THE THEOREM OF DEDEKIND IN THE IDEAL THEORY OF ZOLOTAREV*

BY

H. T. ENGSTROM†

I. INTRODUCTION

Let $K(\theta)$ be the algebraic field generated by a root θ of the irreducible equation

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0$$

and let p be a rational prime. The theorem of Dedekind on the connection between ideals and higher congruences which is fundamental in the theory of algebraic numbers is the following:

THEOREM 1. *If p is not a divisor of the index of θ, and*

$$f(x) \equiv \Phi_1(x)^{e_1}\cdot \Phi_2(x)^{e_2} \cdots \Phi_r(x)^{e_r} \pmod{p}$$

is the decomposition of $f(x)$ in prime functions (mod p) *then*

$$p = \mathfrak{p}_1^{e_1}\cdot\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_r^{e_r}$$

is the prime ideal decomposition of p in $K(\theta)$, and $N\mathfrak{p}_i = p^{f_i}$ where f_i is the degree of $\Phi_i(x)$. Furthermore

$$\mathfrak{p}_i = (p, \Phi_i(\theta)).$$

This theorem was first used by Zolotarev‡ in 1874 as a definition of ideals. This definition is not general on account of the exceptional character of the index divisors, for the ideal decomposition on this definition depends on the particular equation used to define the field. Dedekind first attempted to establish a definition of ideals in terms of the equation defining the field, but for a general theory he was forced to his abstract definition which is now classical.§ He proved Theorem 1 on this basis in 1878.¶ Zolotarev also gave

* Presented to the Society, November 29, 1930; received by the editors in January, 1930.

† National Research Fellow, California Institute of Technology.

‡ G. Zolotarev, *Théorie des nombres entiers complexes, avec une application au calcul intégral*, Bulletin de l'Académie des Sciences, St. Petersburg, 1874. Abstracted in Fortschritte der Mathematik, vol. 6 (1874), p. 177.

§ Dirichlet, *Vorlesungen über Zahlentheorie*, edited by Dedekind, 4th edition, §72–85 and §141.

¶ R. Dedekind, *Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen*, Göttinger Abhandlungen, 1878, p. 15.

up his attempt to define ideals directly in terms of the equation defining the field and in 1880[*] he succeeded in giving a general definition. On the basis of this definition Theorem 1 is no longer obvious. In the following paper I give a simple proof of the theorem by first developing the theory of congruences for ideal moduli in terms of the Zolotarev ideals.

The problem of determining the prime ideal decomposition of a rational prime p in the general case was solved by Kronecker's theory of forms.[†] Hensel[‡] in 1894 showed that in this theory there exists an analogy to the Theorem of Dedekind which is valid for all primes. The calculation of the prime ideal decomposition by this method, however, is based on an integral base of the field. In the Zolotarev theory the ideal decomposition may also be calculated for any p from an integral base of the field.[§] The problem of determining the ideal decomposition of p directly from the equation defining the field is solved by the Theorem of Ore.[||] In a later paper I shall establish these results directly from the Zolotarev definition.

II. Fundamental definitions and theorems on Zolotarev ideals

Greek letters are used to represent the integers of an algebraic field K of nth degree. Italic letters represent rational integers and p a rational prime.

DEFINITION 1. *ω_1 is said to divide ω_2* (mod p)*if there exists a c, prime to p, such that $c\cdot\omega_2/\omega_1$ is an integer of K.*

The notation $\omega_1|\omega_2$ will be used to denote the divisibility of ω_2 by ω_1 (mod p).

DEFINITION 2. *If $\epsilon|1$ then ϵ is a unit* (mod p).

DEFINITION 3. *If $\omega_1|\omega_2$ and $\omega_2|\omega_1$ then ω_1 and ω_2 are called associates* (mod p).

In questions of divisibility (mod p) associates are not regarded as distinct.

