IC/92/394

INTERNATIONAL CENTRE FOR
THEORETICAL PHYSICS

SOME RELATIVE EXTENSIONS AND THEIR INTEGRAL BASES

Zhang Xianke

and

Xu Fuhua

INTERNATIONAL
ATOMIC ENERGY
AGENCY

UNITED NATIONS
EDUCATIONAL,
SCIENTIFIC
AND CULTURAL
ORGANIZATION

MIRAMARE-TRIESTE

IC/92/394

International Atomic Energy Agency
and
United Nations Educational Scientific and Cultural Organization
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS

SOME RELATIVE EXTENSIONS AND THEIR INTEGRAL BASES

ZHANG Xianke *
International Centre for Theoretical Physics, Trieste, Italy

and

XU Fuhua
Department of Mathematics, University of Science and Technology of China,
Hefei, Anhui, People's Republic of China.

ABSTRACT

It is proved that an algebraic number field of type $(q^s, q^s, \ldots, q^s)$ has relative integral basis over any of its subfield under certain conditions. The conductor and discriminant are also determined using the construction of genus fields of abelian number fields.

MIRAMARE – TRIESTE
November 1992

* Permanent address: Department of Mathematics, University of Science and Technology of China, Hefei, Anhui, People's Republic of China.

1. INTRODUCTION AND MAIN RESULTS

A simple construction for genus fields K_G of abelian number fields K was given in [1]. We will give here a further description of K_G, and then determine the conductor $f(K)$ and discriminant $D(K)$ of K. And finally we use these results to prove that an extension L/K of type $(q^s, q^s, \ldots, q^s)$ has a relative integral basis.

Let L be an algebraic number field, K a subfield of L. The ring O_K of integers of K is a Dedekind domain, and O_L is a torsion-free O_K-module. So the construction theorem for modules over Dedekind domain of E. Steinitz (1912) and I. Kaplansky (1952) implies that $O_L \simeq O_K^{n-1} \oplus J$, where $n = [L : K]$, J is an ideal of K. J is unique upto a principal ideal (i.e. the class of J is uniquely determined). Therefore, the ideal class $[J]$ represented by J totally determines the structure of O_L. In particular, when J is principal (for example, if the class number of K is 1, then J is principal; but in general, J could be non-principal), then O_L is a free O_K-module, and L/K is said to have a relative integral basis. In this case, there are integers $w_1, w_2, \ldots, w_n$ of L, such that $O_L = O_K w_1 \oplus \ldots \oplus O_K w_n$. Suppose that $D = D(L/K)$ is the discriminant of L/K, and $\Delta = \Delta(L/K)$ is the discriminant of any K-basis of L, then D/Δ is a square of some ideal of K. E. Artin proved that 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.

Beginning from examples, many literatures study the existence of relative integral basis for cyclic quartic fields and fields of type (2,2) (e.g. see [2–3]). We solved the problem completely for cyclic quartic fields and fields of type $(q, q, \ldots, q)$ (q is any prime, see [4–6]). We will study here fields of type $(q^s, q^s, \ldots, q^s)$ (i.e., Galois group $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbf{Z}/q^s\mathbf{Z})^n$, a direct product of n cyclic groups of order q^s). The situation is more complex than that for $s = 1$ (especially when $q = 2$), and the proof is different. We will first discuss the genus field K_G of an abelian field K. (By definition, K_G is the maximal abelian subfield of the Hilbert class field of K; K_G is also the maximal abelian field such that finite prime divisors are all unramified in K_G/K). Then by that we determine the conductor $f(K)$ of K ($f(K)$ is the minimal positive integer f such that $K \subset \mathbb{Q}(\zeta_f)$, where ζ_f denote a f-th primitive unity root.) Then we consider the character group $\hat{K}$ (as a subgroup of the character group modulo f), and determine the discriminant $D(K)$ of K. Finally, we find $D(L/K)$ and $\Delta(L/K)$ and discuss relative integral basis of L/K using Artin's theorem.

Lemma 1 [1] Let K be a cyclic number field of degree q^s over rationals $\mathbb{Q}$, q a prime number, s a positive integer. Then the genus field of K is

$$K_G = \prod_p \Omega_p = K \prod_{p \neq q} \Omega_p \ , \tag{1}$$

where p runs over prime numbers ramified in K, the ramification index of p in K is denoted $e(p, K) = e(p) = q^{e_p}$, Ω_p is the unique cyclic subfield of degree $e(p)$ in $Q(\zeta_p)$ when $p \neq q$, while Ω_q is a subfield of degree $e(q)$ in $Q(\zeta_q t)$ for a properly large positive integer t.

