S. WATANABE
KODAI MATH. J.
14 (1991), 485—491

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:
$\boldsymbol{Z}\cdots$ the ring of rational integers
$[\omega_0, \omega_1, \cdots, \omega_{n-1}]$ $(\omega_0=1)\cdots$ an integral basis of k
$\omega_i\omega_j=\sum_{k=0}^{n-1} x_{ijk}\omega_k$ $(i, j=0, 1, \cdots, n-1;\ x_{ijk}\in\boldsymbol{Z})$
X, U_j $(0\leqq j\leqq n-1)\cdots$ indeterminates
$\xi=\sum_{j=0}^{n-1}\omega_j U_j$
$\xi^{(i)}=\sum_{j=0}^{n-1}\omega_j^{(i)}U_j$ $(0\leqq i\leqq n-1)$
$a_{ik}=\sum_{j=0}^{n-1}x_{ijk}U_j.$

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

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

where $P_i(X, U_0, U_1, \cdots, U_{n-1})$ 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* $e(\geqq 1)$, $c_i^{(r)}$ *and* $k_r^{(s)}$ *satisfying*

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

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 $(1)_e$, 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 $(1)_e$,

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

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.

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

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

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

Then

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

Proof. If $s\geqq r>w_1>\cdots>w_z$, 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) $$B(i,\ s,\ 1,\ r)=-c_i^{(s)}-\sum_{r>w_1>s} c_i^{(w_1)}c_{w_1}^{(s)}.$$

Further

$$\sum_{z=2}^{r-s-1} B(i,\ s,\ z,\ r)=\sum_{z=2}^{r-s-1}\{\sum_{r>w_1>\cdots>w_{z-1}>s}(-1)^z c_i^{(w_1)}c_{w_1}^{(w_2)}\cdots c_{w_{z-1}}^{(s)}c_s^{(s)}$$
$$+\sum_{r>w_1>\cdots>w_z>s}(-1)^z c_i^{(w_1)}c_{w_1}^{(w_2)}\cdots c_{w_z}^{(s)}\}$$
$$=-\sum_{z=1}^{r-s-2}\sum_{r>w_1>\cdots>w_z>s}(-1)^z c_i^{(w_1)}c_{w_1}^{(w_2)}\cdots c_{w_z}^{(s)}$$
$$+\sum_{z=2}^{r-s-1}\sum_{r>w_1>\cdots>w_z>s}(-1)^z c_i^{(w_1)}c_{w_1}^{(w_2)}\cdots c_{w_z}^{(s)}$$
$$=-\sum_{r>w_1>s}(-1)c_i^{(w_1)}c_{w_1}^{(s)}$$
$$+\sum_{r>w_1>\cdots>w_{r-s-1}>s}(-1)^{r-s-1}c_i^{(w_1)}c_{w_1}^{(w_2)}\cdots c_{w_{r-s-1}}^{(s)}.$$

Therefore

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

Similarly

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

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

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

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

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

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

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

Then $b_{ik\,r+1}=b_{ikr}-c_i^{(r)}b_{rkr}$.

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

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

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

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

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

Therefore

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

$$=a_{ik}+\sum_{z=1}^{r}\sum_{r>w_1>\cdots>w_z} A(i, w_1, \cdots, w_z)a_{w_z k}+A(i, r)a_{rk}$$

$$+\sum_{z=2}^{r+1}\sum_{r>w_2>\cdots>w_z} A(i, r, w_2, \cdots, w_z)a_{w_z k} \qquad (\text{by } w_z\geqq 0)$$

$$=a_{ik}+\sum_{z=1}^{r}\sum_{r>w_1>\cdots>w_z} A(i, w_1, \cdots, w_z)a_{w_z k}-c_i^{(r)}a_{rk}$$

$$-c_i^{(r)}\sum_{z=1}^{r}\sum_{r>w_1>\cdots>w_z} A(r, w_1, \cdots, w_z)a_{w_z k} \qquad (\text{by } (6))$$

$$=b_{ikr}-c_i^{(r)}b_{rkr}.$$

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

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

Proof. By definition

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

Therefore we have

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

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

$$N\xi\equiv\left(\sum_{j=0}^{n-1}c_j^{(0)}U_j\right)^r|b_{ikr}| \qquad (\text{mod } p) \tag{7}$$

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

(7) holds when $r=0$, since $b_{ik0}=a_{ik}$. Suppose that (7) holds when $r\leqq e-1$. 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

$$\sum_{k=r}^{n-1} c_k^{(r)} b_{ikr} = \sum_{k=0}^{n-1} c_k^{(r)} b_{ikr}$$

$$= \sum_{k=0}^{n-1} c_k^{(r)} a_{ik} + \sum_{z=1}^{r} \sum_{r>w_1>\cdots>w_z} A(i,\ w_1,\ \cdots,\ w_z) \sum_{k=0}^{n-1} c_k^{(r)} a_{w_z k}$$

$$\equiv \sum_{j=0}^{n-1} \sum_{s=0}^{r} k_r^{(s)} c_j^{(r-s)} \Big(c_i^{(s)} + \sum_{z=1}^{r} \sum_{r>w_1>\cdots>w_z} A(i,\ w_1,\ \cdots,\ w_z) c_{w_z}^{(s)} \Big) U_j$$

$$\pmod p \quad \text{(by Lemma 2)}$$

$$\equiv c_i^{(r)} \sum_{j=0}^{n-1} c_j^{(0)} U_j \qquad \pmod p \quad \text{(by Lemma 1, 3).}$$

Therefore

$$N\xi \equiv \Big(\sum_{j=0}^{n-1} c_j^{(0)} U_j \Big)^{r+1} |b_{ikr} - c_i^{(r)} b_{rkr}| \qquad \pmod p$$

$$= \Big(\sum_{j=0}^{n-1} c_j^{(0)} U_j \Big)^{r+1} |b_{ik\, r+1}| \qquad \text{(by Lemma 4).}$$

So we get

$$N\xi \equiv \Big(\sum_{j=0}^{n-1} c_j^{(0)} U_j \Big)^{e} |b_{ike}| \qquad \pmod p,$$

hence $\prod_{i=0}^{n-1} (X-\xi^{(i)})$ is divisible by $\Big(X - \sum_{j=0}^{n-1} c_j^{(0)} U_j \Big)^e$ 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 $\boldsymbol{Q}(\alpha)$, $\alpha^3+3\alpha+31=0$.

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 $\boldsymbol{Q}(\alpha)$, and

$$\omega_1^2 = -\omega_0 + \omega_1 + 3\omega_2,$$

$$\omega_1\omega_2 = -10\omega_0 - \omega_1 - \omega_2,$$

$$\omega_2^2 = 7\omega_0 - 3\omega_1.$$

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

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

Hence $3 = P_1 P_2^2$.

The following Theorem is an application of Theorem 5.

THEOREM 7. *Let notation be as follows:*
α······*an algebraic integer of degree* n,
$f(X)$······*the minimal polynomial of* α,
$g_i(X)$ $(i=0, 1, \cdots, n-1)$······*a monic polynomial of degree* i,
$G_i(X)=g_i(X)/a_i$ $(a_i\in \boldsymbol{Z})$,
$[G_0(\alpha), G_1(\alpha), \cdots, G_{n-1}(\alpha)]$······*an integral basis of* $\boldsymbol{Q}(\alpha)$,
$g_i(X)g_j(X)=f(X)q_{ij}(X)+r_{ij}(X)$ $(\deg r_{ij}(X)\leqq n-1)$,
$F_{ij}(X)=f(X)q_{ij}(X)$,
$p^{m_i}\| a_i$.
Suppose that there exist ratsonal inteZers b *and* $e(\geqq 1)$ *such that* $F_{ij}^{(r)}(b)\equiv 0$ $(\mathrm{mod}\, p^{m_i+m_j+1})$ *and* $G_i^{(r)}(b)\in \boldsymbol{Z}$ $(i, j=0, 1, \cdots, n-1;\ r=0, 1, \cdots, e-1)$, *arethe* $F_{ij}^{(r)}(X)$ *and* $G_i^{(r)}(X)$ *are the* r-th *derivative of* $F_{ij}(X)$ *and* $G_i(X)$ *respectively. Then* p *is dsvisible by* P^e *in* $\boldsymbol{Q}(\alpha)$, *where*

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

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

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

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

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

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

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

By definition $(g_ig_j)^{(r)}(b)\equiv r_{ij}^{(r)}(b)$ $(\mathrm{mod}\, p^{m_i+m_j+1})$, since $F_{ij}^{(r)}(b)\equiv 0$ $(\mathrm{mod}\, p^{m_i+m_j+1})$. Therefore $(g_ig_j)^{(r)}(b)\equiv \sum_{k=0}^{n-1} y_{ijk}g_k^{(r)}(b)$ $(\mathrm{mod}\, p^{m_i+m_j+1})$ by (10). Dividing both sides by a_ia_j, we get

$$(G_iG_j)^{(r)}(b)\equiv \sum_{k=0}^{n-1} x_{ijk}G_k^{(r)}(b) \qquad (\mathrm{mod}\, p) \tag{11}$$

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

$$c_i^{(s)}=a_sG_i^{(s)}(b)/s! \quad \text{and} \quad k_r^{(s)}=a_r/a_sa_{r-s}. \tag{12}$$

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

$$\sum_{s=0}^{r} k_r^{(s)} c_i^{(s)} c_j^{(r-s)}=\sum_{s=0}^{r}(a_r/a_s a_{r-s})(a_s G_i^{(s)}(b)/s!)(a_{r-s}G_j^{(r-s)}(b)/(r-s)!)$$

$$=(a_r/r!)\sum_{s=0}^{r}\binom{r}{s}G_i^{(s)}(b)G_j^{(r-s)}(b)$$

$$=(a_r/r!)(G_iG_j)^{(r)}(b)$$

$$\equiv(a_r/r!)\sum_{k=0}^{n-1}x_{ijk}G_k^{(r)}(b) \quad (\bmod p) \quad (\text{by } (11))$$

$$=\sum_{k=0}^{n-1}x_{ijk}c_k^{(r)} \quad (\text{by } (12)).$$

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

Example 8. Factorization of 2 in $\boldsymbol{Q}(\alpha)$, $f(\alpha)=\alpha^3-\alpha^2-2\alpha-8=0$. (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 $\boldsymbol{Q}(\alpha)$. 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

$$P_1=(2, \alpha, (\alpha^2-\alpha)/2),$$

$$P_2=(2, \alpha, (\alpha^2-\alpha-2)/2) \quad \text{and}$$

$$P_3=(2, \alpha-1, (\alpha^2-\alpha-2)/2),$$

by Theorem 7. So we have $2=P_1P_2P_3$.

REFERENCES

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

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