Math. J. Okayama Univ. 26 (1984), 27−41

ON INTEGRAL BASES OF PURE QUARTIC FIELDS

TAKEO FUNAKURA

0. The aim of the paper is to report some topics related to integral bases of pure quartic fields. In Section 1, we shall give their explicit bases which Ljunggren [11] stated without proof in the case of "real" fields. Wada [18] made a method of computation of integral bases of any biquadratic field, but we shall give a direct and simple proof of Theorem 1. In Section 2, we shall study a relative integral bases over the quadratic subfield. In Section 3, we shall study common inessential discriminant divisors and power integral bases. The results of Theorems 4 and 6 are analogous to Hall [9] and Dummit-Kislowsky [4]. We shall prove Theorem 5 without depending on Engstrom [5]. Finally we shall determine all power integral bases in terms of solvability of some diophantine equations.

Let β_m be the root of an irreducible polynomial $X^4 - m$ $(m \in \mathbf{Z})$ over $\mathbf{Q}$ such that

$$\arg \beta_m = \begin{cases} 0 & \text{if } m \text{ is positive,} \\ \pi/4 & \text{if } m \text{ is negative.} \end{cases}$$

Then $\mathbf{Q}(\beta_m)$ is called a *pure quartic field*. Now it is sufficient without loss of generality to treat only of the form $m = ab^2c^3$, where (i) $a \neq 1$, b and c are square free and pairwise prime; (ii) b and c are positive; (iii) $|a| \geqq c$ if a is odd; (iv) c is odd; (v) $m \neq -4$. We set

$$\alpha = \beta_m{}^2/bc, \quad \beta = \beta_m, \quad \gamma = \beta_m{}^3/bc^2$$
$$E = \mathbf{Q}(\alpha), \quad F = \mathbf{Q}(\beta) = \mathbf{Q}(\gamma).$$

Throughout the paper, we assume the above conditions and use these notations.

1. First of all, we prove

Theorem 1. *The numbers* 1, λ, μ, ν *given by the following table form an integral basis of a pure quartic field* F *with* m.

m	1	λ	μ	ν
$1 \pmod 8$	1	$\frac{1+\alpha}{2}$	β	$\frac{ab+\alpha+b\beta+\gamma}{4}$
$2 \pmod 4$ $3 \pmod 4$	1	α	β	γ
$4 \pmod{16}$ $5 \pmod 8$	1	$\frac{1+\alpha}{2}$	β	$\frac{\beta+\gamma}{2}$
$12 \pmod{32}$	1	α	$\frac{1+\alpha+\beta}{2}$	$\frac{\beta+\gamma}{2}$
$28 \pmod{32}$	1	α	$\frac{1+\alpha+\beta}{2}$	$\frac{4\alpha+b\beta+2\gamma}{8}$

(The table contains all cases since m is not divisible by 8.)

Proof. By the general theory, an integral basis of F is given by integers 1, λ, μ, ν in F of the type

$$\begin{aligned}\lambda &= x_1+x_2\alpha \\ \mu &= y_1+y_2\alpha+y_3\beta \qquad (x_i, y_i, z_i \in \mathbf{Q}) \\ \nu &= z_1+z_2\alpha+z_3\beta+z_4\gamma,\end{aligned}$$

such that x_2, y_3, z_4 are the smallest positive rational numbers as possible. Since 1, λ form an integral basis of the quadratic field E, it is obvious that λ is taken as in the table. In order to determine μ and ν, we need several lemmas.

Lemma 1. *Let K/k be a quadratic extension of number fields. Then α is an integer in K if and only if both* $\mathrm{Norm}_{K/k}\alpha$ *and* $\mathrm{Trace}_{K/k}\alpha$ *are integers in k.*

Lemma 2. *Let $d \neq 1$ be a square free rational integer. A quadratic residue system modulo 4 of integers in $\mathbf{Q}(\sqrt{d})$ is given by*

$$\begin{array}{lllll} 0, & 1, & \frac{d+1+2\sqrt{d}}{4}, & \frac{d+9+6\sqrt{d}}{4} & \text{if } d \equiv 1 \pmod 4 \\ 0, & 1, & 2, & 3+2\sqrt{d} & \text{if } d \equiv 2 \pmod 4 \\ 0, & 1, & 3, & 2\sqrt{d} & \text{if } d \equiv 3 \pmod 4). \end{array}$$

The proofs of Lemmas 1 and 2 are straightforward and omitted.

Lemma 3. *A number $s\beta+t\gamma$ $(s, t \in \mathbf{Q})$ is an integer in F if and only if*

(i) $s, t \in \mathbf{Z}$ *if* $m \equiv 2, 3 (\mathrm{mod}\ 4)$,

(ii) $s_0 = 2s$, $t_0 = 2t \in \mathbf{Z}$, *and* $s_0 \equiv t_0 (\mathrm{mod}\ 2)$ *otherwise.*

