60. On the Reduction of Binary Cubic Forms with Positive Discriminants. I

By Masao ARAI
Gakushuin Girls' High School

(Communicated by Shokichi IYANAGA, M. J. A., Sept. 12, 1990)

In a former paper [1], we used the quadruple of integers, named *Voronoi quadruple* (abridged *V-quadruple*), to obtain an integral basis of an order of a cubic field. The same quadruple has been already used by Mathews [2] to develop a theory of reduction of binary cubic forms with negative discriminants. Davenport [3] has given a reduction theory for the case of positive discriminants using another method. In this paper we shall give a reduction theory of binary cubic forms with positive discriminants using the quadruple introduced in [1]. Our main results will be given in § 1. In a subsequent note II, applying this theory and that of Mathews' [2] to the theory of cubic fields, we shall give a method of the construction of a table of non-conjugate cubic fields with discriminants less than a given positive number in absolute value.

§ 1. A binary cubic form

(1) $$f(x, y)=ax^3+bx^2y+cxy^2+dy^3, \quad (a, b, c, d)\in Z^4$$

and another cubic form

(2) $$f'(x, y)=a'x^3+b'x^2y+c'xy^2+d'y^3, \quad (a', b', c', d')\in Z^4$$

are defined to be *equivalent* if there exists a set of integers p, q, r, s which satisfy

(3) $$f'(x, y)=f(px+qy, rx+sy), \quad ps-qr=\pm 1.$$

We express the equivalence as $f\sim f'$ or $(a, b, c, d)\sim(a', b', c', d')$. In such a case, we can write $M=\begin{pmatrix} p & q \\ r & s \end{pmatrix}$, $M\in GL(2, Z)$, and it is easily verified that

$$(a', b', c', d')=(a, b, c, d)\mathbf{M},$$

where

$$\mathbf{M}=\begin{bmatrix} p^3 & 3p^2q & 3pq^2 & q^3 \\ p^2r & p(ps+2qr) & q(2ps+qr) & q^2s \\ pr^2 & r(2ps+qr) & s(ps+2qr) & qs^2 \\ r^3 & 3r^2s & 3rs^2 & s^3 \end{bmatrix}\in GL(4, Z).$$

The mapping $\nu: M\to\mathbf{M}$ gives an injective homomorphism from $GL(2, Z)$ to $GL(4, Z)$ as $\begin{bmatrix} X'^3 \\ X'^2Y' \\ X'Y'^2 \\ Y'^3 \end{bmatrix}=\mathbf{M}\begin{bmatrix} X^3 \\ X^2Y \\ XY^2 \\ Y^3 \end{bmatrix}$ follows from $\begin{bmatrix} X' \\ Y' \end{bmatrix}=M\begin{bmatrix} X \\ Y \end{bmatrix}$.

The discriminant of the form (1) is the invariant

$$D=b^2c^2-4ac^3-4b^3d+18abcd-27a^2d^2.$$

The Hessian of the form (1) is the quadratic covariant

(4) $$h(x, y)=Ax^2+Bxy+Cy^2,$$

where

$$A=b^2-3ac,\ B=bc-9ad,\quad \text{and}\quad C=c^2-3bd.$$

We write $H(a, b, c, d)=(A, B, C)$. A simple calculation shows that if the equivalence (3) holds between the cubic forms (1) and (2), then

$$h'(x, y)=h(px+qy,\ rx+sy)$$

holds between the corresponding Hessians, where

$$h'(x, y)=A'x^2+B'xy+C'y^2.$$

In this case, we have

$$(A', B', C')=(A, B, C)\tilde{M},$$

where

$$\tilde{M}=\begin{bmatrix} p^2 & 2pq & q^2 \\ pr & ps+qr & qs \\ r^2 & 2rs & s^2 \end{bmatrix} \in GL(3, Z).$$

The mapping $\nu_1 : M \rightarrow \tilde{M}$ gives a homomorphism with kernel $\left\{\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, -\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right\}$, from $GL(2, Z)$ to $GL(3, Z)$, as $\begin{bmatrix} X'^2 \\ X'Y' \\ Y'^2 \end{bmatrix}=\tilde{M}\begin{bmatrix} X^2 \\ XY \\ Y^2 \end{bmatrix}$ follows from $\begin{bmatrix} X' \\ Y' \end{bmatrix}=M\begin{bmatrix} X \\ Y \end{bmatrix}$. If $D>0$, the Hessian is positive definite, and we have always

