ALGEBRAISCHE ZAHLENTHEORIE II

KATHARINA HÜBNER

Inhaltsverzeichnis

Date: 16. April 2025.

1. Kreisteilungskörper

Wir wollen unser Repertoire an Beispielen für Zahlkörper um die Kreisteilungskörper erweitern. Das sind die endlichen Erweiterungen von $\mathbb{Q}$, die durch Adjunktion einer primitiven n-ten Einheitswurzel ζ_n (für ein $n \in \mathbb{N}$) entstehen.

1.1. **Wiederholung aus der Algebra.** Die grundlegenden Eigenschaften von Kreisteilungskörpern sollten aus der Algebra bekannt sein. In diesem Abschnitt geben wir eine Zusammenfassung der wichtigsten Eigenschaften.

Definition 1.1. Sei n eine natürliche Zahl und K ein Körper. Eine *n-te Einheitswurzel* in K ist ein Element $\zeta \in K$, das Nullstelle des Polynoms $T^n - 1$ ist.

Die Menge der n-ten Einheitswurzeln in einem Körper bildet eine Gruppe bezüglich der Multiplikation. Wir bezeichnen sie mit $\mu_n(K)$. Genauer kann sie beschrieben werden als die n-Torsionsuntergruppe von $K^\times$. Da $T^n - 1$ in K maximal n Nullstellen hat, ist die Ordnung von $\mu_n(K)$ kleiner oder gleich n. Insbesondere ist $\mu_n(K)$ eine endliche Untergruppe von $K^\times$ und somit zyklisch. Für einen Erzeuger ζ von $\mu_n(K)$ gilt $\zeta^n = 1$, also

$$m := \mathrm{ord}(\zeta) = \#\mu_n(K) \mid n.$$

In der Tat sehen wir daraus, dass

$$\mu_m(K) = \mu_n(K)$$

und die Kardinalität von $\mu_m(K)$ ist m, also enthält $\mu_m(K)$ die maximal mögliche Anzahl von Elementen. In dem Fall sagen wir auch, dass K die m-ten Einheitswurzeln enthält. Beispielsweise enthält $\mathbb{Q}$ nur die ersten und zweiten Einheitswurzeln (also 1 und -1), aber sonst keine weiteren. Das gleiche gilt für $\mathbb{R}$. Die komplexen Zahlen $\mathbb{C}$ dagegen enthalten alle n-ten Einheitswurzeln für jede natürliche Zahl n. Es sind genau die Elemente der Form $e^{2\pi ik/n}$ für $k, n \in \mathbb{N}$.

Definition 1.2. Es enthalte K die n-ten Einheitswurzeln. Ein Erzeuger ζ_n von $\mu_n(K)$ heißt *primitive n-te Einheitswurzel*.

Die Wahl einer primitiven n-ten Einheitswurzel $\zeta_n \in K$ induziert einen Isomorphismus

$$\begin{aligned} \mathbb{Z}/n\mathbb{Z} &\longrightarrow \mu_n(K), \\ k &\longmapsto \zeta_n^k. \end{aligned}$$

Die Ordnung von ζ_n^k ist $n/\mathrm{ggT}(n,k)$. Insbesondere ist ζ_n^k genau dann eine primitive n-te Einheitswurzel, wenn k teilerfremd zu n ist. Die Anzahl der Restklassen $[k]$ modulo n, so dass k teilerfremd zu n ist, ist durch die Eulersche φ-Funktion gegeben. Folglich gilt

$$\#\{\zeta \in \mu_n(K) \text{ primitiv}\} = \varphi(n).$$

Die n-ten Einheitswurzeln sind genau die Nullstellen von $T^n - 1$ in K. Nehmen wir nun an, dass K die n-ten Einheitswurzeln enthält. Ist $\zeta \in \mu_n(K)$ bereits in $\mu_m(K)$ für einen Teiler m von n enthalten, so ist ζ bereits eine Nullstelle von $T^m - 1$. Das Polynom $T^m - 1$ ist ein Teiler von $T^n - 1$. Da $T^n - 1$ separabel ist, ist $T^m - 1$ ein Teiler der Multiplizität 1. Eine primitive n-te Einheitswurzel kann nun beschrieben werden als eine Nullstelle von

$T^n - 1$, die keine Nullstelle von $T^m - 1$ ist für einen echten Teiler m von n. Mithilfe von etwas Kombinatorik und der Möbiusschen μ Funktion

$$\mu : \mathbb{N} \longrightarrow \mathbb{C},$$
$$d \longmapsto \mu(d) := \begin{cases} (-1)^m & d = p_1 \cdot \ldots \cdot p_m \text{ Primfaktorzerlegung mit } p_i \neq p_j \\ 0 & d \text{ nicht quadratfrei} \end{cases}$$

erhalten wir folgende Proposition.

Proposition 1.3. *Es gibt eine natürliche Bijektion*

$$\{\zeta \in \mu_n(K) \text{ primitiv}\} \cong \{\text{Nullstellen von } \Phi_n := \prod_{m|n} (T^m - 1)^{\mu(n/m)}\}$$

Die rationale Funktion Φ_n ist in der Tat ein Polynom und heißt *n-tes Kreisteilungspolynom*. Wegen obiger Bijektion ist Φ_n ein Teiler von $T^n - 1$ und hat die alternative Darstellung

$$\Phi_n(T) = \prod_{\substack{\zeta \in \mu_n(K) \\ \text{primitiv}}} (T - \zeta).$$

Da die Anzahl der n-ten Einheitswurzeln gleich $\varphi(n)$ ist, erhalten wir, wenn wir den Grad von Φ_n betrachten, folgende Formel

$$\varphi(n) = \sum_{m|n} m\mu(n/m),$$

die schon aus der elementaren Zahlentheorie bekannt ist.

Wenn $n = p^k$ eine Potenz einer Primzahl p ist, vereinfacht sich die Darstellung von Φ_n:

$$\Phi_n(T) = \Phi_{p^k}(T) = \frac{T^{p^k} - 1}{T^{p^{k-1}} - 1}.$$

Insbesondere ist

$$\Phi_p(T) = \frac{T^p - 1}{T - 1} = T^{p-1} + T^{p-2} + \ldots + T + 1$$

und hat den Grad $p - 1$.

Wir wollen nun die Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ für eine primitive n-te Einheitswurzel $\zeta_n \in \mathbb{C}$ beschreiben. Da ζ_n die Gruppe $\mu_n(\mathbb{C})$ der n-ten Einheitswurzeln erzeugt, ist $\mathbb{Q}(\zeta_n)$ der Zerfällungskörper von $T^n - 1$ und insbesondere unabhängig von der Wahl von ζ_n. Wir können daher auch alternativ schreiben

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\mu_n).$$

Wir nennen $\mathbb{Q}(\mu_n)$ den *n-ten Kreisteilungskörper* von $\mathbb{Q}$.

Aus obiger Überlegung folgt außerdem, dass die Erweiterung $\mathbb{Q}(\mu_n)/\mathbb{Q}$ galoissch ist. Da ζ_n ein primitives Element der Erweiterung $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ ist, ist die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ eindeutig durch ihre Wirkung auf ζ_n bestimmt. Für $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ muss $\sigma(\zeta_n)$ wieder eine primitive n-te Einheitswurzel sein. Es gilt also

$$\sigma(\zeta_n) = \zeta_n^{\chi_n(\sigma)}$$

für ein Element $\chi_n(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^\times$. Die Abbildung

$$\chi_n : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \longrightarrow \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$$
$$\sigma \longmapsto \chi(\sigma)$$

ist ein Gruppenhomomorphismus. Sie heißt *zyklotomischer Charakter*.

Proposition 1.4. *Der zyklotomische Charakter χ_n induziert einen Isomorphismus*

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \xrightarrow{\sim} \left(\mathbb{Z}/n\mathbb{Z}\right)^\times.$$

Beweis. Algebra. □

Daraus schließen wir auch, dass

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \#\left(\mathbb{Z}/n\mathbb{Z}\right)^\times = \varphi(n).$$

Wir wollen nun ein besonderes Element der Galoisgruppe betrachten, dass immer in $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ enthalten ist (für $n \geq 3$), nämlich die komplexe Konjugation F. Auf den Einheitswurzeln $\zeta \in \mathbb{C}$ wirkt sie folgendermaßen:

$$F(\zeta) = \zeta^{-1}.$$

Das sieht man sofort, wenn man sich daran erinnert, dass ζ von der Form $e^{2\pi ik/n}$ ist. Die komplexe Konjugation F hat Ordnung 2. Der entsprechende Fixkörper

$$\mathbb{Q}(\zeta_n)^+ := \mathbb{Q}(\zeta_n)^F$$

ist vom Grad $\varphi(n)/2$ über $\mathbb{Q}$ und

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n)^+] = 2.$$

Tatsächlich gilt

Lemma 1.5.

$$\mathbb{Q}(\zeta_n)^+ = \mathbb{Q}(\zeta_n + \zeta_n^{-1}).$$

Beweis. Das sieht man indem man die Wirkung von F auf ein allgemeines Element x von $\mathbb{Q}(\zeta_n)$ untersucht. Hierbei beachte man, dass die Potenzen ζ_n^k für $k \in \{0, \ldots, n-1\}$ teilerfremd zu n eine Basis von $\mathbb{Q}(\zeta_n)$ über $\mathbb{Q}$ bilden. □

Falls n das Produkt zweier teilerfremder natürlicher Zahlen m und k ist, gibt uns der chinesische Restsatz einen Isomorphismus

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}$$

und für die Einheitengruppen

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^\times \cong \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/k\mathbb{Z}\right)^\times.$$

Für die Gruppe der Einheitswurzeln bedeutet das

$$\mu_n(\mathbb{C}) \cong \mu_m(\mathbb{C}) \times \mu_k(\mathbb{C})$$

und für die entsprechenden Galoisgruppen

$$\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\mu_m)/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_k)/\mathbb{Q}).$$

Via Galoistheorie können wir diese Aussage in folgende Aussage über Körpererweiterungen übersetzen: Der Erweiterungskörper $\mathbb{Q}(\mu_n)$ von $\mathbb{Q}$ ist das Kompositum (in $\mathbb{C}$) von $\mathbb{Q}(\mu_m)$ und $\mathbb{Q}(\mu_k)$:

$$\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_m)\mathbb{Q}(\mu_k).$$

und $\mathbb{Q}(\mu_m)$ und $\mathbb{Q}(\mu_k)$ sind linear disjunkt (in unserem Fall von Galoiserweiterungen bedeutet das einfach $\mathbb{Q}(\mu_m) \cap \mathbb{Q}(\mu_k) = \mathbb{Q}$). Ist

$$n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$$

die Primfaktorzerlegung von n, so erhalten wir

$$\mathbb{Q}(\mu_n) = \mathbb{Q}(\mu_{p_1^{k_1}}) \cdot \ldots \cdot \mathbb{Q}(\mu_{p_r^{k_r}})$$

und

$$\mathrm{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{p_1^{k_1}})/\mathbb{Q}) \times \ldots \times \mathrm{Gal}(\mathbb{Q}(\mu_{p_r^{k_r}})/\mathbb{Q}).$$

In vielen Fällen ist es ausreichend die Erweiterungen $\mathbb{Q}(\mu_{p^k})/\mathbb{Q}$ für eine Primzahl p und eine natürliche Zahl k zu untersuchen. Das entsprechende Resultat für $\mathbb{Q}(\mu_n)$ für beliebige natürliche Zahlen n folgt dann durch Kompositumbildung.

1.2. **Der Ganzheitsring und die Diskriminante.** Wir fixieren eine natürliche Zahl $n \in \mathbb{N}$ und betrachten den Kreisteilungskörper $K = \mathbb{Q}(\mu_n) = \mathbb{Q}(\zeta_n)$. In diesem Abschnitt wollen wir den Ganzheitsring $\mathcal{O}_K$ und die Diskriminante d von K bestimmen. Da ζ_n eine Nullstelle des normierten Polynoms

$$T^n - 1 \in \mathbb{Z}[T]$$

ist, ist ζ_n ganz über $\mathbb{Z}$. Daher folgt

$$\mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_K.$$

A priori könnte $\mathcal{O}_K$ echt größer sein.

Zunächst widmen wir uns einer bestimmten Sorte von Einheiten in $\mathcal{O}_K$, also Elementen von $E_K := \mathcal{O}_K^\times$.

Lemma 1.6. *Für $k, \ell \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$ ist*

$$\frac{1-\zeta_n^k}{1-\zeta_n^\ell} \in E_K.$$

Beweis. Da ℓ und k Einheiten in $\mathbb{Z}/n\mathbb{Z}$ sind, gibt es $r \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times$, so dass

$$k = r\ell$$

gilt. Mit der geometrischen Summenformel erhalten wir

$$\frac{1-\zeta_n^k}{1-\zeta_n^\ell} = \frac{1-(\zeta_n^\ell)^r}{1-\zeta_n^\ell} = 1 + \zeta_n^\ell + \ldots + (\zeta_n^\ell)^{r-1} \in \mathbb{Z}[\zeta_n] \subseteq \mathcal{O}_K.$$

Genauso zeigt man

$$\left(\frac{1-\zeta_n^k}{1-\zeta_n^\ell}\right)^{-1} = \frac{1-\zeta_n^\ell}{1-\zeta_n^k} \in \mathcal{O}_K.$$

Daraus folgt

$$\frac{1-\zeta_n^k}{1-\zeta_n^\ell} \in E_K.$$

□

Mit anderen Worten kann man sagen, dass für zwei primitive n-te Einheitswurzeln ζ und ζ' das Element

$$\frac{1-\zeta}{1-\zeta'}$$

eine Einheit ist, also ein Element von E_K.

Definition 1.7. Einheiten der Form

$$\frac{1-\zeta}{1-\zeta'}$$

für primitive n-te Einheitswurzeln ζ und ζ' nennt man *Kreisteilungseinheiten.*

Wir beschäftigen uns nun zunächst mit den Kreisteilungskörpern der Form $\mathbb{Q}(\zeta_{p^r})$ für eine Primzahl p und eine natürliche Zahl r. Deren Struktur ist einfacher und vieles kann man explizit berechnen. Am Schluss werden wir daraus auf Aussagen über $\mathbb{Q}(\zeta_n)$ für beliebiges n schließen.

Lemma 1.8. *Sei $\zeta := \zeta_{p^r}$ eine primitive p^r-te Einheitswurzel und*

$$\lambda := 1 - \zeta.$$

Dann ist das Hauptideal

$$(\lambda) = (1-\zeta) \subseteq \mathcal{O}_K$$

ein Primideal vom Trägheitsgrad 1 (über $\mathbb{Z}$) und es gilt

$$(p) = (\lambda)^{\varphi(p^r)} = (\lambda)^{[\mathbb{Q}(\zeta):\mathbb{Q}]}$$

(für die Eulersche φ-Funktion).

Beweis. Nach Proposition 1.4 sind die Potenzen ζ^k für $k \in \left(\mathbb{Z}/p^r\mathbb{Z}\right)^\times$ genau die $\varphi(p^r)$ verschiedenen Galoiskonjugierten von ζ über $\mathbb{Q}$. Damit ist das Minimalpolynom von ζ gleich

$$\prod_{k\in(\mathbb{Z}/p^r\mathbb{Z})^\times} (T - \zeta^k).$$

Nach Proposition 1.3 ist das genau das p^r-te Kreisteilungspolynom

$$\Phi_{p^r}(T) = \frac{T^{p^r}-1}{T^{p^{r-1}}-1} = 1 + T^{p^{r-1}} + T^{2p^{r-1}} + \ldots + T^{p^r}.$$

Setzen wir in beiden Darstellungen des Minimalpolynoms $T = 1$, erhalten wir die Gleichung

$$p = \prod_{k\in(\mathbb{Z}/p^r\mathbb{Z})^\times} (1-\zeta^k) = \prod_{k\in\mathbb{Z}/p^r\mathbb{Z}} \frac{1-\zeta^k}{1-\zeta} \cdot (1-\zeta)^{\varphi(p^r)}.$$

Die Faktoren $(1-\zeta^k)/(1-\zeta)$ sind Einheiten nach Lemma 1.6. Daher folgt

$$(p) = (1-\zeta)^{\varphi(p^r)} = (\lambda)^{\varphi(p^r)}$$

als Ideale von $\mathcal{O}_K$. Wir untersuchen nun die fundamentale Gleichung

$$[\mathbb{Q}(\zeta):\mathbb{Q}] = gef$$

(für die Anzahl der Primideale g über p vom Verzweigungsindex e und Trägheitsgrad f). Aus der obigen Idealgleichung folgt, dass der Verzweigungsindex e ein Vielfaches von $\varphi(p^r)$ sein muss. Da $\varphi(p^r) = [\mathbb{Q}(\zeta):\mathbb{Q}]$, ist die einzige Möglichkeit, dass (λ) prim ist, $e = \varphi(p^r)$ und $f = g = 1$. □

Die Erkenntnisse über das Primideal $(\lambda) = (1-\zeta)$ für eine primitive p^r-te Einheitswurzel ζ werden eine wichtige Rolle spielen bei der Bestimmung des Ganzheitsrings $\mathcal{O}_K$. Wir brauchen noch eine weitere Zutat, nämlich die Diskriminante der Basis $\{1, \zeta, \ldots, \zeta^{\varphi(p^r)-1}\}$ von $K = \mathbb{Q}(\zeta)$ über $\mathbb{Q}$. Die Verbindung zum Ganzheitsring wird dann über die Inklusion

$$d(1, \zeta, \ldots, \zeta^{\varphi(p^r)-1})\mathcal{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$$

aus Algebraischer Zahlentheorie 1 (AZT 1), Satz 3.11 hergestellt.

Lemma 1.9. *Die Diskriminante der Basis*

$$\{1, \zeta, \ldots, \zeta^{\varphi(p^r)-1}\} \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K$$

von $K := \mathbb{Q}(\zeta)$ über $\mathbb{Q}$ ist

$$d(1, \zeta, \ldots, \zeta^{\varphi(p^r)-1}) = (-1)^{\frac{\varphi(p^r)}{2}} p^{p^{r-1}(rp-r-1)}$$

(hierbei nehmen wir immer noch an $p^r \neq 2$).

Beweis. Wir setzen $K = \mathbb{Q}(\zeta)$ und

$$d := \varphi(p^r) = [\mathbb{Q}(\zeta) : \mathbb{Q}].$$

Die Galoiskonjugierten von ζ sind die Potenzen ζ^k für $k \in \left(\mathbb{Z}/p^r\mathbb{Z}\right)^\times$. Daher liefert die Formel für die Diskriminante (AZT 1, Korollar 3.8):

$$d(1, \zeta, \ldots, \zeta^{d-1}) = \prod_{i<j} (\zeta^j - \zeta^i)^2 = (-1)^{\frac{d(d-1)}{2}} \prod_{i \neq j} (\zeta^j - \zeta^i),$$

wobei die Indizes i, j Elemente von $\{0, 1, \ldots, p^r - 1\}$ sind, die teilerfremd zu p^r sind. Das können wir mithilfe der Ableitung des Kreisteilungspolynoms

$$\Phi_{p^r}(T) = \prod_i (T - \zeta^i)$$

umschreiben. Setzt man in die Ableitung

$$\Phi'_{p^r}(T) = \sum_j \prod_{i \neq j} (T - \zeta^i)$$

für T den Wert ζ^j ein, erhält man

$$\Phi'_{p^r}(\zeta^j) = \prod_{i \neq j} (\zeta^j - \zeta^i).$$

Die Diskriminante wird dann zu

$$d(1, \zeta, \ldots, \zeta^{d-1}) = (-1)^{\frac{d(d-1)}{2}} \prod_j \Phi'_{p^r}(\zeta^j) = (-1)^{\frac{d(d-1)}{2}} \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \sigma(\Phi'_{p^r}(\zeta)).$$

Auf der rechten Seite steht das Produkt über alle Galoiskonjugierten von $\Phi'(\zeta)$, also nach AZT 1, Satz 2.8, die Norm von $\Phi'_{p^r}(\zeta)$:

$$d(1, \zeta, \ldots, \zeta^{d-1}) = (-1)^{\frac{d(d-1)}{2}} N_{K/\mathbb{Q}}(\Phi'_{p^r}(\zeta).$$

Jetzt müssen wir noch $\Phi'_{p^r}(\zeta)$ berechnen. Ableiten von

$$\Phi_{p^r}(T) = \frac{T^{p^r} - 1}{T^{p^{r-1}} - 1}$$

ergibt

$$\Phi'_{p^r}(T) = \frac{(T^{p^{r-1}} - 1) p^r T^{p^r - 1} - (T^{p^r} - 1) p^{r-1} T^{p^r - - 1}}{(T^{p^{r-1}} - 1)^2}.$$

Setzen wir nun $T = \zeta$ ein, fällt der zweite Summand im Zähler weg und wir können einen Faktor $(\zeta^{p^{r-1}} - 1)$ kürzen:

$$\Phi'_{p^r}(\zeta) = \frac{p^r \zeta^{-1}}{\zeta^{p^{r-1}} - 1}.$$

Die Potenz $\zeta^{p^{r-1}}$ ist eine primitive p-te Einheitswurzel, wir nennen sie ζ_p. Dann wird die Diskriminante zu

$$d(1,\zeta,\dots,\zeta^{d-1}) = (-1)^{\frac{d(d-1)}{2}} \frac{N_{K/\mathbb{Q}}(p^r\zeta^{-1})}{N_{K/\mathbb{Q}}(\zeta_p - 1)} = (-1)^{\frac{d(d-1)}{2}} \frac{p^{rd} N_{K/\mathbb{Q}}(\zeta^{-1})}{N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p-1)^{[K:\mathbb{Q}(\zeta_p)]}}.$$

Es gilt

$$[K:\mathbb{Q}(\zeta_p)] = \frac{\varphi(p^r)}{\varphi(p)} = p^{r-1}.$$

Über die Gleichung

$$p = \prod_{i=1}^{p-1}(1-\zeta_p^i) = N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p)$$

aus dem Beweis von Lemma 1.8 (für $r=1$) können wir die Norm von $\zeta_p - 1$ berechnen:

$$N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p - 1) = (-1)^{p-1} N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(1-\zeta_p) = (-1)^{p-1}p.$$

Das ergibt dann für die Norm bezüglich $K/\mathbb{Q}$:

$$\begin{aligned} N_{K/\mathbb{Q}}(\zeta_p - 1) &= N_{K/\mathbb{Q}(\zeta_p)}(N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p-1)) \\ &= \big(N_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p-1)\big)^{[K:\mathbb{Q}(\zeta_p)]} \\ &= (-1)^{(p-1)p^{r-1}} p^{p^{r-1}} = (-1)^d p^{p^{r-1}}. \end{aligned}$$

Jetzt fehlt noch

$$N_{K/\mathbb{Q}}(\zeta) = \prod_{k\in(\mathbb{Z}/p^r\mathbb{Z})^\times} \zeta^k$$

Ist p ungerade, so ist die einzige Potenz von ζ, die in $\mathbb{Q}$ enthalten ist, gleich 1, also ist die Norm gleich 1. Für $p=2$ muss man die Summe über alle ungeraden natürlichen Zahlen kleiner 2^r berechnen:

$$\sum_{m=1}^{2^{r-1}} (2m-1) = 2^{r-1}(2^{r-1}+1) - 2^{r-1} = 2^{2(r-1)} = 2^r \cdot 2^{r-2}.$$

Das ist durch 2^r teilbar (für $r>1$, aber den Fall $2^r = 2$, also $r=1$ und $p=2$ haben wir ausgeschlossen). Daher ist

$$N_{K/\mathbb{Q}}(\zeta) = \zeta^{2^{2(r-1)}} = 1$$

auch in diesem Fall.

Setzen wir alles zusammen, erhalten wir

$$d(1,\zeta,\dots,\zeta^{d-1}) = (-1)^{\frac{d(d-1)}{2}+d} \frac{p^{rd}}{p^{p^{r-1}}} = (-1)^{\frac{d(d+1)}{2}} p^{rd-p^{r-1}}.$$

Jetzt erinnern wir uns daran, dass

$$d = \varphi(p^r) = (p-1)p^{r-1}.$$

Damit erhalten wir

$$d(1,\zeta,\dots,\zeta^{d-1}) = (-1)^{\frac{d(d+1)}{2}} p^{p^{r-1}(rp-r-1)}.$$

Außerdem ist d gerade (hier brauchen wir $p^r \neq 2$). Deshalb gilt

$$(-1)^{\frac{d(d+1)}{2}} = (-1)^{\frac{d}{2}} = (-1)^{\frac{\varphi(p^r)}{2}}.$$

□

Proposition 1.10. *Sei p eine Primzahl und r eine natürliche Zahl. Dann gilt für $K = \mathbb{Q}(\zeta_{p^r})$:*

$$\mathcal{O}_K = \mathbb{Z}[\zeta].$$

Beweis. Für $p^r = 2$ ist $K = \mathbb{Q}$ und die Behauptung ist klar. Wir nehmen im Folgenden $p^r \neq 2$ an.

Wir wissen aus Lemma 1.8, dass der Trägheitsgrad des Primideals $(\lambda) = (1-\zeta)$ über p gleich 1 ist, also

$$\mathcal{O}_K/\lambda\mathcal{O}_K \cong \mathbb{Z}/p\mathbb{Z}.$$

Daraus folgt

$$\mathcal{O}_K = \mathbb{Z} + \lambda\mathcal{O}_K = \mathbb{Z}[\zeta] + \lambda\mathcal{O}_K.$$

Setzen wir auf der rechten Seite für $\mathcal{O}_K$ wieder $\mathbb{Z}[\zeta] + \lambda\mathcal{O}_K$ ein, so erhalten wir iterativ:

$$\begin{aligned}\mathcal{O}_K &= \mathbb{Z}[\zeta] + \lambda\mathcal{O}_K \\ &= \mathbb{Z}[\zeta] + \lambda(\mathbb{Z}[\zeta] + \lambda\mathcal{O}_K) \\ &= \mathbb{Z}[\zeta] + \lambda^2\mathcal{O}_K \\ &\vdots \\ &= \mathbb{Z}[\zeta] + \lambda^n\mathcal{O}_K\end{aligned}$$

für jedes $n \in \mathbb{N}$.

Die Strategie ist nun zu zeigen, dass $\lambda^n\mathcal{O}_K$ für genügend großes n bereits in $\mathbb{Z}[\zeta]$ enthalten ist. Wir betrachten die Basis

$$\{1, \zeta, \ldots, \zeta^{d-1}\} \subseteq \mathcal{O}_K$$

von K über $\mathbb{Q}$. Dann gilt nach AZT 1, Satz 3.11:

$$d(1, \zeta, \ldots, \zeta^{d-1}) \cdot \mathcal{O}_K \subseteq \mathbb{Z}[\zeta].$$

Setzen wir die Berechnung der Diskriminante aus Lemma 1.9 ein, so erhalten wir

$$p^{p^{r-1}(pr-r-1)}\mathcal{O}_K \subseteq \mathbb{Z}[\zeta] \subseteq \mathcal{O}_K.$$

Außerdem wissen wir aus Lemma 1.8, dass

$$p\mathcal{O}_K = \lambda^{\varphi(p^r)}\mathcal{O}_K = \lambda^{p^{r-1}(p-1)}$$

gilt. Daraus folgt

$$\lambda^{p^r(p-1)(pr-r-1)}\mathcal{O}_K \subseteq \mathbb{Z}[\zeta]$$

Wenn wir also die Gleichung

$$\mathcal{O}_K = \mathbb{Z}[\zeta] + \lambda^n\mathcal{O}_K$$

für eine natürliche Zahl $n \geq p^r(p-1)(pr-r-1)$ untersuchen, dann gilt $\lambda^n\mathcal{O}_K \subseteq \mathbb{Z}[\zeta]$ und folglich können wir schließen, dass

$$\mathcal{O}_K = \mathbb{Z}[\zeta].$$

□

An dieser Stelle haben wir den Ganzheitsring eines Kreisteilungskörpers der Form $\mathbb{Q}(\zeta_{p^r})$ bestimmt:

$$\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$$

und

$$\{1, \zeta_{p^r}, \ldots, \zeta_{p^r}^{\varphi(p^r)-1}\}$$

ist eine Ganzheitsbasis. Um einen allgemeinen Kreisteilungskörper zu behandeln brauchen wir folgendes allgemeine Resultat über Komposita von Körpererweiterungen.

