PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 94, Number 3, July 1985

A SIMPLE CONSTRUCTION OF GENUS FIELDS OF ABELIAN NUMBER FIELDS

ZHANG XIANKE

ABSTRACT. Simple elementary construction of the genus field K^* (= maximal abelian subfield of the Hilbert class field) of any abelian number field K is given without using class field theory. When K is of type $(l, \ldots, l)$ with l prime, the construction is more explicit. These results contain some former results and show that the main result in [**8**] has mistakes.

Let K be an abelian extension of the rational field $\mathbf{Q}$. The genus field K^* of K is, by definition of Leopoldt [**1**], the maximal absolute abelian number field containing K, which is unramified at all the finite prime ideals of K. Usually, the determination of genus fields involves application of class field theory (see [**1-3**]). In this paper, we will determine genus fields not using class field theory. We use only Hilbert ramification theory [**4**].

It is sufficient to assume the degree of K a power of a prime. In fact, if $[K : \mathbf{Q}] = l_1^{s_1} \cdots l_t^{s_t}$ (l_i are distinct rational primes, $s_i > 0$), then it follows that $K = K_1 \cdots K_t$ and $K^* = K_1^* \cdots K_t^*$, where K_i^* is the genus field of K_i and $[K_i : \mathbf{Q}] = l_i^{s_i}$ $(1 \leq i \leq t)$ [**2**].

THEOREM 1. *Let K be an absolute abelian number field of degree l^s, $l \in \mathbf{Z}$ be a rational prime, $s \geq 1$. Then the genus field of K is*

$$K^* = K \prod_{p \neq l} C_p = \prod_{p} C_p \quad (\textit{composite}),$$

where $p \in \mathbf{Z}$ runs over rational primes ramified in K, $e(p)$ is the ramification index of p in $K/\mathbf{Q}$, C_p is the unique subfield of degree $e(p)$ of $\mathbf{Q}(\varsigma_p)$ $(p \neq l)$, C_l is a subfield of degree $e(l)$ of $\mathbf{Q}(\varsigma_{l^t})$ for some t, $\varsigma_m = \exp(2\pi i/m)$.

PROOF. The field C_p $(p \neq l)$ is well defined since $e(p)|p-1$, which can be proved easily by elementary method [**4**, p. 126]. Alternatively, the Kronecker-Weber theorem (which has an elementary proof in [**4**]) yields that $K \subset \mathbf{Q}(\varsigma_m)$ for some m. Let $p^a || m$, then the ramification index of p in $\mathbf{Q}(\varsigma_m)$ is $p^{a-1}(p-1)$, so that $e(p)|(p^{a-1}(p-1), l^s)$, $e(p)|p-1$.

Let K' be the inertia field of p $(\neq l)$ in KC_p. We assert that

$$KC_p = K' C_p. \tag{3}$$

In fact, let E and E_1 be the inertia group and first ramification group of p in KC_p, respectively. It is well known that E/E_1 is cyclic and $|E_1|$ is a power of p. But $|E_1|$ divides now $[KC_p : \mathbf{Q}]$, a power of l, and it follows that $|E_1| = 1$ and E is cyclic with order $|E| \geq |E_K| = e(p)$. On the other hand, the restriction map $\sigma \mapsto (\sigma|_{C_p}, \sigma|_K)$

Received by the editors June 27, 1984.
1980 *Mathematics Subject Classification*. Primary 12A35; Secondary 12A65.
Key words and phrases. Number field, genus field, abelian extension.
©1985 American Mathematical Society
0002-9939/85 \$1.00 + \$.25 per page

defines an imbedding $E \to E_{C_p} \times E_K$, where E_k denotes the inertia group of p in any field k. Hence E has no element of order $> e(p)$. This implies $|E| = e(p)$. Since $K' \cap C_p = \mathbf{Q}$, it follows that

$$[K'C_p : \mathbf{Q}] = [K' : \mathbf{Q}][C_p : \mathbf{Q}] = [K' : \mathbf{Q}]e(p) = [K' : \mathbf{Q}][KC_p : K'] = [KC_p : \mathbf{Q}].$$

This proves (3).