Proof. A number $s\beta+t\gamma$ is an integer in F if and only if $(s\beta+t\gamma)^2$ is an integer in E, because its Trace and Norm for F/E are 0 and $-(s\beta+t\gamma)^2$ respectively. Since both

$$(s\beta+t\gamma)\beta = abct+bcs\alpha \quad \text{and} \quad (s\beta+t\gamma)\gamma = abcs+abt\alpha$$

are integers in F and so are in E, we can put

$$s = u/2bc, \quad t = v/2ab \qquad (u, v \in \mathbf{Z}).$$

Thus we have

$$(s\beta+\mathrm{t}\gamma)^2 = \frac{uv}{2b}+\frac{au^2+cv^2}{4abc}\alpha$$

and so $b|uv$ and $abc|(au^2+cv^2)$. By the assumption on a, b and c, we get $a|v$, $b|v$, $b|u$ and $c|u$, so that u/bc and v/ab are rational integers. Therefore we can put $s = s_0/2$, $t = t_0/2$ $(s_0, t_0 \in \mathbf{Z})$. Since $\beta/2$ and $\gamma/2$ are not integers, it holds $s_0 \equiv t_0 (\mathrm{mod}\ 2)$. Furthermore supposing $s_0 \equiv t_0 \equiv 1 (\mathrm{mod}\ 2)$, we easily see that $(s\beta+t\gamma)^2$ is an integer in E if and only if $b \equiv 0 (\mathrm{mod}\ 2)$ or $ac \equiv 1 (\mathrm{mod}\ 4)$. Thus the lemma is proved.

Using these lemmas, we shall determine μ and ν. Since $2y_3\beta = 2\mu-\mathrm{Trace}_{F/E}\,\mu$ is an integer in F, we have $y_3 = 1/2$ or 1 from Lemma 3. Supposing $y_3 = 1/2$, we see that

$$\mathrm{Norm}_{F/E}\mu = (y_1+y_2\alpha)^2-\beta^2/4$$

is an integer in E. Thus we obtain

$$(\mathrm{Trace}_{F/E}\,\mu)^2 = (2y_1+2y_2\alpha)^2 \equiv bc\alpha (\mathrm{mod}\ 4).$$

By Lemma 2, we must have

$$b \equiv 0 (\mathrm{mod}\ 2) \text{ and } ac \equiv 3 (\mathrm{mod}\ 4).$$

Conversely if $m \equiv 12 (\mathrm{mod}\ 16)$, then it holds

$$(1+\alpha)^2 \equiv bc\alpha (\mathrm{mod}\ 4).$$

Accordingly we can take as μ, $(1+\alpha+\beta)/2$ if $m\equiv 12(\mathrm{mod}\ 16)$, β if otherwise. Similarly we can determine ν. Since $2z_3\beta+2z_4\gamma=2\nu-\mathrm{Trace}_{F/E}\nu$ is an integer, we have $(z_3, z_4)=((2l+1)/4, 1/4)$, $(l/2, 1/2)$, or $(l/2, 1)$ for some $l\in\mathbf{Z}$. $\mathrm{Norm}_{F/E}\nu$ is an integer in E if and only if the congruence

$$(*)\qquad (2z_1+2z_2\alpha)^2\equiv(2z_3\beta+2z_4\gamma)^2\ (\mathrm{mod}\ 4)$$

holds. Suppose now that $(z_3, z_4)=((2l+1)/4, 1/4)$ and $m\not\equiv 2, 3(\mathrm{mod}\ 4)$. $\mathrm{Norm}_{E/\mathbf{Q}}$ of the right side of $(*)$ is equal to $-ab^2c\{(a-c)/4-cl(l+1)\}^2$, which has to be a quadratic residue modulo 8 in $\mathbf{Z}$. Therefore

(i) $ac\equiv 1(\mathrm{mod}\ 8)$, $b\equiv 1(\mathrm{mod}\ 2)$, i.e., $m\equiv 1(\mathrm{mod}\ 8)$,

(ii) $ac\equiv 7(\mathrm{mod}\ 8)$, $b\equiv 0(\mathrm{mod}\ 2)$, i.e., $m\equiv 28(\mathrm{mod}\ 32)$,

or (iii) $ac\equiv 1(\mathrm{mod}\ 4)$, $b\equiv 0(\mathrm{mod}\ 2)$, i.e., $m\equiv 4(\mathrm{mod}\ 16)$.

Hence if $m\equiv 1(\mathrm{mod}\ 8)$ or $28(\mathrm{mod}\ 32)$, then it is sufficient to show that $\mathrm{Norm}_{F/E}$ of ν given by the table is an integer in E. It is immediate, for if $m\equiv 1(\mathrm{mod}\ 8)$ then

$$\mathrm{Norm}_{F/E}\left(\frac{ab+\alpha+b\beta+\gamma}{4}\right)=\frac{1}{2}\left\{ab^2\left(\frac{a-c}{8}\right)+ac\left(\frac{1-b^2}{8}\right)+b\left(\frac{a-b^2c}{8}\right)\alpha\right\},$$

and if $m\equiv 28(\mathrm{mod}\ 32)$ then

$$\mathrm{Norm}_{F/E}\left(\frac{4\alpha+b\beta+2\gamma}{8}\right)=ac\left(\frac{1-(b/2)^2}{4}\right)-(b/2)\left(\frac{a+(b/2)^2c}{8}\right)\alpha.$$

Lemma 2 implies that if $m\equiv 4(\mathrm{mod}\ 16)$ then the right side of $(*)$, $\dfrac{abc(2l+1)}{2}+\dfrac{ab+bc(2l+1)^2}{4}\alpha$, is not a quadratic residue modulo 4. Therefore if neither $m\equiv 1(\mathrm{mod}\ 8)$ nor $\mathrm{m}\equiv 28(\mathrm{mod}\ 32)$, then the denominator of z_3 is 1 or 2. Furthermore if $\mathrm{m}\equiv 4(\mathrm{mod}\ 16)$, $5(\mathrm{mod}\ 8)$, or $12(\mathrm{mod}\ 32)$, then by Lemma 3, a number $(\beta+\gamma)/2$ is an integer in F, so that we can take it as ν. Finally substituting $(z_3, z_4)=(l/2, 1/2)$ for the right side of $(*)$, we obtain $2abc+(ab+bcl^2)\alpha$ which is not a quadratic residue modulo 4 if $m\equiv$ 2 or|3(mod 4). Then we may take γ as ν. Hence the proof is completed.