Proposition 1.11. *Sei A ein Dedekindring mit Quotientenkörper $K = K(A)$. Wir betrachten zwei endliche Galoiserweiterungen L/K und L'/K, für die gilt $L \cap L' = K$. Wir nehmen an, dass die Ganzabschlüsse A_L und $A_{L'}$ über A Ganzheitsbasen*

$$\{e_1, \dots, e_n\} \quad \{e'_1, \dots, e'_{n'}\}$$

besitzen (mit $n = [L : K]$ und $n' = [L' : K]$). Sind die Diskriminanten d und d' von L und L' teilerfremd in A, so ist

$$\{e_i e'_j\}_{\substack{1 \le i \le n \\ 1 \le j \le n'}}$$

eine Ganzheitsbasis von LL' und $d^{n'} d'^{n}$ ist die Diskriminante.

Beweis. Aus Algebra wissen wir, dass

$$\{e_i e'_j\}_{\substack{1 \le i \le n \\ 1 \le j \le n'}}$$

eine Basis von LL'/K ist. Außerdem ist LL'/K galoissch mit Galoisgruppe

$$\mathrm{Gal}(LL'/K) \cong \mathrm{Gal}(L/K) \times \mathrm{Gal}(L'/K).$$

Schreiben wir

$$\mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_n\}, \qquad \mathrm{Gal}(L'/K) = \{\sigma'_1, \dots, \sigma'_{n'}\},$$

so erhalten wir explizit

$$\mathrm{Gal}(LL'/K) = \{\sigma_i \sigma_j\}_{\substack{1 \le i \le n \\ 1 \le j \le n'}},$$

wobei die σ_i trivial auf L' und die σ'_j trivial auf L operieren.

Wir können jedes Element $\alpha \in A_{LL'}$ eindeutig in der Form

$$\alpha = \sum_{ij} \alpha_{ij} e_i e'_j$$

mit Koeffizienten $\alpha_{ij} \in K$ schreiben. Um zu zeigen, dass die $e_i e'_j$ eine Ganzheitsbasis bilden, müssen wir nachweisen, dass die jeweiligen Koeffizienten α_{ij} für jedes $\alpha \in A_{LL'}$ schon in A enthalten sind.

Wir betrachten die Matrix

$$T := (\sigma'_i e'_j)_{ij} \in M_{n'}(A_{L'}) \subseteq M_{n'}(A_{LL'}).$$

Mit ihrer Hilfe kann man die Diskriminante von L' berechnen:

$$d' = (\det T)^2.$$

Wir betrachten außerdem für $j = 1, \dots, n'$ die Elemente

$$\beta_j := \sum_{i=1}^{n} \alpha_{ij} e_i \in L \subseteq LL'$$

und die Vektoren

$$a := \begin{pmatrix} \sigma'_1 \alpha \\ \vdots \\ \sigma'_{n'} \alpha \end{pmatrix}, \qquad b := \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{n'} \end{pmatrix}$$

in $(LL')^{n'}$. Es gilt sogar $a \in A_{LL'}^{n'}$, aber für b wissen wir das nicht. Nach Definition von α gilt

$$a = Tb.$$

Wir multiplizieren diese Gleichung mit der adjunkten Matrix T^{ad} und erhalten

$$T^{ad}a = T^{ad}Tb = \det T \cdot b.$$

Daraus folgt

$$\det T \cdot b \in A_{LL'}^{n'}$$

und insbesondere auch

$$d'b = (\det T)^2 b \in A_{LL'}^{n'}.$$

Komponentenweise bedeutet das gerade

$$d'\beta_j = \sum_{i=1}^{n} d'\alpha_{ij} e_i \in A_{LL'}$$

für alle $j = 1, \ldots, n'$. Da $\{e_1, \ldots, e_n\}$ eine Ganzheitsbasis von A_L über A ist, folgt daraus

$$d'\alpha_{ij} \in A$$

für alle Indizes i und j.

Vertauschen wir die Rollen von L und L', so erhalten wir mit dem gleichen Argument, dass

$$d\alpha_{ij} \in A$$

für alle i und j. Da d und d' teilerfremd sind, folgt daraus

$$\alpha_{ij} \in A$$

für alle Indizes i und j.

Nun fehlt noch die Berechnung der Diskriminante von LL' über K. Sie das Quadrat der Determinante der Matrix

$$M := (\sigma_k \sigma'_\ell e_i e'_j)_{(k,\ell),(i,j)}.$$

Hierbei indizieren k und ℓ die Zeilen und i und j die Spalten. Wir müssen für die Paare (k, ℓ) und (i, j) nur eine Ordnung festlegen um eine tatsächliche Matrix zu erhalten. Für die Diskriminante spielt die Ordnung keine Rolle, da umsortieren nur das Vorzeichen der Determinante der Matrix ändert und wir diese am Schluss quadrieren. Wir sortieren also die Paare (k, ℓ) lexikografisch:

$$(1,1), (2,1), \ldots, (n,1), (1,2), \ldots, (n,2), \ldots, (1,n'), \ldots, (n,n')$$

und genauso für (i, j). Als $(n' \times n')$ Blockmatrix von $(n \times n)$-Matrizen können wir dann M in der Form

$$M = \begin{pmatrix} (\sigma_k e_i)_{ki} & & 0 \\ & \ddots & \\ 0 & & (\sigma_k e_i)_{ki} \end{pmatrix} \begin{pmatrix} \sigma'_1 e'_1 \mathbb{1}_n & \cdots & \sigma'_1 e'_{n'} \mathbb{1}_n \\ \vdots & \ddots & \vdots \\ \sigma'_{n'} e'_1 \mathbb{1}_n & \cdots & \sigma'_{n'} e'_{n'} \mathbb{1}_n \end{pmatrix}$$

schreiben. Dann können wir die Diskriminante folgendermaßen berechnen:

$$d(e_i e'_j) = (\det M)^2 = (\det(\sigma_k e_i)_{ki})^{2n'} (\det(\sigma'_\ell e'_j)_{\ell j})^{2n} = d^{(n')} (d')^n.$$

□

Die obige Proposition können wir nun auf $\mathbb{Q}(\zeta_n)$ anwenden um den Ganzheitsring und die Diskriminante zu bestimmen.

Satz 1.12. *Sei n eine natürliche Zahl mit Primfaktorzerlegung*

$$n = p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}.$$

Für eine primitive n-te Einheitswurzel ζ_n ist

$$\{1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}\}$$

eine Ganzheitsbasis von $\mathbb{Q}(\zeta_n)$. Insbesondere gilt

$$\mathcal{O}_K = \mathbb{Z}[\zeta_n].$$

Die Diskriminante von $\mathbb{Q}(\zeta_n)$ ist

$$d = (-1)^{\frac{r\varphi(n)}{2}} \frac{n^{\varphi(n)}}{\prod_{i=1}^r p_i^{\varphi(n)/(p_i-1)}}.$$

Beweis. Zunächst machen wir uns klar, dass wir Proposition 1.11 auf das Kompositum

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(p_1^{k_1}) \cdot \ldots \cdot \mathbb{Q}(p_r^{k_r})$$

anwenden können. Das liegt daran, dass $\mathbb{Q}(\zeta_{p_i^{k_i}})$ die Ganzheitsbasis $\{1, \zeta_{p_i^{k_i}}, \ldots, \zeta_{p_i^{k_i}}^{\varphi(p_i^{k_i})}\}$ besitzt und die Diskriminante eine p_i-Potenz ist (also sind alle Diskriminanten teilerfremd).

Die Produkte $\zeta_{p_1^{k_1}}^{i_1} \cdot \ldots \cdot \zeta_{p_r^{k_r}}^{i_r}$ bilden nach Proposition 1.11 eine Ganzheitsbasis von $\mathbb{Q}(\zeta_n)$. Sie liegen alle in $\mathbb{Z}[\zeta_n]$. Da $\mathbb{Z}[\zeta_n]$ im Ganzheitsring enthalten ist, folgt daraus

$$\mathcal{O}_K = \mathbb{Z}[\zeta_n]$$

oder in anderen Worten $\{1, \zeta_n, \ldots, \zeta_n^{\varphi(n)-1}\}$ ist eine Ganzheitsbasis.

Wir berechnen nun noch die Diskriminante. Damit die Notation nicht zu lang wird, setzen wir

$$K_i := \mathbb{Q}(\zeta_{p_i^{k_i}})$$

und

$$d := \varphi(n), \qquad d_i := \varphi(p_i^{k_i}).$$

Dann gilt

$$d = d_1 \cdot \ldots \cdot d_r$$

Nun gibt uns Proposition 1.11

$$d_K = \prod_{i=1}^r d_{K_i}^{[K:K_i]} = \prod_{i=1}^r d_{K_i}^{d/d_i}.$$

Für d_{K_i} können wir die Formel aus Lemma 1.9 einsetzen:

$$\begin{aligned}
d_K &= \prod_{i=1}^r \left((-1)^{\frac{d_i}{2}} p_i^{p_i^{k_i-1}(p_i k_i - k_i - 1)} \right)^{d/d_i} \\
&= \prod_{i=1}^r (-1)^{\frac{d}{2}} p_i^{d(k_i - \frac{1}{p_i-1})} \\
&= (-1)^{\frac{rd}{2}} \frac{(\prod_{i=1}^r p_i^{k_i})^d}{\prod_{i=1}^r p_i^{d/(p_i-1)}} \\
&= (-1)^{\frac{rd}{2}} \frac{n^d}{\prod_{i=1}^r p_i^{d/(p_i-1)}}.
\end{aligned}$$

□

1.3. **Einheitswurzeln über endlichen Körpern.** Wir wollen zusammentragen, was wir darüber wissen, welche Einheitswurzeln in einem endlichen Körper $\mathbb{F}$ enthalten sind.

Lemma 1.13. *Sei p eine Primzahl und $r \in \mathbb{N}$. Dann gilt*

$$\mu(\mathbb{F}_{p^r}) = \mu_{p^r-1}(\overline{\mathbb{F}}_{p^r})$$

und

$$\#\mu_{p^r-1}(\mathbb{F}_{p^r}) = p^r - 1$$

Beweis. Wir wissen schon, dass für alle $x \in \mathbb{F}_{p^r}$ gilt:

$$x^{p^r} = x$$

Falls $x \neq 0$, gilt sogar

$$x^{p^r-1} = 1$$

Jedes Element von $\mathbb{F}_{p^r}^\times$ ist also eine Nullstelle des Polynoms $T^{p^r-1} - 1$ oder in anderen Worten: jedes $x \in \mathbb{F}_{p^r}^\times$ ist eine (p^r-1)-te Einheitswurzel. Da außerdem

$$\#\mathbb{F}_{p^r}^\times = p^r - 1$$

enthält $\mathbb{F}_{p^r}$ alle (p^r-1)-ten Einheitswurzeln, □

Damit können wir untersuchen, was passiert, wenn man zu einem endlichen Körper eine primitve m-te Einheitswurzel adjungiert:

Proposition 1.14. *Wir betrachten den endlichen Körper $\mathbb{F}_p$, eine natürliche Zahl m teilerfremd zu p und eine primitive m-te Einheitswurzel $\zeta_m \in \overline{\mathbb{F}}_p$. Sei*

$$f := \operatorname{ord}\Big(\underbrace{[p]}_{\substack{\text{Restklasse von} \\ p \text{ in } \mathbb{Z}/m\mathbb{Z}}} \in \big(\mathbb{Z}/m\mathbb{Z}\big)^\times \Big)$$

Dann gilt

$$[\mathbb{F}_p(\zeta_m) : \mathbb{F}_p] = f$$

Beweis. Der Körper $\mathbb{F}_p(\zeta_m)$ ist endlich der Kardinalität p^r für eine noch zu bestimmende natürliche Zahl r. Es gilt dann $\mathbb{F}_p(\zeta_m)/\mathbb{F}_{p^r}$ und $[\mathbb{F}_p(\zeta_m) : \mathbb{F}_p] = r$. Wir wissen aus Lemma 1.13, dass

$$\mu(\mathbb{F}_{p^r}) = \mu_{p^r-1}(\overline{\mathbb{F}}_p)$$

Somit ist r die kleinste natürliche Zahl n, so dass $\zeta_m \in \mu_{p^n-1}(\overline{\mathbb{F}}_p)$, also

$$\begin{aligned} r &= \min_{n\in\mathbb{N}}\{\zeta_m^{p^n-1} = 1\} \\ &= \min_{n\in\mathbb{N}}\{m \mid p^n - 1\} \\ &= \min_{n\in\mathbb{N}}\{m \mid p^n - 1\} \\ &= \min_{n\in\mathbb{N}}\{p^n \equiv 1 \pmod m\} = f \end{aligned}$$

□

1.4. **Zerlegungsverhalten in Kreisteilungskörpern.** In Abschnitt 1.2 haben wir schon gesehen, dass in $\mathcal{O}_{\mathbb{Q}(\zeta_{p^r})}$ gilt

$$(p) = (\lambda)^{\varphi(p^r)} = (1-\zeta_{p^r})^{\varphi(p^r)}$$

Das heißt, p ist in der Erweiterung $\mathbb{Q}(\zeta_{p^r})/\mathbb{Q}$ rein verzweigt. Wir wollen nun das Zerlegungsverhalten einer beliebigen Primzahl in einem Kreisteilungskörper $\mathbb{Q}(\zeta_n)$ untersuchen.

Satz 1.15. *Sei n eine natürliche Zahl mit Primfaktorzerlegung $n = \prod_p p^{r_p}$ (für $r_p \in \mathbb{N}$, $r_p = 0$ für fast alle p). Für jede Primzahl p definieren wir*

$$f_p := \min\left\{k \in \mathbb{N} \mid p^k \equiv 1 \pmod{\frac{n}{p^{r_p}}}\right\} = \operatorname{ord}\left\{[p] \in \left(\mathbb{Z}/_{(n/p^{r_p})\mathbb{Z}}\right)^\times\right\}$$

Dann hat p in $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ die Primfaktorzerlegung

$$(p) = (\mathfrak{p}_1 \dots \mathfrak{p}_g)^{\varphi(p^{r_p})}$$

für $g = \frac{\varphi(n/p^{r_p})}{f_p}$ und paarweise verschiedene Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_g \subseteq \mathcal{O}_{\mathbb{Q}(\zeta_n)}$ vom Trägheitsgrad f_p.

Beweis. Wir wollen die Zerlegung von $p\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ mithilfe von Satz 8.36 aus AZT 1 bestimmen. Dafür betrachten wir das primitive Element ζ_n von $\mathbb{Q}(\zeta_n)/\mathbb{Q}$. Aus Satz 1.12 wissen wir, dass $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$. Daher ist der Führer von ζ_n trivial und Satz 8.36 gibt uns das Zerlegungsverhalten für jede beliebige Primzahl. Wir müssen nun die Zerlegung des Minimalpolynoms von ζ_n, also des n-ten Kreisteilungspolynoms Φ_n modulo p untersuchen.

Behauptung:

$$\Phi_n(T) \equiv (p_1(T) \dots p_g(T))^{\varphi(p^{r_p})} \pmod{p}$$

Nach Satz 8.36 aus AZT 1 folgt aus dieser Behauptung die Aussage des Satzes. Um die Behauptung zu zeigen, setzen wir $= n/p^{r_p}$. Dann gilt $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_{p^{r_p}}) = \mathbb{Q}$ und $Q(\zeta_n) = \mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_{p^{r_p}})$. Außerdem ist wegen $(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/m\mathbb{Z})^\times \times (\mathbb{Z}/p^{r_p}\mathbb{Z})^\times$

$$\left\{\zeta_m^k \zeta_{p^{r_p}}^\ell \mid k \in \left(\mathbb{Z}/_{m\mathbb{Z}}\right)^\times, \ell \in \left(\mathbb{Z}/_{p^{r_p}\mathbb{Z}}\right)^\times\right\}$$

gerade die Menge der primitiven n-ten Einheitswurzeln (und die $\zeta_m^k \zeta_{p^{r_p}}^\ell$ sind paarweise verschieden). Daraus folgt

$$\Phi_n(T) = \prod_{\substack{k \in (\mathbb{Z}/m\mathbb{Z})^\times \\ \ell \in (\mathbb{Z}/p^{r_p}\mathbb{Z})^\times}} (T - \zeta_m^k \zeta_{p^{r_p}}^\ell)$$

Für ein Primideal $\mathfrak{p} \mid (p)$ gilt:

$$T^{p^{r_p}} - 1 \equiv (T-1)^{p^{r_p}} \pmod{p}$$

Daraus folgt

$$[\zeta_{p^{r_p}}^\ell]_\mathfrak{p} = [1] \in k(\mathfrak{p}) = {}^{\mathcal{O}_{\mathbb{Q}(\zeta_{p^{r_p}})}}/_\mathfrak{p}$$

Also gilt

$$\begin{aligned}\Phi_n(T) &= \prod_{k,\ell}(T - \zeta_m^k \zeta_{p^{r_p}}^{\ell}) \\ &\equiv \prod_{k}(T - \zeta_m^k)^{\varphi(p^{r_p})} \pmod{\mathfrak{p}} \\ &\varphi_m(T)^{\varphi(p^{r_p})} \pmod{\mathfrak{p}}\end{aligned}$$

Das heißt also $[\Phi_n(T)]_{\mathfrak{p}} = [\Phi_m(T)^{\varphi(p^{r_p})}]_{\mathfrak{p}}$ in $k(\mathfrak{p})$. Beide Seiten liegen schon in $\mathbb{F}_p = k(p) \subseteq k(\mathfrak{p})$. Daher gilt

$$\Phi_n(T) \equiv \Phi_m(T)^{\varphi(p^{r_p})} \pmod{p}$$

Nun müssen wir noch $[\Phi_m(T)]_p \in \mathbb{F}_p[T]$ in irreduzible Faktoren zerlegen. Da m und p teilerfremd sind, ist $[\Phi_m(T)]_p$ separabel. Das liegt daran, dass $[\Phi_m(T)]_p$ ein Teiler von $[T^m - 1]_p$ ist und $[T^m - 1]_p$ ist separabel. Es gilt in $\overline{\mathbb{F}}_p[T]$:

$$[\Phi_m(T)]_p = \prod_{k \in (\mathbb{Z}/m\mathbb{Z})^\times} (T - [\zeta_m]^k)$$

Die irreduziblen Faktoren sind die Minimalpolynome einer primitiven m-ten Einheitswurzel $[\zeta_m]_{\mathfrak{p}}^k$. Ihr Grad ist $[\mathbb{F}_p([\zeta_m]_{\mathfrak{p}}^k) : \mathbb{F}_p] = f_p$ nach Proposition 1.14. Nach der fundamentalen Gleichung (oder Vergleich der Grade der Polynome) ist die Anzahl der irreduziblen Faktoren gleich

$$g = \frac{\varphi(n)}{\varphi(p^{r_p}) f_p} = \frac{\varphi(n/p^{r_p})}{f_p}$$

□

Korollar 1.16. *(i) Sei $p \neq 2$ eine Primzahl. Dann verzweigt p in $\mathbb{Q}(\zeta_n)$ genau dann, wenn $p \mid n$ und p ist voll zerlegt genau dann, wenn $p \equiv 1 \pmod{n}$.*

(ii) Die Primzahl 2 verzweigt genau dann in $\mathbb{Q}(\zeta_n)$, wenn $4 \mid n$. Nur für $n = 1, 2$ ist 2 voll zerlegt.

Beweis. (i) Nach Satz 1.15 ist p genau dann verzweigt, wenn $\varphi(p^{r_p}) \neq 1$. Das ist genu dann der Fall, wenn $p \mid n$. Außerdem ist p genau dann voll zerlegt, wenn $\varphi(p^{r_p}) = 1$ und $f_p = 1$. Die erste Gleichung behauptet $p \nmid n$ und die zweite Gleichung $\operatorname{ord}\{[p]_n \in \left(\mathbb{Z}/n\mathbb{Z}\right)^\times\} = 1$, also anders ausgedrückt $p \equiv 1 \pmod{n}$.

(ii) Es ist $\varphi(2^{r_2}) = 1$ genau dann, wenn $r_2 \in \{0, 1\}$. Das heißt 2 verzweigt genau dann, wenn $r_2 \geq 2$, also $4 \mid n$. Damit 2 voll zerlegt sein kann, muss gelten $\varphi(2^{r_2}) = 1$ also $r_2 \in \{0, 1\}$ und $f_2 = 1$, also

$$\operatorname{ord}\left\{[2]_n \in \left(\mathbb{Z}/(n/2^{r_2})\mathbb{Z}\right)^\times\right\} = 1$$

das heißt

$$2 \equiv 1 \pmod{n/2^{r_2}}$$

Diese Kongruenz gilt aber nur, wenn $n/2^{r_2} = 1$, also $n = 1$ und $r_2 = 0$ oder $n = 2$ und $r_2 = 1$.

□

1.5. **Das quadratische Reziprozitätsgesetz.** *Erinnerung*: Für eine Primzahl p und eine natürliche Zahl n ist das *Legendresymbol* folgendermaßen definiert:

$$\left(\frac{n}{p}\right) := \begin{cases} 0 & n \equiv 0 \pmod{p} \\ 1 & [n]_p \text{ ist ein Quadrat in } \mathbb{F}_p \\ -1 & [n]_p \text{ ist kein Quadrat in } \mathbb{F}_p \end{cases}$$

Im Fall $\left(\frac{n}{p}\right) = 1$ sagt man auch, dass n ein *quadratischer Rest* modulo p ist und falls $\left(\frac{n}{p}\right) = -1$, dass n kein quadratischer Rest modulo p ist.

Beispiel 1.17.

$$\left(\frac{n}{5}\right) = \begin{cases} 0 & 5 \mid n \\ 1 & n \equiv \pm 1 \pmod{5} \\ -1 & n \equiv -2 \pmod{5} \end{cases}$$

Lemma 1.18. *Für $n, m \in \mathbb{N}$ und eine Primzahl p gilt*

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$$

Beweis. Unter dem Isomorphismus

$$\varphi : \mathbb{F}_p^\times \xrightarrow{\sim} \mathbb{Z}/(p-1)\mathbb{Z}$$

entsprechen die Quadrate gerade den Restklassen von geraden Zahlen. Daher ist $\left(\frac{mn}{p}\right) = 1$ genau dann, wenn $\varphi(mn) = \varphi(m) + \varphi(n)$ gerade ist. Das tritt genau dann ein, wenn $\varphi(m)$ und $\varphi(n)$ entweder beide gerade oder beide ungerade sind. Das heißt, dass $\left(\frac{mn}{p}\right) = 1$ ist genau dann, wenn entweder $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) = 1$ oder $\left(\frac{m}{p}\right) = \left(\frac{n}{p}\right) = -1$. Das beweist die Multiplikativität. □

Nach AZT 1, Beispiel 8.37 gibt es folgenden Zusammenhang mit dem Zerlegungsverhalten in quadratischen Zahlkörpern: Für eine ungerade Primzahl p und eine quadratfreie natürliche Zahl n gilt

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & p \text{ zerfällt in } \mathbb{Q}(\sqrt{n}) \\ -1 & p \text{ träge in } \mathbb{Q}(\sqrt{n}) \\ 0 & p \text{ verzweigt in } \mathbb{Q}(\sqrt{n}) \end{cases}$$

Satz 1.19. *Für ungerade Primzahlen p und q gilt*

(i)

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \cdot (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

(ii) Erster Ergänzungssatz:

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

(iii) Zweiter Ergänzungssatz:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Beweis. (ii) Es ist $\left(\frac{-1}{p}\right)$ genau dann gleich 1 wenn p in $\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$ zerfällt, also nach Korollar 1.16 wenn $p \equiv 1 \pmod 4$. Das ist genau dann der Fall, wenn $(-1)^{\frac{p-1}{2}} = 1$.

