J. E. Carroll
H. Kisilevsky

Initial layers of $\mathbb{Z}_l$-extensions of complex quadratic fields


<http://www.numdam.org/item?id=CM_1976__32_2_157_0>
INITIAL LAYERS OF $\mathbb{Z}_l$-EXTENSIONS OF COMPLEX QUADRATIC FIELDS

J. E. Carroll and H. Kisilevsky*

Introduction

If $F$ is a number field and $l$ a prime, a $\mathbb{Z}_l$-extension, $K$, of $F$ is a normal extension with Galois group topologically isomorphic to the additive $l$-adic integers. For example, the extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a $\mathbb{Z}_l$-extension, where $\mathbb{Q}(\zeta)$ is the subfield of $\mathbb{Q}(\mu_{\infty})$ the cyclotomic field of all $l$ power roots of unity which is fixed by an automorphism of order $l - 1$. For any number field $F$, the $\mathbb{Z}_l$-extension $F \cdot \mathbb{Q}(\zeta)/F$ is called the cyclotomic $\mathbb{Z}_l$-extension of $F$. If $L$ is the composite of all $\mathbb{Z}_l$-extensions of $F$, then $\text{Gal}(L/F) \cong \mathbb{Z}_l^a$ for an integer $a$. It is known that $r_2 + 1 \leq a \leq d$ where $r_2$ is the number of complex embeddings of $F$ and $d = [F : \mathbb{Q}]$ (see [6]), and Leopoldt's conjecture is equivalent to $a = r_2 + 1$.

In this article, we consider the case that $F$ is a complex quadratic field. We try to find a canonical $\mathbb{Z}_l$-extension, $K_2$, of $F$, disjoint from the cyclotomic $\mathbb{Z}_l$-extension, $K_1$, of $F$ such that $L = K_1K_2$ (c.f. [4], [8]). We determine the initial layers of $K_2$ in some cases by considering the torsion subgroup, $T$, of the Galois group of the maximal abelian $l$-ramified, i.e., unramified at all primes not dividing $l$, pro-$l$ extension of $F$.

For an abelian group $A$, and a prime $l$, we denote by $A(l)$ the $l$-power torsion subgroup of $A$, and by $A_l$ the subgroup of elements of $A$ of exponent $l$.

I

Let $F/\mathbb{Q}$ be normal and let $l$ be a prime number. Let $M$ be the maximal normal extension of $F$ such that the Galois group, $G = \text{Gal}(M/F)$ is an abelian pro-$l$ group and such that $M/F$ is $l$-ramified. Then $M$ is a normal

* Supported in part by NSF Grant GP-40871.
extension of $\mathbb{Q}$ and $\text{Gal}(F/\mathbb{Q})$ acts on $G$ by conjugation. We shall consider the structure of $G$ as a $\mathbb{Z}_l$-module and as a $\text{Gal}(F/\mathbb{Q})$-module.

**Lemma (1):** If $[F : \mathbb{Q}] < \infty$, then $G$ is a finitely generated $\mathbb{Z}_l$-module.

**Proof:** It suffices to show that $G/IG$ is finite [9, §6]. Now $G/IG$ is a quotient of the Galois group over $F(\zeta)$ of the composite of all cyclic, degree $l$, $l$-ramified extensions of $F(\zeta)$, where $\zeta$ is a primitive $l$th root of 1. Thus, it is enough to show that $F(\zeta)$ has only finitely many cyclic $l$-ramified extensions of degree $l$. By Kummer theory, all such extensions are of the form $F(\zeta, \alpha^{1/l})$, $\alpha \in F(\zeta)$. But $F(\zeta, \alpha^{1/l})/F(\zeta)$ is $l$-ramified if and only if the principal ideal $(\alpha) = \mathfrak{A} \mathfrak{B}^l$ where $\mathfrak{A}$ is a product of primes dividing $l$. Let $A$ be the set of all such $\alpha$. Then we have an exact sequence,

$$0 \to U_\mathfrak{S}/U_\mathfrak{S}^l \to A/F(\zeta)^{*l} \to (C_S)_l \to 0$$

where $S$ is the set of primes of $F(\zeta)$ dividing $l$, $U_\mathfrak{S}$ is the group of $S$-units in $F(\zeta)$, and $(C_S)_l$ is the group of elements of exponent $l$ in the $S$-class group of $F(\zeta)$. But $C_S$ is finite and, by the $S$-unit theorem, $U_\mathfrak{S}$ is finitely generated. Hence $A/F(\zeta)^{*l}$ is finite.

**Corollary (2):** $G \approx T \oplus \mathbb{Z}_l^a$ where $T$ is a finite abelian $l$-group.

**Proof:** $G$ is a finitely generated module over $\mathbb{Z}_l$, which is a p.i.d.

We now restrict our attention to $F$ complex quadratic. By the validity of Leopoldt's conjecture in this case, $a = 2$. Let $\tau$ denote complex conjugation on $M$. Then $\tau$ generates $\text{Gal}(F/\mathbb{Q})$ and so acts on $G$. The torsion subgroup, $T$, of $G$ is stabilized by $\tau$ so the fixed field, $L$, of $T$ is normal over $\mathbb{Q}$, and $\tau$ acts on $\text{Gal}(L/F) \approx \mathbb{Z}_l \oplus \mathbb{Z}_l$. It is easy to see that $L$ is the composite of all $\mathbb{Z}_l$-extensions of $F$. In particular, if $K_1$ is the cyclotomic $\mathbb{Z}_l$-extension of $F$, then $K_1 \subset L$. We consider the question of finding a complement, $K_2$, to $K_1$, i.e. a $\mathbb{Z}_l$-extension, $K_2/F$, such that $K_1 \cap K_2 = F$ and $K_2/\mathbb{Q}$ is normal.

