65. On the Reduction of Binary Cubic Forms with Positive Discriminants. II

By Masao ARAI
Gakushuin Girls' High School

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

This is a continuation of [2].

§1. Strictly reduced forms in a modified sense. For actual computation there is some interest to consider the following definition instead of Definition 1 in [2].

Definition 1′. *If a binary cubic form* $f(x, y)=ax^3+bx^2y+cxy^2+dy^3$, $(a, b, c, d)\in Z^4$ *with discriminant* $D>0$ *and its Hessian* $h(x, y)=Ax^2+Bxy+Cy^2$, *satisfies*

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

then we call the cubic form $f(x, y)$ strictly reduced in a modified sense, *or more briefly* m-strictly reduced.

Instead of Theorem 1 and Theorem 2 of [2], we have the following

Theorem 3. (1) *For any binary cubic form* $f(x, y)$ *with positive discriminant, there exists a* m-*strictly reduced form* $f'(x, y)$ *which is equivalent to* $f(x, y)$.

(2) *If two* m-*strictly reduced binary cubic forms are equivalent, they coincide.*

Sketch of proof. We shall rewrite the conditions in Definition 1:

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

Define

$V_0=\{(a, b, c, d)\in V \mid D>0$ and $ax^3+bx^2y+cxy^2+dy^3$ *is strictly reduced*$\}$,

$V_{01}=\{(a, -b, c, -d) \mid (a, b, c, d)\in V_0\}$, and

$V_{02}=\{(a, b, c, d) \mid (a, b, c, d)\in V_0\cup V_{01},\ d>0\}$.

Then we see that if (a, b, c, d) with $(A, B, C)=H(a, b, c, d)$ is in V_{01} (resp. in V_{02}), then (a, b, c, d) satisfies the conditions

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

$$\lfloor \mathrm{V}' \quad B=0 \textit{ implies } d>0,$$

resp. the conditions

$$\begin{cases} (\mathrm{I}) & -A\leq B\leq A\leq C, \\ (\mathrm{II}) & a>0,\ d>0, \\ \mathrm{III}_1 & A=B \textit{ implies } 3a-2b>0, \\ (\mathrm{III}) & A=-B \textit{ implies } 3a+2b>0, \\ (\mathrm{IV}) & A=C,\ A\neq|B| \textit{ implies } a-d<0, \end{cases}$$

and vice versa. Now, by lemma below, III_1 is removable. Clearly, there is a bijective mapping Φ from V_0 to V_{02} such that

$$\Phi(a, b, c, d)=\begin{cases}(a, & b, c, & d) & \text{if } d>0 \\ (a, & -b, c, & -d) & \text{if } d<0\end{cases}.$$

This completes the proof.

Lemma. *$A=B$, $a>0$, $d>0$ implies $3a-2b>0$.*

Sketch of proof. Using the identities $9Ca^2-3Bab+Ab^2=A^2$ and $Cc^2-3Bcd+9Ad^2=C^2$, from the assumption $B=A\leq C$, we obtain $3a-b+c\leq 0$ and $b-c+3d+b\varepsilon=0$, $\varepsilon\geq 0$ respectively. Hence, $3a+3d+b\varepsilon\leq 0$, and this gives $b<0$. Thus $3a-2b>0$.

§ 2. Application to enumeration of cubic fields. The theory of cubic forms given above, together with the results of our former paper [1] on cubic fields, can be used for enumeration of all cubic fields with discriminants ranging in the given interval. Concerning cubic fields with negative discriminants, a table of these fields with discriminants with absolute value $\leq$1,000 was given already by Mathews [3], which was enlarged to $\leq$20,000 by Angell [5]. Angell [6] gave also a table of such fields with positive discriminants $\leq$100,000. Llorente and Oneto [7] used another method to the same effect and completed some missing fields in Angell's table.

In this paper, we have considered until now only the cubic forms with positive discriminants, but from now on we shall consider also those with negative discriminants and put

