19. *On the Group of Units of a Non-Galois Quartic or Sextic Number Field*

By Ken NAKAMULA
Department of Mathematics, Tokyo Metropolitan University

(Communicated by Shokichi IYANAGA, M. J. A., Feb. 12, 1980)

All number fields we consider are in the complex number field. The symbol $\langle S\rangle$ denotes a multiplicative group generated by S.

For a finite extension $k/\boldsymbol{Q}$, let E_k be the group of units of k, and E'_k be the group generated by all units of proper subfields of k together with roots of unity in k. We define the group H_k of relative units of k by

$H_k=\{\varepsilon\in E_k \mid N_{k/k'}(\varepsilon)$ is a root of unity for a proper subfield k' of $k\}$.

Let us consider the problem to construct E_k with the help of E'_k. It is interesting to utilize H_k together with E'_k when $(E_k:E'_k)=+\infty$. Hasse [2] has treated such a case when k is a real cyclic quartic number field. We are going to treat the case when k is a non-galois quartic (resp. sextic) number field having a quadratic subfield (resp. a quadratic and a cubic subfields). Then the galois closure of $k/\boldsymbol{Q}$ is a dihedral extension of degree 8 or 12 over $\boldsymbol{Q}$. We restrict our investigation on such extensions.

From now on, we assume $n=2$ or 3. Let $L/\boldsymbol{Q}$ be a galois extension of degree $4n$ with the galois group

$$G=\langle\sigma,\tau\rangle;\qquad \sigma^{2n}=\tau^2=(\sigma\tau)^2=1.$$

The invariant subfield of the subgroup $\langle\tau\rangle$ (resp. $\langle\sigma^3\tau\rangle$, $\langle\sigma^n\rangle$) is denoted by K (resp. F, Ω), and the maximal abelian subfield by Λ. Then K and F are non-galois number fields of degree $2n$ which we are going to study. The quadratic subfield of K (resp. F) is denoted by K_2 (resp. F_2). When $n=3$, the cubic subfield of both K and F is denoted by K_3. The quartic field Λ is the composite field of K_2 and F_2 which contains another quadratic subfield Λ_2. Note that $\Lambda=\Omega$ when $n=2$.

It is easy to show the following, which is in Nagell [6] when $n=2$.

Proposition 1. *When* $L\cap\boldsymbol{R}=\Omega$, *we have* $E_K=E'_K$ *and* $E_F=E'_F$.

Therefore we treat the two cases:

$$\text{Case I: } L\cap\boldsymbol{R}=K.\qquad \text{Case II: } L\subset\boldsymbol{R}.$$

Taking into account that all roots of unity of L is contained in the quartic subfield Λ, we take and fix a generator ω (resp. ζ, ρ) of the group of roots of unity of Λ (resp. Λ_2, F_2).

1. Type of E_K and E_F. A typical example of K and F are a pure number field of degree $2n$. The method, which is used in Stender [8],

[9], [10] in such cases, to determine fundamental units of K and F is based on the following easy lemma of group theory:

Let E be a free abelian group of rank r, and E_i be m subgroups of rank r_i $(1\leq i\leq m)$. Assume that there are m natural numbers n_i and m homomorphisms $f_i: E\to E_i$ which satisfy $f_i(x)=x^{n_i}$ for $x\in E_i$ and $f_i(x)=1$ for $x\in E_j$ $(j\neq i)$. Then $\langle E_1,\cdots,E_m\rangle=E_1\times\cdots\times E_m$ (direct product). Thus we put $f:=f_1\times\cdots\times f_m$, $H:=\mathrm{Ker}(f)=\{x\in E\,|\,f_i(x)=1\ (1\leq i\leq m)\}$ and $r_0:=\mathrm{rank}\,(H)$. Then we have