Corollary 1. *The discriminant $d(F)$ of F is*

$$d(F)=\begin{cases}-2^2a^3b^2c^3 & \text{if } m\equiv 1(\mathrm{mod}\ 8),\ 28(\mathrm{mod}\ 32),\\ -2^4a^3b^2c^3 & \text{if } m\equiv 4(\mathrm{mod}\ 16),\ 5(\mathrm{mod}\ 8),\ 12(\mathrm{mod}\ 32),\\ -2^8a^3b^2c^3 & \text{if } m\equiv 2(\mathrm{mod}\ 4),\ 3(\mathrm{mod}\ 4).\end{cases}$$

Proof. This is immediate from Theorem 1.

Lemma 4. *A pure quartic field F with $m = ab^2c^3$ is Galois over $\mathbf{Q}$ if and only if $ac = -1$, that is, $m = -b^2$, in which case $F = \mathbf{Q}(\sqrt{-1}, \sqrt{2b})$.*

Proof. Suppose that $F/\mathbf{Q}$ is Galois and $ac \neq -1$. Since $\sqrt{-1}\,\beta$ is conjugate to β, we have $\sqrt{-1} \in F$. On the other hand, the assumption $ac \neq -1$ yields $\sqrt{-1} \notin E$. Therefore $F = E(\sqrt{-1})$, which implies $\beta \in \mathbf{Q}(\sqrt{-1}, \alpha)$, that is,

$$\beta = a_0 + a_1\sqrt{-1} + a_2\alpha + a_3\sqrt{-1}\,\alpha \quad (a_i \in \mathbf{Q})$$

and so

$$bc\alpha = \beta^2 = (a_0 + a_2\alpha)^2 - (a_1 + a_3\alpha)^2 + 2(a_0 + a_2\alpha)(a_1 + a_3\alpha)\sqrt{-1}.$$

Thus we get either $a_0 + a_2\alpha = 0$ or $a_1 + a_3\alpha = 0$. In the former case, we have $bc\alpha = -(a_1 + a_3\alpha)^2$, so that $a_1{}^2 + a_3{}^2ac = 0$, giving $ac = -1$ as ac is square free. In the latter case, we have $\beta = a_0 + a_2\alpha \in E$. A contradiction arises in either case. Hence if $F/\mathbf{Q}$ is Galois, then $ac = -1$. The converse is obvious.

As to a generalization of Lemma 4, see [8].

Corollary 2. *Let $n \geqq 2$ be a square free rational integer. An integral basis of $\mathbf{Q}(\sqrt{-1}, \sqrt{n})$ is given by*

$$1,\ \sqrt{-1},\ \frac{1+\sqrt{n}}{2},\ \frac{\sqrt{-1}+\sqrt{-n}}{2} \quad \textit{if} \quad n \equiv 1 (\mathrm{mod}\ 4)\ ;$$
$$1,\ \sqrt{-1},\ \frac{\sqrt{n}+\sqrt{-n}}{2},\ \frac{\sqrt{n}-\sqrt{-n}}{2} \quad \textit{if} \quad n \equiv 2 (\mathrm{mod}\ 4)\ ;$$
$$1,\ \sqrt{-1},\ \frac{1+\sqrt{-n}}{2},\ \frac{\sqrt{-1}+\sqrt{n}}{2} \quad \textit{if} \quad n \equiv 3 (\mathrm{mod}\ 4)\ .$$

Proof. We take $b = n/2$ when n is even. As b is odd, we have $m = -b^2 \equiv 3(\mathrm{mod}\ 4)$, and so by Theorem 1,

$$1,\ \lambda = \alpha = \sqrt{-1},\ \mu = \beta = \frac{1+\sqrt{-1}}{\sqrt{2}}\sqrt{b} = \frac{\sqrt{n}+\sqrt{-n}}{2},$$
$$\nu = \gamma = \frac{-1+\sqrt{-1}}{\sqrt{2}}\sqrt{b} = \frac{-\sqrt{n}+\sqrt{-n}}{2}$$

form an integral basis of $F = \mathbf{Q}(\sqrt{-1}, \sqrt{n})$. Next we take $b = 2n$ when n is odd. Then $m = -b^2 \equiv 28(\mathrm{mod}\ 32)$, and

$$1,\quad \lambda=\alpha=\sqrt{-1},\quad \mu=\frac{1+\alpha+\beta}{2}=\frac{1+\sqrt{-1}+\sqrt{n}+\sqrt{-n}}{2},$$
$$\nu-\frac{b-2(-1)^{(b-2)/4}}{8}\beta=\frac{2\alpha+(-1)^{(b-2)/4}\beta+\gamma}{4}$$
$$=\frac{1}{2}\left\{\sqrt{-1}-\frac{1-(-1)^{(n-1)/2}}{2}\sqrt{n}+\frac{1+(-1)^{(n-1)/2}}{2}\sqrt{-n}\right\}$$

form an integral basis of $F=\mathbf{Q}(\sqrt{-1},\sqrt{n})$. The rest is simple arithmetic.

