CHAPTER I

PRELIMINARIES

Unique factorization of ideals in algebraic number fields. Let $\mathbf{k}$ be a finite extension of the rational number field $\mathbf{Q}$. An *integer* of $\mathbf{k}$ is an element of $\mathbf{k}$ which satisfies a monic irreducible polynomial with coefficients in the ring of *rational* integers $\mathbf{Z}$. The integers of $\mathbf{k}$ form a ring $\mathbf{o}$ that is finitely generated over $\mathbf{Z}$. Every ideal of $\mathbf{o}$ is finitely generated, and every prime ideal is maximal.

A subset a of $\mathbf{k}$ is a *fractional* ideal of $\mathbf{o}$ if a is an $\mathbf{o}$-module such that for some element γ of $\mathbf{o}$ depending on a we have $\gamma a \subset o$. Any non-zero element α of $\mathbf{k}$ generates a principal fractional ideal $(\alpha) = \alpha\mathbf{o}$. (If α is a root of polynomial $a_0x^n + a_1x^{n-1} + \cdots + a_n$ over $\mathbf{Z}$, then $a_0^n\alpha$ is an integer in $\mathbf{k}$, and $a_0^n(\alpha) = (a_0^n\alpha) \subset \mathbf{o}$.) The product of fractional ideals a and b is the fractional ideal generated by products $\alpha\beta$ with α in a and β in b. For principal fractional ideals, we have $(\alpha)(\beta) = (\alpha\beta)$. Every non-trivial fractional ideal a of $\mathbf{o}$ is invertible: there is a fractional ideal a' so that $aa' = \mathbf{o}$. Non-zero principal fractional ideals are invertible because if $\alpha \neq 0$ then $(\alpha)(\alpha^{-1}) = (1) = \mathbf{o}$. In fact,

Although $\mathbf{o}$ is not in general a unique factorization domain, every non-trivial fractional ideal $\mathbf{a}$ of $\mathbf{o}$ has a unique factorization

$$a = p_1^{n_1} \dots p_k^{n_k},$$

where $p_1, \dots, p_g$ are distinct prime ideals of $\mathbf{o}$ and the rational integer exponents n_i are non-zero (but may be positive or negative).

Valuations and completions. A *valuation* of field $\mathbf{k}$ is a non-negative real-valued function ψ defined on $\mathbf{k}$ satisfying

$$\begin{aligned} \psi(\alpha) &= 0 \quad \text{ if and only if } \alpha = 0, \\ \psi(\alpha\beta) &= \psi(\alpha)\psi(\beta), \\ \psi(\alpha + \beta) &\leq \psi(\alpha) + \psi(\beta). \end{aligned}$$

Valuation ψ is non-trivial if there is some α in $\mathbf{k}$ for which $\psi(\alpha) \neq 0$ and $\psi(\alpha) \neq 1$. Two valuations ψ_1 and ψ_2 are equivalent if a sequence converges to zero with respect to ψ_1 if and only if it converges to zero with respect to ψ_2, in which case there is some positive real constant c such that $\psi_1(\alpha) = \big(\psi_2(\alpha)\big)^c$.

Valuations are classified as *archimedean* or *non-archimedean.* A valuation is non-archimedian if it satisfies the stronger inequality

$$\psi(\alpha+\beta) \le \max\big(\psi(\alpha), \psi(\beta)\big), \tag{1.1}$$

otherwise it is archimedian. Every archimedian valuation of $\mathbf{Q}$ is equivalent to the ordinary absolute value.

