

## ON A FACTORIZATION OF A PRIME NUMBER IN AN ALGEBRAIC NUMBER FIELD

BY SHÔICHI WATANABE

We study in this paper a factorization of a prime number  $p$  in an algebraic number field  $k$  of degree  $n$ .

NOTATION. Let notation be as follows:

$\mathbf{Z}$  ... the ring of rational integers

$[\omega_0, \omega_1, \dots, \omega_{n-1}]$  ( $\omega_0=1$ ) ... an integral basis of  $k$

$\omega_i \omega_j = \sum_{k=0}^{n-1} x_{ijk} \omega_k$  ( $i, j=0, 1, \dots, n-1$ ;  $x_{ijk} \in \mathbf{Z}$ )

$X, U_j$  ( $0 \leq j \leq n-1$ ) ... indeterminates

$\xi = \sum_{j=0}^{n-1} \omega_j U_j$

$\xi^{(i)} = \sum_{j=0}^{n-1} \omega_j^{(i)} U_j$  ( $0 \leq i \leq n-1$ )

$a_{ijk} = \sum_{j=0}^{n-1} x_{ijk} U_j$ .

The following fact is well known: if  $p = \prod_{i=1}^g P_i^{e_i}$  is the factorization of  $p$  in  $k$ , then

$$\prod_{i=0}^{n-1} (X - \xi^{(i)}) \equiv \prod_{i=1}^g P_i(X, U_0, U_1, \dots, U_{n-1})^{e_i},$$

where  $P_i(X, U_0, U_1, \dots, U_{n-1})$  is an irreducible polynomial mod  $p$  in  $k$ . We shall show an application of this result.

LEMMA 1. *Let notation be as above. Suppose that there exist rational integers  $e(\geq 1)$ ,  $c_i^{(r)}$  and  $k_r^{(s)}$  satisfying*

$$(1)_e \quad \begin{cases} \sum_{s=0}^r k_r^{(s)} c_i^{(s)} c_j^{(r-s)} \equiv \sum_{k=0}^{n-1} x_{ijk} c_k^{(r)} \pmod{p}, \\ c_i^{(s)} = \begin{cases} 1 & (\text{if } s=i) \\ 0 & (\text{if } s>i), \end{cases} \\ 0 \leq r \leq e-1, \quad 0 \leq i \leq n-1, \quad 0 \leq j \leq n-1, \quad r, i, j \in \mathbf{Z}. \end{cases}$$

---

Received September 17, 1990; revised June 14, 1991.

Then  $k_r^{(r)} \equiv 1 \pmod{p}$ .

*Proof.* By definition of  $x_{ijk}$ ,

$$x_{i0k} = \begin{cases} 1 & (\text{if } k=i) \\ 0 & (\text{if } k \neq i). \end{cases}$$

So putting  $j=0$  in (1)<sub>e</sub>, we have

$$\sum_{s=0}^r k_r^{(s)} c_i^{(s)} c_0^{(r-s)} \equiv c_i^{(r)} \pmod{p}.$$

By the condition about  $c_i^{(s)}$  in (1)<sub>e</sub>,

$$c_0^{(r-s)} = \begin{cases} 1 & (\text{if } s=r) \\ 0 & (\text{if } s \neq r). \end{cases}$$

Therefore  $k_r^{(r)} c_i^{(r)} \equiv c_i^{(r)} \pmod{p}$ . Putting  $i=r$ , we have  $k_r^{(r)} \equiv 1 \pmod{p}$ .