As to any bicyclic biquadratic field, see Brid-Parry [2], Fujisaki [6], [7], Nakahara [15], [16], and Williams [19], since in this paper we treat only pure quartic Galois fields $\mathbf{Q}(\sqrt{-1},\sqrt{n})$.

2. We shall consider a relative integral basis of a pure quartic field F over the subfield E. For any ω_1, $\omega_2\in F$, their discriminant over E coincides with that of 1, $\omega_1'\omega_2$, where ω_1' is conjugate to ω_1 over E. Hence if there exists a relative integral basis then we may take $\omega_1=1$, $\omega_2=\xi$. Numbers 1, ξ form an integral basis of F over E if and only if 1, λ, ξ, $\lambda\xi$ form an integral basis of F over $\mathbf{Q}$. Let $f(x)$ be the minimal polynomial of ξ over E and let $d(E)$ be the discriminant of E. The discriminant of 1, λ, ξ, $\lambda\xi$ is equal to

$$d(E)^2\mathrm{Norm}_{E/\mathbf{Q}}f'(\xi)^2.$$

Thus 1, ξ form a relative integral basis if and only if it holds

$$\mathrm{Norm}_{E/\mathbf{Q}}f'(\xi)^2=-2^x ab^2c,$$

where $x=-2$ if $m\equiv 28 \pmod{32}$; $x=0$ if $m\equiv 12 \pmod{32}$; $x=2$ if $m\equiv 1 \pmod 8$; $x=4$ if otherwise. On the other hand, we set

$$\begin{aligned}\xi&=x+y\lambda+z\mu+w\nu && (x,y,z,w\in\mathbf{Z})\\ &=x'+y'\alpha+z'\beta+w'\gamma && (x',y',z',w'\in\mathbf{Q})\end{aligned}$$

and then we have

$$\mathrm{Norm}_{E/\mathbf{Q}}f'(\xi)^2=-2^4ab^2c(cz'^2-aw'^2)^2,$$

which implies

$$\begin{aligned}&c(4z+bw)^2-aw^2=\pm 8 && \text{if } m\equiv 1 \pmod 8),\\ &cz^2-aw^2=\pm 1 && \text{if } m\equiv 2,\ 3 \pmod 4),\\ &c(2z+w)^2-aw^2=\pm 4 && \text{if } m\equiv 4 \pmod{16},\ 5 \pmod 8),\end{aligned}$$

$$c(z+w)^2-aw^2 = \pm 1 \qquad \text{if } m\equiv 12(\text{mod } 32),$$
$$c(2z+(b/2)w)^2-aw^2 = \pm 2 \qquad \text{if } m\equiv 28(\text{mod } 32).$$

Hence the existence of relative integral bases corresponds with the solvability in Z of the equation

$$|aX^2-cY^2| = e,$$

where $e=1$ if $m\equiv 2, 3(\text{mod } 4)$ or $12(\text{mod } 32)$; $e=2$ if $m\equiv 28(\text{mod } 32)$; $e=4$ if $m\equiv 4(\text{mod } 16)$ or $5(\text{mod } 8)$; $e=8$ if $m\equiv 1(\text{mod } 8)$. For, if $m\equiv 1(\text{mod } 8)$ then $aX^2-cY^2 = \pm 8$ implies that either $Y-bX$ or $Y+bX$ is divided by 4 since b is odd, and the rest is obvious.

Theorem 2. *All pure quartic fields which contain a given quadratic field* $\mathrm{Q}(\sqrt{n})$, *where* $n\neq 1$ *is a square free rational integer, have relative integral bases over* $\mathrm{Q}(\sqrt{n})$ *if and only if all prime divisors of* n *are principal ideals in* $\mathrm{Q}(\sqrt{n})$ *and further so are the prime divisors of* 2 *if* $n\not\equiv 3(\text{mod } 8)$.

Proof. In the case of $n\equiv 2(\text{mod } 4)$: Any divisor a of n is a square of some ideal A in $\mathrm{Q}(\sqrt{n})$. If A is principal in $\mathrm{Q}(\sqrt{n})$, then $X^2-nY^2=\pm a$ is solvable, that is, $aX^2-cY^2=\pm 1$ is solvable, where $c=n/a$. Hence $\mathrm{Q}(\sqrt[4]{ab^2c^3})$ for any square free b has relative integral bases over $\mathrm{Q}(\sqrt{n})$. Conversely since for any rational prime divisor p of n, the field $\mathrm{Q}(\sqrt[4]{p(n/p)^3})$ has relative integral bases over $\mathrm{Q}(\sqrt{n})$, the equation $|X^2-nY^2|=p$ is solvable, so that the prime divisors of p are principal. Therefore this case is completed. The other cases are similar and omitted.

Remark. We can not remove the exception "$n\equiv 3(\text{mod } 8)$" from Theorem 2. For example, in the case of $n=-13$, the divisor $(2,1+\sqrt{-13})$ of 2 is not principal, while $|-13X^2-Y^2|=1$ has a trivial solution, so that every $\mathrm{Q}(\sqrt[4]{-13b^2})$ has relative integral bases over $\mathrm{Q}(\sqrt{-13})$.