Archimedian valuations on $\mathbf{k}$. If $\mathbf{k}$ is generated by α_0 over the rational field $\mathbf{Q}$, let $f_0(x)$ be the irreducible polynomial over $\mathbf{Q}$ satisfied by α_0. Over the real field $\mathbf{R}$, $f_0(x)$ splits into a product of r_1 linear and r_2 irreducible quadratic factors. Corresponding to the r_1 roots of linear factors, there will be r_1 isomorphisms $\sigma_1, \ldots, \sigma_{r_1}$ of $\mathbf{k}$ onto subfields of $\mathbf{R}$. Corresponding to the r_2 conjugate pairs of roots of quadratic factors, there will be r_2 pairs $(\tau_1, \bar{\tau}_1), \ldots, (\tau_{r_2}, \bar{\tau}_{r_2})$ of isomorphisms of $\mathbf{k}$ onto subfields of the complex field $\mathbf{C}$. Members of each pair $(\tau_j, \bar{\tau}_j)$ differ by complex conjugation.

$$\bar{\tau}_j(\alpha) = \overline{\tau_j(\alpha)}$$

These $r_1 + 2r_2$ isomorphisms do not depend on the choice of α_0. Each isomorphism σ_i of $\mathbf{k}$ into $\mathbf{R}$ determines an archimedian valuation on $\mathbf{k}$; the *normalized* valuation is defined using the ordinary real absolute value.

$$|\alpha|_{\sigma_i} = |\sigma_i(\alpha)| \tag{1.2}$$

Each pair $(\tau_j, \bar{\tau}_j)$ of isomorphisms of $\mathbf{k}$ into $\mathbf{C}$ determines an archimedian valuation on $\mathbf{k}$; the *normalized* valuation is defined using the square of the ordinary complex absolute value.

$$|\alpha|_{\tau_j} = |\alpha|_{\bar{\tau}_j} = \tau_j(\alpha)\bar{\tau}_j(\alpha) = \tau_j(\alpha)\overline{\tau_j(\alpha)} = |\tau_j(\alpha)|^2 \tag{1.3}$$

Non-archimedian valuations on $\mathbf{k}$. Let ψ be a non-trivial non-archimedian valuation of $\mathbf{k}$. Every rational integer a satisfies $\psi(a) \le 1$, because

$$\psi(a) = \psi(1 + \cdots + 1) \le \max(\psi(1), \ldots, \psi(1)) = 1.$$

Every integer α in $\mathbf{o}$ satisfies $\psi(\alpha) \le 1$, because α is a root of a monic polynomial $x^n + a_1x^{n-1} + \cdots + a_n$ with rational integer coefficients and by (1.1) we have

$$\begin{aligned} \psi(\alpha)^n &\le \max\left(\psi(a_1)\psi(\alpha^{n-1}), \ldots, \psi(a_{n-1})\psi(\alpha), \psi(a_n)\right) \\ &\le \max\left(\psi(\alpha)^{n-1}, \ldots, \psi(\alpha), 1\right), \end{aligned}$$

which is possible only if $\psi(\alpha) \leq 1$. The subset of elements α of $\mathbf{o}$ satisfying $\psi(\alpha) < 1$ is a prime ideal of $\mathbf{o}$ which depends only of the equivalence class of ψ.

Conversely, we can construct a non-trivial non-archimedian valuation of $\mathbf{k}$ for each prime ideal of $\mathbf{o}$. Let p be a prime ideal of $\mathbf{o}$. If α is a non-zero element of $\mathbf{k}$, consider fractional ideal (α). We have

$$(\alpha) = p^m b$$

where b is a (possibly trivial) fractional ideal relatively prime to p. Put $\operatorname{ord}(p, \alpha) = m$. Choose a positive real constant c. Define p-adic valuation ψ_c by

$$\psi_c(\alpha) = \begin{cases} c^{\operatorname{ord}(p,\alpha)} & \text{for } \alpha \neq 0 \\ 0 & \text{for } \alpha = 0. \end{cases}$$

This is a non-trivial non-archimedian valuation on $\mathbf{k}$; different choices for c produce equivalent valuations. Thus there is a one-to-one correspondence between equivalence classes of non-trivial non-archimedian valuations of $\mathbf{k}$ and prime ideals of the ring $\mathbf{o}$.

