52. On Voronoï's Theory of Cubic Fields. I

By Masao ARAI
Gakushuin Girls' High School

(Communicated by Shokichi IYANAGA, M. J. A., April 13, 1981)

In his thesis [1], G. Voronoï developed an elaborate theory on the arithmetic of cubic fields, the results of which are explained in detail in Delone and Faddeev's book [2]. In this note, we shall make an additional remark to this theory, by means of which we shall give an algorithm to obtain an integral basis of such a field. In a subsequent note, we shall discuss the type of decomposition in prime factors of rational primes.

Let $K=\boldsymbol{Q}(\theta)$ be a cubic field, θ being a root of an irreducible cubic equation with coefficients from $\boldsymbol{Z}$. The ring of integers in K will be denoted by O_K. Orders of K, i.e. subrings of O_K containing 1 and constituting 3-dimensional free $\boldsymbol{Z}$-modules, are denoted generally by O. A basis of O of the form $[1, \xi, \eta]$ is called *unitary* and two bases $[1, \xi, \eta]$, $[1, \xi', \eta']$ are called *parallel* if $\xi-\xi', \eta-\eta' \in \boldsymbol{Z}$. Parallelism is an equivalence relation between unitary bases of O. A unitary basis $[1, \alpha, \beta]$ was called *normal* by Voronoï, if $\alpha\beta \in \boldsymbol{Z}$. To avoid confusion (especially in case $K/\boldsymbol{Q}$ is a Galois extension) we shall call a unitary, normal basis in the above sense a *Voronoï basis*, abridged *V-basis*. It is easily shown that there is a unique V-basis parallel to a given unitary basis of O. $[1, \alpha, \beta]$ being a V-basis, let $X^3+a_1X^2+a_2X+a_3$, $X^3+b_1X^2+b_2X+b_3$ be the minimal polynomials of α, β respectively. Then it is shown that $a_2/b_1=a_3/\alpha\beta=a$ and $b_2/a_1=b_3/\alpha\beta=d$ are integers. Put $a_1=b$, $b_1=c$. The quadruple $(a, b, c, d) \in \boldsymbol{Z}^4$ thus determined is called *V-quadruple* associated to $[1, \alpha, \beta]$. We write $\varphi[1, \alpha, \beta]=(a, b, c, d)$.

Conversely, when a V-quadruple (a, b, c, d) is given, let α be a root of $X^3+bX^2+acX+a^2d=0$, and put $\beta=ad/\alpha$. Then we have $\varphi[1, \alpha, \beta]=(a, b, c, d)$. α is determined only up to conjugacy, but the discriminant of the order $[1, \alpha, \beta]$ is determined by (a, b, c, d). We shall denote it by $D(a, b, c, d)$.

Now, if $[1, \alpha, \beta]$, $[1, \alpha', \beta']$ are two V-bases of O, we have $(1, \alpha', \beta')=(1, \alpha, \beta)A$, where A is a (3, 3)-matrix with entries $a_{ij} \in \boldsymbol{Z}$ $(i, j=1, 2, 3)$, $a_{11}=1$, $a_{21}=a_{31}=0$ and $\begin{pmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{pmatrix} \in GL(2, \boldsymbol{Z})$. Conversely, if $[1, \alpha, \beta]$ is a V-basis and A is a matrix of this form, then, choosing a_{12}, a_{13} $(\in \boldsymbol{Z})$ suitably (there is unique choice of such a_{12}, a_{13}), and putting $(1, \alpha', \beta')=(1, \alpha, \beta)A$, $[1, \alpha', \beta']$ becomes another V-basis of O. For simplification, we shall write $a_{22}=k$, $a_{32}=l$, $a_{23}=m$, $a_{33}=n$ and say that $[1, \alpha', \beta']$ is obtained from $[1, \alpha, \beta]$ by $M=\begin{pmatrix} k & m \\ l & n \end{pmatrix} \in GL(2, \boldsymbol{Z})$. Then we have the following

Theorem 1. *Let* $[1, \alpha, \beta]$ *be a V-basis of an order O in a cubic field K and* $[1, \alpha', \beta']$ *another V-basis of the same order obtained from* $[1, \alpha, \beta]$ *by* $M=\begin{pmatrix} k & m \\ l & n \end{pmatrix} \in GL(2, \boldsymbol{Z})$. *If* $\varphi[1, \alpha, \beta]=(a, b, c, d)$, $\varphi[1, \alpha', \beta']=(a', b', c', d')$, *then* $(a', b', c', d')=(a, b, c, d)\boldsymbol{M}$, *where*

$$\boldsymbol{M}=\begin{vmatrix} k & m \\ l & n \end{vmatrix}\begin{bmatrix} k^3 & -3k^2m & 3km^2 & -m^3 \\ -k^2l & k(kn+2lm) & -m(2kn+lm) & m^2n \\ kl^2 & -l(2kn+lm) & n(kn+2lm) & -mn^2 \\ -l^3 & 3l^2n & -3ln^2 & n^3 \end{bmatrix} \in GL(4, \boldsymbol{Z}).$$

Sketch of proof. When $\varphi[1, \alpha, \beta]=(a, b, c, d)$, then we have $\alpha^2=-ac-b\alpha-a\beta$, $\beta^2=-bd-d\alpha-c\beta$, $\alpha\beta=ad$. We obtain the result by direct calculation using this.

