TOKYO J. MATH.
VOL. 8, NO. 1, 1985

On Bases of Purely Cubic Fields over Quadratic Fields

Kiyoshi NAGATA

Sophia University
(Communicated by Y. Kawada)

Let K/k be a relative algebraic number field of degree n. It is known that under a certain condition there exist n elements of K, say $\omega_1, \cdots, \omega_n$, satisfying

$$O_K = O_k\omega_1 \oplus \cdots \oplus O_k\omega_n ,$$

where O_K, O_k are the rings of integers of K, k respectively. We call a set of these $\omega_1, \cdots, \omega_n$ a relative integral basis w.r.t. K/k. It is not still easy to have a relative integral basis explicitly. H. Wada have determined one in case that $k=\boldsymbol{Q}(\sqrt{-3})$, $K=k(\sqrt[3]{A})$ with A being an element of k, in [1]. In this paper, we have got a basis under some hypotheses by the same method in [1] when $k=\boldsymbol{Q}(\sqrt{m})$, $K=k(\sqrt[3]{A})$ with m being a square free rational integer and A being an element of k.

§1. Now, let m be a square free integer and k be the field $\boldsymbol{Q}(\sqrt{m})$ as we mentioned above. For some cubic free integer A of k, let K be the field $k(\sqrt[3]{A})$. The purpose of this paper is to get a basis $\omega_1, \omega_2, \omega_3$ of O_K over O_k, on the following hypotheses H1, H2:

H1. Any prime ideal $\mathfrak{p}$ in O_k which divides (3) is principal.

H2. $A=fg^2$, f and g being in O_k such that (f) and (g) have no square ideal factors and are relatively prime.

We will see that these hypotheses H1, H2 are sufficient for the existance of relative integral basis. But these may not be always necessary. The hypothesis H2 is necessary only for the convenience of the calculation in our method. It seems that the hypothesis H1 is more essential. But we will not discuss this problem in this paper.

Put $\bar{A}=f^2g$, $\theta=\sqrt[3]{A}$ and $\bar{\theta}=\sqrt[3]{\bar{A}}$. By the relation $\theta^2=g\bar{\theta}$, any element of K can be expressed as the form $\omega=\alpha+\beta\theta+\gamma\bar{\theta}$ with $\alpha, \beta, \gamma \in k$. It can be easily verified that ω is in O_K iff there exist s, t and u in O_k such that $3\alpha=s$, $-3\alpha^2+3\beta\gamma fg=t$ and $\alpha^3+\beta^3A+\gamma^3\bar{A}-3\alpha\beta\gamma fg=u$. Hence

Received October 15, 1983

$$(3\beta)^3A\cdot(3\gamma)^3\bar{A}=(3\cdot3\beta\gamma fg)^3=((3\alpha)^2+3t)^3=(s^2+3t)^3\ ,$$
$$(3\beta)^3A+(3\gamma)^3\bar{A}=3(3\alpha)(3\beta)(3\gamma)fg-(3\alpha)^3+3^3u=3s(s^2+3t)-s^3+3^3u\ ,$$

are in O_k. Since (A) and $(\bar{A})$ contain no cubic ideal factors, both 3β and 3γ are in O_k. Therefore, the following are necesary and sufficient for ω being in O_K:

$$\omega=\frac{a+b\theta+c\bar{\theta}}{3}\ , \quad \text{where } a, b, c \text{ are in } O_k\ .$$

(1) $\quad bcfg\equiv a^2 \quad \mathrm{mod}(3)$.

(2) $\quad a^3+b^3A+c^3\bar{A}\equiv 3abcfg \quad \mathrm{mod}(3)^3$.

First of all, we will prove the following lemma.

LEMMA. *Let $\mathfrak{p}$ be a prime ideal in O_k which divides (3), $\omega=(a+b\theta+c\bar{\theta})/3$ be in O_K where a, b, c are in O_k. Then the following conditions are equivalent:*
(i) *$\mathfrak{p}$ divides (a).*
(ii) *$\mathfrak{p}$ divides (b).*
(iii) *$\mathfrak{p}$ divides (c).*

PROOF. Since ω is in O_K, we have

(1)′ $\quad bcfg\equiv a^2 \quad \mathrm{mod}\ \mathfrak{p}$,

(2)′ $\quad a^3+b^3A+c^3\bar{A}\equiv 3abcfg \quad \mathrm{mod}\ \mathfrak{p}^3$.

From (1)′, (ii)→(i) and (iii)→(i) are obvious. If both of (i) and (ii) hold, then from (2)′ $\mathfrak{p}^3$ divides $(c^3\bar{A})$, which implies (iii) by (H2). Similarly we have (i) and (iii)→(ii). We assume (i). From (1)′ and (2)′, we have

(1)″ $\quad b^3A\cdot c^3\bar{A}\equiv 0 \quad \mathrm{mod}\ \mathfrak{p}^3$,

(2)″ $\quad b^3A+c^3\bar{A}\equiv 0 \quad \mathrm{mod}\ \mathfrak{p}^3$.