Since $\mathbf{o}$ is finitely generated over $\mathbf{Z}$ and prime ideals of $\mathbf{o}$ are maximal, the quotient ring $\mathbf{o}/p$ is a finite field. Let $\mathrm{N}p$ be the number of elements in $\mathbf{o}/p$. The *normalized* p-adic valuation of $\mathbf{k}$ is defined by

$$|\alpha|_p = (\mathrm{N}p)^{-\operatorname{ord}(p,\alpha)} \qquad \text{for } \alpha \neq 0.$$

The concept of *prime* of $\mathbf{k}$ is generalized to mean *equivalence class of non-trivial valuations on* $\mathbf{k}$. We have non-archimedian *finite* primes of $\mathbf{k}$ corresponding to prime ideals of ring $\mathbf{o}$, and archimedian *infinite* primes defined by (1.2) and (1.3). Taking the product over all primes p using normalized valuations, we have

$$\prod_p |\alpha|_p = 1 \qquad \text{for } \alpha \in \mathbf{k}, \alpha \neq 0.$$

Completion of k with respect to a non-trivial valuation. An infinite sequence $\{\alpha_i\}$ of elements of $\mathbf{k}$ is Cauchy with respect to valuation ψ on $\mathbf{k}$ if and only if $\lim_{i,j\to\infty} (\psi(\alpha_i - \alpha_j)) = 0$. The set of Cauchy sequences forms a ring, in which the set of sequences converging to zero is a maximal ideal. The quotient ring $\mathbf{k}_p$ is a field that depends only on the prime p determined by ψ. The valuation can be extended to $\mathbf{k}_p$ by defining $\psi(\{\alpha_i\}) = \lim_{i\to\infty} \psi(\alpha_i)$ (the right side converges in $\mathbf{R}$). Then $\mathbf{k}_p$ is complete with respect to the extended valuation. There is a natural isomorphism $\sigma : \mathbf{k} \to \mathbf{k}_p$ mapping each element of $\mathbf{k}$ to a constant sequence.

If p is archimedian then $\mathbf{k}_p$ is isomorphic to the real field $\mathbf{R}$ or the complex field $\mathbf{C}$, depending whether the valuation is defined by (1.2) or (1.3). If p is non-archimedian then $\mathbf{k}_p$ is the field of p-adic numbers. Since the p-adic valuation takes a discrete set of values, a basic neighborhood $U_m(\alpha_0)$ of α_0 in $\mathbf{k}_p$, defined for $m > 0$ by

$$U_m(\alpha_0) = \big\{\alpha \in \mathbf{k}_p \;\big|\; |\alpha - \alpha_0|_p < (Np)^m\big\} = \big\{\alpha \in \mathbf{k}_p \;\big|\; |\alpha - \alpha_0|_p \leq (Np)^{m-1}\big\},$$

has the property of being both open and closed. The ring $\mathbf{o}_p$ of p-adic integers defined by

$$\mathbf{o}_p = \big\{\alpha \in \mathbf{k}_p \;\big|\; |\alpha|_p \leq 1\big\}$$

has the following properties. (1) $\mathbf{o}$ is contained in $\mathbf{o}_p$ and is dense in $\mathbf{o}_p$. (2) Every ideal of $\mathbf{o}_p$ is principal. (3) The only prime ideal of $\mathbf{o}_p$ is $p = \big\{\alpha \in \mathbf{o}_p \;\big|\; |\alpha|_p < 1\big\}$. (4) The only proper ideals of $\mathbf{o}_p$ are $p, p^2, p^3, \ldots$. (5) $\mathbf{o}_p$ is open, closed and compact; (6) $\mathbf{o}_p/p$ is a finite field isomorphic to $\mathbf{o}/p$. (Note: symbol p denotes ideals of both $\mathbf{o}$ and $\mathbf{o}_p$, but the context will resolve any ambiguity.)