The mapping $\Gamma: M \rightarrow \boldsymbol{M}$ gives an injective homomorphism from $GL(2, \boldsymbol{Z})$ to $GL(4, \boldsymbol{Z})$, as

$$\begin{bmatrix} Y^3 \\ XY^2 \\ X^2Y \\ X^3 \end{bmatrix}=\boldsymbol{M}\begin{bmatrix} Y'^3 \\ X'Y'^2 \\ X'^2Y' \\ X'^3 \end{bmatrix}$$

follows from $(X', Y')=(X, Y)M$. For the generators $A=\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, $B=\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ of $GL(2, \boldsymbol{Z})$ we have

$$\boldsymbol{A}=\Gamma(A)=\begin{bmatrix} 1 & 3 & 3 & 1 \\ 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \qquad \boldsymbol{B}=\Gamma(B)=\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}.$$

Now, θ being a primitive integral element of $K=\boldsymbol{Q}(\theta)$, $\boldsymbol{Z}+\boldsymbol{Z}\theta+\boldsymbol{Z}\theta^2=O$ is an order of K and $[1, \theta, \theta^2]$ is a unitary basis of O. It is easy to obtain a V-basis $[1, \alpha, \beta]$ of O parallel to $[1, \theta, \theta^2]$. As $\varphi[1, \alpha, \beta]=(a, b, c, d)$ we obtain a V-quadruple which is determined by θ.

If $O_K \supsetneqq O$, O is said to be *extendible*, as O can be extended to another order $O' \supsetneqq O$. An algorithm to have a basis of O_K can be therefore obtained, if we find algorithms to solve the following two problems.

(1) To decide whether O is extendible:

(2) If O is extendible, to find an extension O' of O $(O' \supsetneqq O)$.

In fact, we surely obtain O_K in a finite number of steps in extending successively O.

Every O has a V-basis to which corresponds a V-quadruple. Thus it is convenient to express the solution of (1), (2) in terms of V-quadruples.

Theorem 2. *Let $[1, \alpha, \beta]$ be a V-basis of an order O and let $\varphi[1, \alpha, \beta]=(a, b, c, d)$. If there is a rational integer $n\geq 2$ satisfying one of the following three conditions $(C_1)_n$, $(C_2)_n$ or $(C_3)_n$, then O is extendible.*

$(C_1)_n$ $n|c,\ n^2|d$

$(C_2)_n$ $n|b,\ n^2|a$

$(C_3)_n$ $n|a, b, c, d$.

(1) *If (a, b, c, d) satisfies $(C_1)_n$, then $[1, \alpha, \beta/n]$ is V-basis of the order $O'=\boldsymbol{Z}+\boldsymbol{Z}\alpha+\boldsymbol{Z}\beta/n$ which is an extension of O and $\varphi[1, \alpha, \beta/n]=(an, b, c/n, d/n^2)$.*

(2) *If (a, b, c, d) satisfies $(C_2)_n$, then $[1, \alpha/n, \beta]$ is V-basis of the order $O'=\boldsymbol{Z}+\boldsymbol{Z}\alpha/n+\boldsymbol{Z}\beta$ which is an extension of O and $\varphi[1, \alpha/n, \beta]=(a/n^2, b/n, c, dn)$.*

(3) *If (a, b, c, d) satisfies $(C_3)_n$, then $[1, \alpha/n, \beta/n]$ is V-basis of the order $O'=\boldsymbol{Z}+\boldsymbol{Z}\alpha/n+\boldsymbol{Z}\beta/n$ which is an extension of O and $\varphi[1, \alpha/n, \beta/n]=(a/n, b/n, c/n, d/n)$.*

We omit the easy proof. In each of above cases we shall write (1) $(a, b, c, d)\boldsymbol{C}_n^{(1)}=(an, b, c/n, d/n^2)$, (2) $(a, b, c, d)\boldsymbol{C}_n^{(2)}=(a/n^2, b/n, c, dn)$ and (3) $(a, b, c, d)\boldsymbol{C}_n^{(3)}=(a/n, b/n, c/n, d/n)$ respectively.

It is to be noticed here that between the discriminants D_O and $D_{O'}$ of O and O', we have $D_{O'}=D_O/n^2$ in cases (1), (2) and $D_{O'}=D_O/n^4$ in case (3).

