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).

discriminant divisor, as in this case $a\equiv d\equiv 0$, $b\equiv c\equiv 1$ (mod. 2) does not hold.

Now we have the following

Theorem 5. *Let p be a prime and K a cubic field. Let $[1,\alpha,\beta]$ be a V-basis of O_K, and $\varphi[1,\alpha,\beta]=(a,b,c,d)$. Suppose $p\nmid a$. We shall write $I=\{i\in \boldsymbol{Z}\,;\,0\leq i\leq p-1\}$ and put $(1,l_i,m_i,n_i)=(1,b,ac,a^2d)A^i$ for $i\in I$.* (I may be replaced, by the way, by any full system of representants mod. p.) *The decomposition of p into a product of prime ideals of K is obtained as follows.* (All the congruences in the following are meant mod. p.)

(1) *If $n_i\not\equiv 0$ for every $i\in I$, then $(p)=\mathfrak{P}$,* $\deg\mathfrak{P}=3$.

(2) *If $n_i\equiv 0$ for only one $i\in I$* (i.e. $n_{i'}\not\equiv 0$ *for all $i'\not\equiv i$, $i'\in I$*), *then we are in one of the two cases:*

(2.1) *If $m_i\not\equiv 0$, then $(p)=\mathfrak{p}\mathfrak{q}$ where $\mathfrak{p}=(p,\alpha-i)$, $\mathfrak{q}=(p,\alpha^2+(b+i)\alpha+ac+bi+i^2)$,* $\deg\mathfrak{p}=1$, $\deg\mathfrak{q}=2$.

(2.2) *If $m_i\equiv 0$, then $l_i\equiv 0$ and $(p)\equiv\mathfrak{p}^3$ where $\mathfrak{p}=(p,\alpha-i)$,* $\deg\mathfrak{p}=1$.

(3) *If $n_i\equiv n_j\equiv 0$ for $i,j\in I$, $i\neq j$, then we are in one of the two cases:*

(3.1) *If $m_i\not\equiv 0$, $m_j\not\equiv 0$, then there exists $k\in I$, $k\neq i$, $k\neq j$ such that $n_k\equiv 0$, and $(p)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ where $\mathfrak{p}_1=(p,\alpha-i)$, $\mathfrak{p}_2=(p,\alpha-j)$, $\mathfrak{p}_3=(p,\alpha-k)$,* $\deg\mathfrak{p}_1=\deg\mathfrak{p}_2=\deg\mathfrak{p}_3=1$.

(3.2) *If $m_i\equiv 0$, then $m_j\not\equiv 0$, $l_i\not\equiv 0$, $n_k\not\equiv 0$ for any $k\in I$, $k\neq i,j$ and $(p)=\mathfrak{p}_1^2\mathfrak{p}_2$ where $\mathfrak{p}_1=(p,\alpha-i)$, $\mathfrak{p}_2=(p,\alpha-j)$,* $\deg\mathfrak{p}_1=\deg\mathfrak{p}_2=1$.

This theorem follows easily from the following

Lemma. *If $F(X)=X^3+lX^2+mX+n$, $l,m,n\in\boldsymbol{Z}$ is a cubic irreducible polynomial, then putting $(1,l_i,m_i,n_i)=(1,l,m,n)A^i$, we have $F(X)=(X-i)^3+l_i(X-i)^2+m_i(X-i)+n_i$.*

(1) *If $n_i\not\equiv 0$ for all $i\in I$, then $F(X)$ is irreducible* mod. p.

(2) *If $n_i\equiv 0$, $m_i\not\equiv 0$, then $F(X)\equiv(X-i)F_1(X)$ where $F_1(X)=(X-i)^2+l_i(X-i)+m_i$.*

(3) *If $n_i\equiv m_i\equiv 0$, $l_i\not\equiv 0$, then $F(X)\equiv(X-i)^2F_2(X)$ where $F_2(X)=(X-i)+l_i$.*

(4) *If $n_i\equiv m_i\equiv l_i\equiv 0$, then $F(X)\equiv(X-i)^3$.*

Example 1. We take the same field as in *I*.

$K=\boldsymbol{Q}(\alpha)$ where α is a root of $X^3+3X+3=0$. O_K has a V-basis $[1,\alpha,\beta]$ with $\varphi[1,\alpha,\beta]=(1,0,3,3)$, and $(O_K:\boldsymbol{Z}[\alpha])=1$. We obtain the decomposition of primes p, $2\leq p\leq 13$ into products of prime ideals of K, observing Table (a) below, as follows:

$(2)=$prime ($n_0=3\not\equiv 0$, $n_1=7\not\equiv 0$ (mod. 2));

$(3)=\mathfrak{p}^3$, $\mathfrak{p}=(3,\alpha)$ ($n_0=3\equiv 0$, $m_0=3\equiv 0$, $l_0=0\equiv 0$ (mod. 3));

