

ON UNIT GROUPS OF ABSOLUTE ABELIAN NUMBER FIELDS OF DEGREE pq

HIDEO YOKOI

In this note, we denote by \mathbb{Q} the rational number field, by \mathbf{E}_Ω the whole unit group of an arbitrary number field Ω of finite degree, and by r_Ω the rank of \mathbf{E}_Ω^* , where generally \mathbf{G}^* for an arbitrary abelian group \mathbf{G} means a maximal torsion-free subgroup of \mathbf{G} . $(N_{K/\Omega}\mathbf{E}_K)^*$ is shortly denoted by $N_{K/\Omega}^*\mathbf{E}_K$ and $(\mathbf{G}_1 : \mathbf{G}_2)$ is, as usual, the index of a subgroup \mathbf{G}_2 in \mathbf{G}_1 .

We first prove the following lemma.

LEMMA. *Let \mathbf{F} be a free abelian group of finite rank n , and \mathbf{G} be a subgroup of \mathbf{F} such that for a rational prime number l , \mathbf{G} contains the group \mathbf{F}^l consisting of all the l -th powers α^l of α in \mathbf{F} . Then, for an arbitrarily given basis $(\varepsilon_1, \dots, \varepsilon_n)$ of \mathbf{F} , \mathbf{G} has the basis $(\omega_1, \dots, \omega_n)$ of the following form:*

$$\omega_i = \begin{cases} \varepsilon_{\pi_i}^l \cdot \dots \cdot \varepsilon_{\pi_s}^s & i = 1, \dots, s, (s \geq 0) \\ \varepsilon_{\pi_i} \prod_{j=1}^s \varepsilon_{\pi_j}^{a_{ij}} & i = s+1, \dots, n, \end{cases}$$

where a_{ij} are rational integers with $0 \leq a_{ij} < l$ and (π_1, \dots, π_n) is a suitable permutation of $(1, \dots, n)$.

Proof. By the elementary divisor theory, there exist a basis (f_1, \dots, f_n) of \mathbf{F} and a basis (g_1, \dots, g_n) of \mathbf{G} such that we may write $(g_1, \dots, g_n) = (f_1, \dots, f_n)L$, where L is a $n \times n$ diagonal matrix with diagonal elements e_{i+1}/e_i ($i = 1, \dots, n-1$). By the assumption, however, all the l -th powers of the elements in \mathbf{F} are contained in \mathbf{G} , so we have $e_1 = \dots = e_s = l$, $e_{s+1} = \dots = e_n = 1$ for some integer s ($0 \leq s \leq n$). We express this basis (f_1, \dots, f_n) of \mathbf{F} by using the basis $(\varepsilon_1, \dots, \varepsilon_n)$ of \mathbf{F} :

$$(f_1, \dots, f_n) = (\varepsilon_1, \dots, \varepsilon_n)U,$$

where U is an unimodular matrix of degree n .

Received August 5, 1959.

We now consider the $s \times s$ minor determinants which are contained in the first s rows of $V = U^{-1}$. Since V is unimodular, the greatest common divisor of these minor determinants is equal to 1. Hence in these minor determinants there exists a minor determinant which is prime to l . Let j_1, \dots, j_s be column indices of it. Namely, let the minor determinant

$$\begin{vmatrix} v_{1 j_1}, & \dots, & v_{1 j_s} \\ \vdots & & \vdots \\ v_{s j_1}, & \dots, & v_{s j_s} \end{vmatrix}$$

of $V = (v_{ij})$ be prime to l . Let

$$\begin{vmatrix} v_{1 1}, & \dots, & v_{1 n} \\ \vdots & & \vdots \\ v_{s 1}, & \dots, & v_{s n} \\ l v_{s+1 1}, & \dots, & l v_{s+1 n} \\ \vdots & & \vdots \\ l v_{n 1}, & \dots, & l v_{n n} \end{vmatrix} = V_1$$

and consider the $s \times s$ minor determinants which are contained in the j_1 -th, \dots , j_s -th columns of V_1 . Then the minor determinant with row indices $(1, \dots, s)$ is equal to the corresponding minor determinant of V and the minor determinants with other row indices are obtained from those of V by multiplying some powers of l . Since the greatest common divisor of the $s \times s$ minor determinants which are contained in the j_1 -th, \dots , j_s -th columns of V is equal to 1, the greatest common divisor of the corresponding minor determinants of V_1 is also equal to 1. Hence there exists a $n \times n$ unimodular matrix W such that the j_1 -th, \dots , j_s -th columns are equal to those of V_1 .

