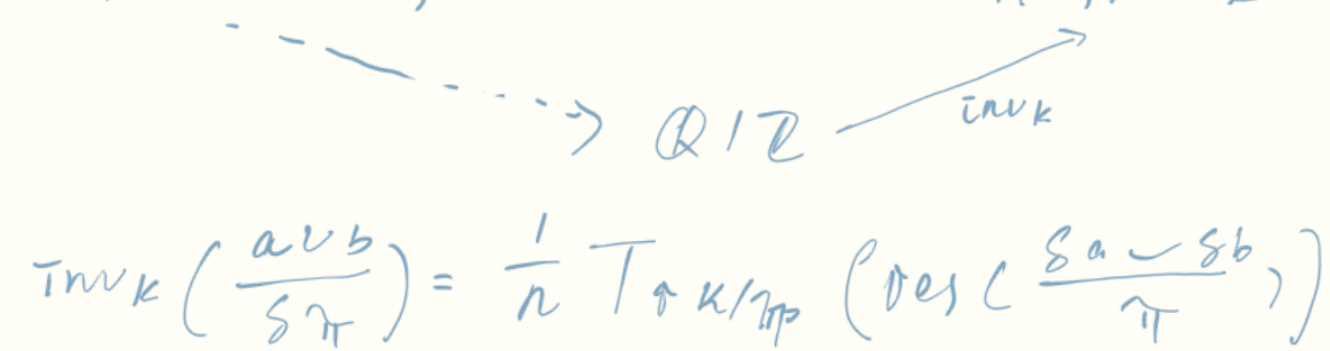


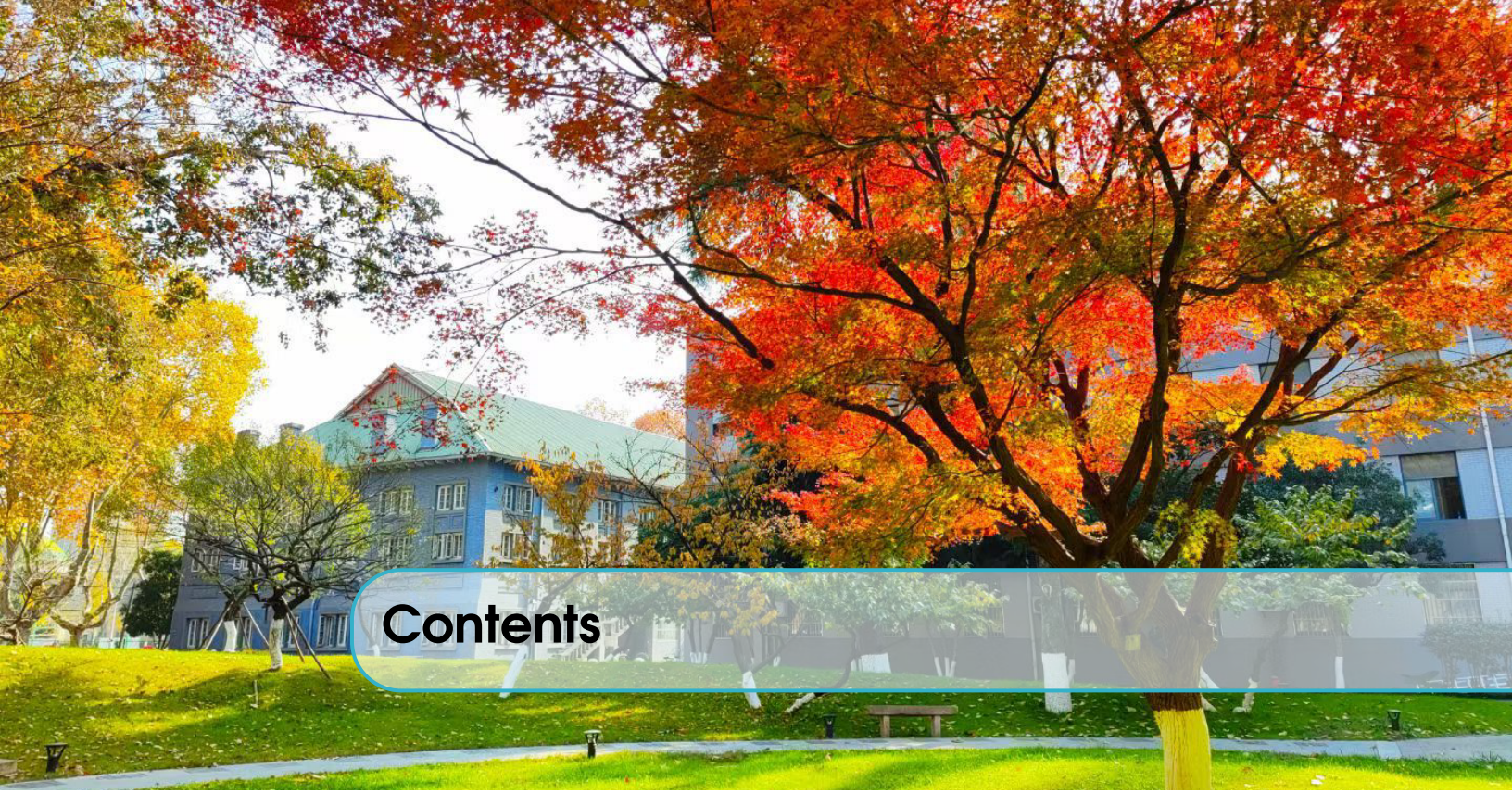
Local Fields

The Theory of Valuation and Local Fields

Lecture Notes

I have organized my notes on local field theory with the aim of summarizing my work on number theory in local contexts and to understand some of the language of class field theory, as I still wish to engage in some work in algebraic number theory. The reference textbook is GTM67, Local Fields, which primarily covers valuation theory, ramification theory, Galois cohomology, and local class field theory.

First release, August 2014



Contents

Part I

LOCAL FIELDS (BASIC FACTS)

1. Discrete Valuation Rings and Dedekind Dom

1.1 Definition of Discrete Valuation Ring

Definition 1.1.1 — Discrete Valuation Ring, Residue Field, Unit. A ring A is called a discrete valuation ring if it's a principal ideal domain , which has a unique nonzero prime ideal $\mathfrak{m}(A)$.

The field $A/\mathfrak{m}(A)$ is called the residue field of A. The invertible elements of A are those elements that do not belong to $\mathfrak{m}(A)$; They form a multiplicative group, usually called the units of A or the units of the residue field of A.

In a principal ideal domain thenonzero prime ideal is the ideal of the form πA, where π is an irreducible element. The above definition is saying that A has a unique irreducible element, up to multiplication by an invertible element, such an element is called a uniformizing element of A.

The nonzero ideal of A is of the form of $\pi^n A$, where π is a uniformizing element. If $x \neq 0$ is any element of A, one can write as $x = \pi^n u$, with $n \in \mathbb{N}$ and u is invertible; The integer n is called the valuation or the order of x, denoted by $v(x)$, it doesn't depend on the choice of π.

Let K be the field of fractions of A, K^* the multiplicative group of nonzero elements of K. If $x = a/b$ is any element in K^*, can be also written as the form $\pi^n u$, with $n \in \mathbb{Z}$. The following properties hold:

- (a)The map $v : K^* \to \mathbb{Z}$ is a surjective homomorphism.
- (b)One has $v(x+y) \geq \inf(v(x), v(y))$, we make the convention that $v(0) = +\infty$.

The function v determines the ring A: it's the set of those $x \in K$s.t. $v(x) \geq 0$; similarly, $\mathfrak{m}(A)$is the set of those $x \in K$ s.t. $v(x) > 0$.

Proposition 1.1.1 Let K be a field and $v : K^* \to \mathbb{Z}$ is a homomorphism with the properties as above. Then the set A of $x \in K$ s.t. $v(x) \geq 0$ is a discrete valuation ring, the associated valuation is v.

Indeed, let π be an element s.t. $v(\pi) = 1$. Every $x \in A$ can be written as the form of $x = \pi^n u$, where $n = v(x)$ and $v(u) = 0$, i.e. u is invertible. Thus every nonzero ideal of A has the form of $\pi^n A$, where $n \geq 0$, which shows that A is a discrete valuation ring.

■ **Example 1.1** Let p be a prime number, and $\mathbb{Z}_{(p)}$ be the subset of the set of rational numbers $\mathbb{Q}$, consists of those fractions r/s, where s isn't divisible by p; This is a discrete valuation ringwith the residue field the field $\mathbb{F}_p$ of p elements. If v_p represents the associated valuation, $v_p(x)$ is just the

exponent of p in the decomposition of x into prime factors. ∎

An analogous procedure applies to any principal ideal domain (and even to any Dedekind domain).

∎ **Example 1.2** Let k be a field and let $k((T))$ be the field of formal power series in one variable over k. For every nonzero formal series

$$f(T) = \sum_{n \geq n_0} a_n T^n, a_{n_0} \neq 0, \tag{1.1}$$

one defines the order $v(f)$ of f tuples be the integer n_0. We obtain a discrete valuation of $k(x(T))$, whose valuation ring is $k[[T]]$, the set of formal series with nonnegative exponents; its residue field is k. ∎

∎ **Example 1.3** Let V be a normal algebraic variety of dimension n and W be an irreducible subvariety of dimension $n-1$. Let $A_{V/W}$ be the local ring of V along W i.e. the set of rational functions f on V which are defined at least at one point of W. The normality hypothesis shows that $A_{V/W}$ is integerally closed; the dimension hypothesis shows that it is a one-dimensional local ring; therefore it's a discrete valuation ring; the residue field is the field of rational functions on W. If $v_W(f)$ represents associated valuation and if f is a rational function on V, the integer $v_W(f)$ is called the order of f along W, it's the multiplicity of W in the divisor of zeros and poles of f. ∎

∎ **Example 1.4** Let S be a Riemann surface i.e. a one-dimensional complex manifold and let $\mathbb{P} \in S$. The ring $\mathfrak{H}_{\mathbb{P}}$ of functions holomorphic in a neighborhood of $\mathbb{P}$ is a discrete valuation ring, isomorphic to three subring of convergent power series in $\mathbb{C}[[T]]$, its residue field is $\mathbb{C}$. ∎

1.2 Characterisations of Discrete Valuation Rings

Proposition 1.2.1 Let A be a commutative ring. A is a discrete valuation ringif and only if A is a Noetherian ring and the maximal ideal is generated by a non-nilpotent element.

R When we know A is an integral domain, the proof becomes simpler.

Proposition 1.2.2 Let A be a Noetherian integral domain. A is a discrete valuation ringif and only if it satisfies the following two conditions:

- (i)A is integrally closed.
- (ii)A has a unique nonzero prime ideal.

Lemma 1.2.3 Let A be a discrete valuation ring, and let x_i be elements of the field of fractions of A, s.t. $v(x_i) > v(x_1)$ for $i \geq 2$. One then has

$$x_1 + x_2 + \cdot + x_n \neq 0. \tag{1.2}$$

Proposition 1.2.4 Let $(A, \mathfrak{m})$ be a Noetherian local domain of Krull dimension one. The following are equivalent:

(i) A is a DVR.
(ii) A is integrally closed.
(iii) The maximal ideal $\mathfrak{m}$ is principal.
(iv) $\dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1$, where $k = A/\mathfrak{m}$ is the residue field.

R Every invertible ideal of a local ring is principal.

1.3 Dedekind Domains

R Reminder. Let A be an integral domain, K its field of fractions, and let S be a subset of A that is multiplicatively stable and contains 1 (such a set will be called *multiplicative*); suppose also that 0 does not belong to S.

The set of those elements of K of the form x/s, $x \in A$, $s \in S$ is a ring that will be denoted $S^{-1}A$. The map $\mathfrak{p}' \mapsto \mathfrak{p}' \cap A$ is a bijection of the set of prime ideals of $S^{-1}A$ onto the set of those prime ideals of A that do not meet S.

This applies notably when $S = A - \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal of A. The ring $S^{-1}A$ is then denoted $A_{\mathfrak{p}}$; it is a local ring with maximal ideal $\mathfrak{p}A_{\mathfrak{p}}$ and residue field the field of fractions of $A/\mathfrak{p}$; the prime ideals of $A_{\mathfrak{p}}$ correspond to those prime ideals of A that are contained in $\mathfrak{p}$. One says that $A_{\mathfrak{p}}$ is the localisation of A at $\mathfrak{p}$.

Proposition 1.3.1 Let A be a Noetherian integral domain. The following conditions are equivalent:

1. A is a Dedekind domain (i.e., it is integrally closed and has Krull dimension one).
2. For every non-zero prime ideal $\mathfrak{p}$ of A, the localization $A_{\mathfrak{p}}$ is a discrete valuation ring (DVR).

R Let A be a subring of a field K, S be a multiplicative subset of A not containing 0. An element of K is integral on $S^{-1}A$ if and only if it has the form of a'/s where a' is integral on A and s belongs to S (Passage to rings of fractions commutes with integral closure).

■ **Example 1.5** Every principal ideal domain is Dedekind domain. The ring of integers of an algebraic number field is Dedekind domain . If V is an affine algebraic variety defined on an algebraically closed field k, the coordinate ring $k[V]$ of V is a Dedekind domain if and only if V is non-singular, irreducible and of dimension ≤ 1. ■

Proposition 1.3.2 In a Dedekind domain , every nonzero fractional ideal is invertible.

Corollary 1.3.3 The nonzero fractional ideals of a Dedekind domain consist a group under multiplication. This group is called the ideal group of the ring.

Proposition 1.3.4 If $x \in A, x \neq 0$, the only finitely many prime ideals contain x.

Corollary 1.3.5 If denote $v_{\mathfrak{p}}$ the valuation of K defined by $A_{\mathfrak{p}}$, then for every $x \in K^*$, the number $v_{\mathfrak{p}}(x)$ is almost all zero.

Proposition 1.3.6 Every fractional ideal α of A can be written uniquely as the form

$$a = \prod p^{v_{\mathfrak{p}}(a)}. \tag{1.3}$$

where $v_{\mathfrak{p}}(a)$ are integers almost all zero.

The following formulas are immediate:

$$v_{\mathfrak{p}}(a \cdot b) = v_{\mathfrak{p}}(a) + v_{\mathfrak{p}}(b) \tag{1.4}$$

$$v_{\mathfrak{p}}((b : a)) = v_{\mathfrak{p}}(b \cdot a^{-1}) = v_{\mathfrak{p}}(b) - v_{\mathfrak{p}}(a) \tag{1.5}$$

$$v_{\mathfrak{p}}(a + b) = \inf(v_{\mathfrak{p}}(a), v_{\mathfrak{p}}(b)) \tag{1.6}$$

$$v_{\mathfrak{p}}(xA) = v_{\mathfrak{p}}(x). \tag{1.7}$$

Furthermore,

Lemma 1.3.7 — Approximation Lemma. Let k be a positive integer, $\mathfrak{p}_i$ be distinct ideals of A for every $i, 1 \leq i \leq k$, x_i elements of K, and n_i integers. Then exists an $x \in K$ s.t. $v_{\mathfrak{p}_i}(x - x_i) \geq n_i$, and $v_{\mathfrak{q}}(x) \geq 0$ for $\mathfrak{q} \neq \mathfrak{p}_1, \mathfrak{p}_2, \cdots, \mathfrak{p}_k$.

Corollary 1.3.8 A Dedekind domain with only finitely many prime ideals is principal.

1.4 Extensions

In this section, let K be a field and let L be a finite extension of K of degree $n = [L : K]$. Let A be a Dedekind domain with field of fractions K. We denote by B the integral closure of A in L. We know that $K \cdot B = L$; in particular, the field of fractions of B is L. We make the following crucial hypothesis:

(F) The ring B is a finitely generated A-module.

R This hypothesis (F) holds, for instance, when L/K is a separable extension. It also holds when A is an algebra of finite type over a field, or when A is a complete discrete valuation ring.

Proposition 1.4.1 If A is a Dedekind domain, then B is Dedekind.

Lemma 1.4.2 Let $A \subseteq B$ be rings, with B is the integral closure of A. If $\mathfrak{P} \subseteq \mathfrak{Q}$ is a prime ideal of B and satisfies $\mathfrak{P} \cap A = \mathfrak{Q} \cap A$, then $\mathfrak{P} = \mathfrak{Q}$.

Keep the hypothesis above. If $\mathfrak{P}$ is a nonzero prime ideal of B and if $\mathfrak{p} = \mathfrak{P} \cap A$, we say $\mathfrak{P}$ divides $\mathfrak{p}$ or $\mathfrak{P}$ is above $\mathfrak{p}$, and denote it $\mathfrak{P}|\mathfrak{p}$.