Ideles over k. Consider the product $\prod_p \mathbf{k}_p^*$ over all primes of $\mathbf{k}$. If $\mathbf{i}$ is an element of the product then $\mathbf{i}_p$ is its p-th coordinate. Let $|\mathbf{i}_p|_p$ be denoted simply by $|\mathbf{i}|_p$. The *Idele group* $\mathbf{I_k}$ is defined by

$$\mathbf{I_k} = \big\{\mathbf{i} \in \prod_p \mathbf{k}_p^* \;\big|\; |\mathbf{i}|_p = 1 \quad \text{for all but a finite number of primes } p\big\}.$$

Define $|\mathbf{i}|$ by

$$|\mathbf{i}| = \prod_p |\mathbf{i}|_p \qquad \text{for } \mathbf{i} \in \mathbf{I_k},$$

and define subgroup $\mathbf{I}^0_{\mathbf{k}}$ by

$$\mathbf{I}^0_{\mathbf{k}} = \big\{\mathbf{i} \in \mathbf{I_k} \;\big|\; |\mathbf{i}| = 1\big\}.$$

The multiplicative group $\mathbf{k}^*$ is a subgroup of $\mathbf{I}^0_{\mathbf{k}}$ because of product formula (1.4).

For the topology of $\mathbf{I_k}$, let E be any finite set of primes containing all infinite primes; for each prime p in E let ϵ_p be a positive real number. Then a basic neighborhood of idele $\mathbf{i}_0$ is the set

$$\begin{aligned} U(E, \{\epsilon_p\}) = \big\{\mathbf{i} \in \mathbf{I_k} \;\big|\; & |\mathbf{i}(\mathbf{i}_0)^{-1}|_p = 1 \text{ if } p \notin E; \\ & |\mathbf{i}(\mathbf{i}_0)^{-1} - 1|_p < \epsilon_p \text{ and } |(\mathbf{i}_0)\mathbf{i}^{-1} - 1|_p < \epsilon_p \text{ if } p \in E\big\}. \end{aligned}$$

Arithmetic in a finite extension of k. Let $\mathbf{K}/\mathbf{k}$ be a finite extension of degree n. The ring $\mathbf{O}$ of integers in $\mathbf{K}$ is a free $\mathbf{o}$-module of degree n. A prime ideal p of $\mathbf{o}$ generates an ideal $p\mathbf{O}$ of $\mathbf{O}$ which splits into a finite product

$$p = \wp_1^{e_1} \dots \wp_g^{e_g},$$

where $\wp_1, \dots, \wp_g$ are distinct primes ideals of $\mathbf{O}$. Each $\wp_i$-adic valuation of $\mathbf{K}$ extends the p-adic valuation of $\mathbf{k}$, so $\mathbf{K}_{\wp_i}$ is an extension of $\mathbf{k}_p$.

There is a correspondence between the splitting of p in $\mathbf{K}$ and the splitting of a generating polynomial in $\mathbf{k}_p$. Let $\mathbf{K} = \mathbf{k}(\alpha)$, and let α be a root of monic irreducible polynomial $f(x)$ with coefficients in $\mathbf{k}$. Suppose that $\wp_i, \dots, \wp_g$ are the distinct primes of $\mathbf{K}$ dividing p. For each $\wp_i$, let $\sigma_i : \mathbf{K} \to \mathbf{K}_{\wp_i}$ be the natural isomorphism. Let $f_i(x)$ be the monic irreducible polynomial over $\mathbf{k}_p$ satisfied by $\sigma_i(\alpha)$. Then the polynomials $f_1(x), \dots, f_g(x)$ are all distinct, and

$$f(x) = f_1(x) \dots f_g(x).$$

Element $\sigma_i(\alpha)$ generates $\mathbf{K}_{\wp_i}$ over $\mathbf{k}_p$, so $[\mathbf{K}_{\wp_i} : \mathbf{k}_p] = \deg\big(f_i(x)\big)$, and

$$[\mathbf{K} : \mathbf{k}] = \sum_{i=1}^{g} [\mathbf{K}_{\wp_i} : \mathbf{k}_p] \tag{1.4}$$

Except for a finite number of *ramified* primes p, all of the exponents e_i are equal to 1. A prime for which all of the e_i are equal to one is *unramified in* $\mathbf{K}$. Each of the finite fields $\mathbf{O}_{\wp_i}/\wp_i$ is a finite extension of finite field $\mathbf{o}_p/p$; Let f_i be the degree of this extension.