(5) $$4AC-B^2=3D>0, \qquad A>0, \qquad C>0.$$

Hermite has called the binary cubic form (1) *reduced* if its Hessian (4) is reduced, that is, if (A, B, C) satisfies

(6) $$0 \leq B \leq A \leq C.$$

Two equivalent reduced cubic forms f and f' do not necessarily coincide, as shown by a counter-example:

$f(x, y)=x^3-6xy^2-2y^3$, $f'(x, y)=f(x+y, -y)=x^3+3x^2y-3xy^2-3y^3$, $h(x, y)=h'(x, y)=18x^2+18xy+36y^2$, where f and f' are reduced and $f \sim f'$, but $f \neq f'$.

Now, we introduce the following definition:

Definition 1. *If a binary cubic form* (1) *with discriminant* $D>0$ *and its Hessian* (4) *satisfies*

$$\begin{cases} \text{I} & 0 \leq B \leq A \leq C, \\ \text{II} & a>0, \\ \text{III} & A=B \ \textit{implies}\ 3a-2b>0, \\ \text{IV} & A=C,\ A \neq B \ \textit{implies}\ a-|d|<0, \\ \text{V} & B=0 \ \textit{implies}\ d<0, \end{cases}$$

then we call the cubic form (1) strictly reduced.

In § 2 we shall prove:

Theorem 1. *For any binary cubic form $f(x, y)$ with positive discriminant, there exists a strictly reduced form $f'(x, y)$ which is equivalent to $f(x, y)$.*

In our proof, we shall give a procedure of reduction.

In § 3, we shall prove furthermore:

Theorem 2. *If two strictly reduced binary cubic forms are equivalent, they coincide.*

Throughout this note, V, V_1, V_0 will denote three sets defined as follows:

$V=\{(a,b,c,d)\in Z^4 \mid ax^3+bx^2y+cxy^2+dy^3$ *is irreducible over* $\boldsymbol{Q}$ *and* $D>0\}$

$V_1=\{(a,b,c,d)\in V \mid ax^3+bx^2y+cxy^2+dy^3$ *is reduced*$\}$

$V_0=\{(a,b,c,d)\in V_1 \mid ax^3+bx^2y+cxy^2+dy^3$ *is strictly reduced*$\}$

§ 2. In §§ 2, 3 of this paper will occur the following 8 special matrices belonging to $GL(2,Z)$:

$$I=\begin{pmatrix}1&0\\0&1\end{pmatrix},\ F=\begin{pmatrix}-1&-1\\1&0\end{pmatrix},\ G=\begin{pmatrix}0&1\\-1&-1\end{pmatrix},\ P=\begin{pmatrix}1&1\\0&-1\end{pmatrix},\ Q=\begin{pmatrix}-1&0\\1&1\end{pmatrix},$$

$$R=\begin{pmatrix}0&1\\1&0\end{pmatrix},\ S=\begin{pmatrix}1&0\\0&-1\end{pmatrix},\ T=\begin{pmatrix}1&1\\0&1\end{pmatrix}.$$

In the following four lemmas, we assume (a,b,c,d), $(a',b',c',d')\in V$, $(a',b',c',d')=(a,b,c,d)M$, and $(A',B',C')=(A,B,C)\tilde{M}$, where $M=\nu(M)$, $\tilde{M}=\nu_1(M)$, $M\in GL(2,Z)$, and $(A,B,C)=H(a,b,c,d)$.

Lemma 1. *In calculating* (a',b',c',d') *and* (A',B',C') *for given* (a,b,c,d) *with Hessian* (A,B,C) *for* $M=-I,P,R,-R,S,T^n$, *we obtain*:

	M	M^{-1}	(a',b',c',d')	(A',B',C')
(1)	$-I$	$-I$	$(-a,-b,-c,-d)$	(A,B,C)
(2)	P	P	$(a,3a-b,3a-2b+c,a-b+c-d)$	$(A,2A-B,A-B+C)$
(3)	R	R	(d,c,b,a)	(C,B,A)
(4)	$-R$	$-R$	$(-d,-c,-b,-a)$	(C,B,A)
(5)	S	S	$(a,-b,c,-d)$	$(A,-B,C)$
(6)	T^n		$(a,3na+b,3n^2a+2nb+c,$ $n^3a+n^2b+nc+d)$	$(A,2nA+B,$ $n^2A+nB+C)$

Lemma 2. *In each of the cases* (1)–(5) *of* Lemma 1, *the following holds*:

