# Algebraic Number Theory

notes by Weizhe Zheng

February 8, 2010

# Part I
# Global fields and local fields

## 1 Global fields

**Definition 1.1.** A *number field* is a finite extension of the field $\mathbb{Q}$ of rational numbers. A *function field* is a finite extension of the field $\mathbb{F}_q(T)$ of rational functions over a finite field $\mathbb{F}_q$. A *global field* is either a number field or a function field.

**Remark 1.2.** (i) For any number field $K$, there exists a unique embedding $\mathbb{Q} \to K$ since $\mathbb{Q}$ is prime field.

(ii) If $k$ is a field and $K$ is a finite extension of $k(T)$, then every element $T'$ of $K$ transcendental over $k$ defines a $k$-embedding $k(T) \to K$ sending $T$ to $T'$ such that $K$ is a finite extension of $k(T')$.

Any number field is a separable extension of $\mathbb{Q}$ since $\mathbb{Q}$ has characteristic 0. For function fields we have the following result.

**Proposition 1.3.** *Let $k$ be a perfect field, $K$ be a finite extension of $k(T)$. Then there exists an element $T'$ of $K$ such that $K$ is a finite separable extension of $k(T')$.*

This follows from the following.

**Theorem 1.4** (Lüroth)**.** *Let $k$ be a perfect field, $K$ be a subfield of $k(T)$ containing $k$. Then there exists $T'$ in $K$ such that $K = k(T')$.*

# 2 Places

Let $K$ be a field.

**Definition 2.1.** An *absolute value* on $K$ is a function $K \to \mathbb{R}_{\geq 0}$ sending $x$ to $|x|$ such that, for any $x$ and $y$ in $K$, we have

(a) $|x| = 0$ if and only if $x = 0$;

(b) $|xy| = |x||y|$; and

(c) $|x + y| \leq |x| + |y|$ (triangle inequality).

The absolute value is *ultrametric* if, for any $x$ and $y$ in $K$, $|x + y| \leq \max\{|x|, |y|\}$ (strong triangle inequality). An absolute value is *Archimedean* if it is not ultrametric.

A *valued field* is a field endowed with an absolute value. An *ultrametric field* is a field endowed with an ultrametric absolute value.

An absolute value defines a metric on $K$ and hence a topology on $K$. The map $K \to \mathbb{R}_{\geq 0}$ sending $x$ to $|x|$ is continuous if we endow $\mathbb{R}_{\geq 0}$ with the Euclidean topology.

**Example 2.2.** (i) $|x| = 1$ for all $x \neq 0$ defines an ultrametric absolute value on $K$, called the *trivial* absolute value on $K$. It defines the discrete topology on $K$.

(ii) If $|-|$ is an absolute value on $K$, then $|-|^\alpha$ is an absolute value on $K$ for $0 < \alpha \leq 1$. If $|-|$ is an ultrametric absolute value on $K$, then $|-|^\alpha$ is an ultrametric absolute value on $K$ for $\alpha > 0$.

(iii) On $\mathbb{Q}$, the usual absolute value is an absolute value, denoted by $|-|_\infty$.

**Definition 2.3.** Two absolute values on $K$ are *equivalent* if they define the same topology on $K$. A *place* of $K$ is an equivalent class of nontrivial absolute values on $K$.

I.2.p1 **Proposition 2.4.** *Let $|-|_1$ and $|-|_2$ be two absolute values on $K$. The following conditions are equivalent*

*(a) $|-|_1$ and $|-|_2$ are equivalent.*

*(b) $|-|_1 = |-|_2^\alpha$ for some $\alpha > 0$.*

*(c) For any $x$ in $K$, $|x|_1 < 1$ if and only if $|x|_2 < 1$.*

I.2.ta **Theorem 2.5** (Approximation)**.** *Let $v_1, \ldots, v_n$ be pairwise distinct places of $K$. Then the image of the diagonal map $K \to \prod_{i=1}^n K_{v_i}$ is dense, where $K_{v_i}$ is $K$ endowed with the topology defined by $v_i$. In other words, if $|-|_1, \ldots, |-|_n$ are absolute values on $K$ representing $v_1, \ldots, v_n$, respectively, then for any $x_1, \ldots, x_n$ in $K$ and $\epsilon > 0$, there exists $x$ in $K$ such that $|x - x_i|_i < \epsilon$.*

This follows from I.2.p1 2.4.