Consider the matrix

$$U \begin{pmatrix} \overbrace{l \dots l}^s & \overbrace{\dots}^{n-s} \\ \vdots & \\ & l & & \\ & & 1 & \dots \\ & & & \dots & 1 \end{pmatrix} W.$$

Then the j_1 -th, \dots , j_s -th columns are obtained from those of UV by multiplying l . Let P be a $n \times n$ matrix corresponding to a permutation $(1, \dots, s, s+1, \dots, n)$. Then, since UV is the unit matrix of degree n we have

$$P^{-1}U \begin{pmatrix} \overbrace{l \dots l}^s & & \\ & \ddots & \\ & & l & & \\ & & & 1 & \dots & 1 \end{pmatrix} WP = \begin{pmatrix} l & 0 & Y \\ \vdots & \vdots & \vdots \\ 0 & l & \\ \vdots & \vdots & \vdots \\ 0 & & X \end{pmatrix}.$$

Taking the determinants of both sides, we have $|X| = \pm 1$, i.e. X is an unimodular matrix of degree $n - s$. Hence we have

$$P^{-1}U \begin{pmatrix} \overbrace{l \dots l}^s & & \\ & \ddots & \\ & & l & & \\ & & & 1 & \dots & 1 \end{pmatrix} WP \begin{pmatrix} \overbrace{1 \dots 1}^s & & 0 \\ & \ddots & \\ & & 1 & & \\ & & & 0 & X^{-1} \end{pmatrix} = \begin{pmatrix} \overbrace{l \dots l}^s & & A \\ & \ddots & \\ & & l & & \\ & & & 1 & \dots & 1 \\ & & & & 0 & X^{-1} \end{pmatrix},$$

where $A = (a_{ij})$ is an integral $s \times (n - s)$ matrix. Moreover, let $a_{ij} = -lb_{ij} + a'_{ij}$ with the smallest non-negative residue $a'_{ij} \pmod{l}$ and set $B = (b_{ij})$. Then the product

$$P^{-1}U \begin{pmatrix} \overbrace{l \dots l}^s & & 0 \\ & \ddots & \\ & & l & & \\ & & & 1 & \dots & 1 \\ & & & & 0 & X^{-1} \end{pmatrix} WP \begin{pmatrix} \overbrace{1 \dots 1}^s & & 0 \\ & \ddots & \\ & & 1 & & \\ & & & 0 & X^{-1} \end{pmatrix} \begin{pmatrix} \overbrace{1 \dots 1}^s & & B \\ & \ddots & \\ & & 1 & & \\ & & & 0 & X^{-1} \\ & & & & 1 & \dots & 1 \end{pmatrix}$$

is the matrix transforming the basis $(\epsilon_1, \dots, \epsilon_n)P = (\epsilon_{\pi_1}, \dots, \epsilon_{\pi_n})$ of \mathbb{F} into the basis

$$(g_1, \dots, g_n)WP \begin{pmatrix} \overbrace{1 \dots 1}^s & & 0 \\ & \ddots & \\ & & 1 & & \\ & & & 0 & X^{-1} \end{pmatrix} \begin{pmatrix} \overbrace{1 \dots 1}^s & & B \\ & \ddots & \\ & & 1 & & \\ & & & 0 & X^{-1} \\ & & & & 1 & \dots & 1 \end{pmatrix} = (\omega_1, \dots, \omega_n)$$

of \mathbb{G} , where (π_1, \dots, π_n) is a permutation of $(1, \dots, n)$. This basis $(\omega_1, \dots, \omega_n)$ of \mathbb{G} has the required properties of our lemma.

