Valuation Theory

Algebraic number fields: Let α be an algebraic number with degree n and let P be the minimal polynomial for α (the minimal polynomial P for α is the unique polynomial $P = a_0x^n + \cdots + a_n$ with $a_0 > 0$ and that $a_0, \ldots, a_n$ are integers and are relatively prime). By the *conjugate* of α, we mean the zeros $\alpha_1, \ldots, \alpha_n$ of P. The algebraic number field k generated by α over the rational $\mathbf{Q}$ is defined the set of numbers $Q(\alpha)$ where $Q(x)$ is a any polynomial with rational coefficinets; the set can be regarded as being embedded in the complex number field $\mathbf{C}$ and thus the elements are subject to the usual operations of addition and multiplication. To see k is actually a field, let P be the minimal polynomial for α, then P, Q are relative prime, so $PS + QR = 1$, then $R(\alpha) = 1/Q(\alpha)$. The field has degree n over $\mathbf{Q}$, and one denote $[k : \mathbf{Q}] = n$. A *number* field is a finite extension of the field of rational numbers.

Algebraic integers: An algebraic number is said to be an algebraic integer if the coefficient of the highesy power of x in the minimal polynomial P is 1. The algebraic integers in an algebraic number field form a ring R. The ring has an integral basis, that is, there exist elements $\omega_1, \ldots, \omega_n$ in R such that every element in R can be expressed uniquely in the form $u_1\omega_1 + \cdots + u_n\omega_n$ for some rational integers $u_1, \ldots, u_n$.

UFD: One calls R is UFD if every element of R can be expressed uniquely as a product of irreducible elements. The fundamental theorem of arithmetic asserts that the ring of integers in $k = \mathbf{Q}$ has this property. Nevertheless, it is known from the poineering studies of Kummer and Dedekind that a unique factorization property can be restored by the introduction of ideals, and this forms the central theme of algebraic number theory.

Ramification and Relative degree: Let p be a prime number. Let k be a number field, and let R be the ring of algebraic integers. If we lift (p) to R (where (p) is the ideal generated by p on $\mathbf{Z}$) and factor $(p)R$ as $\prod_{i=1}^{g} \mathcal{P}_i^{e_i}$, we say that $\mathcal{P}_i$ divides p. The positive integer e_i is called the *ramification index* of $\mathcal{P}_i$ over (p). We say that (p) *ramifies* in R (or in k) if $e_i > 1$ for at least one i. We can prove that R/P_i is a finite extension of the field $\mathbf{Z}/p\mathbf{Z}$. The degree $f_i = [R/\mathcal{P}_i : \mathbf{Z}/p\mathbf{Z}]$ of this extension is called the *relative degree*(or the *residue class degree*, or the *inertical degree*) of $\mathcal{P}_i$ over (p). We have

$$\sum_{i=1}^{g} e_i f_i = [R/pR : \mathbf{Z}/p\mathbf{Z}] = [k : \mathbf{Q}].$$

Norm of Ideals: If I is a nonzero ideal of R, we define the *norm* of I by $N(I) = |R/I|$. We can show that te norm is finite, so if $\mathcal{P}$ is a nonozero prime ideal of R, then $R/\mathcal{P}$ is a finite field. It can be shown that if $\mathcal{P}$ is a nonozero prime ideal of R, then $\mathcal{P}$ divides exactly one rational prime p. The norm $\mathcal{N}(\mathcal{P})$ equal to $p^{f_\mathcal{P}}$ where p is a rational prime and $f_\mathcal{P}$ is a positive integer (note $f_\mathcal{P} = [R/\mathcal{P} : \mathbf{Z}/p\mathbf{Z}]$). The norm of principal ideal (p) is $N(p) = p^n$.

Absolute Values: By an *absolute value* over a field k, we mean a real-valued function

$$| \ | : k \to [0, \infty)$$

such that (1) $|x| = 0$ if and only if $x = 0$; (2) $|xy| = |x||y|$, (3) $|x + y| \leq |x| + |y|$. The absolute value is called *non-archimedean* if in addtion, (3)' $|x + y| \leq \max\{|x|, |y|\}$.

Over $\mathbf{Q}$ there is a stardard way to put absolue values.

The set of standard absolute values on a number field k is the set of M_k consisting of all standard absolute values on k whose restriction to $\mathbf{Q}$ is one of the absolute values on $\mathbf{Q}$. Let k' be an extension of k, let $v \in M_k, w \in M_{k'}$, we say $w|v$ if the restriction of w is v.

Let $v \in M_k$, we write $\|x\|_v = |x|_v^{n_v}$, where $n_v = [k_v : \mathbf{Q}_v]$. The we have the product formula:

$$\prod_{v \in M_k} \|x\|_v = 1.$$

Proof: Let $x \in k$, and $v_0 \in M_\mathbf{Q}$, then (see Lang, Corollary 2 to Theorem 2)

$$\prod_{v \in M_k, v|v_0} \|x\|_v = |N_{k/\mathbf{Q}}(x)|_v.$$

Hence

$$\prod_{v \in M_k} \|x\|_v = \prod_{v_0 \in M_\mathbf{Q}} \prod_{v \in M_k, v|v_0} \|x\|_v = \prod_{v_0 \in M_\mathbf{Q}} |N_{k/\mathbf{Q}}(x)|_v = 1.$$

This proves the produc formula.