□

Lemma 2 The minimal value of t in Lemma 1 can be taken as

$$t = \begin{cases} 0, & \text{if } e_q = 0 \text{ (i.e. } q \text{ is unramified in } K); \\ 2, & \text{if } q = 2, e_2 = 1 \text{ and } \Omega_2 = \mathbb{Q}(\sqrt{-1}\,); \\ e_q + \bar{q}, & \text{otherwise (where } \bar{q} = 1 \text{ or } 2 \text{ according to } \\ & \qquad q \text{ is odd or } q = 2) . \end{cases} \tag{2}$$

Moreover, Ω_q is cyclic when $t \neq 0$.

□

Theorem 1 Let K be a cyclic number field of degree q^s, q any prime, s any positive integer. Then the conductor $f(K)$ of K is

$$f = q^t\, p_1 p_2 \ldots p_r\ , \tag{3}$$

where $p_i \equiv 1 \pmod{q^{e_{p_i}}}$ are distinct prime numbers ($q^{e_{p_i}} = e(p_i)$ is the ramification index of p_i in K) $(1 \le i \le r)$; t is as in Lemma 2, in particular $t \in \{0, 2, 3, \ldots, s + \bar{q}\}$. And if $t \neq s + \bar{q}$, there is a p_i $(1 \le i \le r)$ such that $e_{p_i} = s$. Conversely, for any positive integer f as above, there is a cyclic field of degree q^s having conductor f.

□

If $K = K_1 K_2 \ldots K_n$, then $f(K) = Lcm\{f(K_1), \ldots, f(K_n)\}$. Hence we have

Corollary 1 Let K be a number field of type $(q^{s_1}, q^{s_2}, \ldots, q^{s_n})$ (i.e., $\mathrm{Gal}(K) \simeq \mathbf{Z}/q^{s_1}\mathbf{Z} \times \ldots \times \mathbf{Z}/q^{s_n}\mathbf{Z}$), q any prime number, $s_1, \ldots, s_n$ positive integers. Then the conductor of K is

$$f(K) = q^t\, p_1 p_2 \ldots p_r\ , \tag{4}$$

where $p_i \equiv 1 \pmod q$ are distinct prime numbers, $t \in \{0, 2, 3, \ldots, s + \bar{q}\}, s = \max\limits_i\ s_i$.

□

Corollary 2 Let K be an abelian number field of degree n, $n = q_1^{s_1} q_2^{s_2} \ldots q_n^{s_n}$, q_i are distinct prime numbers, and s_i are positive integers $(1 \le i \le n)$. Then the conductor of K is

$$f(K) = q_1^{t_1} q_2^{t_2} \ldots q_n^{t_n}\ p_1 p_2 \ldots p_r\ , \tag{5}$$

where $p_1, \ldots, p_r$ are pairwisely distinct prime numbers, and for each p_i $(1 \le i \le r)$ there is a q_j $(1 \le j \le n)$ such that $p_i \equiv 1 \pmod{q_j}$; $t_i \in \{0, 2, 3, \ldots, T_i + \bar{q}\}$, and $T_i (\le s_i)$ is the q_i–exponent of $\mathrm{Gal}(K)$ (i.e., $q_i^{T_i}$ is the maximal order of elements in its q_i–sylow subgroup).

□

Theorem 2 Let L be a number field of type $(q^s, q^s, \ldots, q^s)$ with degree q^{sn} over rationals $\mathbb{Q}$, where q is any prime number, and s any positive integer. Then the (absolute)

discriminant of L factorizes as

$$D(L) = c \prod_p p^{v_p}\ , \tag{6}$$

where $c = -1$ or $+1$ according to L being imaginary quadratic field or nct;

$$v_p = q^{sn} - q^{sn-e}, \qquad \text{if} \quad p \neq q;$$

$$v_q = (e+1) q^{sn} - q^{sn-e} \left(1 + \frac{q^e - 1}{q - 1}\right), \quad \text{if} \quad p = q \neq 2;$$

