International Journal of Current Research and Modern Education (IJCRME)
Impact Factor: 6.725, ISSN (Online): 2455 - 5428
(www.rdmodernresearch.com) Volume 2, Issue 2, 2017

SPLITTING OF RATIONAL PRIMES IN THE RING OF ALGEBRAIC INTEGERS

Rahul Arora
Chhawani Mohalla, Near Pipal Chowk, Ludhiana, Punjab

Cite This Article: Rahul Arora, "Splitting of Rational Primes in the Ring of Algebraic Integers", International Journal of Current Research and Modern Education, Volume 2, Issue 2, Page Number 28-29, 2017.

Abstract:

We know that the primes in Z (hereafter referred as rational primes) are irreducible in Z i.e they don't have proper factorization. If R is any factorization domain such that Z is properly contained in R then are these rational primes also irreducible in R? The answer to this question in general is No. For example, 2 is prime in Z but 2 is not prime in Z[i] as we can write 2 as: 2 = (1 + i)(1 – i) where both 1 + i & 1 – i are irreducible (rather non units) in Z[i]. In this paper we will see how the rational primes spilt in the ring of algebraic integers.

Key Words: Algebraic Number Field, Integral Basis, Discriminant & Ramify

1. Introduction:

An Algebraic number field is a subfield of C (field of complex numbers) of the form Q(α_1,α_2,…..α_n), where α_1,α_2,…..α_n are algebraic numbers. Let K be an algebraic number field. A basis for O_K is called an integral basis for K. Let {α_1,α_2,…..α_n} be an integral basis for K. Then D(α_1,α_2,…..α_n) is called the discriminant of K and is denoted by d(K) or d_K. Moreover, in any algebraic number field K, every proper integral ideal of O_K can be expressed uniquely up to order as a product of prime ideals. Let p be a rational prime. Suppose <p> factors in O_K as <p>= $P_1^{e_1}P_2^{e_2} \dots \dots P_g^{e_g}$, where $P_1, P_2 \dots \dots P_g$ are distnict prime ideals of O_K lying above p where, $e_i = e_K(P_i)$; i = 1,2,…,g. If $e_i > 1$ for some i ∊ {1,2,….,g} then p is said to be ramify in K.

Definition 1.1: (Basis of an Ideal)

Let K be an algebraic number field of degree n. Let I be a nonzero ideal of O_K . If { α_1,α_2,…..α_n} is a set of elements of I such that every element β∊ I can be expressed uniquely in the form as β = $x_1\alpha_1 + x_2\alpha_2 \dots \dots .. + x_n\alpha_n$ where x_1,x_2,…..,x_n ∊ Z then { α_1,α_2,…..α_n} is called a basis for the ideal I.

Definition 1.2: (Discriminant of n Elements in an Algebraic Number Field of Degree n)

Let K be an algebraic number field of degree n. Let α_1,α_2,…..,α_n be n elements of the field K. Let σ_k ; 1 ≤ k ≤ n denote the n distnict monomorphisms from K to C. For i = 1,2,….,n let $\alpha_i^{(1)} = \sigma_1(\alpha_i) = \alpha_i$, $\alpha_i^{(2)} = \sigma_2(\alpha_i)$,……, $\alpha_i^{(n)} = \sigma_n(\alpha_i)$ denote the conjugate of α_i relative to K. Then the discriminant of { α_1,α_2,…..α_n} is

$$D(\alpha_1,\alpha_2,\dots\alpha_n) = \left(det \begin{bmatrix} \alpha_1^{(1)} & \cdots & \alpha_n^{(1)} \\ \vdots & \ddots & \vdots \\ \alpha_1^{(n)} & \cdots & \alpha_n^{(n)} \end{bmatrix} \right)^2$$

Definition 1.3: (Discriminant of an Ideal)

Let K be an algebraic number field of degree n. Let I be an nonzero ideal of O_K . Let { α_1,α_2,…..α_n} be a basis of I. Then the discriminant D(I) of the ideal I is the nonzero integer given by D(I) = D(α_1,α_2,…..α_n).

Definition 1.4: (Index of θ)

Let K be an algebraic number field of degree n. Let θ∊ K be such that K = Q(θ). Then the index of θ,denoted by ind(θ) is the positive integer given by D(θ) = D(1, θ, θ^2, ….,θ^n) = $(ind(\theta))^2$ d(K).

Note that if D(θ) is square free then ind(θ) = 1 and D(θ) = d(K). Thus {1, θ, θ^2, ….,θ^n} is an integral basis for K.

2. Main Section:

Let θ be a root of $x^4 + x + 1 = 0$. Let $f(x) = x^4 + x + 1$, is monic and irreducible over Z. [K:Q] = 4.

Theorem 2.1:

Let a , b be integers such that $x^4 + ax + b$ is irreducible over Z. Let θ be a root of $x^4 + ax + b$ so that K = Q(θ) is a quartic field and θ∊ O_K. Then, D(θ) = $-27a^4 + 256b^3$

As a = b = 1. Thus, D(θ) = -27 + 256 = 229. Since D(θ) is square free. Therefore, d_K = D(θ).

Hence {1, θ, θ^2, θ^3 } is an integral basis of K.