LEMMA 2. Under the assumption of Lemma 1, we have

$$\sum_{k=0}^{n-1} c_k^{(r)} a_{ik} \equiv \sum_{j=0}^{n-1} \sum_{s=0}^r k_r^{(s)} c_i^{(s)} c_j^{(r-s)} U_j \pmod{p}.$$

*Proof.*

$$\begin{aligned} \sum_{k=0}^{n-1} c_k^{(r)} a_{ik} &= \sum_{k=0}^{n-1} c_k^{(r)} \sum_{j=0}^{n-1} x_{ijk} U_j = \sum_{j=0}^{n-1} \left( \sum_{k=0}^{n-1} x_{ijk} c_k^{(r)} \right) U_j \\ &\equiv \sum_{j=0}^{n-1} \sum_{s=0}^r k_r^{(s)} c_i^{(s)} c_j^{(r-s)} U_j \pmod{p}. \end{aligned}$$

LEMMA 3. Let notation be as in Lemma 1. Put

$$\begin{aligned} A(i, w_1, \dots, w_z) &= (-1)^z c_i^{(w_1)} c_{w_1}^{(w_2)} \dots c_{w_{z-1}}^{(w_z)}, \\ B(i, s, z, r) &= \sum_{r > w_1 > \dots > w_z} A(i, w_1, \dots, w_z) c_{w_z}^{(s)}. \end{aligned}$$

Then

$$\sum_{z=1}^r B(i, s, z, r) = \begin{cases} -c_i^{(s)} & (\text{if } s < r) \\ 0 & (\text{if } s \geq r). \end{cases}$$

*Proof.* If  $s \geq r > w_1 > \dots > w_z$ , then  $w_z < s$ , so  $c_{w_z}^{(s)} = 0$ . Therefore  $B(i, s, z, r) = 0$ . Suppose  $s < r$ . Since

$$c_{w_1}^{(s)} = \begin{cases} 1 & (\text{if } w_1 = s) \\ 0 & (\text{if } w_1 < s), \end{cases}$$

we have

$$(2) \quad B(i, s, 1, r) = -c_i^{(s)} - \sum_{r > w_1 > s} c_i^{(w_1)} c_{w_1}^{(s)}.$$

Further

$$\begin{aligned} \sum_{z=2}^{r-s-1} B(i, s, z, r) &= \sum_{z=2}^{r-s-1} \left\{ \sum_{r > w_1 > \dots > w_{z-1} > s} (-1)^z c_i^{(w_1)} c_{w_1}^{(w_2)} \dots c_{w_{z-1}}^{(s)} c_s^{(s)} \right. \\ &\quad \left. + \sum_{r > w_1 > \dots > w_z > s} (-1)^z c_i^{(w_1)} c_{w_1}^{(w_2)} \dots c_{w_z}^{(s)} \right\} \\ &= - \sum_{z=1}^{r-s-2} \sum_{r > w_1 > \dots > w_z > s} (-1)^z c_i^{(w_1)} c_{w_1}^{(w_2)} \dots c_{w_z}^{(s)} \\ &\quad + \sum_{z=2}^{r-s-1} \sum_{r > w_1 > \dots > w_z > s} (-1)^z c_i^{(w_1)} c_{w_1}^{(w_2)} \dots c_{w_z}^{(s)} \\ &= - \sum_{r > w_1 > s} (-1) c_i^{(w_1)} c_{w_1}^{(s)} \\ &\quad + \sum_{r > w_1 > \dots > w_{r-s-1} > s} (-1)^{r-s-1} c_i^{(w_1)} c_{w_1}^{(w_2)} \dots c_{w_{r-s-1}}^{(s)}. \end{aligned}$$

Therefore

$$(3) \quad \sum_{z=2}^{r-s-1} B(i, s, z, r) = \sum_{r > w_1 > s} c_i^{(w_1)} c_{w_1}^{(s)} + (-1)^{r-s-1} c_i^{(r-1)} c_{r-1}^{(r-2)} \dots c_{s+1}^{(s)}.$$

Similarly

$$(4) \quad B(i, s, r-s, r) = (-1)^{r-s} c_i^{(r-1)} c_{r-1}^{(r-2)} \dots c_{s+1}^{(s)}.$$