$$v_2 = \begin{cases} v_{21} = (e+1) 2^{sn} - 2^{sn-e}, & \text{if } p = q = 2, f(\chi) \not\equiv 4 (mod\ 8)(\forall \chi \in \hat{L}); \\ v_{22} = (e+1) 2^{sn}, & \text{if } p = q = 2, f(\chi) \equiv 4 (mod\ 8)(\exists x \chi \in \hat{L}), \\ & \quad \text{and } f(\chi) \equiv 0 (mod\ 8)(\exists \chi \in \hat{L}); \\ v_{23} = 2^{sn}, & \text{if } p = q = 2, f(\chi) \equiv 4 (mod\ 8)(\exists \chi \in \hat{L}), \\ & \quad \text{and } f(\chi) \not\equiv 0 (mod\ 8)(\forall \chi \in \hat{L}), \end{cases}$$

where $q^e = \max\limits_{1 \le i \le n} e(p, K_i)$ is the maximum of ramification indexes of p in K_i $(1 \le i \le n)$, $\hat{L}$ is the character group of K, $f(\chi)$ is the conductor of $\chi \in \hat{L}$ (i.e., conductor of the fixing subfield of $\{g \in \mathrm{Gal}(L) | g\chi = 1\}$). Moreover, we have $p \equiv 1 (mod\ q^e)$ if $p \neq q$.

□

Example 1 When L is of type $(2, 2, \ldots, 2)$, we have $s = 1, q = 2, e = 1$. Then $v_{21} = 3 \times 2^{n-1}, v_{22} = 2^{n+1}, v_{23} = 2^n$, coinciding with results of [5] and [7]. In this case, we may assume $L = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, \ldots, \sqrt{m_n})$ as in [7]; then in cases $v_2 = 0, v_{21}, v_{22}$, or v_{23}, we have respectively $(m_1, m_2, \ldots, m_n)\ (mod\ 4) = (1, \ldots, 1), (2, 1, \ldots, 1), (2, 3, 1, \ldots, 1)$, or $(3, 1, \ldots, 1)$.

□

Example 2 When L is of type $(q, q, \ldots, q)$, i.e., $s = 1$ and q is odd prime, then Theorem 2 gives $D(L) = f(L)^{q^n - q^{n-1}}$, coinciding with result in [8].

□

Example 3 When L is a cyclic field of degree q^s, we have $n = 1$ and

$$v_p = q^s - q^{s-e}, \qquad \text{if} \quad p \neq q;$$

$$v_q = (e+1) q^s - q^{s-e} \left(1 + \frac{q^e - 1}{q - 1}\right), \quad \text{if} \quad p = q \neq 2;$$

$$v_2 = \begin{cases} (e+1) 2^s - 2^{s-e}, & \text{if } f(L) \not\equiv 4\ (mod\ 8); \\ 2^s, & \text{if } f(L) \equiv 4\ (mod\ 8)\ . \end{cases}$$

□

Notice that if we denote v_p in Theorem 2 as $v_p(s, e)$, then $v_p(s+1, e) = q\ v_p(s, e)$ in all cases. And the maximal value of e is s, and v_p assumes its maximal value at $e = s$. From this, we can systematically determine the values of $v_p(s, e)$ (and hence $D(L)$) in various cases. For example, if L is a cyclic field of degree 2, 4, 8, or 16, then the possible values of v_2 are respectively 0, 2, 3; 0, 4, 6, 11; 0, 8, 12, 22, 31; 0, 16, 24, 44, 62, 79.

Theorem 3 Suppose that L and its subfield K are number fields of type $(q^s, q^s, \ldots, q^s)$ where q is an odd prime number. Then L/K has a relative integral basis.

Theorem 4 Suppose that L and its subfield K are number fields of type $(2^s, 2^s, \ldots, 2^s)$ with degree 2^{sn} and 2^{sm} respectively. If $n - m > e$ and $n - m > 1$, then L/K has a relative integral basis, where $2^e = \max_i e(2, K_i)$ is the maximum of the ramification indexes $e(2, K_i)$ of 2 in K_i $(1 \le i \le n)$, and $L = K_1 K_2 \ldots K_n$ with K_i cyclic fields of degree 2^s.