This relation is also equivalent to that $\mathfrak{P}$ contains the ideal $\mathfrak{p}B$ generated by $\mathfrak{p}$. Denoted by $e_{\mathfrak{P}}$ the expontent of $\mathfrak{P}$ in the decomposition of $\mathfrak{p}B$ into prime ideals, thus:

$$e_{\mathfrak{P}} = v_{\mathfrak{P}}(\mathfrak{p}B), \mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{p}}}. \tag{1.8}$$

The integer $e_{\mathfrak{P}}$ is called the ramification index of $\mathfrak{P}$ in the extension L/K.

On the other hand, if $\mathfrak{P}$ divides $\mathfrak{p}$, the the field $B/\mathfrak{P}$ is the extension of the field $A/\mathfrak{p}$. Since B is finitely generated on A, $B/\mathfrak{P}$ is extension of $A/\mathfrak{p}$ with finite degree. The degree of the extension is called the residue degree of $\mathfrak{P}$ in the extension L/K, denoted by $f_{\mathfrak{P}}$, thus:

$$f_{\mathfrak{P}} = [B/\mathfrak{P} : A/\mathfrak{p}]. \tag{1.9}$$

When there;s only one prime ideal $\mathfrak{P}$ can divides $\mathfrak{p}$ and $f_{\mathfrak{P}} = 1$, we say L/K is totally ramified at $\mathfrak{p}$.

When $e_{\mathfrak{P}} = 1$ and $B/\mathfrak{P}$ is separable over $A/\mathfrak{p}$, we say L/K is unramified at $\mathfrak{P}$. If L/K is unramified for all prime ideal $\mathfrak{P}$ divides $\mathfrak{p}$, we say L/K is unramified above or at $\mathfrak{p}$.

Proposition 1.4.3 Let $\mathfrak{p}$ is a nonzero prime ideal of A, the ring $B/\mathfrak{p}B$ is a $A/\mathfrak{p}$-algebra with the degree $n = [L : K]$, is isomorphic to the product $\prod_{\mathfrak{P}|\mathfrak{p}} B.\mathfrak{P}^{e_{\mathfrak{P}}}$, we have:

$$n = \sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}} f_{\mathfrak{P}}. \tag{1.10}$$

Corollary 1.4.4 The prime ideal $\mathfrak{P}$ which divides a prime ideal $\mathfrak{p}$ of A is at least 1 and at most n. If A has only finite ideal, then so has B, thus is principal.

R When the hypothesis (F) doesn't hold, the sum of $e_{\mathfrak{P}} f_{\mathfrak{P}}$ is still equal to the degree of $B/\mathfrak{p}B$, but this degree can be $< n$.

Let $\mathfrak{P}$ is a nonzero prime ideal of B, and $\mathfrak{p} = A \cap \mathfrak{P}$. Obviously, if $x \in K$, then $v_{\mathfrak{P}}(x) = e_{\mathfrak{p}} v_{\mathfrak{p}}(x)$. We say the valuation $v_{\mathfrak{P}}$ prolongs or extends the valuation $v_{\mathfrak{p}}$ with index $e_{\mathfrak{P}}$. Conversely:

Theorem 1.4.5 — The Fundamental Identity. Let $\mathfrak{p}$ be a non-zero prime ideal of A. Let the factorization of the ideal $\mathfrak{p}B$ in B be

$$\mathfrak{p}B = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_g^{e_g} \tag{1.11}$$

where the $\mathfrak{P}_i$ are the distinct prime ideals of B lying above $\mathfrak{p}$. For each i, the integer $e_i = v_{\mathfrak{P}_i}(\mathfrak{p}B)$ is called the **ramification index** of $\mathfrak{P}_i$ over $\mathfrak{p}$. The degree of the residue field extension $f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$ is called the **inertia degree**. These quantities are related by the fundamental identity:

$$[L : K] = \sum_{i=1}^{g} e_i f_i \tag{1.12}$$

1.5 The Norm and Inclusion Homomorphisms

We denote I_A, I_B the ideal group of A and B. We will define two homomorphisms:

$$i : I_A \to I_B \tag{1.13}$$

$$N : I_B \to I_A \tag{1.14}$$

Since I_A (resp. I_B) is the free abelian group generated by the nonzero prime ideal $\mathfrak{p}$ of A (resp. $\mathfrak{P}$ of B), so we just define $i(\mathfrak{p})$ and $N(\mathfrak{P})$:

$$i(\mathfrak{p}) = \mathfrak{p}B = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{P}}} \tag{1.15}$$

$$N(\mathfrak{P}) = \mathfrak{p}^{f_{\mathfrak{P}}} \text{ if } \mathfrak{P}|\mathfrak{p}. \tag{1.16}$$

We can see $N(i(\mathfrak{a})) = \mathfrak{a}^n$ for every $\mathfrak{a} \in I_A$. The homomorphism i maps the ideal $\mathfrak{a}$ of A to the ideal $\mathfrak{a}B$ of B generated by $\mathfrak{a}$.

These two homomorphisms may be interpreted in a more suggestive manner by means of suitable Grothendieck groups:

Let $\mathscr{C}_A$ be the category of A-module with finite length. If $M \in \mathscr{C}_A$ and if M is of length m, M has a composition series:

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_m = M, \tag{1.17}$$

every M_i/M_{i-1} being isomorphic to a simple A-module, i.e. to a quotient $A/\mathfrak{p}_i$, where $\mathfrak{p}_i$ is a nonzero prime ideal of A. By the Jordan-Holder theorem, the sequence of $A/\mathfrak{p}_i$ only depends on M, and we can define

$$\chi_A(M) = \prod p_i. \tag{1.18}$$

■ **Example 1.6** When $M = \mathfrak{b}/\mathfrak{a}$, where $\mathfrak{b}$ and $\mathfrak{a}$ are nonzero fractional ideals with $a \subseteq b$, one has $\chi_A(M) = \mathfrak{a}\cdot\mathfrak{b}^{-1}$. In particular, $\chi_A(A/\mathfrak{a}) = \mathfrak{a}$ if $\mathfrak{a} \subseteq A$. ■

The map $\chi_A : \mathscr{C}_A \to I_A$ is multiplicative, that's if there's a exact sequence of A-module with finite length:

$$0 \to M' \to M \to M'' \to 0, \tag{1.19}$$

we have $\chi_A(M) = \chi_A(M')\chi_A(M'')$. Conversely, every multiplicative $f : \mathscr{C}_A \to G$, where G is an abelian group, can be uniquely written as the form of $g \circ \chi_A$, where g is a homomorphism of I_A to G. In other words, χ_A identifies the Grothendieck group $\mathscr{C}_A$ with the ideal group I_A.

SImilarly, we define $\mathscr{C}_B$ and $\chi_B : \mathscr{C}_B \to I_B$. Obviously, every B-module with finite length is also of finite length as an A-module. Thus we can define an exact functor $\mathscr{C}_B \to \mathscr{C}_A$, hence a homomorphism of I_B to I_A. This homomorphism is just the norm. That's saying:

Proposition 1.5.1 If M is a B-module with finite length, then $\chi_A(M) = N(\chi_B(M))$

Every A-module M of finite length defines by tensor product with B a module M_B of finite length.

Proposition 1.5.2 If M is an A-module with finite length, then $\chi_B(M_B) = i(\chi_A(M))$

Proposition 1.5.3 If $x \in L$ then $N(x,B) = N_{L/K}(x)A$.

Lemma 1.5.4 Let A be a principal ideal domain , $u : A^n \to A^n$ is a linear map with $\det(u) \neq 0$, then $\det(u)A = \chi_A(\mathrm{Coker}\, u)$

1.6 Example: Simple Extensions

Let A be a local ring and the residue field of it is k. Let n be a positive integer, $f \in A[X]$ be a monic polynomial of degree n. Let B_f is the quotient ring of $A[X]$ by the principal ideal (f) generated by f. It is a free and finite type A-algebra over A, with the basis $\{1, X, \cdots, X^{n-1}\}$. Denote $\mathfrak{m}$ the maximal ideal of A, and set $\overline{B_f} = B_f/\mathfrak{m}B_f = A[X]/(\mathfrak{m}, f)$. If denotes by $\overline{f}$ the image of $f \in k[X]$ by reduction mod $\mathfrak{m}$. Then we have

$$\overline{B_f} = k[X]/(\overline{f}) \tag{1.20}$$

Let $\overline{f} = \prod_{i\in I} \varphi_u^{e_i}$ be the decomposition of the polynomial $\overline{f}$ into irreducible factors in $k[X]$, and for each i, choose a polynomial $g_i \in A[X]$ satisfies $\overline{g_i} = \varphi_i$. We have:

Lemma 1.6.1 Let $\mathfrak{m}_i = (\mathfrak{m}, g_i)$ be the ideal of B_f generated by g_i and the canonical image of B_f. The ideals $\mathfrak{m}_i, i \in I$ is maximal and distinct, and every maximal ideal of $\overline{B_f}$ is equal to one of them. The quotient field is isomorphic to the field $k_i = k[X]/(\varphi_i)$.

Suppose that A is a discrete valuation ring; we give two special cases in which B_f is also a discrete valuation ring.

1.6.1 (i)Unramified case

Proposition 1.6.2 If A is a discrete valuation ring, and if $\overline{f}$ is irreducible, then B_f is a discrete valuation ring, the maximal ideal of it is $\mathfrak{m}B_f$, and the residue field is $k[X]/(\overline{f})$.

Corollary 1.6.3 If K is the field of the fractions of A, the the polynomial f is irreducible in $K[X]$. If L denotes the field $K[X]/(f)$, then the ring B_f is the integral closure of A in L.

Corollary 1.6.4 If $\overline{f}$ is a separable polynomial, the extension L/K is unramified.

Proposition 1.6.5 Let A be a discrete valuation ring, K be the field of fractions, and let maps L be the finite extension of K with the degree n. Let B be the integral closure of A in L. Suppose B is a discrete valuation ring, and the residue field $\overline{L}$ of B is the extension of the residue field k of A with the degree n. Let x be any element in B, the image $\bar{x}$ in $\overline{L}$ generate $\overline{L}$ on k, and let f be the characteristic polynomial of x on K. Then the homomorphism of $A[X]$ to B which maps X to x defines a isomorphism of B_f to B.

1.6.2 (ii)Totally ramified case

Proposition 1.6.6 Suppose A is a discrete valuation ringand that f has the following form:

$$f = X^n + a_1 X^{n-1} + \cdots + a_n, a_i \in \mathfrak{m}, a_i \notin \mathfrak{m}^2. \tag{1.21}$$

Then B_f is a discrete valuation ring, with the maximal ideal is generated by the image x of X, and the residue field is k.

Corollary 1.6.7 The polynomial f is irreducible in $K[X]$, and if $L = K[X]/(f)$, then B_f is the integral closure of A in L.

Here again there is a converse:

Proposition 1.6.8 Let A be a discrete valuation ring, K be the residue field, and let L be the finite extension of K with the degree n. Let B be the integral closure of A in L. Suppose B is a discrete valuation ring, and the associated valuation prolongs that of A with ramification index n. Let x be a uniformizing element of B, and let f be the characteristic polynomial of x on K. Then f is an Eisenstein polynomial, and the homomorphism of $A[X]$ to B which maps X to x defines an isomorphism of B_f to B.

1.7 Galois Extensions

We suppose L/K is a Galois extension and the Galois group is $G(L/K)$.

Corollary 1.7.1 Let $\mathfrak{p}$ be a non-zero prime ideal of A. The ramification indices $e_{\mathfrak{P}}$ and the inertia degrees $f_{\mathfrak{P}}$ are the same for all prime ideals $\mathfrak{P}$ of B lying above $\mathfrak{p}$. Let us denote them by $e_{\mathfrak{p}}$ and $f_{\mathfrak{p}}$. If $g_{\mathfrak{p}}$ is the number of prime ideals of B above $\mathfrak{p}$, the fundamental identity becomes:

$$n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}} \tag{1.22}$$

Corollary 1.7.2 Let $\mathfrak{p}$ is a nonzero prime ideal of A. The integers $e_{\mathfrak{P}}$ and $f_{\mathfrak{P}}$ only depend on $\mathfrak{p}$. If denote them by $e_{\mathfrak{p}}, f_{\mathfrak{p}}$, and if $g_{\mathfrak{p}}$ denote the number of prime ideal $\mathfrak{P}$ divides $\mathfrak{p}$,then

$$n = e_{\mathfrak{p}} f_{\mathfrak{p}} g_{\mathfrak{p}}. \tag{1.23}$$

Let $\mathfrak{P}$ be a prime ideal of B lying above $\mathfrak{p}$.

Definition 1.7.1 The **decomposition group** of $\mathfrak{P}$, denoted $D_{\mathfrak{P}}$, is the subgroup of G consisting of automorphisms that fix $\mathfrak{P}$:

$$D_{\mathfrak{P}} = \{s \in G \mid s(\mathfrak{P}) = \mathfrak{P}\} \tag{1.24}$$

The index $[G : D_{\mathfrak{P}}]$ is equal to $g_{\mathfrak{p}}$. The fixed field of $D_{\mathfrak{P}}$, denoted K_D, is called the **decomposition field**.

Every automorphism $s \in D_{\mathfrak{P}}$ induces an automorphism $\bar{s}$ of the residue field $\overline{L} = B/\mathfrak{P}$ over $\overline{K} = A/\mathfrak{p}$. This gives a group homomorphism $\varepsilon : D_{\mathfrak{P}} \to \mathrm{Gal}(\overline{L}/\overline{K})$.

Definition 1.7.2 The **inertia group** of $\mathfrak{P}$, denoted $T_{\mathfrak{P}}$, is the kernel of the homomorphism ε. An element $s \in D_{\mathfrak{P}}$ is in $T_{\mathfrak{P}}$ if and only if it acts trivially on the residue field, i.e.,

$$s(b) \equiv b \pmod{\mathfrak{P}} \quad \text{for all } b \in B \tag{1.25}$$

The fixed field of $T_{\mathfrak{P}}$, denoted K_T, is called the **inertia field**.

Proposition 1.7.3 The residue extension L/R is normal and the homomorphism

$$\varepsilon : D \to G(L/K) \tag{1.26}$$

defines isomorphism of D/T onto $G(L/K)$.

We continue to denote by $\overline{L_s}$ the largest separable extension of $\overline{K}$ in $\overline{L}$. We have shown that it's a Galois extension of $\overline{K}$ with Galois group D/T. Take

$$f_0 = [\overline{L_s} : \overline{K}] = [\overline{L} : \overline{K}]_s, p^s = [\overline{L} : \overline{L_s}] = [\overline{L} : \overline{K}]_i, \tag{1.27}$$

so that

$$f = f_0 p^s. \tag{1.28}$$

Proposition 1.7.4 With the notation as above, let x, x_T, w_D, v be the discrete valuations defined by the ideals $\mathfrak{P}, \mathfrak{P}_T, \mathfrak{P}_D, \mathfrak{p}$. Then

- (a)$[L : K_T] = ep^s, [K_T, K_D] = f_0, [K_D, D] = g$.
- (b)w prolongs w_T with index e; w_T and w_D prolong v with index 1.
- (c)$\overline{K_T} = \overline{L_s}, \overline{K_D} = \overline{K}$. In particular, $[\overline{L} : \overline{K_T}] = p^s, [\overline{K_T}, \overline{K_D}] = f_0, [\overline{K_D}, \overline{K}] = 1$.

Corollary 1.7.5 If $\overline{L}/\overline{K}$ is separable then it is a Galois extension with Galois group D/T, and we have $\overline{K_T} = \overline{L}$,$[L : K_T] = e, [K_T : K_D] = f, [K_D : K] = g$.

Indeed, $p^s = 1$ in that case.

R The residue extension $\overline{L}/\overline{K}$ is separable in each of the following case (which cover most of the applications):

- $\overline{K}$ is perfect.
- The order of the inertia group T is prime to the characteristic p of the residue field $\overline{K}$ (indeed, we have seen that the order of this group is divisible by p^s).

Proposition 1.7.6

- (a)$\mathrm{D}(L/E) = \mathrm{D}(L/K) \cap \mathrm{G}(L/E)$ and $\mathrm{T}(L/E) = \mathrm{T}(L/K) \cap \mathrm{G}(L/E)$.

