RELATIVE EXTENSIONS OF ABELIAN NUMBER FIELDS
WITH PRIME POWER DEGREE

Zhang XianKe
Department of Mathematics, Tsinghua University,
Beijing 100084, People’s Republic of China
and
International Centre for Theoretical Physics, Trieste, Italy.

ABSTRACT

Suppose that \( L \supseteq K \) are abelian number fields whose degrees are powers of a prime number \( q \). (1) The extension \( L/K \) is proved to have a relative integral basis under certain simple conditions. In particular, it has a relative integral basis if \( [L : K] \geq x^* \) (when \( q \neq 2 \)) or \( \geq x^* + 1 \) (when \( q = 2 \)) (where \( x^* \) is the exponent of \( \text{Gal}(L) \)). (2) Discriminant \( D(L/K) \) is given here explicitly, and necessary and sufficient conditions are obtained for \( D(L/K) \) to be generated by a rational square. In particular, \( D(L/K) \) is generated by a rational square if \( [L : K] \geq x^* \) or \( x^* + 1 \) (when \( q \) is odd or 2). The above results contain many results for more special fields \( L \) and \( K \) in literature.

1991 Mathematics Subject Classification: 11R20, 11R29, 11C30, 11R04

Keywords: number field, abelian field, relative integral basis, relative extension

MIRAMARE – TRIESTE
September 1997

\(^1\)Regular Associate of the ICTP.
We use the symbols and results of [1]. For any prime number $q$, let $L$ be an abelian extension over the rationals $\mathbb{Q}$ with degree $q^S$. Such a field $L$ is also said to be an (abelian) $q$-field. Then naturally $L$ is a compositum

$$L = K_1K_2\cdots K_n$$

(1)

where $K_i$ is a cyclic field with degree $q^{s_i}$ ($1 \leq i \leq n$). Let

$$s^* = \max_{1 \leq i \leq n} \{ s_i \}$$

(2)
then $x^* = q^{s^*}$ is the exponent of (the Galois group $\text{Gal}(L/\mathbb{Q})$ of ) $L$. Denote by $E(p, F)$, $e(p, F)$ ($= q^{s^*}$), and $f(p, F)$ the inertia group, ramification index, and residue class degree respectively for a prime number $p$ in $F$ (i.e. those for the prime ideal factors of $p$ in $F$ over $p$), and define $e = e_L$ by

$$q^e = \max_{1 \leq i \leq n} e(p, K_i).$$

(3)

Let $\hat{L}$ denote the character group of $L$, let $\text{con}(\chi)$ denote the conductor of $\chi \in \hat{L}$. Then we know by [1] that the (absolute) discriminant of $L$ is

$$D(L) = c \prod_p p^{v_p},$$

(4)

where $c = \pm 1$, and $c = -1$ if and only if $L$ is an imaginary quadratic field, and

$$v_p = q^S - q^{s^*-e},$$
when $p \neq q$;

$$v_q = (e + 1)q^S - q^{s^*-e}(1 + \frac{q^e - 1}{q - 1}),$$
when $p = q \neq 2$;

and

$$v_2 = v_{21} = (e + 1)2^S - 2^{s^*-e},$$
when $p = q = 2$ and $\text{con}(\chi) \not\equiv 4(\text{mod } 8)$ for all $\chi \in \hat{L}$, otherwise

$$v_{22} = (e + 1)2^S$$
or

$$v_{23} = 2^S$$
according to $\text{con}(\chi) \equiv 0(\text{mod } 8)$ for some $\chi \in \hat{L}$ or not.

Let $K$ be any subfield of a $q$-field $L$. Assume a prime number $p$ has the following decomposition in the field $K$:

$$(p) = pO_K = (\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g)^{e(p, K)}$$

(6)
where $\mathfrak{p}_i$ are distinct prime ideals of $K$ ($1 \leq i \leq g$). Denote

$$(p)^{e(p, K) - 1} = \mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_g$$

(7)
In fact we will use the classical scheme for the identification of ideals in different fields, i.e., if $I_1$ and $I_2$ are ideals of fields $F_1$ and $F_2$ and $K_1O_{F_1F_2} = I_2O_{F_1F_2}$ then one says $I_1 = I_2$. 

2
Theorem 1. Suppose that $L \supset K$ are abelian $q$-fields and $[L : K] = q^N$, then the relative discriminant of $L$ over $K$ is

$$D(L/K) = \prod_p (p)^{u_p},$$

where

$$u_p = q^{N-e'} - q^{N-e}, \quad u_q = (e-e')q^N + q^{N-e}(q^{e-e'} - 1)(q-2)/(q-1), \quad u_2 = \begin{cases} (e-e')2^N + 2N-e(2e-e' - 1), & \text{if } L/K \in C_2(1,1); \\ (e-e')2^N, & \text{if } L/K \in C_2(2,2); \\ 2^N, & \text{if } L/K \in C_2(3,1); \end{cases}$$

here $e'$ is defined to $K$ just as $e$ to $L$; and $L/K \in C_2(i,j)$ means $p = q = 2$ and $v_2(D(L)) = v_2i, v_2(D(K)) = v_2j$.