**Proposition 2.6.** *Let $|-|$ be an absolute value on $K$. The following conditions are equivalent*

*(a) $|-|$ is ultrametric;*

*(b) $|n| \leq 1$ for all $n \in \mathbb{Z}$;*

*(c) The map $K^\times \to \mathbb{R}_{>0}$ sending $x$ to $|x|$ is continuous if we endow $\mathbb{R}_{>0}$ with the discrete topology.*

**Corollary 2.7.** *If the characteristic of $K$ is positive, then every absolute value on $K$ is ultrametric.*

**Definition 2.8.** A *valuation* (of height 1) on $K$ is a function $v\colon K^\times \to \mathbb{R} \cup \{\infty\}$ such that, for any $x$ and $y$ in $K$, we have

(a) $v(x) = \infty$ if and only if $x = 0$;

(b) $v(xy) = v(x) + v(y)$; and

(c) $v(x + y) \geq \min\{v(x), v(y)\}$.

Fix $0 < \epsilon < 1$. For any valuation $v$ on $K$, $|x|_v = \epsilon^{v(x)}$ defines an ultrametric absolute value on $K$. $v \mapsto |-|_v$ gives a bijection from valuations on $K$ to ultrametric absolute values on $K$. We say two valuations $v_1$ and $v_2$ on $K$ are *equivalent* if the corresponding absolute values on $K$ are equivalent.

**Example 2.9.** (i) $v(x) = 0$ for all $x \neq 0$ defines a valuation on $K$, called the trivial valuation on $K$. It corresponds to the trivial absolute value on $K$.

(ii) If $v$ is a valuation on $K$, then $\alpha v$ is a valuation on $K$ equivalent to $v$ for any $\alpha > 0$. Conversely, by I.2.p1 2.4, two valuations $v_1$ and $v_2$ on $K$ are equivalent if and only if $v_1 = \alpha v_2$ for some $\alpha > 0$.

(iii) Let $p$ be a prime number. For any $x$ in $\mathbb{Q}^\times$, $x = p^a r/s$, where $a$, $r$ and $s$ are integers such that $(r, p) = (s, p) = 1$. Put $v_p(x) = a$. This defines a discrete valuation $v_p$ on $\mathbb{Q}$, called the *$p$-adic valuation* on $\mathbb{Q}$. Put $|x|_p = p^{-v_p(x)}$.

If $v$ is a valuation on $K$, $\mathcal{O} = \{x \mid v(x) \geq 0\}$ is a ring, called the *ring* of $v$; $\mathfrak{m} = \{x \mid v(x) > 0\}$ is a maximal ideal, called the *ideal* of $v$. If $v$ is trivial, $\mathcal{O} = K$, $\mathfrak{m} = 0$.

I.2.pr **Proposition 2.10.** *Let $v$ be a nontrivial valuation on $K$, $\mathcal{O}$ be the ring of $v$, $\mathfrak{m}$ be the ideal of $v$. Then $\mathcal{O}$ is a normal local domain of dimension 1. Moreover the following conditions are equivalent*

*(a) $\mathcal{O}$ is a discrete valuation ring;*
*(b) $\mathcal{O}$ is Noetherian;*
*(c) $\mathfrak{m}$ is principal;*
*(d) $v(K^\times)$ is a discrete subgroup of $\mathbb{R}$.*

A valuation $v$ is called *discrete* if it satisfies the conditions of I.2.pr 2.10. It is called *normalized* if $v(K^\times) = \mathbb{Z}$. A generator of $\mathfrak{m}$ is called a *uniformizer* of $v$.

**Definition 2.11.** Let $\Gamma$ be a subset of $\mathbb{R}$. A *major subset* of $\Gamma$ is a subset of $\Gamma$ of the form $\emptyset$, $\Gamma$, $\Gamma \cap \mathbb{R}_{>x}$, or $\Gamma \cap \mathbb{R}_{\geq x}$ for some $x$ in $\mathbb{R}$.

I.2.p3 **Proposition 2.12.** *Let $v$ be a valuation on $K$, $\mathcal{O}$ be the ring of $v$. The map $M \mapsto v(M - \{0\})$ from the set of sub-$\mathcal{O}$-modules of $K$ to the set of major subsets of $v(K^\times)$ is a bijection. In other words, for any absolute value corresponding to $v$, the sub-$\mathcal{O}$-modules of $K$ are $0$, $K$, $\mathring{B}(0,r)$, and $\bar{B}(0,r)$, $r > 0$.*

I.2.p3c **Corollary 2.13.** *The map $I \mapsto v(I - \{0\})$ from the set of ideals of $\mathcal{O}$ to the set of major subsets of $v(\mathcal{O} - \{0\})$ is a bijection. In other words, for any absolute value corresponding to $v$, the ideals of $\mathcal{O}$ are $0$, $\mathring{B}(0,r)$, and $\bar{B}(0,r)$, $0 < r \leq 1$.*

I.2.p4 **Proposition 2.14.** *Let $v_1, \dots, v_n$ be pairwise distinct ultrametric places of $K$, $\mathcal{O}_1, \dots, \mathcal{O}_n$ be the corresponding rings, $\mathfrak{m}_1, \dots, \mathfrak{m}_n$ be the corresponding ideals, $A = \cap_{i=1}^n \mathcal{O}_i$, $\mathfrak{p}_i = \mathfrak{m}_i \cap A$, $i = 1, \dots, n$. Then $\mathrm{Frac}(A) = K$, the maximal ideals of $A$ are $\mathfrak{p}_1, \dots, \mathfrak{p}_n$, which are pairwise distinct, and $A_{\mathfrak{p}_i} = \mathcal{O}_i$, $i = 1, \dots, n$.*

This follows from I.2.ta 2.5.

