PACIFIC JOURNAL OF MATHEMATICS
Vol 66, No 1, 1976

INTEGRAL BASES FOR BICYCLIC BIQUADRATIC FIELDS OVER QUADRATIC SUBFIELDS

ROBERT H. BIRD AND CHARLES J. PARRY

Explicit conditions are given for a bicyclic biquadratic number field to have an integral basis over a quadratic subfield.

A classical question of algebraic number theory is, "When does an algebraic number field K have an integral basis over a subfield k?"

A complete and explicit answer to the above question is given here when K is a bicyclic biquadratic number field and k is a quadratic subfield. Moreover, an explicit integral basis is given for K/k whenever one exists. In the cases where k is imaginary or k is real and has a unit of norm -1, the conditions involve only rational congruences. When k is real and the fundamental unit of ϵ has norm $+1$, the conditions sometimes involve ϵ.

1. Notation and preliminary remarks. Throughout this article the following notation shall be used:

Q: field of rational numbers.
Z: rational integers.
m, n: square free integers.
$l=(m,n)>0$, $m=m_1l$, $n=n_1l$ and $d=m_1n_1$.
$K=Q(\sqrt{m},\sqrt{n})$: bicyclic biquadratic field.
$k=Q(\sqrt{m})$.
$\delta_{L/M}$: different of an extension L/M.
$N(\epsilon)$: norm of the unit ϵ.
p, q: odd prime numbers.

An integral basis for K over Q has been determined in **[1, 3, 6]**. Here an integral basis for K over $k=Q(\sqrt{m})$ will be determined whenever it exists. In these considerations the roles of n and d are interchangeable so it will only be necessary to consider seven pairs of congruence classes for (m,n) modulo 4; namely $(1,1)$, $(1,2)$, $(1,3)$, $(2,1)$, $(2,3)$, $(3,1)$ and $(3,2)$.

It follows immediately from **[5]** that K has an integral basis over k if and only if $K=k(D^{\frac{1}{2}})$ where (D) is the discriminant of K over k. Since K is a quadratic extension of k the discriminant is the square of the different δ. In **[3, 6]** the different of K over Q is explicitly determined by:

$$\delta^2_{K/Q} = \begin{cases} (lm_1n_1) \text{ when } (m,n) \equiv (1,1) \pmod 4. \\ (4lm_1n_1) \text{ when exactly one of } m \text{ and } n \text{ is } 1 \pmod 4. \\ (8lm_1n_1) \text{ when } (m,n) \text{ is } (2,3) \text{ or } (3,2) \pmod 4. \end{cases}$$

Since $\delta_{K/Q} = \delta_{K/k} \cdot \delta_{k/Q}$ and $\delta_{k/Q} = (\sqrt{m})$ or $(2\sqrt{m})$ according as $m \equiv 1 \pmod 4$ or not, the following useful result is obtained:

LEMMA I. *The different* $\delta = \delta_{K/k}$ *is determined* (and hence the discriminant) *by*:

$$\delta^2 = \begin{cases} (n_1) \text{ when } n \equiv 1 \pmod 4. \\ (4n_1) \text{ when } m \equiv 1 \text{ and } n \not\equiv 1 \pmod 4. \\ (2n_1) \text{ when } m \not\equiv 1 \text{ and } n \not\equiv 1 \pmod 4. \end{cases}$$

2. Imaginary subfield k. Although some of our results here will also apply to the real case we shall be primarily concerned with the case where k is an imaginary quadratic field. The main result of this section is:

THEOREM I. *If $k = Q(\sqrt{m})$ is an imaginary quadratic field then K has an integral basis over k if and only if one of the following conditions hold*:

(a) *At least one of m or n is* $1 \pmod 4$ *and* $l = 1$ *or* $-m$.

(b) $(m,n) \equiv (2,3) \pmod 4$ *and* $m = -2l$.

(c) $m = -1$.