[*] G. Zolotarev, *Sur la théorie des nombres complexes*, Journal de Mathématiques, (3), vol. 6 (1880), pp. 51–84, 129–166. For a modern account of the theory see N. Tchebotarev, *The foundations of the ideal theory of Zolotarev*, American Mathematical Monthly, vol. 37 (1930), pp. 117–128.

[†] L. Kronecker, *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*, Journal für Mathematik, vol. 92 (1882), pp. 1–122.

[‡] K. Hensel, *Untersuchungen der Fundamentalgleichung einer Gattung für reelle Primzahl als Modul und Bestimmung der Theiler ihrer Diskriminante*, Journal für Mathematik, vol. 113 (1894), pp. 61–83.

[§] Cf. N. Tchebotarev, loc. cit.

[||] Ö. Ore, *Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern*, Mathematische Annalen, vol. 98 (1927), Theorem 9, p. 585.

DEFINITION 4. *If π is not a unit* (mod p) *and $\pi|\omega_1\omega_2$ only when $\pi|\omega_1$ or $\pi|\omega_2$ then π is said to be a prime* (mod p).

THEOREM 2. *Each integer in K has a unique decomposition in primes* (mod p).

THEOREM 3. *There exists a complete residue system* (mod p) *in K,*

$$\alpha_0 = p, \alpha_1, \quad \alpha_2, \cdots, \alpha_\sigma \quad (\sigma = p^n - 1), \tag{1}$$

such that $\alpha_i|p$, $i=1, 2, \cdots, \sigma$.

THEOREM 4. *All prime divisors* (mod p) *of p are contained in the set* (1).

DEFINITION 5. *For each rational prime p, to each prime divisor π*(mod p) *we associate a symbol $\mathfrak{P}$, called a prime ideal divisor, and say that an integer ω contains the ideal divisor $\mathfrak{P}^k$ if ω is divisible* (mod p) *by π^k.*

Corresponding to each rational prime dividing $N(\omega)$ as a modulus, ω will contain certain ideal divisors. We write ω symbolically as the product of all ideal divisors contained in ω, i.e.,

$$\omega = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\ \mathfrak{P}_r^{e_r}.$$

THEOREM 5. *Each integer in K has a unique decomposition in prime ideal divisors.*

An integer ω of the field is determined to an absolute algebraic unit by its divisors for the rational primes which divide its norm as moduli. Theorem 5 is a symbolic statement that a representation of an integer ω by its divisors for the rational primes dividing $N(\omega)$ as moduli is unique (cf. Tchebotarev, loc. cit. p. 125).

DEFINITION 6. *If $\mathfrak{P}$ is the prime ideal divisor associated with the prime divisor π* (mod p), *the power of p dividing $N(\pi)$ is called the norm, $N(\mathfrak{P})$, of $\mathfrak{P}$.*

DEFINITION 7. *The norm of a product of prime ideal divisors is the product of the norms of the factors.*

III. CONGRUENCES FOR IDEAL MODULI

Let $\omega_1, \omega_2, \cdots, \omega_n$ be an integral base of K and π an arbitrary integer of K. Then

$$\pi\cdot\omega_j = a_{1j}\omega_1 + a_{2j}\omega_2 + \cdots + a_{nj}\omega_n \qquad (j = 1, 2, \cdots, n), \tag{2}$$

where $N(\pi) = \pm|a_{ij}|$. We determine a normal base for multiples of π as follows. Of all multiples of π in the form

$$c_1\omega_1 + c_2\omega_2 + \cdots + c_i\omega_i, \quad c_i \neq 0, \tag{3}$$

let Ω_i be that for which $|c_i|$ is least. Since $N(\pi)\omega_i$ is of the form (3) such integers exist. We obtain the set

$$\begin{aligned} \Omega_1 &= b_{11}\omega_1, \\ \Omega_2 &= b_{21}\omega_1 + b_{22}\omega_2, \\ &\cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot\ \cdot \\ \Omega_n &= b_{n1}\omega_1 + b_{n2}\omega_2 + \cdots + b_{nn}\omega_n. \end{aligned} \tag{4}$$