(i) Wir betrachten den Kreisteilungskörper $\mathbb{Q}(\zeta_q)$ die Galoisgruppe

$$G := \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$$

ist zyklisch vom Grad $q-1$. Da $q \neq 2$ ist, ist $q-1$ gerade und G besitzt eine eindeutig bestimmte Untergruppe H vom Index 2. Wir bezeichnen mit

$$K := \mathbb{Q}(\zeta_q)^H$$

den Fixkörper von H. Dann ist K ein quadratischer Zahlkörper, also von der Form

$$K = \mathbb{Q}(\sqrt{d})$$

für eine quadratfreie ganze Zahl d. Die Erweiterung $K/\mathbb{Q}$ verzweigt genau in den Primteilern der Diskriminante d_K. Diese haben wir in AZT 1, Beispiel 3.19 berechnet:

$$d_K = \begin{cases} 4d & d \equiv 2,3 \pmod 4 \\ d & d \equiv 1 \pmod 4 \end{cases}$$

Andererseits verzweigt $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ genau in der Primzahl q. Daher kann $K/\mathbb{Q}$ als Zwischenerweiterung von $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ höchstens in q verzweigen und insbesondere nicht in 2. Somit muss $d_K = d = \pm q$ gelten und $d \equiv 1 \pmod 4$. Das ist äquivalent zu $d = (-1)^{\frac{q-1}{2}} q$. Nun kommt p ins Spiel Sei g die Anzahl der Primideale in $\mathcal{O}_{\mathbb{Q}(\zeta_q)}$ über p. Nach Hilbertscher Verzweigungstheorie gilt

$$g = \frac{\#G}{\#Z_p}$$

für die Zerlegungsgruppe $Z_p \subseteq G$ für Primideale über p. Da $\mathbb{Q}(\zeta_q)/\mathbb{Q}$ abelsch ist, ist die Zerlegungsgruppe für alle Primideale über p gleich und wir können tatsächlich einfach Z_p schreiben. Es ist also g genau dann gerade, wenn $(G : Z_p)$ gerade ist. Da G zyklisch ist, ist das genau dann der Fall

$$Z_p \subseteq H$$

Das bedeutet äquivalent, dass p in $K/\mathbb{Q}$ voll zerlegt ist. Nach Beispiel 8.37 ist das äquivalent zu

$$\left(\frac{d}{p}\right) = 1$$

Die linke Seite berechnen wir folgendermaßen:

$$\begin{aligned} \left(\frac{d}{p}\right) &= \left(\frac{(-1)^{\frac{q-1}{2}} q}{p}\right) \\ &= \left(\frac{-1}{p}\right)^{\frac{q-1}{2}} \cdot \left(\frac{q}{p}\right) \\ &= (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right) \end{aligned}$$

Andererseits ist die Anzahl der Primideale über p nach Satz 1.15 gleich

$$g = \frac{\varphi(q)}{f_p} = \frac{q-1}{f_p},$$

wobei $f_p = \mathrm{ord}_{(\mathbb{Z}/q\mathbb{Z})^\times}([p]_q)$. Das heißt g ist gerade genau dann, wenn

$$f_p \mid \frac{q-1}{2}$$

Nach Definition von f_p ist das äquivalent zu $[p]_q^{\frac{q-1}{2}} = 1$ in $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$. Da $\left(\mathbb{Z}/q\mathbb{Z}\right)^\times$ zyklisch der Ordnung $q-1$ ist, ist das genau dann der Fall, wenn $[p]_q$ ein Quadrat ist, also

$$\left(\frac{p}{q}\right) = 1$$

Damit haben wir gezeigt

$$(-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right) = 1 \Leftrightarrow \left(\frac{p}{q}\right) = 1$$

Da $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$ nur die Werte ± 1 annehmen könne, folgt daraus

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right)$$

(iii) Für den zweiten Ergänzungssatz betrachten wir den Kreisteilungskörper

$$\mathbb{Q}(\zeta_8)$$

Wir behaupten, dass

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(i)\mathbb{Q}(\sqrt{2})$$

Da i eine primitive vierte Einheitswurzel ist, folgt $\mathbb{Q}(i) \subseteq \mathbb{Q}(\zeta_8)$. Außerdem ist $\mathbb{Q}(\sqrt{2}) \cap \mathbb{Q}(i) = \mathbb{Q}$ und $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = \varphi(8) = 4$. Daher reicht es zu zeigen, dass

$$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\zeta_8)$$

also $\sqrt{2} \in \mathbb{Q}(\zeta_8)$. Ein guter Ansatz ist, zu vermuten, dass $\mathbb{Q}(\sqrt{2})$ gerade die maximale reelle Teilerweiterung $\mathbb{Q}(\zeta_8)^+$ ist. Es gilt nach Lemma 1.5:

$$\mathbb{Q}(\zeta_8)^+ = \mathbb{Q}(\zeta_8 + \zeta_8^{-1})$$

Tatsächlich gilt

$$(\zeta_8 + \zeta_8^{-1})^2 = \zeta_8^2 + 2 + \zeta_8^{-2} = i + 2 - i = 2$$

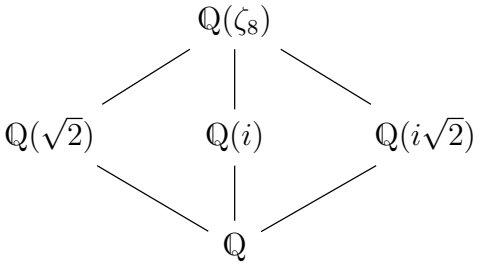
Das heißt $\zeta_8 + \zeta_8^{-1} = \pm\sqrt{2}$ und folglich

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(\zeta_8 + \zeta_8^{-1}) = \mathbb{Q}(\zeta_8)^+ \subseteq \mathbb{Q}(\zeta_8)$$

Damit ist die Behauptung

$$\mathbb{Q}(\zeta_8) = \mathbb{Q}(i)\mathbb{Q}(\sqrt{2})$$

gezeigt. Um $\left(\frac{2}{p}\right)$ zu bestimmen, müssen wir untersuchen, ob p in der Erweiterung $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ träge oder zerlegt ist. Dafür benutzen wir die Informationen wir über $\mathbb{Q}(\zeta_8)$ und seine Zwischenkörper



haben. Es ist

$$\mathrm{Gal}(\mathbb{Q}(\zeta_8)/\mathbb{Q}) \cong \left(\mathbb{Z}/8\mathbb{Z}\right)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

Also gilt $f_p = \mathrm{ord}_{(\mathbb{Z}/8\mathbb{Z})^\times}([p]_8) \in \{1,2\}$. Wenn $f_p = 1$ ist, bedeutet das, dass p in $\mathbb{Q}(\zeta_8)$ voll zerlegt ist, was nach Korollar 1.16 äquivalent ist zu $p \equiv 1 \pmod 8$. In diesem Fall ist p auch in $\mathbb{Q}(\sqrt{2})$ zerlegt. In allen anderen Fällen ist $f_p = 2$ und die Anzahl g der Primideale von $\mathcal{O}_{\mathbb{Q}(\zeta_8)}$ über p ist auch 2. Nach dem ersten Ergänzungssatz (ii) ist p in $\mathbb{Q}(i)$ genau dann zerlegt, wenn $p \equiv 1 \pmod 4$. Ist $p \equiv 5 \pmod 8$, muss p in $\mathbb{Q}(\sqrt{2})$ träge sein, da sonst p in $\mathbb{Q}(i)$ und $\mathbb{Q}(\sqrt{2})$, folglich auch in $\mathbb{Q}(\zeta_8)$, voll zerlegt wäre.

Bis jetzt wissen folgendes:

$p \pmod 8$	p in $\mathcal{O}_{\mathbb{Q}(\sqrt{2})}$
1	zerlegt
3	?
5	träge
7	?

Für den Fall, dass $p = 3, 5 \pmod 8$ ist, reicht es nicht, $p \pmod 8$ zu betrachten. Wir müssen p modulo 16 untersuchen, was darauf hinausläuft, den Kreisteilungskörper $\mathbb{Q}(\zeta_{16})$ zu studieren. Es gilt

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q}) \cong \left(\mathbb{Z}/16\mathbb{Z}\right)^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

Hierbei entspricht das Element

$$(1,0) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$$

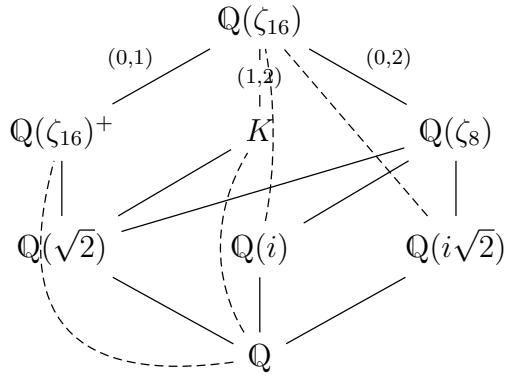
der komplexen Konjugation $F \in \mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q})$. Der Fixkörper von F ist

$$\mathbb{Q}(\zeta_{16})^+ = \mathbb{Q}(\zeta_{16} + \zeta_{16}^{-1})$$

Außerdem ist $\mathbb{Q}(\zeta_8) \subseteq \mathbb{Q}(\zeta_{16})$ mit

$$[\mathbb{Q}(\zeta_{16}) : \mathbb{Q}(\zeta_8)] = 2$$

Daraus schließen wir, dass die Zwischenkörper von $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$ die folgenden sind:



Wobei die gestrichelten Erweiterungen jeweils Galoisgruppe $\mathbb{Z}/4\mathbb{Z}$ haben. Der Trägheitsgrad von p berechnet sich folgendermaßen:

$$f_p = \mathrm{ord}_{(\mathbb{Z}/16\mathbb{Z})^\times}([p]_{16}) = \begin{cases} 1 & p \equiv 1 \pmod{16} \\ 2 & p \equiv -1, \pm 7 \pmod{16} \\ 4 & p \equiv \pm 3, \pm 5 \pmod{16} \end{cases}$$

Falls $p \equiv 1, 5, -7, -3 \pmod{16}$ ist, wissen wir schon aus der Betrachtung modulo 8, was passiert. Ist $p \equiv 3$ oder -5 modulo 16, hat die Trägheitsgruppe T_p Ordnung 4. Außerdem ist die Trägheitsgruppe für unverzweigte Erweiterungen immer zyklisch (da sie dann isomorph zr Galoisgruppe der Restklassenkörpererweiterung ist). Daher gilt entweder $T_p = \mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q}(i))$ oder $T_p = \mathrm{Gal}(\mathbb{Q}(\zeta_{16})/\mathbb{Q}(i\sqrt{2}))$. Das bedeutet, dass p entweder in $\mathbb{Q}(i)$ oder in $\mathbb{Q}(i\sqrt{2})$ voll zerlegt ist. Dann muss p in $\mathbb{Q}(\sqrt{2})$ träge sein, da sonst p auch in $\mathbb{Q}(\zeta_8)$ voll zerlegt wäre.

Ist $p \equiv -1$ oder 7 modulo 16, so hat die Trägheitsgruppe T_p Ordnung 2. Da $\mathbb{Q}(\sqrt{2})$ in allen Zwischenkörpern L von $\mathbb{Q}(\zeta_{16})/\mathbb{Q}$ mit $[\mathbb{Q}(\zeta_{16}) : L] = 2$ enthalten ist, folgt, dass p in $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ voll zerlegt ist.

Zusammenfassend haben wir folgendes herausgefunden:
p träge in $\mathbb{Q}(\sqrt{2}) \Leftrightarrow p \equiv \pm 3, \pm 5 \pmod{16}$
p zerlegt in $\mathbb{Q}(\sqrt{2}) \Leftrightarrow p \equiv \pm 1, \pm 7 \pmod{16}$ Im ersten Fall gilt $p^2 \equiv -7 \pmod{16}$ und im zweiten Fall $p^2 \equiv 1 \pmod{16}$. Außerdem gilt im ersten Fall $\left(\frac{2}{p}\right) = -1$ und im zweiten Fall $\left(\frac{2}{p}\right) = 1$. Daraus folgt das Endresultat:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

□

1.6. **Fermats letzter Satz.** Es gibt viele Tripel (a, b, c) natürlicher Zahlen, für die $a^2 + b^2 = c^2$ gilt, z.B. $(a, b, c) = (3, 4, 5)$. Allerdings hat die Gleichung $a^n + b^n = c^n$ für $n > 2$ keine nichttriviale ganzzahlige Lösung. Nichttrivial bedeutet hier, dass keine der Zahlen a, b, c gleich Null ist. Dies war lange Zeit eine Vermutung, die von Fermat Fermat im Jahr 1637 aufgestellt wurde. Fermat selbst hat der Überlieferung nach behauptet, einen Beweis gefunden zu haben, hat ihn allerdings nicht aufgeschrieben. Man vermutet, dass Fermats Beweisidee der Strategie von Kummer folgte. Diese besteht darin, die Gleichung $a^n + b^n = c^n$ in $\mathbb{Q}(\zeta_n)$ folgendermaßen umzuschreiben:

$$b^n = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (c - \zeta_n^k a)$$

und dann die Primfaktorzerlegung in $\mathcal{O}_{\mathbb{Q}(\zeta_n)} = \mathbb{Z}[\zeta_n]$ beider Seiten zu untersuchen, m einen Widerspruch zu produzieren. Allerdings funktioniert die Strategie mit elementaren Mitteln nur, wenn in der Primfaktorzerlegung nur Hauptideale auftauchen. Leider ist die Klassenzahl nicht für alle Kreisteilungskörper $\mathbb{Q}(\zeta_n)$ gleich 1. Vermutlich ist das der Punkt, den Fermat übersehen hat. Man glaubt nämlich nicht, dass Fermat mit den Mitteln seiner Zeit in der Lage war, einen korrekten Beweis zu liefern. Tatsächlich wurde die Vermutung erst im Jahr 1994 durch Andrew Wiles bewiesen. Sein Beweis beruht auf tiefgründigen Erkenntnissen über Verbindungen von elliptischen Kurven zu Modulformen. In den Übungen werden wir einen Teil von Kummers Beweis nachvollziehen. Dazu macht man sich zunächst klar, dass es reicht, den Satz für $n = p$ eine Primzahl zu zeigen. In den Übungen werden wir einen Teil von Kummers Beweis nachvollziehen. Dazu macht man sich zunächst klar, dass es reicht, den Satz für $n = p$ eine Primzahl zu zeigen. Das heißt für eine Primzahl $p \neq 2$ wollen wir zeigen, dass es keine nichttrivialen ganzzahligen Lösungen $(a, b, c) \in \mathbb{Z}^3$ der Gleichung

$$a^p + b^p = c^p$$

gibt. Um einen elementaren Beweis führen zu können, reicht es anzunehmen, dass p nicht die Klassenzahl von $\mathbb{Q}(\zeta_p)$ teilt. Solche Primzahlen heißen *regulär*. In den Übungen wird der einfachste Fall behandelt:

Satz 1.20. *Sei $p \neq 2$ eine reguläre Primzahl. Dann gibt es keine nichttriviale ganzzahlige Lösung (a, b, c) der Gleichung*

$$a^p + b^p = c^p$$

so dass $p \nmid abc$.

Beweis. Übungen. □

Es ist nicht völlig außer Reichweite zu zeigen, dass $a^p + b^p = c^p$ keine nichttrivialen ganzzahligen Lösungen besitzt, auch ohne die Bedingung $p \nmid abc$. Allerdings braucht man dafür p-adische L-Funktionen.

2. Lokalisierung

2.1. Das Konzept der Lokalisierung.

Definition 2.1. Sei A ein Ring. Eine Teilmenge $S \subseteq A$ heißt multiplikativ, falls

(i) $1 \in S$,
(ii) aus $s, t \in S$ folgt $st \in S$.

Beispiel 2.2. (i) Für ein Element f eines Rings A ist

$$S_f := \{f^n \mid n \in \mathbb{N} \cup \{0\}\}$$

eine multiplikative Teilmenge.

(ii) Für ein Primideal $\mathfrak{p} \subset A$ ist

$$S_{(\mathfrak{p})} := \{s \in A \mid s \notin \mathfrak{p}\}$$

multiplikativ.

Die Idee von Lokalisierung besteht darin, alle Elemente einer multiplikativen Teilmenge eines Rings zu invertieren. Die Lokalisierung $S^{-1}A$ sollte grob gesprochen aus allen Brüchen $\frac{a}{s}$ für $a \in A$ und $s \in S$ bestehen.

Formal wird die Lokalisierung über eine universelle Eigenschaft definiert:

Definition 2.3. Sei A ein Ring und $S \subseteq A$ eine multiplikative Teilmenge. Die Lokalisierung von A in S ist ein Ringhomomorphismus

$$\iota : A \to S^{-1}A,$$

so dass $\iota(s)$ für alle $s \in S$ invertierbar ist und es für jeden Ringhomomorphismus $\varphi : A \to B$ mit $\varphi(s)$ invertierbar für alle $s \in S$ eine eindeutige Faktorisierung

$$A \xrightarrow{\iota} S^{-1}A \overset{\varphi}{\longrightarrow} B$$

gibt.

Wie bei allen universellen Eigenschaften ist die Lokalisierung eindeutig bis auf eindeutigen Isomorphismus, wenn sie denn existiert.

Proposition 2.4. *Sei A ein Ring und $S \subseteq A$ eine multiplikative Teilmenge. Dann existiert die Lokalisierung $A \to S^{-1}A$.*

Beweis. Auf $S \times A$ definieren wir folgende Äquivalenzrelation:

$$(s_1, a_1) \sim (s_2, a_2) \Leftrightarrow \exists\, t \in S : t(s_1 a_2 - s_2 a_1) = 0$$

(Das Element $t \in S$ wird nur gebraucht für den Fall, dass S Nullteiler von A enthält.) Dann ist $(S \times A)/\sim$ ein Ring, wenn man folgende Operationen für $(s_1, a_1), (s_2, a_2) \in S \times A$ definiert:

$$(s_1, a_1) + (s_2, a_2) := (s_1 s_2, a_1 s_2 + a_2 s_1)$$

$$(s_1, a_1) \cdot (s_2, a_2) := (s_1 s_2, a_1 a_2)$$

mit neutralem Element der Addition $(1, 0)$ und neutralem Element der Multiplikation $(1, 1)$.

Wir benutzen für die Äquivalenzklasse von (s, a) die Notation $\frac{a}{s}$. Dann ist die oben definierte Addition und Multiplikation gerade den Rechenregeln für Brüche nachempfunden.

Wir definieren den Ringhomomorphismus

$$\iota : A \to S^{-1}A$$

$$a \mapsto \frac{a}{1}.$$

Dann erfüllt ι die universelle Eigenschaft: Für $\varphi : A \to B$, so dass $\varphi(s)$ für alle $s \in S$ eine Einheit ist, ist die gesuchte Faktorisierung

$$A \xrightarrow{\iota} S^{-1}A \xrightarrow{\overline{\varphi}} B, \qquad A \xrightarrow{\varphi} B$$

durch

$$\overline{\varphi} : S^{-1}A \to B, \frac{a}{s} \mapsto \varphi(a)\varphi(s)^{-1}$$

gegeben. □

Proposition 2.5. *Sei A ein Ring und $S \subseteq A$ eine multiplikative Teilmenge. Wir betrachten die Lokalisierung $\iota : A \to S^{-1}A$. Dann haben wir folgende zueinander inverse Bijektionen*

$$\{\text{Ideale } I \subseteq A \text{ mit } I \cap S = \varnothing\} \overset{\sim}{\leftrightarrow} \{\text{echte Ideale von } S^{-1}A\}$$

$$I \mapsto S^{-1}I := \left\{ \frac{a}{s} \mid a \in I, s \in S \right\}$$

$$\iota^{-1}(J) \mapsfrom J$$

Eingeschränkt auf Primideale erhalten wir eine Bijektion

$$\{\text{Primideale } \mathfrak{p} \subset A \text{ mit } \mathfrak{p} \cap S = \varnothing\} \simeq \{\text{Primideale von } S^{-1}A\}$$

Beweis. Wir müssen zeigen:

(i) $S^{-1}I \neq S^{-1}A$
(ii) $S^{-1}\mathfrak{p}$ ist ein Primideal für $\mathfrak{p} \subset A$ prim.
(iii) $\iota^{-1}(J) \cap S = \varnothing$
(iv) $S^{-1}(\iota^{-1}(J)) = J$
(v) $\iota^{-1}(S^{-1}I) = I$

(i) Wir müssen zeigen dass $1 \notin S^{-1}I$. Falls $1 \in S^{-1}I$, würde es $a \in I$ und $s \in S$ geben mit
$$1 = \frac{1}{1} = \frac{a}{s}$$
Dann gibt es $t \in S$ mit $t(a-s) = 0$. Da $a \in I$ folgt daraus $ts \in I$, also $ts \in I \cap S$, was im Widerspruch zu $I \cap S = \varnothing$ steht.

(ii) Angenommen $\frac{a}{s} \cdot \frac{b}{t} \in S^{-1}\mathfrak{p}$. Das bedeutet, dass es ein $c \in \mathfrak{p}$ und $r \in S$ gibt mit $\frac{ab}{st} = \frac{c}{r}$. Nach Definition der Äquivalenzrelation heißt das, dass es $v \in S$ gibt mit
$$v(abr - cst) = 0$$
Da $c \in \mathfrak{p}$, folgt $vcst \in \mathfrak{p}$, also auch $vabr \in p$. Da $\mathfrak{p}$ prim ist, ist einer der Faktoren v, a, b, r in $\mathfrak{p}$ enthalten. Nach Annahme gilt $\mathfrak{p} \cap S = \varnothing$, also liegen v und r nicht in $\mathfrak{p}$. Also gilt entweder $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Das wiederum impliziert $\frac{a}{s} \in S^{-1}\mathfrak{p}$ oder $\frac{b}{s} \in S^{-1}\mathfrak{p}$.

(iii) Sei $a \in \iota$. Dann ist $\iota(a) = \frac{a}{1} \in J$. Wäre nun auch a auch in S enthalten, so hätte $\frac{a}{1}$ das Inverse $\frac{1}{a}$ und es würde gelten $\frac{a}{1} \cdot \frac{1}{a} = \frac{a}{a} = \frac{1}{1} \in J$. Aber ein echtes Ideal enthält nie die 1.

(iv)
$$S^{-1}(\iota^{-1}(P)) = \left\{ \frac{a}{s} \mid s \in S, \frac{a}{1} \in P \right\}$$
Das ist offensichtlich in P enthalten. Aber für $\frac{a}{s} \in P$ gilt $\frac{a}{s} = \frac{a}{1} \cdot \frac{1}{s}$. Einer der beiden Faktoren muss in P enthalten sein. Aber $\frac{1}{s}$ ist eine Einheit, folglich nicht in P. Daraus schließen wir, dass $\frac{a}{1} \in P$. Also gilt auch die umgekehrte Inklusion.

(v) Es gilt
$$\begin{aligned} \iota^{-1}(S^{-1}\mathfrak{p}) &= \left\{ a \in A \mid \exists b \in \mathfrak{p}, s \in S : \frac{a}{1} = \frac{b}{s} \right\} \\ &= \{ a \in A \mid \exists b \in \mathfrak{p}, s, t \in S : t(as - b) = 0 \}. \end{aligned}$$
Das ist wegen $\mathfrak{p} \cap S = \varnothing$ in $\mathfrak{p}$ enthalten. Für jedes $a \in \mathfrak{p}$ wiederum erhalten wir $t(as - b) = 0$ für $t = s = 1$ und $b = a$.

□

Korollar 2.6. *Für ein Primideal $\mathfrak{p}$ in einem Ring A ist*
$$A_{\mathfrak{p}} := S_{(\mathfrak{p})}^{-1} A$$
(für $S_{(\mathfrak{p})} = A \setminus \mathfrak{p}$) ein lokaler Ring mit Maximalideal $S_{(\mathfrak{p})}^{-1}\mathfrak{p}$.

Beweis. Nach Proposition 2.5 entsprechen die Primideale von $A_{\mathfrak{p}}$ den Primidealen $\mathfrak{q}$ von A, so dass
$$\mathfrak{q} \cap (A \setminus \mathfrak{p}) = \varnothing$$
gilt. Das ist äquivalent zu $\mathfrak{q} \subseteq \mathfrak{p}$. □

Korollar 2.7. *Sei A ein Ring und S eine multiplikative Teilmenge.*

(i) Ist A noethersch, so auch $S^{-1}A$.

(ii) Ist $\mathfrak{p} \subset A$ maximal, so auch $S^{-1}\mathfrak{p}$.

Beweis. (i) Wir müssen zeigen, dass jede aufsteigende Kette
$$J_1 \subseteq J_2 \subseteq J_3 \subseteq \dots$$

von Idealen in $S^{-1}A$ stationär wird. Nach Proposition 2.5 ist diese Idealkette von der Form

$$S^{-1}I_1 \subseteq S^{-1}I_2 \subseteq S^{-1}I_3 \subseteq \dots$$

für eine Idealkette

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$$

in A. Diese wird stationär, da A noethersch ist.

(ii) Angenommen $S^{-1}\mathfrak{p}$ ist einem echten Ideal $\mathcal{M}$ enthalten, dann gibt es ein Ideal $m \subset A$ mit $m \cap S = \varnothing$ und $\mathcal{M} = S^{-1}m$. Es muss gelten $\mathfrak{p} \subseteq m$. Da $\mathfrak{p}$ maximal ist, folgt $\mathfrak{p} = m$ also $S^{-1}\mathfrak{p} = \mathcal{M}$.

□

2.2. **Diskrete Bewertungsringe.** Im nächsten Abschnitt werden wir uns mit Lokalisierung in Dedekindringen beschäftigen. Insbesondere wollen für einen Dedekindring A und ein Primideal $\mathfrak{p} \neq (0)$ die Lokalisierung $A_\mathfrak{p}$ untersuchen. Es wird sich herausstellen, dass $A_\mathfrak{p}$ ein diskreter Bewertungsring ist. Zur Vorbereitung wollen wir diese Klasse von Ringen untersuchen.

Definition 2.8. Ein diskreter Bewertungsrings ist ein lokaler Hauptidealring, der kein Körper ist.

In einem diskreten Bewertungsrings gibt es genau zwei Primideale, nämlich das Maximalideal und (0). Das liegt daran, dass A als Hauptidealring ein Dedekindring ist, also jedes Primideal ungleich (0) maximal ist. Da A außerdem lokal ist, gibt es nur ein Maximalideal und dies ist ungleich (0), da A kein Körper ist. Es drängt sich die Frage auf, woher die Bezeichnung „diskreter Bewertungsring“ kommt. Das wollen wir nun erklären. Das Maximalideal $\mathfrak{p}$ von A ist ein Hauptideal. Wir wählen einen Erzeuger $\pi \in \mathfrak{p}$.

Definition 2.9. Ein Erzeuger des Maximalideals eines diskreten Bewertungsrings heißt *Uniformisierende*.

Da A ein Dedekindring ist, hat jedes gebrochene Ideal ungleich (0) eine eindeutige Primfaktorzerlergung. Das einzige Primideal ungleich Null ist aber (π) für eine Uniformisierende π. Daher gilt für jedes Element $a \in K(A)^\times$ eine Gleichung der Form

$$(a) = (\pi)^{n_a}$$

mit einer eindeutig bestimmten ganzen Zahl n. Für $a = 0$ setzten wir $n_a = \infty$. Wir betrachten folgende Funktion

$$v : K(A) \to \mathbb{Z} \cup \{\infty\}$$

$$a \mapsto n_a$$

Wir werden gleich sehen, dass v die Axiome für eine diskrete Bewertung erfüllt.

Definition 2.10. Eine *diskrete Bewertung* auf einem Körper K ist eine Abbildung $v : K \to \mathbb{Z} \cup \{\infty\}$ mit folgenden Eigenschaften für $a, b \in K$:

(i) $v(a) = \infty \Leftrightarrow a = 0$
(ii) $v(ab) = v(a) + v(b)$
(iii) $v(a + b) \geq \min(v(a), v(b))$

Die Bewertung heißt trivial, wenn $v(a) = 0$ für alle $a \in K^\times$.

Die Bezeichnung „diskret“ bezieht sich auf die Tatsache, dass die Wertegruppe $\mathbb{Z}$ diskret ist. Im Laufe der Vorlesung werden wir allgemeinere Bewertungen kennen lernen, die nicht diskret sind.

Lemma 2.11. *Für einen diskreten Bewertungsring A ist die oben definierte Abbildung $v : K(A) \to \mathbb{Z} \cup \{\infty\}$ eine nichttriviale diskrete Bewertung.*

Beweis. (i) Nach Konstruktion ist $v(a)$ genau dann gleich ∞, wenn $a = 0$ ist.

(ii) Für $a, b \in K(A)^\times$ ist $(a) = (\pi)^{v(a)}$ und $(b) = (\pi)^{v(b)}$. Daraus erhalten wir

$$(ab) = (a) \cdot (b) = (\pi)^{v(a)} \cdot (\pi)^{v(b)} = (\pi)^{v(a)+v(b)}$$

Ist eines der beiden Elemente a oder b gleich Null, ist sowohl $v(ab)$ als auch $v(a)+v(b)$ gleich ∞. Daher gilt die Gleichung auch in diesem Fall.

(iii) Auch hier ist die Aussage offensichtlich richtig, falls a oder b oder beide gleich Null sind. Für $a, b \in K(A)^\times$ folgern wir aus $(a) = (\pi)^{v(a)}$ und $(b) = (\pi)^{v(b)}$ die Existenz von Einheiten $u_a, u_b \in A^\times$, so dass $a = u_a\pi^{v(a)}$ und $b = u_b\pi^{v(b)}$ gilt. Ohne Beschränkung der Allgemeinheit nehmen wir an, dass $v(b) \geq v(a)$ ist. Dann schreiben wir

$$a + b = u_a\pi^{v(a)} + u_b\pi^{v(b)} = \pi^{v(a)}(u_a + u_b\pi^{v(b)-v(a)})$$

Da $v(b) \geq v(a)$ ist, ist

$$u_a + u_b\pi^{v(b)-v(a)} \in A$$

Nach Konstruktion haben alle Elemente von A nichtnegative Bewertung. Daher gilt mit (ii):

$$\begin{aligned} v(a + b) &= v(\pi^{v(a)}) + v(u_a + u_b\pi^{v(b)-v(a)}) \\ &\geq v(\pi^{v(a)}) \\ &= v(a) \\ &= \min\{v(a), v(b)\} \end{aligned}$$

Die Bewertung ist offensichtlich nichttrivial. Beispielsweise gilt $v(\pi) = 1 \neq 0$. □

Andererseits können wir jeder nichttrivialen diskreten Bewertung einen diskreten Bewertungsring zuordnen.