We feel an interst in Theorem 2 as compared with the Mann's result in [13], "all quadratic extension fields of a number field have relative integral bases if and only if all its ideals are principal". Theorem 2 asserts that it is impossible to replace the former "all" with "infinitely many" in Mann's result.

In the imaginary case, we have

Theorem 3. *An imaginary pure quartic field F with $m = ab^2c^3$ $(a < 0)$ has no relative integral basis over the quadratic subfield E if and only if either $c \neq 1$ or $m \equiv 1 (\mathrm{mod}\ 8)$, $28 (\mathrm{mod}\ 32)$, except for $(a, c) = (-7, 1)$, $(-5, 3)$, in which case there exists relative integral bases.*

Corollary 3. *Let n be a square free positive integer. Every pure quartic field which contains the subfield $\mathbf{Q}(\sqrt{-n})$ has relative integral bases over $\mathbf{Q}(\sqrt{-n})$ if and only if $n = 1$, 2, 7, or a prime number congruent to 3 or 5 modulo 8.*

3. Finally we shall consider a power integral basis and a common inessential discriminant divisors. Let O_F be the ring of all integers in F. For $\xi \in O_F$, we set $i(\xi) = [O_F : \mathbf{Z}[\xi]]$, which is called the *index of an element* ξ and let $i(F)$ be the greatest common divisor of all finite indices $i(\xi)$. We say that $i(F)$ is *the index of a field F*. The prime divisors of $i(F)$ are called *common inessential discriminant divisors*. An integer ξ satisfying $i(\xi) = 1$, that is, $O_F = \mathbf{Z}[\xi]$, is called a *power integral basis of F*. If there is such a basis, then there is no common inessential discriminant divisor. But after Dedekind we have obtained many examples of number fields which have neither common inessential discriminant divisors nor power integral bases. Let $m(F)$ be the minimal of all finite indices $i(\xi)$ on F. We shall see in Theorem 7 that there also exist infinitely many pure quartic fields F with $m(F) = 1$. By definition, it holds $i(F) \leqq m(F)$. Thus $m(F) = 1$ leads $i(F) = 1$, but the converse does not always hold. We note that there exists a power integral basis if and only if $m(F) = 1$.

Lemma 5. *For any integer*

$$\begin{aligned} \xi &= x + y\lambda + z\mu + w\nu & (x, y, z, w \in \mathbf{Z}) \\ &= x' + y'\alpha + z'\beta + w'\gamma & (x', y', z', w' \in \mathbf{Q}), \end{aligned}$$

the discriminant $d(\xi)$ is equal to

$$-2^8 a^3 b^2 c^3 (aw'^2 - cz'^2)^2 | b^2 (aw'^2 - cz'^2)^2 + 4ac(y'^2 - bz'w')^2 |^2$$

and the index $i(\xi)$ is given by the following table.

m	$i(\xi)$
$1 \pmod 8$	$\left\lvert\dfrac{aw^2-c(4z+bw)^2}{8}\right\rvert$ $\times\left\lvert b^2\left\{\dfrac{aw^2-c(4z+bw)^2}{8}\right\}^2+ac\left\{\dfrac{(2y+w)^2-b(4z+bw)w}{4}\right\}^2\right\rvert$
$2 \pmod 4$ $3 \pmod 4$	$\lvert aw^2-cz^2\rvert\times\lvert b^2(aw^2-cz^2)^2+4ac(y^2-bzw)^2\rvert$
$4 \pmod{16}$ $5 \pmod 8$	$\left\lvert\dfrac{aw^2-c(2z+w)^2}{4}\right\rvert$ $\times\left\lvert 4b^2\left\{\dfrac{aw^2-c(2z+w)^2}{4}\right\}^2+ac\{y^2-b(2z+w)w\}^2\right\rvert$
$12 \pmod{32}$	$\lvert aw^2-c(z+w)^2\rvert$ $\times\left\lvert\dfrac{(b/2)^2\{aw^2-c(z+w)^2\}^2+ac\{(2y+z)^2-b(z+w)w\}^2}{4}\right\rvert$
$28 \pmod{32}$	$\left\lvert\dfrac{aw^2-c(2z+(b/2)w)^2}{2}\right\rvert\times\left\lvert\dfrac{(b/2)^2\{(aw^2-c(2z+(b/2)w)^2)/2\}^2}{16}\right.$ $\left.+\dfrac{ac\{2(2y+z+w)^2-(b/2)(2z+(b/2)w)w\}^2}{16}\right\rvert$

Proof. The lemma follows from the identity $d(\xi)=d(F)i(\xi)^2$.

Lemma 6. *The number $m(F)$ is not less than the following;*

(I) *Real field* ($m=ab^2c^3$, $a>0$)

b^2 *if* $m\equiv 1 \pmod 8$, 2, $3 \pmod 4$,

$4b^2$ *if* $m\equiv 4 \pmod{16}$, $5 \pmod 8$,

$\min\{(4ac+b^2)/16, b^2/2\}$ *if* $m\equiv 12 \pmod{32}$,

$\min\{(4ac+b^2)/64, b^2/8\}$ *if* $m\equiv 28 \pmod{32}$,

(II) *Imaginary field* ($m=ab^2c^3$, $a<0$)

$\min\{(-a+c)/8, -2a, 2c\}$ *if* $m\equiv 1 \pmod 8$,

$\min\{-a, c\}$ *if* $m\equiv 2$, $3 \pmod 4$, $12 \pmod{32}$,

$\min\{(-a+c)/4, -a, c\}$ *if* $m\equiv 4 \pmod{16}$, $5 \pmod 8$,

$\min\{(-a+c)/2, -2a, 2c\}$ *if* $m\equiv 28 \pmod{32}$.