□

2. PROOFS OF THEOREMS AND LEMMAS

Proof of Lemma 2 If $q = 2$ and $e_2 \ge 2$, then by Lemma 1 we have

$$K \subset K_G \subset \mathbb{Q}(\zeta_{q^t})\mathbb{Q}(\zeta_{p_1}) \ldots \mathbb{Q}(\zeta_{p_g}) = L . \tag{7}$$

Let $E_K(p)$ denote the ramification group of p in K. Then $E_K(2) \simeq E_{K_G}(2)$ is the image of $E_L(2)$ under the restrict homomorphism. Since K is cyclic, so $E_K(2)$ is cyclic and $E_L(2)$ should have element of order 2^{e_2}. By $E_L(2) \simeq \mathrm{Gal}(Q(\zeta_{q^t}))$, we thus know that the minimal value of t can be assumed as $e_2 + 2$. It also follows from

$$E_K(2) \simeq E_{K_G}(2) \simeq E_{\Omega_2}(2) \times \ldots \times E_{\Omega_g}(2) \simeq E_{\Omega_2}(2) \simeq \mathrm{Gal}(\Omega_2) . \tag{8}$$

The other part of the lemma can be proved similarly.

Proof of Theorem 1 By (7) we know $f(K) \le f$. Since $K \subset \mathbb{Q}(\zeta_{f(K)}) = L$, there is a surjective homomorphism $E_L(p) \to E_K(p)$, so from the proof of Lemma 2 we have $f(K) \ge f$. We have $p_i \equiv 1 \ (mod\, e(p_i))$ since $\mathbb{Q}(\zeta_{p_i})$ has cyclic subfield Ω_{p_i} of degree $e(p_i)$ (see Lemma 1). In addition we note that e_q can be s (for example, consider the case K being cyclic subfield of degree q^s of $\mathbb{Q}(\zeta_{q^{s+2}})$), so by Lemma 2 we have $t \in \{0, 2, \ldots, s + \bar{q}\}$. If $t \ne s + \bar{q}$ (i.e., q is not totally ramified in K), then there is a p_i ramified totally in K (note that if p is a prime ramified in the subfield of degree q of K, then p ramifies totally in K since no subfield of K can be the inertia field of p), thus we have $e_{p_i} = s$.

Conversely, for f as in (5), let g_i be a generator of $(\mathbf{Z}/p_i\mathbf{Z})^\times$ (here denote $p_0 = q^t$ if $t \ne 0$), then the order of

$$g_0^{q^t - \bar{q}/e(q)} \ldots g_r^{(p_r - 1)/e(p_r)}$$

is q^s since one of the numbers $e(q), \ldots, e(p_r)$ is equal to q^s as mentioned above. By the duality of abelian group, $(\mathbf{Z}/f\mathbf{Z})^\times$ has quotient group of order q^s. Hence we know $\mathbb{Q}(\zeta_f)$ has a cyclic subfield K of degree q^s and obviously $f(K) = f$.

Proof of Theorem 2 We may assume

$$L = K_1 K_2 \ldots K_n , \tag{9}$$

where K_i are cyclic fields of degree q^s $(1 \le i \le n)$. Let the conductors of K_i and L be

$$f(K_i) = q^{t_i} \prod_{p | f(K_i)} p, \quad f(L) = q^t \prod_{p | f(L)} p . \tag{10}$$

Let the character group of K_i be $\hat{K}_i = <\chi_i>$ and χ_i factorize as

$$\chi_i = \varphi_{i(q)} \prod_p \varphi_{i(p)} , \tag{11}$$

where $\varphi_{i(p)}$ denote character modulo p, and $\varphi_{i(q)}$ character modulo q^{t_i}. Then the character group of L is

$$\hat{L} = <\chi_1, \ldots, \chi_n> = \{\chi = \chi_1^{k_1} \ldots \chi_n^{k_n} | k_1, \ldots, k_n \in \mathbf{Z}/q^s\mathbf{Z}\} .$$