(1) $V_1\ni(a,b,c,d) \iff V_1\ni(a',b',c',d')$

(2) $V_1\ni(a,b,c,d),\ A=B \iff V_1\ni(a',b',c',d'),\ A'=B'$

(3) $V_1\ni(a,b,c,d),\ A=C \iff V_1\ni(a',b',c',d'),\ A'=C'$

(4) $V_1\ni(a,b,c,d),\ A=C \iff V_1\ni(a',b',c',d'),\ A'=C'$

(5) $V_1\ni(a,b,c,d),\ B=0 \iff V_1\ni(a',b',c',d'),\ B'=0$

Lemma 3. *In each of the cases* (1)–(5) *of* Lemma 1, *the following inequality holds*:

(1) $aa'<0$,

(2) $(3a-2b)(3a'-2b')\leq 0$,

(3) $(a-d)(a'-d')\leq 0$,

(4) $(a+d)(a'+d')\leq 0$,

(5) $dd'<0$.

We omit the easy proofs of Lemmas 1–3.

Lemma 4. $f(x,y)=ax^3+bx^2y+cxy^2+dy^3$ *is reducible over* $\boldsymbol{Q}$, *if one of the following conditions* (1), (2), (3) *holds*:

(1) $A=B,\ 3a-2b=0$,

(2) $A=C,\ A\neq -B,\ a-d=0$,

(3) $A=C, A\neq B, a+d=0$.

Indeed, we have under each of these conditions:

(1) $f(x, y)=(2x+y)\left(\frac{a}{2}x^2+\frac{a}{2}xy+dy^2\right)$,

(2) $f(x, y)=(x+y)(ax^2-(a-b)xy+ay^2)$,

(3) $f(x, y)=(x-y)(ax^2+(a+b)xy+ay^2)$.

Proof of Theorem 1. We prove the theorem by showing the procedure of performing actually successive linear transformations of (a_1, b_1, c_1, d_1) in V to obtain a (a, b, c, d) in V_0. Put $(a, b, c, d)=(a_1, b_1, c_1, d_1)$. 1) Apply R if neccesary, to get $A\leq C$ (where, "apply R" means, "apply $\nu(R)$ to (a, b, c, d) to obtain $(a', b', c', d')=(a, b, c, d)\nu(R)$, and simultaneously, apply $\nu_1(R)$ to (A, B, C) to obtain $(A', B', C')=(A, B, C)\nu_1(R)$, where $(A, B, C)=H(a, b, c, d)$"). Rewrite now (a', b', c', d') by (a, b, c, d) to go to the next step. (We always do the same to go on, without repeating this comment.) 2) Apply $-I$ if neccesary, to get $a>0$. 3) Apply T^n with appropriate n, to get $-A\leq B\leq A$. 4) If $B<0$, then apply S to get $0\leq B\leq A$. 5) If $A>C$, go back to 1) and repeat the same procedure. Since we have $A>0$, $C>0$, and the value of A decreases each time as we proceed, we get $0\leq B\leq A\leq C$ and $a>0$ after a finite number of these procedures. 6) If $0<B<A<C$, we are done. 7) If $0=B<A<C$, applying S if neccesary, we obtain (a, b, c, d) in V_0. 8) If $A=B$, we apply P if neccesary and obtain (a, b, c, d) in V_0 in view of Lemma 4 (1). 9) If $0\leq B<A=C$, according to $d>0$ or $d<0$, we apply R or $-R$ if neccesary and obtain (a, b, c, d) satisfying I–IV of Definition 1 in view of Lemma 4 (2) or (3). 10) if $B>0$, we are done. 11) If $B=0$ applying S if neccesary, we can find (a, b, c, d) in V_0.

§ 3. In the following three lemmas, we assume (a, b, c, d), $(a', b', c', d')\in V_1$, $(a', b', c', d')=(a, b, c, d)\boldsymbol{M}$ and $(A', B', C')=(A, B, C)\tilde{M}$, where $\boldsymbol{M}=\nu(M)$, $\tilde{M}=\nu_1(M)$, $M=\begin{pmatrix} p & q \\ r & s \end{pmatrix}\in GL(2, Z)$ and $(A, B, C)=H(a, b, c, d)$.