It is readily shown that every multiple of π in K is a linear combination of $\Omega_1, \Omega_2, \cdots, \Omega_n$ with rational coefficients and conversely. Furthermore, if a multiple of π has the form (3) then $c_i \equiv 0 \pmod{b_{ii}}$. Since the integers (2) also form a base for multiples of π, the determinants $|a_{ij}|$ and $|b_{ij}|$ are each divisible by the other, i.e., $N(\pi) = \pm b_{11} \cdot b_{22} \cdots b_{nn}$.

Suppose that π is a prime $\pmod{p}$ and that $\mathfrak{P}$ is the prime ideal divisor associated with π. Let $N(\mathfrak{P}) = p^f$, i.e., $N(\pi) = p^f q$ where $(p, q) = 1$. We prove the following lemmas:

Lemma 1. *If* $\omega_i \equiv 0 \pmod{\mathfrak{P}}$ *then* $b_{ii} \not\equiv 0 \pmod{p}$.

For if $\omega_i \equiv 0 \pmod{\mathfrak{P}}$ there exists a c, prime to p, such that $c\omega_i$ is a multiple of π. Hence $c \equiv 0 \pmod{b_{ii}}$ and therefore $b_{ii} \not\equiv 0 \pmod{p}$.

Lemma 2. $b_{ii} \not\equiv 0 \pmod{p^2}$, $i = 1, 2, \cdots, n$.

For since $\pi | p$ there exists a c, prime to p, such that cp, and hence $cp\omega_i$, is a multiple of π. Hence $cp \equiv 0 \pmod{b_{ii}}$ and therefore $b_{ii} \not\equiv 0 \pmod{p^2}$.

From Lemmas 1 and 2 we obtain the following theorem:

Theorem 6. *If* $N(\pi) = p^f q$, $(p, q) = 1$, *precisely* f *of the integers* $b_{11}, b_{22}, \cdots, b_{nn}$ *are divisible by* p.

Let $\omega_{i_1}, \omega_{i_2}, \cdots, \omega_{i_n}$ be the basis integers for which $b_{ii} \equiv 0 \pmod{p}$ retaining the order in (4). We have the following theorem:

Theorem 7. *If* α *is a linear combination of* $\omega_{i_1}, \omega_{i_2}, \cdots, \omega_{i_f}$ *with rational coefficients, then*

$$\alpha = c_1\omega_{i_1} + c_2\omega_{i_2} + \cdots + c_f\omega_{i_f} \equiv 0 \pmod{\mathfrak{P}} \tag{5}$$

if and only if

$$c_1\omega_{i_1} + c_2\omega_{i_2} + \cdots + c_f\omega_{i_f} \equiv 0 \pmod{p}. \tag{6}$$

For if $\alpha \equiv 0 \pmod{\mathfrak{P}}$ there exists a c, prime to p, such that $c\alpha$ is a multiple of π. Hence $c \cdot c_f \equiv 0 \pmod{b_{i_f i_f}}$ and therefore $c_f \equiv 0 \pmod{p}$. Since $\pi | p$ it follows that

$$c_1\omega_{i_1} + c_2\omega_{i_2} + \cdots + c_{f-1}\omega_{i_{f-1}} \equiv 0 \qquad (\text{mod } \mathfrak{P}).$$

Hence $c_{f-1} \equiv 0$ (mod p). Continuing in this way we obtain (6).

THEOREM 8. *Every integer ω in K satisfies a congruence of the form*

$$\omega \equiv c_1\omega_{i_1} + c_2\omega_{i_2} + \cdots + c_f\omega_{i_f} \qquad (\text{mod } \mathfrak{P}). \tag{7}$$

If $b_{ii} \not\equiv 0$ (mod p) we may choose a d_i such that $d_ib_{ii} \equiv 1$ (mod p). Multiplying Ω_i in (4) by d_i we obtain, since $\Omega_i \equiv 0$ (mod $\mathfrak{P}$),

$$\omega_i \equiv r_1\omega_1 + r_2\omega_2 + \cdots + r_{i-1}\omega_{i-1} \qquad (\text{mod } \mathfrak{P}).$$

Hence, by successive elimination of the ω_i's for which $b_{ii} \not\equiv 0$ (mod p) from the expression for ω in terms of the basis integers, we obtain (7).