Lemma 1. (i) *The group* $\langle H, E_1\times\cdots\times E_m\rangle=H\times E_1\times\cdots\times E_m$. (ii) *The image* $f(E)$ *contains* $E_1^{n_1}\times\cdots\times E_m^{n_m}$ *and the inverse image* $f^{-1}(E_1^{n_1}\times\cdots\times E_m^{n_m})=H\times E_1\times\cdots\times E_m$. *Therefore* $r=r_0+r_1+\cdots+r_m$, *and the index* $(E:H\times E_1\times\cdots\times E_m)$ *divides* $n_1^{r_1}\cdots n_m^{r_m}$. (iii) *If* n_i $(1\leq i\leq m)$ *are pairwise relatively prime, a basis* $\{y_i\}_{i=1}^{s}$ $(s:=r-r_0)$ *of* $f(E)$ *can be chosen so that* $y_1,\cdots,y_{r_1}\in E_1$; $y_{r_1+1},\cdots,y_{r_1+r_2}\in E_2$; $\cdots$; $y_{s-r_m+1},\cdots,y_s\in E_m$.

In Lemma 1, if we regard E as $E_K/\langle -1\rangle$ (resp. $E_F/\langle\rho\rangle$) and E_i as the groups of units of maximal proper subfields of K (resp. F) modulo roots of unity, then the relative norm maps from K (resp. F) satisfy the condition of f_i, and then H can be regarded as $H_K/\langle -1\rangle$ (resp. $H_F/\langle\rho\rangle$). Hence we have

Corollary 1 (Nagell [6]). *Let* $n=2$. (i) *In Case* I, *let* $E_{K_2}=\langle -1,\eta_2\rangle$ *with* $\eta_2>1$, $H_K=\langle -1,\varepsilon_1\rangle$ *with* $\varepsilon_1>1$, *and let* $H_F(=E_F)=\langle\rho,\varepsilon_0\rangle$. *Then* $E_K=\langle -1,\varepsilon_1,\varepsilon_2\rangle$, *where*

$$\varepsilon_2=\eta_2 \text{ if } \pm\eta_2\notin N_{K/K_2}(E_K),\ \varepsilon_2=\sqrt{\eta_2} \text{ or } \sqrt{\varepsilon_1\eta_2} \text{ otherwise.}$$

(ii) *In Case* II, *let* $E_{K_2}=\langle -1,\eta_2\rangle$ *with* $\eta_2>1$, *and* $H_K=\langle -1,\varepsilon_0,\varepsilon_1\rangle$ *with* $\varepsilon_0>1$ *and* $\varepsilon_1>1$. *Then* $E_K=\langle -1,\varepsilon_0,\varepsilon_1,\varepsilon_2\rangle$, *where*

$$\varepsilon_2=\eta_2 \text{ if } \pm\eta_2\notin N_{K/K_2}(E_K), \text{ and } \varepsilon_2=\sqrt{\varepsilon_0^{\mu}\varepsilon_1^{\nu}\eta_2}\ (\mu,\nu=0 \text{ or } 1) \text{ otherwise.}$$

Corollary 2. *Let* $n=3$. (i) *In Case* I, *let* $E_{K_2}=\langle -1,\eta_2\rangle$ *with* $\eta_2>1$, $E_{K_3}=\langle -1,\eta_3\rangle$ *with* $\eta_3>1$, $H_K=\langle -1,\varepsilon_1\rangle$ *with* $\varepsilon_1>1$, *and let* $H_F=\langle\rho,\varepsilon_0\rangle$. *Then* $E_K=\langle -1,\varepsilon_1,\varepsilon_2,\varepsilon_3\rangle$ *and* $E_F=\langle\rho,\varepsilon_0,\varepsilon_3'\rangle$, *where* ε_2, ε_3 *and* ε_3' *are given by*:

$$\varepsilon_2=\eta_2 \text{ if } \eta_2\notin N_{K/K_2}(E_K), \text{ and } \varepsilon_2=\sqrt[3]{\eta_2} \text{ or } \sqrt[3]{\varepsilon_1\eta_2^{\pm1}} \text{ otherwise;}$$
$$\varepsilon_3=\eta_3 \text{ if } \eta_3\notin N_{K/K_3}(E_K), \text{ and } \varepsilon_3=\sqrt{\eta_3} \text{ or } \sqrt{\varepsilon_1\eta_3} \text{ otherwise;}$$
$$\varepsilon_3'=\eta_3 \text{ if } \eta_3\notin N_{F/K_3}(E_F), \text{ and } \varepsilon_3'=\sqrt{\rho^{\mu}\varepsilon_0^{\nu}\eta_3}\ (\mu,\nu=0 \text{ or } 1,\ \mu^2+\nu^2\neq 0) \text{ otherwise.}$$