$(5)=$prime ($n_0=3\not\equiv 0$, $n_1=7\not\equiv 0$, $n_2=17\not\equiv 0$, $n_3=39\not\equiv 0$, $n_4=79\not\equiv 0$ (mod. 5));

$(7)=\mathfrak{p}\mathfrak{q}$, $\mathfrak{p}=(7, \alpha-1)$, $\mathfrak{q}=(7, \alpha^2+\alpha+4)$ ($n_1=7\equiv 0$, $n_0=3\not\equiv 0$, $n_2=17 \not\equiv 0$, $n_3=39\not\equiv 0$, $n_4\equiv n_{-3}=-33\not\equiv 0$, $n_5\equiv n_{-2}=-11\not\equiv 0$, $n_6\equiv n_{-1}=-1\not\equiv 0$, $m_1=6\not\equiv 0$ (mod. 7));

$(11)=\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$, $\mathfrak{p}_1=(11, \alpha+3)$, $\mathfrak{p}_2=(11, \alpha+2)$, $\mathfrak{p}_3=(11, \alpha-5)$ ($n_8\equiv n_{-3} =-33\equiv 0$, $n_9\equiv n_{-2}=-11\equiv 0$, $n_5=143\equiv 0$ (mod. 11));

$(13)=\mathfrak{p}_1^2\mathfrak{p}_2$, $\mathfrak{p}_1=(13, \alpha-5)$, $\mathfrak{p}_2=(13, \alpha-3)$ ($n_5=143\equiv 0$, $m_5=78\equiv 0$, $n_3=39\equiv 0$ (mod. 13)).

Table (a)

i	$(1,$	$l_i,$	$m_i,$	$n_i)$
-3	(1,	-9,	30,	-33)
-2	(1,	-6,	15,	-11)
-1	(1,	-3,	6,	-1)
0	(1,	0,	3,	3)
1	(1,	3,	6,	7)
2	(1,	6,	15,	17)
3	(1,	9,	30,	39)
4	(1,	12,	51,	79)
5	(1,	15,	78,	143)

Table (b)

i	$(1,$	$l_i,$	$m_i,$	$n_i)$
-3	(1,	-9,	33,	-37)
-2	(1,	-6,	18,	-12)
-1	(1,	-3,	9,	1)
0	(1,	0,	6,	8)
1	(1,	3,	9,	15)
2	(1,	6,	18,	28)
3	(1,	9,	33,	53)

Example 2. $K=\boldsymbol{Q}(\alpha)$ where α is a root of $X^3+6X+8=0$. O_K has a V-basis $[1, \alpha, \beta]$ with $\varphi[1, \alpha, \beta]=(2, 0, 3, 2)$, and $(O_K : \boldsymbol{Z}[\alpha])=2$. K has no inessential discriminant divisor.

If $p\neq 2$, we have the decomposition of p observing $(1, 0, 6, 8)A^i$, $0\leq i\leq p-1$. Table (b) shows that:

$(3)=\mathfrak{p}^3$, $\mathfrak{p}=(3, \alpha-1)$ ($n_1\equiv m_1\equiv l_1\equiv 0$ (mod. 3));

$(5)=\mathfrak{p}\mathfrak{q}$, $\mathfrak{p}=(5, \alpha-1)$, $\mathfrak{q}=(5, \alpha^2+\alpha+2)$ ($n_1\equiv 0$, $n_i\not\equiv 0$, $i=-1, 0, 2, 3$, $m_1\not\equiv 0$ (mod. 5));

$(7)=\mathfrak{p}\mathfrak{q}$, $\mathfrak{p}=(7, \alpha-2)$, $\mathfrak{q}=(7, \alpha^2+2\alpha+3)$ ($n_2\equiv 0$, $n_i\not\equiv 0$, $i=-3, -2, -1, 0, 1, 3$, $m_2\not\equiv 0$ (mod. 7)).

For $p=2$, we form $(7, 9, 6, 2)=(2, 0, 3, 2)\boldsymbol{AB}$ to obtain $\alpha'\in O_K$ with $\varphi[1, \alpha', \beta']=(7, 9, 6, 2)$, so that $2\nmid(O_K : \boldsymbol{Z}[\alpha'])$. (See the proof of Theorem 4.) α' is a root of $X^3+9X^2+42X+98=0$. By observing $(1, 9, 42, 98)$, and $(1, 12, 63, 150)=(1, 9, 42, 98)A$, we have

$(2)=\mathfrak{p}_1^2\mathfrak{p}_2$, $\mathfrak{p}_1=(2, \alpha')$, $\mathfrak{p}_2=(2, \alpha'-1)$.

Acknowledgement. The author wishes to express here his hearty thanks to Prof. S. Iyanaga for his warm guidance and encouragement, and also to Messrs. H. Wada and K. Okutsu for their invaluable advice in writing this paper.