$$f_i = [\mathbf{O}_{\wp_i}/\wp_i : \mathbf{o}_p/p]$$

Then $[\mathbf{K}_{\wp_i} : \mathbf{k}_p] = e_i f_i$, and

$$n = e_1 f_1 + \dots e_g f_g.$$

$\mathbf{O}_{\wp_i}$ is a free $\mathbf{o}_p$-module of degree $e_i f_i$. For each $\mathbf{K}_{\wp} = \mathbf{K}_{\wp_i}$ over $\mathbf{k}_p$, with $e = e_i$ and $f = f_i$, a basis may be found as follows. Choose elements $\omega_1, \dots, \omega_f$ of $\mathbf{O}_{\wp}$ which map to a basis of $\mathbf{O}_{\wp}/\wp$ over $\mathbf{o}_p/p$. Choose an element π of $\mathbf{O}_{\wp}$ which generates ideal $\wp$ (which is a principle ideal of $\mathbf{O}_{\wp}$). Then the ef products $\pi^j \omega_k$, where $0 \le j < e$ and $1 \le k \le f$, are a basis of $\mathbf{K}_{\wp}$ over $\mathbf{k}_p$ and of $\mathbf{O}_{\wp}$ over $\mathbf{o}_p$.

Norm and Trace functions. Extension field $\mathbf{K}$ is an n-dimensional vector space over $\mathbf{k}$. For each α in $\mathbf{K}$, the operation of multiplication by α defines a linear transformation $T_\alpha : \mathbf{K} \to \mathbf{K}$, where $T_\alpha(\beta) = \alpha\beta$. The *norm* $\mathbf{N}_{\mathbf{K}/\mathbf{k}}$ and *trace* $\mathbf{S}_{\mathbf{K}/\mathbf{k}}$ are functions from $\mathbf{K}$ to $\mathbf{k}$ defined by

$$\mathbf{N}_{\mathbf{K}/\mathbf{k}}(\alpha) = \det(T_\alpha), \qquad \mathbf{S}_{\mathbf{K}/\mathbf{k}}(\alpha) = \mathrm{trace}(T_\alpha).$$

If $\mathbf{L}$ is an intermediate subfield, $\mathbf{K} \supset \mathbf{L} \supset \mathbf{k}$, then we have

$$\mathbf{N}_{\mathbf{K}/\mathbf{k}}\alpha = \mathbf{N}_{\mathbf{L}/\mathbf{k}}\mathbf{N}_{\mathbf{K}/\mathbf{L}}\alpha.$$

For each prime p of $\mathbf{k}$, let $\wp_1, \ldots, \wp_g$ be the primes of $\mathbf{K}$ which divide p, and let $\sigma_i : \mathbf{K} \to \mathbf{K}_{\wp_i}$ be the natural isomorphism. If α of $\mathbf{K}$, then

$$\mathbf{N}_{\mathbf{K}/\mathbf{k}}(\alpha) = \prod_{i=1}^{g} \mathbf{N}_{\mathbf{K}_{\wp_i}/\mathbf{k}_p}\bigl(\sigma_i(\alpha)\bigr) \qquad \mathbf{S}_{\mathbf{K}/\mathbf{k}}(\alpha) = \sum_{i=1}^{g} \mathbf{S}_{\mathbf{K}_{\wp_i}/\mathbf{k}_p}\bigl(\sigma_i(\alpha)\bigr). \tag{1.5}$$

If α is identified with $\sigma_i(\alpha)$ then we may write $\mathbf{N}_{\mathbf{K}/\mathbf{k}}(\alpha) = \prod_{\wp|p} \mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}(\alpha)$ and $\mathbf{S}_{\mathbf{K}/\mathbf{k}}(\alpha) = \sum_{\wp|p} \mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}(\alpha)$. Finally, for any element β in $\mathbf{K}_{\wp_i}$ we have

$$\left|\mathbf{N}_{\mathbf{K}_{\wp_i}/\mathbf{k}_p}\beta\right|_p = |\beta|_{\wp_i}.$$