- (b)If E/K is Galois, the diagram below is commutative, and its rows and columns are exact:

$$\begin{array}{ccccccccc}
 & & 1 & & 1 & & 1 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & T(L/E) & \longrightarrow & T(L/K) & \longrightarrow & T(E/K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & D(L/E) & \longrightarrow & D(L/K) & \longrightarrow & D(E/K) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & G(\overline{L}/\overline{E}) & \longrightarrow & G(\overline{L}/\overline{K}) & \longrightarrow & G(\overline{E}/\overline{K}) & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 1 & & 1 & & 1 & &
\end{array}$$

R When one wants to study the decomposition or inertia groups above a given prime ideal $\mathfrak{p}$ of A , one may, if one wishes, replace A by the discrete valuation ring $A_{\mathfrak{p}}$; this reduction to the local case can be pushed further: one may even replace $A_{\mathfrak{p}}$ by its completion.

1.8 Frobenius Substitution

Definition 1.8.1 — Frobenius Element. Let L/K be a Galois extension. Let $\mathfrak{P}$ be a prime ideal of B above a prime ideal $\mathfrak{p}$ of A. Assume that the extension is **unramified** at $\mathfrak{P}$ (so the inertia group $T_{\mathfrak{P}} = \{1\}$) and that the residue field $\overline{K} = A/\mathfrak{p}$ is **finite** with q elements.

In this case, the decomposition group $D_{\mathfrak{P}}$ is isomorphic to the Galois group $\mathrm{Gal}(\overline{L}/\overline{K})$. This latter group is cyclic, generated by the Frobenius automorphism $x \mapsto x^q$. The unique element $s_{\mathfrak{P}} \in D_{\mathfrak{P}}$ that corresponds to this generator is called the **Frobenius element** (or Frobenius substitution) of $\mathfrak{P}$. It is uniquely characterized by the property:

$$s_{\mathfrak{P}}(b) \equiv b^q \pmod{\mathfrak{P}} \quad \text{for all } b \in B \tag{1.29}$$

The Frobenius element $s_{\mathfrak{P}}$ generates the decomposition group $D_{\mathfrak{P}}$.

$$s_{\mathfrak{P}}(b) \equiv b^q \pmod{\mathfrak{P}} \quad \text{for all } b \in B. \tag{1.30}$$

The element $s_{\mathfrak{P}}$ is called the Frobenius substitution of $\mathfrak{P}$ (or attached to $\mathfrak{P}$). Its definition shows that it generates the decomposition group of $\mathfrak{P}$; its order is equal to $f_{\mathfrak{P}}$. It is often denoted $(\mathfrak{P}, L/K)$. Here are two samples of functorial properties that it enjoys:

Proposition 1.8.1 Let E be a subfield of L containing K, and let $\mathfrak{P}_E = \mathfrak{P} \cap E$. Then:

a) $(\mathfrak{P}, L/E) = (\mathfrak{P}, L/K)^f$, with $f = [E : K]$.

b) If E is Galois over K, the image of $(\mathfrak{P}, L/K)$ in $G(E/K)$ is $(\mathfrak{P}_E, E/K)$.

Returning to the extension L/K, if $t \in G(L/K)$, one has (by transport of structure) the formula:

$$(t(\mathfrak{P}), L/K) = t(\mathfrak{P}, L/K)t^{-1}. \tag{1.31}$$

In particular, if $G(L/K)$ is abelian, $(\mathfrak{P}, L/K)$ depends only on $\mathfrak{p} = \mathfrak{P} \cap A$; it is the Artin symbol of $\mathfrak{p}$ and is denoted $(\mathfrak{p}, L/K)$. One defines by linearity the Artin symbol for any ideal $\mathfrak{a}$ of A that does not contain a ramified prime, and one denotes it again by $(\mathfrak{a}, L/K)$ [the notations

$$\left(\frac{L/K}{\mathfrak{a}}\right), \text{ or simply } \left(\frac{L}{\mathfrak{a}}\right), \tag{1.32}$$

are also found in the literature].

We state without proof:

Theorem 1.8.2 — Artin Reciprocity Law. Let L be a finite abelian extension of a number field K, A the ring of integers of K, and $\mathfrak{p}_i$ the prime ideals of A that ramify in L/K. Then there exist positive integers n_i such that the conditions

(*i*) $v_{\mathfrak{p}_i}(x-1) \geq n_i$ for all i,

(*ii*) x is positive in every real embedding of K that is not induced by a real embedding of L, imply $(xA, L/K) = 1$.

Furthermore, every automorphism $s \in G(L/K)$ is of the form $(\mathfrak{a}, L/K)$ for a suitable ideal $\mathfrak{a}$ (in fact, one even has $s = (\mathfrak{p}, L/K)$ for infinitely many prime ideals $\mathfrak{p}$ of A).

■ **Example 1.7** Let n be a positive integer, $K = \mathbb{Q}$, and let $L = \mathbb{Q}(\zeta_n)$ be the field of nth roots of unity. The Galois group $G(L/K)$ is a subgroup $G'(n)$ of the group $G(n)$ of invertible elements of $\mathbb{Z}/n\mathbb{Z}$ (cf. Bourbaki, *Alg.*, Chap. V); if $x \in G'(n)$, the automorphism σ_x associated to x transforms a root of unity ζ_n into its xth power. If $(p,n) = 1$, one sees easily (e.g., by using the results of Chap. IV, §4) that p is unramified, and that the Artin symbol $(p, L/K)$ is equal to σ_p. It follows by linearity that the Artin symbol of a positive integer m prime to n is equal to σ_m. Consequently, $G'(n) = G(n)$, that is to say

$$[L : K] = \varphi(n) \tag{1.33}$$

(irreducibility of the cyclotomic polynomial). Moreover, if $m > 0$, and if $m \equiv 1 \pmod{n}$, one gets $(m, L/K) = 1$, which verifies the Artin reciprocity law for this case. [The fact that $s = (p, L/K)$ for infinitely many primes p is equivalent to Dirichlet's theorem on the infinity of prime numbers belonging to an arithmetic progression.] ■

Once the Artin symbol has been determined in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$, for every subfield E of $\mathbb{Q}(\zeta_n)$. Such a field is abelian over $\mathbb{Q}$. Conversely, every finite abelian extension of $\mathbb{Q}$ can be obtained in this way (theorem of Kronecker-Weber). In particular, every quadratic field $\mathbb{Q}(\sqrt{d})$ can be embedded in a suitable field $\mathbb{Q}(\zeta_n)$; this result can also be checked by various elementary methods (Gauss sums, for example). Thus one has a procedure for determining the Artin symbol $(p, \mathbb{Q}(\sqrt{d})/\mathbb{Q})$; by comparing the result with that given by a direct computation, one obtains the *quadratic reciprocity law*.

2. Completion

2.1 Absolute Values and the Topology Defined by a Discrete Valuation

Let K be a field with a discrete valuation v. We can define a metric topology on K using an **absolute value**.

Definition 2.1.1 — Absolute Value. An **absolute value** on a field K is a function $|\cdot| : K \to \mathbb{R}_{\geq 0}$ satisfying for all $x, y \in K$:

1. $|x| = 0$ if and only if $x = 0$.
2. $|xy| = |x||y|$.
3. $|x+y| \leq |x| + |y|$ (Triangle Inequality).

If it satisfies the stronger condition $|x+y| \leq \max(|x|, |y|)$, it is called **non-archimedean** or **ultrametric**. Otherwise, it is **archimedean**.

Given our discrete valuation v, we can construct a non-archimedean absolute value. Choose a real number $c \in (0,1)$ and define:

$$|x|_v = c^{v(x)} \quad \text{for } x \in K^\times, \quad \text{and} \quad |0|_v = 0.$$

This is an ultrametric absolute value, and the topology it induces on K is independent of the choice of c. The ideals $\mathfrak{m}^n = \{x \in K \mid v(x) \geq n\}$ form a basis of open neighborhoods of 0 in this topology.

Theorem 2.1.1 — Ostrowski's Theorem. Every non-trivial absolute value on the field of rational numbers $\mathbb{Q}$ is equivalent to either:

1. The standard real absolute value $|\cdot|_\infty$.
2. The p-adic absolute value $|\cdot|_p$ for some prime number p.

R This theorem can be generalized. For any number field K, its absolute values fall into two classes:

- **Archimedean absolute values**, which arise from embeddings of K into $\mathbb{C}$.

- **Non-archimedean absolute values**, which arise from the prime ideals of its ring of integers (i.e., from discrete valuations).

The formula $|f(x)|^c$ mentioned in the original text describes the archimedean case, not the general case.

With the concept of a topology from an absolute value, we can now properly define a local field.

Definition 2.1.2 — Local Field. A **local field** is a field K equipped with a non-trivial absolute value, such that K is locally compact with respect to the topology induced by this absolute value.

■ **Example 2.1** The classical examples of local fields are:

- The field of real numbers $\mathbb{R}$ and complex numbers $\mathbb{C}$ (archimedean local fields).
- The field of p-adic numbers $\mathbb{Q}_p$ for any prime p.
- Finite extensions of $\mathbb{Q}_p$.
- The field of formal Laurent series $\mathbb{F}_q((T))$ over a finite field $\mathbb{F}_q$.

All these fields are completions of a global field ($\mathbb{Q}$ or $\mathbb{F}_q(T)$) with respect to one of its absolute values. ■

2.2 Extensions of a Complete Field

Proposition 2.2.1 Let K be a field on which a discrete valuation v is defined, having a valuation ring A. Suppose that K is complete in the topology which is defined by v. Let L/K is a finite extension of K, and B be the integral closure of A in L. Then B is a discrete valuation ring, and a free A-module with the rank n. Furthermore, L is complete in the topology defined by B.

Corollary 2.2.2 If e (resp. f) represents the ramification index (resp. the residue degree) of L over K, then $ef = n$.

Corollary 2.2.3 There's a unique valuation w of L that prolongs v.

Corollary 2.2.4 Two elementary of L which are conjuate over K have the same valuation.

Corollary 2.2.5 For every $x \in L$, $w(x) = \frac{1}{n} v\left(N_{L/K}(x)\right)$, where $n = [L : K]$

In terms of absolute values, this corollary means that the topology of L can be defined by the norm

$$\|x\|_L = \left\|N_{L/K}(x)\right\|_K . \tag{2.1}$$

Note that if K is locally compact and $\|\cdot\|_K$ is normalised, then so is $\|\cdot\|_L$.

2.3 Extension and Completion

Theorem 2.3.1 Let L/K is an extension of finite degree n, v is a discrete valuation of K with the ring A, and B is the integral closure of A in L. Suppose that A-module B is finitely generated, w_i is the different prolongations of v to L, e_i, f_i is the corresponding numbers. Let $\hat{K}$ and $\hat{L}_i$ is respectively the completions of K and L for v and w_i.

- (i)The field $\hat{L}_i$ is an extension of K of degree $n_i = e_i f_i$.
- (ii)The valuation $\hat{w}_i$ is the unique valuation of $\hat{L}_i$ prolonging $\hat{v}$ and

$$e_i = e(\hat{L}_i/K), \text{ and } f_i = f(\hat{L}_i/\hat{K}). \tag{2.2}$$

- (iii)The canonical homomorphism $\varphi : L \otimes_K \hat{K} \to \prod_i \hat{L}_i$ is an isomorphism.

Corollary 2.3.2 The fields $\hat{L}_i$ are the composites of the extensions $\hat{K}$ and L of K.

Corollary 2.3.3 If $x \in L$, and the characteristic polynomial F of x in L/K is equal to the product of the characteristic polynomial F_i of x in $\hat{L}_i/\hat{K}$. In particular, if Tr and N (resp. Tr_i and N_i) denote the trace and norm of L/K (resp. $\hat{L}_i/\hat{K}$), then

$$\mathrm{Tr}(x) = \sum \mathrm{Tr}_i(x), \mathrm{N}(x) = \prod \mathrm{N}_i(x). \tag{2.3}$$

The polynomial F is also the characteristic polynomial of x in K-algebra $L \otimes_K \hat{K}$.

Corollary 2.3.4 If L/K is separable, then so is $\hat{L}_i/\hat{K}$.

Corollary 2.3.5 If L/K is a Galois extension with group G, and if D_i denote the decomposition group of w_i in G, then the extension $\hat{L}_i/\hat{K}$ is Galois with Galois group D_i.

The isomorphism $\varphi : L \otimes_K \hat{K} \to \prod_i \hat{L}_i$ merely expresses the decomposition of $L \otimes_K \hat{K}$ considered as a Galois algebra in this case.

We now go on to the discrete valuation ringitself:

Proposition 2.3.6 With the hypothesis and notation as above, let B_i be the valuation ring of the valuation w_i. The canonical homomorphism

$$\varphi : B \otimes_A \hat{A} \to \prod_i \hat{B}_i \tag{2.4}$$

is then an isomorphism.

R The ring $B \otimes_A \hat{A}$is the completion $\hat{B}$ of B for the natural topology on the semilocal ring B. Its decomposition into direct factors $\hat{B}_i$ is a special case of a general property of semilocal rings.

2.4 Structure of Complete Discrete Valuation Rings I: Equal Characteristic Case

Let A be a complete discrete valuation ringwith the field of fractions K and residue field $\hat{K}$. Let S be a system of representatives of $\hat{K}$ in A, π is a uniformizer of A.

Proposition 2.4.1 Every element $a \in A$ can be written uniquely as a convergent series

$$a = \sum_{n \geq 0} s_n \pi^n, \text{ with } s_n \in S. \tag{2.5}$$

Similarly, every element $x \in K$ can be written as

$$x = \sum_{n \geq -\infty} s_n \pi^n, \text{ with } s_n \in S. \tag{2.6}$$

the series requiring only finitely many terms with negative exponents.

■ **Example 2.2** If $A = \mathbb{Z}_p$, we can take S be the set of nonnegative integers, or consists of 0 and the $(p-1)$st roots of unity. ■

Theorem 2.4.2 Let A be a complete discrete valuation ringwith the residue field $\overline{K}$. Suppose A and $\overline{K}$ have the same characteristic and $\overline{K}$ is complete. Then A is isomorphic to $\overline{K}[[T]]$.

It all comes down to showing that A contains a system of representatives which is a field. We will distinguish two cases, depending on the characteristic:

(i) The characteristic of $\overline{K}$ is 0, we need the following propositions:

Proposition 2.4.3 Let A be a local ring which is Hausdorff for the topology defined by the decreasing sequence $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots$ of ideals and complete, s.t. $\mathfrak{a}_n \cdot \mathfrak{a}_m \subseteq \mathfrak{a}_{n+m}$. Suppose that $\overline{K} = A/\mathfrak{a}_1$ is a field with the characteristic 0. Then A contains a system of representatives of $\overline{K}$ which is a field.

Proposition 2.4.4 Let A be a local ring which is Hausdorff for the topology defined by the decreasing sequence $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots$ of ideals and complete, s.t. $\mathfrak{a}_n \cdot \mathfrak{a}_m \subseteq \mathfrak{a}_{n+m}$. Suppose that $\mathfrak{a}_1$ is the maximal ideal of A and let $\overline{K} = A/\mathfrak{a}_1$. Let $f(X)$be a polynomial with the coefficients in A s.t. the reduced polynomial $\overline{f} \in \overline{K}[X]$ has a simple root λ in $\overline{K}$. Then f has a unique root x in A s.t. $\bar{x} = \lambda$.

(ii)The fields K and$\overline{K}$ have characteristic $p \neq 0$, we need the following results:

We will say that a ring Λ with characteristic p is complete if the endomorphism $x \mapsto x^p$ of Λ is an automorphism (i.e. it's a surjective). Then every element $x \in \Lambda$ has a unique pth root, denoted by $x^{p^{-1}}$. When Λ is a field, this is the usual definition of a perfect field.

Proposition 2.4.5 Let A be a local ring which is Hausdorff for the topology defined by the decreasing sequence $\mathfrak{a}_1 \supseteq \mathfrak{a}_2 \supseteq \cdots$ of ideals and complete, s.t. $\mathfrak{a}_n \cdot \mathfrak{a}_m \subseteq \mathfrak{a}_{n+m}$. Suppose that the residue ring $\overline{K} = A/\mathfrak{a}_1$ is a perfect ring with characteristic p. Then:

- (i)There exists a unique system of representatives $f : \overline{K} \to A$ which commutes with pth powers:$f(\lambda^p) = f(\lambda)^p$.
- (ii)$a \in A$ belongs to $S = f(\overline{K})$ if and only if for all $n \geq 0$, a is a p^nth power.
- (iii)This system of representatives is multiplicative, i.e. we have $f(\lambda\mu) = f(\lambda) \cdot f(\mu)$.
- (iv)If A has characteristic p, this system of representatives is additive, i.e. $f(\lambda + \mu) = f(\lambda) + f(\mu)$.

