2 \)-rank of \( S_K \) in Theorems 5.12, 5.13, 5.14, 5.15 and 5.18. If there are ambiguous ideal classes which are not strongly ambiguous, the maximum value of \( s_1 \) is given.
Corollary 6.7. Let \( L = \mathbb{Q}(N^{1/2}) \). In the following cases \( S_L \) is trivial or cyclic.

- Let \( N = p^a \), where \( p \equiv \pm 2 \pmod{5} \) is a prime, \( 1 \leq a \leq 4 \).
- Let \( N = q_1^{a_1} q_2^{a_2} \) where \( q_i \equiv \pm 2 \pmod{5} \) but \( q_i \not\equiv \pm 7 \pmod{25} \), \( 1 \leq a_i \leq 4 \) for \( i = 1, 2 \) such that \( N \equiv \pm 1, \pm 7 \pmod{25} \).
- Let \( N = p^a \), where \( p \equiv -1 \pmod{5} \) is a prime, \( 1 \leq a \leq 4 \).
- Let \( N = p_1^{a_1} p_2^{a_2} \) where \( p_i \equiv \pm 7 \pmod{5} \) (mod 25), \( 1 \leq a_i \leq 4 \) for \( i = 1, 2 \) such that \( N \equiv \pm 1, \pm 7 \pmod{25} \).
- Let \( N = p^a q^b \) where \( p \equiv \mp 7 \pmod{25} \), \( q \equiv \pm 2 \pmod{5} \) but \( q \not\equiv \pm 7 \pmod{25} \) and \( 1 \leq a, b \leq 4 \) such that \( N \not\equiv \pm 1, \pm 7 \pmod{25} \).
- Let \( N = q_1^{a_1} q_2^{a_2} \) where \( q_i \equiv \pm 2 \pmod{5} \) but \( q_i \not\equiv \pm 7 \pmod{25} \), \( 1 \leq a_i \leq 4 \) for \( i = 1, 2 \) such that \( N \not\equiv \pm 1, \pm 7 \pmod{25} \).
- Let \( N = p^a q^b \) where \( p \equiv \mp 7 \pmod{25} \), \( q \equiv \pm 2 \pmod{5} \) but \( q \not\equiv \pm 7 \pmod{25} \), \( 1 \leq a, b \leq 4 \) such that \( N \not\equiv \pm 1, \pm 7 \pmod{25} \).
- Let \( N = p^a q^b \), where \( p \equiv -1 \pmod{5} \) and \( q \equiv \pm 7 \pmod{25} \) are primes, \( 1 \leq a, b \leq 4 \).

Proof. In all these situations, \( \text{rank}(S_K / \lambda S_K)^+ = 0 \). From Theorem 5.12, 5.13, 5.14, 5.15 follows that for each of these cases except the last case \( t = 0 \) or 1. In the last case, we see from Theorem 5.18 that \( t = 2 \) and \( s_1 \geq 1 \). Thus \( \text{rank} S_L \leq 1 \). The result follows. Note that, in the first two cases the class groups are trivial.

Remark. Let \( f \) be a normalized cuspidal Hecke eigenform of weight \( k \) and level \( N \). Let \( K_f \) denote the extension of \( \mathbb{Q}_5 \) generated by the \( q \)-expansion coefficients \( a_n(f) \) of \( f \). It is known that \( K_f \) is a finite extension of \( \mathbb{Q}_5 \). In the case \( N \) is prime and \( 5 | |N| - 1 \), it is known [16] that there exists unique (up to conjugation) weight 2 normalized cuspidal Hecke eigenform defined over \( \mathbb{Q}_5 \), satisfying the congruence

\[
a_i(f) \equiv 1 + l \pmod{p}
\]

where \( p \) is the maximal ideal of the ring of integer of \( K_f \), and \( l \not\equiv N \) are primes. In this situation it is also known that \( K_f \) is a totally ramified extension of \( \mathbb{Q}_5 \) and \( [K_f : \mathbb{Q}_5] = e_5 \). Calegari and Emerton [1] showed that \( e_5 = 1 \) if the class group of \( \mathbb{Q}(N^{1/2}) \) is cyclic. They also showed that if \( N \equiv 1 \pmod{5} \), and the 5-class group of \( \mathbb{Q}(N^{1/2}) \) is cyclic, then \( \prod_{i=1}^{(N-1)/2} l_i^i \) is not a 5th power modulo \( N \). This corollary gives us information when 5-class group of \( \mathbb{Q}(N^{1/2}) \) is cyclic for various \( N \).
Table 4. Structure of 5 class group of $L$.

<table>
<thead>
<tr>
<th>$n$</th>
<th>$S_L$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2 \times 7$</td>
<td>1</td>
</tr>
<tr>
<td>$3 \times 7$</td>
<td>1</td>
</tr>
<tr>
<td>$7 \times 43$</td>
<td>1</td>
</tr>
<tr>
<td>$2 \times 3 \times 7$</td>
<td>$C_5$</td>
</tr>
<tr>
<td>$2 \times 13 \times 7$</td>
<td>$C_5$</td>
</tr>
<tr>
<td>$7 \times 107$</td>
<td>$C_5$</td>
</tr>
<tr>
<td>$3 \times 13 \times 7$</td>
<td>$C_5 \times C_5$</td>
</tr>
<tr>
<td>19, 29, 59, 79, 89, 109, 139, 149, 179, 199, 229, 239, 269, 349</td>
<td>$C_5$</td>
</tr>
<tr>
<td>7 \times 19, 7 \times 29, 7 \times 59, 7 \times 79, 7 \times 89, 7 \times 149, 7 \times 199</td>
<td>$C_5$</td>
</tr>
<tr>
<td>43 \times 19, 43 \times 29, 43 \times 59, 43 \times 79, 43 \times 89, 43 \times 149, 43 \times 199</td>
<td>$C_5$</td>
</tr>
<tr>
<td>11, 41, 61, 71, 101, 151, 191, 241, 251, 271</td>
<td>$C_5$</td>
</tr>
<tr>
<td>31, 131, 181</td>
<td>$C_5 \times C_5$</td>
</tr>
<tr>
<td>211, 281</td>
<td>$C_5 \times C_5 \times C_5$</td>
</tr>
</tbody>
</table>

Acknowledgments

It is a pleasure to thank Dipendra Prasad for clarifications regarding genus theory. We are also indebted to Suprio Bhar for help with some computer codes in SAGE. We would like to acknowledge our gratitude to Georges Gras who drew our attention to his work which we were initially ignorant of. We also thank Mahesh Kakde who suggested that some results may be of interest to Iwasawa theorists and suggested us to send them to John Coates. We are grateful to Coates for his subsequent suggestion to highlight Theorem 5.16 which may be useful in studying elliptic curves over towers of the form $\mathbb{Q}(e^{\frac{2\pi i}{5n}}, x^{1/5})$. Finally, we are extremely grateful to the referee who not only first brought our attention to the work of Rédei, Greither, Kučera et al. but made several constructive suggestions which led us to use the right language and to prove more results than we had earlier. In particular, thanks to him, the section 6 is now simpler and more general than what we had.

References