Theorem 3. *Let O be an order of K and (a, b, c, d) the V-quadruple corresponding to a V-basis of O, and q the maximum prime such that $q^2|D_O$. Put $(a_i, b_i, c_i, d_i)=(a, b, c, d)A_i$, $0\leq i\leq q-1$. We have $O=O_K$ if none of the conditions $(C_1)_p$, $(C_2)_p$, $(C_3)_p$ is satisfied for (a_i, b_i, c_i, d_i), $0\leq i\leq q-1$, for any prime p such that $p^2|D_O$.*

Sketch of Proof. By Theorem 1, any of the V-quadruples corresponding to V-bases of O can be written in the form $(a, b, c, d)\boldsymbol{M}$ where $\boldsymbol{M}=\Gamma(M)$, $M\in GL(2, Z)$. If $O_K\supsetneqq O$, it can be easily proved that O_K has a V-basis $[1, \gamma, \delta]$ such that $[1, s\gamma, st\delta]$ with $0<s, t\in \boldsymbol{Z}$, $st>1$ is a V-basis of O. Then for $\varphi[1, s\gamma, st\delta]=(a', b', c', d')=(a, b, c, d)\boldsymbol{M}$, we have (i) $s>1\Rightarrow s|a', b', c', d'$ and (ii) $t>1\Rightarrow t|c', t^2|d'$, so that the condition $(C_3)_p$ with $p|s$ or $(C_1)_p$ with $p|t$ is satisfied.

Furthermore, if $(C_3)_p$ or $(C_1)_p$ is satisfied for $(a', b', c', d')=(a, b, c, d)\boldsymbol{M}$, then it can be proved that there exists an i, $0\leq i\leq p-1$ such that one of the three conditions $(C_1)_p$, $(C_2)_p$, or $(C_3)_p$ is also satisfied for $(a', b', c', d')\boldsymbol{M}^{-1}\boldsymbol{A}^i=(a, b, c, d)\boldsymbol{A}^i$, by observing the entries of the matrix $\boldsymbol{M}^{-1}\boldsymbol{A}^i$.

Example. An integral basis of $K=\boldsymbol{Q}(\theta)$, where θ is a root of $X^3-6X^2+120X+424=0$. Let $[1, \alpha, \beta]$ be a V-basis of $O=\boldsymbol{Z}+\boldsymbol{Z}\theta+\boldsymbol{Z}\theta^2$. In this case we have $\alpha=\theta$, $\beta=424/\theta$ and $\varphi[1, \alpha, \beta]=(1, -6, 120, 424)$. $D_O=-(2^3\cdot 3^4)^2\cdot 3\cdot 13$ has square prime factors 2 and 3. We see that

$(1, -6, 120, 424)$ satisfies the condition $(C_1)_2$. Thus we form $(1, -6, 120, 424)C_2^{(1)}=(2, -6, 60, 106)$ which has the discriminant $D(2, -6, 60, 106)=-(2^2\cdot 3^4)^2\cdot 3\cdot 13$. $(2, -6, 60, 106)$ satisfies $(C_3)_2$. So we form $(2, -6, 60, 106)C_2^{(3)}=(1, -3, 30, 53)$ which has discriminant $D(1, -3, 30, 53)=-(3^4)^2\cdot 3\cdot 13$. $(1, -3, 30, 53)$ satisfies none of the conditions $(C_\nu)_3$, $\nu=1, 2, 3$. So we test $(1, -3, 30, 53)A=(1, 0, 27, 81)$ which satisfies $(C_1)_9$. Thus we form $(1, 0, 27, 81)C_9^{(1)}=(9, 0, 3, 1)$ which has discriminant $D(9, 0, 3, 1)=-(3^2)^2\cdot 3\cdot 13$ and satisfies $(C_2)_3$. We continue to form $(9, 0, 3, 1)C_3^{(2)}=(1, 0, 3, 3)$ with discriminant $D(1, 0, 3, 3)=-3^2\cdot 3\cdot 13$ which satisfies none of $(C_\nu)_3$, $\nu=1, 2, 3$. So we test $(1, 0, 3, 3)A=(1, 3, 6, 7)$, which satisfies none of $(C_\nu)_3$, $\nu=1, 2, 3$. Neither does $(1, 3, 6, 7)A=(1, 6, 15, 17)$. Thus we see that $[1, \gamma, \delta]$ with $\varphi[1, \gamma, \delta]=(1, 0, 3, 3)$ is an integral basis of K. (γ is a root of $X^3+3X+3=0$ and $\delta=3/\gamma$.)

References

[1] G. Voronoï: Concerning algebraic integers derivable from a root of an equation of the third degree. Master's Thesis, St. Petersburg (1894) (in Russian).

[2] B. N. Delone and D. K. Faddeev: Theory of Irrationalities of the Third Degree. Trans. Math. Monographs, vol. 10, Amer. Math. Soc. (1964).