(1)″ says that $\mathfrak{p}^2$ divides (b^3A) or $(c^3\bar{A})$, and (2)″ says that $\mathfrak{p}^2$ divides (b^3A) iff $\mathfrak{p}^2$ divides $(c^3\bar{A})$. Thus (b^3A) and $(c^3\bar{A})$ are divisible by $\mathfrak{p}^2$, but from (H2) we get that $\mathfrak{p}^2$ does not divide both A and $\bar{A}$. Therefore we get (ii) or (iii). Q.E.D.

When we begin to consider the congruences (1) and (2), we may immediately notice that we have to consider them according to the way of decomposition of the ideal (3) in O_k. Fortunately the way of decomposition of the ideal (p) in O_k, where p is a rational prime number, is not so complicated and is well known. It depends only on the value of the Legendre symbol (m/p). Especially when $p=3$, there are following three cases.

(I) $m\equiv 0 \bmod 3$, that is $(3)=\mathfrak{p}^2$ in O_k.

(II) $m\equiv 1 \bmod 3$, that is $(3)=\mathfrak{p}_1\mathfrak{p}_2$ in O_k, $\mathfrak{p}_1\neq\mathfrak{p}_2$.

(III) $m\equiv -1 \bmod 3$, that is $(3)=\mathfrak{p}$ in O_k.

Since $1, \theta, \bar\theta$ are in O_K, we may consider ω modulo $O_k\oplus O_k\theta\oplus O_k\bar\theta$ and except a factor of unit.

§ **2.** *Case* (I). Let $\mathfrak{p}=(\pi)$ with π in O_k. In this case we can choose $\{0, \pm 1\}$ as a complete system of representatives of $O_k/\mathfrak{p}$ and, without loss of generality, we may assume $f\not\equiv -1$, $g\not\equiv -1 \bmod \mathfrak{p}$. For any $\omega=(a+b\theta+c\bar\theta)/3$ $(a, b, c\in O_k)$, we may consider the only three cases as follows:

(I-1) $\mathfrak{p}^2$ divides (a) and does not divide both (b) and (c).

(I-2) $\mathfrak{p}$ divides (a) only once.

(I-3) $\mathfrak{p}$ does not divide (a).

Case (I-1). Since $\mathfrak{p}$ divides (a), from the lemma, we have $(b), (c)$ are divisible by $\mathfrak{p}$. Thus (1) holds. And (2) is equivalent to $b^3A+c^3\bar A\equiv 0 \bmod \mathfrak{p}^6$, from which we can see that $\mathfrak{p}^2$ divides (b) iff $\mathfrak{p}^2$ divides (c). This says both (b) and (c) are divisible by $\mathfrak{p}$ only once.

Put $b=e\pi$, $c=e'\pi$, where we may assume $e, e'=\pm 1$, because $(\pi^2)=(3)$. Then (2) is equivalent to

$$(3)\qquad (eg+e'f)fg\equiv 0 \quad \bmod \mathfrak{p}^3 .$$

Since (fg) is divisible at most once by $\mathfrak{p}$, we have $eg\equiv -e'f \bmod \mathfrak{p}^2$, which says $f\equiv g\equiv 1 \bmod \mathfrak{p}$ and $e=-e'\neq 0$. Then (3) is equivalent to

$$\begin{aligned} efg(g-f)&\equiv 0 \quad \bmod \mathfrak{p}^3 ,\\ g&\equiv f \quad \bmod \mathfrak{p}^3 . \end{aligned}$$

In this case, $\omega=(\theta-\bar\theta)/\pi$.

Case (I-2). Similarly as in (I-1), we see that $\mathfrak{p}$ divides $(b), (c)$ and thus (1) holds. Putting $a\pi, b\pi, c\pi$ instead of a, b, c in (2), we have

$$a^3+b^3fg^2+c^3f^2g\equiv 3abcfg \quad \bmod \mathfrak{p}^3 .$$

Repeating the same argument in (I-1), we may assume $a=1$, $b=e$, $c=e'$ with e, $e'=0, \pm 1$, and (2) is

$$(4)\qquad 1+efg^2+e'f^2g\equiv 3ee'fg \quad \bmod \mathfrak{p}^3 .$$

This shows that $fg\not\equiv 0 \bmod \mathfrak{p}$. Thus $f\equiv g\equiv 1 \bmod \mathfrak{p}$. Put $f=1+\pi x$, $g=1+\pi y$ with x, y in O_k. Then (4) is

$$(4)' \quad (1+e+e')+(e-e')(x-y)\pi+\{e(y^2+2xy)+e'(x^2+2xy)\}\pi^2 \equiv 3ee' \mod \mathfrak{p}^3 .$$

Replacing $\mathrm{mod}\ \mathfrak{p}^3$ by $\mathrm{mod}\ \mathfrak{p}$, we have $1+e+e' \equiv 0 \mod \mathfrak{p}$. Hence $(e, e')=(0, -1)$, $(-1, 0)$ or $(1, 1)$.
When $e=0$, $e'=-1$, $(4)'$ is

$$\begin{aligned} &(x-y)(1-\pi x) \equiv 0 && \mathrm{mod}\ \mathfrak{p}^2 , \\ &x \equiv y && \mathrm{mod}\ \mathfrak{p}^2 . \end{aligned}$$