Furthermore, when an integral basis exists, it can be determined by the following table:

TABLE I

Basis	$(m,n) \pmod 4$	Conditions
$1, (1+\sqrt{n})/2$	$(\ ,1)$	$l = 1$
$1, (\sqrt{m}+\sqrt{d})/2$	$(\ ,1)$	$l = \pm m$
$1, \sqrt{\pm n_1}$	$(1,n)$, $n \not\equiv 1 \pmod 4$	$l = 1$ or $\pm m$
$1, (\sqrt{m}+\sqrt{d})/2$	$(2,3)$	$l = \pm m/2.$
$1, (\sqrt{n}+\sqrt{-n})/2$	$(3,2)$	$m = -1$

The proof will follow from a series of lemmas. First, even when m is positive, it is easily seen that the conditions of Theorem I are sufficient for the existence of an integral basis.

LEMMA II. *Whenever the conditions of any line of Table I are fulfilled, even when m is positive, then K has the stated integral basis over k.*

Proof. In each case it is a simple matter to check that the given basis is a basis of integers with discriminant equal to that given by Lemma I.

Our attention will now be directed to proving that the conditions of Theorem I are necessary for the existence of an integral basis when m is negative.

LEMMA III. *If m is negative and at least one of m or n is* 1 (mod 4) *then an integral basis exists if and only if $l = 1$ or $-m$.*

Proof. From Lemma I and Mann's criteria the existence of an integral basis is seen to be equivalent to the condition

$$K = k(\sqrt{\epsilon n_1})$$

where ϵ is a unit of k. When $m \neq -1$ or -3 the only units of k are ± 1 so the above condition implies that $Q(\sqrt{\pm n_1})$ is a quadratic subfield of K. Thus $n_1 = n = ln_1$ or $-n_1 = d = m_1 n_1$, so either $l = 1$ or $l = -m$. If $m = -1$ or -3 then $l = (n, m)$ must necessarily be 1 or $-m$.

LEMMA IV. *If m is negative and* $(m, n) \equiv (2, 3)$ (mod 4) *then an integral basis exists if and only if $m = -2l$.*

Proof. Here Mann's criteria is equivalent to

$$K = k(\sqrt{\pm 2n_1})$$

so that $Q(\sqrt{\pm 2n_1})$ is a quadratic subfield of K. Since $n \equiv 3$ (mod 4) this implies that $d = m_1 n_1 = \pm 2n_1$ so that $m_1 = \pm 2$. Since m is negative $m_1 = -2$ and so $m = -2l$.

LEMMA V. *When m is negative and* $(m, n) \equiv (3, 2)$ (mod 4) *then an integral basis exists if and only if $m = -1$.*

Proof. Again Mann's criteria gives

$$K = k(\sqrt{2\epsilon n_1})$$

with ϵ a unit of k. When $m \neq -1$ then $\epsilon = \pm 1$ so $Q(\sqrt{\pm 2n_1})$ is again a quadratic subfield of K. Thus $l = 2$ or $m_1 = -2$ both of which are impossible with $m \equiv 3 \pmod 4$. Hence K has no integral basis over k unless $m = -1$.

The next result is a stronger version of Theorem 4 of **[5]** for our special case.

COROLLARY I. *If m is negative then k has odd class number if and only if $K = k(\sqrt{n})$ has an integral basis over k for every square free integer n.*

Proof. It is well known that k has odd class number if and only if $m = -1, -2$ or $-p$ with $p \equiv 3 \pmod 4$. If m is one of these values it is immediate from Theorem I that an integral basis exists. Conversely if m has two distinct prime divisors p and p' then it follows from Theorem I that $K = k(\sqrt{ap})$ has no integral basis over k when a is integer satisfying $(a, m) = 1$ and $ap \equiv 1 \pmod 4$. Finally if $m = -p$ with $p \equiv 1 \pmod 4$ then $m \equiv 3 \pmod 4$ so no integral basis exists for any $n \equiv 2 \pmod 4$.