(ii) *In Case* II, *let* $E_{K_2}=\langle -1,\eta_2\rangle$ *with* $\eta_2>1$, $E_{K_3}=\langle -1,\eta_3,\eta_4\rangle$ *with* $\eta_3>1$, $\eta_4>1$, *and let* $H_K=\langle -1,\varepsilon_0,\varepsilon_1\rangle$ *with* $\varepsilon_0>1$, $\varepsilon_1>1$. *Then* $E_K=\langle -1,\varepsilon_0,\varepsilon_1\cdots,\varepsilon_4\rangle$, *where* ε_i $(i=2,3,4)$ *are given by*:

$$\varepsilon_2=\eta_2 \text{ if } \eta_2\notin N_{K/K_2}(E_K), \text{ and } \varepsilon_2=\sqrt[3]{\varepsilon_0^{\mu}\varepsilon_1^{\nu}\eta_2}\ (\mu,\nu=\pm1 \text{ or } 0) \text{ otherwise;}$$
$$\varepsilon_3=\eta_3 \text{ if } \pm\eta_3\notin N_{K/K_3}(E_K), \text{ and } \varepsilon_3=\sqrt{\varepsilon_0^{\mu}\varepsilon_1^{\nu}\eta_3}\ (\mu,\nu=0 \text{ or } 1) \text{ otherwise;}$$
$$\varepsilon_4=\eta_4 \text{ if } \pm\eta_4,\ \pm\eta_3\eta_4\notin N_{K/K_3}(E_K), \text{ and } \varepsilon_4=\sqrt{\varepsilon_0^{\mu}\varepsilon_1^{\nu}\eta_3^{\lambda}\eta_4}\ (\mu,\nu,\lambda=0 \text{ or } 1) \text{ otherwise.}$$

2. Minkowski unit. In order to investigate the relation between E_K and E_F, the following group homomorphisms are useful when $n=2$ (resp. 3):

$$\varphi: K^\times \to F^\times;\ \varphi(x):=x^{1+\sigma}\ (\text{resp. } x^{\sigma+\sigma^2}),$$
$$\psi: F^\times \to K^\times;\ \psi(y):=y^{1+\sigma^3}\ (\text{resp. } y^{\sigma+\sigma^2}).$$

Then it is easy to see

Lemma 2. (i) *$\varphi(H_K)\subset H_F$ and $\psi(H_F)\subset H_K$.*

(ii) *When $n=2$ (resp. 3),*

$$\psi\circ\varphi(x)=x^2N_{K/K_2}(x)^\sigma\ (\textit{resp. } x^{-3}N_{K/K_2}(x)N_{K/K_3}(x^2))\ \textit{for } x\in K^\times,$$
$$\varphi\circ\psi(y)=y^2N_{F/F_2}(y)^\sigma\ (\textit{resp. } y^{-3}N_{F/F_2}(y)N_{F/K_3}(y^2))\ \textit{for } y\in F^\times.$$

From this lemma follow the following propositions.