When $e=-1$, $e'=0$, $(4)'$ is

$$\begin{aligned} &(x-y)(1-\pi y) \equiv 0 && \mathrm{mod}\ \mathfrak{p}^2 , \\ &x \equiv y && \mathrm{mod}\ \mathfrak{p}^2 . \end{aligned}$$

When $e=1$, $e'=1$, $(4)'$ is

$$\begin{aligned} &(x^2+y^2+4xy)\pi^2 \equiv 0 , && \mathrm{mod}\ \mathfrak{p}^3 , \\ &(x-y)^2 \equiv 0 && \mathrm{mod}\ \mathfrak{p} , \\ &x \equiv y && \mathrm{mod}\ \mathfrak{p} . \end{aligned}$$

Hence we only have the following two cases

$$f \equiv g \quad \mathrm{mod}\ \mathfrak{p}^3 \quad \text{and} \quad \omega=\frac{1-\theta}{\pi} , \quad \frac{1-\bar{\theta}}{\pi} , \quad \frac{1+\theta+\bar{\theta}}{\pi} .$$

$$f \equiv g \quad \mathrm{mod}\ \mathfrak{p}^2 \quad \text{and} \quad \omega=\frac{1+\theta+\bar{\theta}}{\pi} .$$

Case (I-3). In this case, since there exists the inverse of a mod 3, we may assume $a=1$. Then (1) and (2) become as follows:

$$(5) \qquad bcfg \equiv 1 \quad \mathrm{mod}\ \mathfrak{p}^2 .$$

$$\begin{aligned} &1+b^3fg^2+c^3f^2g-3bcfg \equiv 0 && \mathrm{mod}\ \mathfrak{p}^6 , \\ &(1-b^3fg^2)(c^3f^2g-1)+(bcfg)^3-3bcfg+2 \equiv 0 && \mathrm{mod}\ \mathfrak{p}^6 , \\ &(1-b^3fg^2)(c^3f^2g-1)+(bcfg-1)^2(bcfg+2) \equiv 0 && \mathrm{mod}\ \mathfrak{p}^6 . \end{aligned}$$

Applying (5) to $(bcfg-1)^2(bcfg+2)$,

$$(6) \qquad (b^3fg^2-1)(c^3f^2g-1) \equiv 0 \quad \mathrm{mod}\ \mathfrak{p}^6 .$$

From (5), we have

$$\begin{aligned} &(bcfg)^3-3(bcfg)^2+3bcfg-1 \equiv 0 && \mathrm{mod}\ \mathfrak{p}^6 , \\ &(bcfg)^3-1 \equiv 3bcfg(bcfg-1) && \mathrm{mod}\ \mathfrak{p}^6 , \\ &(bcfg)^3 \equiv 1 && \mathrm{mod}\ \mathfrak{p}^4 . \end{aligned}$$

From (6), c^3f^2g-1 or b^3fg^2-1 is divisible by $\mathfrak{p}^3$. For example, let b^3fg^2-1 be divisible by $\mathfrak{p}^3$. Then

$$b^3fg^2\equiv 1\equiv b^3c^3f^3g^3 \mod \mathfrak{p}^3 ,$$

which says

$$c^3f^2g\equiv 1 \mod \mathfrak{p}^3 .$$

Hence (6) is equivalent to

$$b^3fg^2\equiv c^3f^2g\equiv 1 \mod \mathfrak{p}^3 . \tag{7}$$

Now let $(O_k/\mathfrak{p}^2)^*$, $(O_k/\mathfrak{p}^3)^*$ be the multiplicative groups of $O_k/\mathfrak{p}^2$, $O_k/\mathfrak{p}^3$ respectively and put $\sigma=-1+\pi$, $\tau=1+\pi^2$. Since $(O_k/\mathfrak{p}^2)^*$, $(O_k/\mathfrak{p}^3)^*$ have order 6, 18 respectively and from the tables 1, 2 we have

$$(O_k/\mathfrak{p}^2)^*=\langle\sigma \bmod \mathfrak{p}^2\rangle ,$$
$$(O_k/\mathfrak{p}^3)^*=\langle\sigma \bmod \mathfrak{p}^3\rangle\times\langle\tau \bmod \mathfrak{p}^3\rangle .$$

TABLE 1.

s	0	1	2	3
$\sigma^s \bmod \mathfrak{p}^2$	1	$-1+\pi$	$1+\pi$	-1

order $\sigma=6$

TABLE 2.