**Theorem (3):** If $l$ is odd or if $l = 2$ and all quadratic subextensions of $L/F$ are normal over $\mathbb{Q}$, then there is a unique complement, $K_2$, to $K_1$. Furthermore, if we write

$$\text{Gal}(L/F) = H_1 \oplus H_2 \text{ where } H_i = \text{Gal}(L/K_i) \approx \mathbb{Z}_l,$$

then $\tau$ inverts the elements of $H_1$ and acts trivially on $H_2$. 
PROOF: We have an exact sequence

\[ 0 \to H_1 \to \text{Gal}(L/F) \to \mathbb{Z}_l \to 0 \]

which implies that \( H_1 \cong \mathbb{Z}_l \). Let \( a \) be a generator of \( \text{Gal}(L/F) \) modulo \( H_1 \). Since \( K_1/Q \) is normal abelian, \( H_1 \) is a \( \tau \) submodule and \( a' = a + h_1 \) for some \( h_1 \in H_1 \). Now \( \tau \) has order 2, so either inverts \( H_1 \) or acts trivially. But if \( \tau \) acted trivially we would have \( a = a'^2 = a + 2h_1 \) so \( h_1 = 0 \) and \( a^2 = a \). This would imply that \( L/Q \) was abelian and that if \( L \) were the subfield of \( L \) fixed by \( \tau \), then \( L/Q \) would be \( l \)-ramified abelian with \( \text{Gal}(L/Q) \cong \mathbb{Z}_l \oplus \mathbb{Z}_l \) contradicting the Kronecker-Weber theorem. Therefore, \( \tau \) inverts \( H_1 \). Now if \( h_2 \in 2H_1 \) and we let \( h_2 = a + h_1/2 \), then \( h_2 = h_2 \) so we can take \( H_2 \) to be the \( \mathbb{Z}_l \)-module generated by \( h_2 \). But \( H_1 = 2H_1 \) for \( l \) odd. For \( l = 2 \), the sequence (1) implies that \( h_1 \in 2H_1 \) if and only if \( h_1 \in 2 \text{Gal}(L/F) \) since \( \mathbb{Z}_2 \) has no torsion. But all quadratic subfields of \( L/F \) are normal over \( Q \) if and only if

\[ a^2 \equiv a \mod 2 \text{Gal}(L/F). \]

To show uniqueness, it is enough to show that any cyclic submodule of \( \text{Gal}(L/F) \) which is invariant under \( \tau \) lies in \( H_1 \) or \( H_2 \). This follows from the following lemma.

**LEMMA (4):** The \( \mathbb{Z}_l \)-submodules of \( H_1 \oplus H_2 \) invariant by \( \tau \) are of the form \( l^{m_1}H_1 \oplus l^{m_2}H_2 \) for \( l \) odd, and of the form \( 2^{m_1}H_1 \oplus 2^{m_2}H_2 \) or \( \langle 2^{m_1}H_1 \oplus 2^{m_2}H_2, 2^{m_1-1}h_1 + 2^{m_2-1}h_2 \rangle \) where \( h_i \) is a generator of \( H_i \) as a \( \mathbb{Z}_2 \)-module for \( l = 2 \).

**Proof:** Let \( H \) be invariant under \( \tau \). If \( a_1h_1 + a_2h_2 \in H, \ a_i \in \mathbb{Z}_l \) then \( (1+\tau)(a_1h_1 + a_2h_2) = 2a_2h_2 \in H, \ (1-\tau)(a_1h_1 + a_2h_2) = 2a_1h_1 \in H \). If \( l \) is odd we get \( a_ih_i \in H \) so \( H \) is the direct sum of its projections onto the \( H_i \). If \( l = 2 \) we see \( 2^{m_1}H_1 \oplus 2^{m_2}H_2 \subset H \subset 2^{m_1-1}H_1 \oplus 2^{m_2-1}H_2 \) for some \( m_1, m_2 \) and, noting that \( \langle 2^{m_1}H_1 \oplus 2^{m_2}H_2, 2^{m_1-1}h_1 + 2^{m_2-1}h_2 \rangle \) is in fact invariant under \( \tau \), we are done.

**Remarks:**

(i) If \( l \) is odd, then \( H_1 = (1-\tau)\text{Gal}(L/F), H_2 = (1+\tau)\text{Gal}(L/F) \).

(ii) By [2, § 3], if \( F = \mathbb{Q}(\sqrt{-d}) \) where at least one odd prime dividing \( d \) is not congruent to \( \pm 1 \) modulus 8, then all quadratic subextensions of \( L/F \) are normal over \( \mathbb{Q} \). This condition is not necessary, however, since, e.g., \( \mathbb{Q}(\sqrt{-p}), p \equiv 9(16) \) also has this property. From now on we assume that all quadratic subextensions of \( L \) are normal over \( \mathbb{Q} \).
THEOREM (5): If \( l \) is odd, then \( G \cong T \oplus H_1 \oplus H_2 \) where \( T \) is a finite abelian \( l \)-group, and \( \tau \) inverts the elements of \( T \) and of \( H_1 \) and acts trivially on \( H_2 \).