THEOREM 1. *Let K/Q be a cyclic extension of degree l^2 , where l is a prime number, and denote by Ω its subfield of degree l and by $(\epsilon_1, \dots, \epsilon_{r_\Omega})$ a system of fundamental units of Ω . Then, there exists a system of fundamental units*

$$\begin{cases} N_{K/\Omega_q} E_i = \pm 1, N_{K/\Omega_p} E_i = \bar{\varepsilon}_i & i = n + 1, \dots, r_{\Omega_p}, \\ N_{K/\Omega_p} E_i = \pm 1, N_{K/\Omega_q} E_i = \bar{\eta}_{i-r_{\Omega_p}} & i = r_{\Omega_p} + m + 1, \dots, r_{\Omega_p} + r_{\Omega_q}. \end{cases}$$

For, if $N_{K/\Omega_q} E_i = \prod_{j=1}^{r_{\Omega_q}} \bar{\eta}_j^{x_{ij}}$ ($i = n + 1, \dots, r_{\Omega_p}$) resp.

$$N_{K/\Omega_p} E_i = \prod_{j=1}^{r_{\Omega_p}} \bar{\varepsilon}_j^{y_{ij}} \quad (i = r_{\Omega_p} + m + 1, \dots, r_{\Omega_p} + r_{\Omega_q})$$

and $qy - px = px' - qy' = 1$ for some rational integers $x_{ij}, y_{ij}, x, x', y, y'$, then $\bar{E}_i = E_i^{qy} \bar{\varepsilon}_i^{-x} \prod_{j=1}^{r_{\Omega_q}} \bar{\eta}_j^{-x_{ij}y}$ resp. $\bar{E}_i = E_i^{px'} \bar{\eta}_i^{-y} \prod_{j=1}^{r_{\Omega_p}} \bar{\varepsilon}_j^{-y_{ij}x'}$ satisfy the required conditions.

For such $E_i, H_i = E_i^p \varepsilon_{\pi_i}^{-1} \prod_{j=1}^n \varepsilon_{\pi_j}^{-a_{ij}}$ ($n < i \leq r_{\Omega_p}$) resp. $H_i = E_i^q \eta_{\pi'_i}^{-1} \prod_{j=1}^m \eta_{\pi'_j}^{-b_{ij}}$ ($r_{\Omega_p} + m < i \leq r_{\Omega_p} + r_{\Omega_q}$) are relative units, and so they are written in the form

$$E_i = \sqrt[p]{\varepsilon_{\pi_i} \prod_{j=1}^n \varepsilon_{\pi_j}^{a_{ij}} H_i} \quad \text{resp.} \quad E_i = \sqrt[q]{\eta_{\pi'_i} \prod_{j=1}^m \eta_{\pi'_j}^{b_{ij}} H_i}.$$

Finally, if for any unit E of $K, N_{K/\Omega_p} E = \pm \prod_{i=1}^{r_{\Omega_p}} \bar{\varepsilon}_i^{x_i}$ and $N_{K/\Omega_q} E = \pm \prod_{i=1}^{r_{\Omega_q}} \bar{\eta}_i^{y_i}$ with rational integers x_i, y_i , then $H = E \prod_{i=1}^{r_{\Omega_p}} E_i^{-x_i} \prod_{j=1}^{r_{\Omega_q}} E_{r_{\Omega_p}+j}^{-y_j}$ is a relative unit of K , and so the unit E is written, by using the relative unit H , in the form $E = \prod_{i=1}^{r_{\Omega_p}} E_i^{x_i} \prod_{j=1}^{r_{\Omega_q}} E_{r_{\Omega_p}+j}^{y_j} H$. Therefore, the above obtained $\{E_i\}$ forms a system of fundamental units of K together with the relative fundamental units and it is evident that the equation

$$\mathbf{Q}_K \cdot (\mathbf{E}_{\Omega_p}^* : N_{K/\Omega_p}^* \mathbf{E}_K) (\mathbf{E}_{\Omega_q}^* : N_{K/\Omega_q}^* \mathbf{E}_K) = p^{r_{\Omega_p}} \cdot q^{r_{\Omega_q}}$$

holds.

