

Algebraic Number Theory II
Exercise Sheet 6¹

Exercise 6.1 (6 points). Let K be a field and $\|\cdot\|$ be a non-archimedean absolute value on K , i.e. a function $\|\cdot\| : K \rightarrow \mathbb{R}_{\geq 0}$ such that

$$\begin{aligned} \|x \cdot y\| &= \|x\| \cdot \|y\|, \\ \|x + y\| &\leq \max\{\|x\|, \|y\|\}, \\ \|x\| = 0 &\iff x = 0. \end{aligned}$$

Let (A, \mathfrak{m}) be the associated valuation ring and valuation ideal, i.e.

$$\begin{aligned} A &= \{x \in K \mid \|x\| \leq 1\}, \\ \mathfrak{m} &= \{x \in K \mid \|x\| < 1\}. \end{aligned}$$

Show:

- (a) (A, \mathfrak{m}) is a local ring.
- (b) A is integrally closed.
- (c) $\dim A \leq 1$, i.e. \mathfrak{m} and (0) are the only prime ideals.
(*Hint*: Show and use the following
Lemma: $\forall x, y \in K : \|x\| \leq \|y\| \implies x \in yA$.)
- (d) The following conditions are equivalent:
 - (i) A is noetherian.
 - (ii) Every ideal in A is principal.
 - (iii) \mathfrak{m} is principal.
 - (iv) $\|\cdot\|$ is discrete, i.e. $\|K^\times\|$ is a discrete subgroup of $\mathbb{R}_{>0}$.
(*Hint*: Using the Lemma from part (c), you can add the following to the list of equivalent conditions:
 - (v) $\exists \pi \in \mathfrak{m} : \|\pi\| = \sup_{m \in \mathfrak{m}} \|m\|$.
 - (vi) $\forall \text{ideal } \mathfrak{a} \subset A \exists \alpha \in \mathfrak{a} : \|\alpha\| = \sup_{a \in \mathfrak{a}} \|a\|$.)

Exercise 6.2 (6 points). Let $p \in \mathbb{Z}$ be a prime number. The p -adic absolute value $\|\cdot\|_p : \mathbb{Q} \rightarrow \mathbb{R}_{\geq 0}$ is defined as $\|x\|_p = \left(\frac{1}{p}\right)^{v_p(x)}$, where $v_p(x) := m$ if $x = p^m \frac{a}{b}$, $\gcd(ab, p) = 1$ and $v_p(0) := \infty$. Consider the sequence $(a_n)_{n \in \mathbb{N}}$ with $a_n := a^{p^n}$, for some $a \in \mathbb{Z}$. Show:

- (a) The sequence (a_n) is a Cauchy sequence w.r.t. the p -adic absolute value $\|\cdot\|_p$ of \mathbb{Q} .
(*Hint*: Show $a^{p^{n+1}} \equiv a^{p^n} \pmod{p^{n+1}}$ by counting the number of units in $\mathbb{Z}/p^{n+1}\mathbb{Z}$. Or use induction, e.g. via showing that $x \equiv y \pmod{p^n}$ implies $x^p \equiv y^p \pmod{p^{n+1}}$.)

¹Questions? Mail to henrik.russell@math.fu-berlin.de or come to office A3, 112

- (b) The sequence (a_n) does not have a limit in \mathbb{Q} for $a \not\equiv 0, \pm 1 \pmod{p}$.

(*Hint:* Find an algebraic equation that must be satisfied by the limit of (a_n) , and show that the solutions in \mathbb{Q} of this equation do not yield the limit as $\lim a_n \equiv a \pmod{p}$.)

- (c) The limit of (a_n) is called the *Teichmüller lift* of $\bar{a}_n \in \mathbb{F}_p$ (for any $n \in \mathbb{N}$) in the completion \mathbb{Z}_p of the discrete valuation ring $\mathbb{Z}_{(p)}$, i.e. of the localization of \mathbb{Z} at p . Show that the Teichmüller lift yields a well-defined homomorphism of multiplicative groups $\tau : \mathbb{F}_p^\times \rightarrow \mathbb{Z}_p^\times$ whose image is the set of $(p-1)^{\text{th}}$ roots of unity in \mathbb{Z}_p . Verify that τ coincides with the unique multiplicative system of representatives that you know from the lectures.