# 3 Places of $\mathbb{Q}$ and $k(T)$

**Theorem 3.1.** *The places of $\mathbb{Q}$ are the places defined by $|-|_\infty$ and $|-|_p$, where $p$ runs over all primes numbers. They are pairwise distinct.*

Let $\mathbb{F}_q$ be a finite field. Every absolute value on $\mathbb{F}_q(T)$ is trivial on $\mathbb{F}_q$. More generally, for any field $k$, we now determine all the absolute values on $k(T)$ trivial on $k$.

**Example 3.2.** (i) Let $\mathcal{P}$ be the set of monic irreducible polynomials in $k[T]$. Every $f$ in $k(T)^\times$ can be uniquely decomposed as

$$f = \lambda \prod_{P \in \mathcal{P}} P^{v_P(f)},$$

where $\lambda$ is in $k^\times$, $v_P(f)$ is in $\mathbb{Z}$ and is zero for all but a finite number of $P$. Then $v_P$ is a valuation of $k(T)$.

(ii) For $f = \frac{P}{Q}$ in $k(T)^\times$ with $P$ and $Q$ in $k[T] - \{0\}$, define the degree of $f$ to be $\deg f = \deg P - \deg Q$. Then $v_\infty(f) = -\deg f$ is a valuation on $k(T)$.

**Theorem 3.3.** *The places of $k(T)$ inducing the trivial absolute value on $k$ are those defined by $v_P$, $P \in \mathcal{P}$ and $v_\infty$. They are pairwise distinct.*

This establishes a bijection between places of $k(T)$ trivial on $k$ and closed points of the scheme $\mathbb{P}^1_k$.

I.3.p **Proposition 3.4.** *Let $(K, |-|)$ be an ultrametric valued field. For $f = a_0 + a_1X + \cdots + a_nX^n$ in $K[T]$, define $|f|_{\max} = \max_{0 \le i \le n} |a_i|$. This extends unique to an ultrametric absolute value on $K(T)$, which extends $|-|$ on $K$.*

# 4 Completion

Let $(K, |-|)$ be a valued field. Then the completion of $K$

$$\hat{K} = \{\text{Cauchy sequences in } K\}/\{\text{sequences in } K \text{ converging to } 0\}$$

is a field. The absolute value on $K$ extends by continuity to an absolute value on $\hat{K}$. We have $|\hat{K}| = \mathbb{R}_{\ge 0}$ if $K$ is Archimedean, and $|\hat{K}| = |K|$ if $K$ is ultrametric. Moreover, if $K$ is ultrametric, the map $\mathcal{O}_K/\mathfrak{m}_K \to \mathcal{O}_{\hat{K}}/\mathfrak{m}_{\hat{K}}$ is an isomorphism.

**Example 4.1.** (i) The completion of $\mathbb{Q}$ with respect to $v_\infty$ is $\mathbb{R}$. The completion of $\mathbb{Q}$ with respect to $v_p$ is $\mathbb{Q}_p$, the field of $p$-adic numbers.

(ii) Let $k$ be a field, $P$ be a monic irreducible polynomial in $k[T]$, $k_P = k[T]/(P)$. Then $k_P$ is a finite extension of $k$ and the completion of $k(T)$ with respect to $v_P$ is the field $k_P((P))$ of Laurent series. In particular, the completion of $k(T)$ with respect to $v_T$ is $k((T))$. The completion of $k(T)$ with respect to $v_\infty$ is $k((\frac{1}{T}))$.

I.4.tG **Theorem 4.2** (Gelfand-Mazur)**.** *Any Banach algebra over $\mathbb{C}$ that is a division algebra is isomorphic to $\mathbb{C}$.*

I.4.t1 **Theorem 4.3.** *Let $K$ be a complete Archimedean valued field. Then $K$ is isomorphic to either $\mathbb{R}$ or $\mathbb{C}$ as a topological field.*

This follows from I.4.tG 4.2.

**Corollary 4.4.** *Any Archimedean valued field is a subfield of $\mathbb{C}$.*

Let $K$ be a field with a discrete valuation. Then the maps

$$\mathcal{O}_{\hat{K}} \to \varprojlim_{n\in\mathbb{N}} \mathcal{O}_{\hat{K}}/\mathfrak{m}_{\hat{K}}^n, \quad \mathcal{O}_K/\mathfrak{m}_K^n \to \mathcal{O}_{\hat{K}}/\mathfrak{m}_{\hat{K}}^n$$

are isomorphisms.