Lemma 2.12. *Sei K ein Körper und*

$$v : K \to \mathbb{Z} \cup \{\infty\}$$

eine nichttriviale diskrete Bewertung. Dann ist $\mathcal{O}_v := \{a \in K \mid v(a) \geq 0\}$ ein diskreter Bewertungsring mit Maximalideal $m_v := \{a \in K \mid v(a) > 0\}$.

Beweis. Zuallererst müssen wir uns davon überzeugen, dass $\mathcal{O}_v$ ein Ring ist, also abgeschlossen unter Addition und Multiplikation. Außerdem muss O_v die Elemente 0 und 1 enthalten und mit a sein Negatives $-a$. Es gilt nach Axiom (i)

$$v(0) = \infty \geq 0$$

Also ist 0 in $\mathcal{O}_v$ enthalten. Aus (ii) folgt

$$v(1) = v(1 \cdot 1) = v(1) + v(1).$$

Da $v(1)$ nach (i) nicht ∞ ist, folgt daraus $v(1) = 0$, also $1 \in \mathcal{O}_v$. Für $a, b \in \mathcal{O}_v$ ist $v(ab) = v(a) + v(b) \geq 0$. Also $ab \in O_v$. Nach (iii) gilt

$$v(a+b) \geq \min\{v(a), v(b)\} \geq 0$$

Daher ist auch $a + b \in \mathcal{O}_v$. Um zu sehen dass $-a \in \mathcal{O}_v$ liegt, berechnen wir mithilfe von (ii)

$$2v(-a) = v((-a)^2) = v(a^2) \geq 0.$$

Daraus folgt $v(-a) \geq 0$, also $-a \in \mathcal{O}_v$.

Wir behaupten nun, dass $\mathcal{O}_v$ lokal ist mit Maximalideal

$$m_v := \{a \in K \mid v(a) > 0\}.$$

Dass m_v ein Ideal von $\mathcal{O}_v$ ist, rechnet man in derselben Weise nach wie die Behauptung, dass $\mathcal{O}_v$ ein Ring ist. Um zu zeigen, dass $\mathcal{O}_v$ lokal ist mit Maximalideal m_v, müssen wir uns nur davon überzeugen, dass

$$O_v \setminus m_v = \mathcal{O}_v^\times,$$

oder mit anderen Worten

$$O_v^\times = \{a \in K \mid v(a) = 0\}.$$

Ist $v(a) = 0$, so ist $a \neq 0$ und $\frac{1}{a}$ ein wohldefiniertes Element von K. Es gilt

$$0 = v(1) = v\left(a \cdot \frac{1}{a}\right) = v(a) + v\left(\frac{1}{a}\right).$$

Also ist $v(a) = v(\frac{1}{a}) = 0$, daher ist $\frac{1}{a}$ in $\mathcal{O}_v^\times$ enthalten.

Ist $u \in \mathcal{O}_v^\times$ mit Inversen $u^{-1} \in \mathcal{O}_v^\times$, so gilt

$$0 = v(1) = v(u \cdot u^{-1}) = v(u) + v(u^{-1})$$

Da $v(u) \geq 0$ und $v(u^{-1}) \geq 0$, folgt daraus $v(u) = v(u^{-1}) = 0$. Damit ist die Behauptung bewiesen. Da die Bewertung nichttrivial ist, ist $m_v \neq (0)$ und $\mathcal{O}_v$ ist kein Körper.

Es verbleibt noch zu zeigen, dass $\mathcal{O}_v$ ein Hauptidealring ist. Dafür betrachten wir ein Ideal $\mathfrak{a} \subseteq \mathcal{O}_v$. Alle Elemente von $\mathfrak{a}$ haben eine nichtnegative Bewertung. Es gibt folglich ein Element $a \in \mathfrak{a}$ mit minimaler Bewertung. Ist $a = 0$, also $v(a) = \infty$, folgt $\mathfrak{a} = (0)$. Angenommen $a \neq 0$. Es gilt zu zeigen, dass $\mathfrak{a} \subseteq (a)$. Sei dazu $b \in \mathfrak{a} \setminus (a)$. Da a minimale Bewertung hat, ist $v(b) = v(a) + r$ für ein $r \in \mathbb{Z}$. Sei $x \in \mathcal{O}_v$ ein Element mit $v(x) = r$. Dann ist $v(b) = v(ax)$. Es muss ein $u \in \mathcal{O}_v$ geben, so dass $b = axu$. Das ist ein Widerspruch dazu, dass $b \notin (a)$. □

2.3. **Lokalisierung in einem Dedekindring.**

Proposition 2.13. *Sei A ein Dedekindring und $S \subseteq A$ eine multiplikative Teilmenge. Dann ist auch $S^{-1}A$ ein Dedekindring.*

Beweis. Nach Korollar 2.7 ist $S^{-1}A$ Noethersch und jedes Primideal $\mathfrak{p} \neq (0)$ in $S^{-1}A$ ist maximal. Wir müssen noch zeigen, dass $S^{-1}A$ ganzabgeschlossen ist. Zuerst stellen wir fest, dass

$$K(A) = K(S^{-1}A) = (A \setminus \{0\})^{-1}A.$$

Wir betrachten ein Element $x \in K(A)$, das Nullstelle eines normierten Polynoms

$$P(X) = X^n + \frac{a_{n-1}}{s_{n-1}}X^{n-1} + \ldots + \frac{a_1}{s_1}X + \frac{a_0}{s_0}$$

in $S^{-1}A[X]$ ist. Wir können durch Erweiterung der Brüche erreichen, dass $s := s_{n-1} = s_{n-2} = \ldots = s_1 = s_0$, also

$$P(X) = X^n + \frac{a_{n-1}}{s} + \ldots + \frac{a_1}{s}X + \frac{a_0}{s}.$$

Dann ist sx Nullstelle des normierten Polynoms

$$Q(X) = X^n + a_{n-1}X^{n-1} + a_{n-2}sX^{n-2} + \ldots + a_1 s^{n-2}X + a_0 s^{n-1}$$

in $A[X]$. Da A ganzabgeschlossen ist, folgt $sx \in A$, also $x = \frac{sx}{s} \in S^{-1}A$. □

Satz 2.14. *Ein noetherscher nullteilerfreier Ring A ist genau dann ein Dedekindring, wenn für jedes Primideal $\mathfrak{p} \neq (0)$ die Lokalisierung ein diskreter Bewertungsring ist.*

Beweis. Wir nehmen an, dass A ein Dedekindring ist, und wollen für ein Primideal $\mathfrak{p} \neq (0)$ zeigen, dass $A_\mathfrak{p}$ ein diskreter Bewertungsring ist.

Nach 2.13 ist $A_\mathfrak{p}$ als Lokalisierung von A wieder ein Dedekindring. Gemäß der Beschreibung der Primideale einer Lokalisierung (2.5) hat $A_\mathfrak{p}$ genau zwei Primideale (0) und $\mathfrak{p}A_\mathfrak{p}$. Um einzusehen, dass $A_\mathfrak{p}$ ein diskreter Bewertungsring ist, müssen wir uns noch davon überzeugen, dass $A_\mathfrak{p}$ ein Hauptidealring ist. Alle nichttrivialen Ideale von $A_\mathfrak{p}$ sind nach Existenz der Primfaktorzerlegung von der Form $(\mathfrak{p}A_\mathfrak{p})^n$ für $n \geq 0$. Außerdem impliziert die Eindeutigkeit der Primfaktorzerlegung, dass

$$(\mathfrak{p}A_\mathfrak{p})^n \subsetneq (\mathfrak{p}A_\mathfrak{p})^{n+1}.$$

Daher können wir ein Element

$$a \in (\mathfrak{p}A_\mathfrak{p})^n \setminus (\mathfrak{p}A_\mathfrak{p})^{n+1}$$

wählen. Dann gilt $(a) = (\mathfrak{p}A_\mathfrak{p})^n$ und somit ist $(\mathfrak{p}A_\mathfrak{p})^n$ ein Hauptideal.

Somit haben wir geszeigt, dass $A_\mathfrak{p}$ ein lokaler Hauptidealring ist, aber kein Körper (da (0) nicht maximal ist). □

Für die Rückrichtung brauchen wir folgendes Lemma.

Lemma 2.15. *Sei A ein nullteilerfreier Ring. Dann gilt*

$$A = \bigcap_{\substack{\mathfrak{m} \subseteq A \\ \text{maximal}}} A_\mathfrak{m},$$

wobei der Durchschnitt im Quotientenkörper $K(A)$ gebildet wird.

Beweis. Da A nullteilerfrei ist, ist der kanonische Homomorphismus $A \to A_\mathfrak{m}$ für alle Maximalideale $\mathfrak{m}$ injektiv. Tatsächlich kann A und $A_\mathfrak{m}$ als Teilringe von $K(A)$ auffassen. Es gilt offensichtlich

$$A \subseteq \bigcap_{\mathfrak{m} \subseteq A} A_\mathfrak{m}.$$

Für die umgekehrte Inklusion betrachten wir ein Element $x \in \bigcap_{\mathfrak{m} \subseteq A} A_\mathfrak{m}$ und wollen zeigen, dass x in A enthalten ist. Als Element des Quotientenkörpers $K(A)$ kann man x in der Form $x = \frac{a}{b}$ für $a, b \in A$ und $b \neq 0$ schreiben. Wir wollen zeigen, dass das Ideal

$$I = \{y \in A \mid ya \in (b)\} \subseteq A$$

das Einsideal ist. Dann gilt nämlich $1 \in I$ und somit $a = 1 \cdot a \in (b)$, was wiederum bedeutet, dass $c \in A$ existiert mit $a = cb$, also $\frac{a}{b} = \frac{cb}{b} = c \in A$. Wäre $I \neq A$, so gäbe es

ein Maximalideal $\mathfrak{m}$, das I enthält. Da nach Annahme $x = \frac{a}{b} \in A_{\mathfrak{m}}$, gibt es $c, d \in A$ mit $d \notin \mathfrak{m}$, so dass

$$x = \frac{a}{b} = \frac{c}{d}.$$

Daraus folgt

$$ad = bc \in (b),$$

also $d \in I \subseteq \mathfrak{m}$. Das steht im Widerspruch zur Annahme $d \notin \mathfrak{m}$. □

Fortsetzung des Beweises von Satz 2.14. Wir nehmen an, dass alle lokalen Ringe $A_{\mathfrak{p}}$ für $\mathfrak{p} \neq (0)$ diskrete Bewertungsringe sind. Wir müssen zeigen:

(i) A ist ganzabgeschlossen.
(ii) jedes Primideal $\mathfrak{p} \neq (0)$ von A ist maximal.

(ii). Wäre $\mathfrak{p}$ nicht maximal, so gäbe es ein Primideal $\mathfrak{q}$ mit

$$(0) \subsetneqq \mathfrak{p} \subsetneqq \mathfrak{q}$$

In $A_{\mathfrak{q}}$ gilt dann aber

$$(0) \subsetneqq \mathfrak{p}A_{\mathfrak{q}} \subsetneqq \mathfrak{q}A_{\mathfrak{q}}$$

nach Proposition 2.5. Allerdings hat $A_{\mathfrak{q}}$ als diskreter Bewertungsring nur zwei verschiedene Primideale. (i) Sei $a \in K(A)$ ganz über A, dann ist a auch ganz über dem größeren Ring $A_{\mathfrak{p}}$ für $\mathfrak{p} \neq (0)$. Als diskreter Bewertungsring ist $A_{\mathfrak{p}}$ ein Hauptidealring, also ganzabgeschlossen. Daher gilt nach Lemma 2.15

$$a \in \bigcap_{\mathfrak{p} \neq (0)} A_{\mathfrak{p}} = A$$

Damit ist der Beweis vollbracht. □

Sei A ein Dedekindring und $\mathfrak{p} \neq (0)$ eine Primideal. Da $A_{\mathfrak{p}}$ ein diskreter Bewertungsring ist, erhalten wir nach Lemma 2.11 eine diskrete Bewertung

$$v_{\mathfrak{p}} : K(A) \to \mathbb{Z} \cup \{\infty\}$$

auf dem Quotientenkörper von A. Wir nennen diese die $\mathfrak{p}$-*adische Bewertung.*

3. Bewertungstheorie

3.1. **Bewertungen.** Sei K ein Körper wir haben in Abschnitt 2.2 diskrete Bewertungen als Abbildungen

$$v : K \to \mathbb{Z} \cup \{\infty\}$$

mit den Eigenschaften

(i) $a = 0 \Leftrightarrow v(a) = \infty$
(ii) $v(ab) = v(a) + v(b)$
(iii) $v(a + b) \geq \min\{v(a), v(b)\}$

kennen gelernt. In diesem Abschnitt werden wir Bewertungen im Allgemeinen einführen. Zuerst wollen wir im Falle diskreter Bewertungen von der additiv geschriebenen Gruppe $\mathbb{Z}$ zu einer multiplikativen Gruppe übergehen. Dazu wählen wir eine reelle Zahl λ mit $0 < \lambda < 1$. Wir betrachten den Gruppenhomomorphismus

$$\mathbb{Z} \to \mathbb{R}_{>0}, m \mapsto \lambda^m.$$

Da $\lambda < 1$ ist, dreht er die Ordnung um, das heißt für $m, n \in \mathbb{Z}$ gilt

$$m < n \Leftrightarrow \lambda^m > \lambda^n.$$

Außerdem setzen wir ihn fort zu

$$\mathbb{Z} \cup \{\infty\} \to \mathbb{R}_{\geq 0},$$

indem wir ∞ auf 0 abbilden. Die Verkettung

$$|\cdot| : K \xrightarrow{v} \to \mathbb{Z} \cup \{\infty\} \to \mathbb{R}_{\geq 0}$$

ist dann eine Abbildung mit folgenden Eigenschaften:

(i) $|a| = 0 \Leftrightarrow a = 0$
(ii) $|ab| = |a| \cdot |b|$
(iii) $|a + b| \leq \max\{|a|, |b|\}$.

Beispiel 3.1. Im Falle der p-adischen Bewertung auf $\mathbb{Q}$ wählt man meistens $\lambda = \frac{1}{p}$. Die zugehörige multiplikative Bewertung bezeichnet man mit $|\cdot|_p$. Es gilt beispielsweise $|p^n|_p = \frac{1}{p^n}$.

Um auch den reellen und den komplexen Absolutbetrag mit einzuschließen, müssen wir die Bedingung (iii) etwas abschwächen.

Definition 3.2. Eine *reellwertige Bewertung* (oder reelle Bewertung) auf einem Körper K ist eine Abbildung

$$|\cdot| : K \to \mathbb{R}_{\geq 0}$$

mit den Eigenschaften

(i) $a = 0 \Leftrightarrow |a| = 0$
(ii) $|ab| = |a| \cdot |b|$ (Multiplikativität)
(iii) $|a + b| \leq |a| + |b|$ (Dreiecksungleichung)

Beispiel 3.3. (i) Jede diskrete Bewertung oder genauer gesagt die zugehörige multiplikative Bewertung ist eine reelle Bewertung.
(ii) Der Standardabsolutbetrag

$$|\cdot| : \mathbb{Q} \to \mathbb{R}_{\geq 0}$$
$$x \mapsto \begin{cases} x, & \text{falls } x \geq 0 \\ -x, & \text{falls } x < 0 \end{cases}$$

ist eine reelle Bewertung.
(iii) Der Betrag

$$|\cdot| : \mathbb{C} \to \mathbb{R}_{\geq 0}$$
$$x + iy \mapsto \sqrt{x^2 + y^2}$$

ist eine reelle Bewertung.

Definition 3.4. Eine reelle Bewertung heißt *archimedisch*, falls es für jedes $x \in K$ eine natürliche Zahl n gibt mit

$$|x| < |n|.$$

Ansonsten heißt sie nicht-archimedisch.

Beispiel 3.5. Der reelle und der komplexe Absolutbetrag sind archimedisch. Die p-adische Bewertung auf $\mathbb{Q}$ ist nichtarchimedisch, da für alle $n \in N$ gilt $|n| \leq 1$.

Lemma 3.6. *Eine reelle Bewertung $|\cdot| : K \to \mathbb{R}_{\geq 0}$ ist genau dann nichtarchimedisch, wenn für alle $a, b \in K$ gilt*

$$|a + b| \leq \max\{|a|, |b|\}.$$

Man nennt die Ungleichung

$$|a + b| \leq \max\{|a|, |b|\}$$

die starke Dreiecksungleichung.

Beweis. Gilt für alle Elemente die starke Dreiecksungleichung, so erhalten wir insbesondere für $n \in \mathbb{N}$:

$$|1 + \ldots + 1| \leq \max\{|1|, \ldots, |1|\} = |1| = 1.$$

Wir nehmen nun an, die Bewertung ist nichtarchimedisch. Das heißt es gibt $c \in K$, so dass $|c| \geq |n|$ für alle natürlichen Zahlen. Für $x \in K$ mit $|x| \geq 1$ gilt dann

$$|1 + x|^n = |(1 + x)^n| = \left|\sum_{i=0}^{n} \binom{n}{i} x^i\right| \leq \sum_{i=0}^{n} \left|\binom{n}{i}\right| |x|^i.$$

Da $\binom{n}{i}$ eine natürliche Zahl ist, gilt $|\binom{n}{i}| \leq |c|$ und somit

$$|1 + x|^n \leq (n + 1) \cdot |c| \cdot |x|^i \leq (n + 1)|c|.$$

Daraus folgt

$$|1 + x| \leq \sqrt[n]{(n + 1)|c|}.$$

Im Limes $n \to \infty$ erhalten wir

$$|1 + x| \leq 1.$$

Um daraus die starke Dreiecksungleichung zu folgern betrachten wir $a, b \in K$ und nehmen ohne Beschränkung der Allgemeinheit an, dass $|a| \leq |b| \neq 0$. Dann können wir obiges Argument auf $x = \frac{a}{b}$ anwenden:

$$|a + b| = |b| \cdot \left|1 + \frac{a}{b}\right| \leq |b| = \max\{|a|, |b|\}.$$

□

In der Literatur taucht oft eine weitere Definition einer Bewertung auf, die allgemeinere Wertegruppen als $\mathbb{R}_{\geq 0}$ zulässt. Allerdings muss man dann direkt mit der starken Dreiecksungleichung arbeiten. Um so eine Bewertung zu definieren, müssen wir zunächst festlegen, was wir als Wertegruppe zulassen.

Definition 3.7. Eine *total geordnete abelsche Gruppe* ist eine abelsche Gruppe Γ (multiplikativ) zusammen mit einer Totalordnung „$\leq$“, so dass für $a, b, c \in \Gamma$ gilt

$$a \leq b \Rightarrow ac \leq bc$$

Erinnerung: Eine Totalordnung auf einer Menge M ist eine Relation „$\leq$“, die folgende Eigenschaften erfüllt für $a, b, c \in M$:

(i) $a \leq a$ (Reflexivität)
(ii) $a \leq b, b \leq c \Rightarrow a \leq c$ (Transitivität)
(iii) $a \leq b, b \leq a \Rightarrow a = c$ (Antisymmetrie)
(iv) $a \leq b$ oder $b \leq a$ (Totalität)

Beispiel 3.8. (i) $\mathbb{R}_{>0}$ ist eine total geordnete abelsche Gruppe.
(ii) Für jedes Element $a \in \mathbb{R}_{>0}$ ist $a^{\mathbb{Z}}$ eine total geordnete abelsche Gruppe. Allgemeiner ist jede Untergruppe von $\mathbb{R}_{>0}$ eine total geordnete abelsche Gruppe.

(iii) $\mathbb{R}_{>0} \times \mathbb{R}_{>0}$ mit der lexikografischen Ordnung ist eine total geordnete abelsche Gruppe. Die lexikografische Ordnung ist folgendermaßen definiert:

$$(a_1, b_1) \leq (a_2, b_2) \Leftrightarrow a_1 < a_2 \text{ oder } a_1 = a_2 \text{ und } b_1 \leq b_2.$$

Man kann zeigen, dass sich $\mathbb{R}_{>0} \times \mathbb{R}_{>0}$ nicht ordnungserhaltend in $\mathbb{R}_{>0}$ einbetten lässt.

Definition 3.9. Eine *Bewertung* auf einem Körper K ist eine Abbildung

$$|\cdot| : K \to \Gamma \cup \{0\}$$

für eine total geordnete abelsche Gruppe Γ, die folgenden Eigenschaften genügt:

(1) $|a| = 0 \Leftrightarrow a = 0$,
(2) $|ab| = |a| \cdot |b|$,
(3) $|a + b| \leq \max\{|a|, |b|\}$

Lemma 3.10. *Sei*

$$|\cdot| \colon K \longrightarrow \Gamma \cup \{0\}$$

eine (nichtarchimedische) Bewertung. Für Elemente $x, y \in K$ mit $|x| \neq |y|$ gilt

$$|x + y| = \max\{|x|, |y|\}$$

(und nicht nur $|x + y| \leq \max\{|x|, |y|\}$).

Beweis. Ohne Beschränkung der Allgemeinheit können wir annehmen $|x| < |y|$. Dann gilt

$$\begin{aligned} |y| &= |(y + x) - x| \\ &= \max\{|x + y|, |x|\}. \end{aligned}$$

Wäre $\max\{|x + y|, |x|\} = |x|$, so erhielten wir $|y| \leq |x|$, aber das steht im Widerspruch zur Annahme $|x| < |y|$. Also gilt

$$|y| \leq \max\{|x + y|, |x|\} = |x + y|.$$

Aus der starken Dreiecksungleichung wissen wir außerdem

$$|x + y| \leq \max\{|x|, |y|\} = |y|.$$

Insgesamt erhalten wir

$$|x + y| = |y| = \max\{|x|, |y|\}.$$

□

Definition 3.11. Zwei Bewertungen

$$|\cdot|_1 : K \to \Gamma_1 \cup \{0\},$$

$$|\cdot|_2 : K \to \Gamma_2 \cup \{0\}$$

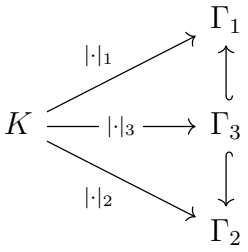
heißen äquivalent, wenn es eine Bewertung

$$|\cdot|_3 : K \to \Gamma_3 \cup \{0\}$$

und ordnungserhaltende injektive Homomorphismen

$$\Gamma_3 \hookrightarrow \Gamma_1, \Gamma_3 \hookrightarrow \Gamma_2,$$

so dass folgendes Diagramm kommutiert:



Definition 3.12. Sei K ein Körper und $v : K \to \cup\{\infty\}$ eine diskrete Bewertung wie in Definition 2.10. Für zwei reelle Zahlen λ_1, λ_2 mit $0 < \lambda_1, \lambda_2 < 1$ sind die Bewertungen

$$K \to \mathbb{R}_{\geq 0},$$

$$x \mapsto \lambda_1^{v(x)}$$

$$x \mapsto \lambda_2^{v(x)}$$

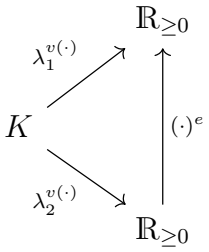
äquivalent. Um das zu sehen, definieren wir

$$e := \frac{\log \lambda_1}{\log \lambda_2},$$

Also $\lambda_1 = \lambda_2^e$ und betrachten den Isomorphismus

$$\mathbb{R}_{\geq 0} \xrightarrow{(\cdot)^e} \mathbb{R}_{\geq 0}$$

Dann kommutiert das Diagramm



und somit sind die beiden Bewertungen äquivalent.

Lemma 3.13. *Zwei reelle Bewertungen*

$$|\cdot|_1 : K \to \mathbb{R}_{\geq 0},$$

$$|\cdot|_2 : K \to \mathbb{R}_{\geq 0}$$

sind genau dann äquivalent, wenn es eine reelle Zahl $\alpha > 0$ gibt, so dass für alle $x \in K$ gilt

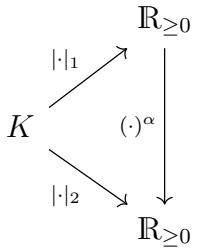
$$|x|_2 = |x|_1^{\alpha}.$$

Beweis. Angenommen es gibt $\alpha \in \mathbb{R}$, $\mathfrak{a} > 0$, das die Bedingungen erfüllt. Dann ist

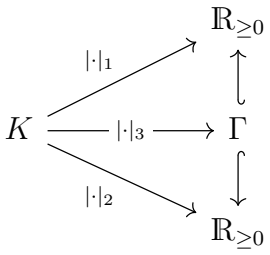
$$\mathbb{R}_{>0} \to \mathbb{R}_{>0},$$

$$r \mapsto r^{\alpha}$$

ein Isomorphismus, so dass das Diagramm



kommutiert. Nehmen wir nun an, dass ein kommutatives Diagramm



existiert. Daraus können wir folgern, dass für $x, y \in K$ gilt

$$|x|_1 \leq |y|_1 \Leftrightarrow |x|_2 \leq |y|_2$$

Das liegt daran, dass in Γ entweder $|x|_3 \leq |y|_3$ oder $|x|_3 \geq |y|_3$ gilt und weil die beiden Einbettungen $\Gamma \hookrightarrow \mathbb{R}_{>0}$ ordnungserhaltend sind, gelten die gleichen Ungleichung für $|\cdot|_1$ und $|\cdot|_2$. Ist $|\cdot|_3$ die triviale Bewertungen (die alles außer 0 auf $1 \in \Gamma$ abbildet), so sind auch $|\cdot|_1$ und $|\cdot|_2$ trivial und wir sind fertig. Ist $|\cdot|_3$ nichttrivial, gibt es $x_0 \in K$, so dass $|x_0| > 1$. Dann ist auch

$$|x_0|_1 > 1, |x_0|_2 > 1.$$

Es gibt dann eine eindeutig bestimmte reelle Zahl $\alpha > 0$, so dass

$$|x_0|_2 = |x_0|_1^\alpha$$

Für beliebiges $x \in K^\times$ finden wir zunächst $\beta \in \mathbb{R}$, so dass

$$|x|_1 = |x_0|_1^\beta$$

Ist $\beta \in \mathbb{N}$, so folgt

$$\left|\frac{x}{x_0^\beta}\right|_1 = 1$$

und somit auch $\left|\frac{x}{x_0^\beta}\right|_2 = 1$. Daraus folgt

$$|x|_2 = |x_0|_2^\beta = |x_0|_1^{\alpha\beta} = |x|_1^\alpha.$$

Ist $\beta \in \mathbb{Q}$, schreiben wir $\beta = \frac{\beta'}{\beta''}$ für $\beta', \beta'' \in \mathbb{N}$. Dann gilt

$$\left|\frac{x^{\beta''}}{x_0^{\beta'}}\right|_1 = 1,$$

also $\left|\frac{x^{\beta''}}{x_0^{\beta'}}\right|_2 = 1$ und wir können ähnlich wie zuvor argumentieren. Für $\beta \in \mathbb{R} \setminus \mathbb{Q}$ und $n \in \mathbb{N}$ bezeichnen wir mit $m_n \in \mathbb{Z}$ die ganze Zahl, so dass gilt

$$m_n < n\beta < m_n + 1$$

Daraus folgt

$$|x_0|_1^{m_n} < |x_0|_1^{n\beta} < |x_0|_1^{m_n+1}$$

Per Definition von β gilt $|x_0|_1^{n\beta} = |x|_1^n$, also

$$|x_0|_1^{m_n} < |x|_1^n < |x_0|_1^{m_n+1}$$

Da m_n und n ganze Zahlen sind, können wir das äquivalent umformen zu

$$|x_0^{m_n}|_1 < |x^n|_1 < |x_0^{m_n+1}|_1$$

Da $|\cdot|_1$ und $|\cdot|_2$ äquivalent sind, folgt

$$|x_0^{m_n}|_2 < |x^n|_2 < |x_0^{m_n+1}|_2,$$

was wir zu

$$|x_0|_2^{\frac{m_n}{n}} < |x|_2 |x_0|_2^{\frac{m_n+1}{n}}$$

umformen können. Aus $m_n < n\beta < m_n + 1$ folgt

$$\frac{m_n}{n} < \beta \frac{m_n+1}{n}$$

Da $\frac{m_n+1}{n} - \frac{m_n}{n} = \frac{1}{n}$, konvergieren sowohl $\frac{m_n}{n}$ als auch $\frac{m_n+1}{n}$ gegen β. Daraus folgt $|x|_2 = |x_0|_2^\beta$ und wir können wie zuvor argumentieren:

$$|x|_2 = |x_0|_2^\beta = |x_0|_1^{\alpha\beta} = |x|_1^\alpha.$$

□

3.2. **Bewertungsringe.**

Lemma 3.14. *Sei $|\cdot| : K \to \Gamma \cup \{0\}$ eine Bewertung auf einem Körper K. Dann ist*

$$\mathcal{O}_{|\cdot|} := \{x \in K \mid |x| \leq 1\}$$

ein lokaler Ring mit Maximalideal

$$\mathfrak{m}_{|\cdot|} := \{x \in K \mid |x| < 1\}$$

Beweis. Genauso wie für diskrete Bewertungsringe (Lemma 2.12). □

Definition 3.15. Ein Bewertungsring ist ein nullteilerfreier Ring A mit der Eigenschaft, dass für jedes Element $x \in K(A)^\times$ entweder x oder x^{-1} in A enthalten ist.

