MINIMAL BASIS AND INESSENTIAL DISCRIMINANT DIVISORS FOR A CUBIC FIELD

LEONARD TORNHEIM

In terms of the coefficients α, β, γ of a defining equation

$$\phi(\theta) = \theta^3 + \alpha\theta^2 + \beta\theta + \gamma = 0 \tag{1}$$

of a cubic field F over the rational number field Q, Albert [1] has given an explicit formula for a minimal basis, that is, a basis of the integers of $Q(\theta)$ over the rational integers. We solve this same problem with a shorter proof and a simpler result. This basis is then used to find the maximal inessential discriminant divisor, that is, the square root of the quotient of the g.c.d. of the discriminants of all integers of $Q(\theta)$ by the discriminant of $Q(\theta)$. It is known [3] that the only prime dividing it is 2; we determine the power as 2^0 or 2^1.

We first secure a normalized generating quantity.

LEMMA 1. *If K is any cubic field, then $K = Q(\theta)$ with*

$$\theta^3 + a\theta^2 + b = 0, \tag{2}$$

where (i) *a and b are rational integers,* (ii) *no factor of a has its cube dividing b, and* (iii) *if $3 \| a$, then the discriminant $\Delta = -b(4a^3 + 27b)$ of θ is not divisible by 3^4 unless $3 \mid b$.*

Here $g^n \| y$ means $g^n \mid y$ and $g^{n+1} \nmid y$.

Proof. The substitution $\theta' = \theta + \alpha/3$ is used to obtain an equation of form (1) with α zero. Follow this by the substitution $\theta' = 1/\theta$ to obtain (2). For Conditions (i) and (ii) it is obvious that a substitution $\theta' = k\theta$ will be effective. If (iii) does not hold apply the substitution $\theta' = ab - 3b\theta + a^2\theta^2$; then $\theta'^3 + c\theta'^2 + d = 0$ where

$$c = -a(6b + a^3), \quad d = -b^3(4a^3 + 27b) = b^2\Delta.$$

Received February 10, 1954.

Now $3^2 \| c$ since $(b, 3) = 1$. Also $3^4 | d$. If $3^6 | d$, then the quantity $\theta'' = \theta'/9s$ satisfies the conditions of the lemma, where s is the largest integer for which $(s, 3) = 1$, $s | c$, and $s^3 | d$. If $3^6 \nmid d$ use $\theta'' = \theta'/3s$.

Essentially the following lemma is given by Sommer [2; p. 261].

LEMMA 2. *The integers of $Q(\theta)$, where θ is described in Lemma 1, have a basis over the integers given by*

$$\omega_1 = 1, \quad \omega_2 = \frac{-B + \theta}{D}, \quad \omega_3 = \frac{B^2 + aB + (B + a)\theta + \theta^2}{D^2 D_1}$$

with B, D, D_1 rational integers satisfying

$$3B + a \equiv 0 \, (D), \tag{3}$$

$$3B^2 + 2aB \equiv 0 \, (D^2 D_1), \tag{4}$$

$$B^3 + aB^2 + b \equiv 0 \, (D^3 D_1^2), \tag{5}$$

$$-\Delta = b(4a^3 + 27b) \equiv 0 \, (D^6 D_1^2), \tag{6}$$

and D, D_1 are maximal subject to these conditions.

Proof. We shall first prove that $D = 1$. Let p be a prime dividing B and D. By (3), p also divides a. But then by (5), $p^3 | b$, contradicting the choice of θ. Hence $(B, D) = 1$.

From (3) and (4), we have $aB \equiv 0(D)$. Therefore $D | a$. But by (3), $D = 3$ or 1.

If $D = 3$, then $3 \nmid b$ because from (5) we would get $D | B$. But then (6) contradicts (iii) of Lemma 1. Hence $D = 1$.

Therefore the problem is equivalent to determining the largest D_1 for which there is a solution B satisfying (4), (5), (6), when $D = 1$. It is sufficient to find solutions of these congruences with D_1 replaced by prime powers p^r and then D_1 will be their product. A value of B can be found from solutions modulo p^r by using the Chinese remainder theorem.