**Proposition 4.5.** *Let $\mathcal{O}$ be a complete discrete valuation ring, $\pi$ be a uniformizer, $\Sigma$ be a system of representatives for $\mathcal{O}/\mathfrak{m}$. Then every $x$ in $\mathcal{O}$ can be written uniquely as the convergent series $x = x_0 + x_1\pi + \cdots + x_n\pi^n + \ldots$, where $x_i$ is in $\Sigma$ for $i$ in $\mathbb{N}$.*

I.4.p2 **Proposition 4.6.** *Let $K$ be a field with a place, $E$ be a Hausdorff topological $K$-vector space of finite dimension, $(e_i)_{1\le i\le n}$ be a basis for $E$. Assume either $\dim_K E = 1$ or $K$ complete. Then the $K$-linear map $K^n \to E$ sending $(x_i)_{1\le i\le n}$ to $\sum_{1\le i\le n} x_i e_i$ is a homeomorphism.*

**Proposition 4.7** (Inverse function theorem)**.** *Let $(K, |-|)$ be a complete ultrametric field, $\mathcal{O}$ be the ring of the valuation, $f$ be a polynomial in $\mathcal{O}[X]$, $\alpha$ in $\mathcal{O}$. Then $f$ induces a homeomorphism $\mathring{B}(\alpha, \eta) \to \mathring{B}(f(\alpha), \eta^2)$, where $\eta = |f'(\alpha)|$.*

The inverse is constructed by Newton's method.

**Corollary 4.8.** *Suppose $|f(\alpha)| < |f'(\alpha)|^2$. Then there exists a unique $\beta$ in $\mathcal{O}$ such that $f(\beta) = 0$ and $|\beta - \alpha| < |f'(\alpha)|$. Moreover, $|\beta - \alpha| < |f(\alpha)/f'(\alpha)|$ and $f(\beta) = f(\alpha)$.*

**Corollary 4.9.** *Let $f$ be in $\mathcal{O}[X]$, $\bar{\alpha}$ in the residue field $\kappa$ of $K$ be a simple root of the reduction $\phi(f) \in \kappa[X]$ of $f$, that is, $(\phi(f))(\bar{\alpha}) = 0$ and $(\phi(f)')(\bar{\alpha}) \neq 0$. Then $f$ has a unique root $\alpha$ in $\mathcal{O}$ with reduction $\bar{\alpha}$.*

This can be generalized as follows.

I.4.pH **Proposition 4.10** (Hensel's lemma)**.** *Let $K$ be a complete ultrametric field, $\mathcal{O}$ be the ring of the valuation, $\mathfrak{p} \neq \mathcal{O}$ be an ideal of $\mathcal{O}$, $\phi\colon \mathcal{O}[X] \to (\mathcal{O}/\mathfrak{p})[X]$ be the reduction map, $f$ be a polynomial in $\mathcal{O}[X]$, $\phi(f) = \bar{g}\bar{h}$, where $\bar{g}$ and $\bar{h}$ are polynomials in $(\mathcal{O}/\mathfrak{p})[X]$ and $\bar{g}$ is monic. Suppose that $\bar{g}$ and $\bar{h}$ are strongly coprime, that is, that they generate the ideal $(\mathcal{O}/\mathfrak{p})[X]$. Then there exists a unique pair $(g, h)$ of polynomials in $\mathcal{O}[X]$ with $g$ monic such that $f = gh$, $\phi(g) = \bar{g}$, $\phi(h) = \bar{h}$. Moreover, $g$ and $h$ are coprime.*

I.4.pHc **Corollary 4.11.** *Let $f = a_0 + a_1X + \cdots + a_nX^n$ be an irreducible polynomial in $K[X]$ with $a_0a_n \neq 0$. Then $|f|_{\max} = \max\{|a_0|, |a_n|\}$.*

I.4.t2 **Theorem 4.12.** *Let $(K, |-|)$ be a complete valued field, $L$ be a finite extension of $K$ of degree $n$. Then $|\alpha| = \sqrt[n]{|\mathrm{Nm}_{L/K}(\alpha)|}$, $\alpha \in L$ is the unique absolute value on $L$ extending $|-|$.*

The existence follows from I.4.t1 4.3 and I.4.pHc 4.11. The uniqueness follows from I.4.p2 4.6 if $|-|$ is nontrivial and I.5.11c 5.3 if $|-|$ is trivial.