Definition 3.16. Ein nullteilerfreier Ring A ist genau dann ein Bewertungsring, wenn es eine Bewertung

$$|\cdot| : K(A) \to \Gamma \cup \{0\}$$

auf dem Quotientenkörper gibt, so dass

$$\mathcal{O}_{|\cdot|} = A.$$

Beweis. Angenommen $A = \mathcal{O}_{|\cdot|}$ für eine Bewertung $|\cdot| : K(A) \to \Gamma \cup \{0\}$. Für $x \in K(A)^\times$ gilt entweder $|x| \leq 1$ oder $|x| > 1$. Im ersten Fall ist $x \in A$ und im zweiten Fall $x^{-1} \in A$.

Wir nehmen nun an, dass A ein Bewertungsring ist. Wir definieren folgende Ordnungsrelation auf $\Gamma := K(A)^\times / A^\times$:

$$[x] \leq [y] \Leftrightarrow \frac{x}{y} \in A.$$

Das hängt nicht von der Wahl eines Repräsentanten ab: Ist $x = ux'$ und $y = vy'$ für $x, x', y, y' \in K(A)^\times$ und $u, v \in A^\times$, so ist

$$\frac{x}{y} = \frac{u}{v} \cdot \frac{x'}{y'},$$

also $\frac{x}{y} \in A$ genau dann, wenn $\frac{x'}{y'} \in A$. Jetzt müssen wir die Axiome einer Totalordnung überprüfen:

(i) $[x] \leq [x]$ ist richtig, da $1 \in A$.

(ii) Gilt $[x] \leq [y]$ und $[y] \leq [z]$, also $\frac{x}{y}, \frac{y}{z} \in A$, so folgt

$$\frac{x}{z} = \frac{x}{y} \cdot \frac{y}{z} \in A,$$

also $[x] \leq [z]$.

(iii) Gilt $[x] \leq [x]$ und $[y] \leq [x]$, also $\frac{x}{y} \in A$ und $\frac{y}{x} \in A$, so ist $u := \frac{x}{y}$ eine Einheit in A und folglich gilt

$$[x] = [uy] = [y].$$

(iv) Seien $x, y \in K(A)^\times$. Dann gilt entweder $\frac{x}{y} \in A$ oder $\frac{y}{x} \in A$. Im ersten Fall folgt daraus $[x] \leq [y]$ und im zweiten Fall $[y] \leq [x]$.

Wir behaupten nun, dass

$$|\cdot| : K(A) \to {}^{K(A)^\times}\!/_{A^\times} \cup \{0\}$$
$$x \mapsto \begin{cases} [x] & x \in K(A)^\times \\ 0 & x = 0 \end{cases}$$

eine Bewertung auf $K(A)$ definiert. Es ist klar, dass $|x| = 0$ genau dann, wenn $x = 0$. Auch die Multiplikativität folgt sofort. Um die starke Dreiecksungleichung zu zeigen, nehmen wir $x, y \in K(A)$. Ist x, y oder $x + y$ gleich Null, ist die Aussage klar. Daher nehmen wir an

$$x, y, x + y \in K(A)^\times.$$

Außerdem nehmen wir an $[x] \leq [y]$. Dann gilt

$$\frac{x+y}{y} = \left(\frac{x}{y} + 1\right) \in A,$$

also

$$[x + y] \leq [y] = \max\{[x], [y]\}.$$

Schließlich bemerken wir noch, dass

$$a = \{x \in K \mid |x| \leq 1\}$$

nach Konstruktion gilt. □

Proposition 3.17. *Zwei Bewertungen*

$$|\cdot|_1 : K \to \Gamma_1 \cup \{0\}$$
$$|\cdot|_2 : K \to \Gamma_2 \cup \{0\}$$

sind genau dann äquivalent, wenn ihre Bewertungsringe übereinstimmen, also

$$\mathcal{O}_{|\cdot|_1} = \mathcal{O}_{|\cdot|_2}.$$

Oder mit anderen Worten, wenn für $x, y \in K$ gilt

$$|x|_1 \leq |y|_1 \Leftrightarrow |x|_2 \leq |y|_2.$$

Beweis. Sind $|\cdot|_1$ und $|\cdot|_2$ äquivlant, so folgern wir für $x, y \in K$ wie im Beweis von Lemma 3.13, dass

$$|x|_1 \leq |y|_1 \Leftrightarrow |x|_2 \leq |y|_2.$$

Das impliziert $\mathcal{O}_{|\cdot|_1} = \mathcal{O}_{|\cdot|_2}$.

Nun nehmen wir an, dass

$$\mathcal{O}_{|\cdot|_1} = \mathcal{O}_{|\cdot|_2} =: \mathcal{O}.$$

Dann gilt

$$\begin{aligned}\mathcal{O}^\times &= \{x \in K \mid |x|_1 = 1\} \\ &= \{x \in K \mid |x|_2 = 1\}.\end{aligned}$$

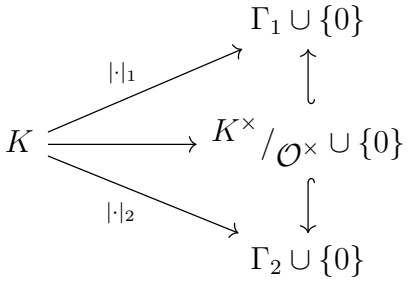
Die Abbildung

$$|\cdot|_1 : K^\times \to \Gamma_1$$

ist ein Homomorphismus mit Kern $\mathcal{O}^\times$. Daher bekommen wir einen injektiven Gruppenhomomorphismus

$$K^\times/_{\mathcal{O}^\times} \hookrightarrow \Gamma_1.$$

Statten wir $K^\times/\mathcal{O}^\times$ mit der im Beweis von Definition 3.16 konstruierten Ordnung aus, dann ist die obige Inklusion ordnungserhaltend. Wr erhalten ein kommutatives Diagramm



und somit sind die Bewertungen $|\cdot|_1$ und $|\cdot|_2$ äquivalent. □

3.3. **Klassifikation von Bewertungen.** Wir wollen für verschiedene Körper untersuchen, welche Bewertungen es gibt.

Proposition 3.18. *Sei $\mathbb{F}$ ein endlicher Körper. Dann ist jede Bewertung*

$$|\cdot| : \mathbb{F} \to \Gamma \cup \{0\}$$

und auch jede reelle Bewertung

$$|\cdot| : \mathbb{F} \to \mathbb{R}_{\geq 0}$$

trivial.

Beweis. Sei $\#\mathbb{F} = p^n$ für eine Primzahl p und $n \in N$. Dann gilt für alle $x \in \mathbb{F}^\times$

$$x^{p^n-1} = 1,$$

folglich

$$|x|^{p^n-1} = |x^{p^n-1}| = |1| = 1$$

und somit $|x| = 1$. □

Korollar 3.19. *Jede Bewertung auf einem Körper K der Charakteristik $p > 0$ ist nichtarchimedisch.*

Beweis. Das Bild der natürlichen Abbildung

$$\mathbb{Z} \to K$$
$$n \mapsto n \cdot 1_K$$

ist $\mathbb{F}_p \subseteq K$, und auf $\mathbb{F}_p$ ist nach Proposition 3.18 jede Bewertung trivial. Daher gilt

$$|n| = 1$$

für alle $n \in \mathbb{N}$ und somit ist die Bewertung nichtarchimedisch. □

Als nächstes untersuchen wir Bewertungen auf $\mathbb{Q}$. Unser Ziel ist es, zu zeigen, dass jede Bewertung auf $\mathbb{Q}$ entweder äquivalent zum Standardabsolutbetrag $|\cdot|_\infty$ ist oder zu einer p-adischen Bewertung $|\cdot|_p$ für eine Primzahl p. Zunächst überzeugen wir uns davon, dass diese Bewertungen paarweise nicht äquivalent sind.

Lemma 3.20. *Seien $|\cdot|_1$ und $|\cdot|_2$ zwei äquivalente reelle Bewertungen auf einem Körper K. Dann ist $|\cdot|_1$ archimedisch genau dann, wenn $|\cdot|_2$ archimedisch ist.*

Beweis. Wenn $|\cdot|_1$ archimedisch ist, gibt es für jedes Element $x \in K$ eine natürliche Zahl n, so dass

$$|x|_1 < |n|_1.$$

Da $|\cdot|_1$ und $|\cdot|_2$ äquivalent sind, gilt auch

$$|x|_2 < |n|_2$$

und somit ist $|\cdot|_2$ archimedisch. □

Korollar 3.21. *Der Standardabsolutbetrag auf $\mathbb{Q}$ ist zu keiner p-adischen Bewertung $|\cdot|_p$ für eine Primzahl p äquivalent.*

Lemma 3.22. *Seien $p \neq q$ Primzahlen. Dann ist $|\cdot|_p$ nicht äquivalent zu $|\cdot|_q$.*

Beweis. Es gilt $|p| = \frac{1}{p} < 1 = |1|_p$. Aber $|p|_q = 1 = |1|_q$. Daher können dide Bewertungen nicht äquivalent sein. □

Bevor wir unser Hauptresultat, den Satz von Ostrowski beweisen können, brauchen wir noch eine kleine Vorbereitung

Lemma 3.23. *Sei $|\cdot|$ eine reelle Bewertung auf einem Körper K und $m, n > 1$ natürliche Zahlen. Dann gilt*

$$|m| \leq \max\{1, |n|^{\frac{\log m}{\log n}}\}.$$

Beweis. Wir schreiben m in der Form

$$m = a_0 + a_1 n + \ldots + a_r n^r$$

für $a_i \in \{0, \ldots, n-1\}$. Dann ist $n^r \leq m$ also

$$r \leq \frac{\log m}{\log n}.$$

Die Bewertung von a_i können wir folgendermaßen abschätzen:

$$|a_i| = |\underbrace{1 + \ldots + 1}_{a_i \text{ mal}}| \leq a_i \cdot |1| = a_i \leq n.$$

Wenn $|n| \leq 1$ ist, so gilt $|n^i| = |n|^i \leq 1$ für alle $i = 0, \ldots, r$. Ist $|n| > 1$, so gilt $|n^i| \leq |n|^r$ für alle $i = 0, \ldots, r$. Insgesamt folgt

$$|n| \leq \max\{1, |n|^r\}$$

□

Dann gilt für die Bewertung von m:

$$\begin{aligned} |m| &\leq \sum_{i=0}^{r} |a_i||n|^i \\ &\leq (r+1) \cdot n \cdot \max\{1, |n|^r\} \\ &\leq \left(\frac{\log m}{\log n} + 1\right) \cdot n \cdot \max\{1, |n|^{\frac{\log m}{\log n}}\} \end{aligned}$$

Die gleiche Überlegung können wir für m^k für $k \in \mathbb{N}$ statt m durchführen und erhalten

$$|m| = \sqrt[k]{|m|^k} \leq \sqrt[k]{k\frac{\log m}{\log n} + 1} \cdot \sqrt[k]{n} \cdot \max\{1, |n|^{\frac{\log m}{\log n}}\}$$

Im Limes $k \to \infty$ folgt

$$|m| \leq \max\{1, |n|^{\frac{\log m}{\log n}}\}.$$

Satz 3.24 (Satz von Ostrowski)**.** *Jede nichttriviale reelle Bewertung auf* $\mathbb{Q}$ *ist entweder äquivalent zu* $|\cdot|_p$ *für eine Primzahl* p *oder zu* $|\cdot|_\infty$*.*

Beweis. Wir behandeln zunächst den Fall einer archimedischen Bewertung $|\cdot|$. Es gibt eine natürliche Zahl m, so dass

$$|m| > 1$$

Da $|1| = 1$, muss $m > 1$ sein. Nach Lemma 3.23 gilt für jede natürliche Zahl $n > 1$

$$|m| \leq \max\{1, |n|^{\frac{\log m}{\log n}}\}.$$

Weil $|m| > 1$ ist, muss auch $|n| > 1$ sein und

$$|m| \leq |n|^{\frac{\log m}{\log n}}.$$

Das gleiche Argument mit vertauschten Rollen für m und n ergibt

$$|n| \leq |m|^{\frac{\log n}{\log m}}.$$

Folglich gilt

$$|n|^{\frac{1}{\log n}} = |m|^{\frac{1}{\log m}} =: C$$

für alle natürlichen Zahlen $m, n > 1$. Das können wir zu

$$|n| = C^{\log n} = e^{\log C \cdot \log n} = n^{\log C}$$

umformen.

Für $n = 0$ oder $n = 1$ gilt die Formel trivialerweise und für $n \in \mathbb{Z}$, $n < 0$ erhalten wir

$$|n| = |-1| \cdot |-n| = |-n| = (-n)^{\log C} = |n|_\infty^{\log C},$$

wobei $|\cdot|_\infty$ den Standardabsolutbetrag

$$|x|_\infty = \begin{cases} x & x \geq 0 \\ -x & x < 0 \end{cases}$$

bezeichnet. Für ein allgemeines Element $x \in \mathbb{Q}^\times$ finden wir ganze Zahlen m, n mit $m \neq 0$, so dass $x = \frac{n}{m}$. Dann folgt

$$|x| = \frac{|n|}{|m|} = \frac{|n|_\infty^{\log C}}{|m|_\infty^{\log C}} = \left|\frac{n}{m}\right|_\infty^{\log C}$$

Nach Lemma 3.13 ist $|\cdot|$ äquivalent zu $|\cdot|_\infty$.

Jetzt nehmen wir an, dass $|\cdot|$ eine nichtarchimedische Bewertung ist. Dann gilt

$$|n| \leq 1$$

für alle natürlichen Zahlen n. Da die Bewertung $|\cdot|$ nicht trivial ist, gibt es $n \in \mathbb{N}$ mit

$$|n| < 1.$$

Sei

$$n = p_1^{r_1} \cdot \ldots \cdot p_k^{r_k}$$

die Primfaktorzerlegung von n. Dann gilt

$$1 > |n| = |p_1|^{r_1} \cdot \ldots \cdot |p_k|^{r_k}$$

Da die Bewertung aller Faktoren kleiner oder gleich 1 ist, gibt es einen Index i, so dass für $p := p_i$ gilt

$$|p| < 1.$$

Wegen der starken Dreiecksungleichung ist

$$\mathfrak{a} := \{x \in \mathbb{Z} \mid |x| < 1\}$$

ein Ideal von $\mathbb{Z}$ und es gilt außerdem $p\mathbb{Z} \subseteq \mathfrak{a}$. Da $p\mathbb{Z}$ maximal ist, gilt entweder $\mathfrak{a} = p\mathbb{Z}$ oder $\mathfrak{a} = \mathbb{Z}$. Der zweite Fall kann nicht eintreten, da $|1| = 1$.

Für eine beliebige rationale Zahl x schreiben wir

$$x = p^k \frac{m}{n}$$

für $k, m, n \in \mathbb{Z}$ mit $n \neq 0$ und $p \nmid mn$. Dann sind m und n nicht in $\mathfrak{a}$ und folglich gilt $|m| = |n| = 1$. Daraus erhalten wir

$$|x| = |p|^k$$

und $|\cdot|$ ist äquivalent zu $|\cdot|_p$. □

Bemerkung 3.25. Der Beweis des nichtarchimedischen Teils von Satz 3.24 zeigt auch, dass jede nicht unbedingt reelle Bewertung

$$|\cdot| : \mathbb{Q} \to \Gamma \cup \{0\}$$

äquivalent zu einer p-adischen Bewertung $|\cdot|_p$ für eine Primzahl p ist.

Korollar 3.26. *Jede reelle Bewertung mit diskreter Wertegruppe ist nichtarchimedisch.*

Beweis. Archimedische Bewertungen gibt es nach Korollar 3.19 nur für Körper K der Charakteristik 0. Dann enthält K den Körper $\mathbb{Q}$ der rationalen Zahlen. Hat eine Bewertung

$$|\cdot| : K \to \mathbb{R}_{\geq 0}$$

diskrete Wertegruppe, so gilt dasselbe auch für die Einschränkung $|\cdot|_\mathbb{Q}$ auf $\mathbb{Q}$. Aber $|\cdot|_\mathbb{Q}$ ist nach Satz 3.24 äquivalent zum Absolutbetrag $|\cdot|_\infty$. □

In vielen zahlentheoretischen Fragen verhält sich der Körper der rationalen Funktionen $\mathbb{F}(T)$ für einen endlichen Körper $\mathbb{F}$ ähnlich wie der Körper der rationalen Zahlen $\mathbb{Q}$. Das ist auch was die möglichen Bewertungen angeht der Fall.

Zunächst arbeiten wir über einem beliebigen Körper K. Wir erinnern uns daran, dass $K[T]$ ein Dedekindring ist, dessen Primideale gerade die Hauptideale sind, die von irreduziblen Polynomen $P \in K[T]$ erzeugt werden. Nach Satz 2.14 ist die Lokalisierung $K[T]_{(P)}$ ein diskreter Bewertungsring mit Maximalideal $PK[T]_{(P)}$. Die zugehörige additive diskrete Bewertung

$$v_P : K(T) \to \mathbb{Z} \cup \{\infty\}$$

ist folgendermaßen definiert: wegen der Existenz und Eindeutigkeit der Primfaktorzerlegung in $K[T]$ können wir jedes Element $h \in K(T)$ in der Form

$$h(T) = P(T)^{n_P} \frac{f(T)}{g(T)}$$

für zu P teilerfremde Polynome $f, g \in K[T]$ mit $g \neq 0$ schreiben. Dann gilt

$$v_P(h) = n_p.$$

Die entsprechende multiplikative Bewertung

$$|\cdot|_P : K(T) \to \mathbb{R}_{\geq 0}$$

normieren wir folgendermaßen:

$$|n|_P := p^{-\deg(P) v_P(h)}$$

falls $p = \operatorname{char} K > 0$ und $|h|_P := e^{-\deg v_P(h)}$ für $\operatorname{char} K = 0$.

Ist P von der Form $T - a$ für $a \in K$, so kann man v_P auch als Nullstellenordnung in a interpretieren: Für $h \in K(T)$ gilt per Definition

$$h(T) = (T-a)^{v_{T-a}(h)} \frac{f(T)}{g(T)}$$

für Polynome f und g mit $f(a) \neq 0$ und $g(a) \neq 0$. Wenn $v_{T-a}(h)$ negativ ist, hat h einen Pol in a der Ordnung $-v_{T-a}(h)$. Wir bezeichnen $|\cdot|_{T-a}$ auch mit $|\cdot|_a$.

Es gibt auf $K(T)$ noch folgende weitere diskrete Bewertung

$$\begin{aligned} v_\infty : K(T) &\to \mathbb{Z} \cup \{\infty\} \\ \frac{f}{g} &\mapsto \deg g - \deg f \end{aligned}$$

wobei $g \neq 0$ ist und $\deg 0 = -\infty$.

Lemma 3.27. *v_∞ ist eine diskrete Bewertung.*

Beweis. Zuallererst überzeugen wir uns davon, dass v_∞ wohldefiniert ist. Falls f, f', g, g' Elemente von $K[T]$ sind mit $g, g' \neq 0$ und

$$\frac{f}{g} = \frac{f'}{g'},$$

dann gilt $g'f = gf'$ und folglich

$$\begin{aligned} \deg(g') + \deg(f) &= \deg(g'f) \\ &= \deg(gf') \\ &= \deg(g) + \deg(f'), \end{aligned}$$

also

$$\deg(g) - \deg(f) = \deg(g') - \deg(f').$$

Jetzt weisen wir noch die Axiome für Bewertungen nach:

(i) $v_\infty(0) = -\deg(0) = \infty$

(ii) Für $f, f', g, g' \in K[T]$ mit $g, g' \neq 0$ gilt

$$\begin{aligned} v_\infty\left(\frac{ff'}{gg'}\right) &= \deg(gg') - \deg(ff') \\ &= [\deg(g) - \deg(f)] + [\deg(g') - \deg(f')] \\ &= v_\infty\left(\frac{f}{g}\right) + v_\infty\left(\frac{f'}{g'}\right). \end{aligned}$$

(iii) Wir betrachten $f, f' \in K[T]$ und nehmen ohne Beschränkung der Allgemeinheit an, dass $\deg(f) \geq \deg(f')$. Dann gilt

$$\deg(f + f') \leq \deg(f).$$

(Es gilt nicht unbedingt Gleichheit, da sich die Leitkoeffizienten im Fall $\deg(f) = \deg(f')$ wegkürzen könnten.) Das bedeutet

$$v_\infty(f + f') = -\deg(f + f') \geq -\deg(f) = v_\infty(f) = \min\{v_\infty(f), v_\infty(f')\}$$

Für allgemeine Elemente $h, h' \in K(T)$ finden wir $g \in K(T)^\times$ mit $gh, gh' \in K[T]$. Daraus folgt mit (ii):

$$\begin{aligned} v_\infty(h + h') &= v_\infty\left(\frac{gh + gh'}{g}\right) \\ &= v_\infty(gh + gh') - v_\infty(g) \\ &\leq \min\{v_\infty(gh), v_\infty(gh') - v_\infty(g)\} \\ &= \min\{v_\infty(h), v_\infty(h')\}. \end{aligned}$$

□

Wir normieren die entsprechende multiplikative Bewertung

$$|\cdot|_\infty : K(T) \to \mathbb{R}_{\geq 0}$$

folgendermaßen. Für $h \in K(T)$ setzen wir

$$|h|_\infty = \left(\frac{1}{p}\right)^{v_\infty(h)},$$

falls $\operatorname{char} K = p > 0$ und

$$|h|_\infty = e^{-v_\infty(h)},$$

falls $\operatorname{char} K = 0$.

Die Bewertung $|\cdot|_\infty$ ist nicht äquivalent zu einer der vorher beschriebenen Bewertungen $|\cdot|_P$, da $|T|_P \geq 0$ ist für alle irreduziblen Polynome P, aber $|T|_\infty = -1$.

Bemerkung 3.28. Die Bewertung $|\cdot|_\infty$ auf $K(T)$ hat nichts mit der Bewertung $|\cdot|_\infty$ auf $\mathbb{Q}$ zu tun. Leider ist die weit verbreitete Notation etwas ungünstig. Der Index ∞ für die Bewertung $|\cdot|_\infty$ auf $K(T)$ hat eine geometrische Erklärung. unter dem Automorphismus

$$\begin{aligned} \iota : K(T) &\to K(T) \\ T &\mapsto \frac{1}{T} \end{aligned}$$

wird $|\cdot|_\infty$ in $|\cdot|_0$ überführt: Für $f \in K[T]$ der Form

$$f(T) = a_n T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0$$

mit $a_i \in K, a_n \neq 0$ erhalten wir

$$\begin{aligned} |\iota(f)|_\infty &= \left| f(\frac{1}{T}) \right| \\ &= \left| \frac{a_n}{T^n} + \frac{a_{n-1}}{T^{n-1}} + \ldots + \frac{a_1}{T} + a_0 \right| \\ &= \left| \frac{1}{T^n} \right| \cdot |a_n + a_{n-1}T + \ldots + a_1 T^{n-1} + a_0 T^n|_\infty \end{aligned}$$

Der Grad von $a_n + a_{n-1}T + \ldots + a_1 T^{n-1} + a_0 T^n$ ist gleich $n-k$, wobei k die kleinste natürliche Zahl ist, so dass $a_k \neq 0$. Das heißt

$$a_n + a_{n-1}T + \ldots + a_0 T^n = a_n + a_{n-1}T + \ldots + a_{k+1}T^{n-k-1} + a_k T^{n-k}$$

mit $a_k \neq 0$. Daher gilt

$$|\iota(f)|_\infty = n - (n-k) = k$$

Andererseits gilt dann aber

$$\begin{aligned} f(T) &= a_n T^n + a_{n-1}T^{k-1} + \ldots + a_{k+1}T^{k+1} + a_k T^k \\ &= T^k(a_n T^{n-k} + a_{n-1}T^{n-k-1} + \ldots + a_{k+1}T + a_k) \end{aligned}$$

und somit

$$|f|_0 = k = |\iota(f)|_\infty.$$

Die Bewertung $|\cdot|_\infty$ kann man somit interpretieren als die Bewertung, die zum Primideal $\left(\frac{1}{T}\right)$ von $K\left[\frac{1}{T}\right]$ gehört, also die Nullstellenordnung in 0 bezüglich der Variable $\frac{1}{T}$. Wenn $\frac{1}{T}$ gleich Null ist, bedeutet das $T = \infty$ (grob gesprochen).

Satz 3.29 (Satz von Ostrowski für Funktionenkörper)**.** *Sei $\mathbb{F}$ ein endlicher Körper. Dann ist jede Bewertung auf $\mathbb{F}(T)$ äquivalent zu $|\cdot|_\infty$ oder zu einer Bewertung $|\cdot|_P$ für ein irreduzibles Polynom $P \in \mathbb{F}[T]$.*

Beweis. Das Argument ist ähnlich wie der Beweis des Satzes von Ostrowski für $\mathbb{Q}$, siehe Übungen. □

Gibt es auf einem Körper K nicht-triviale Bewertungen, so kann man auf $K(T)$ Bewertungen konstruieren, die weder äquivalent zu Bewertungen der Form $|\cdot|_P$ für ein irreduzibles Polynom P sind noch äquivalent zu $|\cdot|_\infty$. Das ist der Grund dafür, dass wir in Satz 3.29 angenommen haben, dass der Grundkörper endlich ist.

