66. On Voronoï's Theory of Cubic Fields. II

By Masao ARAI
Gakushuin Girls' High School

(Communicated by Shokichi IYANAGA, M. J. A., May 12, 1981)

In utilizing the V-quadruple defined in our Note I[1], we shall give an algorithm to determine the type of decomposition of a rational prime in a cubic field.

Let p be a given prime, α an integer of the cubic field K such that $K=\boldsymbol{Q}(\alpha)$ and $f(X)$ the minimal polynomial of α. If p does not divide the index $(O_K:\boldsymbol{Z}[\alpha])$, then the type of decomposition of p in K is determined by the type of decomposition of $f(X)$ mod. p in irreducible polynomials mod. p by a classical theorem.

Now if $[1,\alpha,\beta]$ is a V-basis of O_K and $\varphi[1,\alpha,\beta]=(a,b,c,d)$, then we have $|a|=(O_K:\boldsymbol{Z}[\alpha])$ because $\alpha^2=-ac-b\alpha-a\beta$.

Let us first settle the case where K has inessential discriminant divisor and $p=2$. The only possible inessential discriminant divisor of a cubic field is 2, and it is known that K has such a divisor if and only if $a\equiv d\equiv 0$, $b\equiv c\equiv 1$ (mod. 2) where (a,b,c,d) is, as above, $\varphi[1,\alpha,\beta]$ for a V-basis $[1,\alpha,\beta]$ of O_K. Furthermore, it is also known that 2 is decomposed in K in the form $(2)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, with $\mathfrak{p}_1=(2,\alpha+1)$, $\mathfrak{p}_2=(2,\beta+1)$, $\mathfrak{p}_3=(2,\alpha+\beta)$ (cf. [2], p. 120).

The following theorem assures that all other cases can be treated by the classical theorem cited above.

Theorem 4. *Let p be an odd prime and K be any cubic field, or else let p be any prime and K be a cubic field without inessential discriminant divisor. Then O_K has a V-basis $[1,\alpha,\beta]$ such that $\varphi[1,\alpha,\beta]=(a,b,c,d)$ with $p\nmid a$.*

Proof. Let $[1,\alpha,\beta]$ be a V-basis of O_K and put $\varphi[1,\alpha,\beta]=(a,b,c,d)$. If $p\nmid a$, then we are done. If $p\mid a$, then consider $(a_i,b_i,c_i,d_i)=(a,b,c,d)A^i\boldsymbol{B}$ where $\boldsymbol{A}$, $\boldsymbol{B}$ are 4×4 matrices given in I. We have

$$a_{-1}=-a+b-c+d,$$
$$a_0=d,$$
$$a_1=a+b+c+d.$$

If p is odd and a_{-1},a_0,a_1 are all divisible by p, then a,b,c,d are also divisible by p contrary to Theorem 2. So $p\nmid a_i$ for $i=-1,0$ or 1, and for (a_i,b_i,c_i,d_i) we have a V-basis $[1,\alpha_i,\beta_i]$ of O_K with $\varphi[1,\alpha_i,\beta_i]=(a_i,b_i,c_i,d_i)$.

In case $p=2$, we can prove in the same way if K has no inessential

1) Proc. Japan Acad., 57A, 226–229 (1981).