Thus we wish to determine the maximal value e of r for which there exists a solution B of the simultaneous congruences

$$B(3B + 2a) \equiv 0 \, (p^r), \tag{7}$$

$$(8) \qquad B^3 + aB^2 + b \equiv 0 \ (p^{2r}),$$

$$(9) \qquad -\Delta = b(4a^3 + 27b) \equiv 0 \ (p^{2r}).$$

The power p^e exists because of (9); in fact if $p^u \| \Delta$, then $e \leq s$, where $s = [u/2]$.

Case I. $(p, 3b) = 1$. *Then* $e = s$. For, let B be a solution of

$$L = 3B + 2a \equiv 0 \ (p^s);$$

hence (7) is satisfied. By (9)

$$4a^3 \equiv -27b \ (p^{2s}).$$

Now

$$L^3 - 3aL^2 \equiv 0 \ (p^{2s}).$$

This on expansion gives

$$27B^3 + 27B^2a - 4a^3 \equiv 0 \ (p^{2s}),$$

which with the above formula shows that (8) is satisfied. Thus (7), (8), (9) hold with $r = s$. Hence $e \geq s$. But since $e \leq s$ we have $e = s$.

Case II. $p \mid 3b$.

IIi. $(p, 2a) = 1$. *Then* $e = s$. For, by (9), $p^u \| b$. Simply take $B \equiv 0(p^s)$ to see that (7), (8), (9) hold with $r = s$.

IIii. $p \mid b$, $p \mid a$. *Then* $e = 0$ *if* $p \| b$ *and* $e = 1 = s - 1$ *if* $p^2 \| b$. Notice that $p^3 \nmid b$ by (ii) of Lemma 1. First, if $p^2 \mid b$, taking $B \equiv 0(p)$ presents a solution of the congruences with $r = 1$; thus $e \geq 1$. On the other hand, if $e \geq 1$, then $p \mid B$ by (8); so that $p^2 \mid b$ again by (8). Finally, if $e > 1$ then $p^3 \mid b$ by (8) since $p \mid B$ by the preceding sentence. This is a contradiction to (ii) of Lemma 1; hence $e \leq 1$. It is easy to see that if $p \neq 3$, then $s = 1$ when $p \| b$ and $s = 2$ when $p^2 \| b$. If $p = 3$, then $s = 2$ unless $p^2 \| b$, $p^2 \mid a$ and then $s = 3$.

IIiii. $p = 3$, $p \mid a$, $p \nmid b$. Notice that then $s = 1$ by (9) and (iii) of Lemma 1.

IIiii (1). $3^2 \mid a$. *Then* $e = 0$ *unless* $b \equiv \pm 1 \ (3^2)$ *in which case* $e = 1$. Now

$e \leq s = 1$. Furthermore, the fact that $e = 1$ if and only if $b \equiv \pm 1\ (3^2)$ is a consequence of (8) since only then does $B^3 + b \equiv 0\ (3^2)$ have a solution for $(3, b) = 1$, the solution being given by $B \equiv -b\ (3)$; (7) and (9) always hold with $r = 1$.

IIiii (2). $3 \| a$. *Then* $e = 0$, *unless* $b + a \equiv \pm 1\ (3^2)$, *in which case* $e = 1$. That $e \leq 1$ is a consequence of (9) and (iii) of Lemma 1. If $r = 1$, then (7) and (9) always hold and (8) has a solution if and only if $b + a \equiv \pm 1\ (3^2)$. For, if B satisfies (8) then $3 \nmid B$; hence $B^2 \equiv 1\ (3)$, $aB^2 + b \equiv a + b\ (3^2)$. But $B^3 \equiv \pm 1\ (3^2)$ so that $a + b \equiv -B^3 \equiv \mp 1\ (3^2)$. Conversely, if $a + b \equiv \mp 1\ (3^2)$, take $B \equiv -(a + b) \equiv \pm 1 \equiv -b\ (3)$; then $B^3 + aB^2 + b \equiv \pm 1 + a + b \equiv 0\ (3^2)$.

IIiv. $p = 2$, $2 | b$, $2 \nmid a$. Define t and c by $2^t \| b$, $b = 2^t c$.