**Corollary 4.13.** *Let $(K, |-|)$ be as in the theorem, $L$ be an algebraic extension of $K$. Then there exists a unique extension of $|-|$ to $L$.*

**Proposition 4.14** (Krasner's lemma)**.** *Let $(K, |-|)$ be a complete ultrametric field, $L$ be a Galois extension of $K$, $\alpha$ be in $L$ and $\beta$ be in $K$. Suppose $|\beta - \alpha| < |\sigma(\alpha) - \alpha|$ for all $\sigma$ in $\mathrm{Gal}(L/K)$ satisfying $\sigma(\alpha) \neq \alpha$. Then $\alpha$ is in $K$.*

This is often applied in the following way. Let $\bar{K}$ be an algebraic closure of $K$, $\alpha$ and $\beta$ be in $\bar{K}$ with $\alpha$ separable over $K$. Suppose $|\beta - \alpha| < |\alpha' - \alpha|$ for all $K$-conjugates $\alpha' \neq \alpha$ of $\alpha$. Then $K(\alpha) \subset K(\beta)$.

I.4.pKc1 **Corollary 4.15.** *Let $K$ be a complete ultrametric field whose absolute value is nontrivial, $L$ be an algebraic extension of $K$. If $L$ is complete, then the separable degree and the inseparable height of $L$ over $K$ are both finite.*

Recall that the *inseparable height* of an element $x$ in $L$ over $K$ is

$$\inf\{n \mid x^{p^n} \text{ is separable over } K\},$$

where $p$ is the characteristic exponent of $K$. The *inseparable height* of $L$ over $K$ is the maximum of the inseparable heights of the elements of $L$ over $K$.

The corollary follows from the proposition and Baire category theorem.

**Example 4.16.** Let $k$ be a field of characteristic $p > 0$,

$$L = k(X_1, X_2, \dots, X_n, \dots)((T))$$

endowed with the $T$-adic topology, $K = L^p$. Then $L$ and $K$ are complete and $L/K$ is an infinite purely inseparable extension of height 1.

I.4.pKc2 **Corollary 4.17.** *The completion of a separably closed ultrametric field is separably closed.*

**Example 4.18.** For any complete discrete valuation field $K$, the separable closure $K^{\text{sep}}$ is not complete by 4.15, but the completion of $K^{\text{sep}}$ is separably closed by 4.17. In particular, for any prime number $p$, the algebraic closure $\overline{\mathbb{Q}_p}$ of $\mathbb{Q}_p$ is not complete, and the completion $\mathbb{C}_p$ of $\overline{\mathbb{Q}_p}$ is algebraically closed.

# 5 Extension of places

Let $L/K$ be a field extension. The restriction of any absolute value on $L$ is an absolute value on $K$.

**Definition 5.1.** Let $w$ be a valuation of $L$, $v = w|K$. The *ramification index* of $w$ over $v$ is $e(w/v) = [w(L^\times) : v(K^\times)]$. The *inertia degree* of $w$ over $v$ is $f(w/v) = [\kappa_w : \kappa_v]$, where $\kappa_w$ and $\kappa_v$ are the residue fields of $w$ and $v$, respectively.

I.5.l1 **Lemma 5.2.** *Let $L/K$ be a finite extension of fields, $n = [L : K]$, $w$ be a valuation on $L$, $v = w|L$. Then*

$$e(w/v)f(w/v) \le n.$$

*In particular, $e(w/v)$ and $f(w/v)$ are both finite.*

I.5.l1c **Corollary 5.3.** *Let $L/K$ be an algebraic field extension, $|-|$ be an absolute value on $L$. If the restriction of $|-|$ is trivial, then $|-|$ is trivial.*

I.5.p1 **Proposition 5.4.** *Let $L/K$ be an algebraic field extension. Then any absolute value on $K$ can be extended to an absolute value on $L$.*

This follows from Zorn's lemma and 5.7 below.

I.5.p1c1 **Corollary 5.5.** *Let $L/K$ be a purely inseparable field extension. Then any absolute value on $K$ can be extended uniquely to an absolute value on $L$.*

I.5.p1c2 **Corollary 5.6.** *Let $L/K$ be a field extension. Then any valuation on $K$ can be extended to a valuation on $L$.*

This follows from Zorn's lemma and I.3.p 3.4.

I.5.p2 **Proposition 5.7.** *Let $L/K$ be a finite extension of fields, $v$ be an absolute value on $K$. Then there are only finitely many absolute values $w_1, \ldots, w_g$ of $L$ above $v$. If*

$$\phi\colon \widehat{K_v} \otimes_K L \to \prod_{i=1}^{g} \widehat{L_{w_i}}$$

*denotes the ring homomorphism induced by the diagonal embedding of $L$, then $\phi$ is surjective and $\operatorname{Ker}\phi$ is the radical of $\widehat{K_v} \otimes_K L$. Moreover,*

$$\sum_{i=1}^{g} n_i \leq g,$$

*where $n_i = [\widehat{L_{w_i}} : \widehat{K_v}]$, $1 \leq n \leq g$ and $n = [L : K]$.*

This follows from approximation theorem I.2.fa4.p2 2.5, 4.6 and I.4.t2 4.12.