s	0	1	2	3
$\sigma^s \bmod \mathfrak{p}^3$	1	$-1+\pi$	$1-2\pi+\pi^2$	-1

order $\sigma=6$

t	0	1	2	3
$\tau^t \bmod \mathfrak{p}^3$	1	$1+\pi^2$	$1-\pi^2$	1

order $\tau=3$

Since b, c appear in (7) as b^3, c^3 with modulus $\mathfrak{p}^3$ and $f\equiv g\equiv 1 \bmod \mathfrak{p}$, we may put $b=\sigma^{\bar b}$, $c=\sigma^{\bar c}$, $f=\sigma^{2\bar f}\tau^{\bar f'}$, $g=\sigma^{2\bar g}\tau^{\bar g'}$ with integers $\bar b$, $\bar c$, $\bar f$, $\bar g$, $\bar f'$, $\bar g'$ such that $0\leqq\bar b$, $\bar c<6$, $0\leqq\bar f$, $\bar g$, $\bar f'$, $\bar g'<3$. And (7) is

$$\sigma^{3\bar b+2\bar f+4\bar g}\tau^{\bar f'+2\bar g'}\equiv\sigma^{3\bar c+4\bar f+2\bar g}\tau^{2\bar f'+\bar g'}\equiv 1 \mod \mathfrak{p}^3 .$$

We see that this is equivalent to

$$\bar f'=\bar g' \quad\text{and}\quad 3\bar b+2\bar f+4\bar g\equiv 3\bar c+4\bar f+2\bar g\equiv 0 \mod 6 , \tag{8}$$

$3\bar b+2\bar f+4\bar g\equiv 0 \bmod 6$ says $\bar f\equiv\bar g \bmod 3$. Hence $\bar f=\bar g$. Therefore we have

$$\bar{f}'=\bar{g}', \quad \bar{f}=\bar{g}, \quad \bar{b}=\text{even}, \quad \bar{c}=\text{even}.$$

This means (7) is equivalent to

$$(9) \qquad f\equiv g \mod \mathfrak{p}^3, \qquad b\equiv c\equiv 1 \mod \mathfrak{p}.$$

Applying this to (5), we also have

$$(10) \qquad bcf^2\equiv 1 \mod \mathfrak{p}^2.$$

Consequently we have following three cases. The first is $f\not\equiv g \mod \mathfrak{p}^2$ and any element of O_K is given as a linear combination of $1, \theta, \bar{\theta}$ over O_k. The second is $f\equiv g \mod \mathfrak{p}^2$, $f\not\equiv g \mod \mathfrak{p}^3$ and any element of O_K is given as a linear combination of $1, \theta, (1+\theta+\bar{\theta})/\pi$ over O_k. The last case is $f\equiv g \mod \mathfrak{p}^3$ and in this case $1, \theta, \bar{\theta}, (1+\theta+\bar{\theta})/\pi, (1-\theta)/\pi, (1-\bar{\theta})/\pi, (\theta-\bar{\theta})/\pi, (1+b\theta+c\bar{\theta})/3$, where $b\equiv c\equiv 1 \mod \mathfrak{p}$ and $bcf^2\equiv 1 \mod \mathfrak{p}^2$, are sufficient to generate O_K over O_k.

We will show that we can choose $1, (1-\theta)/\pi, (f+\theta+\bar{\theta})/3$ for basis. If we take b, c as $b\equiv c\equiv f^{-1} \mod \mathfrak{p}^2$, then b, c satisfy $b\equiv c\equiv 1 \mod \mathfrak{p}$ and $bcf^2\equiv 1 \mod \mathfrak{p}^2$. Since $(1+b\theta+c\bar{\theta})/3$ is in O_K so is $(f+fb\theta+fc\bar{\theta})/3$ and we may see $(f+\theta+\bar{\theta})/3$ is in O_K. Now we must only show that any element of O_K is expressed as a linear combination of $1, (1-\theta)/\pi, (f+\theta+\bar{\theta})/3$. Let $(a+b\theta+c\bar{\theta})/3$ be in O_K, then so is $(a+b\theta+c\bar{\theta})/3-c(f+\theta+\bar{\theta})/3=\{(a-cf)+(b-c)\theta\}/3$. But $\{(a-cf)+(b-c)\theta\}/3$ becomes 0 or $\pm(1-\theta)/\pi \mod O_k\oplus O_k\theta\oplus O_k\bar{\theta}$. Hence $(a+b\theta+c\bar{\theta})/3$ is given as a linear combination of $1, (1-\theta)/\pi, (f+\theta+\bar{\theta})/3$. Thus we have proved the following theorem.

THEOREM I. *Let $k=Q(\sqrt{m})$ with $m\equiv 0 \mod 3, K=k(\sqrt[3]{A})$ with an integer A of k. We assume that* H1 *and* H2 *hold and $f\not\equiv -1 \mod \mathfrak{p}$, $g\not\equiv -1 \mod \mathfrak{p}$. Put $\theta=\sqrt[3]{A}$, $\bar{\theta}=\theta^2/g$, $\mathfrak{p}=(\pi)$. Then a basis of O_K as O_k-module and the relative discriminant $d(K/k)$ are given as follows*:

(a) *When $f\not\equiv g \mod \mathfrak{p}^2$, then $\{1, \theta, \bar{\theta}\}$ is a basis and $d(K/k)=(3^3f^2g^2)$.*

(b) *When $f\not\equiv g \mod \mathfrak{p}^2$, $f\not\equiv g \mod \mathfrak{p}^3$ then $\{1, \theta, (1+\theta+\bar{\theta})/\pi\}$ is a basis and $d(K/k)=(3^2f^2g^2)$.*