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

A quadruple $(a, b, c, d)\in V$ can be considered as the V-quadruple of a cubic field as we have shown in [1]. For $(a, b, c, d)\in V$, there exists a pair of cubic numbers (α, β), such that

$$\begin{cases} \alpha^3+b\alpha^2+ac\alpha+a^2d=0, \\ \beta^3+c\beta^2+bd\beta+ad^2=0, \\ \alpha\beta=ad. \end{cases}$$

hold. We have an order $\mathcal{O}=\boldsymbol{Z}+\boldsymbol{Z}\alpha+\boldsymbol{Z}\beta$ of the cubic field $\boldsymbol{K}=\boldsymbol{Q}(\alpha)$ with integral basis $[1, \alpha, \beta]$ of $\mathcal{O}$. The Theorems 2 and 3 of [1] give a necessary and sufficient condition on $(a, b, c, d)\in V$ to the effect that $\mathcal{O}$ be the maximal order of $\boldsymbol{K}$. Davenport [4] gives furthermore the conditions on (a, b, c, d) for $|D|\leq X$ for a given upper bound X of the discriminant D (p. 185 and p. 194 for cases $D>0$ and $D<0$, respectively). In case $D>0$, our Theorem 3 allow us to judge when two quadruples give rise to one and the same field

or different fields. (Conjugate fields correspond obviously to the same quadruple.) Corresponding judgement for the case $D<0$ can be made by the result of Mathews [3]. Thus we can enumerate all non-conjugate cubic fields with $|D|\leq X$ by elementary computation. The author computed using a personal computer, setting $X=100{,}000$ for $D>0$ (reps. $X=20{,}000$ for $D<0$), and obtained a table of the cubic fields, consisting of quadruples (a, b, c, d) and D's. Each (a, b, c, d) corresponds to a cubic field $\boldsymbol{K}=\boldsymbol{Q}(\alpha)$ with discriminant D of $\boldsymbol{K}$, where the minimal polynomial of α over $\boldsymbol{Q}$ is $X^3+bX^2+acX+a^2d$. The first element a of the quadruple indicates the so-called index of this polynomial over $\boldsymbol{K}$, and $[1, \alpha, (\alpha^2+b\alpha)/a]$ is an integral basis of $\boldsymbol{K}$. The total number of the totally real (resp. complex) cubic fields is 4,804 (resp. 3,169), confirming the results of Llorente and Oneto [7] (resp. Angell [5]). We give here just first 10 of these fields for $D>0$ and $D<0$ in the order of magnitude of $|D|$.

D	$(a,$	$b,$	$c,$	$d)$	D	$(a,$	$b,$	$c,$	$d)$
*49	(1	−1	−2	1)	−23	(1	1	2	1)
*81	(1	0	−3	1)	−31	(1	0	1	1)
148	(1	−1	−3	1)	−44	(1	2	2	2)
*169	(1	1	−4	1)	−59	(1	0	2	1)
229	(1	0	−4	1)	−76	(1	1	3	1)
257	(1	−2	−3	1)	−83	(1	1	1	2)
316	(1	−2	−3	2)	−87	(1	2	3	3)
321	(1	−1	−4	1)	−104	(2	2	3	1)
*361	(1	2	−5	1)	−107	(1	1	3	2)
404	(1	1	−5	1)	**−108	(1	3	3	3)

(Rem. *: *Galois cubic field*, **: *pure cubic field.*)

Remark. A cubic field is *Galois* if and only if it has discriminant D of the form $D=m^2$, $m=Z$. In view of equality $4AC-B^2=3D$ and Lemmas 6, 7 of § 3 in [2] and Theorems 2, 3 in [1], we see that a Galois cubic field corresponds to one and only one strictly reduced binary cubic form having V-quadruple of the form $(a, b, -3a+b, -a)$ with gcd $(a, b)=1$, $D=m^2$, $m=9a^2-3ab+b^2$ where (i) m is square-free in case $3\nmid b$ and (ii) $m/9$ is square-free in case $3\mid b$, respectively. The number of such fields with $D<100{,}000$ is 51.

Acknowledgements. The author wishes to express here his hearty thanks to Prof. S. IYANAGA, M. J. A for his warm guidance and encouragement, and also to Messrs. K. Okutsu, H. Wada and Miss M. Yokota for their kind advices in writing this paper.

References

[1] M. Arai: On Voronoi's theory of cubic fields. I. Proc. Japan Acad., 57A, 226–229 (1981).

[2] ——: On the reduction of binary cubic form with positive discriminants. I. ibid., **66A**, 226–231 (1990).
[3] 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).
[4] H. Davenport: On the class-number of binary cubic forms. I, II. ibid., **26**, 183–192; 192–198 (1951).
[5] I. O. Angell: A table of complex cubic fields. Bull. London Math., Soc., **5**, 37–38 (1973).
[6] ——: A table of totally real cubic fields. Math. Comp., **30**, 184–187 (1976).
[7] P. Llorente and A. V. Oneto: On the Real Cubic fields. ibid., **39**, 689–692 (1982).