From Theorems 7 and 8 we obtain immediately

THEOREM 9. *The norm of a prime ideal divisor $\mathfrak{P}$ is equal to the number of incongruent residue classes* (mod $\mathfrak{P}$) *of integers in K.*

To extend Theorem 9 to any ideal divisor we prove the following lemma:

LEMMA 3. *The number of incongruent classes* (mod $\mathfrak{M}\cdot\mathfrak{N}$) *is equal to the product of the number of classes* (mod $\mathfrak{M}$) *and the number of classes* (mod $\mathfrak{N}$).

For we may determine an integer μ of K divisible by $\mathfrak{N}$ such that $\mu/\mathfrak{N}$ is prime to $\mathfrak{M}$.* Then, if η_i and ζ_i run over a complete residue system (mod $\mathfrak{M}$) and (mod $\mathfrak{N}$) respectively, the integers $\eta_i\mu+\zeta_i$ form a complete residue system (mod $\mathfrak{M}\cdot\mathfrak{N}$) as may be shown in the usual way. Using Definition 7 we obtain the following theorem:

THEOREM 10. *The norm of an ideal divisor $\mathfrak{M}$ is equal to the number of incongruent classes* (mod $\mathfrak{M}$) *of integers in K.*

The theorems on congruences for ideal moduli in Section 8 of Hilbert's report† follow directly.

IV. THE THEOREM OF DEDEKIND

Let θ be a primitive integer of K and a root of the equation

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n = 0. \tag{8}$$

If $\omega_1, \omega_2, \cdots, \omega_n$ is an integral base of K and

$$\theta^{i-1} = a_{1i}\omega_1 + a_{2i}\omega_2 + \cdots + a_{ni}\omega_n \qquad (i = 1, 2, \cdots, n), \tag{9}$$

* The existence of μ follows from the independence theorem of Tchebotarev, loc. cit., p. 127.

† D. Hilbert, Jahresbericht der Deutschen Mathematiker-Vereinigung, vol. 4 (1894–95), pp. 191–192.

we have

$$D_\theta = k_\theta^2 d$$

where D_θ is the discriminant of θ, d is the discriminant of K, and $k_\theta = |a_{ij}|$ is the index of θ. By solving (9) for $\omega_1, \omega_2, \cdots, \omega_n$ we obtain the following theorem:

THEOREM 11. *Every integer ω in K can be expressed in the form*

$$\omega = \frac{b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1}}{k_\theta}.$$

The following theorem follows from Definition 3:

THEOREM 12. *If p does not divide k_θ then every integer of K is associate* (mod p) *to a polynomial in θ.*

THEOREM 13. *If $F(x)$ and $G(x)$ are relatively prime* (mod p), *then $F(\theta)$ and $G(\theta)$ are relatively prime* (mod p).

For if $F(x)$ and $G(x)$ are relatively prime (mod p) there exist polynomials $A(x)$ and $B(x)$ such that

$$A(x)F(x) + B(x)G(x) \equiv 1 \qquad (\text{mod } p)$$

and hence

$$A(\theta)F(\theta) + B(\theta)G(\theta) \equiv 1 \qquad (\text{mod } p).$$

Since all primes (mod p) divide p (mod p) it follows that any common divisor of $F(\theta)$ and $G(\theta)$ must be a unit (mod p).