These formulae hold for all primes of $\mathbf{k}$, both finite and infinite. We can now show that the product formula holds in the extension field. For α in $\mathbf{K}$, we have

$$\prod_{\wp} |\alpha|_\wp = \prod_p \left(\prod_{\wp|p} \left|\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\alpha\right|_p \right) = \prod_p \left|\mathbf{N}_{\mathbf{K}/\mathbf{k}}\alpha\right|_p = 1 \tag{1.6}$$

A norm for ideals can also be defined. If a is an ideal of $\mathbf{O}$ then $\mathbf{N}_{\mathbf{K}/\mathbf{k}}a$ is the ideal of $\mathbf{o}$ generated by all elements $\mathbf{N}_{\mathbf{K}/\mathbf{k}}\alpha$ for α in $\mathbf{O}$. For principal ideal $a = (\alpha)$, we have $\mathbf{N}_{\mathbf{K}/\mathbf{k}}a = (\mathbf{N}_{\mathbf{K}/\mathbf{k}}\alpha)$. For each prime ideal $\wp_i$ of $\mathbf{O}$ dividing prime p of $\mathbf{o}$, a fundamental property of the norm is

$$\mathbf{N}_{\mathbf{K}/\mathbf{k}}\wp_i = p^{f_i}.$$

The *different* $\delta_{\mathbf{K}/\mathbf{k}}$ is an ideal of $\mathbf{O}$ determined by defining its inverse to be

$$\delta_{\mathbf{K}/\mathbf{k}}^{-1} = \left\{\alpha \in \mathbf{K} \mid \beta \in \mathbf{O} \Longrightarrow \mathbf{S}_{\mathbf{K}/\mathbf{k}}(\alpha\beta) \in \mathbf{o}\right\},$$

and the *discriminant* $\mathbf{D}_{\mathbf{K}/\mathbf{k}}$ is the norm $\mathbf{N}_{\mathbf{K}/\mathbf{k}}\delta_{\mathbf{K}/\mathbf{k}}$ of the different. A prime of $\mathbf{k}$ is ramified in $\mathbf{K}$ if and only if it divides the discriminant. Suppose that $x_1, \ldots, x_n$

forms an integral basis of $\mathbf{O}$ over $\mathbf{o}$. The discriminant is the following principal ideal.

$$\mathbf{D}_{\mathbf{K}/\mathbf{k}} = \Big(\det \left(\mathbf{S}_{\mathbf{K}/\mathbf{k}}(x_i x_j) \right) \Big)$$

For each $\wp$ of $\mathbf{K}$, the local different $\delta_{\mathbf{K}_\wp/\mathbf{k}_p}$ is determined by its inverse

$$\delta^{-1}_{\mathbf{K}_\wp/\mathbf{k}_p} = \left\{ \alpha \in \mathbf{K}_\wp \mid \beta \in \mathbf{O}_\wp \Longrightarrow \mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}(\alpha\beta) \in \mathbf{o}_p \right\},$$

and the local discriminant $\mathbf{D}_{\mathbf{K}_\wp/\mathbf{k}_p}$ is the norm $\mathbf{N}_{\mathbf{K}_\wp/\mathbf{k}_p}\delta_{\mathbf{K}_\wp/\mathbf{k}_p}$ of the local different. Then p ramifies in $\mathbf{K}_\wp$ if and only if it divides $\mathbf{D}_{\mathbf{K}_\wp/\mathbf{k}_p}$, which is equivalent to saying $\mathbf{D}_{\mathbf{K}_\wp/\mathbf{k}_p}$ is not trivial. If $x_1, \ldots, x_m$ is an integral basis of $\mathbf{O}_\wp$ over $\mathbf{o}_p$, then

$$\mathbf{D}_{\mathbf{K}_\wp/\mathbf{k}_p} = \Big(\det \left(\mathbf{S}_{\mathbf{K}_\wp/\mathbf{k}_p}(x_i x_j) \right) \Big)$$