Lemma 5. *In this situation, we have*

(1) $(A', B', C')=(A, B, C)$, $0\leq B\leq A\leq C$.

$$\begin{cases} Ap^2+Bpr+Cr^2=A, & (2) \\ 2Apq+B(ps+qr)+2Crs=B, & (3) \\ Aq^2+Bqs+Cs^2=C. & (4) \end{cases}$$

$$\begin{cases} (A-B)pr=0, & (5) \\ (A-C)r^2=0, & (6) \\ p^2+pr+r^2=1. & (7) \end{cases}$$

(8) $\begin{pmatrix} p \\ r \end{pmatrix}=\pm\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \pm\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \pm\begin{pmatrix} 1 \\ -1 \end{pmatrix}$.

Proof. (1) is obvious from the definition of V_1. (2)–(4) follow in rewriting (1). (5)–(7): $Ap^2+Bpr+Cr^2=A$, $B\geq 0$ implies $pr\leq 0$ which implies $Apr\leq Bpr$. $A\leq C$ implies $Ar^2\leq Cr^2$. Clearly $p^2+pr+r^2\geq 1$. $Ap^2+Bpr+Cr^2\geq A(p^2+pr+r^2)\geq A=Ap^2+Bpr+Cr^2$. By considering these inequalities, we obtain (5)–(7). (8) is clear from (7).

Lemma 6. *In this situation, we have*
(1) $B<A<C$ *implies* $M=\pm I$,
(2) $B<A=C$ *implies* $M=\pm I, \pm R$,
(3) $B=A<C$ *implies* $M=\pm I, \pm P$,
(4) $B=A=C$ *implies* $M=\pm I, \pm F, \pm G, \pm P, \pm Q, \pm R$.

Sketch of proof. Case (1) $B<A<C$: By Lemma 5(5)–(7), $\begin{pmatrix}p\\r\end{pmatrix}=\pm\begin{pmatrix}1\\0\end{pmatrix}$. $ps-qr\pm 1$ implies $s=\pm 1$. By Lemma 5(3), $\pm 2Aq+Bps=B$. $B<A$ implies $q=0$, $ps=1$. Thus, $M=\pm I$.

Case (2) $B<A=C$: By Lemma 5(5), (8), $\begin{pmatrix}p\\r\end{pmatrix}=\pm\begin{pmatrix}1\\0\end{pmatrix}, \pm\begin{pmatrix}0\\1\end{pmatrix}$. (2–1): If $\begin{pmatrix}p\\r\end{pmatrix}=\pm\begin{pmatrix}1\\0\end{pmatrix}$ then $M=\pm I$ as in case (1). (2–2): If $\begin{pmatrix}p\\r\end{pmatrix}=\pm\begin{pmatrix}0\\1\end{pmatrix}$, then by Lemma 5(3), $Bqr\pm 2Cs=B$. $B<C$ implies $s=0$, $qr=1$. Thus $M=\pm R$.

Case (3) $B=A<C$: By Lemma 5(6), (8), (3), $2q+s=p$, $\begin{pmatrix}q\\s\end{pmatrix}=\begin{pmatrix}0\\p\end{pmatrix}$, $\begin{pmatrix}p\\-p\end{pmatrix}$. Thus, $M=\pm I, \pm P$.

Case (4) $B=A=C$: By Lemma 5(4), $q^2+qs+s^2=1$. Thus, $\begin{pmatrix}q\\s\end{pmatrix}=\pm\begin{pmatrix}1\\0\end{pmatrix}, \pm\begin{pmatrix}0\\1\end{pmatrix}, \pm\begin{pmatrix}1\\-1\end{pmatrix}$. By Lemma 5(3), $2pq+ps+qr+2rs=1$. (4–1): If $\begin{pmatrix}p\\r\end{pmatrix}=\pm\begin{pmatrix}1\\0\end{pmatrix}$, then $\pm(2q+s)=1$. $\begin{pmatrix}q\\s\end{pmatrix}=\pm\begin{pmatrix}0\\1\end{pmatrix}, \pm\begin{pmatrix}1\\-1\end{pmatrix}$. Thus $M=\pm I, \pm P$. (4–2): If $\begin{pmatrix}p\\r\end{pmatrix}=\pm\begin{pmatrix}0\\1\end{pmatrix}$, then $\pm(q+2s)=1$, $\begin{pmatrix}q\\s\end{pmatrix}=\pm\begin{pmatrix}1\\0\end{pmatrix}, \pm\begin{pmatrix}-1\\1\end{pmatrix}$. Thus, $M=\pm R, \pm G$. (4–3): If $\begin{pmatrix}p\\r\end{pmatrix}=\pm\begin{pmatrix}1\\-1\end{pmatrix}$, then $\pm(q-s)=1$, $\begin{pmatrix}q\\s\end{pmatrix}=\pm\begin{pmatrix}1\\0\end{pmatrix}, \pm\begin{pmatrix}0\\-1\end{pmatrix}$. Thus, $M=\pm F, \pm Q$.