Proof. Considering congruences modulo suitable powers of 2, we see that the insides of $\{\ldots\}$ and $\lvert\ldots\rvert$ in Lemma 5 are rational integers. This yields the lemma.

Theorem 4. *The number $m(F)$ is unbounded as F runs over the set of pure quartic fields.*

Proof. This follows from Lemma 6.

We easily see that 2 and 3 have the following factorizations into prime ideals in F, where f_i and e_i are degrees and ramification indices of prime ideals respectively.

Prime	$[f_1, f_2, f_3]$	$[e_1, e_2, e_3]$	Condition	
2	[1]	[4]	$m \equiv 2,\ 3 (\mathrm{mod}\ 4),\ 12 (\mathrm{mod}\ 32)$	
	[2]	[2]	$m \equiv 5 (\mathrm{mod}\ 8),\ 20 (\mathrm{mod}\ 32)$	
	[1,1]	[2,2]	$m \equiv 4,\ 28 (\mathrm{mod}\ 32)$	
	[2,1]	[1,2]	$m \equiv 9 (\mathrm{mod}\ 16)$	
	[1,1,1]	[1,1,2]	$m \equiv 1 (\mathrm{mod}\ 16)$	
3	[1]	[4]	$3 \mid ac$	
	[2]	[2]	$3 \mid b$,	$ac \equiv 2 (\mathrm{mod}\ 3)$
	[1,1]	[2,2]	$3 \mid b$	$ac \equiv 1 (\mathrm{mod}\ 3)$
	[2,2]	[1,1]	$3 \nmid abc$,	$ac \equiv 2 (\mathrm{mod}\ 3)$
	[1,1,2]	[1,1,1]	$3 \nmid abc$,	$ac \equiv 1 (\mathrm{mod}\ 3)$.

Therefore by referring to Engstrom [5], we obtain

Theorem 5.

$$i(F) = \begin{cases} 2 & \textit{if}\ \ m \equiv 1 (\mathrm{mod}\ 16), \\ 1 & \textit{otherwise}. \end{cases}$$

Alternative Proof of Theorem 5. This is a direct proof without depending on Engstrom [5].

Now the greatest common divisor of

$$i(\beta) = \sqrt{-2^8 a^3 b^6 c^9 / d(F)} \quad \text{and} \quad i(\alpha+\gamma) = \sqrt{-2^8 a^7 b^2 c^3 (ab^2+4c)^2 / d(F)}$$

is 1 or a non-zero power of 2 according as $m \equiv 2,\ 3 (\mathrm{mod}\ 4)$ or $m \equiv 0,\ 1 (\mathrm{mod}\ 4)$. Consequently if $m \equiv 9 (\mathrm{mod}\ 16)$, $4 (\mathrm{mod}\ 16)$, $5 (\mathrm{mod}\ 8)$ or $12 (\mathrm{mod}\ 16)$, then it is sufficient to find an integer with an odd index. In the case of $m \equiv 1 (\mathrm{mod}\ 16)$, we must show that every finite index is even and that there exists an integer ξ such that $i(\xi)$ is not divided by 4. In fact, we can easily check the following integers with odd indices ;

$$\begin{array}{ll} \lambda+\mu & \text{if } m\equiv 4(\text{mod } 16),\ 5(\text{mod } 8), \\ \mu & \text{if } m\equiv 12(\text{mod } 32), \\ \nu & \text{if } m\equiv 9(\text{mod } 16),\ 28(\text{mod } 64), \\ \{-(b+2)\lambda+2b\mu+4\nu\}/4 & \text{if } m\equiv 60(\text{mod } 64). \end{array}$$

In the cace of $m\equiv 1(\text{mod } 16)$, if $\{aw^2-c(4z+bw)^2\}/8$ is odd then both z and w are odd and so $\{(2y+w)^2-b(4z+bw)w\}/4$ is odd. Therefore it follows from Lemma 5 that any $i(\xi)$ is even if $m\equiv 1(\text{mod } 16)$. On the other hand,

$$i(\lambda+\mu) = 2c^2(a+4b^2c)$$

is not divided by 4. Hence the proof is completed.

Theorem 6. *There exist infinitely many pure quartic fields which have neither inessential common discriminant divisors nor power integral bases.*

Proof. This follows from Theorems 4 and 5.

The similar results to Theorem 6 are contained in Hall [9], Nakahara [15], [16], and Dummit-Kislowsky [4].

Theorem 7-a. *A real pure quartic field F with* $m = ab^2c^3$ $(a > 0)$ *has a power integral basis if and only if m satisfies one of the following conditions, where* $X, Y \in \mathbf{Z}$.