Next we suppose that K is imaginary. Then either p or q is equal to 2, and so if we put $q = 2$, then p is odd prime and Ω_p is imaginary quadratic and Ω_2 is real. The relative units are roots of unity and the relative norm $N_{K/\Omega_2} \zeta$ of a root of unity ζ in Ω_p generates the whole unit group \mathbf{E}_{Ω_p} except the case of $\Omega_p = \mathbf{Q}(\sqrt{-3})$ $p = 3$.

For any basis $(\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_{r_{\Omega_2}})$ of $N_{K/\Omega_2}^* \mathbf{E}_K$, there exists a system of units $(E_1, \dots, E_{r_{\Omega_2}})$ of K such that $N_{K/\Omega_2} E_i = \bar{\varepsilon}_i, N_{K/\Omega_p} E_i = 1$ ($i = 1, \dots, r_{\Omega_2}$), and they are written in the form $E_i = \sqrt{\bar{\varepsilon}_i H_i}$, where H_i are relative units and so roots of unity. Such a system of units $\{E_i\}$ forms a system of fundamental units of K .

Example 1. If we assume in Theorem 2 that K is real and $p = 2, q = 3$, we

may take $\varepsilon, \{\eta, \eta'\}$ and $\{H, H'\}$ as a system of fundamental units of Ω_3, Ω_2 and a system of relative fundamental units of K respectively, where η' resp. H' means a conjugate of η resp. H .²⁾ Then, we may consider the following 15 types of system of fundamental units of K :

\mathbf{Q}_K System of fundamental units of K

- 1 $\{\varepsilon, \eta, \eta', H, H'\}$
- 3 $\{\sqrt[3]{\varepsilon HH'}, \eta, \eta', H, H'\}, \{\sqrt[3]{\varepsilon H^2 H'^2}, \eta, \eta', H, H'\}$
- 4 $\{\varepsilon, \sqrt{\eta}, \sqrt{\eta'}, H, H'\}, \{\varepsilon, \sqrt{\eta H}, \sqrt{\eta' H'}, H, H'\}$
 $\{\varepsilon, \sqrt{\eta H}, \sqrt{\eta' H H'}, H, H'\}, \{\varepsilon, \sqrt{\eta H H'}, \sqrt{\eta' H}, H, H'\}$
- 12 $\{\sqrt[3]{\varepsilon H H'}, \sqrt{\eta}, \sqrt{\eta'}, H, H'\}, \{\sqrt[3]{\varepsilon H^2 H'^2}, \sqrt{\eta}, \sqrt{\eta'}, H, H'\}$
 $\{\sqrt[3]{\varepsilon H H'}, \sqrt{\eta H}, \sqrt{\eta' H'}, H, H'\}, \{\sqrt[3]{\varepsilon H^2 H'^2}, \sqrt{\eta H}, \sqrt{\eta' H'}, H, H'\}$
 $\{\sqrt[3]{\varepsilon H H'}, \sqrt{\eta H'}, \sqrt{\eta' H H'}, H, H'\}, \{\sqrt[3]{\varepsilon H^2 H'^2}, \sqrt{\eta H'}, \sqrt{\eta' H H'}, H, H'\}$
 $\{\sqrt[3]{\varepsilon H H'}, \sqrt{\eta H H'}, \sqrt{\eta' H}, H, H'\}, \{\sqrt[3]{\varepsilon H^2 H'^2}, \sqrt{\eta H H'}, \sqrt{\eta' H}, H, H'\}$.

THEOREM 3. *Let K/\mathbf{Q} be a real and non-cyclic abelian extension of degree l^2 , where l is a prime number. Denote by Ω_i ($i = 1, \dots, l+1$) $l+1$ subfields of degree l and by $\{\varepsilon_{ij}\}$ ($j = 1, \dots, r_{\Omega_i}$) a system of fundamental units of Ω_i .*