Beispiel 3.30. Sei $|\cdot|$ eine nichttriviale reelle nichtarchimedische Bewertung auf einem Körper K (zum Beispiel $K = \mathbb{Q}$ und $|\cdot| = |\cdot|_p$ für eine Primzahl p). Wir wählen $r \in \mathbb{R}_{\geq 0}$ und definieren für ein Polynom

$$f(T) = a_n T^n + a_{n-1}T^{n-1} + \ldots + a_1 T + a_0$$

in $K[T]$

$$|f|_r := \max_{i=0,\ldots,n} \{|a_i| r^i\}$$

Für $h \in K(T)$ schreiben wir $h = \frac{f}{g}$ für $f, g \in K[T]$ und $g \neq 0$ und setzen

$$|h|_r := \frac{|f|_r}{|g|_r}.$$

Man kann zeigen, dass das eine reelle Bewertung

$$|\cdot|_r : K(T) \to \mathbb{R}_{\geq 0}$$

definiert, die nicht äquivalent zu $|\cdot|_P$ oder $|\cdot|_\infty$ ist.

Mit diesem Prinzip kann auch nicht-reelle Bewertungen konstruieren: Wir betrachten $\Gamma := \mathbb{R}_{>0} \oplus \lambda^{\mathbb{Z}}$ für $\lambda \in \mathbb{R}$, $0 < \lambda < 1$ mit der lexikografischen Ordnung. Die Gruppe $\lambda^{\mathbb{Z}}$ ist isomorph zu $\mathbb{Z}$, nur wollen wir sie multiplikativ schreiben.

Dann definieren wir für $r \in \mathbb{R}_{>0}$ und

$$f = a_n T^n + \ldots + a_1 T + a_0$$
$$|f|_r := \max\{(|a_i|, \lambda^i)\} \in \Gamma$$

Das definiert eine Bewertung auf $K(T)$, die nicht reell ist.

3.4. **Topologie zu einer Bewertung.** Sei

$$|\cdot| : K \to \mathbb{R}_{\geq 0}$$

eine reelle Bewertung. Für $x, y \in K$ definieren wir den Abstand

$$d(x, y) = |x - y|.$$

Das ist eine Metrik auf K, das heißt eine Funktion $K \times K \to \mathbb{R}_{\geq 0}$, so dass für $x, y, z \in K$ gilt:

(1) $d(x, y) = 0 \Leftrightarrow x = y$ (Definitheit)
(2) $d(x, y) = d(y, x)$ (Symmetrie)
(3) $d(x, y) \leq d(x, z) + d(z, y)$ (Dreiecksungleichung)

Jede Metrik definiert eine Topologie. Genauer gesagt ist eine Teilmenge $U \subseteq K$ offen genau dann, wenn es für jedes Element $x \in K$ eine reelle Zahl $\varepsilon > 0$ gibt, so dass

$$B_\varepsilon := \{y \in K \mid \underbrace{d(x, y)}_{=|x-y|} < \varepsilon\} \subseteq U.$$

Ist $x = 0$ bilden die entsprechenden Teilmengen

$$B_\varepsilon(0) = \{y \in K \mid |y| < \varepsilon\}$$

eine Umgebungsbasis. Das besondere hierbei ist, dass die $B_\varepsilon(0)$ im Falle einer nichtarchimedischen Bewertung wegen der strikten Dreiecksungleichung sogar Untergruppen von K sind.

Eine weitere Besonderheit im nichtarchimedischen Fall ist, dass auch

$$\overline{B_\varepsilon(x)} := \{y \in K \mid |x - y| \leq \varepsilon\}$$

offen ist. Der Grund ist der folgende: Für $x' \in B_\varepsilon(x)$ ist

$$B_\varepsilon(x') = \{y \in K \mid |x' - y| < \varepsilon\} \subseteq \overline{B_\varepsilon(x)},$$

da für $y \in B_\varepsilon(x')$ gilt

$$\begin{aligned} |x - y| &= |(x - x') + (x' - y)| \\ &\leq \max\{|x - x'|, |x' - y|\} \\ &\leq \varepsilon. \end{aligned}$$

Lemma 3.31. *Mit oben beschriebener Topologie wird K zum topologischen Körper, das heißt, Addition, Multiplikation und Inversenbildung sind stetig.*

Beweis. Wir betrachten die Addition

$$+ : K \times K \to K$$

Für $x, y \in K$ und $\varepsilon > 0$ müssen wir $\delta > 0$ finden, so dass für alle $x', y' \in K$ gilt:

$$|x - x'|, |y - y'| < \delta \Rightarrow |(x + y) - (x' + y')| < \varepsilon$$

Das ist für $\delta := \frac{\varepsilon}{2}$ erfüllt: Gilt $|x - x'|, |y - y'| < \delta$, so folgt mit der Dreiecksungleichung

$$\begin{aligned} |(x + y) - (x' + y')| &= |(x - x') + (y - y')| \\ &\leq |x - x'| + |y - y'| \\ &< \delta + \delta \\ &= 2\delta \\ &= \varepsilon. \end{aligned}$$

Der Beweis für die Stetigkeit der Multiplikation und der Inversenbildung ist ähnlich. □

Proposition 3.32. *Für zwei reelle Bewertungen $|\cdot|_1$ und $|\cdot|_2$ sind folgende Aussagen äquivalent*

(1) $|\cdot|_1$ und $|\cdot|_2$ sind äquivalent
(2) Die von $|\cdot|_1$ und $|\cdot|_2$ induzierten Topologien stimmen überein.

Beweis. Angenommen $|\cdot|_1$ und $|\cdot|_2$ sind äquivalent. Sind $|\cdot|_1$ und $|\cdot|_2$ trivial, so definieren beide Bewertungen die diskrete Topologie auf K. Ist $|\cdot|_1$ und somit auch $|\cdot|_2$ nichttrivial, so wählen wir $a \in K$ mit $|a|_1 < 1$. Dann konvergiert $|a^n|_1 = |a|_1^n$ gegen Null und für jeden Punkt bilden die Bälle

$$B_{|a^n|_1}(x) := \{y \in K \mid |x - y|_1 < |a^n|_1\}$$

eine Umgebungsbasis von x in der von $|\cdot|_1$ induzierten Topologie.

Da $|\cdot|_2$ äquivalent zu $|\cdot|_1$ ist, gilt nach Proposition 3.17 auch $|a|_2 < 1$ und mit der gleichen Argumentation bilden

$$B_{|a^n|_2}(x) := \{y \in K \mid |x - y|_2 < |a^n|_2\}$$

eine Umbegungsbasis von x in der zu $|\cdot|_2$ induzierten Topologie. Nach Proposition 3.17 gilt

$$|x - y|_1 < |a^n|_1 \Leftrightarrow |x - y|_2 < |a^n|_2$$

und somit

$$B_{|a^n|_1}(x) = B_{|a^n|_2}(x).$$

Das heißt, die Topologien stimmen überein.

Nun nehmen wir an, dass die von $|\cdot|_1$ und $|\cdot|_2$ induzierten Topologien gleich sind. Insbesondere konvergiert für $x \in K$ die Folge x^n bezüglich $|\cdot|_1$ genau dann gegen Null, wenn sie bezüglich $|\cdot|_2$ gegen Null konvergiert. Andererseits wissen wir, dass $|x^n|_1 = |x|_1^n$ genau dann gegen Null konvergiert, wenn $|x|_1 < 1$ gilt. Das heißt x^n ist eine Nullfolge bezüglich $|\cdot|_1$ genau dann, wenn $|x| < 1$. Die gleiche Überlegung gilt für $|\cdot|_2$. Wir wissen nun

$$|x|_1 < 1 \Leftrightarrow |x|_2 < 1$$

Daraus folgt mit Proposition 3.17, dass $|\cdot|_1$ und $|\cdot|_2$ äquivalent sind. □

Bemerkung 3.33. Auch eine nicht notwendigerweise reelle Bewertung

$$|\cdot| : K \to \Gamma \cup \{0\}$$

definiert eine Topologie auf K. Äquivalente Bewertungen definieren die gleiche Topologie. Allerdings können auch nichtäquivalente Bewertungen die gleiche Topologie induzieren. Unter milden Voraussetzungen (für sogenannte mikrobielle Bewertungen, das sind solche für die es $x \in K^\times$ gibt mit $|x|^n \to 0$.) ist

$$K^\circ := \{x \in K \mid |x|^n \text{ ist beschränkt}\}$$

ein Bewertungsring von K mit

$$\mathcal{O}_{|\cdot|} \subseteq K^\circ \subsetneq K$$

Die zu K° gehörige Bewertung ist reell und die induzierte Topologie ist die gleiche wie die von $|\cdot|$ induzierte.

Daraus schließen wir, dass die von zwei Bewertungen $|\cdot|_1$ und $|\cdot|_2$ induzierten Topologien auf K genau dann gleich sind, wenn die entsprechenden Bewertungsringe K° gleich sind.

Satz 3.34 (Schwache Approximation)**.** *Seien $|\cdot|_1, \ldots, |\cdot|_n$ paarweise nichtäquivalente reelle Bewertungen auf einem Körper K und $a_1, \ldots, a_n \in K$. Dann gibt es für jedes $\varepsilon > 0$ ein Element $x \in K$, so dass*

$$|x - a_i| < \varepsilon$$

für alle $i = 1, \ldots, n$.

Beweis. Zunächst zeigen wir folgende Behauptung: $\exists z \in K$ mit $|z|_1 > 1$ und $|z|_j < 1$ für $j = 2, \ldots, n$.
Wir führen den Beweis per Induktion über n. Wir beginnen mit $n = 2$. Da $|\cdot|_1$ und $|\cdot|_2$ nicht äquivalent sind, gibt es nach Proposition 3.17 ein Element $\alpha \in K$ mit $|\alpha|_1 > 1$ und $|\alpha|_2 \leq 1$ und $\beta \in K$ mit $|\beta|_1 \leq 1$ und $|\beta|_2 > 1$. Dann gilt für $z := \frac{\alpha}{\beta}$: $|z|_1 > 1$ und $|z|_2 < 1$.
Wir nehmen nun an, dass es $z' \in K$ gibt mit $|z'|_1 > 1$ und $|z'|_j < 1$ für $j = 2, \ldots, n-1$. Außerdem können wir laut Induktionsanfang ein Element $<\in K$ finden mit $|y|_1 > 1$ und $|y|_n < 1$.
1. Fall: $|z'|_n \leq 1$. Dann erfüllt $z := z'^m \cdot y$ für hinreichend großes $m \in \mathbb{N}$ die geforderten Bedingungen.
2.Fall:$|z'| > 1$. Dann betrachten wir die Folge

$$t_m := \frac{z'^m}{1 + z'^m} = \frac{1}{(\frac{1}{z'})^m + 1}.$$

Bezüglich $|\cdot|_1$ und $|\cdot|_n$ konvergiert t_m gegen 1 und bezüglich $|\cdot|_2, \ldots, |\cdot|_{n-1}$ gegen 0. Daher erfüllt $z := t_m y$ für hinreichend großes m die geforderten Bedingungen. Somit ist die Behauptung bewiesen.

Für ein Element $z \in K$ wie aus der Behauptung betrachten wir die Folge

$$t_m := \frac{z^m}{1 + z^m}.$$

Sie konvergiert bezüglich $|\cdot|_1$ gegen 1 und bezüglich $|\cdot|_j$ für $j = 2, \ldots, n-1$ gegen 0. Für genügend großes m gilt folglich

$$|1 - t_m|_1 < \frac{\varepsilon}{n\alpha_1}$$

$$|t_m|_j < \frac{\varepsilon}{n\alpha_1},$$

für $j = 2, \ldots, n-1$, wobei

$$\alpha_1 := \begin{cases} |a_1|_1 & a_1 \neq 0 \\ 1 & a_1 = 0 \end{cases}$$

Vertauschen wir die Rollen von $|\cdot|_1$ und $|\cdot|_i$ für $i > 1$ erhalten wir $y_i \in K$ mit $|1-y_i| < \frac{\varepsilon}{n\alpha_i}$ und $|y_i|_j < \frac{\varepsilon}{n\alpha_i}$ für $i \neq j$, wobei $\alpha_i = \begin{cases} |a_i|_i & a_i \neq 0 \\ 1 & a_i = 0 \end{cases}$ Für

$$x := a_1 y_1 + \ldots + a_n y_n$$

gilt dann

$$\begin{aligned} |x - a_i| &= |a_1 y_1 + \ldots + a_{i-1} y_{i-1} + a_i(y_i - 1) + a_{i+1} y_{i+1} + \ldots + a_n y_n| \\ &< n\frac{\varepsilon}{n} = \varepsilon. \end{aligned}$$

□

Korollar 3.35. *Für paarweise inäquivalente reelle Bewertungen $|\cdot|_1, \ldots, |\cdot|_n$ auf einem Körper K sei $K_i = K$ mit der von $|\cdot|_i$ induzierten Topologie. Dann liegt das Bild der Diagonalabbildung*

$$\begin{aligned} K &\to \prod_{i=1}^{n} K_i \\ x &\mapsto (x, \ldots, x) \end{aligned}$$

dicht.

3.5. **Vollständig bewertete Körper.** Sei $(K, |\cdot|)$ ein reell bewerteter Körper. Im letzten Abschnitt haben wir K mit einer Metrik und einer Topologie versehen. Durch die Metrik erhalten wir für Folgen in K einen Begriff von Konvergenz und auch Cauchyfolgen sind definiert.

Definition 3.36. $(K, |\cdot|)$ heißt *vollständig*, wenn jede Cauchyfolge in K konvergiert.

Ist $(K, |\cdot|)$ nicht notwendigerweise vollständig, so kann man die Vervollständigung konstruieren. Ihre universelle Eigenschaft ist die folgende:

Definition 3.37. Die Vervollständigung von $(K, |\cdot|)$ ist ein vollständig bewerteter Körper $(\widehat{K}, |\cdot|\hat{})$ zusammen mit einem Körperhomomorphismus

$$\iota : K \to \widehat{K}$$

mit $|\cdot|\hat{}_K = |\cdot|$, der universell ist mit dieser Eigenschaft.

Um zu zeigen, dass die Vervollständigung existiert, geben wir eine explizite Beschreibung an. Die Konstruktion ist die gleiche wie die, die man durchführt,um $\mathbb{R}$ aus $\mathbb{Q}$ zu konstruieren. In der Tat ist dies ein Spezialfall, da $\mathbb{R}$ die Vervollständigung von $\mathbb{Q}$ bezüglich $|\cdot|_\infty$ ist.

Wir sagen, dass zwei Cauchyfolgen $(x_n)_{n\in\mathbb{N}}$ und $(y_n)_{n\in\mathbb{N}}$ *äquivalent* sind, wenn $(x_n - y_n)_{n\in\mathbb{N}}$ eine Nullfolge ist. In dem Fall schreiben wir $(x_n) \sim (y_n)_{n\in\mathbb{N}}$.

Wir definieren

$$\widehat{K} := \{\text{Cauchyfolgen in } K\}_{/\sim}.$$

Wir definieren die Summe und das Produkt zweier Cauchyfolgen $(x_n)_{n\in\mathbb{N}}$ und $(y_n)_{n\in\mathbb{N}}$ gliedweise:

$$(x_n)_{n\in\mathbb{N}} + (y_n)_{n\in\mathbb{N}} := (x_n + y_n)_{n\in\mathbb{N}}$$
$$(x_n)_{n\in\mathbb{N}} \cdot (y_n)_{n\in\mathbb{N}} := (x_n y_n)_{n\in\mathbb{N}}$$

Außerdem definieren wir folgenden Homomorphismus

$$\begin{aligned}\iota : K &\to \widehat{K},\\ x &\mapsto (x, x, x, \ldots).\end{aligned}$$

Dann muss man folgende Aussagen prüfen (was wir uns hier ersparen):

- Addition und Multiplikation definieren Operationen auf $\widehat{K}$, die $\widehat{K}$ zu einem Körper machen.
- Die Bewertung $|\cdot|$ setzt sich stetig fort zu folgender Bewertung $|\cdot|\hat{}$ auf $\widehat{K}$:
$$|(x_n)_{n\in\mathbb{N}} := \lim_{n\to\infty} |x_n|.$$
- $(K, |\cdot|) \to (\widehat{K}, |\cdot|\hat{})$ erfüllt die universelle Eigenschaft.

Beispiel 3.38. Die Vervollständigung von $\mathbb{Q}$ bezüglich $|\cdot|_\infty$ ist $\mathbb{R}$. Bezüglich einer p-adischen Bewertung ist die Vervollständigung gleich $\mathbb{Q}_p$, dem Körper der p-adischen Zahlen.

Die Vervollständigung von $K(T)$ bezüglich $|\cdot|_0 = |\cdot|_T$ ist

$$K(\!(T)\!) := \left\{ \sum_{k=-N}^{\infty} a_k T^k \mid a_k \in K, N \in \mathbb{Z} \right\}$$

mit der Bewertung

$$\left| \sum_{k=-N}^{\infty} a_k T^k \right|_T^{\wedge} := e^{-\min\{k\geq -N | a_k \neq 0\}}.$$

Dass das tatsächlich die Vervollständigung von $K(T)$ bezüglich $|\cdot|_0$ ist, werden wir in den Übungen nachprüfen.

Lemma 3.39. *Sei $(K, |\cdot|)$ reell bewertet, nichtarchimedisch mit Vervollständigung $(\widehat{K}, |\cdot|\hat{})$. Dann gilt:*

(1) $|K^\times| = |\widehat{K}^\times|\hat{}$ (die Wertegruppen stimmen überein)
(2) $\mathcal{O}_{\widehat{K}} = \widehat{\mathcal{O}_K}$

Beweis. (1) Sei $(x_n)_{n\in N}$ eine Cauchyfolge in K und $\alpha := \lim |x_n| = |(x_n)_{n\in\mathbb{N}}|\hat{}$. Wir müssen zeigen, dass $\alpha \in |K|$. Ist $\alpha = 0$, ist das klar. Ansonsten gibt es $N \in \mathbb{N}$, so dass für $m, n \geq N$ gilt:
(i) $|x_n| > \frac{\alpha}{2}$
(ii) $|x_n - x_m| < \frac{\alpha}{2}$
Dann gilt für $n, m \geq N$

$$\begin{aligned}|x_n| &= |x_m + (x_n - x_m)|\\ &= \max |x_m|, |x_n - x_m|\\ &= |x_m|.\end{aligned}$$

Hierbei haben wir benutzt, dass

$$|x_m| > \frac{\alpha}{2} > |x_n - x_m|$$

gilt und deshalb nach Lemma 3.10 die Dreiecksungleichung eine Gleichung ist. Wir schließen, dass für $n \geq N$ die Werte stationär werden und somit

$$\alpha = |x_N| \in |K^\times|.$$

(2) Aus Stetigkeitsgründen folgt, dass alle Elemente in $\widehat{O_K}$ Bewertung kleiner oder gleich 1 haben, das heißt

$$\widehat{O}_K \subseteq \mathcal{O}_{\widehat{K}}.$$

Ist $(x_n)_{n\in\mathbb{N}}$ eine Cauchyfolge in K, deren Äquivalenzklasse in $\mathcal{O}_{\widehat{K}}$ liegt, so gilt

$$|(x_n)_{n\in\mathbb{N}}|\hat{} = \lim_{n\to\infty} |x_n| \leq 1$$

Im Beweis von (1) haben wir gesehen, dass für genügend große n die Werte $|x_n|$ stationär werden. Die entsprechenden Folgenglieder x_n liegen dann schon in $\mathcal{O}_K$. Schmeißen wir die endlich vielen Folgenglieder, die nicht in $\mathcal{O}_K$ sind, heraus, so erhalten wir eine äquivalente Cauchyfolge, die noch dazu in $\mathcal{O}_K$ liegt. Diese definiert ein Element von $\widehat{O_K}$.

□

Satz 3.40 (Henselsches Lemma)**.** *Sei $(K, |\cdot|)$ ein vollständiger, nichtarchimedisch reell bewerteter Körper mit Bewertungsring $\mathcal{O}$. Sei $f \in \mathcal{O}[T]$ ein Polynom und $a_0 \in \mathcal{O}$, so dass*

$$|f(a_0)| < |f'(a_0)|^2.$$

Dann gibt es eine Nullstelle $a \in \mathcal{O}$ von f mit

$$|a_0 - a| < |f'(a_0)|.$$

Beweis. Die Idee besteht darin, mithilfe des Newtonverfahrens eine Cauchyfolge $(a_n)_{n\in\mathbb{N}}$ zu konstruieren, die dann gegen eine Nullstelle von f konvergiert.

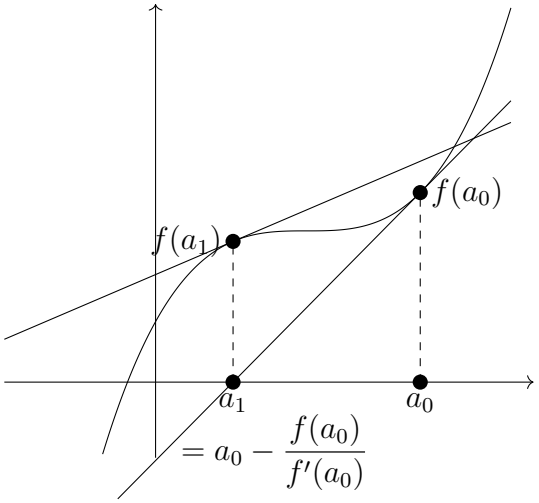


ABBILDUNG 1. Das klassische Newton-Verfahren

Formal: Wir definieren induktiv folgende Folge $(a_n)_{n\geq 0}$ in $\mathcal{O}$:

- a_0 ist das gegebene Element a_0 mit $|f(a_0)| < |f'(a_0)^2|$. Insbesondere ist $f'(a_0) \neq 0$

- Ist a_n konstruiert mit $f'(a_n) \neq 0$, so setzen wir

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$$

Wir setzen $\varepsilon := \left|\frac{f(a_0)}{f'(a_0)^2}\right| < 1$. *Behauptung*:

(1) $|f'(a_n)| = |f'(a_0)|$, also inbesondere $f'(a_0) \neq 0, \forall n$ und wir können immer a_{n+1} definieren.
(2) $|f(a_n)| \leq \varepsilon^n |f(a_0)|$
(3) $|a_n - a_{n-1}| \leq \varepsilon^n |f'(a_0)|$ (für $n \geq 1$)

Beweis der Behauptung: Für $n = 0$ ist die Aussage klar. Wir nehmen nun an, dass (1),(2),(3) für a_n gelten und weisen sie für $a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$ nach.

(1) Für Polynome existiert an jedem Punkt die Taylorentwicklung. Hier entwickeln wir die Ableitung f' im Punkt a_n:

$$f'(T) = f'(a_n) + (T - a_n)g(T)$$

für ein Polynom $g(T) \in \mathcal{O}[T]$. Setzten wir $T = a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$, erhalten wir

$$f'(a_{n+1}) = f'(a_n) - \frac{f(a_n)}{f'(a_n)} \underbrace{g(a_{n+1})}_{\in \mathcal{O}}$$

Da

$$\begin{aligned}\left|\frac{f(a_n)}{f'(a_n)} g(a_{n+1})\right| &\leq \left|\frac{f(a_n)}{f'(a_n)}\right| \\ &\leq \frac{\varepsilon^n |f(a_0|)}{|f'(a_0)|} \\ &= \varepsilon^{n+1} |f'(a_0)| \\ &= \varepsilon^{n+1} |f'(a_n)| \\ &< |f'(a_n)|,\end{aligned}$$

gilt nach Lemma 3.10 Gleichheit bei der Dreiecksungleichung:

$$\begin{aligned}|f'(a_{n+1})| &= \max\left\{|f'(a_n)|, \left|\frac{f(a_n)}{f'(a_n)} g(a_{n+1})\right|\right\} \\ &= |f'(a_n)| = |f'(a_0)|\end{aligned}$$

(2) Wir betrachten die Taylorentwicklung von f in a_n:

$$f(T) = f(a_n) + f'(a_n)(T - a_n) + (T - a_n)^2 h(T)$$

für ein Polynom $h \in \mathcal{O}[T]$ und setzen $T = a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}$:

$$\begin{aligned}f(a_{n+1}) &= f(a_n) + f'(a_n) \cdot \frac{f(a_n)}{f'(a_n)} + \frac{f(a_n)^2}{f'(a_n)^2} h(a_{n+1}) \\ &= \frac{f(a_n)^2}{f'(a_n)^2} h(a_{n+1}).\end{aligned}$$

Dann gilt

$$\begin{aligned}
|f(a_{n+1})| &= \left|\frac{f(a_n)^2}{f'(a_n)^2}\right| |h(a_{n+1})| \\
&\leq \left|\frac{f(a_n)^2}{f'(a_n)^2}\right| \\
&\leq \frac{(\varepsilon^n |f(a_0)|)^2}{|f'(a_0)|^2} \\
&= \varepsilon^{2n} \cdot \left|\frac{f(a_0)}{f'(a_0)^2}\right| \cdot |f(a_0)| \\
&= \varepsilon^{2n+1} |f(a_0)| \\
&\leq \varepsilon^{n+1} |f(a_0)|.
\end{aligned}$$

(3)

$$\begin{aligned}
|a_{n+1} - a_n| &= \left|\frac{f(a_n)}{f'(a_n)}\right| \\
&\leq \frac{\varepsilon^n |f(a_0|)}{|f'(a_0)|} \\
&= \varepsilon^{n+1} |f'(a_0)|
\end{aligned}$$

Aus (3) folgt, dass $(a_n)_{n\geq 0}$ eine Cauchyfolge ist, da

$$\begin{aligned}
|a_{n+k} - a_n| &\leq \max_{i=1,\dots,k} \{|a_{n+i} - a_{n+i-1}\} \\
&\leq \max_{i=1,\dots,k} \{\varepsilon^{n+i}|\} \\
&= \varepsilon^{n+1} |f'(a_0)|
\end{aligned}$$

Da K vollständig ist, konvergiert die Folge gegen ein Element $a \in K$. Nun ist $a_n \in \mathcal{O}$ für alle $n \geq 0$ und somit gilt nach Lemma 3.39 (2) sogar $a \in \mathcal{O}$. Aus (2) folgt, dass $(f(a_n))_{n\geq 0}$ gegen 0 konvergiert. Weil f als Polynom stetig ist, folgt daraus

$$f(a) = 0.$$

Außerdem gilt nach (3)

$$\begin{aligned}
|a - a_0| &= \lim_{n\to\infty} |a_n - a_0| \\
&\leq \lim_{n\to\infty} \varepsilon |f'(a_0)| \\
&= \varepsilon |f'(a_0)| \\
&< |f'(a_0)|.
\end{aligned}$$

□

Oft wird folgende Folgerung aus Satz 3.40 als Henselsches Lemma bezeichnet:

Korollar 3.41. *Sei $(K, |\cdot|)$ ein vollständiger nichtarchimedisch reell bewerteter Körper mit Bewertungsring $\mathcal{O}$, Maximalideal $\mathfrak{m}$ und Restklassenkörper*

$$k := \mathcal{O}/\mathfrak{m}.$$

Sei $f \in \mathcal{O}[T]$ ein Polynom, dessen Restklassen $[f] \in k[T]$ eine einfache Nullstelle $\overline{a} \in k$ hat. Dann besitzt f eine eindeutig bestimmte Nullstelle $a \in \mathcal{O}$ mit $[a] = \overline{a}$.

Beweis. Wir wählen ein Urbild $a_0 \in \mathcal{O}$ von $\overline{a}$. Dann gilt

$$[f(a_0)] = [f](\overline{a}) = 0,$$

also $|f(a_0)| < 1$. Da $[f]$ in $\overline{a}$ eine einfache Nullstelle hat, gilt $[f'(a_0)] = [f]'(\overline{a}) \neq 0$, also $|f'(a_0)| = 1$. Insbesondere folgt

$$|f(a_0)| < |f'(a_0)|^2.$$

Damit sind die Voraussetzungen für Satz 3.40 erfüllt und wir erhalten eine Nullstelle $a \in \mathcal{O}$ von f mit

$$|a - a_0| < |f'(a_0)| = 1.$$

Das bedeutet $[a] = [a_0] = \overline{a}$.