Lemma 2.4.6 If $a \equiv b \mod \mathfrak{a}_n$, then $a^p \equiv b^p \mod \mathfrak{a}_{n+1}$

2.5 Structure of Complete Discrete Valuation Rings II: Unequal Characteristic Case

Let A be a complete discrete valuation ring, with the field of fractions K, the residue field $\overline{K}$. Suppose the characteristic of A is different from that of $\overline{K}$, i.e. the characteristic of A is 0, and that of $\overline{K}$ is $p \neq 0$. Then we can identify $\mathbb{Z}$ with a subring of A and $p \in \mathbb{Z}$ an element of A. Since p becomes zero in $\overline{K}$, so $v(p) \geq 1$, where v is the discrete valuation associated with A. The integer $e = v(p)$ is called the absolute ramification index of A. Observe that the injection $\mathbb{Z} \to A$ extends by continuity to an injection of the ring $\mathbb{Z}_p$ of p-adic integers into A; when the residue field $\overline{K}$ is finite field with $q = p^f$ elements, we know that A is a free $\mathbb{Z}_p$-module of rank $n = ef$, and K is an extension of degree n

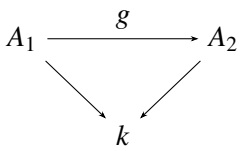
of p-adic field $\mathbb{Q}_p$; the integer e can then ne interpreted as the ramification index of the extension $K/\mathbb{Q}_p$.

Returning to the general case, we will say that A is absolutely unramified if $e = 1$, i.e., if p is a local uniformizer of A.

Theorem 2.5.1 For every perfect field k of characteristic p, there exists a complete discrete valuation ring, and only one up to unique isomorphism which is absolutely unramified and has k as its residue field.

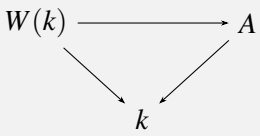
We denote this ring $W(k)$.

If A_1 and A_2 satisfy the conditions of the theorem, there's a unique isomorphism $g : A_1 \to A_2$ which makes commutative the diagram:



In the ramified case, we have:

Theorem 2.5.2 Let A be a complete discrete valuation ring, whose characteristic is different from that of the residue field k. Let e is its absolute ramification index. Then there exists a unique homomorphism of $W(k)$ to A, which makes commutative the diagram:



This homomorphism is injective and A is a free $W(k)$-module of rank e.

■ **Example 2.3** Let X_α be a family of indeterminates, and let S be the ring of $p^{-\infty}$ polynomials in X_α with integer coefficients, i.e. the union of the rings $\mathbb{Z}\left[X_\alpha^{p^{-\infty}}\right]$ for all n. If we provide S with p-adic filtration $\{p^n S\}_{n\geq 0}$ and complete it, we obtain a strict p-ring that will be denoted $\hat{S} = \hat{\mathbb{Z}}\left[X_\alpha^{p^{-\infty}}\right]$. The residue ring $\hat{S}/p\hat{S}$ is the ring $\mathbb{F}_p\left[X_\alpha^{p^{-\infty}}\right]$. It's perfect of characteristic p.

Note that the X_α are multiplicative representatives in $\hat{S}$ since they admit p^nth roots for all n. ■

Let us apply this to the case in which the indeterminates are $X_0,\ldots,X_n,\ldots$, and $Y_0,\ldots,Y_n,\ldots$; in the ring $\hat{\mathbb{Z}}\left[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}\right]$ thus obtained, consider the two elements

$$x = \sum_{i=0}^{\infty} X_i p^i \quad \text{and} \quad y = \sum_{i=0}^{\infty} Y_i p^i. \tag{2.7}$$

If $*$ denotes one of the operations $+, \times, -$, the composite $x * y$ is an element of the ring, therefore can be written in a unique way in the form:

$$x * y = \sum_{i=0}^{\infty} f(Q_i^*)\, p^i, \quad \text{with } Q_i^* \in \mathbb{F}_p\left[X_i^{p^{-\infty}}, Y_i^{p^{-\infty}}\right]. \tag{2.8}$$

The Q_i^* are $p^{-\infty}$-polynomials with coefficients in the prime field $\mathbb{F}_p$; one can speak of the value of such a polynomial when elements of a perfect ring k of characteristic p are substituted for the indeterminates. We will see that these functions allow us to determine the structure of a strict p-ring. More precisely:

Proposition 2.5.3 Let A be a p-ring with residue ring k and let $f : k \to A$ be the system of multiplicative representatives in A. Let $\{\alpha_i\}$ and $\{\beta_i\}$ be two sequences of elements of k. Then

$$\sum_{i=0}^{\infty} f(\alpha_i)\, p^i * \sum_{i=0}^{\infty} f(\beta_i)\, p^i = \sum_{i=0}^{\infty} f(\gamma_i)\, p^i \tag{2.9}$$

with $\gamma_i = Q_i^*(\alpha_0, \alpha_1, \ldots; \beta_0, \beta_1, \ldots)$.

This is Teichmüller representatives.

Proposition 2.5.4 Let A and A' be two p-rings with residue rings k and k', and suppose that A is strict. For every homomorphism $\phi : k \to k'$, there exists a unique homomorphism $g : A \to A'$ making commutative the diagram:

$$\begin{array}{ccc} A & \xrightarrow{g} & A' \\ \downarrow & & \downarrow \\ k & \xrightarrow{\phi} & k' \end{array}$$

Corollary 2.5.5 Two strict p-rings having the same residue ring are canonically isomorphic.

Lemma 2.5.6 Let $\varphi : k \to k'$ be a surjective homomorphism, the rings k and k' being perfect of characteristic p. If there exists a strict p-ring A with residue ring k, then there also exists a strict p-ring A' with residue ring k'.

Theorem 2.5.7 For every perfect ring k of characteristic p, there exists a unique strict p-ring $W(k)$ with residue ring k.

We have see that $W(k)$ is a functor of k. There's an isomorphism $\mathrm{Hom}(k,k') \simeq \mathrm{Hom}(W(k), W(k'))$.

R The functions Q_i^* that define the operations of $W(k)$ involve the p^nth roots of the X_n and Y_n. If one wishes to have polynomials in the usual sense, it is necessary to re-define the coordinates α_i of a by:

$$a = \sum_{i=0}^{\infty} f(\alpha_i)^{p^{-i}} p^i. \tag{2.10}$$

One is then led to introduce the Witt vectors which we study in the next section.

2.6 Witt Vectors

Let p be a prime number, $(X_0, \ldots, X_n, \ldots)$ a sequence of indeterminates, and consider the following polynomials (called Witt polynomials):

$$\begin{aligned} W_0 &= X_0, \\ W_1 &= X_0^p + pX_1, \\ &\vdots \\ W_n &= \sum_{i=0}^{i=n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \cdots + p^n X_n. \end{aligned} \tag{2.11}$$

If $\mathbb{Z}'$ denotes the ring $\mathbb{Z}[p^{-1}]$, it is clear that the X_i can be expressed as polynomials with respect to the W_i with coefficients in $\mathbb{Z}'$:

$$X_0 = W_0, \quad X_1 = p^{-1}W_1 - W_0^p, \ldots, \text{etc.} \tag{2.12}$$

Let $(Y_0, \ldots, Y_n, \ldots)$ be another sequence of indeterminates.

Theorem 2.6.1 For every $\Phi \in \mathbb{Z}[X,Y]$, there exists a unique sequence $\varphi_0, \varphi_1, \varphi_2, \cdots, \varphi_n, \cdots$ in $\mathbb{Z}[X_0, X_1, X_2, \cdots, X_n, \cdots, Y_0, Y_1, Y_2, \cdots, Y_n, \cdots]$ s.t.

$$W_n(\varphi_0, \varphi_1, \varphi_2, \cdots, \varphi_n, \cdots) = \Phi(W_n(X_0, X_1, X_2, \cdots, X_n, \cdots), W_n(Y_0, Y_1, Y_2, \cdots, Y_n, \cdots)), n = 0, 1, 2, \cdots. \tag{2.13}$$

We now denote $S_0, S_1, S_2, \cdots, S_n, \cdots$ (resp. $P_0, P_1, P_2, \cdots, P_n, \cdots$) the polynomials $\varphi_0, \varphi_1, \varphi_2, \cdots, \varphi_n, \cdots$ associated with the polynomial

$$\Phi(X,Y) = X + Y \text{ (resp. } \Phi(X,Y) = X \cdot Y \text{)} \tag{2.14}$$

If A is arbitrary commutative ring, and if $\mathfrak{a} = (a_0, a_1, a_2, \cdots, a_n, \cdots)$, $\mathfrak{b} = (b_0, b_1, b_2, \cdots, b_n, \cdots)$ are element in $A^{\mathbb{N}}$, then we take:

$$\mathfrak{a} + \mathfrak{b} = (S_0(a,b), S_1(a,b), S_2(a,b), \cdots, S_n(a,b), \cdots) \tag{2.15}$$

$$\mathfrak{a} \cdot \mathfrak{b} = (P_0(a,b), P_1(a,b), P_2(a,b), \cdots, P_n(a,b), \cdots) \tag{2.16}$$

Theorem 2.6.2 The above laws of composition make $A^{\mathbb{N}}$ into a commutative unitary ring called the ring of Witt vectors with coefficients in A and denoted $W(A)$.

■ **Example 2.4** We have

$$S_0(a,b) = a + b, S_1(a,b) = a_1 + b_1 + \frac{a_0^p + b_0^p - (a_0 + b_0)^p}{p} \tag{2.17}$$

$$P_0(a,b) = a_0 \cdot b_0, P_1(a,b) = b_0^p a_1 + b_1 a_0^p + p a_1 b_1. \tag{2.18}$$

Instead of considering vectors of infinite length, we restrict to the vectors $(a_0, a_1, a_2, \cdots a_{n-1})$ with n components. Due to the polynomial φ_i only involve variables of index $\leq i$, we have these vectors form a ring $W_n(A)$, which is the quotient ring of $W(A)$, is called the ring of Witty vectors of length n.

We have $W_1(A) = A$. The ring $W(A)$ is the projective limit of the rings $W_n(A)$ as $n \to +\infty$. ■

2.6.1 The Maps V and r

If $\alpha = (a_0, \ldots, a_n, \ldots)$ is a Witt vector, one defines the vector $V\alpha$ by:

$$V\alpha = (0, a_0, \ldots, a_{n-1}, \ldots) \quad \text{(“shift”)}. \tag{2.19}$$

The map $\mathrm{V} : W(A) \to W(A)$ is additive. To see this, it suffices to verify when p is invertible in A, and in that case the homomorphism

$$W_* : W(A) \to A^{\mathbb{N}} \tag{2.20}$$

transforms V into the map which sends $(w_0, w_1, \ldots)$ to $(0, pw_0, \ldots)$.

By passage to the quotient, one deduces from V an additive map of $W_n(A)$ into $W_{n+1}(A)$. There are exact sequences

$$0 \to W_k(A) \xrightarrow{V^r} W_{k+r}(A) \to W_r(A) \to 0. \tag{2.21}$$

If $x \in A$, set

$$r(x) = (x, 0, \ldots, 0, \ldots). \tag{2.22}$$

This defines a map $r : A \to W(A)$. When p is invertible in A, W_* transforms r into the mapping that sends x to $(x, x^p, \ldots, x^{p^n}, \ldots)$. One deduces by the same reasoning as above the formulas:

$$r(xy) = r(x) \cdot r(y), \quad x, y \in A \tag{2.23}$$

$$(a_0, a_1, \ldots) = \sum_{n=0}^{\infty} \mathrm{V}^n(r(a_n)), \quad a_i \in A \tag{2.24}$$

$$r(x) \cdot (a_0, \ldots) = (xa_0, x^p a_1, \ldots, x^{p^n} a_n, \ldots), \quad x, a_i \in A. \tag{2.25}$$

Theorem 2.6.3 If k is a perfect ring of characteristic p, $W(k)$ is a strict p-ring with residue ring k.

Corollary 2.6.4 $W(\mathbb{F}_p) = \mathbb{Z}_p$ and $W_n(\mathbb{F}_p) = \mathbb{Z}/p^n\mathbb{Z}$.

2.6.2 The Map F

Suppose that k is a ring of characteristic p (not necessarily perfect). The map $x \mapsto x^p$ is a homomorphism of k into k. Therefore it defines a map $\mathrm{F} : W(k) \to W(k)$ given by the formula

$$\mathrm{F}(a_0, a_1, \ldots) = (a_0^p, a_1^p, \ldots), \tag{2.26}$$

and this is a ring homomorphism.

Furthermore, one has the identity $\mathrm{VF} = p = \mathrm{FV}$: for it suffices to check this when k is perfect; in that case, applying the isomorphism θ above, one finds:

$$\theta(\mathrm{FV}\alpha) = \sum_{i=0}^{\infty} f(a_i)^{p^{-i}} p^{i+1} = p\theta(\alpha) = \theta(p\alpha), \tag{2.27}$$

which gives the identity.

R In Grothendieck's language of schemes, the preceding constructions define, for each n, a ring scheme W_n, affine and of finite type over $\mathrm{Spec}(\mathbb{Z})$. For any ring A, the ring $W_n(A)$ is just the set of points of W_n with values in A.

Part II

RAMIFICATION

3. Discriminant and Different

In this chapter, A is a Dedekind domain and K is the field of fractions of it.

3.1 Lattices

Let V be a finite dimensional vector space over K. A lattice of V (with respect to A) is a sub-A-module X of V that is finitely generated and spans V. If A is principal, this means that X is a free A-module of rank $[V:K]$; one can often reduce to this case by localisation, i.e., by replacing A with $A_\mathfrak{p}$ and X with $A_\mathfrak{p}X = X_\mathfrak{p}$.

Let X_1 and X_2 be two lattices of V; if $X_2 \subset X_1$, then X_1/X_2 is a module of finite length, and its invariant $\chi(X_1/X_2)$, which is a non-zero ideal of A, was defined in Chap. I, §5. We wish to extend this definition to get an invariant for any pair of lattices:

Lemma 3.1.1 If X_1 and X_2 are lattices of V, then the fractional ideal $\chi(X_1/X_3)\cdot\chi(X_2/X_3)^{-1}$, defined for every lattice $X_3 \subset X_1 \cap X_2$, depends only on X_1 and X_2.

We may therefore associate to X_1 and X_2 the non-zero fractional ideal

$$\chi(X_1,X_2) = \chi(X_1/X_3)\cdot\chi(X_2/X_3)^{-1} \quad \text{for} \quad X_3 \subset X_1 \cap X_2. \tag{3.1}$$

Proposition 3.1.2 The following formulas are valid:

(a) $\chi(X_1,X_2)\cdot\chi(X_2,X_3)\cdot\chi(X_3,X_1) = 1$;

(b) $\chi(X_1,X_2)\cdot\chi(X_2,X_1) = 1$;

(c) $\chi(X_1,X_2) = \chi(X_1/X_2)$ if $X_1 \supset X_2$.

We may therefore associate to X_1 and X_2 the non-zero fractional ideal

$$\chi(X_1,X_2) = \chi(X_1/X_3)\cdot\chi(X_2/X_3)^{-1} \quad \text{for} \quad X_3 \subset X_1 \cap X_2. \tag{3.2}$$

Proposition 3.1.3 If u is a K-automorphism of V and X a lattice of V, then $\chi(X,uX) = (\det(u))$ (principal ideal generated by $\det(u)$).

(The symbol uX denotes the image of X under u.)

This result suggests the following direct definition of the ideal $\chi(X,X')$:

Let $n = [V : K]$, and let $W = \bigwedge^n V$; it is a one-dimensional vector space over K. To each lattice X of V, let us associate $X_W = \bigwedge^n X$, which may be identified with a lattice of W; as $[W : K] = 1$, if D and D' are two lattices of W, there is a unique non-zero fractional ideal $\mathfrak{a}$ of K such that $D' = \mathfrak{a}D$ (namely, $\chi(D, D')$).

Applying this to $D = X_W$ and $D' = X'_W$, we obtain an ideal which is none other than $\chi(X, X')$: this follows from localisation and applying Proposition 2.

3.2 Discriminant of a Lattice with Respect to a Bilinear Form

We now suppose that the vector space V is provided with a non-degenerate bilinear form $T(x, y)$.

Let $n = [V : K]$. It is known that T extends to a non-degenerate bilinear form (again denoted by T) on the exterior algebra of V, and, in particular, on $W = \bigwedge^n V$; this form induces an isomorphism

$$T : W \otimes_k W \to K. \tag{3.3}$$

Let X be a lattice of V, and let X_W be its nth exterior power, identified with a lattice of W. The image of $X_W \otimes_A X_W$ under T is a non-zero fractional ideal of K, which is called the discriminant of X with respect to T; we denote it by $\mathfrak{d}_{X,T}$ or simply $\mathfrak{d}_X$ when that does not lead to confusion.