Proof. For any automorphism $\rho \in \text{Gal}(L/Q)$ (the Galois group of $L$ over $Q$), we have

$$\rho D(L/K) = D(\rho L/\rho K) = D(L/K).$$

So if $\varphi_1^a \| D(L/K)$ for any prime factor $\varphi_1$ of $D(L/K)$, then we have

$$(\varphi_1 \cdots \varphi_g)^a \| D(L/K)$$

(see equation (6)). Let

$$e(p, K)f(p, K)g(p, K) = [K : Q].$$

Then we have

$$D(L/K) = \prod_p (\prod_{\varphi \mid p} \varphi)^a(p) = \prod_p (p)^{a(p)/e(p, K)},$$

$$N_{K/Q}D(L/K) = \prod_p (p)^{a(p)f(p, K)g(p, K)},$$

$$N_{K/Q}D(L/K) = D(L)/D(K)^{[L : K]} = \prod_p (p)^{v_p - v'_p[L : K]},$$

where $v'_p = v_p(D(K))$ is defined to $K$ just as $v_p$ to $L$ in Theorem 1 of [1]. Thus

$$u_p = a(p)/e(p, K) = a(p)f(p, K)g(p, K)/(e(p, K)f(p, K)g(p, K))$$

$$= (v_p - v'_p[L : K])/[K : Q].$$

Then we calculate $u_p$ in different cases using Theorem 1 of [1], and obtain the theorem.

Theorem 2. Suppose that $L \supset K$ are abelian $q$-fields. Then $D(L/K)$ is a principal ideal generated by a rational number (denoted by $D(L/K) \in Q$) if and only if

$$[L : K] \begin{cases} \geq c(p, L), & \text{when } p \neq q, \text{ or } p = q \neq 2, \text{ or } L/K \in C_2(1, 1); \\ \geq c(p, K), & \text{when } L/K \in C_2(2, 1) \end{cases}$$
for prime numbers \( p \) with \( e(p, L) \neq e(p, K) \). In particular, if \([L : K] \geq q^*\), then \( D(L/K) \in \mathbb{Q} \).

**Proof.** Note that \( D(L/K) \in \mathbb{Q} \) if and only if \( u_p \) (in Theorem 1) are (positive) integers for primes \( p \mid D(L/K) \) (i.e. \( e(p, L) \neq e(p, K) \)). So considering and calculating case by case via Theorem 1, we obtain Theorem 2.

**Example 1.** Suppose that \( L \) and its subfield \( K \) both are of type \((q^*, \cdots, q^*)\), then Theorem 1 asserts that \( D(L/K) \in \mathbb{Q} \).

**Example 2.** Suppose that the field \( L \) is cyclic (and \( K \neq \mathbb{Q} \)), then theorem 2 asserts \( D(L/K) \not\in \mathbb{Q} \). In fact, there is always a prime \( p \) with \( e(p, L) = [L : \mathbb{Q}] \) and \( L/K \not\in C_2(2, 1) \) \((v_2(D(L)) \neq v_{22})\). For example, let \( L \) be a cyclic quartic field, then \( L \) has a unique quadratic subfield \( K = \mathbb{Q}(\sqrt{u}) \), and we have \( D(L/K) = (2^t \sqrt{u}) \) by [8].

**Theorem 3** Suppose that \( L \supseteq K \) are abelian \( q \)-fields. Then \( D(L/K) \) is a principal ideal generated by a square of a rational number (denoted by \( D(L/K) \in \mathbb{Q}^{q^*} \)) if and only if

\[
[L : K] >\begin{cases} 
\geq e(p, L), & \text{when } q \neq 2; \\
> e(p, L), & \text{when } q = 2 \neq p, \text{ or } L/K \in C_2(1, 1); \\
> e(p, K), & \text{when } L/K \in C_2(2, 1) 
\end{cases}
\]

for prime numbers \( p \) with \( e(p, L) \neq e(p, K) \). In particular, if \([L : K] \geq q^*\) or \(2^{q^*} + 1\) (according to \( q \) odd or even), then \( D(L/K) \in \mathbb{Q}^{q^*} \).

**Proof.** Suppose that we have \( D(L/K) \in \mathbb{Q} \). Then \( D(L/K) \in \mathbb{Q}^{q^*} \) if and only if \( u_p \equiv 0 \pmod{2} \) for primes \( p \mid D(L/K) \). So a careful examination of \( u_p \) via Theorem 1 and Theorem 2 gives Theorem 3.