DEFINITION 8. *By Theorems* 3 *and* 12 *we may choose any prime function $\phi(x)$* (mod p) *in such a way that $\phi(\theta)|p$. We shall call such prime functions "normal."*

THEOREM 14. *If p does not divide k_θ and $\phi(x)$ is a normal prime function* (mod p) *then $\phi(\theta)$ is either a prime or a unit* (mod p).

Every polynomial $F(x)$ is either prime (mod p) to $\phi(x)$ or divisible (mod p) by $\phi(x)$. In the first case $F(\theta)$ is prime (mod p) to $\phi(\theta)$. In the second case $F(\theta)$ is divisible (mod p) by $\phi(\theta)$, for we have

$$F(\theta) = \phi(\theta)G(\theta) + pH(\theta),$$

and since $\phi(\theta)|p$, it follows that $\phi(\theta)|F(\theta)$. Hence every integer in K is either divisible by $\phi(\theta)$ or prime to it and, by Definition 2, it follows that $\phi(\theta)$ is either a prime or a unit (mod p).

THEOREM 15. *If p does not divide k_θ and $\phi(x)$ is a normal prime function* (mod p) *of fth degree, then* $N(\phi(\theta)) \not\equiv 0$ (mod p^{f+1}).

Suppose that $N(\phi(\theta)) \equiv 0$ (mod p). Then $\phi(\theta)$ is not a unit (mod p) and hence is a prime (mod p). Let $\mathfrak{P}$ be the prime ideal divisor associated with the prime divisor $\phi(\theta)$. We have

$$\phi(\theta) = \theta^f + c_1\theta^{f-1} + \cdots + c_f \equiv 0 \qquad (\text{mod } \mathfrak{P}).$$

Hence, from Theorem 12, any integer ω in K satisfies a congruence of the form

$$\omega \equiv b_1\theta^{f-1} + b_2\theta^{f-2} + \cdots + b_f \qquad (\text{mod } \mathfrak{P}).$$

Since $p \equiv 0$ (mod $\mathfrak{P}$), it follows that the number of incongruent classes of integers in K is less than or equal to p^f, i.e., $N(\mathfrak{P}) \leqq p^f$. Hence, by Definition 6, $N(\phi(\theta)) \not\equiv 0$ (mod p^{f+1}).

We are now prepared to prove the anologue of Dedekind's theorem:

THEOREM 16. *If p does not divide k_θ and*

$$f(x) \equiv \phi_1(x)^{e_1}\phi_2(x)^{e_2} \cdots \phi_r(x)^{e_r} \qquad (\text{mod } p)$$

where $\phi_i(x)$ is a normal prime function (mod p) *of degree f_i, $i=1, 2, \cdots, r$, then*

$$cp = \epsilon\cdot\phi_1(\theta)^{e_1}\cdot\phi_2(\theta)^{e_2} \cdots \phi_r(\theta)^{e_r}, \tag{10}$$

where $(c, p)=1$ and ϵ is a unit (mod p), *is the decomposition of p in distinct prime divisors* (mod p).

For let

$$f(x) = \phi_1(x)^{e_1}\phi_2(x)^{e_2} \cdots \phi_r(x)^{e_r} + pM(x).$$

Then

$$-pM(\theta) = \phi_1(\theta)^{e_1}\phi_2(\theta)^{e_2} \cdots \phi_r(\theta)^{e_r}.$$

Taking the norm of both sides we have

$$-p^nN(M(\theta)) = N(\phi_1(\theta))^{e_1}N(\phi_2(\theta))^{e_2} \cdots N(\phi_r(\theta))^{e_r}.$$

Since $\sum_{i=1}^{r} e_if_i = n$, it follows from Theorem 15 that $N(M(\theta)) \not\equiv 0$ (mod p) and furthermore $N(\phi_i(\theta)) \equiv 0$ (mod p^{f_i}). Hence $\phi_i(\theta)$, $i=1, 2, \cdots, r$, is a prime (mod p) and furthermore, by Theorem 13, $\phi_i(\theta)$ and $\phi_j(\theta)$ are distinct (mod p) for $i\neq j$. Also, $M(\theta)$ is a unit (mod p) and there exists a c, prime to p, such that $c/M(\theta) = \epsilon$ is a unit (mod p) and (10) follows.