3. Real subfield k. When k is a real subfield it follows from Mann's criteria and Lemma I that K will have an integral basis over k if and only if $K = k(\sqrt{2^e \epsilon n_1})$ where $e = 0$ or 1 and ϵ is a unit of k. Now every unit ϵ of k has the form $\epsilon = \pm \epsilon_0^j$ where ϵ_0 is a fundamental unit and j is an integer. For any field k it is easily seen that $\epsilon_0^3 = b_0 + c_0\sqrt{m}$ with $b_0, c_0 \in Z$. Since only the parity of j is important we shall assume that $j = 0$, 1 or 3 with the latter choice being made to insure that $\epsilon = b + c\sqrt{m}$ with $b, c \in Z$. Furthermore when ϵ_0 has norm -1 it is easily seen that $j = 0$ and whenever $j = 0$ the conditions of Theorem I are necessary and sufficient for K to have an integral basis over k.

From now on we shall only be concerned with fields k where ϵ_0 and hence ϵ has norm $+1$. The following results on units will be very useful.

LEMMA VI. *Let $\epsilon = \epsilon_0$ or ϵ_0^3 have the form $b + c\sqrt{m}$ with $b, c \in Z$ and let the norm of ϵ be $+1$. If $m \equiv 1$ or $2 \pmod 4$ then $(b, c) \equiv (1, 0) \pmod 2$ and $c \equiv 0 \pmod 4$ whenever $m \equiv 1 \pmod 4$. Furthermore*

$$\sqrt{\epsilon} = s\sqrt{u} + t\sqrt{v} \tag{1}$$

with $(u, v) = 1$ and $uv = m$. If $m \equiv 3 \pmod 4$ then either $c \equiv 0 \pmod 4$ and equation (1) holds or $(b, c) \equiv (0, 1) \pmod 2$ and

$$\sqrt{\epsilon}=\frac{s\sqrt{2u}+t\sqrt{2v}}{2} \tag{2}$$

with the above conditions on u and v.

Proof. The congruence conditions are easy to verify. By **[4]**

$$\sqrt{\epsilon}=\frac{\sqrt{N(\epsilon+1)}+\sqrt{-N(\epsilon-1)}}{2}$$

$$=\frac{\sqrt{2(b+1)}+\sqrt{2(b-1)}}{2}.$$

When b is odd set $4s^2u=2(b+1)$ and $4t^2v=2(b-1)$ with u and v square free. It is easily seen that $(u,v)=1$. Also $c^2m=b^2-1=4s^2t^2uv$ so $uv=m$. When b is even set $s^2u=b+1$ and $t^2v=b-1$ with u and v square free. As above $(u,v)=1$ and $uv=m$.

Our main objective of this section is to prove the following result:

THEOREM II. *If $k=Q(\sqrt{m})$ is a real quadratic field then K has an integral basis over k if and only if one of the following conditions hold:*

(a) *At least one of m, n is* 1 (mod 4) *and either $l=1$, m, u, or v with u and v determined by equation* (1).

(b) $(m,n)\equiv(2,3)$ (mod 4) *and* $2l=m$, u *or* v.

(c) $(m,n)\equiv(3,2)$ (mod 4) *and* $l=u$ *or* v *where* u *and* v *are determined by equation* (2).

Furthermore, when $l=1$, $m/2$ or m an integral basis is given by Table I and when $l=u$, v, $u/2$, $v/2$ an integral basis is given by Table II below. For this table we set $\sqrt{\epsilon}=(s\sqrt{ru}+t\sqrt{ru})/r$ where $r=1$ or 2. Unless otherwise stated it will be assumed that $r=1$ and $l=u$ or v.

TABLE II

Basis	(m,n) (mod 4)	Conditions
$1,(1+\sqrt{\epsilon n_1})/2$	$(\ ,1)$	$bn_1\equiv 1,\ c\equiv 0\pmod 4$
$1,(\sqrt{m}+\sqrt{\epsilon n_1})/2$	$(3,1)$	$bn_1\equiv 3,\ c\equiv 0\pmod 4$
$1,(1+\sqrt{m}+\sqrt{\epsilon n_1})/2$	$(2,1)$	$bn_1\equiv 3,\ c\equiv 2\pmod 4$
$1,\sqrt{\epsilon n_1}$	$(1,3)$ *or* $(1,2)$	
$1,\sqrt{2\epsilon n_1}/2$	$(3,2)$	$r=2$
$1,(\sqrt{m}+\sqrt{2\epsilon n_1})/2$	$(2,3)$	$2l=u$ *or* v