PROOF: By Corollary 2, \( G \cong T \oplus H_1 \oplus H_2 \) as \( \mathbb{Z}_l \)-modules, where \( T \) is invariant under \( \tau \). Choose \( a_1, a_2 \in G \) such that \( a_i + T \) generates \( H_i \). Then
\[
a'_1 = -a_1 + t_1, \quad a'_2 = a_2 + t_2, \quad t_i \in T.
\]
Applying \( \tau \) again we have
\[
a_1 = a'_1^2 = a_1 - t_1 + t'_1, \quad a_2 = a'_2^2 = a_2 + t_2 + t'_2.
\]
Thus \( t'_1 = t_1, \quad t'_2 = -t_2 \). Let \( h_1 = a_1 - t_1/2, \quad h_2 = a_2 + t_2/2 \). Then \( h'_1 = -h_1, \quad h'_2 = h_2 \). It follows that we can write \( G = T \oplus H_1 \oplus H_2 \) where \( H_i \) is now taken to be the cyclic module generated by \( h_i \). Now write \( T = (1 + \tau)T \oplus (1 - \tau)T \) so that \( \tau \) acts trivially on the first factor and inverts the second. Let \( K' \) be the subfield of \( M \) fixed by \( (1 - \tau)T \oplus H_1 \). Then \( K'/F \) is an abelian \( l \)-ramified pro-\( l \) extension such that \( \tau \) acts trivially on \( \text{Gal}(K'/F) \). Hence \( K'/Q \) is abelian and so if \( K'' \) is the subfield of \( K' \) fixed by \( \tau \), then \( K''/Q \) is an abelian \( l \)-ramified pro-\( l \) extension with
\[
\text{Gal}(K''/Q) \cong \mathbb{Z}_l \oplus (1 + \tau)T.
\]
By the Kronecker-Weber theorem, \( (1 + \tau)T = 0 \). Thus \( \tau \) inverts all elements of \( T \).

REMARK: When \( l = 2 \) an analogous decomposition into the direct sum of \( \tau \)-modules is not generally possible. If all odd primes dividing the discriminant of \( F \) are congruent to \( \pm 1 \) modulo 8, for example, such a decomposition can not occur even if the conditions of Theorem 3 are satisfied.

II

We next consider the finite group \( T \)

THEOREM (6): Let \( S \) be the set of primes dividing \( l \) in \( F \); \( U_\wp \) the group of units in the completion \( F_\wp \) of \( F \) at \( \wp \); \( \bar{U} \) the closure of the group of units, \( U \), of \( F \) in \( \prod_{\wp \in S} U_\wp \); and let \( C \) be the class group of \( F \). Then we have an exact sequence
\[
0 \to (\prod_{\wp \in S} U_\wp)/\bar{U}(l) \to T \to C(l).
\]
PROOF (c.f. [2]): By class field theory, \( \text{Gal}(M/F) \cong J/F^*J^S(l) \) where \( J \) is the idèle group of \( F \) and \( J^S \) is the subgroup, \( J^S = \prod_{p \in S} \{1\} \times \prod_{p \notin S} U_p \). The map

\[
J \rightarrow C, \quad (x_p) \mapsto \text{class of } \prod p^{y_p(x_p)}
\]

is continuous and \( F^*J^S \) lies in the kernel, so we obtain a continuous surjection \( J/F^*J^S \rightarrow C \). The kernel of this map is naturally isomorphic to \( (\prod_{p \in S} U_p)/\bar{U} \), and we obtain the desired sequence by taking \( l \)-power torsion.

We note that since \( F \) is complex quadratic, \( U \) is finite, so \( U = \bar{U} \).

**COROLLARY (7):** If \( l \) is odd then \( T \rightarrow C(l) \) is injective unless \( l = 3 \) and \( F = \mathbb{Q}(\sqrt{-3m}) \), \( m \equiv 1(3) \), \( m \neq 1 \). In this case \( (\prod_{p \in S} U_p)/U(3) \) has order 3.

**PROOF:** If \( l > 3 \), then \( U_p \) contains no primitive \( l \)-th root of 1 as \( [F_p : F] \leq 2 \). Since \( U \) consists of roots of 1, the quotient has no element of order \( l \). If \( l = 3 \), then \( U_p \) contains a primitive cube root of 1 exactly when \( F = \mathbb{Q}(\sqrt{-3m}) \), \( m \equiv 1(3) \) but no ninth root of 1, and \( U \) contains no cube root of 1 unless \( m = 1 \). Since there is only one prime in \( S \),

\[
((\prod_{p \in S} U_p)/U(3))
\]

has order 3, if \( m \neq 1 \) (and is trivial for \( m = 1 \)).

**COROLLARY (8):** If \( l = 2 \), \( T \rightarrow C(2) \) is injective unless \( F = \mathbb{Q}(\sqrt{-d}) \) and \( d \equiv \pm 1(8) \). If \( d \equiv \pm 1(8) \) we have an exact sequence

\[
0 \rightarrow \mathbb{Z}/2\mathbb{Z} \rightarrow T \rightarrow \text{image } T \rightarrow 0
\]

which splits if \( d \equiv -1(8) \) and does not split if \( d \equiv 1(8) \).