Proposition 2. *Let $n=2$. The notation being as in Corollary 1, we have*

$$(H_K:\langle -1,\psi(H_F)\rangle)(H_F:\langle\rho,\varphi(H_K)\rangle)=2\ (\textit{resp. } 4)$$

in Case I (*resp. Case* II). *If $\varepsilon_2=\sqrt{\varepsilon_1\eta_2}\in K$ in Case* I, *we have*

$$H_F(=E_F)=\langle\rho,\varphi(\varepsilon_2)\rangle\quad\textit{and}\quad H_K=\langle -1,\psi(\varepsilon_0)\rangle.$$

Proposition 3. *Let $n=3$. The notation being as in Corollary 2, we have*

$$(H_K:\langle -1,\psi(H_F)\rangle)(H_F:\langle\rho,\varphi(H_K)\rangle)=3\ (\textit{resp. } 9)$$

in Case I (*resp. Case* II). *In Case* I, *it holds that*

$$H_F=\langle\rho,\varphi(\varepsilon_2)\rangle\quad\textit{and}\quad H_K=\langle -1,\psi(\varepsilon_0)\rangle$$

if $\varepsilon_2=\sqrt[3]{\varepsilon_1\eta_2^{\pm1}}\in K$, and that $\varepsilon_3=\eta_3$ if and only if $\varepsilon_3'=\eta_3$.

In Case I, we study whether L has a *Minkowski unit*; a unit which together with some of its conjugates forms a set of fundamental units of L (cf. Brumer [1]). A condition that L has a *real M-unit* (Minkowski unit which is real) is obtained by Propositions 2 and 3.

Theorem 1. *When $n=2$ (resp. 3) in Case I, the notation being as in Corollary 1 (resp. 2), the field L has a real M-unit ξ_1 (i.e. $\xi_1\in E_K$ such that $E_L=\langle\omega,\xi_1,\xi_1^\sigma,\cdots,\xi_1^{\sigma^{2n-2}}\rangle$) if and only if*

$$\varepsilon_2=\sqrt{\varepsilon_1\eta_2},\ E_A=\langle\omega,\eta_2\rangle\quad\textit{and}\quad K\neq K_2(\sqrt{2\eta_2}),\ \neq \boldsymbol{Q}(\sqrt[4]{2}),$$
$$(\textit{resp. } \varepsilon_2=\sqrt[3]{\varepsilon_1\eta_2^{\pm1}},\ \varepsilon_3=\sqrt{\varepsilon_1\eta_3},\ E_A=\langle\omega,\eta_2\rangle \textit{ and } E_\Omega=\langle\zeta,\eta_3,\eta_3^\sigma\rangle),$$

and then we can take $\xi_1=\varepsilon_2$ (resp. $\varepsilon_2^{-1}\varepsilon_3$) as an M-unit of L.

The proof of the "only if" part is easy. The "if" part is proved by showing that ε_2 (resp. $\varepsilon_2^{-1}\varepsilon_3$) actually gives an M-unit on account of Proposition 2 (resp. 3) and of the fact that E_L^n is contained in E_L'.

It seems more complicated to see whether L has an M-unit ξ_1 which is not necessarily real (e.g. $E_L=\langle\omega,\xi_1,\xi_1^\sigma,\xi_1^\tau\rangle$ when $n=2$ in Case I). However, we have

Proposition 4. *Let $n=2$ in Case* I. *The notation being as in Corollary 1, the field L has no M-unit if $E_K=\langle -1,\varepsilon_1,\eta_2\rangle$ and $E_A=\langle\omega,\sqrt{\omega\eta_2}\rangle$.*

The proof is given by showing contradiction under the assumption that there is an M-unit in L.

3. Binomial unit. In the following, we assume $K=\boldsymbol{Q}(\theta)$ $(\theta:=\sqrt[2n]{d}>0)$ is a real pure number field of degree $2n$ with a natural number $d>1$. We may suppose that the action of G on $L=\boldsymbol{Q}(\theta,\zeta)$ satisfies that $\theta^{\sigma}=\zeta\theta$, $\theta^{\tau}=\theta$, $\zeta^{\sigma}=\zeta$ and $\zeta^{\tau}=\zeta^{-1}$. Then $F=\boldsymbol{Q}(\sqrt[2n]{-n^n d})$ is a totally imaginary pure number field of degree $2n$. We mention that $\sqrt{\eta_2}\notin K$ when $n=2$ and that $\sqrt[3]{\eta_2}, \sqrt{\eta_3}\notin K$ when $n=3$.

We can construct a set of fundamental units of K in a certain case when K has a *binomial unit*.