R The above definition shows that $\mathfrak{D}_X$ is isomorphic as an A-module to $X_W \otimes_A X_W$; its ideal class (modulo the principal ideals) is thus a square.

Proposition 3.2.1 If X is a free A-module with basis $S = \{e_1, \ldots, e_n\}$, then $\mathfrak{d}_{X,T}$ is the principal ideal generated by the discriminant $D_T(S)$ (in the sense of Bourbaki, *Alg.*, Chap. IX, §2). Recall that $D_T(S) = \det(T(e_i, e_j))$.

R We could have taken the formula $\mathfrak{d}_{X,T} = (\det(T(e_i, e_j)))$ as the definition of $\mathfrak{d}_{X,T}$, at least in the local case.

Proposition 3.2.2 Let X be a lattice of V, and let X_T^* be the set of all $y \in V$ such that $T(x, y) \in A$ for all $x \in X$. Then X_T^* is a lattice of V and

$$\mathfrak{d}_{X,T} = \chi(X_T^*, X). \tag{3.4}$$

Proposition 3.2.3 If X and X' are lattices of V, then

$$\mathfrak{d}_{X',T} = \mathfrak{d}_{X,T} \cdot \chi(X, X')^2. \tag{3.5}$$

Let $\mathfrak{a} = \chi(X, X')$. We saw in §1 that $X'_W = \mathfrak{a} \cdot X_W$ in W; the image of $X'_W \otimes X'_W$ under the isomorphism $T : W \otimes W \to K$ is therefore equal to the product of $\mathfrak{a}^2$ by the image of $X_W \otimes X_W$. ∎

Corollary 3.2.4 If $X' \subset X$, then $\mathfrak{d}_{X',T} = \mathfrak{d}_{X,T} \cdot \mathfrak{a}^2$, where $\mathfrak{a}$ is an ideal of A; $\mathfrak{a} = 1$ if and only if $X' = X$.

Take $\mathfrak{a} = \chi(X/X')$; it is clear that $\mathfrak{a} = 1$ if and only if $X' = X$.

3.3 Discriminant and Different of a Separable Extension

Let L be a finite separable extension of the field K. It is known that the homomorphism $\mathrm{Tr} : L \to K$ is surjective and that the bilinear form $\mathrm{Tr}(xy)$ is non-degenerate on L. Thus the definitions and results of the preceding § are applicable to this form; in particular, the discriminant of a lattice of L (with respect to A) is defined; if this lattice is a free A-module with basis $\{e_i\}$, its discriminant is the ideal generated by $\det(\mathrm{Tr}(e_i e_j))$, and it is known (Bourbaki, *Alg.*, Chap. V, §10, prop. 12) that

$$\det(\mathrm{Tr}(e_i e_j)) = (\det(\sigma(e_i)))^2, \tag{3.6}$$

where σ runs through the set of K-monomorphisms of L into an algebraic closure of K.

In particular, this applies to the integral closure B of A in L; B is a lattice of L. The corresponding discriminant will be denoted $\mathfrak{D}_{B/A}$, or sometimes $\mathfrak{D}_{L/K}$ (when no confusion about A is possible).

Let B^* be the set of all $y \in L$ such that $\mathrm{Tr}(xy) \in A$ for all $x \in B$; B^* is the lattice denoted B^*_{Tr} in the preceding §. It is called the *codifferent* (or "inverse different") of B over A. It is a sub-B-module of L; one sees at once that it is the largest sub-B-module E of L such that $\mathrm{Tr}(E) \subset A$. In particular, as $\mathrm{Tr}(B) \subset A$, one has $B \subset B^*$. The codifferent is thus a fractional ideal of L with respect to B; its inverse is called the *different* of B over A (or of the extension L/K), and is denoted $\mathfrak{D}_{B/A}$ or $\mathfrak{D}_{L/K}$; it is a non-zero ideal of B. The different is related to the discriminant by the next proposition.

Proposition 3.3.1 $\mathfrak{d}_{B/A} = \chi_A(B^*/B) = \mathrm{N}_{L/K}(\mathfrak{D}_{B/A})$.

Corollary 3.3.2 The discriminant $\mathfrak{d}_{B/A}$ is contained in A.

R The preceding proposition shows that the different ($\mathfrak{D}_{B/A}$) determines the discriminant ($\mathfrak{d}_{B/A}$); the converse is not true in general (except, however, when there is only one prime ideal of B over each prime ideal of A, which is the case when one completes).

Proposition 3.3.3 Let a (resp. b) be a fractional ideal of K (resp. L) relative to A (resp. B). The following two properties are equivalent:

(i) $\mathrm{Tr}(b) \subset a$;

(ii) $b \subset a \cdot \mathfrak{D}^{-1}_{B/A}$.

3.4 Elementary Properties of the Different and Discriminant

We keep the notation of the preceding section: L denotes a finite separable extension of K, and B the integral closure of A in L.

(i) Transitivity

Proposition 8. Let M/L be a separable extension of finite degree n, C the integral closure of A in M. Then

$$\mathfrak{D}_{C/A} = \mathfrak{D}_{C/B} \cdot \mathfrak{D}_{B/A} \quad \text{and} \quad \mathfrak{d}_{C/A} = (\mathfrak{d}_{B/A})^n \cdot \mathbf{N}_{L/K}(\mathfrak{d}_{C/B}). \tag{3.7}$$

(ii) Localisation

Proposition 9. If S is a multiplicative subset of A, then

$$S^{-1}\mathfrak{D}_{B/A} = \mathfrak{D}_{S^{-1}B/S^{-1}A} \quad \text{and} \quad S^{-1}\mathfrak{d}_{B/A} = \mathfrak{d}_{S^{-1}B/S^{-1}A}. \tag{3.8}$$

(iii) Completion

Corollary 3.4.1 Let δ be the ideal of $\hat{A}_{\mathfrak{p}}$ generated by the discriminant $\mathfrak{d}_{B/A}$, and let $\mathfrak{d}_{\mathfrak{P}}$ be the discriminant of $\hat{B}_{\mathfrak{P}}$ with respect to $\hat{A}_{\mathfrak{p}}$. Then

$$\delta = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{d}_{\mathfrak{P}}. \tag{3.9}$$

3.5 Unramified Extensions

We keep the notation and hypotheses.

Theorem 3.5.1 Let $\mathfrak{P}$ be a prime ideal of B, and let $\mathfrak{p} = \mathfrak{P} \cap A$. In order that the extension L/K be unramified at $\mathfrak{P}$, it is necessary and sufficient that $\mathfrak{P}$ does not divide the different $\mathfrak{D}_{B/A}$.

Corollary 3.5.2 Let $\mathfrak{p}$ be a prime ideal of A. In order that the extension L/K be unramified at $\mathfrak{p}$, it is necessary and sufficient that $\mathfrak{p}$ does not divide the discriminant $\mathfrak{d}_{B/A}$.

This follows from the fact that $\mathfrak{d}_{B/A} = \mathbf{N}(\mathfrak{D}_{B/A})$.

Corollary 3.5.3 Almost all the prime ideals of B (or of A) are unramified in the extension L/K.

We now examine more closely the structure of unramified extensions, limiting ourselves to the case where A is a complete discrete valuation ring; we denote its residue field by k.

Theorem 3.5.4 Let k'/k be a finite separable extension. Then there exists a finite unramified extension K'/K whose corresponding residue extension is isomorphic to k'/k; this extension is unique, up to unique isomorphism. It is Galois if and only if k'/k is.

Theorem 3.5.5 Let K'/K be a finite unramified extension, with residue extension k'/k, and let K''/K be an arbitrary finite extension, with residue extension k''/k. The set of K-isomorphisms of K' into K'' is then in one-to-one correspondence (by reduction) with the set of k-isomorphisms of k' into k''.

Corollary 3.5.6 Let k_s be the separable closure of k, and let K_{nr} be the inductive limit of the unramified extensions of K that correspond to the finite subextensions of k_s. The field K_{nr} is Galois over K with residue field k_s, and $G(K_{nr}/K) = G(k_s/k)$.

Corollary 3.5.7 Let K''/K be a finite extension, with residue extension k''/k. The subextensions K'/K of K''/K which are unramified over K are in one-to-one correspondence with the separable subextensions k'/k of k''/k.

Corollary 3.5.8 With the hypotheses of corollary 2, there exists a maximal unramified subextension K'/K of K''/K. Its residue extension k'/k is the largest separable subextension of k''/k. We

have

$$e(K''/K) = e(K''/K'), \quad f(K''/K') = [k'' : k]_i, \quad f(K'/K) = [k'' : k]_s. \tag{3.10}$$

R

1. When K and k have the same characteristic, K is isomorphic to $k((T))$. If k' is a finite separable extension of k, the corresponding unramified extension is $K' = k'((T)) = k' \otimes_k K$. When k is a perfect field of characteristic $p > 0$, one has $K' = W(k') \otimes_{W(k)} K$, where $W(k)$ denotes the ring of Witt vectors.
2. The results extend to arbitrary complete local Noetherian rings.

3.6 Computation of Different and Discriminant

Proposition 3.6.1 Let $n = [L : K]$ and let C be a subring of B containing A with an A-basis consisting of powers x^i $(0 \le i \le n-1)$ of an element x. Let f be the characteristic polynomial of x. Then: (i) f has coefficients in A (ii) C^* is a free A-module with basis $x^i/f'(x)$ $(0 \le i \le n-1)$, where $f'(X)$ is the derivative of $f(X)$)

The coefficients of f are integral over A and belong to K; since A is integrally closed, they belong to A, proving (i).

Lemma 3.6.2 — Euler.

$$\mathrm{Tr}(x^i/f'(x)) = 0 \quad \text{for} \quad 0 \le i \le n-2, \quad \text{and} \quad \mathrm{Tr}(x^{n-1}/f'(x)) = 1. \tag{3.11}$$

The set $\tau = \{t \in C \mid tB \subset C\}$ is an ideal of both C and B, called the conductor of B in C.

Corollary 3.6.3 Under the preceding notation and hypotheses,

$$\tau = f'(x) \cdot \mathfrak{D}_{B/A}^{-1}. \tag{3.12}$$

Corollary 3.6.4 When $B = A[x]$, Corollary 1 enables computation of the different $\mathfrak{D}_{B/A}$. The following gives a condition for this case:

Proposition 3.6.5 Suppose B (hence A) is a discrete valuation ring, and L/K is a finite separable extension of their residue fields. Then B has an A-basis $\{1, x, \ldots, x^{n-1}\}$.

(This applies notably when A is a complete discrete valuation ring with perfect residue field.)

Let e be the ramification index, $f = [L : K]$, so $n = ef$. Let π be a uniformizer of B, and $x \in B$ lifting a primitive element of the residue field extension. We require two lemmas:

Lemma 3.6.6 The products $\{x^i \pi^j \mid 0 \le i < f,\ 0 \le j < e\}$ form an A-basis of B.

Lemma 3.6.7 The element x may be chosen such that there exists a monic polynomial $R(X) \in A[X]$ of degree f with $R(x)$ being a uniformizer of B.

R Proposition does not extend to the case where A is merely a discrete valuation ring.

Proposition 3.6.8 Let $\mathfrak{B}$ be a nonzero prime ideal of B, $p = \mathfrak{B} \cap A$, and suppose the residue field extension $L_{\mathfrak{B}}/K_p$ is separable. Then the exponent of $\mathfrak{B}$ in the different $\mathfrak{D}_{B/A}$ satisfies:

$$\ge e_{\mathfrak{B}} - 1 \tag{3.13}$$

with equality iff $e_{\mathfrak{B}}$ is prime to the characteristic of K_p.

1. Upper bound for the different exponent:

$$\leq e_{\mathfrak{B}} - 1 + w(e_{\mathfrak{B}}) \tag{3.14}$$

Reducing to the totally ramified case, valuation computations yield

$$w(f'(\pi)) = \min_{0 \leq i < e} w((e-i)a_i \pi^{e-i-1}) \leq e - 1 + w(e) \tag{3.15}$$

(This bound depends on the degree and ramifying primes.)
2. When the residue characteristic divides $e_{\mathfrak{B}}$, the exponent requires computation via "ramification groups".

3.7 A Differential Characterisation of the Different

Definition 3.7.1 Let B be a commutative A-algebra. The multiplication map $(x,y) \mapsto xy$ induces a homomorphism

$$\theta : B \otimes_A B \to B. \tag{3.16}$$

Let $I = \ker \theta$, and define the module of A-differentials as $\Omega_A(B) = I/I^2$ (this construction is due to E. Kähler). Denoting the image of $x \otimes 1 - 1 \otimes x$ in I/I^2 by $\mathrm{d}x$, every element of $\Omega_A(B)$ can be written as $\sum y_i \, \mathrm{d}x_i$, satisfying:

$$\mathrm{d}(xy) = x\,\mathrm{d}y + y\,\mathrm{d}x \tag{3.17}$$

$$\mathrm{d}a = 0 \quad \text{for } a \in A. \tag{3.18}$$

This module has universal properties.

Proposition 3.7.1 Let A be a Dedekind domain with fraction field K, L/K a finite separable extension, and B the integral closure of A in L. If for every prime ideal $\mathfrak{P}$ of B the residue field extension is separable, then:

1. $\Omega_A(B)$ is generated by one element as a B-module
2. Its annihilator is the different $\mathfrak{D}_{B/A}$

It would be interesting to find a more direct proof and to study the principal parts of order m:

$$P_m(B/A) = (B \otimes_A B)/I^{m+1}. \tag{3.19}$$

4. Ramification Groups

4.1 Notation and Hypotheses

Let K be a field *complete* under a discrete valuation v_K, with valuation ring A_K, maximal ideal p_K, residue field $\overline{K} = A_K/p_K$, and unit group $U_K = A_K^\times$.

For a finite separable extension L/K, let A_L be the integral closure of A_K in L (a complete discrete valuation ring). Define $v_L, p_L, U_L, \overline{L}$ analogously. *We assume the residue extension $\overline{L}/\overline{K}$ is separable.* The ramification index is denoted $e_{L/K}$, residue degree $f_{L/K}$, with $[L:K] = e_{L/K} f_{L/K}$.

4.2 Definition of Ramification Groups; First Properties

Let L/K be a *Galois extension* with group $G = G(L/K)$. Fix an element x generating A_L as an A_K-algebra.

Lemma 4.2.1 For $s \in G$ and integer $i \geq -1$, the following are equivalent:

1. s acts trivially on A_L/p_L^{i+1}
2. $v_L(s(a)-a) \geq i+1$ for all $a \in A_L$
3. $v_L(s(x)-x) \geq i+1$

Proposition 4.2.2 For each $i \geq -1$, define G_i as the set of $s \in G$ satisfying the above conditions. Then:

- $\{G_i\}$ forms a decreasing sequence of normal subgroups of G
- $G_{-1} = G$, G_0 is the inertia subgroup
- $G_i = \{1\}$ for i sufficiently large

Define the function $i_G(s) = v_L(s(x)-x)$ ($i_G(s) \geq 1$ for $s \neq 1$, $i_G(1) = +\infty$), satisfying:

$$i_G(s) \geq i+1 \Leftrightarrow s \in G_i, \quad i_G(tst^{-1}) = i_G(s), \quad i_G(st) \geq \min(i_G(s), i_G(t)). \tag{4.1}$$

This function uniquely determines the filtration $\{G_i\}$.

Proposition 4.2.3 For a subgroup $H \leq G$ fixing K':

$$\forall s \in H, i_H(s) = i_G(s), \quad H_i = G_i \cap H. \tag{4.2}$$

Corollary 4.2.4 Let K_r be the maximal unramified subextension of L/K, with subgroup $H = G_0$. Then $H_i = G_i$ for $i \geq 0$.

R The extension L/K_r is totally ramified, reducing the study of higher ramification groups ($i \geq 0$) to this case.

Proposition 4.2.5 If $H \trianglelefteq G$ corresponds to K'/K, then for $\sigma \in G/H$:

$$i_{G/H}(\sigma) = \frac{1}{e'} \sum_{s \mapsto \sigma} i_G(s) \quad (e' = e_{L/K'}). \tag{4.3}$$

Proposition 4.2.6 — Hilbert's Formula for the Different. The different $\mathfrak{D}_{L/K}$ satisfies:

$$v_L(\mathfrak{D}_{L/K}) = \sum_{s \in G, s \neq 1} i_G(s) = \sum_{i=0}^{\infty} (|G_i| - 1) \tag{4.4}$$

(Note that $|G_i| - 1 = 0$ for i sufficiently large.)