(c) *When $f\equiv g \mod \mathfrak{p}^3$, then $\{1, (1-\theta)/\pi, (f+\theta+\bar{\theta})/\pi\}$ is a basis and $d(K/k)=(f^2g^2)$.*

§**3.** *Case* (II). Let $\mathfrak{p}_1=(\pi_1)$, $\mathfrak{p}_2=(\pi_2)$ with π_1, π_2 in O_k. In this case we can also choose $\{0, \pm 1\}$ as a complete system of representatives of $O_k/\mathfrak{p}_i$ $(i=1, 2)$. Put $f_i=\pm f$, $g_i=\pm g$ so that $f_i\not\equiv -1$, $g_i\not\equiv -1 \mod \mathfrak{p}_i$ and put $A_i=f_ig_i^2$, $\bar{A}_i=f_i^2g_i$, $\theta_i=\sqrt[3]{A_i}$ and $\bar{\theta}_i=\sqrt[3]{\bar{A}_i}$ $(i=1, 2)$. Then $K=k(\theta)=k(\theta_1)=k(\theta_2)$, $\theta=\pm\theta_1=\pm\theta_2$ and $\bar{\theta}=\pm\bar{\theta}_1=\pm\bar{\theta}_2$. From the lemma for any

$\omega=(a+b\theta+c\bar{\theta})/3$ $(a, b, c \in O_k)$, we may consider the only three cases as follows:

(II-1) $\mathfrak{p}_1$ does not divide (a) and $\mathfrak{p}_2$ divides (a).

(II-2) $\mathfrak{p}_1$ divides (a) and $\mathfrak{p}_2$ does not divide (a).

(II-3) Neither $\mathfrak{p}_1$ nor $\mathfrak{p}_2$ divides (a).

Case (II-1). Since both (b) and (c) are divisible by $\mathfrak{p}_2$, from the lemma ω is expressed as the form $\omega_1=(a+b\theta_1+c\bar{\theta}_1)/\pi_1$ and (1) and (2) become as follows:

$$bcf_1g_1\equiv a^2 \mod \mathfrak{p}_1 ,$$
$$a^3+b^3f_1g_1^2+c^3f_1^2g_1\equiv 3abcf_1g_1 \mod \mathfrak{p}_1^3 ,$$

where we may assume $a=1$, b, $c=\pm 1$. Thus (1) and (2) are equivalent to the following (11) and (12):

$$\text{(11)} \qquad bcf_1g_1\equiv 1 \mod \mathfrak{p}_1 ,$$
$$\text{(12)} \qquad 1+b^3f_1g_1^2+c^3f_1^2g_1\equiv 3bcf_1g_1 \mod \mathfrak{p}_1^3 ,$$

where b, $c=\pm 1$. And (12) is equivalent to

$$(1-b^3f_1g_1^2)(c^3f_1^2g_1-1)+(bcf_1g_1-1)^2(bcf_1g_1+2)\equiv 0 \mod \mathfrak{p}_1^3 .$$

From (11) we can see $bcf_1g_1-1\equiv bcf_1g_1+2\equiv 0 \mod \mathfrak{p}_1$. Hence (12) is equivalent to

$$\text{(13)} \qquad (1-b^3f_1g_1^2)(c^3f_1^2g_1-1)\equiv 0 \mod \mathfrak{p}_1^3 .$$

Again from (11) we have $0\equiv(bcf_1g_1-1)^3=(bcf_1g_1)^3-3(bcf_1g_1)^2+3(bcf_1g_1)-1$ $\mod \mathfrak{p}_1^3$. Replacing $\mod \mathfrak{p}_1^3$ by $\mod \mathfrak{p}_1^2$ we have $(bcf_1g_1)^3\equiv 1 \mod \mathfrak{p}_1^2$, which says that $b^3f_1g_1^2\equiv 1 \mod \mathfrak{p}_1^2$ iff $c^3f_1^2g_1\equiv 1 \mod \mathfrak{p}_1^2$. Hence we have

$$\text{(14)} \qquad b^3f_1g_1^2\equiv 1 \mod \mathfrak{p}_1^2 , \qquad c^3f_1^2g_1\equiv 1 \mod \mathfrak{p}_1^2 ,$$

which is equivalent to (11) and (13). The assumption f_1, $g_1\not\equiv -1 \mod \mathfrak{p}_1$ says that $f_1g_1^2\equiv f_1^2g_1\equiv 1 \mod \mathfrak{p}_1$ and $b^3\equiv c^3\equiv 1 \mod \mathfrak{p}_1$. Thus we have $b=c=1$, $f_1g_1^2\equiv 1$, $f_1^2g_1\equiv 1 \mod \mathfrak{p}_1^2$.

