Abstract

Let K = Q(θ) be an algebraic number field with θ in the ring OK of algebraic integers of K and f (x) be the minimal polynomial of θ over the field Q of rational numbers. For a rational prime p, let f (x) = g1 (x)e1 ....gr (x)er be the factorization of the polynomial f (x) obtained by replacing each coefficient of f (x) modulo p into product of powers of distinct irreducible polynomials over Z/pZ with gi (x) monic. In 1878, Dedekind proved that if p does not divide [OK : Z[θ]], then pOK = ℘1e1 ....℘rer , where ℘1 , ..., ℘r are distinct prime ideals of OK , ℘i = pOK + gi (θ)OK with residual degree of (℘i /p) =deg gi (x) where i = 1, 2, ... He also gave a criterion which says that p does not divide [OK : Z[θ]] if and only if for each i, we have either ei = 1 or gi (x) does not divide M (x) where M (x) = p (f (x) − g1 (x)e1 ....gr (x)er). In this work we prove the theorem and the criterion too while giving applications its due.