Corollary 4.2.7 For a subextension K'/K (subgroup H):

$$v_{K'}(\mathfrak{D}_{K'/K}) = \frac{1}{e'} \sum_{s \notin H} i_G(s) \quad (e' = e_{L/K'}). \tag{4.5}$$

R

1. For non-separable residue extensions, modify the ramification group sequence.
2. In the global case (Dedekind domain A), define ramification groups $G_i(\mathfrak{B})$ at a prime $\mathfrak{B}$ by:

$$s \in G_i(\mathfrak{B}) \iff s(x) \equiv x \pmod{\mathfrak{B}^{i+1}} \quad \forall x \in B. \tag{4.6}$$

All results extend naturally to this setting.

4.3 Structure of Higher Ramification Groups

Let K_r be the maximal unramified subextension of L/K, and π a uniformizer of L.

Proposition 4.3.1 For $i \geq 0$ and $s \in G_0$ (inertia group):

$$s \in G_i \iff s(\pi)/\pi \equiv 1 \pmod{p_L^i}. \tag{4.7}$$

Define a filtration of the unit group $U_L = A_L^\times$:

$$U_L^{(0)} = U_L, \quad U_L^{(i)} = 1 + p_L^i \quad (i \geq 1) \tag{4.8}$$

(abbreviated $U_L^i = U_L^{(i)}$).

Proposition 4.3.2 1. $U_L^0/U_L^1 \cong \overline{L}^\times$ (multiplicative group of residue field)

2. For $i \geq 1$, canonical isomorphisms:

$$U_L^i/U_L^{i+1} \cong p_L^i/p_L^{i+1} \cong (\overline{L}, +) \tag{4.9}$$

R The graded ring $\bigoplus p_L^i/p_L^{i+1}$ is a graded $\overline{L}$-algebra. In particular, letting $\Omega_L = p_L/p_L^2$:

$$U_L^i/U_L^{i+1} \cong \Omega_L^{\otimes i} \quad \text{(canonical isomorphism)}. \tag{4.10}$$

Proposition 4.3.3 The map $s \mapsto s(\pi)/\pi$ induces an isomorphism:

$$\theta_i : G_i/G_{i+1} \hookrightarrow U_L^i/U_L^{i+1} \tag{4.11}$$

independent of the choice of uniformizer π.

Explicit description:

- If $s \in G_0$, $s(\pi) = u\pi$ ($u \in U_L$), then $\theta_0(s) = \bar{u} \in \overline{L}^\times$
- If $s \in G_i$ ($i \geq 1$), $s(\pi) = \pi(1+a)$ ($a \in p_L^i$), then $\theta_i(s) = [a] \in p_L^i/p_L^{i+1}$

Corollary 4.3.4 G_0/G_1 is cyclic, isomorphic to a subgroup of roots of unity in $\overline{L}^\times$, of order prime to the characteristic of $\overline{L}$.

Corollary 4.3.5 If the residue field $\overline{L}$ has characteristic 0, then the wild inertia group $G_1 = \{1\}$, and thus the inertia group G_0 is cyclic.

Corollary 4.3.6 If $\overline{L}$ has characteristic $p > 0$:

- G_i/G_{i+1} ($i \geq 1$) are abelian groups, direct products of cyclic groups of order p
- G_1 is a p-group

Corollary 4.3.7 If $\overline{L}$ has characteristic $p > 0$, the inertia group G_0 decomposes as:

$$G_0 \cong (\text{cyclic group of order prime to } p) \rtimes (\text{normal } p\text{-group}). \tag{4.12}$$

Corollary 4.3.8 G_0 is solvable. If $\overline{K}$ is finite, then G is solvable.

Proposition 4.3.9 Let k be an algebraically closed field of characteristic 0, and $K = k((T))$. The algebraic closure of K is:

$$\overline{K} = \bigcup_{n \geq 1} k((T^{1/n})). \tag{4.13}$$

Corollary 4.3.10 Let k be algebraically closed of characteristic 0, and $K = k((T))$. Then $G(\overline{K}/K) \cong \mathbb{Z}$.

R This is a formal analogue of Puiseux's theorem.

Commutators and Ramification Filtration Since $G_i \trianglelefteq G_0$, the group G_0 acts on G_i/G_{i+1} via inner automorphisms. This action is described via the isomorphisms θ_i:

Proposition 4.3.11 For $s \in G_0$, $\tau \in G_i/G_{i+1}$ $(i \geq 1)$:

$$\theta_i(s\tau s^{-1}) = \theta_0(s)^i \theta_i(\tau). \tag{4.14}$$

(Note: $\theta_i(\tau)$ lies in the $\overline{L}$-vector space p_L^i/p_L^{i+1}, and $\theta_0(s) \in \overline{L}^\times$.)

Corollary 4.3.12 For $s \in G_0$, $t \in G_i$ $(i \geq 1)$:

$$sts^{-1}t^{-1} \in G_{i+1} \iff s^i \in G_1 \text{ or } t \in G_{i+1}. \tag{4.15}$$

Corollary 4.3.13 If G is abelian and $e_0 = |G_0/G_1|$, then for any integer i not divisible by e_0:

$$G_i = G_{i+1}. \tag{4.16}$$

Proposition 4.3.14 For $s \in G_i$, $t \in G_j$ $(i, j \geq 1)$:

$$sts^{-1}t^{-1} \in G_{i+j}. \tag{4.17}$$

Lemma 4.3.15 Under the hypotheses of Proposition 10:

$$\theta_{i+j}(sts^{-1}t^{-1}) = (j-i)\theta_i(s)\theta_j(t). \tag{4.18}$$

(This formula makes sense in the graded algebra $\bigoplus p_L^k/p_L^{k+1}$.)

Proposition 4.3.16 The integers $i \geq 1$ satisfying $G_i \neq G_{i+1}$ are all congruent modulo p (the characteristic of $\overline{L}$).

R

1. For abelian G, stronger congruences hold.
2. Proposition 10 is a special case of Lazard's theory of filtered groups ([44]). In his terminology, the Lie algebra $\mathrm{gr}(G_1) = \bigoplus_{i \geq 1} G_i/G_{i+1}$ is abelian.

4.4 The Functions ϕ and ψ; Herbrand's Theorem

For real $u \geq -1$, define:

$$G_u = G_{\lceil u \rceil}, \quad s \in G_u \iff i_G(s) \geq u+1$$

(where $\lceil u \rceil$ is the smallest integer $\geq u$).

Auxiliary Functions

Define:

$$\varphi(u) = \int_{-1}^{u} \frac{\mathrm{d}t}{(G_0 : G_t)}$$

(Note: $\varphi(u) = u$ on $[-1, 0]$). Explicitly $(m \leq u < m+1,\ m \geq 0)$:

$$\varphi(u) = \frac{1}{|G_0|}\left(\sum_{k=1}^{m} |G_k| + (u-m)|G_{m+1}|\right).$$

Proposition 4.4.1 1. φ is continuous, piecewise linear, increasing, concave
2. $\varphi(0) = 0$
3. Derivatives satisfy:
   - Non-integer u: $\varphi'_-(u) = \varphi'_+(u) = 1/(G_0 : G_u)$
   - Integer u: $\varphi'_-(u) = 1/(G_0 : G_u)$, $\varphi'_+(u) = 1/(G_0 : G_{u+1})$

Proposition 4.4.2 Let $\psi = \varphi^{-1}$:
1. ψ is continuous, piecewise linear, increasing, convex
2. $\psi(0) = 0$
3. For $v = \varphi(u)$: $\psi'_-(v) = 1/\varphi'_-(u)$, $\psi'_+(v) = 1/\varphi'_+(u)$
4. v integer $\Rightarrow$ $\psi(v)$ integer

Upper Numbering

Define ramification groups:

$$G^v = G_{\psi(v)} \quad \text{(equivalently } G^{\varphi(u)} = G_u\text{)}$$

satisfying $G^{-1} = G$, $G^0 = G_0$, and $G^v = \{1\}$ for large v.

Proposition 4.4.3 If $H \trianglelefteq G$, then:

$$(G/H)^v = G^v H/H.$$

Proposition 4.4.4 For the fixed field K' of H:

$$\varphi_{L/K} = \varphi_{K'/K} \circ \varphi_{L/K'}, \quad \psi_{L/K} = \psi_{L/K'} \circ \psi_{K'/K}.$$

Lemma 4.4.5

$$\varphi_{L/K}(u) = \frac{1}{|G_0|} \sum_{s \in G} \min(i_G(s), u+1) - 1.$$

Lemma 4.4.6 — Herbrand's theorem. Let H be a normal subgroup of G. An element $sH \in G/H$ belongs to the i-th (lower numbered) ramification group $(G/H)_i$ if and only if there exists a representative $s \in G$ of the coset sH such that $s \in G_i$. The key utility of the upper numbering is that it behaves well with respect to quotients. For any real number $v \geq -1$:

$$(G/H)^v = G^v H/H \tag{4.19}$$

Remarks. 1) For infinite Galois extension L/K, define $G^v = \varprojlim G(L'/K)^v$ (L' finite subextensions), giving a left-continuous filtration.

2) For subextension E/K, define $\varphi_{E/K} = \varphi_{L/K} \circ \psi_{L/E}$ (independent of L).

3) Via value group $\Gamma_L \cong \mathbb{Z}$, identify $T_L = \Gamma_L \otimes \mathbb{R} \cong \mathbb{R}$. Upper numbering indexes ramification groups by T_K.

Theorem 4.4.7 — Hasse-Arf. If G is abelian and v is a jump in $\{G^v\}$, then v is an integer.

Example (p-cyclic group). Let G be cyclic of order p^n ($p = \mathrm{char}\,\overline{K}$). There exist strictly increasing integers $i_0, \ldots, i_{n-1} > 0$ such that:

$$\begin{aligned} G_0 &= \cdots = G_{i_0} = G \\ G_{i_0+1} &= \cdots = G_{i_0+pi_1} = G^{(1)} \\ G_{i_0+pi_1+1} &= \cdots = G_{i_0+pi_1+p^2i_2} = G^{(2)} \\ &\vdots \\ G_{i_0+\cdots+p^{n-1}i_{n-1}+1} &= \{1\} \end{aligned}$$

where $G^{(k)}$ is the subgroup of order p^{n-k}.

4.5 Example: Cyclotomic Extensions of the Field $\mathbb{Q}_p$

We are going to study the fields obtained by adjoining roots of unity to $\mathbb{Q}_p$, starting with those of order prime to p.

Let K be a field complete under a discrete valuation, with finite residue field $k = \mathbb{F}_q$ where $q = p^f$. Take an integer n prime to p, and let K_n (resp. k_n) denote the field obtained by adjoining all n-th roots of unity to K (resp. k). Then: - K_n is an **unramified extension** of K, and its residue field is exactly k_n; - If ζ is a **primitive n-th root of unity**, the valuation ring A_{K_n} of K_n is $A_K[\zeta]$ (the ring generated by A_K and ζ); - The Galois group $G(K_n/K)$ can be **identified** with $G(k_n/k)$ (the Galois group of the residue field extension); this group is **cyclic**, generated by an automorphism s satisfying $s(z) = z^q$ for every n-th root of unity z.

Corollary 4.5.1 The degree $[K_n : K]$ is equal to the smallest integer $r \geq 1$ such that $q^r \equiv 1 \mod n$.

Indeed, r is the smallest integer such that $s^r = 1$.

Corollary 4.5.2 The maximal unramified extension K_{nr} of K is obtained by adjoining to K all the roots of unity of order prime to p. Its Galois group can be identified with $\hat{\mathbb{Z}}$; it admits a generator s such that $s(z) = z^q$ for every root of unity z of order prime to p.

R The element s is none other than the Artin symbol of $\mathfrak{p}_K$.

We next consider the roots of unity of order $n = p^m$, $m \geq 1$; this time we limit ourselves to the ground field $\mathbb{Q}_p$.

Proposition 4.5.3 Let K_n be the field obtained from $K = \mathbb{Q}_p$ by adjoining a primitive n-th root of unity ζ, with $n = p^m$. Then

1. $[K_n : K] = \varphi(n) = (p-1)p^{m-1}$;
2. The Galois group $G(K_n/K)$ is isomorphic to the group of invertible elements in the ring $\mathbb{Z}/n\mathbb{Z}$, denoted $(\mathbb{Z}/n\mathbb{Z})^*$;
3. K_n is a totally ramified extension of K. The element $\pi = \zeta - 1$ is a uniformizer of K_n, and $A_{K_n} = A_K[\zeta]$.

We now determine the ramification groups of $G = G(K_n/K)$. Let v be an integer with $0 \leq v \leq m$, and denote by $G(n)^v$ the subgroup of $G(n)$ consisting of all elements a such that $a \equiv 1 \mod p^v$. The quotient group $G(n)/G(n)^v$ can be identified with $G(p^v)$ (i.e., the Galois group of the extension K_{p^v}/K), so $G(n)^v = G(K_n/K_{p^v})$.

Proposition 4.5.4 The ramification groups G_u of $G(K_n/K)$ are:

$G_0 = G$,
if $1 \leq u \leq p-1$, $G_u = G(n)^1$,
if $p \leq u \leq p^2-1$, $G_u = G(n)^2$,
$\vdots$
if $p^{m-1} \leq u$, $G_u = G(n)^m = \{1\}$.

The fact that the jumps in the upper-numbered filtration $\{G^v\}$ are integers is a direct consequence of the Hasse-Arf Theorem, which states that for a finite abelian extension, the jumps of the upper numbering filtration are always integers.

Specifically, for $0 \leq v \leq m$, $G^v = G(n)^v$ (the subgroup of $G(n)$ consisting of invertible elements congruent to $1 \mod p^v$), and for $v \geq m$, $G^v = \{1\}$.

The jumps in the filtration (G_u) occur at $u = p^k - 1$ for $0 \leq k \leq m-1$ (with $p = 2$ being an exception: 0 is not a jump). This boils down to proving $\varphi_{L/K}(p^k - 1) = k$ for $k = 0, 1, \ldots, m-1$, which is straightforward.

1. The above result becomes more intuitive when taking the limit over m, i.e., introducing $K_{p^\infty} = \bigcup_{m=1}^{\infty} K_{p^m}$. The Galois group of K_{p^∞}/K is the projective limit of the groups $G(p^m) = (\mathbb{Z}/p^m\mathbb{Z})^*$. Since the projective limit of $\mathbb{Z}/p^m\mathbb{Z}$ is the ring $\mathbb{Z}_p$ of p-adic integers, the limit of $G(p^m)$ is naturally identified with the group $U_p = \mathbb{Z}_p^*$ of invertible elements of $\mathbb{Z}_p$. For $\alpha \in U_p$, the associated automorphism $s_\alpha \in G(K_{p^\infty}/K)$ acts on a p^m-th root of unity z by $s_\alpha(z) = z^\alpha$ (the exponent has an obvious meaning here). The group U_p is filtered by the subgroups U_p^v; this filtration can be extended to non-integer values v by setting $U_p^v = U_p^n$ where n is the smallest integer larger than v. The above corollary shows that the canonical isomorphism of U_p onto $G(K_{p^\infty}/K)$ transforms the filtration U_p^v of U_p into the filtration of $G(K_{p^\infty}/K)$ induced by the ramification groups (using the upper numbering).
2. Adjoining all roots of unity to $K = \mathbb{Q}_p$ gives the compositum of K_{nr} and K_{p^∞}. Since these extensions are linearly disjoint over K (one being totally ramified and the other unramified), the Galois group of their compositum $K_{nr}K_{p^\infty}/K$ is isomorphic to the product of the Galois groups $G(K_{nr}/K)$ and $G(K_{p^\infty}/K)$, i.e., $\hat{\mathbb{Z}} \times U_p$. We will see in Chap. XIV, §7 that $K_{nr}K_{p^\infty}$ is indeed the maximal abelian extension of K.

5. The Norm

Let L/K be a Galois extension satisfying the hypotheses of Chapter IV. The norm $N = N_{L/K}$ is a homomorphism $L^* \to K^*$ mapping U_L to U_K and satisfying $v_K(Nx) = f v_L(x)$ where $f = [L:K]$. This gives the commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \xrightarrow{v_L} & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle f} & & \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \xrightarrow{v_K} & \mathbb{Z} & \longrightarrow & 0 \end{array}$$

Following Hasse, we study the effect of N on the filtration subgroups U_L^v and U_K^v. For $v \geq 0$:

$$U_L^v := U_L^n \quad \text{where} \quad n = \min\{k \in \mathbb{Z} \mid k \geq v\} \tag{5.1}$$

(Similarly for U_K^v). Results independent of residue field hypotheses are presented here; finite/quasi-finite residue fields are treated in Chapter XV.