IIiv (1). t odd. From (7), $2 | B$. In the expression on the left in (8), there is only one term, either aB^2 or b, containing 2 to the lowest power. Hence $e \leq [t/2]$. But $B \equiv 0\ (2^r)$ with $r = [t/2]$ does provide a solution of the three congruences. Hence $e = [t/2]$. Notice that $e = s - 1$ since $u = t + 1$ if $t = 1$ but $u = t + 2$ if $t > 1$.

IIiv (2). $t = 2$. Let $4^w \| (4a^3 + 27b)$, then $w \geq 1$. Set $4a^3 + 27b = 4^w H$. By (9), $e \leq w + 1$. Now $e \geq w$ simply by replacing s by w in the solution of Case I. It remains to determine when $e = w + 1$. Then from (7), $2 | B$ and from (8), $2^2 \nmid B$. Also from (7), $3B + 2a \equiv 0\ (2^w)$; that is, $3B = -2a + 2^w S$. Now the product of 27 with the congruence (8) gives

$$4a^3 - 3.2^{2w}\, aS^2 + 2^{3w} S^3 + 27b \equiv 0 \quad (2^{2w+2}).$$

Hence

$$2^{3w} S^3 + 2^{2w} H - 3 \cdot 2^{2w} aS^2 \equiv 0\ (2^{2w+2})$$

or

$$2^w S^3 + H - 3aS^2 \equiv 0\ (2^2).$$

If $S \equiv 0\ (2)$, then $H \equiv 0\ (4)$, an impossibility. Hence S is odd, $S^2 \equiv 1\ (4)$, $S^3 \equiv S\ (4)$, and

$$2^w S + H + a \equiv 0\ (2^2).$$

But since $w \geq 1$, we have $2^w S \equiv 2^w\ (2^2)$. Hence

$$(10) \qquad 2^{w} + H + a \equiv 0 \ (4).$$

If $w = 1$, then $H \equiv a^3 + 27c \equiv 0 \ (2)$, a contradiction to (10). Hence $w > 1$. Conversely, if (10) is true, then all the congruences in this paragraph are satisfied by taking S odd; that is, by taking for B a solution of

$$3B + 2a \equiv 2^{w} \ (2^{w+1}).$$

Hence $e = w + 1$ if and only if (10) is satisfied; that is, $H + a \equiv 0 \ (4)$. Notice from the definition of w that $u = 2 + 2w$; hence $s = w + 1$.

IIiv (3). $t = 2v \ (v > 1)$. From (9), $u = 2v + 2$; hence $e \leq s = v + 1$. Now $B \equiv 0 \ (2^v)$ yields a solution of the congruences with $r = v$; hence $e \geq v$. We determine when $e = v + 1$. Then from (7), B is even. Again from (7) either $2 \| B$ or $2^v | B$. In the first case $v \leq 1$ by (8) and this is a contradiction to $v > 1$; hence $B = 2^v K$. Now (7) holds while (8) implies

$$2^{3v}K^3 + a2^{2v}K^2 + 2^{2v}c \equiv 0 \quad (2^{2v+2}),$$

which gives, since $v > 1$,

$$aK^2 + c \equiv 0 \ (4).$$

Thus K is odd and

$$a + c \equiv 0 \ (4).$$

Conversely, if this last congruence is satisfied and B is taken as a solution of $B \equiv 2^v \ (2^{v+1})$, then B is a solution of (7), (8), and (9).

These deductions are summarized in the following theorem.

THEOREM 1. *Let θ satisfy the conditions of Lemma 1. A minimal basis of $Q(\theta)$ is*

$$\omega_1 = 1, \ \omega_2 = \theta, \ \omega_3 = \{B_2 + aB + (B + a)\theta + \theta^2\}/D,$$

where D is a product of prime powers p^e determined by the prime powers p^{2s} for which $(p^2)^s \| \Delta$ as described below and B is a common solution of the congruences given below:

(1) *If $(p, 3b) = 1$, then $e = s$ and $3B + 2a \equiv 0 \ (p^e)$.*

(2) *If $p | a$, $p \| b$, then $e = 0$. Also $e = s - 1$ if $p \neq 3$ and $e = s - 2$ if $p = 3$.*

(3) *If* $p \mid a$, $p^2 \| b$, *then* $e = 1$ *and* $B \equiv 0\ (p^e)$. *Also* $e = s - 1$ *unless* $p = 3$ *and* $p^2 \mid a$ *and then* $e = s - 2$.