Then, there exists a system of fundamental units $\{E_{ij}\}$ of K with the following properties:

$$E_{ij} = \begin{cases} \varepsilon_{i\pi_j^t} \cdots \cdots \cdots i = 1, \dots, l+1; j = 1, \dots, n_i, \\ l \sqrt{\varepsilon_{i\pi_j^i} \prod_{\substack{s=1, \dots, l+1 \\ t=1, \dots, n_i}} \varepsilon_{s\pi_t^s}^{a_{st}}} \cdots \cdots i = 1, \dots, l+1; j = n_i + 1, \dots, r_{\Omega_i}, \end{cases}$$

where a_{st} are rational integers with $0 \leq a_{st} < l$, $(\pi_1^i, \dots, \pi_{r_{\Omega_i}}^i)$ are suitable permutations of $(1, \dots, r_{\Omega_i})$ and n_i are rational integers with $0 \leq n_i \leq r_{\Omega_i}$ which are determined by K .

Moreover, the unit index (Einheitenindex) Q_K of K is equal to $l^{\sum_{i=1}^{l+1} (r_{\Omega_i} - n_i)}$, and so the product $\mathbf{Q}_K \prod_{i=1}^{l+1} (\mathbf{E}_{\Omega_i}^* : N_{K/\Omega_i}^* \mathbf{E}_K)$ divides the power $l^{\sum_{i=1}^{l+1} r_{\Omega_i}}$, but they are different in general.

Proof. For a fixed system of fundamental units $\{\varepsilon_{ij}\}$ of Ω_i , we consider the following $r_K \times r_K$ matrix $A = (a_{ij})$ with integral coefficients corresponding to a system of fundamental units (E_1, \dots, E_{r_K}) of K . Namely, if the relative

²⁾ Cf. the latter work by H. Hasse in 1).

norm $N_{K/\Omega_i} E_\nu$ of E_ν is $\pm \prod_{j=1}^{r_{\Omega_i}} \varepsilon_{ij}^{b_{\nu,ij}}$ with rational integers $b_{\nu,ij}$, then we put $b_{\nu,ij} = a_{\nu, (i-1)(l+1)+j}$ ($\nu = 1, \dots, r_K; i = 1, \dots, l+1; j = 1, \dots, r_{\Omega_i}$). The matrix corresponding to a second system of fundamental units (E'_1, \dots, E'_{r_K}) , obtained from (E_1, \dots, E_{r_K}) by an unimodular transformation U , is UA . Therefore, in a similar way as in lemma, we may show that there exist a system of fundamental units $\{E_{ij}\}$ of K and a system of suitably rearranged fundamental units $\{\varepsilon_{i\pi_j^t}\}$ of Ω_i such that the corresponding matrix $A = (a_{st})$ is normalized in the following manner:

For a rational integer m with $0 \leq m \leq r_K$,

$$a_{ss} = \begin{cases} 1 \cdot \dots \cdot s = 1, \dots, m, \\ l \cdot \dots \cdot s = m+1, \dots, r_K, \end{cases}$$

$$\begin{cases} 0 \leq a_{st} < l \cdot \dots \cdot s = 1, \dots, m; t = m+1, \dots, r_K, \\ a_{st} = 0 \cdot \dots \cdot \text{for all other pairs } (s, t). \end{cases}$$

On the other hand, since K is real, the relative units of K are only ± 1 . Therefore, if the relative norm $N_{K/\Omega_i} E$ of an unit E in K is $\pm \prod_{j=1}^{r_{\Omega_i}} \varepsilon_{ij}^{b_{ij}}$, then $E^l \prod_{i,j} \varepsilon_{ij}^{-b_{ij}} = \pm 1$, and so E is written in the form $E = \pm \sqrt[l]{\prod_{i,j} \varepsilon_{ij}^{b_{ij}}}$. Hence, we may write the above system of fundamental units $\{E_{ij}\}$ of K in the form

$$E_{ij} = \begin{cases} \pm \varepsilon_{i\pi_j^t} \cdot \dots \cdot i = 1, \dots, l+1; j = 1, \dots, n_i, \\ \pm \sqrt[l]{\varepsilon_{i\pi_j^t} \prod_{\substack{s=1, \dots, l+1 \\ t=1, \dots, n_i}} \varepsilon_{s\pi_{ts}^{ast}}} \cdot \dots \cdot i = 1, \dots, l+1; j = n_i+1, \dots, r_{\Omega_i}, \end{cases}$$

where $\sum_{i=1}^{l+1} n_i = r_K - m$.