If  $z \geq r-s+1$  and  $r > w_1 > \dots > w_z$ , then  $w_z < s$ , so  $c_{w_z}^{(s)} = 0$ . Therefore

$$(5) \quad B(i, s, z, r) = 0 \quad (\text{if } z \geq r-s+1).$$

By (2), (3), (4), (5), we get

$$\sum_{z=1}^r B(i, s, z, r) = \begin{cases} -c_i^{(s)} & (\text{if } s < r) \\ 0 & (\text{if } s \geq r). \end{cases}$$

LEMMA 4. Let  $A(i, w_1, \dots, w_z)$  be as in Lemma 3. Put

$$b_{ikr} = a_{ik} + \sum_{z=1}^r \sum_{r > w_1 > \dots > w_z} A(i, w_1, \dots, w_z) a_{w_z k}.$$

Then  $b_{ikr+1} = b_{ikr} - c_i^{(r)} b_{rk r}$ .

*Proof.* By the definition of  $A(i, w_1, \dots, w_z)$ ,

$$c_i^{(r)} A(r, w_1, \dots, w_z) = -A(i, r, w_1, \dots, w_z).$$

Substituting  $w_{i+1}$  ( $1 \leq i \leq z$ ) for  $w_i$  in  $A(i, r, w_1, \dots, w_z)$ , we have

$$(6) \quad b_i^{(r)} \sum_{z=1}^r \sum_{r > w_1 > \dots > w_z} A(r, w_1, \dots, w_z) a_{w_z k}$$

$$= - \sum_{z=2}^{r+1} \sum_{r > w_2 > \dots > w_z} A(i, r, w_2, \dots, w_z) a_{w_z k}.$$

Therefore

$$\begin{aligned} b_{i k r+1} &= a_{i k} + \sum_{z=1}^{r+1} \sum_{r+1 > w_1 > \dots > w_z} A(i, w_1, \dots, w_z) a_{w_z k} \\ &= a_{i k} + \sum_{z=1}^r \sum_{r > w_1 > \dots > w_z} A(i, w_1, \dots, w_z) a_{w_z k} + A(i, r) a_{r k} \\ &\quad + \sum_{z=2}^{r+1} \sum_{r > w_2 > \dots > w_z} A(i, r, w_2, \dots, w_z) a_{w_z k} \quad (\text{by } w_z \geq 0) \\ &= a_{i k} + \sum_{z=1}^r \sum_{r > w_1 > \dots > w_z} A(i, w_1, \dots, w_z) a_{w_z k} - c_i^{(r)} a_{r k} \\ &\quad - c_i^{(r)} \sum_{z=1}^r \sum_{r > w_1 > \dots > w_z} A(r, w_1, \dots, w_z) a_{w_z k} \quad (\text{by (6)}) \\ &= b_{i k r} - c_i^{(r)} b_{r k r}. \end{aligned}$$

THEOREM 5. Suppose that there exist integers  $e(\geq 1)$ ,  $c_i^{(r)}$  and  $k_r^{(s)}$  satisfying (1)<sub>e</sub>. Then  $p$  is divisible by  $P^e$  in  $k$ , where

$$P = (p, \omega_1 - c_1^{(0)}, \omega_2 - c_2^{(0)}, \dots, \omega_{n-1} - c_{n-1}^{(0)}).$$

*Proof.* By definition

$$\omega_i \xi = \sum_{j=0}^{n-1} \omega_i \omega_j U_j = \sum_{j=0}^{n-1} \sum_{k=0}^{n-1} x_{i j k} \omega_k U_j = \sum_{k=0}^{n-1} a_{i k} \omega_k.$$

Therefore we have

$$\begin{vmatrix} a_{00} - \xi & a_{01} & a_{02} & \dots & a_{0n-1} \\ a_{10} & a_{11} - \xi & a_{12} & \dots & a_{1n-1} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n-10} & a_{n-11} & a_{n-12} & \dots & a_{n-1n-1} - \xi \end{vmatrix} = 0,$$

so  $N\xi = \prod_{i=0}^{n-1} \xi^{(i)} = |a_{i k}|$ , where  $a_{i k}$  is the  $(i+1, k+1)$ -entry of the matrix. Let  $b_{i k r}$  be as in Lemma 4. We shall show that

$$(7) \quad N\xi \equiv \left( \sum_{j=0}^{n-1} c_j^{(0)} U_j \right)^r |b_{i k r}| \pmod{p}$$

holds, where  $b_{i k r}$  is the  $(i-r+1, k-r+1)$ -entry of the matrix.