(4) *If* $p \mid 3b$, $(p, 2a) = 1$, *then* $e = s$ *and* $B \equiv 0\ (p^e)$.

(5) *If* $p = 3$, $3 \mid a$, $3 \nmid b$, *then* $e \leq 1 = s$; *and* $e = s$ *if and only if* $b + a \equiv \pm 1\ (9)$ *and then* $B \equiv -b\ (3)$.

(6) *If* $p = 2$, $(2, a) = 1$, $2^t \| b$ *and*

(a) *if* t *is odd, then* $e = s - 1$ *and* $B \equiv 0\ (2^e)$;

(b) *if* $t = 2$ *then* $e = s - 1$ *unless* $H + a \equiv 0\ (4)$, *where* $H = -\Delta/4^{s-1}b$, *and then* $e = s$. *Also* $3B + 2a \equiv 2^{s-1}\ (2^s)$.

(c) *if* $t > 2$ *and even, then* $e = s - 1$ *unless* $a + c \equiv 0\ (4)$, *where* $c = b/2^t$, *and then* $e = 2$. *Also* $B \equiv 2^{s-1}\ (2^s)$.

The discriminant of $Q(\theta)$ is Δ/D^2. It divides the discriminant $\Delta(\alpha)$ of every integer α of $Q(\theta)$ and hence their g.c.d. G. The largest inessential discriminant divisor F is the square root of the quotient $G/(\Delta/D^2)$.

THEOREM 2. *The largest inessential discriminant divisor* F *is* 1 *except it is* 2 *in Case* 6b *of Theorem* 1 *when*

$$H - 3a + 2^{e-1} \equiv 0\ (2^3) \tag{11}$$

and in Case 6c *when*

$$a + c + 2^{e-1} \equiv 0\ (2^3). \tag{12}$$

Proof. The discriminant $\Delta(\alpha)$ of an integer $\alpha = c_1\omega_1 + c_2\omega_2 + c_3\omega_3$ can be found from the formula

$$\Delta(\alpha) = |a_{ij}|^2 \Delta(\theta),$$

where the elements of the determinant $|a_{ij}| = |a_{ij}(\alpha)|$ are defined by

$$\alpha^{i-1} = a_{i1} + a_{i2}\theta + a_{i3}\theta^2 \qquad (i = 1, 2, 3),$$

Since the discriminant of α is unaltered by addition of a rational number, we have

$$\Delta(\alpha) = \Delta(c_2\omega_2 + c_3\omega_3) = \Delta(\beta),$$

where

$$\beta = [c_2 + c_3 (B + a)/D]\,\theta + (c_3/D)\theta^2.$$

In computing β^2 use the fact that $\theta^3 = -a\theta^2 - b$ and $\theta^4 = a^2\theta - b\theta + ab$. Also since the first row of $|a_{ij}(\beta)|$ is $1, 0, 0$, any rational terms can be ignored. Hence,

$$(13) \qquad |a_{ij}| = \frac{c_3^3(B^3 + aB^2 + b)}{D^3} + \frac{c_2 c_3^2 (3B^2 + 2aB)}{D^2} + \frac{c_2^2 c_3 (3B + a)}{D} + c_2^3.$$

Thus

$$(14) \qquad |a_{ij}(\omega_3)| = \frac{(B^3 + aB^2 + b)}{D^3}$$

and

$$(15) \qquad |a_{ij}(\omega_2 + \omega_3)| - |a_{ij}(\omega_3)| = \frac{(3B^2 + 2aB)}{D^2} + \frac{(3B + a)}{D} + 1.$$

Now, since GD^2/Δ is the quotient of the g.c.d G of $|a_{ij}|^2\Delta$ by Δ/D^2, it equals the g.c.d of $|a_{ij}|\ {}^2D^2$. Hence the inessential discriminant divisor F is the g.c.d of $|a_{ij}|D$.