**PROOF:** See [2, § 2].

We can also bound \( T \) from below in terms of \( C(l) \).

**PROPOSITION (9):** If \( \bar{F} \) is the \( l \)-Hilbert class field of \( F \) then \( \text{Gal}(\bar{F}/\bar{F} \cap L) \) is a quotient of \( T \).

**PROOF:** We have \( \bar{F}L \subseteq M \), so \( \text{Gal}(\bar{F}L/L) \cong \text{Gal}(\bar{F}/\bar{F} \cap L) \) is a quotient of \( \text{Gal}(M/L) = T \).
We are indebted to the referee for pointing out that it is usually (not always) true that $T = \text{Gal}(\bar{F}L/L)$ and that $M = \bar{F}L$.

By lemma 4 the maximal subfield of $L$ whose Galois group over $F$ is acted on by inversion by $\tau$ is $K_2$ for $l$ odd, and $K_2(\sqrt{2})$ for $l = 2$. Since $\text{Gal}(\bar{F}/F)$ is inverted by $\tau$, $\bar{F} \cap L$ lies in these subfields.

**Corollary (10):** Let $l^n$ be the exponent of $C(l)$. Then $|C(l)|/l^n$ divides $|T|$ if $l$ is odd and $|C(2)|/2^{n+1}$ divides $|T|$.

**Proof:** $\text{Gal}(\bar{F} \cap K_2/F)$ is a quotient of $C(l)$ and $\text{Gal}(K_2/F)$ for $l$ odd or of $C(2)$ and $\text{Gal}(K_2(\sqrt{2})/F)$ for $l = 2$.

**III**

The following result is useful in restricting the possible candidates for the initial layers of $K_2$

**Theorem (11):** Let $p \neq l$ be a prime number such that a unique prime $\mathfrak{p}$ of $F$ divides it. Then $K_2$ is the unique $\mathbb{Z}_l$-extension of $F$ in which $\mathfrak{p}$ splits completely.

**Proof:** Let $H$ be the decomposition group of $\mathfrak{p}$ in $\text{Gal}(L/F)$. Since $p^r = \mathfrak{p}$, $H$ is normal in $\text{Gal}(L/Q)$. But since $\mathfrak{p}$ does not ramify in $L$, $H$ is a cyclic $\mathbb{Z}_l$-submodule of $\text{Gal}(L/F)$. Hence, by the proof of Theorem 3, $H \subset H_1$ or $H_2$. But if $H \subset H_1$, then $\mathfrak{p}$ would split completely in $K_1$, which is not the case [3, § II]. Thus $H \subset H_2$, and $\mathfrak{p}$ splits completely in $K_2$. Any two cyclic $\mathbb{Z}_l$-submodules of $\text{Gal}(L/F)$ intersect trivially or in one of the modules so the subgroups fixing any two distinct $\mathbb{Z}_l$-extensions are disjoint. Thus if $\mathfrak{p}$ split completely in any $\mathbb{Z}_l$-extension besides $K_2$, $\mathfrak{p}$ would split completely in $L$, and so in $K_1$, which is not possible.

The following theorem tells us that if $K$ is a sufficiently large cyclic $l$-ramified $l$-extension of $F$ normal over $\mathbb{Q}$, then $K$ must have a sizeable intersection with $K_1$ or $K_2$. If $\tau$ inverts $\text{Gal}(K/F)$, then, the intersection must be with $K_2$.

**Theorem (12):** Let $\ell^r T = 0$. Suppose $K/F$ is a cyclic $l$-ramified extension of degree $\ell^n$ with $n > r$ if $l$ is odd and $n > r + 1$ if $l = 2$, and that $K/Q$ is normal. Then the subextension of $K/F$ of degree $\ell^{n-r}$ if $l$ is odd and $\ell^{n-r-1}$ if $l = 2$ lies either in $K_1$ or $K_2$. 
PROOF: As we noted in the proof of Theorem 5, $G \cong T \oplus H_1 \oplus H_2$ as $\mathbb{Z}_p$-modules (and even as $\tau$ modules for $l$ odd). Let $H$ be the subgroup of $G$ fixing $K$. We consider the case $l$ odd. Since $H$ is normal, by Lemma 4 the projection of $H$ into $H_1 \oplus H_2$ must be of the form $l^{m_1}H_1 \oplus l^{m_2}H_2$. By the cyclicity of $G/H$, either $m_1$ or $m_2$ is 0. Say $m_1 = 0$. Also $l^rH = 0 \oplus l^rH_1 \oplus l^{m_2 + r}H_2 \subset H$. Since $|G/H| = l^n$ we see that, $m_2 + r \geq n$. Thus we see that $H \subset T \oplus H_1 \oplus l^{n-r}H_2$ or if $m_2 = 0$, $T \oplus l^{n-r}H_1 \oplus H_2$, i.e. the subextension of degree $l^{n-r}$ of either $K_1$ or $K_2$ is contained in $K$. The proof for $l = 2$ is similar.