Expressed in terms of the ideal divisors of Zolotarev, Theorem 16 becomes

THEOREM 17. *Under the hypothesis of Theorem* 16,

$$p = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_r^{e_r},\quad N(\mathfrak{P}_i) = p^{f_i},$$

where $\mathfrak{P}_i$ *is a prime ideal divisor associated with the normal prime divisor* $\phi_i(\theta)$ (mod p), $i=1, 2, \cdots, r$.

To express this theorem in the form of Theorem 1 we must remove the condition of normalcy of the divisors $\phi_i(x)$. Suppose that

$$f(x) \equiv \prod_{i=1}^{r}\Phi_i(x)^{e_i} \qquad (\text{mod } p)$$

is a decomposition of $f(x)$ satisfying the conditions of Theorem 1. By Theorems 3 and 12 there exists a prime function decomposition

$$f(x) \equiv \prod_{i=1}^{r}\phi_i(x)^{e_i} \qquad (\text{mod } p)$$

in which the $\phi_i(x)$ are all normal and

$$(11)\qquad \phi_i(x) \equiv \Phi_i(x) \qquad (\text{mod } p;\ i = 1, 2, \cdots, r).$$

This may also be shown directly as follows. Suppose

$$f(x) = \prod_{i=1}^{r}\Phi_i(x)^{e_i} + pM(x).$$

Since we have supposed that p is not an index divisor it follows by a criterion due to Dedekind* that if $e_i>1$ then $M(x)\not\equiv 0$ (modd p, $\Phi_i(x)$). Now let

$$P_i(x) = \left[\prod_{j=1}^{r}\Phi_j(x)^{e_j}\right]\Big/\Phi_i(x) \qquad (i = 1, 2, \cdots, r).$$

We distinguish two types of $\Phi(x)$, (1) those for which $M(x)\equiv 0$ (modd p, $\Phi_i(x)$) and (2) those for which $M(x)\not\equiv 0$ (modd p, $\Phi_i(x)$). If $\Phi_i(x)$ is of type (1) we write $\phi_i(x)=\Phi_i(x)+pP_i(x)$, if $\Phi_i(x)$ is of type (2) we write $\phi_i(x)=\Phi_i(x)$. Then

$$(12)\qquad f(x) = \prod_{i=1}^{r}\phi_i(x)^{e_i} + pM'(x),$$

where $M'(x)\equiv -[P_i(x)]^2$ (modd p, $\Phi_i(x)$) in case (1) and $M'(x)\equiv M(x)$ (modd p, $\Phi_i(x)$) in case (2). Hence $M'(x)\not\equiv 0$ (modd p, $\Phi_i(x)$), $i=1, 2, \cdots r$,

* Cf. P. Bachmann, *Allgemeine Arithmetik der Zahlenkörper*, Leipzig, 1926, p. 277.

i.e., $M'(x)\not\equiv 0$ (modd p, $\phi_i(x)$). Setting $x=\theta$ in (12) we see that $\phi_i(\theta)^{e_i}|p$, $i=1, 2, \cdots, r$, i.e., all the $\phi_i(x)$ are normal.

If $e_i>1$, it follows from (11) that $\Phi_i(\theta)$ is divisible (mod p) by precisely the first power of $\phi_i(\theta)$ and by no other divisors of p. Hence we may write $\phi_i(\theta)$ as the greatest common divisor (mod p) of p and $\Phi_i(\theta)$; symbolically, $\mathfrak{P}_i=(p, \Phi_i(\theta))$. If $e_i=1$, then p will contain precisely the first power of $\phi_i(\theta)$ and again $\mathfrak{P}_i=(p, \Phi_i(\theta))$. Hence we have Theorem 1.

California Institute of Technology,
Pasadena, Calif.