I.5.p2c1 **Corollary 5.8.** *With the notations of I.5.p2 5.7, the following conditions are equivalent*

*(a) $\widehat{K_v} \otimes_K L$ is reduced;*
*(b) $\phi$ is an isomorphism;*
*(c) $\sum_{i=1}^{g} n_i = n$;*
*(d) we have an equality of characteristic polynomials*

$$\operatorname{Ch}_{L/K}(x,T) = \prod_{i=1}^{g} \operatorname{Ch}_{\widehat{L_{w_i}}/\widehat{K_v}}(x,T)$$

*for all $x$ in $L$.*

*Moreover, (d) implies*

$$\operatorname{Tr}_{L/K}(x) = \sum_{i=1}^{g} \operatorname{Tr}_{\widehat{L_{w_i}}/\widehat{K_v}}(x), \operatorname{Nm}_{L/K}(x) = \prod_{i=1}^{g} \operatorname{Nm}_{\widehat{L_{w_i}}/\widehat{K_v}}(x)$$

*and $|\operatorname{Nm}_{L/K}(x)|_v = \prod_{i=1}^{g} |x|_{w_i}^{n_i}$ for all $x$ in $L$.*

I.5.p2c2 **Corollary 5.9.** *If $L/K$ is a finite separable extension, then the conditions of I.5.p2c1 5.8 are satisfied.*

I.5.t1 **Theorem 5.10.** *Let $L/K$ be a finite extension, $v$ be a valuation on $K$, $w_1, \ldots, w_g$ be the extensions of $v$ to $L$. Then*

$$\sum_{i=1}^{g} e(w_i/v) f(w_i/v) \leq n.$$

*Moreover, if equality holds, then $e(w_i/v)f(w_i/v) = [\widehat{L_{w_i}} : \widehat{K_v}]$ for all $1 \leq i \leq g$ and the conditions of 5.8 are satisfied.*

I.5.p2c1

This follows from I.5.l1 5.2 and I.4.p2 4.6.

I.5.p3 **Proposition 5.11.** *Let $L/K$ be a field extension, $v$ be a valuation of $K$, $\mathcal{O}_v$ be the ring of $v$. Then the integral closure of $\mathcal{O}_v$ in $L$ is $\cap_w \mathcal{O}_w$, where $w$ runs over the valuations of $L$ above $v$ and $\mathcal{O}_w$ is the ring of $w$.*

This follows from I.5.p1c2 5.6.

I.5.p3c **Corollary 5.12.** *Let $L/K$ be an algebraic field extension, $v$ be a valuation on $K$, $\mathcal{O}_v$ be the ring of $v$, $A$ be the integral closure of $\mathcal{O}_v$ in $L$. Then $w \mapsto A \cap \mathfrak{m}_w$ gives a bijection from the set of extensions of $v$ to $L$ onto* $\mathrm{Max}(A)$*, the set of maximal ideals of $A$, where $\mathfrak{m}_w$ is the ideal of $w$.*

This follows from I.2.p4 2.14.

**Definition 5.13.** Let $L/K$ be a finite extension of fields, $n = [L : K]$, $w$ be a valuation on $L$, $v = w|L$. The *initial ramification index* of $w$ over $v$ is

$$\epsilon(w/v) = \begin{cases} e(w/v) & \text{if } w \text{ is discrete,} \\ 1 & \text{otherwise.} \end{cases}$$

I.5.p4 **Proposition 5.14.** *Let $L/K$ be a finite extension of fields, $w$ be a valuation on $L$, $v = w|K$, $\mathcal{O}_w$ and $\mathcal{O}_v$ be the rings of $w$ and $v$, respectively, and $\mathfrak{m}_v$ be the ideal of $v$. Then $[\mathcal{O}_w/\mathfrak{m}_v\mathcal{O}_w : \mathcal{O}_v/\mathfrak{m}_v] = \epsilon(w/v)f(w/v)$.*

This follows from I.2.p3c 2.13.

I.5.p5 **Proposition 5.15.** *Let $L/K$ be a finite extension of fields, $v$ be a valuation on $K$, $w_1, \ldots, w_g$ be the extensions of $v$ to $L$, $\mathcal{O}_v$ and $\mathfrak{m}_v$ be the ring and the ideal of $v$, respectively, and $A$ be the integral closure of $\mathcal{O}_v$ in $L$. Then $[A/\mathfrak{m}_v A : \mathcal{O}_v/\mathfrak{m}_v] = \sum_{i=1}^{g} \epsilon(w_i/v) f(w_i/v)$.*

This follows from I.5.p3c 5.12.

