Dedekind's Theorem on splitting of primes and simple extensions of integrally closed domains

Sudesh K. Khanduja
Indian Institute of Science Education and Research, Mohali, India.
E-mail: skhanduja@iisermohali.ac.in

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with $F(x)$ as the minimal polynomial of the algebraic integer θ over $\mathbb{Q}$. Let p be a rational prime.Let

$$F(x) \equiv g_1(x)^{e_1} \dots g_r(x)^{e_r} (mod\ p)$$

be the factorization of $F(x)$ as a product of powers of distinct irreducible polynomials modulo p, with $g_i(x)$ monic polynomials belonging to $\mathbb{Z}[x]$. In 1878, Dedekind proved if p does not divide the index of the subgroup $\mathbb{Z}[\theta]$ in A_K, then $pA_K = \wp_1^{e_1} \dots \wp_r^{e_r}$, where $\wp_1, \dots, \wp_r$ are distinct prime ideals of A_K, $\wp_i = pA_K + g_i(\theta)A_K$ with residual degree of $\wp_i/p$ equal to $\deg g_i(x)$ for all i. In 2006, it was proved that converse of Dedekind's theorem holds, i.e. if for a rational prime p the decomposition of pA_K satisfies the above three properties, then p does not divide $[A_K : \mathbb{Z}[\theta]]$. Dedekind also gave a simple criterion known as Dedekind Criterion to verify when p does not divide $[A_K : \mathbb{Z}[\theta]]$. We will discuss the Dedekind Criterion and its generalizations and will relate it to simple extensions of integrally closed domains. We shall also describe the analogue of Dedekind's theorem for finite extensions of valued fields of arbitrary rank as well as of its converse proved in 2014.