Theorem 2.2:

Let K be an algebraic number field with [K:Q] = n. Let p be a rational prime. Suppose <p> factors in O_K as <p>= $P_1^{e_1}P_2^{e_2} \dots \dots P_g^{e_g}$, where $P_1, P_2 \dots \dots P_g$ are distnict prime ideals of O_K. Suppose that f_i is the inertial degree of P_i in K. Then, $e_1f_1 + e_2f_2 \dots \dots .. + e_gf_g$ = n

Note that g ≤ n

In present case, g ≤ 4

If g = 4: $e_1f_1 + e_2f_2 + e_3f_3 + e_4f_4 = 4$
i.e $e_1 = f_1 = e_2 = f_2 = e_3 = f_3 = e_4 = f_4 = 1$
Thus, <p>= $P_1P_2P_3P_4$; $N(P_i) = p$
If g = 3 : $e_1f_1 + e_2f_2 + e_3f_3 = 4$
Wlog, assume that $e_1f_1 = 2$ and $e_2f_2 = e_3f_3 = 1$
$(e_1, f_1) = (1,2)$, (2,1) and $e_2 = f_2 = e_3 = f_3 = 1$
Thus, <p>= $P_1P_2P_3$; $N(P_1) = p^2$, $N(P_2) = N(P_3) = p$
Or
<p>= $P_1^2P_2P_3$; $N(P_1) = N(P_2) = N(P_3) = p$
If g = 2 : $e_1f_1 + e_2f_2 = 4$
$(e_1, f_1) = (1, 2)$, (2,1) and $(e_2, f_2) = (1,2), (2,1)$
Thus, <p>= P_1P_2 ; $N(P_1) = p^2 = N(P_2)$
Or
<p>= $P_1^2P_2$; $N(P_1) = p$, $N(P_2) = p^2$
Or
<p> = $P_1P_2^2$; $N(P_2) = p$, $N(P_1) = p^2$
Or
<p>= $P_1^2P_2^2$; $N(P_1) = N(P_2) = p$
Wlog, assume that $(e_1, f_1) = 3$ and $(e_2, f_2) = 1$
$(e_1, f_1) = (1, 3)$, (3,1) and $e_2 = f_2 = 1$
Thus ,<p> = P_1P_2 ; $N(P_1) = p^3$, $N(P_2) = p$
Or
<p>= $P_1^3P_2$; $N(P_1) = N(P_2) = p$
If g = 1: $e_1f_1 = 4$
$(e_1, f_1) = (1, 4)$, (4,1)
Thus ,<p> = P_1 ; $N(P_1) = p^4$
Or
<p>= P_1^4 ; $N(P_1) = p$
Let us see how rational primes spilt in O_K

Theorem 2.3:

Let K = Q(θ) be an algebraic number field of degree n such that $O_K = Z[\theta]$. Let p be a rational prime, let $f(x) = irr_Q\theta \in Z[x]$. Let – denote the natural map : $Z[x] \rightarrow Z_p[x]$ where $Z_p = Z/pZ$. Let $\bar{f}(x) = g_1^{e1}(x)\, g_2^{e2}(x)\ldots\ldots g_r^{er}(x)$ where $g_i(x)$ are distnictmonic irreducibles in $Z_p[x]$, $1 \le i \le r$ and $e_1, e_2, \ldots, e_r$ are positive integers. For i = 1,2,…,r, let $f_i(x)$ be any monic polynomial of Z[x] such that $\bar{f_i} = g_i$. Set P_i = <p, $f_i(\theta)$> ; i = 1,2,…,r. Then $P_1, P_2, \ldots, P_r$ are distnict prime ideals of O_K with <p> = $P_1^{e1}P_2^{e2} \ldots\ldots P_r^{e_r}$ and $N(P_i) = p^{deg\, f_i}$; $1 \le i \le r$.

For p = 2, Since $x^4 + x + 1$ is irreducible over Z_2.
Set P = < 2, $\theta^4 + \theta + 1$> but $\theta^4 + \theta + 1 = 0$
Thus P = <2> ; N(P) = 16 and 2 will remain as prime in O_K
For p = 3, $x^4 + x + 1 = (x - 1)(x^3 + x^2 + x + 2)$ over $Z_3[x]$ and $x^3 + x^2 + x + 2$ is irreducible over Z_3
Set P_1 = <3, θ - 1> ; $N(P_1) = 3$
Set P_2 = <3, $\theta^3 + \theta^2 + \theta + 2$> ; $N(P_2) = 27$
Thus, <3> = P_1P_2
For p = 5, $x^4 + x + 1 = (x - 3)(x^3 + 3x^2 + 4x + 3)$ over $Z_5[x]$ and $x^3 + 3x^2 + 4x + 3$ is irreducible over Z_5
Set P_1 = <5, θ - 3> ; $N(P_1) = 5$
Set P_2 = <5 , $\theta^3 + 3\theta^2 + 4\theta + 3$> ; $N(P_2) = 125$
Thus <5> = P_1P_2

Theorem 2.4:

Let K be an algebraic number field. Then the rational prime ramifies in K iff p divides d_K
As d_K = 229 which is a rational prime i.e p = 229 ramifies in O_K
For p = 229, $x^4 + x + 1 = (x - 75)^2 (x^2 + 150x + 158)$ over $Z_{229}[x]$ and $x^2 + 150x + 158$ is irreducible over Z_{229}
Set P_1 = <229, θ - 75> ; $N(P_1) = 229$
Set P_2 = <229, $\theta^2 + 150\theta + 158$ > ; $N(P_2) = (229)^2$
Thus <229> = $P_1^2P_2$

3. References:

1. Saban Alaca and Kenneth S. Williams, Introductory Algebraic Number Theory, Cambridge University Press.