Proof. In our preliminary remarks it was observed that we need only consider fields K satisfying $K=k(\sqrt{2^e\epsilon n_1})$ where $\epsilon=\epsilon_0^j$ ($j=1$ or 3) has norm $+1$. When one of m or n is 1 (mod 4) we wish to show that $K = k(\sqrt{\epsilon n_1})$ exactly when $l = u$ or v. Since

$$\sqrt{\epsilon n_1} = \frac{s\sqrt{run_1} + t\sqrt{rvn_1}}{r} \tag{3}$$

we see that $k(\sqrt{\epsilon n_1}) = K$ if and only if $run_1 = n = ln_1$ and $rvn_1 = d = m_1 n_1$ or vice-versa. In the first case this reduces to $l = ru$ and $m_1 = rv$, but $m = lm_1 = r^2uv$ is square free so $r = 1$ and $l = u$. Similarly in the second case $l = v$. Thus (a) is proven. According to Mann **[5**, p. 170] an integral basis for K over k, when it exists, will be given by

$$1, (a + \sqrt{2^f \epsilon n_1})/2 \tag{4}$$

where a is an integer of k satisfying

$$a^2 \equiv 2^f \epsilon n_1 \equiv 2^f(bn_1 + cn_1\sqrt{m}) \pmod 4 \tag{5}$$

and $f = 0$ or 2 according as $n \equiv 1 \pmod 4$ or not.

When $m \equiv n \equiv 1 \pmod 4$, $a = h + j\omega$ with $\omega = (1+\sqrt{m})/2$ and $h, j \in Z$. Thus (5) becomes

$$a^2 \equiv h^2 + \left(\frac{m-1}{4}\right)j^2 + (2hj + j^2)\omega \equiv bn_1 \pmod 4 \tag{6}$$

with the last congruence following from Lemma VI. Thus $j \equiv 0 \pmod 2$ and $bn_1 \equiv h^2 \equiv 1 \pmod 4$ since bn_1 is odd. Thus we take $a = 1$ here and an integral basis is given by the first line of Table II.

When $m \not\equiv 1$ and $n \equiv 1 \pmod 4$ then $a = h + j\sqrt{m}$ so

$$a^2 = h^2 + j^2 m + 2hj\sqrt{m} \equiv bn_1 + cn_1\sqrt{m} \pmod 4. \tag{7}$$

Thus $c \equiv 0$ and $b \equiv 1 \pmod 2$. When $c \equiv 0 \pmod 4$ congruence (7) reduces to

$$h^2 + j^2 m \equiv bn_1,\ 2hj \equiv 0 \pmod 4. \tag{8}$$

Either $j \equiv 0 \pmod 2$ and $bn_1 \equiv h^2 \equiv 1 \pmod 4$ or $j \equiv 1$, $h \equiv 0 \pmod 2$ so $bn_1 \equiv j^2 m \equiv m \equiv 3 \pmod 4$. The last congruence holds because bn_1 is odd and $m \not\equiv 1 \pmod 4$. Thus when $c \equiv 0 \pmod 4$ an integral basis is given by one of the first two lines of Table II. When $c \equiv 2 \pmod 4$ (7) becomes

$$(9) \qquad h \equiv j \equiv 1 \pmod 2$$

and $bn_1 \equiv h^2 + j^2m \equiv 1 + m \equiv 3 \pmod 4$ with the last congruence following because bn_1 is odd. Thus $a = 1 + \sqrt{m}$ and an integral basis is given by the third line of Table II.

Finally when $m \equiv 1$, $n \not\equiv 1 \pmod 4$ congruence (5) becomes $a^2 \equiv 0 \pmod 4$ so $a = 0$ and an integral basis is given by the fourth line of Table II.