Notice that p is not ramified in K', and the ramification index of each prime p_2 $(\neq p)$ in K' is still $e(p_2)$.

Similarly, for any p_2 $(\neq p, l)$, we have $K'C_{p_2} = K''C_{p_2}$, i.e. $KC_pC_{p_2} = K''C_pC_{p_2}$. Therefore, we have

$$KC_{p_1} \cdots C_{p_r} = K^{(r)}C_{p_1} \cdots C_{p_r}, \tag{4}$$

where every p $(\neq l)$ is not ramified in $K^{(r)}$. Thus we have $K^{(r)} = C_l$ from the Kronecker-Weber theorem (or proving directly as in [**4**]).

In obtaining (4), we have used only the following properties of K: the ramification index of p in K is $e(p)$ and $[K : \mathbf{Q}]$ is a power of l. Now K^*, the genus field of K, also has these properties since K^*/K is unramified. In fact, if a prime number q $(\neq l)$ divides $[K^* : \mathbf{Q}]$, then K^* has a subfield of degree q. Suppose a prime p ramifies in this subfield. It follows that $q|e(p)|l^s$, a contradiction. Therefore, as in the case of K, we have $K^*C_{p_1} \cdots C_{p_r} = C_lC_{p_1} \cdots C_{p_r} = L, K^* \subset L$. On the other hand, the ramification index of p_i in $L/\mathbf{Q}$ is obviously $[C_{p_i} : \mathbf{Q}] = e(p_i)$, i.e., L/K is an unramified extension. Therefore $K^* \supset L$. This completes the proof.

COROLLARY 1. *Let $K = \mathbf{Q}(\sqrt{m_1}, \dots, \sqrt{m_n})$ be an extension of degree 2^n of $\mathbf{Q}$, $m_i \in \mathbf{Z}$ squarefree. Then the genus field of K is*

$$K^* = \mathbf{Q}(\sqrt{p_1^*}, \dots, \sqrt{p_r^*})C_2 = K(\sqrt{p_1^*}, \dots, \sqrt{p_r^*}) \tag{5}$$

where $p_1, \dots, p_r$ are all the odd rational primes ramified in K, $p_i^* = (-1)^{(p-1)/2}p_i$; and

$$C_2 = \begin{cases} \mathbf{Q} & \text{if } e(2) = 1, \\ \mathbf{Q}(\sqrt{-1}) & \text{if } e(2) = 2, T \equiv -1 \pmod 4, \\ \mathbf{Q}(\sqrt{2}) & \text{if } e(2) = 2, T \equiv 2 \pmod 8, \\ \mathbf{Q}(\sqrt{-2}) & \text{if } e(2) = 2, T \equiv -2 \pmod 8, \\ \mathbf{Q}(\sqrt{-1}, \sqrt{2}) & \text{if } e(2) = 4; \end{cases}$$

here $T \in \mathbf{Z}$ is an arbitrary squarefree integer such that $\sqrt{T} \in K$, $T \not\equiv 1 \pmod 4$; $e(2)$ is the ramification index of 2 in K. In particular, $K^* = K_1^* \cdots K_n^*$, where K_i^* is the genus field of $K_i = \mathbf{Q}(\sqrt{m_i})$ $(1 \leq i \leq n)$.

PROOF. From [**5**] we know that the ramification index $e(p) = 2$ or 1 when p is odd, and $e(2) = 2$, 4 or 1. Therefore, Theorem 1 implies formula (5) since $C_{p_i} = \mathbf{Q}(\sqrt{p_i^*})$ $(i = 1, \dots, r)$. It remains to exhibit C_2. The cases $e(2) \neq 2$ are trivial. In case $e(2) = 2$, we have $C_2 = \mathbf{Q}(\sqrt{m})$ with $m = -1, 2$, or -2, and

$$K \subset K^* = \mathbf{Q}(\sqrt{m}, \sqrt{p_1^*}, \dots, \sqrt{p_r^*}).$$

Since $p_i^* \equiv 1 \pmod 4$, we see that every quadratic subfield of K^* has the form $\mathbf{Q}(\sqrt{T})$ where $T \equiv 1 \pmod 4$ or

$$T \equiv \begin{cases} m \pmod 4), & \text{when } m = -1, \\ m \pmod 8), & \text{when } m = \pm 2. \end{cases}$$

Moreover, there must exist some $\sqrt{T} \in K$ with $T \not\equiv 1 \pmod 4$ since 2 is ramified in K (cf. [**5**]). This determines C_2 and completes the proof.