5.1 Lemmas

The next two lemmas are useful in comparing filtered groups.

Lemma 5.1.1 Let

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \longrightarrow & A & \longrightarrow & A'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ 0 & \longrightarrow & B' & \longrightarrow & B & \longrightarrow & B'' & \longrightarrow & 0 \end{array}$$

be a commutative diagram with exact rows. Then there is an exact sequence

$$0 \to \operatorname{Ker} f' \to \operatorname{Ker} f \to \operatorname{Ker} f'' \xrightarrow{\varphi} \operatorname{Coker} f' \to \operatorname{Coker} f \to \operatorname{Coker} f'' \to 0. \tag{5.2}$$

Lemma 5.1.2 Let A (resp. A') be an abelian group provided with a decreasing sequence of subgroups A_n (resp. A'_n). Suppose that $A_0 = A$, $A'_0 = A'$, and that A and A' are complete Hausdorff spaces in the topologies defined by A_n and A'_n (in other words, the canonical homomorphisms $A \to \lim A/A_n$ and

$A' \to \lim A'/A'_n$ are bijective). Let $u : A \to A'$ be a homomorphism sending A_n into A'_n for all n. If the homomorphisms

$$u_n : A_n/A_{n+1} \to A'_n/A'_{n+1} \tag{5.3}$$

defined by u are all injective (resp. surjective), then so is u.

5.2 The Unramified Case

The following results concern properties of norm maps in unramified extensions.

Proposition 5.2.1 If L/K is unramified, the norm map N sends U_L^n into U_K^n for every n. Consider $x = 1+y$ with $y \in p_L^n$. Then $s(x) = 1+s(y)$ holds for all $s \in G$, and $s(y) \in p_L^n$. Consequently,

$$Nx = \prod_{s\in G}(1+s(y)) \equiv 1 + \sum_{s\in G} s(y) \mod p_L^{2n}. \tag{5.4}$$

The norm map induces a homomorphism on quotient groups:

$$N_y : U_L^n/U_L^{n+1} \to U_K^n/U_K^{n+1} \tag{5.5}$$

whose explicit form requires further determination. Recall that U_L/U_L^1 identifies with the multiplicative group L^* of the residue field, while U_L^n/U_L^{n+1} $(n \geq 1)$ identifies with p_L^n/p_L^{n+1} (denoted Ω_L^n), a one-dimensional vector space over L. Since L/K is unramified, Ω_L^n identifies with $L \otimes_K \Omega_K^n$. Incorporating these identifications yields:

Proposition 5.2.2 Assume L/K is unramified. Then:

1. The map $N_0 : L^* \to K^*$ coincides with the norm in the residue field extension L/K.
2. For $n \geq 1$, the map $N_n : L \otimes_K \Omega_K^n \to \Omega_K^n$ coincides with the trace map $Tr_{L/K} \otimes 1$.

Proposition 5.2.3 The following hold:

1. $N(U_L^n) = U_K^n$ for all $n \geq 1$.
2. The quotient group U_K/NU_L is isomorphic to $\bar{K}^*/N\bar{L}^*$.
3. The quotient group K^*/NL^* is isomorphic to $\mathbb{Z}/f\mathbb{Z} \times \bar{K}^*/N\bar{L}^*$, where $f = [L:K] = [\bar{L}:\bar{K}]$.

Corollary 5.2.4 The following conditions are equivalent:

1. $(K^* : NL^*) = f$
2. $U_K = NU_L$
3. $K^* = NL^*$

The equivalence is immediately verifiable.

R

1. Condition (3) holds when K is a finite field (or more generally, quasi-finite).
2. For non-negative real numbers v, Proposition 1 implies $N(U_L^v) \subseteq U_K^v$, with equality when $v > 0$.

5.3 The Cyclic of Prime Order Totally Ramified Case

We assume throughout this section that G is cyclic of prime order l, and that L/K is totally ramified (so $\bar{L} = \bar{K}$). Let π denote a uniformizer of L.

Fix a generator s of G, and set $t = i(s) - 1$ (cf. Chap. IV, §1). The ramification groups satisfy:

$$G = G_0 = \cdots = G_t \tag{5.6}$$
$$\{1\} = G_{t+1} = \cdots \tag{5.7}$$

where $t \neq 0$ precisely when l equals the characteristic p of $\bar{K}$. The function ψ from Chap. IV, §3 is defined as:

$$\psi(x) = \begin{cases} x & x \leq t \\ t + l(x-t) & x \geq t \end{cases} \tag{5.8}$$

Lemma 5.3.1 The different $\mathfrak{D}$ of L/K is p_L^m with $m = (t+1)(l-1)$.
Lemma 5.3.2 For any integer $n > 0$, $\mathrm{Tr}(p_L^n) = p_K^r$ where $r = \lfloor (m+n)/l \rfloor$ and $m = (t+1)(l-1)$.
Lemma 5.3.3 If $x \in p_L^{2n}$, then

$$N(1+x) \equiv 1 + \mathrm{Tr}(x) + N(x) \mod \mathrm{Tr}(p_L^{2n}). \tag{5.9}$$

Proposition 5.3.4 For every integer $n \geq 0$:

$$N(U_L^{\psi(n)}) \subset U_K^n, \tag{5.10}$$
$$N(U_L^{\psi(n)+1}) \subset U_K^{n+1}. \tag{5.11}$$

This induces quotient homomorphisms:

$$N_n : U_L^{\psi(n)}/U_L^{\psi(n)+1} \to U_K^n/U_K^{n+1} \quad (n \geq 0). \tag{5.12}$$

Via uniformizers π' (for K) and π (for L), we identify U_K^n/U_K^{n+1} with $\bar{K}$ and U_L^n/U_L^{n+1} with $\bar{L} = \bar{K}$. Under these identifications:
Proposition 5.3.5 i) For $n = 0$, $N_0 : \bar{K}^* \to \bar{K}^*$ is given by $N_0(\xi) = \xi^l$. This map is injective if $t \neq 0$; if $t = 0$, its kernel is cyclic of order l and equals $\theta_0(G)$ (defined in Chap. IV, §2, Prop. 7).
ii) For $1 \leq n < t$, $N_n : \bar{K} \to \bar{K}$ is given by $N_n(\xi) = \alpha_n \xi^p$ ($\alpha_n \in \bar{K}^*$) and is injective.
iii) For $n = t \geq 1$, $N_t : \bar{K} \to \bar{K}$ is given by $N_t(\xi) = \alpha\xi^p + \beta\xi$ ($\alpha, \beta \in \bar{K}^*$). Its kernel is cyclic of order $p = l$ and equals $\theta_t(G)$.
iv) For $n > t$, $N_n : \bar{K} \to \bar{K}$ is given by $N_n(\xi) = \beta_n \xi$ ($\beta_n \in \bar{K}^*$) and is bijective.

Corollary 5.3.6 The homomorphism N_n is injective for all $n \neq t$. When $n = t$, there exists an exact sequence:

$$0 \to G \xrightarrow{\theta_t} U_L^t/U_L^{t+1} \xrightarrow{N_t} U_K^t/U_K^{t+1}. \tag{5.13}$$

This is immediately verifiable.

Corollary 5.3.7 N_n is surjective for $n > t$. If the residue field R is perfect, surjectivity holds for $n < t$. When R is algebraically closed, N_n is surjective for all n.

Corollary 5.3.8 The following equalities hold:

$$N(U_L^{\psi(n)}) = U_K^n \quad \text{for } n > t, \tag{5.14}$$
$$N(U_L^{\psi(n)+1}) = U_K^{n+1} \quad \text{for } n \geq t. \tag{5.15}$$

When R is algebraically closed, these hold for all n.

Through the filtration structures on $U_L^{\psi(m)}$ and U_K^m, passage to quotients induces homomorphisms:

$$U_L^{\psi(m)}/U_L^{\psi(m+1)} \to U_K^m/U_K^{m+1} \tag{5.16}$$

which decompose as composites of N_m and the canonical projection $U_L^{\psi(m)}/U_L^{\psi(m+1)} \to U_L^{\psi(m)}/U_L^{\psi(m)+1}$. For $m > t$, Corollary 2 ensures surjectivity, and Lemma 2 implies $N : U_L^{\psi(n)} \to U_K^m$ is surjective. Analogous reasoning applies when K is algebraically closed. The equality $N(U_L^{\psi(n)+1}) = U_K^{n+1}$ follows from Proposition 4 and the containment $U_L^{\psi(n)+1} \supset U_L^{\psi(n+1)}$.

Corollary 5.3.9 $N(U_L^{\psi(v)}) = U_K^v$ for real numbers $v > t$ or when K is algebraically closed.

Corollary 5.3.10 The cokernel structure is given by:

$$\mathrm{Coker}(N_t) \simeq K^*/K^* \quad \text{if } t = 0, \tag{5.17}$$
$$\mathrm{Coker}(N_t) \simeq K/\wp(K) \quad \text{if } t \neq 0, \quad \wp(\xi) = \xi^p - \xi. \tag{5.18}$$

For $t = 0$, $N_t(\xi) = \xi^l$ directly yields the result. For $t \neq 0$, the existence of a non-zero η in $\ker N_t$ permits the factorization:

$$N_t(\xi) = \gamma\wp(\xi/\eta) \quad (\gamma \neq 0) \tag{5.19}$$

implying $\mathrm{Im}(N_t) = \gamma\mathrm{Im}(\wp)$.

Corollary 5.3.11 If K is perfect, the norm induces an isomorphism $N : U_L/U_L^n \xrightarrow{\sim} U_K/U_K^n$ for all $n \leq t$. This follows by induction from Corollaries 1 and 2.

Corollary 5.3.12 If K is perfect, the following canonical homomorphisms are isomorphisms:

$$\mathrm{Coker}(N_t) \leftarrow U_K^t/N(U_L^t) \to U_K/NU_L \to K^*/NL^*. \tag{5.20}$$

The isomorphisms are established through three exact sequences:

1. Applying Lemma 1 to:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L^{t+1} & \longrightarrow & U_L^t & \longrightarrow & U_L^t/U_L^{t+1} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & U_K^{t+1} & \longrightarrow & U_K^t & \longrightarrow & U_K^t/U_K^{t+1} & \longrightarrow & 0 \end{array}$$

Since $N(U_L^{t+1}) = U_K^{t+1}$, it follows that $U_K^t/N(U_L^t) \xrightarrow{\sim} \mathrm{Coker}(N_t)$.

2. Applying Lemma 1 to:
$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L^t & \longrightarrow & U_L & \longrightarrow & U_L/U_L^t & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & U_K^t & \longrightarrow & U_K & \longrightarrow & U_K/U_K^t & \longrightarrow & 0 \end{array}$$
Corollary 6 implies $U_K^t/N(U_L^t) \xrightarrow{\sim} U_K/NU_L$.
3. Applying Lemma 1 to:
$$\begin{array}{ccccccccc} 0 & \longrightarrow & U_L & \longrightarrow & L^* & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle \mathrm{id}} & & \\ 0 & \longrightarrow & U_K & \longrightarrow & K^* & \longrightarrow & \mathbb{Z} & \longrightarrow & 0 \end{array}$$
The ramification index $f = 1$ yields $U_K/NU_L \xrightarrow{\sim} K^*/NL^*$.

R When $\bar{K}$ is finite:
- If $l \nmid p$, $\bar{K}^*/\bar{K}^{*l}$ is cyclic of order l.
- If $l = p$, $\bar{K}/\wp(\bar{K})$ is cyclic of order p.

Combining Corollaries 5 and 7, K^*/NL^* is cyclic of order l (cf. Chapter XIII).

5.4 Multiplicative Polynomials and Additive Polynomials

Let k be a field with exponential characteristic p. A polynomial $P \in k[X]$ is **multiplicative** if it satisfies $P(XY) = P(X)P(Y)$ and $P(1) = 1$. Such polynomials are necessarily monomials X^h; define $d(P) = h$. When $h = h_0 p^r$ with h_0 coprime to p, h_0 is called the **separable degree** and denoted $d_s(P) = h_0$. The kernel of the homomorphism $P : k^* \to k^*$ consists of all $d_s(P)$-th roots of unity in k, and its order divides $d_s(P)$. For any two multiplicative polynomials P and Q, their composition $P \circ Q$ remains multiplicative with:

$$d(P \circ Q) = d(P) \cdot d(Q), \tag{5.21}$$
$$d_s(P \circ Q) = d_s(P) \cdot d_s(Q). \tag{5.22}$$

A polynomial P is **additive** if it satisfies $P(X+Y) = P(X) + P(Y)$. For characteristic zero, $P(X) = aX$ ($a \in k$). For characteristic $p > 0$, P is a linear combination of monomials X^{p^n}. If $P \neq 0$ and k is perfect, P decomposes uniquely as:

$$P = (P')^{p^n} = X^{p^n} \circ P' \tag{5.23}$$

where $P' = a_0 + \cdots + a_k X^{p^k}$ ($a_0, a_k \neq 0$). The **degree** is $d(P) = p^{n+k}$, and the **separable degree** is $d_s(P) = p^k$.

The kernel of $P : k \to k$ coincides with that of P', forming an additive subgroup of k whose order divides $d_s(P)$. Since P' is separable, over an algebraic closure it factors as:

$$P' = a_k \prod_{P'(\xi)=0} (X - \xi) \tag{5.24}$$

proving that the kernel of P has order $d_s(P)$ if k contains all roots of P'. For any two additive polynomials P and Q, their composition $P \circ Q$ remains additive with:

$$d(P \circ Q) = d(P) \cdot d(Q), \tag{5.25}$$
$$d_s(P \circ Q) = d_s(P) \cdot d_s(Q). \tag{5.26}$$

R Additive polynomials correspond to k-endomorphisms of the algebraic group G_a, forming a ring (cf. Ore [50] and Whaples [69, 70]).

5.5 The Galois Totally Ramified Case

We assume throughout that L/K is Galois and totally ramified (so $\bar{L} = \bar{K}$). Let ψ denote the function from Chap. IV, §3.

Proposition 5.5.1 For every integer $n \geq 0$:

$$N(U_L^{\psi(n)}) \subset U_K^n, \tag{5.27}$$

$$N(U_L^{\psi(n)+1}) \subset U_K^{n+1}. \tag{5.28}$$

This allows defining homomorphisms:

$$N_0 : \bar{K}^* \to \bar{K}^*, \tag{5.29}$$

$$N_n : \bar{K} \to \bar{K} \quad (n \geq 1). \tag{5.30}$$

Proposition 5.5.2 The homomorphism N_n is induced by a non-constant polynomial P_n:

- Multiplicative when $n = 0$
- Additive when $n \geq 1$

satisfying:

$$d(P_n) = |G_{\psi(n)}|, \tag{5.31}$$

$$d_s(P_n) = (G_{\psi(n)} : G_{\psi(n)+1}) = \psi'_d(n)/\psi'_g(n). \tag{5.32}$$

Moreover, there is an exact sequence:

$$0 \to G_{\psi(n)}/G_{\psi(n)+1} \xrightarrow{\theta} U_L^{\psi(n)}/U_L^{\psi(n)+1} \xrightarrow{N_n} U_K^n/U_K^{n+1} \tag{5.33}$$

where θ maps $s \in G_{\psi(n)}$ to the class of $s(\pi)/\pi$ (π uniformizer of L).

Corollary 5.5.3 N_n is injective if and only if $G_{\psi(n)} = G_{\psi(n)+1}$.

Corollary 5.5.4 N_n is surjective in the following cases:

1. The residue field R is algebraically closed,
2. R is perfect and $G_{\psi(n)} = G_{\psi(n)+1}$,
3. $G_{\psi(n)} = \{1\}$.

Corollary 5.5.5 The following equalities hold:

$$N(U_L^{\psi(n)}) = U_K^n \quad \text{if } G_{\psi(n)} = \{1\}, \tag{5.34}$$

$$N(U_L^{\psi(n)+1}) = U_K^{n+1} \quad \text{if } G_{\psi(n+1)} = \{1\}. \tag{5.35}$$

When K is algebraically closed, these hold for all $n \geq 0$.

Corollary 5.5.6 For non-negative real v, $N(U_L^{\psi(v)}) = U_K^v$ if either $G_{\psi(v)} = \{1\}$ or K is algebraically closed.

R

1. The proof uses the "dèvissage" method starting from cyclic extensions of prime degree; direct approaches exist (e.g., Hasse [33]).
2. When K is finite, Proposition 9 does not uniquely determine P_n. However, there exists a choice invariant under residue extensions (following from the proof), called the **canonical polynomial**.