I.5.t2 **Theorem 5.16.** *With the notations of I.5.p5 5.15, the following conditions are equivalent*

*(a) $A$ is a finite $\mathcal{O}_v$-module;*

*(b) $A$ is a free $\mathcal{O}_v$-module;*

*(c) $[A/\mathfrak{m}_v A : \mathcal{O}_v/\mathfrak{m}_v] = n$;*

*(d) $\sum_{i=1}^{g} e(w_i/v)f(w_i/v) = n$ and $\epsilon(w_i/v) = e(w_i/v)$ for all $1 \leq i \leq g$,*

*where $n = [L : K]$. Moreover, if these conditions are satisfied, then $e(w_i/v)f(w_i/v) \leq [\widehat{L_{w_i}} : \widehat{K_v}]$ for all $1 \leq i \leq g$ and the conditions of I.5.p2c1 5.8 are satisfied.*

This follows from I.5.t1 5.10, I.5.p5 5.15, Nakayama's lemma and the following.

**Lemma 5.17.** *Let $K$ be a field, $v$ be a valuation on $K$, $\mathcal{O}$ be the ring of $v$. Then any finite torsion-free $\mathcal{O}$-module $M$ is free.*

**Proposition 5.18.** *Let $L/K$ be a finite extension of fields.*

*(i) If $L/K$ is purely inseparable, then $\mathrm{Tr}_{L/K}(x) = 0$ for any $x$ in $L$.*

*(ii) If $L/K$ is separable, then $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$ is a non-degenerate $K$-bilinear form on $L$.*

**Definition 5.19.** Let $L/K$ be a finite extension of fields. The *discriminant* of a finite sequence of elements $\alpha_1, \ldots, \alpha_n$ in $L$ over $K$ is the element in $K$ given by

$$D_{L/K}(\alpha_1, \ldots, \alpha_n) = \det(\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)).$$

**Proposition 5.20.** *(i) If $\beta_j = \sum_{j=1}^{n} a_{ji}\alpha_i$, $a_{ij}$ in $K$, $1 \leq j \leq n$, then $D_{L/K}(\beta_1, \ldots, \beta_n) = (\det(a_{ij}))^2 D_{L/K}(\alpha_1, \ldots, \alpha_n)$.*

*(ii) Suppose $L/K$ is separable and $n = [L : K]$. Let $\sigma_1, \ldots, \sigma_n$ be $K$-embeddings of $L$ into a separable closure $K'$ of $K$. Then $D_{L/K}(\alpha_1, \ldots, \alpha_n) = (\det(\sigma_i \alpha_j))^2$. Moreover, $D_{L/K}(\alpha_1, \ldots, \alpha_n) \neq 0$ if and only if $\{\alpha_1, \ldots, \alpha_n\}$ is a $K$-basis of $L$.*

I.5.6 **Proposition 5.21.** *Let $A$ be a normal domain, $K$ be the fraction field of $A$, $L/K$ be a finite separable extension, $B$ be the integral closure of $A$ in $L$, $\{\alpha_1, \ldots, \alpha_n\} \subset B$ be a $K$-basis for $L$, $\{\beta_1, \ldots, \beta_n\} \subset L$ be the dual basis with respect to $\mathrm{Tr}_{L/K}$, $d = D_{L/K}(\alpha_1, \ldots, \alpha_n)$. Then*

$$\alpha_1 A + \ldots \alpha_n A \subset B \subset \beta_1 A + \ldots \beta_n A \subset d^{-1}(\alpha_1 A + \ldots \alpha_n A).$$

**Corollary 5.22.** *Let $A$ be a Noetherian normal domain, $K$ be the fraction field of $A$, $L/K$ be a finite separable extension. Then the integral closure $B$ of $A$ in $L$ is a finite $A$-module.*

**Corollary 5.23.** *Let $A$ be a principal ideal domain, $K$ be the fraction field of $A$, $L/K$ be a finite separable extension. Then the integral closure $B$ of $A$ in $L$ is a free $A$-module of rank $[L:K]$.*

**Corollary 5.24.** *Let $L/K$ be a finite separable field extension, $v$ be a discrete valuation of $K$. Then the conditions of* I.5.t2 *5.16 are satisfied.*

**Proposition 5.25.** *Let $k$ be a field, $K$ be a finite extension of $k(T)$, $L$ be a finite extension of $K$, $v$ be a discrete valuation on $K$, trivial on $k$. Then the conditions of* I.5.t2 *5.16 are satisfied.*

This follows from properties of Nagata rings.