(7) holds when  $r=0$ , since  $b_{i k 0} = a_{i k}$ . Suppose that (7) holds when  $r \leq e-1$ . If we add

$$\sum_{k=r+1}^{n-1} c_k^{(r)} \times (\text{the } (k-r+1)\text{-th column of } |b_{ikr}|)$$

to the first column, then  $(i-r+1, 1)$ -entry becomes

$$\begin{aligned} \sum_{k=r}^{n-1} c_k^{(r)} b_{ikr} &= \sum_{k=0}^{n-1} c_k^{(r)} b_{ikr} \\ &= \sum_{k=0}^{n-1} c_k^{(r)} a_{ik} + \sum_{z=1}^r \sum_{w_1 > \dots > w_z} A(i, w_1, \dots, w_z) \sum_{k=0}^{n-1} c_k^{(r)} a_{w_z k} \\ &\equiv \sum_{j=0}^{n-1} \sum_{s=0}^r k_r^{(s)} c_j^{(r-s)} \left( c_i^{(s)} + \sum_{z=1}^r \sum_{w_1 > \dots > w_z} A(i, w_1, \dots, w_z) c_{w_z}^{(s)} \right) U_j \\ &\quad (\text{mod } p) \quad (\text{by Lemma 2}) \\ &\equiv c_i^{(r)} \sum_{j=0}^{n-1} c_j^{(0)} U_j \quad (\text{mod } p) \quad (\text{by Lemma 1, 3}). \end{aligned}$$

Therefore

$$\begin{aligned} N\xi &\equiv \left( \sum_{j=0}^{n-1} c_j^{(0)} U_j \right)^{r+1} |b_{ikr} - c_i^{(r)} b_{rkr}| \quad (\text{mod } p) \\ &= \left( \sum_{j=0}^{n-1} c_j^{(0)} U_j \right)^{r+1} |b_{ikr+1}| \quad (\text{by Lemma 4}). \end{aligned}$$

So we get

$$N\xi \equiv \left( \sum_{j=0}^{n-1} c_j^{(0)} U_j \right)^e |b_{ike}| \quad (\text{mod } p),$$

hence  $\prod_{i=0}^{n-1} (X - \xi^{(i)})$  is divisible by  $\left( X - \sum_{j=0}^{n-1} c_j^{(0)} U_j \right)^e \text{ mod } p$ . Putting  $X = \xi$ , we get that  $p$  is divisible by  $P^e$ , where  $P$  is as mentioned in Theorem 5.

*Example 6.* Factorization of 3 in  $\mathbf{Q}(\alpha)$ ,  $\alpha^3 + 3\alpha + 31 = 0$ .

Put  $\omega_0 = 1$ ,  $\omega_1 = \alpha$ ,  $\omega_2 = (\alpha^2 - \alpha + 1)/3$ . Then  $[\omega_0, \omega_1, \omega_2]$  is an integral basis of  $\mathbf{Q}(\alpha)$ , and

$$\begin{aligned} \omega_1^2 &= -\omega_0 + \omega_1 + 3\omega_2, \\ \omega_1\omega_2 &= -10\omega_0 - \omega_1 - \omega_2, \\ \omega_2^2 &= 7\omega_0 - 3\omega_1. \end{aligned}$$