Proposition 5.5.7 If K is perfect, then for any $x \in K^*$, there exists an extension K'/K of degree $\leq [L:K]$ such that x is a norm in the corresponding extension L'/K'.

5.6 Application: Proof of the Hasse-ArfTheorem

The following theorem establishes properties of ramification group jumps in abelian extensions:

Theorem 5.6.1 Let K be a field complete under a discrete valuation, and L a finite abelian extension with Galois group G. Assume the residue extension $\bar{L}/\bar{K}$ is separable. If v is a jump in the upper ramification filtration $\{G^v\}$ (i.e., $G^{v+\varepsilon} \neq G^v$ for all $\varepsilon > 0$), then v is an integer.

Theorem 5.6.2 Under the hypotheses of Theorem 1, if μ is an integer satisfying $G_\mu \neq G_{\mu+1}$ (lower numbering), then $\phi_{L/K}(\mu)$ is an integer.

Proposition 5.6.3 Let L/K be cyclic totally ramified with Galois group G, and μ the largest integer with $G_\mu \neq \{1\}$. Then $\phi_{L/K}(\mu)$ is an integer.

Proof. Theorem 1' implies Theorem 1: For a jump v in $\{G^v\}$, set $G' = G^v$ and $G'' = G^{v+\varepsilon}$ (sufficiently small ε). Since $G' \neq G''$, there exists a cyclic quotient $H = G/G''$ where the image H' of G' satisfies $H' \neq \{1\}$. The group H corresponds to a subextension L'/K. Herbrand's theorem gives $H' = H^v$ and $H^{v+\varepsilon} = \{1\}$, and Proposition 11 shows v is an integer.

Proof of Proposition 11: Set $r = |G|$, $r' = |G_\mu|$, $k = r/r'$. Fix a generator $s \in G$, so $G_\mu = \langle \sigma = s^k \rangle$. Define:

$$V = \{x \in L^* \mid Nx = 1\}, \tag{5.36}$$

$$W = \{y^{s-1} \mid y \in U_L\}. \tag{5.37}$$

Lemma 5.6.4 V/W is cyclic (induced by $L^*/U_L \cong \mathbb{Z} \to V/W$).

For non-negative integers m:

$$V_m = V \cap U_L^m, \tag{5.38}$$

$$W_m = W \cap U_L^m. \tag{5.39}$$

Then $\{V_m/W_m\}$ forms a decreasing filtration of V/W.

Lemma 5.6.5 $V_m = W_m$ for m sufficiently large.

Lemma 5.6.6 If m is integer and $G_m = G_{m+1}$, then $V_m = V_{m+1}$.

Lemma 5.6.7 For positive integer m, if the image of W_m in U_L^m/U_L^{m+1} is non-trivial, it is surjective.

Lemma 5.6.8 For integer n with $G_{\psi(n+1)} = \{1\}$, and integer m satisfying $n < \phi(m) < n+1$, the images of V_m and W_m in U_L^m/U_L^{m+1} are both surjective.

Lemma 5.6.9 For integer m, let $n+1$ be the smallest integer $> \phi(m)$. If $G_{\psi(n+1)} = \{1\}$, then $V_m = W_m$.

■

6. Artin Representation

6.1 Representations and Characters

We recall fundamental concepts in representation theory of finite groups (cf. M. Hall [30] or [114]). Let G be a finite group of order g. A **class function** is a complex-valued function satisfying $f(sts^{-1}) = f(t)$ for all $s,t \in G$. Given a finite-dimensional complex vector space V, a **linear representation** is a homomorphism $\rho : G \to \mathrm{GL}(V)$. Its **character** is defined as:

$$\chi_\rho(s) = \mathrm{Tr}(\rho(s)) \tag{6.1}$$

This is a class function satisfying $\chi_\rho(s^{-1}) = \overline{\chi_\rho(s)}$. The dimension $\chi_\rho(1) = \dim V$ is called the **degree** of the representation.

The character of the **unit representation** is denoted $\mathbf{1}_G$, constantly equal to 1 (trivial 1-dimensional representation). The character r_G of the **regular representation** satisfies $r_G(1) = g$ and $r_G(s) = 0$ for $s \neq 1$. The character u_G of the **augmentation representation** fulfills $r_G = u_G + \mathbf{1}_G$.

A character χ is **irreducible** if its representation is irreducible. Every class function decomposes uniquely into irreducible characters:

$$\varphi = \sum_\chi c_\chi \chi, \quad c_\chi \in \mathbb{C} \tag{6.2}$$

Coefficients are determined by the orthogonal inner product:

$$(\varphi, \psi) = \frac{1}{g} \sum_{s \in G} \varphi(s)\overline{\psi(s)} \tag{6.3}$$

Irreducible characters form an orthonormal basis, with $c_\chi = (\varphi, \chi)$. For example:

$$r_G = \sum_\chi \chi(1)\chi, \quad u_G = \sum_{\chi \neq \mathbf{1}_G} \chi(1)\chi \tag{6.4}$$

For a group homomorphism $\alpha : H \to G$, define the **pullback** $\alpha^*(\varphi) = \varphi \circ \alpha$ and **pushforward** $\alpha_*(\psi)$, the latter uniquely determined by Frobenius reciprocity:

$$(\varphi, \alpha_*(\psi))_G = (\alpha^*(\varphi), \psi)_H \tag{6.5}$$

When ψ is a character of an H-representation, $\alpha_*(\psi)$ corresponds to the **induced representation** $\mathbb{C}[G] \otimes_{\mathbb{C}[H]} V$. Key cases: 1. **Subgroup case** ($H \leq G$, α inclusion):
Induced character $\psi^*(s) = \sum_{t \in G/H} \psi(tst^{-1})$ (vanishing when $tst^{-1} \notin H$). 2. **Quotient case** ($G = H/N$, α canonical projection):
Induced character $\psi^*(s) = \frac{1}{|N|} \sum_{t \mapsto s} \psi(t)$.

Theorem 6.1.1 — Brauer's Theorem. Every character of a finite group is a $\mathbb{Z}$-linear combination of characters induced from degree-1 characters of subgroups. (Degree-1 characters are homomorphisms $H \to \mathbb{C}^*$.)

6.2 Artin Representation

Let L/K be a finite Galois extension with Galois group G, satisfying the hypotheses of Chaps. IV and V. Set $f = [\bar{L} : \bar{K}]$. For $s \in G \setminus \{1\}$, recall the integer $i_G(s)$ from Chap. IV, §1, and define:

$$a_G(s) = \begin{cases} -f \cdot i_G(s) & s \neq 1 \\ f \sum_{t \neq 1} i_G(t) & s = 1 \end{cases} \tag{6.6}$$

satisfying $\sum_{s \in G} a_G(s) = 0$, i.e., $(a_G, \mathbf{1}_G) = 0$.

Theorem 6.2.1 The function a_G is the character of a linear representation of G.

Theorem 6.2.2 For every character χ of G, $f(\chi) = (\chi, a_G)$ is a non-negative integer.

Proposition 6.2.3 a_G equals the induced function $(a_{G_0})^*$ from the inertia group G_0.

Proposition 6.2.4 Let u_i be the augmentation character of the ramification group G_i, and u_i^* its induction to G. Then:

$$a_G = \sum_{i=0}^{\infty} \frac{1}{(G_0 : G_i)} u_i^*. \tag{6.7}$$

Corollary 6.2.5 For a class function φ:

$$f(\varphi) = \sum_{i=0}^{\infty} \frac{|G_i|}{|G_0|} (\varphi(1) - \varphi(G_i)) \tag{6.8}$$

where $\varphi(G_i) = \frac{1}{|G_i|} \sum_{s \in G_i} \varphi(s)$.

Corollary 6.2.6 If χ corresponds to a representation V:

$$f(\chi) = \sum_i \frac{|G_i|}{|G_0|} \operatorname{codim} V^{G_i} \tag{6.9}$$

Corollary 6.2.7 $f(\chi)$ is a non-negative rational number.

Proposition 6.2.8 For a normal subgroup $N \triangleleft G$:

$$a_{G/N} = (a_G)^N. \tag{6.10}$$

Corollary 6.2.9 If φ is a class function on G/N and φ' its lift to G, then $f(\varphi) = f(\varphi')$.

Proposition 6.2.10 For a subgroup H (corresponding to subextension K/K), let $b_{K/K}$ be the discriminant. Then:

$$a_G|_H = \lambda r_H + f_{K/K} \cdot a_H, \quad \lambda = v_K(b_{K/K}) \tag{6.11}$$

Corollary 6.2.11 For a character ψ of a subgroup H and its induction ψ^* to G:

$$f(\psi^*) = \lambda\, \psi(1) + f_{K'/K} f(\psi), \quad \lambda = v_K(\mathfrak{d}_{K'/K}). \tag{6.12}$$

Proposition 6.2.12 Let χ be a degree-1 character of G, and c_χ the largest integer such that $\chi|_{G_{c_\chi}}$ is non-trivial (set $c_\chi = -1$ if $\chi = \mathbf{1}_G$). Then:

$$f(\chi) = \varphi_{L/K}(c_\chi) + 1. \tag{6.13}$$

Corollary 6.2.13 Let $H = \ker \chi$, K' the corresponding subextension, and c'_χ the largest integer with $(G/H)_{c'_\chi} \neq 1$ (set $c'_\chi = -1$ if $H = G$). Then:

$$f(\chi) = \varphi_{K'/K}(c'_\chi) + 1 \quad (\text{integer } \geq 0). \tag{6.14}$$

R

1. **Artin's Theorem** (Thm. 1) and its proof are due to Artin [6]. Originally assuming finite residue fields (as Hasse-Arf was then only proved in this case), he reduced to $G = G_1$ via Speiser's theorem (Chap. IV, Prop. 9, Cor. 2). Since G is then a p-group, every irreducible character is induced from a degree-1 subgroup character—a refinement of Brauer's theorem here.
2. Artin's proof essentially uses Hasse-Arf; conversely, Hasse-Arf follows from Artin's theorem.

Terminology.

- The representation in Theorem 1 is called the **Artin representation** (defined by a_G, unique up to isomorphism).
- For a character χ, the ideal $\mathfrak{p}_K^{f(\chi)}$ is its **conductor**, denoted $\mathfrak{f}(\chi)$.

- When χ has degree 1 (cyclic subextension K'/K) and $\bar{K}$ is finite, $\mathfrak{f}(\chi)$ coincides with the class field theoretic conductor. This also holds for $\bar{K}$ algebraically closed ([59], 3.7).

- For irreducible characters of degree > 1, no class field interpretation of $\mathfrak{f}(\chi)$ is known.

6.3 Globalisation

Let L/K be a finite Galois extension with Galois group G, A a Dedekind domain with fraction field K, and B the integral closure of A in L. Assume for primes $\mathfrak{p}$ of A and $\mathfrak{P} \mid \mathfrak{p}$ in B, the residue extension $B/\mathfrak{P}$ over $A/\mathfrak{p}$ is separable. The completion $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is Galois with group $D_{\mathfrak{P}}$. Applying local Artin theory, define $a_{\mathfrak{P}}$ (on $D_{\mathfrak{P}}$, extended by zero to G) and set:

$$a_{\mathfrak{p}} = \sum_{\mathfrak{P}|\mathfrak{p}} a_{\mathfrak{P}} \tag{6.15}$$

Then $a_{\mathfrak{p}} = (a_{\mathfrak{P}})^*$ for any $\mathfrak{P} \mid \mathfrak{p}$, so $a_{\mathfrak{p}}$ is the character of the **Artin representation attached to** $\mathfrak{p}$, induced from any $D_{\mathfrak{P}}$. For a character χ:

$$f(\chi, \mathfrak{p}) = (\chi, a_{\mathfrak{p}}) = f(\chi|_{D_{\mathfrak{P}}}) \tag{6.16}$$

Vanishing for unramified $\mathfrak{p}$, define the **conductor**:

$$\mathfrak{f}(\chi) = \prod_{\mathfrak{p}} \mathfrak{p}^{f(\chi,\mathfrak{p})} \tag{6.17}$$

Proposition 6.3.1 — Properties of the conductor.

1. $\mathfrak{f}(\chi + \chi') = \mathfrak{f}(\chi) \cdot \mathfrak{f}(\chi')$, $\mathfrak{f}(\mathbf{1}_G) = (1)$.
2. For subextension K'/K (subgroup H) and H-character ψ:

$$\mathfrak{f}(\psi^*, L/K) = \mathfrak{b}_{K'/K}^{\psi(1)} \cdot N_{K'/K}(\mathfrak{f}(\psi, L/K')) \tag{6.18}$$

3. If K'/K Galois and χ a G/H-character:

$$\mathfrak{f}(\chi, L/K) = \mathfrak{f}(\chi, K'/K) \tag{6.19}$$

Corollary 6.3.2 $\mathfrak{b}_{K'/K} = \mathfrak{f}(s_{G/H}, L/K)$ ($s_{G/H}$: regular character of G/H).

Corollary 6.3.3 — Artin-Hasse Führerdiskriminantenproduktformel.

$$\mathfrak{b}_{L/K} = \prod_{\chi} \mathfrak{f}(\chi)^{\chi(1)} \quad (\chi \text{ irreducible}) \tag{6.20}$$

$$\text{(Abelian case)} \quad \mathfrak{b}_{L/K} = \prod_{\chi} \mathfrak{f}(\chi) \tag{6.21}$$

Number field case

Let K be a number field (finite over $\mathbb{Q}$), A its integer ring. Define the positive integer:

$$c(\chi, L/K) = \text{gen}\left(\mathfrak{d}_{K/\mathbb{Q}}^{\chi(1)} \cdot N_{K/\mathbb{Q}}(\mathfrak{f}(\chi, L/K))\right) \tag{6.22}$$

satisfying:

Proposition 6.3.4

1. $c(\chi+\chi', L/K) = c(\chi, L/K)\cdot c(\chi', L/K)$, $c(1, L/K) = |d_{K/\mathbb{Q}}|$
2. $c(\psi^*, L/K) = c(\psi, L/K')$
3. $c(\chi, L/K) = c(\chi, K'/K)$

These invariants match Artin L-functions, and $c(\chi, L/K)$ appears in the exponential term of the functional equation for $L(\chi, L/K)$.

6.4 Artin Representation and Homology (for Algebraic Curves)

Let k be an algebraically closed field of characteristic p, Y a projective non-singular connected algebraic curve over k, and G a finite automorphism group. The quotient curve $X = Y/G$ has function field K, while Y has function field L, giving a Galois extension L/K with group G. For $Q \in Y$ (discrete valuation v_Q), the decomposition group is $D_Q = \{s \in G \mid s(Q) = Q\}$. For the local completion L_Q/K_P with group D_Q, define:

$$i_Q(s) = v_Q(s(t) - t) \quad (s \neq 1, t \text{ local uniformizer at } Q) \tag{6.23}$$

Geometric interpretation: if Γ_s is the graph of s and Λ the diagonal in $Y \times Y$, then $i_Q(s)$ equals the intersection multiplicity of $\Lambda \cdot \Gamma_s$ at $Q \times Q$. The Artin character a_Q (defined on D_Q, extended by zero to G) induces:

$$a_P = \sum_{Q \mapsto P} a_Q \quad \text{for } P \in X \tag{6.24}$$

This is the character of the **Artin representation attached to** P.

Fix a prime $l \neq p$. The l-adic homology of Y gives:

$$H_0(Y) = H_2(Y) = \mathbb{Z}_l \quad (\text{characters } h_0 = h_2 = \mathbf{1}_G) \tag{6.25}$$

$$H_1(Y) = T_l(J) \quad (\text{Tate module of Jacobian } J, \text{ character } h_1) \tag{6.26}$$

Set $h = h_0 - h_1 + h_2$. The Euler characteristic is $E(Y) = h(1) = 2 - 2g_Y$ (genus g_Y), and $E(X) = 2 - 2g_X$.

Proposition 6.4.1

$$h = E(X)\cdot r_G - \sum_{P \in X} a_P \tag{6.27}$$

Corollary 6.4.2

$$\sum_{P \in X} a_P = h_1 + E(X)\cdot r_G - 2\cdot \mathbf{1}_G \tag{6.28}$$

1. Results due to Weil [66]: the sum $\sum a_P$ is rational over $\mathbb{Q}_l$.
2. Each Artin representation A_P is rational over $\mathbb{Q}_l$ ([57], [114]), even beyond equal characteristic.
3. However, H_1 and individual A_P are generally not rational over $\mathbb{Q}$ ([57], nº 4,6), precluding a "trivial" definition (cf. Fontaine [78]).