Für die Eindeutigkeit nehmen an $a' \in \mathcal{O}$ ist eine weitere Nullstelle von f mit $[a'] = [a] = \overline{a}$. Dann gilt:

- $f(a) = f(a') = 0$
- $|f'(a)| = |f'(a')| = 1$
- $|a - a'| < 1$.

Aus der Taylorentwicklung von f in a erhalten wir

$$f(a') = f(a) + f'(a)(a' - a) + (a' - a)^2 c$$

für $c \in \mathcal{O}$. Daraus folgt

$$|a' - a| = |a' - a|^2 |c| \leq |a' - a|$$

Da $|a' - a| < 1$, kann das nur stimmen, wenn $|a' - a| = 0$, also $a' = a$. □

Korollar 3.42. *Sei $(K, |\cdot|)$ ein vollständiger, nichtarchimedischer, reell bewerteter Körper mit endlichem Restklassenkörper $k = \mathcal{O}_{|\cdot|}/\mathfrak{m}_{|\cdot|}$ der Kardinalität q. Dann enthält K die $(q-1)$-ten Einheitswurzeln.*

Beweis. Wir betrachten das Polynom

$$f(T) = T^{q-1} - 1 \in \mathcal{O}_{|\cdot|}[T]$$

und seine Restklasse

$$[f](T) = T^{q-1} - 1 \in k[T].$$

Da $\#k = q$, gilt für alle Elemente $\overline{a} \in k^\times$: $\overline{a}^{q-1} = 1$. Daher hat $[f]$ genau $q-1$ verschiedene Nullstellen $\overline{\zeta_1}, \ldots, \overline{\zeta_{q-1}} \in k$.

Diese heben sich nach Korollar 3.41 zu $q-1$ verschiedenen Nullstellen

$$\zeta_1, \ldots, \zeta_{q-1} \in \mathcal{O}_{|\cdot|} \subseteq K$$

von f. Das bedeutet gerade $\mu_{q-1} \subseteq K$. □

Beispiel 3.43. Die p-adischen Zahlen $\mathbb{Q}_p$ enthalten die $(p-1)$-ten Einheitswurzeln:

$$\mu_{p-1} \subseteq \mathbb{Q}_p.$$

4. Erweiterungen bewerteter Körper

Definition 4.1. Eine *Erweiterung bewerteter Körper* $(L, |\cdot|_K)/(K, |\cdot|_K)$ ist eine Körpererweiterung L/K, so dass die Einschränkung von $|\cdot|_L$ auf K gleich $|\cdot|_K$ ist.

Bemerkung 4.2. Auf dem Niveau der Bewertungsringe $\mathcal{O}_L$ von $|\cdot|_L$ und $\mathcal{O}_K$ von $|\cdot|_K$ bedeutet die Bedingung $|\cdot|_L\big|_K = |\cdot|_K$, dass $\mathcal{O}_L \cap K = \mathcal{O}_K$.

4.1. **Der Satz von Chevalley.** Unser Ziel in diesem Abschnitt ist folgendes. Wir betrachten einen bewerteten Körper $(K, |\cdot|)$ und eine endliche Körpererweiterung L/K.

Dann wollen wir die *Fortsetzungen* von $|\cdot|$ nach L beschreiben, das heißt die Bewertungen $|\cdot|'$ von L, die L/K zu einer Erweiterung bewerteter Körper machen.

Ist $|\cdot|$ diskret, also

$$|\cdot| : K \to \lambda^{\mathbb{Z}} \cup \{0\}$$

für $\lambda \in (0,1) \subseteq \mathbb{R}$ können wir unser Wissen über Erweiterungen von Dedekindringen einsetzen. Eigentlich ist die Behandlung dieses Spezialfalls nicht nötig, um den allgemeinen Fall zu untersuchen. Da wir aber schon die ganze Vorarbeit geleistet haben, machen wir es trotzdem.

Satz 4.3. *Sei*

$$|\cdot| : K \to \lambda^{\mathbb{Z}} \cup \{0\}$$

eine diskrete Bewertung auf einem Körper K und L/K eine endliche Körpererweiterung. Sei $\mathcal{O} \subseteq K$ der zu $|\cdot|$ assoziierte diskrete Bewertungsring und $\mathcal{O}_L$ sein Ganzabschluss in L. Dann sind folgende Abbildungen zueinander inverse Bijektionen

$$\begin{aligned} \{(0) \neq \mathfrak{p} \subsetneqq \mathcal{O}_L \text{ prim}\} &\leftrightarrow \{|\cdot|' \text{ Fortsetzung von } |\cdot| \text{ auf } L\} \\ \mathfrak{p} &\mapsto |\cdot|_{\mathfrak{p}} : \text{Bewertung zu } (\mathcal{O}_L)_{\mathfrak{p}} \\ \mathfrak{p}_{|\cdot|'} := \{x \in \mathcal{O}_L \mid |x|' < 1\} &\mapsfrom |\cdot|' \end{aligned}$$

Hierbei wählen wir aus der Äquivalenzklasse von Bewertungen zu $(O_L)_{\mathfrak{p}}$ diejenige aus, deren Einschränkung auf K gleich $|\cdot|$ ist.

Beweis. Nach Satz 2.14 ist $\mathcal{O}$ ein Dedekindring. Der Ganzabschluss $\mathcal{O}_L$ von $\mathcal{O}$ in L ist wieder ein Dedekindring (AZT 1). Daher sind die Lokalisierungen $(\mathcal{O}_L)_{\mathfrak{p}}$ an Primidealen $\mathfrak{p} \neq (0)$ von $\mathcal{O}_L$ nach Satz 2.14 diskrete Bewertungsringe. Sei $|\cdot|_{\mathfrak{p}}$ die zugehörige Bewertung von L. Dann wir wissen wir nun, dass die Zuordnung

$$\mathfrak{p} \mapsto |\cdot|_{\mathfrak{p}}$$

wohldefiniert ist.

Außerdem ist das Maximalideal $\mathfrak{p}(\mathcal{O}_l)_{\mathfrak{p}}$ von $(\mathcal{O}_L)_{\mathfrak{p}}$ gleich

$$\{x \in L \mid |x|_{\mathfrak{p}} < 1\}.$$

Somit gilt nach Proposition 2.5

$$\begin{aligned} \mathfrak{p} &= [\mathfrak{p}(\mathcal{O}_l)_{\mathfrak{p}}] \cap \mathcal{O}_L \\ &= \{x \in \mathcal{O}_L \mid |x|_{\mathfrak{p}} < 1\} \end{aligned}$$

Das zeigt, dass die Verkettung $\mathfrak{p} \mapsto |\cdot|_{\mathfrak{p}}$ mit $|\cdot|' \mapsto \mathfrak{p}_{|\cdot|'}$ gleich der Identität ist. Starten wir mit einer Fortsetzung $|\cdot|'$ von $|\cdot|$ auf L, so ist $\{x \in L \mid |x|' < 1\}$ das Maximalideal $\mathfrak{m}_{|\cdot|'}$ des zugehörigen diskreten Bewertungsrings und

$$\mathfrak{p}_{|\cdot|'} = \{x \in \mathcal{O}_L \mid |x|' < 1\} = \mathfrak{m}_{|\cdot|'} \cap \mathcal{O}_L$$

ist ein nichttriviales Primideal von $\mathcal{O}_L$. Wir behaupten, dass

$$(\mathcal{O}_L)_{\mathfrak{p}_{|\cdot|'}} \subseteq \mathcal{O}_{|\cdot|'}.$$

Da $|\cdot|'$ eine Fortsetzung von $|\cdot|$ ist, folgt $\mathcal{O} \subseteq \mathcal{O}_{|\cdot|'}$. Als diskreter Bewertungsring ist $\mathcal{O}_{|\cdot|'}$ ganzabgeschlossen und enthält somit auch den Ganzabschluss $\mathcal{O}_L$. Außerdem ist $\mathcal{O}_{|\cdot|'}$ lokal und somit faktorisiert $\mathcal{O}_L \hookrightarrow \mathcal{O}_{|\cdot|'}$ über die Lokalisierung $(\mathcal{O}_L)_{\mathfrak{p}_{|\cdot|'}}$.

Nun ist $(\mathcal{O}_L)_{\mathfrak{p}_{|\cdot|'}}$ bereits ein diskreter Bewertungsring. Wir betrachten die Surjektion

$$L^\times / (\mathcal{O}_L)^\times_{\mathfrak{p}_{|\cdot|'}} \twoheadrightarrow L^\times / \mathcal{O}^\times_{|\cdot|'}$$

Beide Gruppen sind isomorph zu $\mathbb{Z}$, da sie isomorph zu den jeweiligen Wertegruppen sind. Jede Surjektion $\mathbb{Z} \twoheadrightarrow \mathbb{Z}$ ist aber ein Isomorphismus. Daher folgt

$$(\mathcal{O}_L)_{\mathfrak{p}_{|\cdot|'}} = \mathcal{O}_{|\cdot|'}$$

und die Verkettung von $|\cdot|' \mapsto \mathfrak{p}_{|\cdot|'}$ mit $\mathfrak{p} \mapsto |\cdot|_{\mathfrak{p}}$ ist auch die Identität. □

Korollar 4.4. *In der Situation von Satz 4.3 gibt es nur endlich viele Fortsetzungen von $|\cdot|$ auf L.*

Beweis. Das liegt daran, dass für die Erweiterung von Dedekindringen $\mathcal{O}_L/\mathcal{O}$ über dem Maximalideal von $\mathcal{O}$ nur endlich viele Primideale $\mathfrak{p} \subseteq \mathcal{O}_L$ liegen. □

Nun wollen wir die Aussage von Satz 4.3 in größerer Allgemeinheit, also nicht nur für diskrete Bewertungen zeigen. Der Schlüssel ist der Fortsetzungssatz von Chevalley. Bevor wir ihn formulieren, definieren wir das Konzept von Dominanz:

Definition 4.5. Seien A, B nullteilerfreie Ringe und $\mathfrak{p} \subseteq A$ und $\mathfrak{q} \subseteq B$ Primideale. Wir sagen, dass $(B, \mathfrak{q})$ das Paar $(A, \mathfrak{p})$ *dominiert*, falls $A \subseteq B$ und $\mathfrak{q} \cap A = \mathfrak{p}$. In dem Fall schreiben wir $(A, \mathfrak{p}) \subseteq (B, \mathfrak{q})$.

Proposition 4.6. *Sei K ein Körper. Dann sind die Paare $(\mathcal{O}, \mathfrak{m})$ für einen Bewertungsring $\mathcal{O}$ von K mit seinem Maximalideal $\mathfrak{m}$ genau die maximalen Elemente bezüglich Dominanz von Paaren $(A, \mathfrak{p})$ mit $A \subseteq K$.*

Beweis. Sei $\mathcal{O}$ ein Bewertungsring von K mit Maximalideal $\mathfrak{m}$ und $(A, \mathfrak{p})$ mit $A \subseteq K$, das $(\mathcal{O}, \mathfrak{m})$ dominiert. Wir wollen zeigen, dass $(A, \mathfrak{p}) = (\mathcal{O}, \mathfrak{m})$. Wenn $\mathcal{O} = K$ ist, ist das klar. Daher nehmen wir im folgenden $\mathcal{O} \neq K$ und somit $\mathfrak{m} \neq 0$ an.

Angenommen $\mathcal{O} \subsetneq A$. Dann gibt es ein Element $a \in A$ it $a \notin \mathcal{O}$. Da ein Bewertungsring von K ist, muss dann $a^{-1} \in \mathcal{O}$ gelten, also wegen $\mathcal{O} \subseteq A$ auch $a^{-1} \in A$. Als Einheit von A ist a^{-1} nicht in $\mathfrak{p}$ enthalten. Nach Annahme gilt $\mathfrak{m} \subseteq \mathfrak{p}$, also ist a^{-1} auch nicht in $\mathfrak{m}$ enthalten. Da $\mathcal{O}$ lokal ist, ist a^{-1} eine Einheit in $\mathcal{O}$, also $a \in O$, was im Widerspruch zur Annahme steht.

Wir nehmen nun an, dass $(\mathcal{O}, \mathfrak{m})$ maximal ist bezüglich Dominanz. Wir bemerken zunächst, dass $\mathcal{O}$ wegen der Maximalität von $(\mathcal{O}, \mathfrak{m})$ ein lokaler Ring mit Maximalideal $\mathfrak{m}$ ist (ansonsten würde $(\mathcal{O}_{\mathfrak{m}}, \mathfrak{m}\mathcal{O}_{\mathfrak{m}})$ das Paar $(\mathcal{O}, \mathfrak{m})$ dominieren und wäre echt größer). Wäre $\mathcal{O}$ kein Bewertungsring, so gäbe es $x \in K^\times$ mit $x, x^{-1} \in \mathcal{O}$. Dann sind $\mathcal{O}[x]$ und $\mathcal{O}[x^{-1}]$ echt größer als $\mathcal{O}$. Wäre $\mathfrak{m}\mathcal{O}[x]$ ein echtes Ideal von $\mathcal{O}[x]$, so gäbe es ein Primideal $\mathfrak{p} \subseteq \mathcal{O}[x]$, das $\mathfrak{m}$ enthält, also $(\mathcal{O}, \mathfrak{m}) \subsetneq (\mathcal{O}[x], \mathfrak{p})$, was aber wegen der Maximalität von $(\mathcal{O}, \mathfrak{m})$ ausgeschlossen ist. Daher gilt

$$\mathfrak{m}\mathcal{O}[x] = \mathcal{O}[x].$$

Die analoge Argumentation für $\mathcal{O}[x^{-1}]$ ergibt

$$\mathfrak{m}\mathcal{O}[x^{-1}] = \mathcal{O}[x^{-1}].$$

Es gibt folglich $a_0, \dots, a_m, b_0, \dots, b_n \in \mathfrak{m}$ mit

$$\sum_{i=0}^{m} a_i x^i = 1, \sum_{i=0}^{n} b_i x^{-i} = 1.$$

Wir nehmen an, dass die Darstellungen so gewählt sind, dass m und n minimal sind. Außerdem können wir annehmen, dass $m \neq n$ gilt. Ansonsten ersetzen wir x durch x^{-1}.

Es gilt

$$\sum_{i=1}^{m} a_i x^i = 1 - a_0 \in \mathcal{O} \setminus \mathfrak{m} = \mathcal{O}^\times.$$

Wir können daher durch $1 - a_0$ teilen und erhalten eine Darstellung

$$1 = \sum_{i=1}^{m} c_i x^i, c_i = \frac{a_i}{1 - a_0}.$$

Multiplizieren mit x^{-n} ergibt

$$x^{-n} = \sum_{i=1}^{m} c_i x^{i-n}.$$

Das setzen wir in die Gleichung $1 = \sum_{i=0}^{n} b_i x^{-i}$ ein:

$$1 = \sum_{i=0}^{n-1} b_i x^{-i} + \sum_{i=1}^{m} b_n c_i x^{i-n}$$

In dieser Darstellung sind alle Exponenten von x in $\{-(n-1), \dots, 0\}$ enthalten, da nach Annahme $m \leq n$ gilt. Das widerspricht aber der Maximalität von n. Daher ist unsere Annahme $x, x' \notin O$ nicht korrekt und es folgt, dass $\mathcal{O}$ ein Bewertungsring ist. Außerdem muss $\mathfrak{m}$ das Maximalideal sein, denn sonst wäre

$$(\mathcal{O}_m) \subsetneqq (\mathcal{O}_m, \mathfrak{m}\mathcal{O}_m).$$

□

Satz 4.7 (Fortsetzungssatz von Chevalley)**.** *Sei A ein Teilring eines Körpers und $\mathfrak{p} \subseteq A$ ein Primideal. Dann gibt es einen Bewertungsring $\mathcal{O}$ von K, so dass $(\mathcal{O}, \mathfrak{m}_\mathcal{O})$ das Paar $(A, \mathfrak{p})$ dominiert.*

Beweis. Wir betrachten die Menge

$$\mathcal{M} := \{(B, \mathfrak{q}) \mid B \subseteq K, (A, \pi) \subseteq (B, \mathfrak{q})\}.$$

Sie ist nicht leer, da $(A, \mathfrak{p}) \in \mathcal{M}$ und partiell geordnet durch Dominanz von Paaren. Wir wollen zeigen, dass $\mathcal{M}$ ein maximales Element besitzt. Dafür überzeugen wir uns davon, dass jede aufsteigende Kette

$$(B_1, q_1) \subseteq (B_2, \mathfrak{q}_2) \subseteq (B_3, \mathfrak{q}_3) \subseteq \dots$$

eine obere Schranke besitzt, nämlich

$$\left(\bigcup_{i=1}^{\infty} B_i, \bigcup_{i=1}^{\infty} \mathfrak{q}_i \right).$$

□

Korollar 4.8. *Sei $(K, |\cdot|)$ ein bewerteter Körper und L/K eine Körpererweiterung. Dann gibt es eine Fortsetzung $|\cdot|'$ von $|\cdot|$ auf L.*

Beweis. Sei $\mathcal{O}$ der Bewertungsring zu $|\cdot|$ und $\mathfrak{m}$ sein Maximalideal. Dann gibt es nach dem Fortsetzungssatz von Chevalley einen Bewertungsring $\mathcal{O}'$ von L mit Maximalideal $\mathfrak{m}'$, so dass $(\mathcal{O}', \mathfrak{m}')$ das Paar $(\mathcal{O}, \mathfrak{m})$ dominiert.

Das bedeutet, dass $\mathcal{O} \subset \mathcal{O}' \cap K$ und $\mathfrak{m} = \mathfrak{m}' \cap \mathcal{O}$. Das bedeutet, dass $(\mathcal{O}' \cap K, \mathfrak{m}' \cap K)$ das Paar $(\mathcal{O}, \mathfrak{m})$ dominiert und noch dazu den gleichen Quotientenkörper hat. Da aber nach Proposition 4.6 maximal ist unter diesen Paaren, folgt $\mathcal{O} = \mathcal{O}' \cap K$, das heißt die entsprechende Bewertung $|\cdot|'$ setzt die Bewertung $|\cdot|$ fort. □

Um die Verallgemeinerung von Satz 4.3 auf beliebige Bewertungsringe zu zeigen, brauchen wir folgendes Lemma. Für diskrete Bewertungsringe wissen wir das bereits.

Lemma 4.9. *Jeder Bewertungsring ist ganzabgeschlossen.*

Beweis. Sei $\mathcal{O}$ ein Bewertungsring mit Maximalideal $\mathfrak{m}$. Sei $x \in K := K(\mathcal{O})$ ganz über $\mathcal{O}$. Das heißt es gibt ein normiertes Polynom

$$P(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0 \in \mathcal{O}[T]$$

mit $P(x) = 0$. Ist $x \notin \mathcal{O}$, so folgt $x^{-1} \in \mathcal{O}$ und sogar $x^{-1} \in \mathfrak{m}$ (da sonst x^{-1} eine Einheit wäre und somit $x \in \mathcal{O}$). Daher gilt

$$1 = -a_{n-1}x^{-1} - a_{n-2}x^{-2} - \ldots - a_0x^{-n} \in \mathfrak{m},$$

was ausgeschlossen ist, da $\mathfrak{m}$ ein Primideal ist. □

Satz 4.10. *Sei K ein Körper in $A \subseteq K$ ein Teilring und A_K sein Ganzabschluss in K. Wir definieren*

$$\mathbb{V} := \{A \subseteq \mathcal{O} \text{ Bewertungsring, } \mathfrak{m}_\mathcal{O} \cap A \text{ ist maximal}\}$$

Dann gilt

$$A_K = \bigcap_{\mathcal{O} \in \mathbb{V}} \mathcal{O}.$$

Beweis. Da alle $\mathcal{O} \in \mathbb{V}$ nach Lemma 4.9 ganzabgeschlossen sind, folgt

$$A_K \subseteq \bigcap_{\mathcal{O} \in \mathbb{V}} \mathcal{O}.$$

Sei nun $x \in \bigcap_{\mathcal{O} \in \mathbb{V}} \mathcal{O}$. Ist

$$x \in A_K[x^{-1}],$$

so sind wir fertig, da es dann $a_0, \ldots, a_{n-1} \in A_K$ gibt mit

$$x = a_0 + a_1x^{-1} + \ldots + a_{n-1}x^{n-1}$$

Dann ist x Nullstelle des normierten Polynoms

$$T^n - a_0T^{n-1} - a_1T^{n-2} - \ldots - a_{n-1} \in A_K[T],$$

also ganz über A_K. Da A_K ganzabgeschlossen ist, folgt $x \in A_K$.

Wir nehmen nun an

$$x \notin A_K[x^{-1}].$$

Dann ist x^{-1} keine Einheit in $A_K[x^{-1}]$ und somit in einem Maximalideal $\mathfrak{m}$ von $A_K[x^{-1}]$ enthalten. Nach Satz 4.7 wird $(A_K[x^{-1}], \mathfrak{m})$ dominiert von einem Paar $(\mathcal{O}, \mathfrak{m}_\mathcal{O})$ bestehend aus einem Bewertungsring $\mathcal{O}$ und seinem Maximalideal $\mathfrak{m}_\mathcal{O}$. Wir wollen nu zeigen, dass

$\mathcal{O} \in \mathbb{V}$ ist. Da $x^{-1} \in \mathfrak{m} \subseteq \mathfrak{m}_{\mathcal{O}}$, ist dann keine Einheit in $\mathcal{O}$ und somit $x \in \mathcal{O}$. Aber das steht im Widerspruch zur Annahme

$$x \in \bigcap_{\mathcal{O} \in \mathbb{V}} \mathcal{O}.$$

Um zu zeigen, dass $\mathcal{O} \in \mathbb{V}$ ist, müssen wir zeigen, dass $\mathfrak{m}_{\mathcal{O}} \cap A$ maximal ist. Wir zeigen zunächst, dass $\mathfrak{m}_{\mathcal{O}} \cap A_K$ maximal ist. Dafür betrachten wir den Ringhomomorphismus

$$\pi : A_K \to {}^{A_K[x^{-1}]}/_{\mathfrak{m}}.$$

Da x^{-1} in $\mathfrak{m}$ enthalten ist, ist $\mathfrak{p}$ surjektiv. Der Kern ist gleich

$$\begin{aligned} \mathfrak{m} \cap A_K &= \mathfrak{m}_{\mathcal{O}} \cap A_K[x^{-1}] \cap A_K \\ &= \mathfrak{m}_{\mathcal{O}} \cap A_K \end{aligned}$$

Also ist

$${}^{A_K}/_{\mathfrak{m}_{\mathcal{O}} \cap A_K} \xrightarrow{\sim} {}^{A_K[x^{-1}]}/_{\mathfrak{m}}$$

ein Körper und $\mathfrak{m}_{\mathcal{O}} \cap A_K$ maximal. Nun betrachten wir

$$\varphi : {}^{A}/_{\mathfrak{m}_{\mathcal{O}} \cap A} \hookrightarrow {}^{A_K}/_{\mathfrak{m}_{\mathcal{O}} \cap A_K}.$$

Da $A \to A_K$ ganz ist, ist auch φ ganz. Außerdem ist ${}^{A_K}/_{\mathfrak{m}_{\mathcal{O}} \cap A_K}$ ein Körper. Dann ist auch ${}^{A}/_{\mathfrak{m}_{\mathcal{O}} \cap A}$ ein Körper, denn für $x \in {}^{A}/_{\mathfrak{m}_{\mathcal{O}} \cap A} \setminus \{0\}$ ist $x^{-1} \in {}^{A_K}/_{\mathfrak{m}_{\mathcal{O}} \cap A_K}$ ganz über ${}^{A}/_{\mathfrak{m}_{\mathcal{O}} \cap A}$.

Das heißt, es gibt $a_0, \ldots, a_{n-1} \in {}^{A}/_{\mathfrak{m}_{\mathcal{O}} \cap A}$ mit

$$x^{-n} + a_{n-1}x^{-(n-1)} + \ldots + a_1 x^{-1} + a_0 = 0$$

Das formen wir um zu

$$\begin{aligned} 1 &= -a_{n-1}x - a_{n-2}x^2 - \ldots - a_0 x^n \\ &= x(-a_{n-1} - a_{n-2}x - \ldots - a_0 x^{n-1}) \end{aligned}$$

Daher ist x invertierbar oder mit anderen Worten $x^{-1} \in {}^{A}/_{\mathfrak{m}_{\mathcal{O}} \cap A}$. Wir haben nun gezeigt, dass $A \cap \mathfrak{m}_{\mathcal{O}}$ maximal ist, also $\mathcal{O} \in \mathbb{V}$. Das beschließt den Beweis. □

Korollar 4.11. *Sei $(K, |\cdot|)$ ein bewerteter Körper mit Bewertungsring $\mathcal{O}$. Für eine Körpererweiterung L/K sei $\mathcal{O}_L$ der Ganzabschluss von $\mathcal{O}$ in L. Dann gilt*

$$\mathcal{O}_L = \bigcap_{\substack{|\cdot|' : L \to \Gamma \cup \{0\} \\ \text{Fortsetzung von } |\cdot|}} \mathcal{O}_{|\cdot|'}$$

Beweis. Man wendet Satz 4.10 auf $\mathcal{O}$ an und beachtet, dass die Bewertungsringe von L, die $(\mathcal{O}, \mathfrak{m}_{\mathcal{O}})$ dominieren, gerade die Fortsetzungen von $|\cdot|$ nach L entsprechen. □

Um nun tatsächlich ein Analogon zu Korollar 4.4 zu erhalten, brauchen wir nur noch die folgenden zwei Aussagen.

Lemma 4.12. *Seien $\mathcal{O}_1, \ldots, \mathcal{O}_n$ Bewertungsringe eines Körpers K mit Maximalidealen $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$. Wir setzen*

$$R := \bigcap_{i=1}^{n} \mathcal{O}_i \text{ und } \mathfrak{p}_i = R \cap \mathfrak{m}_i.$$

Dann gilt für $i = 1, \ldots, n$

$$\mathcal{O}_i = R_{\mathfrak{p}_i}.$$

Beweis. Da $\mathcal{O}_i$ lokal ist, gilt $R_{\mathfrak{p}_i} \subseteq \mathcal{O}_i$. Für die umgekehrte Inklusion nehmen wir ein Element $a_i \in \mathcal{O}_i$ und wollen zeigen, dass a_i schon in $R_{\mathfrak{p}_i}$ liegt. Dafür müssen wir $c \in R \setminus \mathfrak{p}_i$ finden, so dass $ac \in R$. Dann ist

$$a = \frac{ac}{c} \in R_{\mathfrak{p}_i}.$$

Sei $k_i = \mathcal{O}_i/\mathfrak{m}_i$ der Restklassenkörper von $\mathcal{O}_i$. Wir wählen eine Primzahl p, so dass für $i = 1, \ldots, n$ gilt:

- $p > \operatorname{char}(k_i)$
- k_i enthält keine primitive p-te Einheitswurzel

Wir setzen $b = 1 + a + a^2 + \ldots + a^{p-1}$. Dann ist $b \neq 0$. Ansonsten wäre b eine primitive p-te Einheitswurzel und somit auch $[b]_i \in k_i$ eine primitive p-te Einheitwurzel, aber das haben wir ausgeschlossen. Daher ist b invertierbar in K und wir setzen $c = b^{-1}$.