IV. We now compute a few examples

Example 1

Let $l = 2$, $F = \mathbb{Q}(\sqrt{-p})$, where $p \equiv 5 \pmod{8}$. Then $C(2)$ is cyclic, and $\bar{p}_2$ is not a square in $C$, where $p_2$ is the prime of $F$ dividing 2, and $\bar{p}_2$ is the class of $p_2$ in $C$, (see the proof of Lemma 13). Thus $\bar{p}_2$ generates $C(2)$ and $C_s(2) = 0$.

It is not hard to prove that we have an exact sequence similar to that of Theorem 6,

$$0 \to \left( \prod_{p \in S} F_p \right) / U_S(l) \to T \to C_S(l)$$

which in this case reduces to $T = 0$ since $-1, 2, -2$ are non-squares in $F_p = \mathbb{Q}_2(\sqrt{3})$. Let $\varepsilon$ be a fundamental unit of $\mathbb{Q}(\sqrt{p})$ and let $K = F(i, \alpha)$, where $\alpha^4 = 2\varepsilon$. We claim that $K/F$ is cyclic of degree 8, 2-ramified, and that $K/Q$ is normal and non-abelian. First, $K/Q$ is normal, for any automorphism of $K$ sends $\alpha$ to a fourth root of $2\varepsilon$ or $2\varepsilon'$ where $\varepsilon'$ is the conjugate of $\varepsilon$. But $N_{Q(\sqrt{p})/Q}(\varepsilon) = -1$ since $p \equiv 1(4)$, and so

$$(2\varepsilon')(2\varepsilon) = -4 = (1 - i)^4.$$ 

Thus $(1 - i)/\alpha$ is a fourth root of $2\varepsilon'$ in $K$. Next, $\text{Gal}(K/F)$ is cyclic of degree 8, for if $\sigma \in \text{Gal}(K/F)$ is non-trivial on $F(i)$ then $\sigma \varepsilon = \varepsilon'$ so $\sigma \alpha = i^j(1 - i)/\alpha$ for some $j$. Applying $\sigma$ again we see that $\sigma^2 \alpha = i(1 - 1)^j\alpha$, so $\sigma^2$ has order 4 in $\text{Gal}(K/F)$, and hence, $\sigma$ generates $\text{Gal}(K/F)$. It is obvious that $K/F$ is 2-ramified and $K/Q$ is not abelian since $\mathbb{Q}(\sqrt{2\varepsilon})/\mathbb{Q}$ is not normal. By Theorem 12, the quartic subextension, $E$, of $K/F$ lies in $K_2$. Also by applying Lemma 4 the only cyclic 2-ramified degree 8 extensions of $F$ containing $E$ which are normal over $\mathbb{Q}$ are $K$ and $F(i, \beta)$ where $\beta^4 = -2\varepsilon$. Since $-4 = N_{Q(\sqrt{p})/Q}(2\varepsilon) \equiv (2\varepsilon)^2 \pmod{q}$, where $q$ divides $p$ in $Q(\sqrt{p})$, it follows that $2\varepsilon$ is a square in $Q_p(\sqrt{p}) = Q_p(\sqrt{-p})$. [7] Initial layers of $Z_r$-extensions 163
Since \(-1\) is a square but not a fourth power in \(\mathbb{Q}_p(\sqrt{p})\), exactly one of \(2^e\), \(-2^e\) is a fourth power in \(\mathbb{Q}_p(\sqrt{p})\), and so \(p\) splits completely in exactly one of \(K = F(i, \alpha)\) and \(F(i, \beta)\), where \(p\) is the prime of \(F\) dividing \(p\). By Theorem 11, this field is the 8th degree subfield of \(K_2\).

**Remark**: Since \(F(i)\) is the 2-Hilbert class field of \(F\), \(F(i)\) has odd class number and no unramified abelian 2-extension. As \(F(i)\) has a single prime containing 2, it follows, [7], that all subfields of \(K_2\) have odd class number, and hence, the Iwasawa invariants of \(K_2/F\) are trivial.

**Example 2**

Let \(l = 2\). We assume that \(d\) has at least one odd prime divisor \(\neq \pm 1(8)\). This will insure that all 2-ramified quadratic extension of \(F\) are of the form \(F(\sqrt{m})\) or \(F(\sqrt{2m})\) where \(md\) (\(m\) may be negative) [2, § 3]. In this case we claim that if \(2T = 0\), then there will be a unique 2-ramified quadratic extension of \(F\) in which all the odd prime divisors of \(d\) split completely. Theorem 11 then tells us that this must be the quadratic subextension of \(K_2\). We require a lemma.

**Lemma (13)**: Let \(\delta = 0\) or 1 and let \(m|d, m > 0\). Suppose for every odd \(p|d\), the prime \(\mathfrak{p}|p\) in \(F\) splits in \(k = F(\sqrt{-2^\delta m})\). Then \(k\) has a quadratic 2-ramified extension \(K\) such that \(K/Q\) is normal and \(K/F\) is cyclic (in fact \(K/Q\) is dihedral).