Condition	*Power integral basis*
$m\equiv 9(\text{mod } 16)$, $b=1$ $\lvert aX^4-cY^4\rvert = 8$	$\frac{XY-X^2}{2}\lambda+\frac{Y^2-X^2}{4}\mu+X^2\nu$
$m\equiv 2,\ 3(\text{mod } 4)$, $b=1$ $\lvert aX^4-cY^4\rvert = 1$	$XY\lambda+Y^2\mu+X^2\nu$
$m = 3\cdot 2^2$	μ, $\lambda-\mu$
$m = 5\cdot 2^2\cdot 3^3$	$\lambda-\nu$, $\mu-\nu$, ν

Proof. The proof follows from Lemma 6. In the case $m\equiv 1(\text{mod } 8)$, we have $b=1$ and

$$aw^2-c(4z+w)^2 = \pm 8,\quad (2y+w)^2-(4z+w)w = 0.$$

Since $y^2 = w(z-y)$ and $(w, z) = 1$, we obtain $(y, z, w) = \pm(st, st+t^2, s^2)$ and so

$$as^4 - c(2t+s)^4 = \pm 8.$$

In the case $m \equiv 2, 3 \pmod 4$, we have $b = 1$ and

$$aw^2 - cz^2 = \pm 1, \quad y^2 - zw = 0.$$

Similarly we obtain $(y, z, w) = \pm(st, s^2, t^2)$ and so

$$at^4 - cs^4 = \pm 1.$$

In the case $m \equiv 4 \pmod{16}$ or $5 \pmod 8$, there exists no power integral basis as $m(F) \geqq 2$. In the case $m \equiv 12 \pmod{32}$, we have only $a = 3$, $b = 2$, $c = 1$ and

$$3w^2 - (z+w)^2 = -1, \quad (2y+z)^2 - 2(z+w)w = 1.$$

Thus $(y, z, w) = \pm(st, t^2, s^2+st)$ and so

$$3(t^2+2st+2s^2)^2 - (t+2s)^4 = 2.$$

By Ljunggren [12], the equation

$$3X^2 - Y^4 = 2$$

has only the solution $X = Y = 1$ in positive integers. Hence we obtain $(y, z, w) = \pm(0,1,0)$, $\pm(1,-1,0)$. In the case $m \equiv 28 \pmod{32}$, Lemma 5 gives four cases

$$(a, b, c) = (5,2,3),\ (7,2,1),\ (7,6,1),\ (15,2,1),$$

but we easily reject the latter three cases. The first case leads to

$$5w^2 - 3(2z+w)^2 = 2, \quad 2(2y+z+w)^2 - (2z+w)w = 1,$$

which imply $(y, z, w) = \pm(s^2+st, -st, -s^2-st-t^2)$ and so

$$(4s^2+7st+4t^2)^2 - 15(s+t)^4 = 1.$$

Since by Cohn [3],

$$X^2 - 15Y^4 = 1$$

has only the solution $X = 4$, $Y = 1$ in positive integers, we obtain $(y, z, w) = \pm(1,0,-1)$, $\pm(0,1,-1)$, $\pm(0,0,1)$.

Theorem 7-b. *An imaginary pure quartic field F with $m = ab^2c^3$ $(a < 0)$ has a power integral basis if and only if m satisfies one of the following conditions, where $X \in \mathbf{Z}$.*

Condition	*Power integral basis*
$m \equiv 2,\ 3 (\mathrm{mod}\ 4)$ $a \neq -1,\ c = 1,\ b^2+4aX^4 = 1$	$X\lambda+\mu$
$m \equiv 4 (\mathrm{mod}\ 16),\ 5 (\mathrm{mod}\ 8)$ $c = 1,\ 4b^2+aX^4 = 1$	$X\lambda+\mu$
$m \equiv 12 (\mathrm{mod}\ 32)$ $c = 1,\ b^2+4aX^4 = \pm 16$	$\frac{X-1}{2}\mu+\nu$
$m = -7b^2,\ b \equiv 1 (\mathrm{mod}\ 2)$ $9b^2+14(-1)^{(b-1)/2}bX^2-7X^4 = 16$	$\frac{X-1}{2}\lambda-\frac{b-(-1)^{(b-1)/2}}{4}\mu+\nu$
$m = -1$	$\mu,\ \nu$
$m = -3$	$\lambda+\mu,\ \lambda-\mu,\ \mu-\nu,\ \nu$
$m = -2^2 \cdot 3^2$	$2\mu-\nu,\ \lambda-2\mu+\nu,\ \lambda+\mu-\nu,\ \lambda-\mu-\nu$
$m = -2^2 \cdot 5^2$	$\lambda-2\mu+\nu,\ 2\mu-\nu$
$\cdot m = -5 \cdot 3^3$	$\lambda-\nu,\ \nu$
$m = -5 \cdot 31^2 \cdot 3^3$	$\lambda+8\mu-\nu,\ 8\mu-\nu$

Proof. This is similar to that of Theorem 7-a. If $m \equiv 1 (\mathrm{mod}\ 8)$, we have $(a, c) = (-5,\ 3)$, or $(-7, 1)$. In the former case, we get $(z, w) = \pm((b- (-1)^{(b-1)/2})/4, -1)$ and

$$[\{(-1)^{(b-1)/2}b+15(2y+w)^2\}/4]^2-15(2y+w)^4 = 1,$$

which implies $b = 1,\ 31$. In the latter case, the above equation is replaced by