By Hasse's discriminant–conductor theorem, we have

$$d(L) = \prod_{\chi \in \hat{L}} f(\chi) , \tag{12}$$

where $f(\chi) = q^{t_\chi} \prod_p p$ is the conductor of χ, i.e., the conductor of L_χ, the fixed field of $\{g \in \mathrm{Gal}(L) | \chi(g) = 1\}$. Note that the ramification group of p in K_i is $E(p, K_i) \simeq <\varphi_{i(p)}>$, and the ramification index is $e(p, K_i) = \# <\varphi_{i(p)}>$. Put

$$e(p) = q^{e_p} = q^e = \max_i e(p, K_i) , \tag{13}$$

and assume $e(p, K_1) = e(p)$, then the order of $\varphi_p = \varphi_{1(p)}$ is $e(p) = q^{e_p} = q^e$. Thus the p-part of $\chi = \chi_1^{k_1} \ldots \chi_n^{k_n}$ is

$$\chi_{(p)} = \varphi_{1(p)}{}^{k_1} \ldots \varphi_{n(p)}{}^{k_n} . \tag{14}$$

(i) First, we assume $p \ne q$. Let $\varphi_{i(p)} = \varphi_p{}^{b_i}$. Then

$$\chi_{(p)} = \varphi_p^{b_1 k_1 + \ldots + b_n k_n} = \varphi_p^b . \tag{15}$$

Note that there are q^{s-e} distinct numbers $b (mod\ q^s)$ satisfying $b \equiv 0\ (mod\ q^e)$. For each such b, the equation $b_1 k_1 + \ldots + b_n k_n \equiv b\ (mod\ q^s)$ has $q^{s(n-1)}$ solutions $(k_1, \ldots, k_n)\ (mod\ q^s)$. Thus there are $q^{sn} - q^{s-e} \cdot q^{s(n-1)} = q^{sn} - q^{sn-e}$ characters $x \in \hat{L}$ with non-trivial p-part, and $p \| f(\chi)$ for each of these χ. Hence

$$v_p = q^{sn} - q^{sn-e} = q^{sn} - q^{sn-t+1} . \tag{16}$$

(ii) Let $p = q \ne 2$. We also have (15). For any b, the equation $b_1 k_1 + \ldots + b_n k_n = b\ (mod\ q^s)$ has $q^{s(n-1)}$ solutions. There are q^{s-e} numbers $b\ (mod\ q^s)$ with $q^e | b$ (and then $\chi_{(p)} = 1, t_\chi = 0$); $q^{s-e+1} - q^{s-e}$ numbers $b\ (mod\ q^s)$ with $q^{e-1} \| b$ (and then the order of

$\chi_{(p)}$ is $1 = e(p, L_\chi) = e_\chi, t_\chi = e_\chi + 1 = 2$); and $q^{s-e+i} - q^{s-3+i-1}$ numbers $b\ (mod\ q^s)$ with $q^{e-i}\|b$ (and then the order of $\chi_{(p)}$ is $e(p, L_\chi) = e_\chi = i, t_\chi = e + 1 = i + 1$). Thus we have

$$\begin{aligned} v_q &= q^{s(n-1)}\left(q^{s-e+1} - q^{s-e}\right) \times 2 + \left(q^{s-e+2} - q^{s-e+1}\right) \times 3 + \dots \\ &+ \left(q^s - q^{s-1}\right)(e+1) = \\ &= (e+1)q^{sn} - q^{sn-e} - q^{sn-e}(q^e - 1)/(q-1) \,. \end{aligned}$$

(iii) Let $p = 2$. Assume ψ is a primitive character modulo 4. First, let $f(X_i) \not\equiv 4\ (mod\ 8)$, i.e., $\varphi_{i(2)} \neq \psi\ \ (1 \leq i \leq n)$. Then it is similar to the case $p = q \neq 2$, but $t_\chi = e_\chi + 2$ by Lemma 2. Hence we have

$$\begin{aligned} v_q &= 2^{s(n-1)}\left((2^{s-e+1} - 2^{s-e}) \times 3 + \dots + (2^s - 2^{s-1}) \times (e+2)\right) \\ &= (e+1)2^{sn} - 2^{sn-e} \,. \end{aligned}$$