**Proof**: Let \(F_1 = \mathbb{Q}(\sqrt{-2^\delta m})\), \(F_2 = \mathbb{Q}(\sqrt{2^\delta d/m})\). The hypotheses of this lemma imply that all odd \(p\) dividing \(m\) split from \(\mathbb{Q}\) to \(F_2\) and all odd \(p\) dividing \(d/m\) split from \(\mathbb{Q}\) to \(F_1\). We may suppose that if \(2\) divides \(2^\delta d/m\), then 2 does not remain prime in \(F_1\). If it did, then we would have \(\delta = 0\), \(-m \equiv 5(8)\), and \(2|d\). But by the splitting of \(p|d\), we see that \((-m/p) = 1\) for \(p|(d/m)\) and \((d/m)/p) = 1\) for \(p|d/m\), so \((-m, d/m) = 1\) for all odd \(p\) where \((,)\) denotes the rational Hilbert 2-symbol at \(p\). By reciprocity, \(1 = (-m, d/m) = (-m, 2)_2\), and we have a contradiction. Now, for each \(p|2^\delta d/m\) choose a prime \(\mathfrak{p}|p\) in \(F_1\) and let \(\mathfrak{F} = \prod_{\mathfrak{p}|2^\delta d/m}\mathfrak{p}\). Then, since all \(p(2^\delta d/m)\) split or ramify in \(F_1\), we have \(N_{F_1/Q}(\mathfrak{F}) = 2^\delta d/m\). There is an isomorphism

\[
C/C^2 \cong \prod_{\mathfrak{p}|2^\delta} \{\pm 1\} \quad \mathfrak{F} \rightarrow \ldots (N_{E/Q}\mathfrak{B}, \mathcal{D}_p, \ldots)
\]

where \(C\) is the class group of a complex quadratic field, \(E\), of discriminant \(\mathcal{D}\), and \(\prod\{\pm 1\}\) is a subgroup of \(\prod\{\pm 1\}\), [5, § 26, 29]. Using this isomorphism on \(E = \mathbb{Q}(\sqrt{-2^\delta m})\) we see that \(\mathfrak{F}\) is a square in the class group.
of $E$. Hence, there is an element, $\beta$, of $E$ such that $(\beta) = \mathcal{A}\mathcal{B}^2$ for some ideal $\mathcal{B}$. Let $K = k(\sqrt{\beta})$; clearly $K/F$ is 2-ramified. Let $N_{E/Q}\mathcal{B} = b$. Since $\sqrt{\beta}/\sqrt{\beta'} = \sqrt{N_{E/Q}\beta}$ where $\beta'$ is the conjugate of $\beta$, $K$ is normal if it contains $\sqrt{N_{E/Q}\beta} = b\sqrt{2^d/d/m}$, which it does. Let $\sigma \in \text{Gal}(K/F)$ which is not trivial on $k$.

$$\sigma(\sqrt{\beta})\sigma(\sqrt{\beta'}) = \sigma(b\sqrt{2^d/d/m}) = -b\sqrt{2^d/d/m} = -\sqrt{\beta}\sqrt{\beta'} \quad \text{and} \quad \sigma\beta = \bar{\beta}.$$ 

Thus $\sigma^2(\sqrt{\beta}) = \pm\sigma(\sqrt{\beta}) = -\sqrt{\beta}$ and $\sigma$ has order 4 implying that $K/F$ is cyclic. Also since $Q(\sqrt{\beta})/Q$ is not normal, $K/Q$ is not abelian and so is dihedral.

To use this lemma we note that the hypothesis that some odd prime divisor of $d$ is not congruent to $\pm 1(8)$ implies that it does not split in $F(\sqrt{2})$, the quadratic subfield of $K_1$, and hence, does not split in the third quadratic subfield of $L$. If all the odd prime divisors of $d$ split in two 2-ramified quadratic extensions of $F$, then one of these extensions would be disjoint from $L$. But by the lemma we would have a degree 4 cyclic 2-ramified extension, $F'$ of $F$ disjoint from $L$. Hence $\text{Gal}(F'L/L) \approx \mathbb{Z}/4\mathbb{Z}$ would be a quotient of $T$, contradicting the fact that $2T = 0$.

**Example 3** (c.f. [1, § III])

Let $l = 3$ and suppose $F$ has class number prime to 3. From the sequence of Theorem 5 we see that $T \cong \mathbb{Z}/3\mathbb{Z}$ if $d \equiv 3(9)$, $d \neq 3$, and $T = 0$ otherwise as $F_\varphi, \varphi \in S$, contains cube roots of 1 only when $d \equiv 3(9)$. We divide into cases:

**Case (i):** $d \not\equiv 3(9)$: Since $T = 0$, Theorem 12 tells us that any cubic 3-ramified extension of $F$ normal and non-abelian over $Q$ must lie in $K_2$. Let $k = F(\rho)$ where $\rho$ is a primitive cube root of 1, and let $\varepsilon$ be a fundamental unit of $Q(\sqrt{3d})$. First we claim that $k(\rho)/k$ where $\alpha^3 = \varepsilon$ is 3-ramified, $k(\rho)/Q$ is normal, and $k(\rho)/F$ is abelian. It is obvious that $k(\rho)/k$ is 3-ramified. If $\sigma$ is an automorphism of $k(\rho)$ then