Splitting and inertial subgroups in normal extensions. Let σ be an automorphism in the Galois group $G(\mathbf{K} : \mathbf{k})$ of normal extension $\mathbf{K}/\mathbf{k}$. Let $\wp_1, \ldots, \wp_g$ be the prime ideals of $\mathbf{O}$ which divide p. The image $\sigma\wp_i$ of $\wp_i$ is a prime ideal of $\mathbf{O}$ and contains p; therefore $\sigma\wp_i$ is one of the $\wp_j$. For each pair $\wp_i$ and $\wp_j$, there is some automorphism σ so that $\sigma\wp_i = \wp_j$. Therefore there are rational integers e and f depending only on p so that

$$e = e_1 = \cdots = e_g \qquad \text{and} \qquad f = f_1 = \cdots = f_g.$$

The set $S_{\wp_i}$ of automorphisms which leave $\wp_i$ invariant is the *splitting group* of $\wp_i$.

$$S_{\wp_i} = S_{\wp_i}(\mathbf{K} : \mathbf{k}) = \left\{ \sigma \in G(\mathbf{K} : \mathbf{k}) \;\middle|\; \sigma\wp_i = \wp_i \right\}$$

Each subgroup $S_{\wp_i}$ has index g in $G(\mathbf{K} : \mathbf{k})$, so $S_{\wp_i}$ has order ef. Automorphisms in $S_{\wp_i}$ are precisely those which can be extended to the completion $\mathbf{K}_{\wp_i}$, so $S_{\wp_i}(\mathbf{K} : \mathbf{k})$ is the Galois group of $\mathbf{K}_{\wp_i}$ over $\mathbf{k}_p$.

$$S_{\wp_i} = S_{\wp_i}(\mathbf{K} : \mathbf{k}) = G\left(\mathbf{K}_{\wp_i} : \mathbf{k}_p \right)$$

There is a natural homomorphism of $S_{\wp_i}$ to the Galois group of finite field $\mathbf{O}_{\wp_i}/\wp_i$ over $\mathbf{o}_p/p$.

$$S_{\wp_i} \to G\left(\mathbf{O}_{\wp_i}/\wp_i : \mathbf{o}_p/p \right).$$

The kernel $I_\wp$ is the *inertial subgroup of* $\wp_i$. The degree of the finite field extension is f, so the inertial subgroup has order e.

$$I_\wp = I_\wp(\mathbf{K} : \mathbf{k}) = \{ \sigma \in S_\wp(\mathbf{K} : \mathbf{k}) \mid \sigma\alpha = \alpha (\mathrm{mod}\ \wp_i) \text{ for all } \alpha \in \mathbf{O}_{\wp_i} \}.$$

If p is unramified in $\mathbf{K}$ then the inertial subgroup of $\wp_i$ is trivial and the splitting group $S_{\wp_i}$ is isomorphic to $G\left(\mathbf{O}_{\wp_i}/\wp_i : \mathbf{o}_p/p \right)$.

Splitting and inertial subfields. In a normal extension $\mathbf{K}/\mathbf{k}$, the parameters e, f and g of finite prime $\wp$ may be determined from the splitting subgroup $S = S_\wp$ and inertial subgroup $I = I_\wp$ of Galois group G.

$$e = [I : \{1\}] \qquad f = [S : I] \qquad g = [G : S]$$

Two subfields of particular interest are the fixed field of S, or *splitting field* $\mathbf{Z}$, and the fixed field of I, or *inertial field* $\mathbf{T}$. Let p' be the prime of $\mathbf{Z}$ which $\wp$ divides. Since $G(\mathbf{K} : \mathbf{Z}) = S$ then every automorphism σ in $G(\mathbf{K} : \mathbf{Z})$ satisfies $\sigma\wp = \wp$, so $S_\wp(\mathbf{K} : \mathbf{Z}) = G(\mathbf{K} : \mathbf{Z})$, and

$$G(\mathbf{K}_\wp : \mathbf{Z}_{p'}) = S_\wp(\mathbf{K} : \mathbf{Z}) = G(\mathbf{K} : \mathbf{Z}) == S_\wp(\mathbf{K} : \mathbf{k}) = G(\mathbf{K}_\wp : \mathbf{k}_p)$$

and therefore

$$\mathbf{Z}_{p'} = \mathbf{k}_p.$$

$\mathbf{Z}/\mathbf{k}$ has degree g, and p *splits completely* into g primes in $\mathbf{Z}$.