COROLLARY 2. *Let K be an abelian number field with Galois group* $\mathrm{Gal}(K/\mathbf{Q}) \cong (\mathbf{Z}/\mathbf{Z})^n$, *$l$ an odd rational prime. Then the genus field of K is*

$$K^* = C_l C_{p_1} \cdots C_{p_r} = K C_{p_1} \cdots C_{p_r} \tag{6}$$

where C_{p_i} is the unique subfield of degree l of $\mathbf{Q}(\varsigma_{p_i})$ $(1 \leq i \leq r)$, C_l is the unique subfield of degree l of $\mathbf{Q}(\varsigma_{l^2})$ if l is ramified, and $C_l = \mathbf{Q}$ otherwise; $p_1, \ldots, p_r$ are all the ramified rational primes ($\neq l$). In particular, $K^* = K_1^* \cdots K_n^*$, where $K = K_1 \cdots K_n$, K_i are cyclic number fields of degree l.

PROOF. The results of [**6**] show that the ramification index $e(p)$ is always l for every ramified prime p. Thus the corollary follows from Theorem 1.

REMARK. (1) Corollary 1 contains the classical result about the genus fields of quadratic fields. It also contains the results about the genus fields for fields of type $(2, \ldots, 2)$ obtained by Kubokawa in [**7**].

(2) Corollary 1 shows evidently that the main result in [**8**] has some mistakes. In fact, Theorem 1 of [**8**] states that the genus field K^* of any number field K is $K \prod_p \Omega^{(p)}$, where $\Omega^{(p)}$ is a cyclic field of degree e_p^* for each ramified rational prime p, e_p^* denotes the G.C.F. of $(U_p : NU_{\mathfrak{p}_i})$, $\mathfrak{p}_i$ are K-primes over p, U_p and $U_{\mathfrak{p}_i}$ are local unit groups, and N denotes the local norm. It is well known that when K is abelian then $e_p^* = e(p)$, the ramification index of p in K (see, e.g., S. Lang's *Algebraic number theory*, p. 221). However, Corollary 1 implies that K^* has no cyclic subfield of degree 4 even when $e(2) = 4$. This proves the error of [**8**].

REFERENCES

1. H. W. Leopoldt, *Zur Geschlechtertheorie in abelschen Zahlkörpern*, Math. Nachr. **9** (1953), 350–362.
2. M. Ishida, *The genus fields of algebraic number fields*, Lecture Notes in Math., Vol. 555, Springer-Verlag, Berlin and New York, 1976.
3. C. S. Herz, *Construction of class fields*, Lecture Notes in Math., Vol. 21, Springer-Verlag, Berlin and New York, 1966.
4. D. A. Marcus, *Number fields*, Springer-Verlag, Berlin and New York, 1977.
5. Zhang Xianke, *On number fields of type* $(2, \ldots, 2)$, J. China Univ. Sci. Tech. **12** (1982), 29–41.
6. ——, *On number fields of type* $(l, \ldots, l)$, Sci. Sinica Ser. A **1** (1984), 31–38.
7. Y. Kubokawa, *The genus fields for composite of quadratic fields*, J. Saitama Univ. Fac. Ed. Math. Natur. Sci. **26** (1977), 1–3.
8. M. Bhaskaran, *Construction of genus field and some applications*, J. Number Theory **11** (1979), 488–497.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA, HEFEI, ANHUI, THE PEOPLE'S REPUBLIC OF CHINA