$$(\alpha\sigma(\alpha))^3 = \varepsilon\sigma(\varepsilon) = \pm 1$$

or $\varepsilon^2$ so $\alpha\sigma(\alpha) = \pm \rho^i$ or $\pm \rho^i\alpha^2$ and $\sigma(\alpha) \in k(\alpha)$. Hence $k(\alpha)/Q$ is normal. Let $\sigma$ be a lifting of order 2 of the generator of $\text{Gal}(k/F)$ to $k(\alpha)$ and let $\lambda \in \text{Gal}(k(\alpha)/k)$, $\lambda(\alpha) = \rho\alpha$. As above, $\alpha\sigma(\alpha) = \pm \rho^i$, but

$$\alpha\sigma(\alpha) = \sigma(\alpha\sigma(\alpha)) = \pm \rho^{-i},$$
so $i = 0$. From this, it follows that $\sigma \lambda = \lambda \sigma$. Thus $\text{Gal}(k(\alpha)/F)$ is cyclic, and so $\langle \sigma \rangle$ is a characteristic subgroup. Hence its fixed field, $E$, is normal over $Q$. Also $E/Q$ is not abelian, or $k(\alpha)/Q$ would be, so $\text{Gal}(E/Q) \cong S_3$. Finally, we claim that $E = F(\alpha + \sigma(\alpha))$. Clearly, $F(\alpha + \sigma(\alpha)) \subseteq E$ but $\alpha$ satisfies the polynomial $x^2 - (\alpha + \sigma(\alpha))x + 1$ so $[k(\alpha) : F(\alpha + \sigma(\alpha))] \leq 2$.

**Case (ii): $d \equiv 3(\text{mod } 9)$:** We know by earlier remarks in Case (i) and by Lemma 4 that there are two disjoint 3-ramified cubic extensions of $F$ which are dihedral over $Q$. Exactly one of the four cyclic subfields of their composite over $F$ lies in $K_2$. The computation in Case (i) is valid for $d \equiv 3(\text{mod } 9)$ so that $F(\alpha + \sigma(\alpha))/F$ is such an extension, where $\alpha^3 = \varepsilon$ is the fundamental unit in $Q(\sqrt[3]{d})$, and $\sigma$ is a lifting of order 2 of the non-trivial automorphism in $\text{Gal}(F(\sqrt[3]{-3})/F)$. Since $d \equiv 3(\text{mod } 9)$, the principal ideal $(3) = \mathfrak{q}\mathfrak{q}'$ is a product of distinct primes in $Q(\sqrt[3]{3d})$. Let $(\beta) = \mathfrak{q}^m$, where $m$ is the order of $\mathfrak{q}$ in the class group of $Q(\sqrt[3]{3d})$. Since the class number of $F$ is prime to 3, a theorem of Scholz, [10], implies that the class number of $Q(\sqrt[3]{3d})$ is not divisible by 3, and hence $3 \not| m$. Let $\gamma^3 = 3^i\beta$, where $i = 1$ or 2 and $i \equiv m(\text{mod } 3)$. A proof entirely analogous to Case (i) shows that $F(\gamma + \sigma(\gamma))/F$ is a 3-ramified cubic extension of $F$ which has $S_3$ as Galois group over $Q$. We must next determine which field lies in $K_2$ (it is clear that $F(\alpha + \sigma(\alpha)) \neq F(\gamma + \sigma(\gamma))$ as $(\gamma \alpha)^3$ and $(\gamma \alpha^2)^3$ are non-cubes in $k = F(\sqrt[3]{-3})$). For this we must consider the extensions of $k = F(\sqrt[3]{-3})$.

**PROPOSITION (14):** Let $F_1 = Q(\sqrt{d_1})$, $F_2 = Q(\sqrt{d_2})$, $F_3 = Q(\sqrt{d_1 d_2})$, and $k = F_1 F_2$. Suppose $l$ is an odd prime, and let $M_i$ (respectively $M$) be the maximal abelian $l$-ramified $l$-extension of $F_i$ (respectively $k$). If $T_i$ (respectively $T$) is the $l$-torsion subgroup of $\text{Gal}(M_i/F_i)$ (respectively $\text{Gal}(M/k)$), then $T \cong T_1 \oplus T_2 \oplus T_3$ and $M = kM_1 M_2 M_3$.

**PROOF:** Let $\sigma$ generate $\text{Gal}(k/F_1)$ and $\tau$ generate $\text{Gal}(k/F_2)$ and extend these to $\sigma, \tau \in \text{Gal}(M/Q)$, automorphisms of order 2. If $G = \text{Gal}(M/k)$, we can decompose $G$ as a $\langle \sigma, \tau \rangle$ module, so that $G = G_{++} \oplus G_{+-} \oplus G_{-+} G_{--}$, where e.g. $G_{++}$ is the subgroup of $G$ fixed by $\sigma$ and inverted by $\tau$ (i.e. $G_{++} = (1 + \sigma)(1 - \tau)G$). The fixed field $E_1$ of $G_{++} \oplus G_{--} = (1 - \sigma)G$ is a normal extension of $Q$, and is the maximal subextension of $M$ which is abelian over $F_1$. Hence the subfield of $E_1$ fixed by $\sigma$ is contained in $M_1$ and so equal to $M_1$. We proceed similarly for $M_2$ and $M_3$, and since

$$(G_{+-} \oplus G_{--}) \cap (G_{++} \oplus G_{--}) \cap (G_{++} \oplus G_{-+}) = 0,$$
we see that $M = kM_1M_2M_3$. Also the field fixed by $\langle \sigma, \tau \rangle$ and $G_+ + G_- + G_- + G_- = \text{an } \ell\text{-ramified abelian }\ell\text{-extension of }\mathbb{Q}$, and so must be the cyclotomic $\mathbb{Z}_\ell$-extension of $\mathbb{Q}$. Thus $G_+ +$ is torsion free, and since $T_1$ is the torsion subgroup of $G_+ + G_-$, etc., we deduce that $T \approx T_1 \oplus T_2 \oplus T_3$.

