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 simplifica-