As $(O_k/\mathfrak{p}_1^2)^*$ is an abelian group of order 6, it is cyclic. Let $\sigma \mod \mathfrak{p}_1^2$ be a generator, we can express $f_1\equiv\sigma^{\bar{f}_1}$, $g_1\equiv\sigma^{\bar{g}_1} \mod \mathfrak{p}_1^2$ with integers $\bar{f}_1$, $\bar{g}_1$ such that $0\leqq\bar{f}_1$, $\bar{g}_1<6$ and (14) is equivalent to

$$\text{(14)}' \qquad \bar{f}_1+2\bar{g}_1\equiv 0 \mod 6 , \qquad 2\bar{f}_1+\bar{g}_1\equiv 0 \mod 6 .$$

We can easily verify that (14)′ is equivalent to $\bar{f}_1\equiv\bar{g}_1 \mod 6$ under the assumption f_1, $g_1\not\equiv -1 \mod \mathfrak{p}_1$. Thus $\omega_1=(1+\theta_1+\bar{\theta}_1)/\pi_1$ is in O_K iff $f_1\equiv g_1$ $\mod \mathfrak{p}_1^2$.

Case (II-2). Similarly as in (II-1), we have that $\omega_2=(1+\theta_2+\bar{\theta}_2)/\pi_2$ is in O_K iff $f_2\equiv g_2 \bmod \mathfrak{p}_2^2$.

Case (II-3). Let $\omega=(a+b\theta+c\bar{\theta})/3$ be an element in O_K satisfying the condition of (II-3). We may have $\omega_1=\pi_2\omega$, $\omega_2=\pi_1\omega$ satisfying the condition of (II-1), (II-2) respectively. Hence $f_1\equiv g_1 \bmod \mathfrak{p}_1^2$, $f_2\equiv g_2 \bmod \mathfrak{p}_2^2$ hold and $\omega_1=(1+\theta_1+\bar{\theta}_1)/\pi_1$, $\omega_2=(1+\theta_2+\bar{\theta}_2)/\pi_2$. Conversely for any x, y in O_k

$$\begin{aligned} x\omega_1+y\omega_2 &= \frac{1}{\pi_1\pi_2}\{(x\pi_2+y\pi_1)+(x\pi_2\theta_1+y\pi_1\theta_2)+(x\pi_2\bar{\theta}_1+y\pi_1\bar{\theta}_2)\} \\ &= \frac{1}{3}\{\varepsilon(x\pi_2+y\pi_1)+\varepsilon(\pm x\pi_2\pm y\pi_1)\theta+\varepsilon(\pm x\pi_2\pm y\pi_1)\bar{\theta}\} \end{aligned}$$

where ε is the unit in O_k such that $3=\varepsilon\pi_1\pi_2$. As $\mathfrak{p}_1$, $\mathfrak{p}_2$ are relatively prime, we may choose x, y so that the coefficient of $\bar{\theta}$ in the numerator of the above formula is one. For such x, y put $\omega=x\omega_1+y\omega_2=(a+b\theta+\bar{\theta})/3$. We will show that $\{1, \theta, \omega\}$ is a basis of O_K as O_k-module. For any $\omega'=(a'+b'\theta+c'\bar{\theta})/3$ in O_K,

$$\omega'-c'\omega=\frac{1}{3}\{(a'-c'a)+(b'-c'b)\theta\} .$$

From the lemma both $(a'-c'a)$ and $(b'-c'b)$ must be divisible by $\mathfrak{p}_1$, $\mathfrak{p}_2$. So they are divisible by (3). Then

$$\begin{aligned} \omega'-c'\omega &= s+t\theta , \\ \omega' &= s+t\theta+c'\omega , \end{aligned}$$

where $s=(a'-c'a)/3$, $t=(b'-c'b)/3$ in O_k. Thus we have proved the following theorem.

THEOREM II. *Let* $k=\boldsymbol{Q}(\sqrt{m})$ *with* $m\equiv 1 \bmod 3$, $K=(\sqrt[3]{A})$ *with an integer* A *of* k. *We assume that* H1 *and* H2 *hold and* $f_i\not\equiv -1 \bmod \mathfrak{p}_i$, $g_i\not\equiv -1 \bmod \mathfrak{p}_i$ $(i=1, 2)$. *Put* $\theta_i=\sqrt[3]{f_i g_i^2}$, $\bar{\theta}_i=\theta_i^2/g_i$ $(\pi_i)=\mathfrak{p}_i$ $(i=1, 2)$. *Then a basis of* O_K *as* O_k*-module and the relative discriminant* $d(K/k)$ *are given as follows*:

(a) *When* $f_1\not\equiv g_1 \bmod \mathfrak{p}_1^2$, $f_2\not\equiv g_2 \bmod \mathfrak{p}_2^2$, *then* $\{1, \theta, \bar{\theta}\}$ *is a basis and* $d(K/k)=(3^3 f^2 g^2)$.

(b) *When* $f_i\equiv g_i \bmod \mathfrak{p}_i^2$, $f_j\not\equiv g_j \bmod \mathfrak{p}_j^2$ $(i, j=1, 2, i\neq j)$, *then* $\{1, \theta, \omega_i\}$ *is a basis and* $d(K/k)=\mathfrak{p}_i\mathfrak{p}_j^3(f^2g^2)$.