$$9b^2+14(-1)^{(b-1)/2}b(2y+w)^2-7(2y+w)^4 = 16.$$

In the case $m \equiv 2,\ 3 (\mathrm{mod}\ 4)$, we have $c = 1$ $(z, w) = (\pm 1, 0)$ and $4ay^4+b^2 = 1$; further $b = 1,\ c = 1$ and $(y, z, w) = (0, 0, \pm 1)$ if $a = -1$. In the case $m \equiv 4 (\mathrm{mod}\ 16)$ or $5 (\mathrm{mod}\ 8)$, we have $c = 1$, $(z, w) = (\pm 1, 0)$, and $ay^4+4b^2 = 1$; further $c = 1$, $(z, w) = \pm(1, -1)$, $(0, \pm 1)$, and $(b \pm 3y^2)^2 - 12y^4 = 1$ if $a = -3$. By Cohn [3],

$$X^2-12Y^4 = 1$$

has no solution in positive integers, so that $b=1$, $y=0$. In the case $m\equiv 12 \pmod{32}$, we have $c=1$, $(z,w)=(\pm 1,0)$, and $b^2+4a(2y+z)^4 = \pm 16$. In the case $m\equiv 28 \pmod{32}$, we have $a=-1$, $c=1$ and

$$(b/2)^2-\{2(2y+z+w)^2-(b/2)(2z+(b/2)w)w\}^2=\pm 16,$$

which implies $b=6$ or 10, and so y, z, w are determined.

We define two integers ξ, η to be in the same index class if either $\xi-\eta$ or $\xi+\eta$ is a rational integer. If ξ, η are in the same index class, then their discriminants are the same and so their indices are also the same. In paticular, if ξ is a power integral basis, then so is any integer in the index class of ξ. Since we give in Theorem 7 all power integral bases contained in distinct index classes, we obtain

Corollary 4. *The power integral bases of any pure quartic field F are divided into at most four index classes.*

Proof. Ljungrren showed in [11] that $AX^4-BY^4=C$, where A, B, C are positive integers, has at most one solution in positive integers, when $C=1$, 2, 4, 8 (See also Cohn [3].). Hence Theorem 7 yields the corollary.

Corollary 5. *Let $n\geqq 2$ be a square free rational integer. A biquadratic field $\mathrm{Q}(\sqrt{-1},\sqrt{n})$ has a power integral basis if and only if $n=2$, 3, or 5.*

Proof. This follows from Lemma 4 and Theorem 7-b.

Remark. $\mathrm{Q}(\sqrt{-1},\sqrt{2})$ and $\mathrm{Q}(\sqrt{-1},\sqrt{3})$ are the eight and the twelfth cyclotomic fields respectively.

References

[1] M. Arai : On quartic fields having common inessential discriminant divisors, (Japanese), Sugaku 29 (1976), 366−369.

[2] R. H. Brid and C. J. Parry : Integral bases for bicyclic biquadratic fields over quadratic subfields, Pacific J. Math. 66, No. 1, (1976), 29−36.

[3] J. H. E. Cohn : Eight diophantine equations, Proc. London Math. Soc. (3) 16 (1966), 153−166.

[4] D. S. Dummit and H. Kislowsky : Indices in cyclic cubic fields, Number Theory and Algebra, Academic Press, New York (1977), 29−42.

[5] H. T. ENGSTROM : On the common index divisors of an algebraic field, Trans. Amer. Math. Soc. 32 (1930), 223−237.

[6] G. FUJISAKI : Some examples of number fields without relative integral bases, J. Fac. Soc. Univ. of Tokyo 21 (1974), 93−95.

[7] G. FUJISAKI : Note on a paper of E. Artin, Sci. Pap. Coll. Gen. Educ. Univ. of Tokyo 24 (1974), 93−98.

[8] T. FUNAKURA : A note on absolute Galois subfields of pure extension number fields, Bull. Okayama Univ. of Sci. 15 (1979), 5−8.

[9] M. HALL : Indices in cubic fields, Bull. Amer. Math. Soc. 43 (1937), 104−108.

[10] H. HASSE : Number Theory, (English Trans.), Springer-Verlag, Berlin 1981.

[11] W. LJUNGGREN : Eigenschaften der Einheiten reele quadratischer und rein biquadraischer Zahlkörper, Oslo Vid-Akad Skrifter, 1 (1936), No. 12.

[12] W. LJUNGGREN : Ein Satz über die diophantische Gleichung $AX^2-BY^4=C\ (C=1,2,4)$, Tolfte Skandinaviska Mathematikerkongressen i Lund (1953), 188−194.

[13] H. B. MANN : On integral bases, Proc. Amer. Math. Soc. 9 (1958), 167−172.

[14] L. J. MORDELL : Diophantine Equations, Academic Press, London, 1969.

[15] T. NAKAHARA : On a power basis of the integer ring in an abelian biquadratic field, (Japanese), RIMS Kōkyūroku 371 (1979), 31−46.

[16] T. NAKAHARA : On cyclic biquadratic fields related to a problem of Hasse, Monatsh. Math. 94 (1982), 125−132.

[17] W. NARKIEWICZ : Elementary and Analytic Theory of Algebraic Numbers, PWN, Warszawa, 1973.

[18] H. WADA : Integral bases of quadratic extensions over quadratic fields, (Japanese), Sugaku 28 (1976), 257−258.

[19] K. S. WILLIAMS : Integers of biquadratic fields, Canad. Math. Bull. 13 (1970), 519−526.

DEPERTMENT OF GENERAL EDUCATION
OKAYAMA UNIVERSITY OF SCIENCE
1-1 RIDAI-CHO, OKAYAMA 700, JAPAN

(*Received July 20, 1983*)