Then the unit index Q_K of K is equal to $l^m = l^{\sum_{i=1}^{l+1} (r_{\Omega_i} - n_i)}$. The product $Q_K \cdot \prod_{i=1}^{l+1} (E_{\Omega_i}^* : N_{K/\Omega_i}^* \mathbf{E}_K)$ is not necessarily equal to l^{r_K} , but it is a factor of l^{r_K} .

Example 2. In particular, we assume that in Theorem 3, $l=2$ and denote by ε_i ($i = 1, 2, 3$) a fundamental unit of subfield Ω_i respectively. Then, there exist following 8 possible types of normalized matrix:

$$(1.1) \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix} \qquad (2.1) \begin{pmatrix} 2 & & \\ & 2 & \\ & & 2 \end{pmatrix}$$

$$(3.1) \begin{pmatrix} 1 & & \\ & 1 & \\ & & 2 \end{pmatrix} \qquad (3.2) \begin{pmatrix} 1 & 1 & \\ & 1 & \\ & & 2 \end{pmatrix} \qquad (3.3) \begin{pmatrix} 1 & & 1 \\ & 1 & 1 \\ & & 2 \end{pmatrix}$$

$$(4.1) \begin{pmatrix} 1 & & \\ & 2 & \\ & & 2 \end{pmatrix} \quad (4.2) \begin{pmatrix} 1 & 1 & \\ & 2 & \\ & & 2 \end{pmatrix} \quad (4.3) \begin{pmatrix} 1 & 1 & 1 \\ & 2 & \\ & & 2 \end{pmatrix}.$$

Here, the field of type (1.1) does not exist, but there exist infinitely many fields of any other type.³⁾

Furthermore, l^{r_K} is always equal to 2^3 , and for the system of fundamental units of K , unit index Q_K , etc., we have the following tableau:

Type	System of fundamental units	Q_K	$\prod_{i=1}^{l+1} (E_{\Omega_i}^* : N_{K/\Omega_i}^* E_K)$	Q_K	$\prod_{i=1}^{l+1} (E_{\Omega_i}^* : N_{K/\Omega_i}^* E_K)$
(2.1)	$\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$	1	2^3		2^3
(3.1)	$\{\sqrt{\varepsilon_1}, \sqrt{\varepsilon_2}, \varepsilon_3\}$	2^2	2		2^3
(3.2)	$\{\sqrt{\varepsilon_1 \varepsilon_3}, \sqrt{\varepsilon_2}, \varepsilon_3\}$	2^2	1		2^2
(3.3)	$\{\sqrt{\varepsilon_1 \varepsilon_3}, \sqrt{\varepsilon_2 \varepsilon_3}, \varepsilon_3\}$	2^2	1		2^2
(4.1)	$\{\sqrt{\varepsilon_1}, \varepsilon_2, \varepsilon_3\}$	2	2^2		2^3
(4.2)	$\{\sqrt{\varepsilon_1 \varepsilon_2}, \varepsilon_2, \varepsilon_3\}$	2	2		2^2
(4.3)	$\{\sqrt{\varepsilon_1 \varepsilon_2 \varepsilon_3}, \varepsilon_2, \varepsilon_3\}$	2	1		2

In case of imaginary number fields, l is equal to 2 and then Ω_1 is a real quadratic field and Ω_2, Ω_3 are imaginary quadratic fields. Therefore, the fundamental unit of K is either ε or $\sqrt{\zeta\varepsilon}$, where ε is a fundamental unit of Ω_1 and ζ is a root of unity in K such that $\sqrt{\zeta} \notin K$, and so the unit index Q_K of K is equal to 1 or 2.

*Mathematical Institute
Nagoya University*

³⁾ Cf. S. Kuroda, "Über den Dirichletschen Körper", J. Fac. Sci. Imp. Univ. Tokyo, Sec. I, Vol. IV, Part 5 (1943).
T. Kubota, "Über den bzyklischen biquadratischen Zahlkörper", Nagoya Math. J., 10 (1956).