Therefore  $c_0^{(0)} = 1$ ,  $c_1^{(0)} = -1$ ,  $c_2^{(0)} = 1$ ,  $k_0^{(0)} = 1$  satisfy the condition  $(1)_1 \pmod{3}$  of Lemma 1 and  $c_0^{(0)} = 1$ ,  $c_1^{(0)} = c_2^{(0)} = -1$ ,  $c_1^{(1)} = 1$ ,  $c_2^{(1)} = 0$ ,  $k_0^{(0)} = k_1^{(0)} = k_1^{(1)} = 1$  satisfy the condition  $(1)_2 \pmod{3}$  of Lemma 1. So by Theorem 5, 3 is divisible by  $P_1$  and  $P_2^2$ , where

$$P_1 = (3, \omega_1 + 1, \omega_2 - 1), \quad P_2 = (3, \omega_1 + 1, \omega_2 + 1).$$

Hence  $3 = P_1 P_2^2$ .

The following Theorem is an application of Theorem 5.

THEOREM 7. *Let notation be as follows:*

$\alpha$ .....an algebraic integer of degree  $n$ ,

$f(X)$ .....the minimal polynomial of  $\alpha$ ,

$g_i(X)$  ( $i=0, 1, \dots, n-1$ ).....a monic polynomial of degree  $i$ ,

$G_i(X)=g_i(X)/a_i$  ( $a_i \in \mathbf{Z}$ ),

$[G_0(\alpha), G_1(\alpha), \dots, G_{n-1}(\alpha)]$ .....an integral basis of  $\mathbf{Q}(\alpha)$ ,

$g_i(X)g_j(X)=f(X)q_{ij}(X)+r_{ij}(X)$  ( $\deg r_{ij}(X) \leq n-1$ ),

$F_{ij}(X)=f(X)q_{ij}(X)$ ,

$p^{m_i} \parallel a_i$ .

Suppose that there exist rational integers  $b$  and  $e(\geq 1)$  such that  $F_{ij}^{(r)}(b) \equiv 0 \pmod{p^{m_i+m_j+1}}$  and  $G_i^{(r)}(b) \in \mathbf{Z}$  ( $i, j=0, 1, \dots, n-1$ ;  $r=0, 1, \dots, e-1$ ), are the  $F_{ij}^{(r)}(X)$  and  $G_i^{(r)}(X)$  are the  $r$ -th derivative of  $F_{ij}(X)$  and  $G_i(X)$  respectively. Then  $p$  is divisible by  $P^e$  in  $\mathbf{Q}(\alpha)$ , where

$$P=(p, G_1(\alpha)-G_1(b), G_2(\alpha)-G_2(b), \dots, G_{n-1}(\alpha)-G_{n-1}(b)).$$

*Proof.* Put  $G_i(\alpha)G_j(\alpha)=\sum_{k=0}^{n-1} x_{ijk}G_k(\alpha)$  ( $x_{ijk} \in \mathbf{Z}$ ). Then

$$(8) \quad g_i(\alpha)g_j(\alpha)=\sum_{k=0}^{n-1} y_{ijk}g_k(\alpha) \quad (y_{ijk}=x_{ijk}a_i a_j/a_k).$$

On the other hand, since  $g_i(\alpha)g_j(\alpha)=r_{ij}(\alpha)$ , we have

$$(9) \quad r_{ij}(\alpha)=\sum_{k=0}^{n-1} y_{ijk}g_k(\alpha)$$

from (8). Since  $\deg g_k(X) \leq n-1$  and  $\deg r_{ij}(X) \leq n-1$ , we have  $r_{ij}(X)=\sum_{k=0}^{n-1} y_{ijk}g_k(X)$  from (9), so

$$(10) \quad r_{ij}^{(r)}(X)=\sum_{k=0}^{n-1} y_{ijk}g_k^{(r)}(X).$$

By definition  $(g_i g_j)^{(r)}(b) \equiv r_{ij}^{(r)}(b) \pmod{p^{m_i+m_j+1}}$ , since  $F_{ij}^{(r)}(b) \equiv 0 \pmod{p^{m_i+m_j+1}}$ .