Exercise 6.3 (4 points). Let $A = F[X]$ be the polynomial ring in one variable over a field F and $K = \text{Frac}(A) = F(X)$ the field of rational functions over F . Let v be the discrete valuation associated with a prime ideal $\mathfrak{p} = (f)$ generated by an irreducible separable polynomial $f \in F[X]$, i.e. the valuation defined by the discrete valuation ring $A_{\mathfrak{p}}$.

- (a) Let α be a root of f in an algebraic closure \bar{F} , let $E = F(\alpha)$ be the separable field extension generated by α . Let $E(T)$ be the field of rational functions over the field E and w the discrete valuation associated with the prime ideal (T) .

Show that the map

$$F(X) \longrightarrow E(T), \quad \varphi(X) \longmapsto \varphi(\alpha + T)$$

is a homomorphism of discrete valuation fields from $(F(X), v)$ to $(E(T), w)$.

(*Hint:* Use the formal Taylor expansion of $f(\alpha + T)$.)

- (b) Consider the completion $\widehat{E(T)}$ of $(E(T), w)$ and the composition of maps

$$j : F(X) \longrightarrow E(T) \longrightarrow \widehat{E(T)}.$$

Show that one can view $\widehat{E(T)}$ as a completion of $(F(X), v)$: this means that j induces an isomorphism of residue fields and one can identify the Laurent series of elements of $\widehat{F(X)}$ and of $\widehat{E(T)}$.

Exercise 6.4 (6 points). (a) Let A be a discrete valuation ring, K its field of fractions. Let $L | K$ be a finite field extension of degree n , B the integral closure of A in L . Show that the following conditions are equivalent:

- (i) $L | K$ is totally ramified, i.e. B is a discrete valuation ring, and the valuation w of B extends the valuation v of A with ramification index n .
- (ii) $L = K(\rho)$, where ρ is the root of an Eisenstein polynomial $f \in A[X]$, i.e. $f = X^n + a_{n-1}X^{n-1} + \dots + a_0$ with $v(a_i) \geq 1, v(a_0) = 1$.
- (iii) B is a discrete valuation ring of the form $B = A[\rho]$, where ρ is a uniformizer.

(Hints: (i) \Rightarrow (ii) Let ρ be a uniformizer of B and $f = \sum_{i=0}^n a_i X^i$, $a_n = 1$ its characteristic polynomial. Say why the coefficients of f belong to A . Conclude from $f(\rho) = 0$ and the fact

$$w(b_i) \neq w(b_j) \quad \forall i \neq j \implies w\left(\sum_l b_l\right) = \min_l w(b_l)$$

that there are $i \neq j$ such that $w(a_i \rho^i) = w(a_j \rho^j) = \min_l w(a_l \rho^l)$. Taking into account that $w(\rho) = 1, w(a) \equiv 0 \pmod n \quad \forall a \in A$ (why?), check that this can only be fulfilled for $i = n, j = 0$. Show that this implies the Eisenstein condition on f .

(ii) \Rightarrow (iii) What do the maximal ideals of $A[X]/(f)$ look like? Show that $A[X]/(f)$ is a local noetherian ring whose maximal ideal is generated by a non-nilpotent element, hence is a discrete valuation ring, and that this implies that $K[X]/(f)$ is a field. Conclude that f is irreducible, hence that the map $X \mapsto \rho$ gives an isomorphism $K[X]/(f) \xrightarrow{\sim} L$. Show that this yields an isomorphism $A[X]/(f) \xrightarrow{\sim} B$.

(iii) \Rightarrow (i) Compute the residue field of B . Use the formula $[L : K] = \sum_{\mathfrak{p}|p} e_{\mathfrak{p}} f_{\mathfrak{p}}$.

- (b) *Application:* From the lecture you know that any complete discrete valuation ring A of characteristic 0 with perfect residue field k of characteristic $p > 0$ is a totally ramified extension of $W(k)$. Here $W(k)$ is the unique (up to unique isomorphism) discrete valuation ring which is absolutely unramified and has k as its residue field. Then Exercise 6.4 (a) tells us that A is obtained from $W(k)$ by adjoining an element ρ which is the root of an Eisenstein polynomial.

Conversely, any Eisenstein polynomial of degree n defines a totally ramified extension of $W(k)$ of degree n . Show that this yields a complete discrete valuation ring of unequal characteristic.