(iv) Let $p = 2$ and $\varphi_{n(2)} = \psi$. Since $< \psi\varphi', \psi\varphi'', \dots, \psi > = < \varphi', \varphi'', \dots \psi >$, so we may assume $\psi | X_i\ \ (1 \leq i \leq n-1)$. Then the 2-part of $\chi = \chi_1^{k_1} \dots \chi_n^{k_n}$ is

$$\chi_{(2)} = \varphi_2^{b_1 k_1 + \dots + b_{n-1} k_{n-1}} \cdot \psi^{k_n} = \varphi_2^b\, \psi^{k_n} \,,$$

here again we assume the order of $\varphi_2 = \varphi_{1(2)}$ is $\max e(2, K_i)$ and $\varphi_{i(2)} = \varphi_2^{b_i}$. For any $b, b_1k_1 + \dots + b_{n-1}k_{n-1} \equiv b\ (mod\ q^s)$ has $2^{s(n-2)}$ solutions (we assume here $n \geq 2$). There are 2^{s-e} numbers $b\ (mod\ q^s)$ with $2^e | b$, and then $\varphi_2^b = 1, t_x = t_{\psi^{k_n}} = 2$ (if k_n is odd) or 0 (if k_n is even). So there are $2^{s(n-2)} \cdot 2^{s-e} \cdot 2^{s-1}$ characters $\chi \in \hat{L}$ with $t_x = 2$. There are $2^{s-e+1} - 2^{s-e}$ numbers b with $2^{e-1}\|b$, and $2^{s(n-2)} \cdot 2^s$ vectors $(k_1, \dots, k_n)$, and then the order of φ_2^b is 2, so $t_x = 3$ (we assume $b_1 \dots b_{n-1} \neq 0$). Similarly, there are $2^{s-e+i} - 2^{s-e+i-1}$ numbers $b\ (mod\ q^s)$ with $2^{e-i}\|b$ and then $t_x = i + 3$. Hence

$$\begin{aligned} v_2 &= 2^{s(n-2)}(2^{s-e} \cdot 2^{s-1} \cdot 2 + 2^s \times (2^{s-e+1} - 2^{s-e}) \times 3 + \dots \\ &\quad 2^s \times (2^{s-e+i} - 2^{s-e+i-1}) \times (i+2) + \dots \\ &\quad + 2^s \times (2^s - 2^{s-1}) \times (e+2)) \\ &= (e+1) \cdot 2^{ns} \,. \end{aligned}$$

In addition, if $n = 1$, then obviously $v_2 = 2^s$; and if $b_1 \dots n_{n-1} = 0$, then obviously $v_2 = 2^{sn}$ since there are $2^{sn} - 2^{sn-s}$ characters $\chi \in \hat{L}$ containing ψ as a factor and then $t_x = 2$ (note that $k_1, \dots, k_{n-1}$ are arbitrary and k_n is odd). This proves Theorem 2.

Proof of Theorem 3 Let L and K have degrees q^{ns} and q^{ms} respectively. By Theorem 2, the different of L/Q is

$$\mathcal{D}(L/Q) = D(L)^{q^{-sn}} = q^{v_q q^{-sn}} \prod_p p^{v_p q^{-sn}}$$

since

$$\sigma\mathcal{D}(L/Q) = \mathcal{D}(\sigma L/\sigma\mathbb{Q}) = \mathcal{D}(L/\mathbb{Q}) \quad \text{for any} \quad \sigma \in \mathrm{Gal}(L/\mathbb{Q})$$

and

$$D(L) = N_{L/Q}\, \mathcal{D}(L/\mathbb{Q}) = \mathcal{D}(L/\mathbb{Q})^{q^{sn}}$$

then by

$$\tilde{v}_q(L) := v_q q^{-sn} = e + 1 - q^{-e} - \frac{1 - q^{-e}}{q - 1} \equiv e + 1 - (e+1) \equiv 0 \ \ (mod\ 2),$$

and

$$\tilde{v}_p(L) := v_p q^{-sn} = 1 - q^{-e} \equiv 0 \ \ (mod\ 2),$$

so

$$\mathcal{D}(L/K) = \mathcal{D}(L)/\mathcal{D}(K) = q^{v_q(\mathcal{D})} \prod_p p^{v_p(\mathcal{D})} \,,$$

where

$$\begin{aligned} v_q(\mathcal{D}) &= \tilde{v}_q(L) - \tilde{v}_q(K) = (e - e') + \frac{q^{e-e'} - 1}{q^e} \cdot \frac{q-2}{q-1} \,, \\ v_p(\mathcal{D}) &= \tilde{v}_p(L) - \tilde{v}_p(K) = q^{-e}(q^{e-e'} - 1) \,, \end{aligned}$$

here e' is defined for K similar to e for L.