(c) *When* $f_1\equiv g_1 \bmod \mathfrak{p}_1^2$, $f_2\equiv g_2 \bmod \mathfrak{p}_2^2$, *then* $\{1, \theta, \omega\}$ *is a basis and* $d(K/k)=(3f^2g^2)$.

(*Here* $\omega_i=(1+\theta_i+\bar{\theta}_i)/\pi_i$ $(i=1, 2)$, $\omega=x\omega_1+y\omega_2$ *with* x, y *in* O_k *such that the coefficient of* $\bar{\theta}$ *in* 3ω *is one.*)

§4. *Case* (III). From the lemma, we may only consider the case that none of (a), (b), (c) is divisible by (3) and in this case we may assume $a=1$, since $a \bmod(3)$ has the inverse in O_k. Thus (1) is equivalent to

$$bcfg \equiv 1 \mod(3) , \tag{15}$$

and (2) is equivalent to

$$(1-b^3fg^2)(c^3f^2g-1)+(bcfg-1)^2(bcfg+2)\equiv 0 \mod(3)^3 .$$

Applying (15) to $(bcfg-1)^2(bcfg+2)$

$$(1-b^3fg^2)(c^3f^2g-1)\equiv 0 \mod(3)^3 . \tag{16}$$

From (15) we also have

$$(bcfg)^3 \equiv 1 \mod(3)^2 ,$$

which says $b^3fg^3\equiv 1 \mod(3)^2$ iff $c^3f^2g\equiv 1 \mod(3)^2$. From (16), b^3fg^2-1 or c^3f^2g-1 is divisible by $(3)^2$. Hence (16) is equivalent to

$$b^3fg^2\equiv 1 \mod(3)^2 , \qquad c^3f^2g\equiv 1 \mod(3)^2 . \tag{17}$$

In (17) we may consider f, $g \bmod(3)^2$ and b, $c \bmod(3)$. Now put $m=-1+3l$, $\sigma=1+\sqrt{m}$ and $\tau=1+3\sigma$. Then $(O_k/(3))^*$ is the cyclic group of order 8 generated by $\sigma \bmod(3)$ and $(O_k/(3)^2)^*$ is the direct product of the cyclic group of order 24 generated by $\sigma \bmod(3)^2$ and the cyclic group of order 3 generated by $\tau \bmod(3)^2$ (see Table 3, 4). Hence we may put $b=\sigma^{\bar b}$, $c=\sigma^{\bar c}$, $f=\sigma^{\bar f}\tau^{\bar f'}$, $g=\sigma^{\bar g}\tau^{\bar g'}$ with integers $\bar b$, $\bar c$, $\bar f$, $\bar g$, $\bar f'$, $\bar g'$ such that $0\leqq \bar b$, $\bar c<8$, $0\leqq \bar f$, $\bar g<24$, $0\leqq \bar f'$, $\bar g'<3$, and (15) and (17) are equivalent to the following (15)$'$ and (17)$'$:

$$\bar b+\bar c+\bar f+\bar g\equiv 0 \qquad \bmod 8 , \tag{15$'$}$$

$$3\bar b+\bar f+2\bar g\equiv 3\bar c+2\bar f+\bar g\equiv 0 \mod 24 , \qquad \bar f'=\bar g' . \tag{17$'$}$$

Since (17)$'$ induces (15)$'$, the necessary and sufficient condition for the existence of an integer $\omega=(1+a\theta+c\bar\theta)/3$ in O_K is that there exist $\bar b$ and $\bar c$, satisfying (17)$'$, which is equivalent to $\bar f\equiv\bar g \bmod 3$. Turning to f, g, $\bar f\equiv \bar g \bmod 3$, $\bar f'\equiv\bar g' \bmod 3$, for $f\equiv\sigma^{\bar f}\tau^{\bar f'} \bmod(3)^2$, $g\equiv\sigma^{\bar g}\tau^{\bar g'} \bmod(3)^2$ is equivalent to $fg^{-1}\equiv\sigma^{3\bar h} \bmod(3)^2$ for some integer $\bar h$. In this case we may choose b, c so that $b^3fg^2\equiv 1 \bmod(3)^2$, $c^3f^2g\equiv 1 \bmod(3)^2$. Let h be in O_k such that $h\equiv\sigma^{\bar h} \bmod(3)^2$, then $h^3\equiv\sigma^{3\bar h}\equiv fg^{-1} \bmod(3)^2$. Put b, c in O_k such that $b\equiv h^{-1}g^{-1}$, $c\equiv hf^{-1} \bmod(3)$. Then $b^3\equiv h^{-3}g^{-3}\equiv (fg^{-1})^{-1}g^{-3}\equiv f^{-1}g^{-2}$, $c^3\equiv h^3f^{-3}\equiv (fg^{-1})f^{-3}\equiv f^{-2}g^{-1} \bmod(3)^2$ and $(1+b\theta+c\bar\theta)/3$ is in O_K. For any c in O_k, c^*

always denotes an element in O_k such that $c^*c\equiv 1 \bmod (3)$. Since $(1+b\theta+c\bar{\theta})/3$ is in O_K iff $(c^*+c^*b\theta+\bar{\theta})/3$ is in O_K. In this case,