Theorem 2. *Suppose that d is square free and that K has a binomial unit $a-b\theta$ with natural numbers a and b such that $a+1\geq b^{2n}$. Then a set $\{\xi_i\}_{i=1}^n$ of fundamental units of K is given by*

$\xi_1=a-b\theta$, $\xi_2=a+b\theta$; *and* $\xi_3=a^2+ab\theta+b^2\theta^2$ *when* $n=3$.

The theorem is proved by Stender's method in [8], [9] after some calculations. The field, which is considered in Theorem 2, is different from that of Stender [10] if $b>1$.

The simplest example of Theorem 2 is the case when $a=b^{2n}c\pm 1$ with a natural number c and $d=(a^{2n}-1)/b^{2n}$ is square free. There are infinitely many such cases for any fixed (odd when $n=2$) natural number b (see [5]). This example has been treated more in detail in author's article [7] when $n=3$.

By Propositions 2, 3 and Theorem 2, we obtain

Corollary 3. *The assumption being as in Theorem* 2,

$E_F=\langle\rho,\varphi(\xi_1)\rangle$ (*resp.* $\langle\rho,\varphi(\xi_1),\varphi(\xi_1^{\sigma^3})\rangle$) *when* $n=2$ (*resp.* 3).

As an explicit form of a set of fundamental units of K is given in the case of Theorem 2, we can determine E_A and E_Ω according to Kuroda [4] and Iimura [3] and see that the condition of Theorem 1 is satisfied except for the case $d=2$. Thus we have

Theorem 3. *The assumption being as in Theorem* 2, ξ_1 *is a real M-unit of* $L=\boldsymbol{Q}(\theta,\zeta)$ *if* $d\neq 2$.

Lastly, we give an example of L which has no (real or imaginary) M-unit in case when $n=2$. Let $\theta^4=d:=3g^2$ with a square free natural number g which is not divisible by 3. Then the condition of Proposition 4 is verified easily (cf. [4] and [8]).

Proposition 5. *The field* $L=\boldsymbol{Q}(\sqrt[4]{3g^2},\sqrt{-1})$ *has no M-unit if g is a square free natural number prime to* 3.

References

[1] A. Brumer: On the group of units of an absolutely cyclic number field of prime degree. J. Math. Soc. Japan, **21**, 357–358 (1968).

[2] H. Hasse: Arithmetische Bestimmung von Grundeinheit und Klassenzahl in zyklischen kubischen und biquadratischen Zahlkörpern. Abh. Deutsch. Akad. Wiss. Berlin, Math.-Nat. Kl. 1948, nr. 2, 95 pp (1950).

[3] K. Iimura: On the unit groups of certain sextic number fields (to appear in Abh. Math. Seminar Hamburg, **50**).

[4] S. Kuroda: Über den Dirichletschen Körper. J. Fac. Sci. Univ. Tokyo, Sec. IA, **4**, 383–406 (1943).

[5] T. Nagell: Zur Arithmetik der Polynome. Abh. Math. Seminar Hamburg, **1**, 174–194 (1922).

[6] ——: Sur quelques questions dans la théorie des corps biquadratiques. Arkiv för Mathematik, **4**, 347–376 (1961).

[7] K. Nakamula: An explicit formula for the fundamental units of a real pure sextic number field and its galois closure. Pacific J. Math., **83**, 463–471 (1979).

[8] H.-J. Stender: Grundeinheiten für einige unendlich Klassen reinen biquadratischen Zahlkörper mit einer Anwendung auf die diophantische Gleichung $x^4 - ay^4 = \pm c$ ($c=1$, 2, 4 order 8). J. reine angew. Math., **264**, 207–220 (1973).

[9] ——: Über die Einheitengruppe der reinen algebraischen Zahlkörper sechsten Grades. Ibid., **268/269**, 78–93 (1974).

[10] ——: Lösbare Gleichungen $ax^n - by^n = c$ und Grundeinheiten für einige algebraische Zahlkörper vom Grade $n, n=3, 4, 6$. Ibid., **290**, 24–62 (1977) .