Suppose now $(m, n) \equiv (3, 2) \pmod 4$. Here $K = k(\sqrt{2\epsilon n_1})$ is equivalent to $2run_1 = 2^{2e}ln_1$ ($e = 0$ or 1) and $2rvn_1 = 2^{2f}m_1n_1$ ($f = 0$ or 1) or vice versa. Thus $2^{2e}l = 2ru$ and hence $l = u$ and $r = 2$ (since both l and u are odd) or else $l = v$ and $r = 2$. Here $\{1, \sqrt{2\epsilon n_1}/2\}$ forms an integral basis.

Finally consider the case $(m, n) \equiv (2, 3) \pmod 4$. Here $K = k(\sqrt{2\epsilon n_1})$ if and only if $2un_1 = 4ln_1$ and $2vn_1 = m_1n_1$ or vice versa. Thus $2l = u$ or $2l = v$. Here an integral basis is given by the last line of Table II.

COROLLARY I. *If m is positive, then $K = k(\sqrt{n})$ has an integral basis over k for every n if and only if one of the following holds*:

(a) $m = 2$ *or* p.

(b) $m = 2p$ *or* pq *with* $p \equiv q \pmod 4$ *and* $N(\epsilon) = 1$.

Proof. When $m = 2$ or p then $l = 1$ or m so it is clear from (a), (b), and (c) of Theorem II that an integral basis exists. When $m = 2p$ and $N(\epsilon) = 1$ then $l = 1$ or p since n is odd. But $\sqrt{\epsilon} = s\sqrt{2} + t\sqrt{p}$ so $u = 2$ and $v = p$, thus Theorem II is satisfied. When $m = pq$ with $p \equiv q \pmod 4$ and $N(\epsilon) = 1$ then it follows from Lemma VI that $\sqrt{\epsilon} = s\sqrt{p} + t\sqrt{q}$. Thus $u = p$ and $v = q$ so (a) of Theorem II is always satisfied.

To prove the converse first note that if m has 3 or more odd prime divisors then there are at least 8 choices for l, all of which can occur for suitably chosen values of n. But, on the other hand, there are only 4 values of l for which Theorem II is satisfied. When $m = 2pq$ there are four possible values of l which can occur, namely $l = 1$, p, q or pq. However, it is seen from Theorem II (a) and (b) that there are less than four possible values of l where an integral basis does exist. If $m = pq$ with $p \not\equiv q \pmod 4$ and $r = 1$ then when n is even no integral basis exists. If $r = 2$, then no integral basis exists when $l = p$ and n odd. Finally when $m = 2p$ or pq with $N(\epsilon) = -1$ then if $l = p$ and $n \equiv 1 \pmod 4$ no integral basis exists.

COROLLARY II. *If k has odd class number then $K = k(\sqrt{n})$ has an integral basis over k for every integer n.*

Proof. The field $k = Q(\sqrt{m})$ has odd class number if and only if

$$m = 2,\ p,\ 2p_1 \text{ or } p_1p_2$$

with $p_1 \equiv p_2 \equiv 3 \pmod 4$. It is easy to see that when m has a prime divisor $q \equiv 3 \pmod 4$ that ϵ has positive norm. Hence this is an immediate result of Corollary I.

COROLLARY III. *If k is a quadratic number field either every bicyclic biquadratic extension field K has an integral basis over k or there exist infinitely many such K which do* (and don't) *have an integral basis over k.*

Proof. Immediate from Theorems I and II and their corollaries.

REFERENCES

1. A. Adrian Albert, *The integers of normal quartic fields*, Ann. Math., **31** (1930), 381–418.
2. Harvey Cohn, *A Second Course in Number Theory*, John Wiley & Sons, New York, 1962.
3. Elaine Haught, *Bicyclic Biquadratic Number Fields*, Masters Thesis, VPI & SU, 1972.
4. S. Kuroda, *Über die Dirichletschen Körper*, J. Fac. Sci. Univ. Tokyo, **4** (1943), 383–406.
5. Henry B. Mann, *On integral bases*, Proc. Amer. Math. Soc., **9** (1958), 167–172.
6. Kenneth S. Williams, *Integers of biquadratic fields*, Canad. Math. Bull., **13** (1970), 519–526.

Received April 30, 1974.

VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY