MATHEMATICS OF COMPUTATION
VOLUME 58, NUMBER 198
APRIL 1992, PAGES 849–853

FACTORIZATION OF PRIME IDEAL EXTENSIONS IN NUMBER RINGS

ILARIA DEL CORSO

ABSTRACT. Following an idea of Kronecker, we describe a method for factoring prime ideal extensions in number rings. The method needs factorization of polynomials in many variables over finite fields, but it works for any prime and any number field extension.

INTRODUCTION

Let $\mathbf{F} \subset \mathbf{K}$ be number fields, let $\mathcal{O}_{\mathbf{F}} \subset \mathcal{O}_{\mathbf{K}}$ be their corresponding number rings, i.e., the integral closures of $\mathbf{Z}$ in $\mathbf{F}$ and $\mathbf{K}$, respectively, and let $[\mathbf{K} : \mathbf{F}] = d$.

We know that number rings are Dedekind domains, hence any ideal factors uniquely into a product of primes. A very natural problem is to find this factorization explicitly; in particular, one can assume that factorization in $\mathcal{O}_{\mathbf{F}}$ is known and can try to compute factorization in $\mathcal{O}_{\mathbf{K}}$. The crucial step is to find the splitting of $P\mathcal{O}_{\mathbf{K}}$ for any prime ideal P of $\mathcal{O}_{\mathbf{F}}$: in fact any prime factor of an ideal I must occur in the splitting of some $P\mathcal{O}_{\mathbf{K}}$, where P is a prime factor of the norm over $\mathbf{F}$ of I, and the norm itself gives bounds for the exponents.

By a theorem of Kummer, the splitting of $P\mathcal{O}_{\mathbf{K}}$ can easily be determined in all but finitely many cases: one simply takes the minimal polynomial over $\mathcal{O}_{\mathbf{F}}$ of an integral generator α of the extension and factors it modulo P; this gives all that one needs (see [4, p. 79]). Unfortunately, this method works only if the prime integer lying under P does not divide the order of the factor group $\mathcal{O}_{\mathbf{K}}/\mathcal{O}_{\mathbf{F}}[\alpha]$.

For a fixed prime P, one could try to fulfill this condition by choosing α suitably, but this does not yet exclude all exceptions, since there may exist primes dividing the order of $\mathcal{O}_{\mathbf{K}}/\mathcal{O}_{\mathbf{F}}[\alpha]$ for *any* α (see [5, p. 64] for an example).

Originally, this problem was studied and partially solved by Kronecker [2] with an approach different from Kummer's; later, Hensel [1] improved upon Kronecker's result to obtain a method for finding the splitting of all prime ideals (p) of $\mathbf{Z}$ in number rings. This method is based on the factorization modulo p of the polynomial $N_{\mathbf{K}/\mathbf{Q}}(y - \alpha_1 u_1 - \cdots - \alpha_h u_h)$, where $\alpha_1, \ldots, \alpha_h$ is an integral basis of $\mathcal{O}_{\mathbf{K}}$. Surprisingly, this work seems to be nearly forgotten and almost generally unknown.

In this paper we give a modern version of the theorem of Kronecker-Hensel

Received June 21, 1990; revised November 20, 1990.
1991 *Mathematics Subject Classification.* Primary 11R27; Secondary 11Y05.

and generalize it to the case of any prime ideal and any number field extension. Moreover, we are able to simplify the algorithm by showing that it is enough to factor $N_{\mathbf{K}/\mathbf{F}}(y - \omega_1 u_1 - \cdots - \omega_n u_n)$, where $\omega_1, \ldots, \omega_n$ are $\mathscr{O}_\mathbf{F}$-algebra generators of $\mathscr{O}_\mathbf{K}$, thereby generalizing Kummer's theorem as well.

Statement and proof of the theorem

Let $\{\omega_1, \ldots, \omega_n\}$ be any set of generators of the ring $\mathscr{O}_\mathbf{K}$ as an $\mathscr{O}_\mathbf{F}$-algebra, i.e., $\mathscr{O}_\mathbf{K} = \mathscr{O}_\mathbf{F}[\omega_1, \ldots, \omega_n]$. Let $u_1, \ldots, u_n$ be indeterminates, which will be considered as parameters, and $\omega = \omega_1 u_1 + \cdots + \omega_n u_n \in \mathscr{O}_\mathbf{K}[u_1, \ldots, u_n]$.

Given a prime ideal P in $\mathscr{O}_\mathbf{F}$, then $\mathscr{O}_\mathbf{K}/P\mathscr{O}_\mathbf{K}$ is a vector space of dimension d over $\mathscr{O}_\mathbf{F}/P$, whence $(\mathscr{O}_\mathbf{K}/P\mathscr{O}_\mathbf{K})(u_1, \ldots, u_n)$ is itself a vector space and has dimension d over $(\mathscr{O}_\mathbf{F}/P)(u_1, \ldots, u_n)$. More generally, if I is any ideal in $\mathscr{O}_\mathbf{K}$ containing P, then $\mathscr{O}_\mathbf{K}/I$ is a vector space over $\mathscr{O}_\mathbf{F}/P$ and $(\mathscr{O}_\mathbf{K}/I)(u_1, \ldots, u_n)$ is a vector space over $(\mathscr{O}_\mathbf{F}/P)(u_1, \ldots, u_n)$.

We use the following notation: $[\omega]_I$ will be the projection of ω in $(\mathscr{O}_\mathbf{K}/I)(u_1, \ldots, u_n)$; denote by

$$\phi_I : (\mathscr{O}_\mathbf{K}/I)(u_1, \ldots, u_n) \to (\mathscr{O}_\mathbf{K}/I)(u_1, \ldots, u_n)$$

the endomorphism of the $(\mathscr{O}_\mathbf{F}/P)(u_1, \ldots, u_n)$-vector space given by the multiplication by $[\omega]_I$, by $\mathbf{M}_{[\omega]_I}$ the matrix associated with ϕ_I, and by

$$\mathscr{C}_I(y) = \det(y\mathbf{I} - \mathbf{M}_{[\omega]_I}) \in (\mathscr{O}_\mathbf{F}/P)[u_1, \ldots, u_n][y]$$

its characteristic polynomial. Clearly, the characteristic and the minimal polynomials of ϕ_I and of $[\omega]_I$ are the same. Whenever we deal with an ideal of $\mathscr{O}_\mathbf{K}$, we assume tacitly that it contains $P\mathscr{O}_\mathbf{K}$.

Lemma 1. *Let $Q \subset \mathscr{O}_\mathbf{K}$ be a prime ideal. Then $\mathscr{C}_Q(y)$ is irreducible.*

Proof. Let $\mathbf{L} = (\mathscr{O}_\mathbf{F}/P)(u_1, \ldots, u_n)$; the element $[\omega]_Q \in (\mathscr{O}_\mathbf{K}/Q)(u_1, \ldots, u_n)$ is algebraic over $\mathbf{L}$. We know that

$$\mathbf{L}[[\omega]_Q] \cong \frac{\mathbf{L}[y]}{(\mu_{[\omega]_Q}(y))},$$

where $\mu_{[\omega]_Q}$ is the minimal polynomial of $[\omega]_Q$; clearly, $\mu_{[\omega]_Q}$ is irreducible and has the same degree as the extension $\mathbf{L}[[\omega]_Q]/\mathbf{L}$. We claim that $\mathscr{C}_Q(y) = \mu_{[\omega]_Q}(y)$; since the characteristic polynomial is a power of the minimal polynomial, it is enough to prove that they have the same degree.

Let $\sigma_1, \ldots, \sigma_f$ be the automorphisms of $\mathscr{O}_\mathbf{K}/Q$ fixing $\mathscr{O}_\mathbf{F}/P$, and let the $\tilde{\sigma}_i$'s be the automorphisms of $(\mathscr{O}_\mathbf{K}/Q)(u_1, \ldots, u_n)/\mathbf{L}$ extending the σ_i's in the obvious way. Since $\tilde{\sigma}_i([\omega]_Q) \neq \tilde{\sigma}_j([\omega]_Q)$ if $i \neq j$, one has $\deg \mu_{[\omega]_Q}(y) \geq f$ and the result follows. □

Lemma 2. *Let $Q_1, Q_2 \subset \mathscr{O}_\mathbf{K}$ be prime ideals with $Q_1 \neq Q_2$. Then $\mathscr{C}_{Q_1}(y) \neq \mathscr{C}_{Q_2}(y)$.*

Proof. Suppose $\mathscr{C}_{Q_1}(y) = \mathscr{C}_{Q_2}(y)$; let f be the degree of this polynomial. Then $\mathscr{O}_\mathbf{K}/Q_1$ and $\mathscr{O}_\mathbf{K}/Q_2$ are both normal extensions of degree f of $\mathscr{O}_\mathbf{F}/P$, hence there exists an isomorphism of fields

$$\psi : \mathscr{O}_\mathbf{K}/Q_2 \to \mathscr{O}_\mathbf{K}/Q_1$$

fixing $\mathscr{O}_\mathbf{F}/P$. Let

$$\Psi : (\mathscr{O}_\mathbf{K}/Q_2)(u_1, \ldots, u_n) \to (\mathscr{O}_\mathbf{K}/Q_1)(u_1, \ldots, u_n)$$

be the isomorphism extending ψ in the obvious way. Let $||P||$ denote the absolute norm of the ideal P; we know that in $(\mathscr{O}_{\mathbf{K}}/Q_2)(u_1, \ldots, u_n)[y]$ we have

$$\mathscr{C}_{Q_2}(y) = \prod_{h=0}^{f-1} (y - [\omega]_{Q_2}^{||P||^h}), \tag{1}$$

and in $(\mathscr{O}_{\mathbf{K}}/Q_1)(u_1, \ldots, u_n)[y]$

$$\mathscr{C}_{Q_1}(y) = \prod_{h=0}^{f-1} (y - [\omega]_{Q_1}^{||P||^h}). \tag{2}$$

By applying Ψ to equation (1) we obtain the following equality in $(\mathscr{O}_{\mathbf{K}}/Q_1) \circ (u_1, \ldots, u_n)[y]$:

$$\mathscr{C}_{Q_2}(y) = \prod_{h=0}^{f-1} (y - \Psi([\omega]_{Q_2}^{||P||^h})). \tag{3}$$

Since $(\mathscr{O}_{\mathbf{K}}/Q_1)(u_1, \ldots, u_n)[y]$ is a unique factorization domain and $\mathscr{C}_{Q_1}(y) = \mathscr{C}_{Q_2}(y)$, (2) and (3) imply that $\Psi([\omega]_{Q_2}) = [\omega]_{Q_1}^{||P||^h}$. Clearly, we can assume that $\Psi([\omega]_{Q_2}) = [\omega]_{Q_1}$ (this can be obtained by composing ψ with a suitable automorphism of $\mathscr{O}_{\mathbf{K}}/Q_1$), so that $\psi([\omega_k]_{Q_2}) = [\omega_k]_{Q_1}$ for each $k = 1, \ldots, n$. Consider now a generic element $G(\omega_1, \ldots, \omega_n) \in \mathscr{O}_{\mathbf{F}}[\omega_1, \ldots, \omega_n] = \mathscr{O}_{\mathbf{K}}$; we have

$$\psi([G(\omega_1, \ldots, \omega_n)]_{Q_2}) = [G(\omega_1, \ldots, \omega_n)]_{Q_1},$$

hence $[G(\omega_1, \ldots, \omega_n)]_{Q_2} = 0$ if and only if $[G(\omega_1, \ldots, \omega_n)]_{Q_1} = 0$, i.e., if and only if $Q_1 = Q_2$, a contradiction. □

Lemma 3. *Let $Q \subset \mathscr{O}_{\mathbf{K}}$ be a prime ideal such that $Q^2 | P$. Then $\mathscr{C}_Q([\omega]_{Q^2}) \neq 0$.*

Proof. Assume

$$\mathscr{C}_Q([\omega_1]_{Q^2} u_1 + \cdots + [\omega_n]_{Q^2} u_n) = 0, \tag{4}$$

i.e., $\mathscr{C}_Q$ is the minimal polynomial of $[\omega]_{Q^2}$; then

$$\mathbf{E} = (\mathscr{O}_{\mathbf{F}}/P)(u_1, \ldots, u_n)[[\omega]_{Q^2}] \cong \frac{(\mathscr{O}_{\mathbf{F}}/P)(u_1, \ldots, u_n)[y]}{(\mathscr{C}_Q(y))}.$$

By Lemma 1 the polynomial $\mathscr{C}_Q(y)$ is irreducible, hence $\mathbf{E}$ is a field.

Let $F(u_1, \ldots, u_n) = \mathscr{C}_Q([\omega_1]_{Q^2} u_1 + \cdots + [\omega_n]_{Q^2} u_n)$ ($\mathscr{C}_Q$ can be seen as a polynomial with coefficients in $\mathscr{O}_{\mathbf{F}}/P$ and indeterminates $u_1, \ldots, u_n, y$). Then $F(u_1, \ldots, u_n)$ is a polynomial in $u_1, \ldots, u_n$, with coefficients in $\mathbf{E}$, and we have by (4) that $F(u_1, \ldots, u_n) = 0$. Therefore, the partial derivatives $\frac{\partial F}{\partial u_i}$ are also all zero; hence we have

$$\frac{\partial F}{\partial u_i} = [\omega_i]_{Q^2} \mathscr{C}_Q'([\omega]_{Q^2}) + \frac{\partial \mathscr{C}_Q}{\partial u_i}([\omega]_{Q^2}) = 0, \tag{5}$$

where $\mathscr{C}_Q'(y) = \frac{\partial \mathscr{C}_Q}{\partial y}(y)$. Since $\mathscr{C}_Q$ is separable, $\mathscr{C}_Q'([\omega]_{Q^2}) \neq 0$, hence equation (5) implies that $[\omega_i]_{Q^2} \in \mathbf{E}$ for each i. From this it follows that

$$\mathbf{E} = (\mathscr{O}_{\mathbf{K}}/Q^2)(u_1, \ldots, u_n),$$

since $(\mathscr{O}_{\mathbf{K}}/Q^2)$ is not an integral domain; we have a contradiction. □

If $h \in \mathscr{O}_{\mathbf{K}}[u_1, \ldots, u_n]$, we will denote by $\mathrm{cont}(h)$ the ideal generated in $\mathscr{O}_{\mathbf{K}}$ by the coefficients of h.

Theorem. *Let* $\mathscr{C}_P(y) = \mathscr{C}_1(y)^{e_1} \cdot \cdots \cdot \mathscr{C}_r(y)^{e_r}$ *be the factorization of* $\mathscr{C}_P(y)$ *into irreducible factors. Then*

$$P\mathscr{O}_{\mathbf{K}} = Q_1^{e_1} \cdot \cdots \cdot Q_r^{e_r},$$

here $Q_i = (P, J_i)$, *where* $J_i = \operatorname{cont}(\tilde{\mathscr{C}}_i(\omega))$ *and* $\tilde{\mathscr{C}}_i(y)$ *is any monic polynomial in* $\mathscr{O}_{\mathbf{F}}[u_1, \ldots, u_n][y]$ *representing* $\mathscr{C}_i(y)$. *Also,* $f(Q_i|P) = \deg \mathscr{C}_i(y)$.

Proof. Let $Q_1^{e_1} \cdot \cdots \cdot Q_r^{e_r}$ be the prime decomposition of $P\mathscr{O}_{\mathbf{K}}$; we observe that the factorization of $\mathscr{C}_P(y)$ has the same form. In fact, let $I_1, I_2 \subset \mathscr{O}_{\mathbf{K}}$ be ideals such that $P\mathscr{O}_{\mathbf{K}} \subset I_1 I_2$, and consider the following diagram:

$$\begin{array}{ccccccccc} 0 & \to & \frac{\mathscr{O}_{\mathbf{K}}}{I_1}(u_1, \ldots, u_n) & \xrightarrow{\iota} & \frac{\mathscr{O}_{\mathbf{K}}}{I_1 I_2}(u_1, \ldots, u_n) & \xrightarrow{\pi} & \frac{\mathscr{O}_{\mathbf{K}}}{I_2}(u_1, \ldots, u_n) & \to & 0 \\ & & \downarrow \phi_{I_1} & & \downarrow \phi_{I_1 I_2} & & \downarrow \phi_{I_2} & & \\ 0 & \to & \frac{\mathscr{O}_{\mathbf{K}}}{I_1}(u_1, \ldots, u_n) & \xrightarrow{\iota} & \frac{\mathscr{O}_{\mathbf{K}}}{I_1 I_2}(u_1, \ldots, u_n) & \xrightarrow{\pi} & \frac{\mathscr{O}_{\mathbf{K}}}{I_2}(u_1, \ldots, u_n) & \to & 0 \end{array}$$

where ι and π are the obvious maps. The rows are exact sequences of $(\mathscr{O}_{\mathbf{F}}/P)(u_1, \ldots, u_n)$-vector spaces of finite dimension, the ϕ's are $(\mathscr{O}_{\mathbf{F}}/P)(u_1, \ldots, u_n)$-linear maps, and the diagram is clearly commutative; so we have that

$$\mathscr{C}_{I_1 I_2}(y) = \mathscr{C}_{I_1}(y)\mathscr{C}_{I_2}(y)$$

for any I_1, I_2 (see [3, p. 548]), i.e., the characteristic polynomial is multiplicative. Hence,

$$\mathscr{C}_P(y) = \mathscr{C}_{Q_1}(y)^{e_1} \cdot \cdots \cdot \mathscr{C}_{Q_r}(y)^{e_r}. \tag{6}$$

Moreover, Lemmas 1 and 2 imply that (6) is the factorization of $\mathscr{C}_P(y)$ into distinct irreducible factors.

It remains to show that $Q_i = (P, J_i)$. By definition of J_i it follows that $P \subset (P, J_i) \subset Q_i$; on the other hand,

$$\tilde{\mathscr{C}}_{Q_i}(\omega) \not\equiv 0 \pmod{Q_i Q_j}$$

(this follows from Lemma 3, if $i = j$, and from Lemmas 1 and 2, if $i \neq j$); hence $Q_i = (P, J_i)$. □

As already observed, our result generalizes Kummer's theorem; in fact, the homogeneous form $\mathscr{C}_P$ can be seen as a homogenized polynomial in n variables, hence if $\mathscr{O}_{\mathbf{K}} = \mathscr{O}_{\mathbf{F}}[\alpha]$, we have to factor a polynomial in one variable.

We finally remark that this theorem, with the same proof, holds in the more general case of finite integral extensions of Dedekind domains, provided that the residue field $\mathscr{O}_{\mathbf{F}}/P$ is finite.

Acknowledgments

I wish to thank Professor R. Dvornicich and the referee for their valuable suggestions.

Bibliography

1. K. Hensel, *Untersuchung der Fundamentalgleichung einer Gattung für eine reelle Primzahl als Modul und Bestimmung der Theiler ihrer Discriminante*, J. Reine Angew. Math. **113** (1894), 61–83.
2. L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, J. Reine Angew. Math. **92** (1882), 1–122; Werke 2, 237–387.

3. S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1984.
4. D. A. Marcus, *Number fields*, Springer-Verlag, New York, 1977.
5. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, PWN-Polish Scientific Publishers, Warszawa, 1990.

SCUOLA NORMALE SUPERIORE, PIAZZA DEI CAVALIERI 7, I-56126 PISA, ITALY
E-mail address: ilaria@ipisnsva.bitnet