To find F we determine for each prime p the highest power p^f which remains in all the denominators of the $|a_{ij}(\alpha)|$ expressed in their lowest terms. Then F is the quotient of D divided by the product of these prime powers and thus F is the product of all p^{e-f}.

In all cases of Theorem 1 except in 5 when $a + b \equiv \pm 1\ (3^2)$, in 6b when $H + a \equiv 0\ (2^2)$, and in 6c when $a + c \equiv 0\ (2^2)$, B may be chosen to satisfy either

$$B \equiv 0\ (p^{3e})$$

or

$$3B + 2a \equiv 0\ (p^{2e}).$$

In these cases (15) implies, since its first term is then integral, that $e = f$ when $p \nmid a$. But if $p \mid a$ then $p \mid b$ and since we need consider only $e > 0$ we have Case 3 of Theorem 1. Then (14) with $B \equiv 0\ (p^{3e})$ shows that $f = 1 = e$.

Next, in Case 5 when $b+a \equiv \pm 1\ (3^2)$, $3 \nmid B$. If $3^2 \mid a$, then (15) implies that $f=1=e$. But if $3 \| a$ then $a=3a_1$ and $a_1^3+b \not\equiv 0\ (3)$ by (iii) of Lemma 1. Were $f=0$, then $B+2a_1 \equiv 0\ (3)$ by (15), which implies $B \equiv a_1\ (3)$. But then

$$B^3+aB^2+b \equiv a_1^3+b \not\equiv 0\ (3),$$

a contradiction to (8). Hence again $f=e$.

In both Cases 6b and 6c, $2 \mid B$ by (7). Now

$$|a_{ij}(\omega_2+\omega_3)|+|a_{ij}(-\omega_2+\omega_3)|-2|a_{ij}(\omega_3)| = \frac{2(3B+a)}{D}.$$

Since $2 \| 2(3B+a)$, we have $f \geq e-1$.

We now consider in particular Case 6b when $H+a \equiv 0\ (4)$. Then $3B = -2a+2^{e-1}Q$, where Q is odd. Thus

$$27(B^3+aB^2+b) = 4a^3+27b-3Q^2a2^{2e-2}+Q^3 2^{3e-3}.$$

Hence if $f=e-1$, then

$$H-3a+2^{e-1} \equiv 0\ (2^3)$$

by (14), and if this is satisfied then $f=e-1$. For, the first term in (13) has numerator divisible by 2^{2e+1}, and $2^e \| (3B^2+2aB)$ and $2^0 \| (3B+a)$ so that

$$2^{e+1} \mid [c_2c_3^2(3B^2+2aB)+Dc_2^2c_3(3B+a)].$$

Hence in lowest terms $|a_{ij}|$ has a denominator divisible by no power of p greater than $e-1$.

We finally discuss Case 6c when $a+c \equiv 0\ (4)$. Then $B=2^{e-1}+C2^e$, where we may assume that $2^{e+2} \mid C$, and $b=2^{2(e-1)}c$. Hence

$$B^3+aB^2+b \equiv 2^{3e-3}+2^{2e-2}(a+c)\ \ (2^{3e}).$$

If $f=e-1$, then by (14) this expression must be $\equiv 0\ (2^{2e+1})$, so that

$$2^{e-1}+a+c \equiv 0\ (8).$$

If this is satisfied then $f=e-1$ because the first term of (13) has numerator divisible by 2^{2e+1}, and $2^e \| (3B^2+2aB)$ and $2^0 \| (3B+a)$ so that

$$2^{e+1} \mid [c_2 c_3^2 (3B^2 + 2aB) + Dc_2^2 c_3 (3B + a)].$$

References

1. A.A. Albert, *A determination of the integers of all cubic fields*, Ann. of Math., **31** (1930), 550-566.

2. J. Sommer, *Vorlesungen über Zahlentheorie*, Berlin, 1907.

3. E.v. Zylinski, *Zur Theorie der ausserwesentliche Diskrminantenteiler algebraischer Körper*, Math. Ann. **73** (1913), 273-274.

UNIVERSITY OF MICHIGAN