Lemma 7. (1) $A=B=C$ *implies* $c=-3a+b$, $d=-a$ *and vice versa*,
(2) $A=B=C$ *and* ($M=F$ *or* $M=G$) *implies* $(a', b', c', d')=(a, b, c, d)$,
(3) $A=B=C$ *and* ($M=P$ *or* $M=Q$ *or* $M=-R$) *implies* $(a', b', c', d')=(-d, -c, -b, -a)$ *and* $3a'-2b'=-(3a-2b)$.

Sketch of proof. (1) As $Bc-Cb=3Ad$, $Bb-Ac=3Ca$, $A=B=C$ implies $c-b=3d$, $b-c=3a$ which implies $c=-3a+b$, $d=-a$. Conversely, $c=-3a+b$, $d=-a$ implies $A=B=C=9a^2-3ab+b^2$.

(2) If $M=F$, then $(a', b', c', d')=(-a+b-c+d, -3a+2b-c, -3a+b, -a)=(a, b, c, d)$. If $M=G$, then $(a', b', c', d')=(-d, c-3d, -b+2c-3d, a-b+c-d)=(a, b, c, d)$.

(3) If $M=P$, then $(a', b', c', d')=(a, 3a-b, 3a-2b+c, a-b+c-d)=(-d, -c, -b, -a)$. If $M=Q$, then $(a', b', c', d')=(-a+b-c+d, b-2c+3d, -c+3d, d)=(-d, -c, -b, -a)$. $3a'-2b'=-(3a-2b)$ is easily seen.

Proof of Theorem 2. We assume that $(a, b, c, d), (a', b', c', d')\in V_0$, $(a', b', c', d')=(a, b, c, d)M$, $\nu^{-1}(M)=M\in GL(2, Z)$. Our aim is to obtain $(a', b', c', d')=(a, b, c, d)$. Considering the Hessians $H(a, b, c, d)=(A, B, C)$, $H(a', b', c', d')=(A', B', C')$ with $(A', B', C')=(A, B, C)\tilde{M}$, we have (A', B', C')

$=(A, B, C)$ by Lemma 5 (1). To perform the proof, we break up the condition $0 \leq B \leq A \leq C$ into four cases: (1) $B<A<C$, (2) $B<A=C$, (3) $B=A<C$, (4) $B=A=C$.

In case (1), by Lemma 6 (1) and II (i.e. the second condition in Definition 1 § 1. In the follwing, we shall quote in this way the conditions given in Definition 1), we see $M=I$.

In case (2), by Lemma 6 (2), we see $M=\pm I, \pm R$. We subdivide now the cases. (2–1): If $M=\pm I$, then $M=I$ by II. (2–2–1): If $M=\pm R$, $d>0$, then $M=R$ by II. By Lemmas 1–3 (3) and Lemma 4 (2), we find $a'-d'=-(a-d)>0$ which contradicts to IV. (2–2–2): If $M=\pm R$, $d<0$, then $M=-R$ by II. By Lemmas 1–3 (4) and Lemma 4 (3), we find $a'-|d'|=a'+d'=-d-a>0$, which contradicts to IV.

In case (3), by Lemma 6 (3) and II, we have $M=I, P$. If $M=P$, then by Lemmas 1–3 (2) and Lemma 4 (1), we find $3a'-2b'=-(3a-2b)<0$, which contradicts to III.

In case (4), by Lemma 6 (4) and II, we have $M=I, F, G, P, Q, -R$. (4–1): If $M=F, G$, then by Lemma 7 (2), we find $(a', b', c', d')=(a, b, c, d)$. (4–2): If $M=P, Q, -R$, then by Lemma 7 (3), we find $3a'-2b'=-(3a-2b)<0$ which contradicts to III. This completes the proof of Theorem 2.

References

[1] M. Arai: On Voronoi's theory of cubic fields. I. Proc. Japan Acad., **57**A, 226–229 (1981).
[2] G. B. Mathews: On the reduction and classification of binary cubics which have a negative discriminant. Proc. London Math. Soc., (2) **10**, 128–138 (1912).
[3] H. Davenport: The reduction of a binary cubic form. I. J. London Math. Soc., **20**, 14–22 (1945).