We apply this proposition for $F_1 = F = \mathbb{Q}(\sqrt{-d})$, $d \equiv 3 \pmod{9}$, and $F_2 = \mathbb{Q}(\sqrt{3d})$. As we remarked in the beginning of this example, $T$ has order 3. By the same method one sees that $T_3 = 0$, and $T_2$ is the 3-torsion subgroup $(U_3 \times U_3)/\langle \pm 1, \varepsilon \rangle$, where $U_3$ is the group of units in $\mathbb{Q}_3$.

In order that $T_2 \neq 0$, we must have $\varepsilon$ a cube in $\mathbb{Q}_3$. However if $\varepsilon \in \mathbb{Q}_3^3$, then $k(\varepsilon)/k$ would be unramified, and 3 would divide the class number of $k$. It is well-known that the 3-primary subgroup of the class group of $k$ is isomorphic to the product of the 3-primary subgroups of the class groups of $F$ and $F_2$, both of which are trivial. Thus $T \approx T_1$ has order 3. Furthermore, as in Theorem 6, $T$ is isomorphic to the 3-torsion subgroup of $J_k/k^*$.

We choose as representative, the idèle $x = (\rho, 1, \ldots)$ of $J_k$ with a cube root of 1, $\rho$, in the $q_0$ place, and 1 elsewhere, where $q_0$ is a prime of $k$ dividing $q'$ in $\mathbb{Q}(\sqrt{3d})$. We now use a Kummer pairing to find the subfield of $k(\alpha, \gamma)$ which lies in a $\mathbb{Z}_3$-extension of $k$, namely $k(\varepsilon^3\beta^t)$. $s$, $t = 0, 1, 2$, lies in a $\mathbb{Z}_3$-extension of $k$ if and only if the Hilbert 3-symbol $(\varepsilon^3\beta^t)$ is trivial for all $\varepsilon^3\beta^t$.

Now $\varepsilon \equiv \pm 1 \pmod{q'}$, but $\varepsilon \neq \pm 1 \pmod{q_2}$ since otherwise $\varepsilon^2 \in k_3^*$ and as mentioned above $k(\varepsilon)/k$ would be unramified. Thus $\varepsilon \equiv \pm 2$ or 4 (mod $q_2$) and since units congruent to 1 mod $q_2$ are cubes in $k_{q_0}$, $(\rho, \varepsilon)_{q_0} = (\rho, -2)^{\pm 1}_{q_0}$. We compute this symbol using reciprocity in the field $\mathbb{Q}(\rho)$, noting that $k_{q_0} = \mathbb{Q}_3(\rho)$. We have $\prod_{q_0} (\rho, -2)_{q_0} = 1$ where $q$ runs over all primes of $\mathbb{Q}(\rho)$. Since all the symbols are tame except for $q_3$ where $q_3^3$ all but $(\rho, -2)_{q_3}$ and $(\rho, -2)_{q_2}$ are trivial where $q_2$. Since $(\rho, -2)_{q_2} = \rho$, it follows that $(\rho, -2)_{q_0} = (\rho, -2)_{q_0} = \rho^2 \neq 1$. Hence $k(\alpha)$ is not contained in a $\mathbb{Z}_3$-extension of $k$. Reciprocity also shows that $(\rho, 3)_{q_3} = 1$ so that $(\rho, 3^3\beta)_{q_0} = (\rho, \beta)_{q_0} = 1$ if and only if $\beta = \pm 1$ (mod $q_2$). We can alter $\beta$ by powers of $\varepsilon$ to achieve this. Thus $k(\gamma)$ lies in a $\mathbb{Z}_3$-extension of $k$. Since $\sigma$ acts trivially on $\text{Gal}(k(\gamma)/k)$, $k(\gamma) \subset kM$, by the proof of Proposition 14. Hence $F(\gamma + \sigma(\gamma)) \subset k(\gamma) \subset L$, so $F(\gamma + \sigma(\gamma)) \subset L$. But $F(\gamma + \sigma(\gamma))/\mathbb{Q}$ is normal dihedral, so $F(\gamma + \sigma(\gamma)) \subset K_2$.

e.g. if $F_1 = \mathbb{Q}(\sqrt{-21})$, then $F_2 = \mathbb{Q}(\sqrt{7})$, and $\varepsilon = 8 + 3\sqrt{7}$. Take $q = (2 + \sqrt{7})$, so $\sqrt{7} \equiv 5 \pmod{q_2}$ and $-\varepsilon(2 + \sqrt{7}) \equiv 1 \pmod{q_2}$. Thus if $\gamma^3 = -3\varepsilon(2 + \sqrt{7})$ then $F_1(\gamma + \sigma(\gamma))$ begins the normal, non-abelian $\mathbb{Z}_3$-extension of $F$. 
REFERENCES


Pasadena, California 91125