$$\frac{h^*f+(h^*f)h^*g^*\theta+\bar{\theta}}{3}=\frac{h^*f+h^{*2}fg^*\theta+\bar{\theta}}{3}$$

is in O_K, and $fg^*\equiv h^3 \bmod (3)$ says $(h^*f+h\theta+\bar{\theta})/3$ is also in O_K. Now what we have to do is to show that $\{1, \theta, (h^*f+h\theta+\bar{\theta})/3\}$ is a basis. For any $\omega=(a+b\theta+c\bar{\theta})/3$ in O_K, $\omega-c(h^*f+h\theta+\bar{\theta})/3=\{(a-ch^*f)+(b-ch)\theta\}/3$ is in O_K. From the lemma, this implies that both $a-ch^*f$ and $b-ch$ are divisible by 3 and $\omega-c(h^*f+h\theta+\bar{\theta})/3$ is in $O_k\oplus O_k\theta$. Thus we have proved the following theorem.

THEOREM III. *Let $k=Q(\sqrt{m})$ with $m\equiv -1 \bmod 3$, $K=k(\sqrt[3]{A})$ with an integer A of k. We assume that* H2 *holds. Put $\sigma=1+\sqrt{m}$, $\tau=1+3\sigma$. Then any element of $(O_k/(3)^2)^*$ is uniquely expressed in the form $\sigma^x\tau^y$ with integers x, y such that $0\leqq x<24$, $0\leqq y<3$, and a basis of O_K as O_k-module and the relative discriminant $d(K/k)$ are given as follows*:

(a) *When $fg^{-1}\not\equiv\sigma^{3\bar{h}} \bmod (3)^2$ for any integer $\bar{h}$, then $\{1, \theta, \bar{\theta}\}$ is a basis and $d(K/k)=(3^3f^2g^2)$.*

(b) *When $fg^{-1}\equiv\sigma^{3\bar{h}} \bmod (3)^2$ for some integer $\bar{h}$, then $\{1, \theta, (h^*f+h\theta+\bar{\theta})/3\}$ is a basis and $d(K/k)=(3f^2g^2)$.*

(Here h, h^* are elements of O_k satisfying $h\equiv\sigma^{\bar{h}} \bmod (3)$, $h^*\equiv\sigma^{-\bar{h}}$ $\bmod (3)$.)

TABLE 3.

$\sigma=1+\sqrt{m}$, $\#|(O_k/(3))^*|=N3\left(1-\frac{1}{N3}\right)=8$

s	1	2	3	4
$\sigma^s \bmod (3)$	$1+\sqrt{m}$	$-\sqrt{m}$	$1-\sqrt{m}$	-1

TABLE 4.

$\sigma=1+\sqrt{m}$, $\tau=1+3\sigma$, $m=-1+3l$,

$\#|(O_k/(3))^*|=N3^2\left(1-\frac{1}{N3}\right)=8\cdot 9=3\cdot 24$,

s	1	2
$\sigma^s \bmod (3)^2$	$1+\sqrt{m}$	$-\sqrt{m}+3(l+\sqrt{m})$

3	4	5
$1-\sqrt{m}+3\{-1+(1+l)\sqrt{m}\}$	$-1+3\{(-1+l)+l\sqrt{m}\}$	$-1-\sqrt{m}-3\{1+(1+l)\sqrt{m}\}$

6	7	8
$\sqrt{m}-3l\sqrt{m}$	$-1+\sqrt{m}-3l(1+\sqrt{m})$	$1+3\{(-1+l)+l\sqrt{m}\}$

9	10	11
$1+\sqrt{m}-3\{1+(1+l)\sqrt{m}\}$	$-\sqrt{m}-3\{l+(1+l)\sqrt{m}\}$	$1-\sqrt{m}+3(1-l)(1-\sqrt{m})$

12
-1

$\sigma^s\equiv 1 \bmod (3)$ $(s\neq 0)$ iff $s=8$ or 16
When $l\equiv 0 \bmod 3$, then $\sigma^3\equiv 1-3$, $\sigma^{16}\equiv 1+3 \bmod (3)^2$.
When $l\equiv 1 \bmod 3$, then $\sigma^3\equiv 1+3\sqrt{m}$, $\sigma^{16}\equiv 1-3\sqrt{m} \bmod (3)^2$.
When $l\equiv -1 \bmod 3$, then $\sigma^3\equiv 1+3(1-\sqrt{m})$, $\sigma^{16}\equiv 1-3(1-\sqrt{m}) \bmod (3)^2$.

t	1	2	3
$\tau^t \bmod (3)^2$	$1+3\sigma$	$1-3\sigma$	1

Reference

[1] H. WADA, On Cubic Galois Extensions of $\boldsymbol{Q}(\sqrt{-3})$, Proc. Japan Acad., **46** (1970), 397-399.

Present Address:
DEPARTMENT OF MATHEMATICS
SOPHIA UNIVERSITY
KIOI-CHO, CHIYODA-KU, TOKYO 102