International Journal of Applied and Advanced Scientific Research (IJAASR)
Impact Factor: 5.255, ISSN (Online): 2456 - 3080
(www.dvpublication.com) Volume 2, Issue 2, 2017

BEHAVIOUR OF RATIONAL PRIMES IN THE RING OF ALGEBRAIC INTEGERS

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

Cite This Article: Rahul Arora, "Behaviour of Rational Primes in the Ring of Algebraic Integers", International Journal of Applied and Advanced Scientific Research, Volume 2, Issue 2, Page Number 62-64, 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, 13 is prime in Z but 13 is not prime in Z[i] as we can write 13 as: 13 = (2 + 3i)(2 – 3i) where both 2 + 3i & 2 – 3i 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, Norm, 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>= $P_1^{e_1}P_2^{e_2}\ldots\ldots P_g^{e_g}$, where $P_1, P_2 \ldots\ldots P_g$ 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 = $x_1\alpha_1 + x_2\alpha_2 \ldots\ldots. + x_n\alpha_n$ 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

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

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.

Definition 1.5: (Conjugates of θ over Q)

Let θ∈ C be any algebraic number i.eθ is a root of some monic irreducible polynomial p(x) of least degree over Q then the roots of p(x) are called the conjugates of θ over Q.

Definition 1.6: (Norm of an element θ over Q)

It is defined as product of all conjugates of θ over Q. It is denoted by $N_{K|Q}(\theta)$.

Definition 1.7: (Norm of an integral ideal)

Let K be an algebraic number field of degree n. Let I be a nonzero ideal of O_K. Then the norm of the ideal I denoted by N(I), is the positive integer defined by N(I) = $\sqrt{\frac{D(I)}{d(K)}}$

2. Main Section:

Let θ be a root of x^5- 5 = 0.

Let f(x) = x^5- 5, is monic and irreducible over Z. [K:Q] = 5 = n

Then Discriminant of θ is given by: D(θ) = $(-1)^{n(n-1)/2}$ N(f'(θ))

D(θ) = N(5θ^4) = N(5) N(θ^4) = N(5) $(N(\theta))^4$ = 5^5 5^4 = 5^9

By definition of Index of θ, possible values of ind(θ) are 1,5, 5^2, 5^3, 5^4

Theorem 2.1:

Let K = Q(θ) be an algebraic number field of degree n ≥2, where θ is an algebraic integer. If the minimal polynomial of θ satisfies Eisenstein Criteria for a rational prime p, then p does not divide the index of θ.

Since $x^5 – 5$ being the minimal polynomial of θ satisfies Eisenstein Criteria for p = 5, so 5 doesn't divide the ind(θ). Thus only possible value of ind(θ) is 1. Hence D(θ) = d(K).

Therefore $\{1, \theta, \theta^2, \theta^3, \theta^4\}$ 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, $e_1 f_1 + e_2 f_2 \dots \dots .. + e_g f_g$ = n,

Note that g ≤ n

In present case, g ≤ 5

If g = 5: $e_1 f_1 + e_2 f_2 + e_3 f_3 + e_4 f_4 + e_5 f_5 = 5$

i.e $e_1 = f_1 = e_2 = f_2 = e_3 = f_3 = e_4 = f_4 = e_5 = f_5 = 1$

Thus, <p>= $P_1 P_2 P_3 P_4 P_5$; $N(P_i) = p$

If g = 4 : $e_1 f_1 + e_2 f_2 + e_3 f_3 + e_4 f_4 = 5$

Wlog, assume that $e_1 f_1 = 2$ and $e_2 f_2 = e_3 f_3 = e_4 f_4 = 1$

$(e_1, f_1) = (1,2)$, (2,1) and $e_2 = f_2 = e_3 = f_3 = e_4 = f_4 = 1$

Thus, <p>= $P_1 P_2 P_3 P_4$; $N(P_1) = p^2$, $N(P_2) = N(P_3) = N(P_4) = p$

Or

<p>= $P_1^2 P_2 P_3 P_4$; $N(P_1) = N(P_2) = N(P_3) = N(P_4) = p$

If g = 3 : $e_1 f_1 + e_2 f_2 + e_3 f_3 = 5$

$(e_1, f_1) = (1, 2)$, (2,1) and $(e_2, f_2) = (1,2), (2,1)$ and $(e_3, f_3) = (1,1)$