Then it is easy to see that $D(L/K) = N_{L/K}\ \mathcal{D}(L/K) = \mathcal{D}(L/K)^{q^{n-m}}$ is a square (i.e., a principal ideal generated by a square element). On the other hand, since $[L : K] = q^{s(n-m)}$ is odd, so the discriminant Δ of any K-basis of L is a square. Theorem 3 follows from these facts and Artin's theorem mentioned at the beginning.

Proof of Theorem 4 Put $D(L/K) = 2^{v_2^*} \prod_p p^{v_p^*}$. Then, similarly to the proof of Theorem 3, we know that

$$v_p^* = q^{n-m-e}(q^{e-e'} - 1) \equiv 0 \quad (mod\ 2) \,.$$

As for v_2^*, note that $v_{21} = (e+1)2^{sn} - 2^{sn-e}, v_{22} = (e+1)2^{sn}, v_{23} = 2^{sn}$, so $\tilde{v}(L) = v_2 \cdot 2^{-sn} = (e+1) - 2^{-e}, (e+1)$, or 1 respectively. Denote $v(\mathcal{D}) = \tilde{v}(L) - \tilde{v}(K), v^* = v(\mathcal{D}) \cdot 2^{n-m}$. Let the case i/j denote the case $v_2(L) = v_{2i}, v_2(K) = v_{2j}$. Then only the following cases appear: cases 1/1, 2/2, 2/1, 2/3, 3/3 and 3/1. And in all these cases we have $v^* \equiv 0\ (mod\ 2)$. (For example, in Case 1/1, we have $v(\mathcal{D}) = e - e' - 2^{-e} + 2^{-e'}$, $v^* = (e^{e-e'} - 1)2^{n-m-e} \equiv 0\ (mod\ 2)$ since $n - m > e$.) Thus $D(L/K)$ is a square in all cases. Let us show Δ is also a square then. Assume $K = K_1K_2 \dots K_m$, $L = K_1 \dots K_m K_{m+1} \dots K_n$, $K' = K_{m+1} \dots K_n$, where K_i are cyclic fields of degree 2^s. Then $L = KK'$ and a $\mathbb{Q}$-basis of K' is a K-basis of L. Let $\{u_i\}$ be a $\mathbb{Q}$-basis of K_n, $\{v_j\}$ a $\mathbb{Q}$-basis of $K_{m+1} \dots K_{n-1}$ (note that $n - m \geq 2$), then $\{u_iv_j\}$ is a $\mathbb{Q}$-basis of K'. Hence

$$\Delta(L/K) = \Delta(K') = \det\{u_i^\sigma v_j^\tau\} = \Delta(K_n)^{2^{(n-m-1)s}} \cdot \Delta(K_{m+1} \dots K_{n-1})^{2^s}$$

is a square of a rational number. Therefore, by Artin's theorem, we have Theorem 4.

Acknowledgments

One of the authors (Z.X.) would like to thank Professor Abdus Salam, the International Atomic Energy Agency and UNESCO for hospitality at the International Centre for Theoretical Physics, Trieste.

REFERENCES

[1] Zhang Xianke, "A simple construction of genus fields of abelian number fields", Proc. Amer. Math. Soc. **94** (1985), No.3, 393–395.

[2] R. Bird and C. Parry, "Integral bases for bicyclic biquadratic fields over quadratic subfields", Pacific J. Math. **66** (1976), No.1, 29–36.

[3] L.C. Washington, "Relative integral bases", Proc. Amer. Math. Soc. **56** (1976) 93–94.

[4] Zhang Xianke, "Cyclic quartic fields and genus theory of their subfields", J. Number Theory **18** (1984), No.3, 350–355.

[5] Zhang Xianke, "Relative integral bases and units of fields of type $(\ell, \ell, \ldots, \ell)$", Acta Math. Sinica **29** (1986), No.5, 622–627.

[6] Zhang Xianke, "Relative integral bases of cyclic quartic number fields", Acta Math. Sinica **27** (1984), No.3, 425–432.

[7] Zhang Xianke, "On number fields of type $(2, 2, \ldots, 2)$", J. China Univ. Scien. Techn. **12** (1982), No.4, 29–41.

[8] Zhang Xianke, "On number fields of type $(\ell, \ell, \ldots, \ell)$", Scientia Sinica **A27** (1984), No.10, 1018–1026.