Therefore  $(g_i g_j)^{(r)}(b) \equiv \sum_{k=0}^{n-1} y_{ijk}g_k^{(r)}(b) \pmod{p^{m_i+m_j+1}}$  by (10). Dividing both sides by  $a_i a_j$ , we get

$$(11) \quad (G_i G_j)^{(r)}(b) \equiv \sum_{k=0}^{n-1} x_{ijk}G_k^{(r)}(b) \pmod{p}$$

since  $G_i^{(r)}(b) \in \mathbf{Z}$ ,  $p^{m_i} \parallel a_i$  and  $p^{m_j} \parallel a_j$ . Now we put

$$(12) \quad c_i^{(s)}=a_s G_i^{(s)}(b)/s! \quad \text{and} \quad k_r^{(s)}=a_r/a_s a_{r-s}.$$

Then  $c_i^{(s)}$  and  $k_r^{(s)}$  are integers and

$$c_i^{(s)} = \begin{cases} 1 & (\text{if } i=s) \\ 0 & (\text{if } i < s). \end{cases}$$

Further

$$\begin{aligned} \sum_{s=0}^r k_r^{(s)} c_i^{(s)} c_j^{(r-s)} &= \sum_{s=0}^r (a_r/a_s a_{r-s}) (a_s G_i^{(s)}(b)/s!) (a_{r-s} G_j^{(r-s)}(b)/(r-s)!) \\ &= (a_r/r!) \sum_{s=0}^r \binom{r}{s} G_i^{(s)}(b) G_j^{(r-s)}(b) \\ &= (a_r/r!) (G_i G_j)^{(r)}(b) \\ &\equiv (a_r/r!) \sum_{k=0}^{n-1} x_{ijk} G_k^{(r)}(b) \pmod{p} \quad (\text{by (11)}) \\ &= \sum_{k=0}^{n-1} x_{ijk} c_k^{(r)} \quad (\text{by (12)}). \end{aligned}$$

Therefore  $p$  is divisible by  $P^e$  in  $\mathbf{Q}(\alpha)$  by Theorem 5, where  $P$  is as mentioned in Theorem 7 since  $c_i^{(0)} = G_i(b)$ .

*Example 8.* Factorization of 2 in  $\mathbf{Q}(\alpha)$ ,  $f(\alpha) = \alpha^3 - \alpha^2 - 2\alpha - 8 = 0$ . (See [1]). Put  $G_1(X) = X$  and  $G_2(X) = (X^2 - X)/2$ . Then  $[1, G_1(\alpha), G_2(\alpha)]$  is an integral basis of  $\mathbf{Q}(\alpha)$ . Since  $f(X) \equiv X(X-2)(X+1) \pmod{8}$ , we get  $f(0) \equiv f(2) \equiv f(-1) \equiv 0 \pmod{8}$  and  $G_1(0) = G_2(0) = 0$ ,  $G_1(2) \equiv 0$ ,  $G_2(2) = 1$ ,  $G_1(-1) \equiv G_2(-1) \equiv 1 \pmod{2}$ . Therefore 2 is divisible by

$$\begin{aligned} P_1 &= (2, \alpha, (\alpha^2 - \alpha)/2), \\ P_2 &= (2, \alpha, (\alpha^2 - \alpha - 2)/2) \quad \text{and} \\ P_3 &= (2, \alpha - 1, (\alpha^2 - \alpha - 2)/2), \end{aligned}$$

by Theorem 7. So we have  $2 = P_1 P_2 P_3$ .

## REFERENCES

- [1] T. TAKAGI, Algebraic number theory (in Japanese), Iwanami, Tokyo (1982), 76-80.

TOKIWAGIGAKUEN HIGH SCHOOL,  
4-3-20 ODWARA, AOBA, SENDAI 983,  
JAPAN