Thus, <p>= $P_1 P_2 P_3$; $N(P_1) = p^2 = N(P_2)$, $N(P_3) = p$

Or

<p> $= P_1 P_2^2 P_3$; $N(P_1) = p^2$, $N(P_2) = p = N(P_3)$

Or

<p> = $P_1^2 P_2 P_3$; $N(P_1) = p = N(P_3)$, $N(P_2) = p^2$

Or

<p>= $P_1^2 P_2^2 P_3$; $N(P_1) = N(P_2) = N(P_3) = p$

Wlog, assume that $e_1 f_1 = 3$ and $(e_2, f_2) = (e_3, f_3) = (1,1)$

$(e_1, f_1) = (1, 3)$, (3,1) and $e_2 = f_2 = e_3 = f_3 = 1$

Thus ,<p> = $P_1 P_2 P_3$; $N(P_1) = p^3$, $N(P_2) = N(P_3) = p$

Or

<p>= $P_1^3 P_2 P_3$; $N(P_1) = N(P_2) = N(P_3) = p$

If g = 2: $e_1 f_1 + e_2 f_2 = 5$

$(e_1, f_1) = (1, 4)$, (4,1) and $e_2 = f_2 = 1$

Thus ,<p> = $P_1 P_2$; $N(P_1) = p^4$, $N(P_2) = p$

Or

<p>= $P_1^4 P_2$; $N(P_1) = N(P_2) = p$

Wlog, assume that $e_1 f_1 = 3$ and $e_2 f_2 = 2$

$(e_1, f_1) = (1, 3)$, (3,1) and $(e_2, f_2) = (1,2), (2,1)$

Thus, <p>= $P_1 P_2$; $N(P_1) = p^3$, $N(P_2) = p^2$

Or

<p> = $P_1 P_2^2$; $N(P_1) = p^3$, $N(P_2) = p$

Or

<p> = $P_1^3 P_2$; $N(P_1) = p$, $N(P_2) = p^2$

Or

<p> = $P_1^3 P_2^2$; $N(P_1) = N(P_2) = p$

If g = 1: $e_1 f_1 = 5$

$(e_1, f_1) = (1, 5)$, (5,1)

Thus, <p>= P_1 ; $N(P_1) = p^5$

Or

<p>= P_1^5 ; $N(P_1) = p$

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 $\bar{f}(x) = g_1^{e_1}(x)\ g_2^{e_2}(x) \dots ..$

$g_r^{e_r}$(x) where g_i(x) are distinctmonic irreducibles in Z_p[x], 1≤i≤r and e_1, e_2,.....,$e_r$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 , ……, P_r are distnict prime ideals of O_K with <p> = $P_1^{e_1} P_2^{e_2}$ … … $P_r^{e_r}$ and N(P_i) = $p^{\deg f_i}$; 1≤i≤r.

For p = 2

$x^5 - 5 = (x - 1)(x^4 + x^3 + x^2 + x + 1)$ over Z_2[x] and $x^4 + x^3 + x^2 + x + 1$ is irreducible over Z_2

Set P_1 = < 2, θ -1 > ;N(P_1) = 2

Set P_2 = < 2, $\theta^4 + \theta^3 + \theta^2 + \theta + 1$>; N($P_2$) = 2^4 = 16

Thus <2> = $P_1 P_2$

For p = 3

$x^5 - 5 = (x - 2)(x^4 + 2x^3 + x^2 + 2x + 1)$ over Z_3[x] and $x^4 + 2x^3 + x^2 + 2x + 1$ is irreducible over Z_3

Set P_1 = <3, θ - 2> ;N(P_1) = 3

Set P_2 = <3, $\theta^4 + 2\theta^3 + \theta^2 + 2\theta + 1$> ;N($P_2$) = 3^4 = 81

Thus, <3> = $P_1 P_2$

Theorem 2.4:

Let K be an algebraic number field. Then the rational prime ramifies in K iff p divides d_K. As $d_K = 5^9$ and p = 5, which is a rational prime divides d_Ki.e p = 5 ramifies in O_K

For p = 5

$x^5 - 5 = x^5$ over Z_5[x]

Set P = <5, θ>; N(P) = 5

Thus <5> = P^5

3. References:

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