I.5.p7 **Proposition 5.26.** *Let $A \subset B$ be discrete valuation rings, $K$ and $L$ be the fraction fields of $A$ and $B$, $\mathfrak{p}$ and $\mathfrak{P}$ the maximal ideals of $A$ and $B$, respectively, $v$ and $w$ be the corresponding places. Assume either (a) $B$ is a finite $A$-module; or (b) $K$ is complete and $e = e(w/v)$ and $f = f(w/v)$ are finite. Let $\Pi$ be a uniformizer of $w$, $\omega_1, \ldots, \omega_f$ be elements in $B$ such that the images $\overline{\omega_1}, \ldots, \overline{\omega_f}$ form a $A/\mathfrak{p}$-basis of $B/\mathfrak{P}$. Then the homomorphism of $A$-modules*

$$\bigoplus_{i=0}^{e-1} \bigoplus_{j=1}^{f} A \to B$$

*is an isomorphism. Moreover, if $B/\mathfrak{P}$ is a separable extension of $A/\mathfrak{p}$, then there exists $\alpha$ in $B$ such that $B = A[\alpha]$.*

This follows from I.5.l1 5.2, (a) Nakayama's lemma and (b) I.4.p2 4.6.

**Corollary 5.27.** *Let $(K, v)$ be a complete discrete valuation field, $L/K$ be a finite extension. Then the conditions of* I.5.t2 *5.16 are satisfied.*

**Definition 5.28.** Let $(K, v)$ be a complete valuation field, $(L, w)$ be an algebraic extension. If $L/K$ is finite, we say $L/K$ is *unramified*, if the residue field extension is separable and $f(w/v) = [L:K]$. In general, we say $L/K$ is *unramified* if every finite subextension $K' \subset L$ over $K$ is unramified.

An unramified extension is separable.

I.5.pu **Proposition 5.29.** *Let $K$ be a complete valuation field, $L_1$ and $L_2$ be two unramified extension of $K$, $L$ be a composition field of $L_1$ and $L_2$ over $K$. Then $L$ is unramified over $K$.*

This follows from Hensel's lemma I.4.pH 4.10.

**Corollary 5.30.** *Let $K$ be a complete valuation field, $L/K$ be an algebraic extension. Then there exists a unique maximal unramified subextension.*

# 6 Dedekind domains

I.6.p0 **Proposition 6.1.** *Let $A$ be a ring. The following conditions are equivalent*

*(a) $A$ is a discrete valuation ring;*

*(b) $A$ is a normal Noetherian local ring of dimension 1;*

*(c) $A$ is a Noetherian local ring of dimension $\geq 0$ whose maximal ideal is principal.*

I.6.p0c **Corollary 6.2.** *Let $A$ be a Noetherian domain. The following conditions are equivalent*

*(a) $A$ is normal of dimension $\leq 1$;*

*(b) $A_{\mathfrak{p}}$ is a discrete valuation ring for every nonzero prime ideal $\mathfrak{p}$ of $A$.*

**Definition 6.3.** A *Dedekind domain* is a Noetherian domain satisfying the conditions of I.6.p0c 6.2.

**Example 6.4.** The ring of rational integers $\mathbb{Z}$ is a Dedekind domain. For any field $k$, the polynomial ring $k[T]$ is a Dedekind domain.

I.6.tk **Theorem 6.5** (Krull-Akizuki)**.** *Let $A$ be a Noetherian domain of dimension 1, $K$ be the fraction field of $A$, $L/K$ be a finite extension, $B$ be the integral closure of $A$ in $L$. Then $B$ is a Dedekind domain, and above every maximal ideal $\mathfrak{p}$ of $A$, there are only finitely many maximal ideals of $B$.*

**Definition 6.6.** Let $K$ be a number field. The *ring of integers* $\mathcal{O}_K$ of $K$ is the integral closure of $\mathbb{Z}$ in $K$.

**Corollary 6.7.** *$\mathcal{O}_K$ is a Dedekind domain.*

An ideal of a ring $A$ is a sub-$A$-module of $A$. This notion can be generalized as follows.

**Definition 6.8.** Let $A$ be an integral domain, $K$ be the fraction field of $A$. A *fractional ideal of* $A$ is a sub-$A$-module $I$ of $K$. It is *invertible* if there exists a fractional ideal $J$ such that $IJ = A$. A *fractional principal ideal* is a fractional ideal of the form $xA$, $x$ in $K$. The group of (Cartier) *divisors* $\mathrm{Div}(A)$ on $A$ is the group of invertible fractional ideals of $A$. The group of *principal divisors* $\mathrm{Prin.Div}(A)$ on $A$ is the group of invertible fractional principal ideals of $A$. The *Picard group* of $A$ is $\mathrm{Pic}(A) = \mathrm{Div}(A)/\mathrm{Prin.Div}(A)$.

We have $\mathrm{Prin.Div}(A) = K^\times/A^\times$ and hence the following sequence is exact

$$1 \to A^\times \to K^\times \to \mathrm{Prin.Div}(A) \to \mathrm{Div}(A) \to 0.$$