Alternative description of valuations: Let $k = \mathbf{Q}(\alpha)$ be a number field of degree n. We shall recall some well-known facts about valuations of k. Suppose that $n = r + 2s$ and that $\alpha^{(1)}, \cdots, \alpha^{(r)}$ are real and $\alpha^{(r+1)}, \cdots, \alpha^{(r+s)}, \alpha^{(r+s+1)}, \cdots, \alpha^{(n)}$ are comples with $\alpha^{(r+s+j)}$ the conjugate of $\alpha^{(r+j)} (j = 1, \ldots, s)$. Let M_k be the set consisting of integres $1, 2, \ldots, r+s$ and of the prime ideals of the ring of (algebraic) integers of k. If $\upsilon \in M_k$, $1 \leq \upsilon \leq r + s$ and if $x \in k$, then we put $|\alpha|_\upsilon = |\alpha^{(\upsilon)}|$ where $|\ |$ denote the ordinary absolute value.

Now suppose that υ is a prime ideal $\mathcal{P}$. The norm $\mathcal{N}(\mathcal{P})$ equal to $p^{f_\mathcal{P}}$ where p is a rational prime and $f_\mathcal{P}$ is a positive integer (note $f_\mathcal{P} = [R/\mathcal{P} : \mathbf{Z}/p\mathbf{Z}]$). The norm of principal ideal (p) is $N(p) = p^n$. If $x \in k$, $x \neq 0$, then the fractinoal ideal (x) may uniquely be written $(x) = \mathcal{P}^a \mathcal{P}_2^{a_2} \cdots \mathcal{P}_l^{a_l}$, where $a, a_1, \ldots, a_l$ are rational integers. We now put $|x|_\upsilon = p^{-a/e_\mathcal{P}}$ (note that $e_\mathcal{P}$ is needed to make $|p|_\upsilon = p^{-1}$), and put $|0|_\upsilon = 0$. It is clear that $|xy|_\upsilon = |x|_\upsilon |y|_\upsilon$ and that if $x \neq 0$, then $|x|_\upsilon = 1$ for all but finitely many υ. The mappings $x \mapsto |x|_\upsilon$ where $\upsilon \in M_k$ are all the inequivalent valuations of k, and the Archimedean valuations are those where $\upsilon = 1, 2, \ldots, r + s$. For every $\upsilon \in M_k$, there is a completetion k_υ of k with respect to $|\ |_\upsilon$. Put $N_\upsilon = 1$ or $N_\upsilon = 2$ if $1 \leq \upsilon \leq r$ or $r + 1 \leq \upsilon \leq r + s$, respectively; N_υ was defined above when υ is a prime ideal. Put $\|x\|_\upsilon = |x|_\upsilon^{n_\upsilon} = (\mathcal{N}(\mathcal{P}))^{-ord_\mathcal{P} x}$, where $n_\upsilon = [k_\upsilon : \mathbf{Q}_\upsilon] = e_\mathcal{P} f_\mathcal{P}$. It is clear that the definition of $|x|_\upsilon$ can be extended to $x \in k_\upsilon$. The product formula

$$\prod_{\upsilon \in M_k} \|x\|_\upsilon = 1$$

hold for every non-zero $x \in k$.

Example. Let $k = \mathbf{Q}(\sqrt{2})$. Let $x = 3 + \sqrt{2}$. We want to find the valuations of $3 + \sqrt{2}$. There are two archimedean absolute values with $N_\upsilon = 1$, so $\|3 + \sqrt{2}\|_{\upsilon_1} = 3 + \sqrt{2}$, $\|3 + \sqrt{2}\|_{\upsilon_2} = 3 - \sqrt{2}$. To find non-archimedean places, we note that $7 = (3 + \sqrt{2})(3 - \sqrt{2})$. So 7 is the unique prime which $(3 + \sqrt{2})$ devides, and clearly, for $\upsilon = \mathcal{P} \neq (3 + \sqrt{2})$, or $\mathcal{P} \neq (3 - \sqrt{2})$, we have $\|3 + \sqrt{2}\|_\upsilon = 1$. So we only need to consider $\upsilon_3 = (3 + \sqrt{2})$ and $\upsilon_4 = (3 - \sqrt{2})$. For $\upsilon_3 = (3 + \sqrt{2})$, since $a = 1$, we have $|3 + \sqrt{2}|_{\upsilon_3} = 7^{-1}$. Similarily, $|3 + \sqrt{2}|_{\upsilon_4} = 1$. It can be checked that $f_3 = 1$, so $\|3 + \sqrt{2}\|_{\upsilon_3} = |3 + \sqrt{2}|_{\upsilon_3} = 7^{-1}$. It is easy to see that the product formula holds.