If the integer ring \( O_L \) of \( L \) is a free \( O_K \)-module of rank \( r = [L : K] \), then \( L/K \) is said to have a relative integral basis. In this case we have

\[
O_L = O_K w_1 \bigoplus \cdots \bigoplus O_K w_r
\]

for certain \( w_1, \cdots, w_r \in O_L \), and then the set \( \{w_1, \cdots, w_r\} \) is said to be a relative integral basis of \( L/K \). There are many literatures studying the existence of relative integral bases for fields of types \((2, 2)\) and \((4)\) (see [3-6]). We completely solved the problem for fields of type \((q, \cdots, q)\) and cyclic quartic fields in [2, 7-9]. Fields of type \((q^*, \cdots, q^*)\) are also studied in [10].

**Theorem 4** Suppose that \( L \supseteq K \) are abelian \( q \)-fields and \( q \neq 2 \). Then \( L/K \) has a relative integral basis if \([L : K] \geq e(p, L)\) for prime numbers \( p \) with \( e(p, L) \neq e(p, K) \). In particular, if \([L : K] \geq q^*\), then \( L/K \) has a relative integral basis.

**Theorem 5** Suppose that \( L \supseteq K \) are abelian \( 2 \)-fields. Then \( L/K \) has a relative integral basis if \( L/K \) is not cyclic and

\[
[L : K] >\begin{cases} 
eq e(p, L), & \text{when } p \neq 2, \text{ or } L/K \in C_2(1, 1); \\
eq e(p, K), & \text{when } L/K \in C_2(2, 1) 
\end{cases}
\]
for prime numbers \( p \) with \( e(p, L) \neq e(p, K) \). In particular, if \( [L : K] > 2^s \) then \( L/K \) has a relative integral basis.

For the proof of Theorems 4 and 5, note that \( O_K \) is a Dedekind domain, so
\[
O_L \cong O_K^{[L : K] - 1} \bigoplus J
\]
by E. Steinitz and I. Kaplansky, where \( J \) is an ideal of \( K \), unique up to a principal ideal. Let \( \Delta = \Delta(L/K) \subseteq K^*/K^{*2} \) be the discriminant of any \( K \)-basis of \( L \) defined up to a square in \( K \), let \( D = D(L/K) \). Then \( D/\Delta \) is a square of an ideal of \( K \).

**Theorem A** (Artin [11]). The ideals \( (D/\Delta)^{1/2} \) and \( J \) are in the same ideal class of \( K \). Therefore, \( L/K \) has a relative integral basis if and only if \( (D/\Delta)^{1/2} \) is a principal ideal of \( K \).

To prove Theorem 4, we assume that \( L/K \) is a simple extension, say \( L = K(\theta) \); then \( \text{Gal}(L/K) \) acts on the conjugates of \( \theta \) as a permutation group. And \( \text{Gal}(L/K) \) consists of only even permutations since its order is odd; thus \( \Delta(L/K) \in K^{*2} \). So by the above theorem, \( L/K \) has a relative integral basis.

To prove Theorem 5, note that \( L/K \) is not cyclic, so we may assume \( L = L_1L_2 \), where \( L_i/K \) are abelian extensions of degree \( 2^r_i \geq 2(i = 1, 2) \) and \( [L : K] = 2^{r_1 + r_2} \). Let \( \{x_i\} \) and \( \{y_i\} \) be \( K \)-bases of \( L_1 \) and \( L_2 \) respectively, then \( \{x_iy_i\} \) is a \( K \)-basis of \( L \) and
\[
\Delta_{L/K}(\{x_iy_i\}) = \pm \Delta_{L_1/K}([L : L_1]N_{L_1/K}(\Delta_{L_1}(\{y_j\}))
\]
\[
= \pm \Delta_{L_1/K}(\{x_i\})^{2^r_i} \Delta_{L_2/K}(\{y_j\})^{2^r_2} \in \pm K^{*2}
\]
where \( \Delta_{E/F}(\{z_i\}) \) denotes the discriminant of \( \{z_i\} \) as an \( F \)-basis of \( E \). So by Theorem 3 we know that
\[
D/\Delta = D/\Delta_{L/K}(\{x_1y_1\})
\]
is a square of a principal ideal of \( K \). Via Artin’s theorem, this proves Theorems 4 and 5.

**Example 3.** Suppose that \( L \supseteq K \) are fields of type \((q^n, \cdots, q^n)\) with degree \( q^{mn} \) and \( q^{mm} \) respectively, and assume \( n - m \geq 2 \) when \( q = 2 \). Then the above theorems assert that \( D(L/K) \in \mathbb{Q}^{*2} \) and \( L/K \) has a relative integral basis.

The above results include and develop systematically various results for fields of types \((2, \cdots, 2)\), \((q, \cdots, q)\), and \((q^n, \cdots, q^n)\) in literature on relative integral basis obtained via particular methods (see, e.g. [5-10] and references therein).

**Acknowledgement**

The author thanks the International Centre for Theoretical Physics for hospitality and Prof. M.S. Narasimhan for discussions during the preparation of this paper. Project supported by the National Natural Science Foundation of China.
REFERENCE