As to $\mathbf{T}$, let $\wp'$ be the prime of that field which $\wp$ divides. We have $G(\mathbf{K} : \mathbf{T}) = I \subset S$, so every automorphism in $G(\mathbf{K} : \mathbf{T})$ is in the splitting group $S_\wp(\mathbf{K} : \mathbf{T})$ and acts trivially modulo $\wp$. We have

$$I_\wp(\mathbf{K} : \mathbf{T}) = S_\wp(\mathbf{K} : \mathbf{T}) = G(\mathbf{K} : \mathbf{T}) = I.$$

$\mathbf{K}/\mathbf{T}$ is *completely ramified,* having degree e and ramification index e.

Artin symbol. The Galois group $G\left(\mathbf{O}_{\wp_i}/\wp_i : \mathbf{o}_p/p\right)$ is cyclic of order f generated by automorphism $\bar{\alpha} \to \bar{\alpha}^{\mathrm{N}p}$. If p is unramified then for each $\wp_i$ dividing p there exists a unique automorphism σ_i in $S(\wp_i)$ defined by the property

$$\sigma_i\alpha = \alpha^{\mathrm{N}p} (\mathrm{mod}\ \wp_i) \qquad \alpha \in \mathbf{O}_{\wp_i}.$$

This distinguished generator of $S(\wp_i)$ is the *Frobenius automorphism* $\left(\frac{\mathbf{K}:\mathbf{k}}{\wp_i}\right)$.

If $\wp_i$ and $\wp_j$ are two primes in $\mathbf{O}$ dividing p then there is an automorphism τ in $G(\mathbf{K} : \mathbf{k})$ such that $\tau\wp_i = \wp_j$. Then $S(\wp_j) = \tau S(\wp_i)\tau^{-1}$ and

$$\tau\sigma_i\tau^{-1}\alpha = \alpha^{\mathrm{N}p} (\mathrm{mod}\ \wp_j) \qquad \alpha \in \mathbf{O}_{\wp_j}.$$

The Frobenius automorphisms for primes of $\mathbf{K}$ dividing p are therefore conjugate.

$$\left(\frac{\mathbf{K} : \mathbf{k}}{\wp_j}\right) = \tau \left(\frac{\mathbf{K} : \mathbf{k}}{\wp_i}\right) \tau^{-1}$$

When $G(\mathbf{K} : \mathbf{k})$ is abelian the groups $S(\wp_i)$ coincide and the Frobenius automorphisms $\left(\frac{\mathbf{K}:\mathbf{k}}{\wp_i}\right)$ coincide. There is a unique automorphism σ_0 in $G(\mathbf{K} : \mathbf{k})$ depending only on p such that

(1.7) $$\alpha^{\sigma_0} = \alpha^{\mathrm{N}p} (\mathrm{mod}\ \wp) \qquad \alpha \in \mathbf{O}_\wp \text{ for all primes } \wp \text{ of } \mathbf{O} \text{ dividing } p.$$

The automorphism satisfying the above condition is the *Artin symbol* $\left(\frac{\mathbf{K}:\mathbf{k}}{p}\right)$.

Cyclotomic extensions. The cyclotomic extension of $\mathbf{Q}$ generated by n-th roots of unity is the splitting field of $x^n - 1$. The irreducible polynomial over $\mathbf{Z}$ satisfied by primitive n-th roots of unity has degree $\varphi(n)$ (the number of residue classes modulo n that are relatively prime to n). If ζ is a primitive n-th root of unity then a complete set of conjugates consists of all ζ^i where i runs through a set of representatives for the distinct residue classes modulo n that are relatively prime to n. The Galois group $G\big(\mathbf{Q}(\zeta) : \mathbf{Q}\big)$ is isomorphic to the group $\mathbf{Z}_n^*$ of integers relatively prime to n. If $j \in \mathbf{Z}_n^*$ then the automorphism σ determined by j does not depend on the choice of ζ because if $\zeta^\sigma = \zeta^j$ then $(\zeta^i)^\sigma = (\zeta^i)^j$.