Wir wollen nun zeigen, dass $c \in R \setminus \mathfrak{p}_i$ und $ac \in R$. Dafür reicht es für $j = 1, \ldots, n$ die Inklusionen $c \in \mathcal{O}_j$, $ac \in \mathcal{O}_j$ und $c \notin \mathfrak{p}_i$ zu zeigen.

Falls $a \in \mathcal{O}_j$ ist, unterscheiden wir zwei Fälle:

1. $[a]_j = 1$ in k_j. Dann ist

$$\begin{aligned}[b]_j &= 1 + [a]_j + [a]_j^2 + \ldots + [a]_j^{p-1} \\ &= 1 + 1 + 1 + \ldots + 1 \\ &= p \neq 0,\end{aligned}$$

   da $p > \operatorname{char}(k_j)$.

2. $[a]_j \neq 1$ in k_j. Dann ist

$$[b]_j = \frac{1 - [a]_j^p}{1 - [a]_j} \neq 0,$$

   da k_j keine primitive p-te Einheitswurzel enthält.

In beiden Fällen ist $[b]_j \in k_i^\times$, also $b \in \mathcal{O}_j^\times$. Dann gilt auch $c = b^{-1} \in \mathcal{O}_j^\times$ und $ac \in \mathcal{O}_j$. Insbesondere für $j = i$ erhalten wir $c \notin \mathfrak{p}_i$.

Falls $a \notin \mathcal{O}_j$, folgt $a^{-1} \in \mathcal{O}_j$ und das gleiche Argument wie eben zeigt

$$1 + a^{-1} + a^{-2} + \ldots + {}^{-(p-1)} \in \mathcal{O}_j^\times.$$

Daraus folgt

$$c = b^{-1} = a^{-(p-1)} \left(1 + a^{-1} + a^{-2} + \ldots + {}^{-(p-1)}\right)^{-1} \in \mathcal{O}_j$$

$$ac = ab^{-1} = a^{-(p-2)} \left(1 + a^{-1} + a^{-2} + \ldots + {}^{-(p-1)}\right)^{-1} \in \mathcal{O}_j$$

Damit erfüllt c alle Bedingungen und es folgt

$$a = \frac{ac}{c} \in R_{\mathfrak{p}_i}.$$

□

Satz 4.13. *Sei $(K, |\cdot|)$ ein bewerteter Körper und L/K eine algebraische Erweiterung mit endlichem Separabilitätsgrad $[L : K]_s$. Dann gilt für die Anzahl n der Fortsetzungen von $|\cdot|$ nach L*

$$n \leq [L : K]_s$$

Insbesondere ist n endlich.

Beweis. [EP05, Theorem 3.29.] □

Wir haben nun alles beisammen, um die Verallgemeinerung von Korollar 4.4 auf beliebige Bewertungsringe zu beweisen.

Satz 4.14. *Sei $(K, |\cdot|)$ ein bewerteter Körper mit Bewertungsring $\mathcal{O}$. Für eine endliche Körpererweiterung L/K gibt es nur endlich viele Fortsetzungen $|\cdot|'$ von $|\cdot|$ nach L, sowie eine Bijektion*

$$\begin{aligned} \{\mathfrak{p} \subseteq \mathcal{O}_L \text{ maximal}\} &\longleftrightarrow \{\text{Fortsetzungen von } |\cdot|\} \\ \mathfrak{p} &\longmapsto (\mathcal{O}_L)_{\mathfrak{p}} \\ \{x \in \mathcal{O}_L \mid |x|' < 1\} &\longleftarrow\!\shortmid |\cdot|' \end{aligned}$$

Außerdem gilt

$$\mathcal{O}_L = \bigcap_{\substack{\mathfrak{p} \subseteq \mathcal{O}_L \\ \text{maximal}}} (\mathcal{O}_L)_{\mathfrak{p}}.$$

Beweis. Nach Satz 4.13 gibt es nur endlich viele solche Fortsetzungen. Wir bezeichnen mit

$$\mathcal{O}_1, \dots, \mathcal{O}_n \subseteq L$$

die dazugehörigen Bewertungsringe mit jeweiligen Maximalidealen $\mathfrak{m}_i \subseteq \mathcal{O}_i$. Dann gilt nach Korollar 4.11

$$\mathcal{O}_L = \bigcap_{i=1}^{n} \mathcal{O}_i.$$

Das ist ein endlicher Durchschnitt von Bewertungsringen. Wir können darauf Lemma 4.12 anwenden, das besagt, dass

$$\mathcal{O}_i = (\mathcal{O}_L)_{\mathfrak{p}_i},$$

wobei $\mathfrak{p}_i = \mathcal{O}_L \cap \mathfrak{m}_i$.

Wir müssen uns nun noch davon überzeugen, dass $\mathfrak{p}_i$ ein Maximalideal ist. Sei $\mathfrak{m}$ das Maximalideal von $\mathcal{O}$. Da $\mathcal{O}_i$ der Bewertungsring einer Fortsetzung von $|\cdot|$ ist, gilt

$$\begin{aligned} \mathfrak{m} &= \mathcal{O} \cap \mathfrak{m}_i \\ &= \mathcal{O} \cap \mathcal{O}_L \cap \mathfrak{m}_i \\ &= \mathcal{O} \cap \mathfrak{p}_i. \end{aligned}$$

Die Inklusion

$$k := {}^{\mathcal{O}}\!/_{\mathfrak{m}} \hookrightarrow {}^{\mathcal{O}_L}\!/_{\mathfrak{p}_i}$$

ist ganz, weil $\mathcal{O} \hookrightarrow \mathcal{O}_L$ ganz ist. Jede nullteilerfreie ganze Erweiterung eines Körpers ist wieder ein Körper, also ist $\mathfrak{p}_i$ maximal.

Das einzige, das für den Beweis noch fehlt, ist zu zeigen, dass jedes Maximalideal $\mathfrak{M}$ von $\mathcal{O}_L$ von der Form $\mathfrak{m}_i \cap \mathcal{O}_L$ ist. Nach Chevalleys Fortsetzungssatz (Satz 4.7) gibt es einen Bewertungsring $(\mathcal{O}', \mathfrak{m}')$ von L, der $(\mathcal{O}_L, \mathfrak{M})$ dominiert. Dann dominiert $(\mathcal{O}', \mathfrak{m}')$ auch $(\mathcal{O}, \mathfrak{m})$ und folglich ist $(\mathcal{O}', \mathfrak{m}')$ eine Fortsetzung von $(\mathcal{O}, \mathfrak{m})$, also gleich einem der Bewertungsringe $(\mathcal{O}_i, \mathfrak{m}_i)$. Insbesondere gilt

$$\mathfrak{M} = \mathfrak{m}' \cap \mathcal{O}_L = \mathfrak{m}_i \cap \mathcal{O}_L.$$

□

4.2. **Erweiterungen vollständig bewerteter Körper.** Wir betrachten in diesem Abschnitt vollständig reell bewertete Körper $(K, |\cdot|)$. Unser Ziel ist es zu zeigen, dass es für jede endliche Erweiterung L/K nur eine Fortsetzung der Bewertung $|\cdot|$ auf L gibt. Der springende Punkt ist die Erkenntnis, dass wir für jede Fortsetzung $|\cdot|'$ von $|\cdot|$ auf L den Körper L als normierten K-Vektorraum auffassen können. Dann benutzen wir, dass für endlich-dimensionale K-Vektorräume alle Normen äquivalent sind. Das ist das Resultat, das für $\mathbb{R}$-Vektorräume wohl bekannt ist. Es gilt aber für beliebige vollständige reell bewertete Grundkörper.

Zunächst klären wir die Begriffe.

Definition 4.15. Sei $(K, |\cdot|)$ ein reell bewerteter Körper und V ein K-Vektorraum. Eine *Norm* auf V ist eine Funktion

$$\|\cdot\| : V \longrightarrow \mathbb{R}_{\geq 0}$$

mit den Eigenschaften

(i) $\|x\| = 0 \Leftrightarrow x = 0$
(ii) $\|\alpha x\| = |\alpha|\|x\|$
(iii) $\|x + y\| \leq \|x\| + \|y\|$

für alle $x, y \in V$, $\alpha \in K$.

Beispiel 4.16. Wir können K^n immer mit der Supremumsnorm

$$\|(\alpha_1, \ldots, \alpha_n)\| := \max_{i=1,\ldots,n} \{\|\alpha_i\|\}$$

versehen. Dann ist K^n ein vollständig normierter K-Vektorraum.

Definition 4.17. Zwei Normen $\|\cdot\|_1$ und $\|\cdot\|_2$ auf einem K-Vektorraum V heißen *äquivalent*, wenn es Konstanten $c_1, c_2 > 0$ gibt, so dass für alle $x \in V$ gilt

$$c_1\|x\|_1 \leq \|x\|_2 \leq c_2\|x\|_1.$$

Eine Norm $\|\cdot\|$ auf einem K-Vektorraum V induziert eine Metrik

$$d(x, y) := \|x - y\|$$

und damit eine Topologie auf V.

Lemma 4.18. *Zwei äquivalente Normen $\|\cdot\|_1$ und $\|\cdot\|_2$ auf einem K-Vektorraum V induzieren auf V die gleiche Topologie.*

Beweis. Gibt es Konstanten $c_1, c_2 > 0$ wie in der Aussage der Definition, dann folgt für jedes Element $x \in V$

$$B_{\|\cdot\|_1}(x, c_2\varepsilon) \subseteq B_{\|\cdot\|_2}(x, \varepsilon) \subseteq B_{\|\cdot\|_1}\left(x, \frac{\varepsilon}{c_1}\right).$$

Daher stimmen die Umgebungsbasen von x bezüglich $\|\cdot\|_1$ und $\|\cdot\|_2$ überein und die Topologien sind gleich. □

Für $x \in V$ und $A \subseteq V$ setzen wir

$$d(x, A) := \inf_{y \in A} d(x, y).$$

Satz 4.19. *Sei $(K, |\cdot|)$ ein vollständiger reell bewerteter Körper, $(V, \|\cdot\|)$ ein normierter K-Vektorraum, und $W \subseteq V$ ein endlich-dimensionaler Untervektorraum mit Basis $\{w_1, \ldots, w_n\}$. Dann gilt*

(i) Die durch den Isomorphismus

$$\varphi : K^n \xrightarrow{\sim} W$$
$$(\alpha_1, \ldots, \alpha_n) \mapsto \alpha_1 w_1 + \ldots + \alpha_n w_n$$

von der Supremumsnorm auf K^n induzierte Norm auf W ist äquivalent zu $\|\cdot\|_W$.

(ii) Für jedes $x \in V \setminus W$ gilt

$$d(x, W) > 0.$$

Beweis. Wir zeigen (i) und (ii) gleichzeitig per Induktion über die Dimension n von W. Für $n = 0$ ist die Aussage klar. Der Induktionsschritt hat folgende Struktur:

$$\text{(ii) für } n-1 \overset{(1)}{\Rightarrow} \text{(i) für } n \overset{(2)}{\Rightarrow} \text{(ii) für } n$$

(1) Wir bezeichnen mit

$$\|\cdot\|_{\sup} : W \to \mathbb{R}_{\geq 0}$$

die von der Supremumsnorm auf K^n induzierte Norm. Dann gilt für ein Element $\sum_{i=1}^n \alpha_i w_i$ von W

$$\begin{aligned}\|\sum_{i=1}^n \alpha_i w_i\| &\leq \sum_{i=1}^n \|\alpha_i w_i\| = \sum_{i=1}^n |\alpha_i| \cdot \|w_i\| \\ &\leq \sup_{i=1,\ldots,n} |\alpha_i| \cdot \underbrace{\sum_{i=1}^n \|w_i\|}_{=:c_2} \\ &= c_2 \cdot \|\sum_{i=1}^n \alpha_i w_i\|_{\sup}.\end{aligned}$$

Um eine Ungleichung der Form $\|\cdot\|_{\sup} \leq c_1 \|\cdot\|$ zu produzieren, betrachten wir für $i = 1, \ldots, n$ den Untervektorraum von W, der von

$$w_1, \ldots, w_{i-1}, w_{i+1}, \ldots, w_n$$

aufgespannt wird. Nach Annahme gilt

$$d(-w_i, W_i) > 0$$

für alle i. Sei

$$c_1 := \min_{i=1,\ldots,n} d(-w_i, W_i)$$

Für $w = \sum_{i=1}^n \alpha_i w_i \in W \setminus \{0\}$ wählen wir $j \in \{1, \ldots, n\}$ mit $|\alpha_i| = \sup_{i=1,\ldots,n} |\alpha_i|$. Dann folgt

$$\begin{aligned}\|w\| &= |\alpha_j| \cdot \left\| \frac{\alpha_1}{\alpha_j} w_1 + \ldots + w_j + \ldots + \frac{\alpha_n}{\alpha_j} w_n \right\| \\ &\geq |\alpha_j| \cdot d(-w_j, W_j) \geq c_1 \sup_{i=1,\ldots,n} |\alpha_i| \\ &= c_1 \cdot \|w\|_{\sup}.\end{aligned}$$

(2) Sei $x \in V \setminus W$. Wäre $d(x, W) = 0$, so gäbe es für jedes $k \in \mathbb{N}$ ein Element $x_k \in W$ mit

$$d(x_k, x) \leq \frac{1}{k}.$$

Dann ist $(x_k)_{k\in\mathbb{N}}$ eine Cauchyfolge in W. Nach Annahme ist die Norm $\|\cdot\|_W$ äquivalent zur Supremumsnorm $\|\cdot\|_{\sup}$ und bezüglich dieser ist W vollständig. Also konvergiert die Cauchyfolge $(x_k)_{k\in\mathbb{N}}$ gegen ein Element $y \in W$. Dann gilt für $k \in \mathbb{N}$

$$\|x - y\| \leq \|x - x_k\| + \|x_k - y\|$$

und beide Summanden werden für ausreichend große k beliebig klein. Daher folgt $x = y \in W$, was im Widerspruch zur Annahme steht.

□

Korollar 4.20. *Sei $(K, |\cdot|)$ ein vollständiger reell bewerteter Körper und V ein endlich-dimensionaler K-Vektorraum. Dann sind alle Normen auf V äquivalent.*

Beweis. Das ist die Aussage von Satz 4.19 (i) mit $W = V$. □

Korollar 4.21. *Sei $(K, |\cdot|)$ ein vollständiger reell bewerteter Körper und $(V, \|\cdot\|)$ ein normierter K-Vektorraum. Dann ist jeder endlich-dimensionale Untervektorraum $W \subseteq V$ abgeschlossen.*

Beweis. Für $x \in V \setminus W$ ist nach Satz 4.19 (ii)

$$\varepsilon := d(x, W) > 0.$$

Dann ist $B(x, \varepsilon)$ in W enthalten. Das zeigt, dass $V \setminus W$ offen und somit W abgeschlossen ist. □

Korollar 4.22. *Sei $(K, |\cdot|)$ ein vollständiger reell bewerteter Körper und L/K eine endliche Körpererweiterung. Dann gibt es eine eindeutig bestimmte Fortsetzung von $|\cdot|$ nach L.*

Beweis. Nach Korollar 4.8 existiert mindestens eine Fortsetzung $|\cdot|'$ von $|\cdot|$ auf L. Diese macht L zu einem endlich dimensionalen normierten K-Vektorraum. Jede weitere Fortsetzung von $|\cdot|$ definiert nach Korollar 4.20 eine äquivalente Norm und somit die gleiche Topologie auf L. Daher sind die entsprechenden Bewertungen nach Proposition 3.32 äquivalent. Da beide Fortsetzungen von $|\cdot|$ sind, sind sie sogar gleich. □

Beispiel 4.23. Wir betrachten den vollständigen Körper $\mathbb{Q}_p$ und die Erweiterung

$$L = \mathbb{Q}_p[\sqrt{p}].$$

Die eindeutige Fortsetzung $|\cdot|_L$ der p-adischen Bewertung $|\cdot|_p$ auf L muss wegen der Multiplikativität von Bewertungen

$$|\sqrt{p}|_L = \sqrt{|p|_p} = \frac{1}{\sqrt{p}}$$

erfüllen. Wir können darauf auch noch aus einem anderen Blickwinkel schauen. Der Bewertungsring der p-adischen Bewertung $|\cdot|_p$ in $\mathbb{Q}_p$ ist $\mathbb{Z}_p$. Sei $\mathcal{O} = (\mathbb{Z}_p)_L$ der Ganzabschluss von $\mathbb{Z}_p$ in L. Nach Satz 4.14 entsprechen den Maximalideale von $\mathcal{O}$ den Fortsetzungen von $|\cdot|_p$. Da es nur eine Fortsetzung gibt, ist $\mathcal{O}$ lokal. Noch dazu ist $\mathcal{O}$ ein Dedekindring, also ist $\mathcal{O}$ ein diskreter Bewertungsring. In $\mathcal{O}$ gilt

$$p = \sqrt{p}^2,$$

also verzweigt p in L. Nach der fundamentalen Gleichung gilt

$$2 = [L : \mathbb{Q}_p] = e \cdot f \cdot 1.$$

Es folgt $e = 2$ und $f = 1$. Somit ist $(\sqrt{p})$ ein Primideal in $\mathcal{O}$, genauer gesagt das eindeutig bestimmte Maximalideal. Jedes Element $x \in \mathcal{O}$ kann man in der Form

$$x = u(\sqrt{p})^n$$

für eine Einheit $u \in \mathcal{O}^\times$ und $n \in \mathbb{N}$ schreiben. Dann folgt

$$|x|_L = |\sqrt{p}|^n = \frac{1}{\sqrt{p^n}}$$

4.3. **Verzweigung und Trägheit.** Wir betrachten eine endliche Erweiterung $(L, |\cdot|_L)/(K, |\cdot|_K)$ nichtarchimedisch bewerteter Körper. Seien $(\mathcal{O}_K, \mathfrak{m}_K)$ und $(\mathcal{O}_L, \mathfrak{m}_L)$ die zugehörigen Bewertungsringe. Da

$$\mathfrak{m}_K = \mathcal{O}_K \cap \mathfrak{m}_L$$

erhalten wir eine induzierte Erweiterung der Restklassenkörper

$$k := {}^{\mathcal{O}_K}\!/_{\mathfrak{m}_K} \hookrightarrow {}^{\mathcal{O}_L}\!/_{\mathfrak{m}_L} =: \ell.$$

Der *Trägheitsgrad* von L/K ist definiert als

$$f := [\ell : k].$$

Da $|\cdot|_L$ eine Fortsetzung von $|\cdot|_K$ ist, ist die Wertegruppe von K in der von L enthalten:

$$|K^\times|_K \subseteq |L^\times|_L.$$

Wir definieren den *Verzweigungsindex* von L/K als

$$e := \left(|L^\times|_L : |K^\times|_K\right).$$

Beispiel 4.24. Wir wollen uns davon überzeugen, dass die Definition der Verzweigungsindex und des Trägheitsgrades kompatibel mit den entsprechenden Begriffen sind, die wir aus der Welt der Dedekindringe kennen.

Wir betrachten einen Dedekindring A mit Quotientenkörper K. Für eine endliche Erweiterung L/K sei $B = A_L$ der Ganzabschluss von A in L. Wir wählen ein Primideal $\mathfrak{P} \subseteq B$ und setzen $\mathfrak{p} = \mathfrak{P} \cap A$. Dann sind die Lokalisierungen $A_\mathfrak{p}$ und $B_\mathfrak{P}$ diskrete Bewertungsringe, die die Erweiterung L/K zu einer Erweiterung bewerteter Körper machen. Da

$$k(\mathfrak{p}) = {}^{A}\!/_{\mathfrak{p}} \xrightarrow{\sim} {}^{A_\mathfrak{p}}\!/_{\mathfrak{p}A_\mathfrak{p}}$$

und

$$k(\mathfrak{P}) = {}^{B}\!/_{\mathfrak{P}} \xrightarrow{\sim} {}^{B_\mathfrak{P}}\!/_{\mathfrak{P}B_\mathfrak{P}},$$

stimmt die Restklassenkörpererweiterung auf Seiten der Dedekindringe mit der der diskreten Bewertungsringe überein und folglich sind die Trägheitsgrade gleich.

Für die Bestimmung des Verzweigungsindex von $\mathfrak{P}|\mathfrak{p}$ schauen wir uns die Primfaktorzerlegung

$$\mathfrak{p}B = \mathfrak{P}^e \cdot \mathfrak{P}_2^{e_2} \cdot \ldots \cdot \mathfrak{P}_r^{e_r}.$$

Wir können daran den Verzweigungsindex e im Sinne von Erweiterungen von Dedekindringen ablesen.

Um den bewertungstheoretischen Verzweigungsindex zu bestimmen, wählen wir eine Uniformisierende $\pi \in \mathfrak{p}A_\mathfrak{p}$. Dann erzeugt $|\pi|_\mathfrak{p}$ die Wertegruppe $|K^\times|$. In $B_\mathfrak{P}$ gilt

$$\mathfrak{p}B_\mathfrak{P} = (\mathfrak{P}B_\mathfrak{P})^e.$$

Sei Π eine Uniformisierende von $\mathfrak{P}B_{\mathfrak{P}}$. Dann können wir π in der Form

$$\pi = U\Pi^e$$

schreiben, für eine Einheit $U \in B_{\mathfrak{P}}^\times$. Daraus folgt

$$|\pi|_{\mathfrak{p}} = |\pi|_{\mathfrak{P}} = |\Pi|_{\mathfrak{P}}^e.$$

Da $|\Pi|_{\mathfrak{P}}$ die Wertegruppe $|L^\times|$ erzeugt, folgt

$$(|L^\times| : |K^\times|) = e.$$

Wir wollen nun untersuchen, was beim Übergang zur Vervollständigung mit dem Trägheitsgrad und dem Verzweigungsindex passiert.

Lemma 4.25. *Sei $(K, |\cdot|)$ ein bewerteter Körper mit Bewertungsring $\mathcal{O}$, Maximalideal $\mathfrak{m}$ und Restklassenkörper $k = \mathcal{O}/\mathfrak{m}$. Wir bezeichnen mit $\widehat{\mathcal{O}}$, $\widehat{\mathfrak{m}}$ und $\widehat{k}$ die entsprechenden Objekte für die Vervollständigung $\widehat{K}$. Dann gibt es natürliche Isomorphismen*

$$k \xrightarrow{\sim} \widehat{k}$$
$$|K^\times| \xrightarrow{\sim} |\widehat{K}^\times|.$$

Beweis. Wir betrachten die natürliche Inklusion

$$k = {}^{\mathcal{O}}\!/_{\mathfrak{m}} \hookrightarrow {}^{\widehat{\mathcal{O}}}\!/_{\widehat{\mathfrak{m}}} = \widehat{k}.$$

Für $\overline{a} \in \widehat{k}$ wählen wir $a \in \widehat{\mathcal{O}}$ mit $[a] = \overline{a}$. Es ist

$$a + \widehat{\mathfrak{m}} = \left\{x \in \widehat{\mathcal{O}} \mid |a - x| < 1\right\} = B(a, 1)$$

eine offene Umgebung von a. Da $\mathcal{O}$ in $\widehat{\mathcal{O}}$ dicht liegt, gibt es $a_0 \in \mathcal{O}$, das in $a + \widehat{\mathfrak{m}}$ enthalten ist. Dann folgt

$$\overline{a} = [a] = [a_0] \in k$$

und wir haben gezeigt, dass $k \xrightarrow{\sim} \widehat{k}$.

Was die Wertegruppe betrifft, so haben wir die Aussage schon in Korollar 1.16 bewiesen. □

Korollar 4.26. *Sei $(L, |\cdot|_L)/(K, |\cdot|_K)$ eine Erweiterung reell bewerteter Körper. Dann bleiben Trägheitsgrad und Verzweigungsindex beim Übergang zur Erweiterung $\widehat{L}/\widehat{K}$ der Vervollständigungen gleich.*

Wir wollen nun den Trägheitsgrad und Verzweigungsindex mit dem Körpergrad in Verbindung setzen.

Lemma 4.27. *Sei $(L, |\cdot|_L)/(K, |\cdot|_K)$ eine Erweiterung bewerteter Körper mit entsprechenden Bewertungsringen $(\mathcal{O}_L, \mathfrak{m}_L)$ und $(\mathcal{O}_K, \mathfrak{m}_K)$ und Restklassenkörpern $k = {}^{\mathcal{O}_K}\!/_{\mathfrak{m}_K}$ und $\ell = {}^{\mathcal{O}_L}\!/_{\mathfrak{m}_L}$.*

Seien $w_1, \ldots, w_m \in \mathcal{O}_L$ und $\pi_1, \ldots, \pi_n \in L^\times$ mit

(1) $[w_1], \ldots, [w_m] \in \ell$ sind linear unabhängig über k,
(2) $|\pi|_L, \ldots, |\pi_n|_L \in |L^\times|_L$ sind paarweise verschieden modulo $|K^\times|_K$.

Dann gilt für alle $\alpha_{ij} \in K$

$$\begin{aligned}\left|\sum_{i=1}^{m}\sum_{j=1}^{n}\alpha_{ij}w_i\pi_j\right|_L &= \max_{i,j}\left\{|\alpha_{ij}w_i\pi_j|_L\right\}\\ &= \max_{i,j}\left\{|\alpha_{ij}|_K\cdot|\pi_j|_L\right\}\end{aligned}$$

Insbesondere sind die Produkte $w_i\pi_j \in L$ linear unabhängig über K.

Beweis. Wir betrachten zunächst Elemente der Form $\sum_{i=1}^{m}\beta_i w_i$, für $\beta_i \in K$, und wollen zeigen, dass

$$\left|\sum_{i=1}^{m}\beta_i w_i\right|_L = \max_{i=1,\dots,m}\left\{|\beta_i|_K\right\}$$

Sind alle Koeffizienten $\beta_i = 0$, so ist das klar. Wir nehmen nun an, dass nicht alle β_i verschwinden. Wir wählen einen Index r so dass

$$|\beta_r|_K = \max_{i=1,\dots,m}|\beta_i|_K > 0.$$

Dann ist

$$\sum_{i=1}^{m}\frac{\beta_i}{\beta_r}w_i \in \mathcal{O}_L$$

und der Koeffizient von w_r ist gleich 1. Da $[w_1],\dots,[w_m]$ linear unabhängig sind, und nicht alle Koeffizienten der Linearkombination

$$\sum_{i=1}^{m}\left[\frac{\beta_i}{\beta_r}\right]\cdot[w_i] \in \ell$$

verschwinden (der Koeffizient von $[w_r]$ ist 1), ist $[\sum_{1=1}^{m}\frac{\beta_i}{\beta_r}w_i] \neq 0$. Wir folgern daraus, dass

$$\left|\sum_{1=1}^{m}\frac{\beta_i}{\beta_r}w_i\right|_L = 1.$$

Wir erhalten

$$\begin{aligned}\left|\sum_{1=1}^{m}\beta_i w_i\right| &= |\beta_r|_K\cdot\left|\sum_{i=1}^{m}\frac{\beta_i}{\beta_r}w_i\right|\\ &\quad |\beta_r|_K\\ &= \max_{i=1,\dots,m}\left\{|\beta_i|_K\right\}.\end{aligned}$$

Nun betrachten wir $\sum_{1=1}^{m}\sum_{1=1}^{n}\alpha_{ij}w_i\pi_j$. Da $|\pi_j|_L$ modulo $|K^\times|_K$ paarweise verschieden sind, sind die Werte

$$\begin{aligned}\left|\sum_{1=1}^{m}\alpha_{ij}w_i\pi_j\right|_L &= \left|\sum_{1=1}^{m}\alpha_{ij}w_i\right|_L\cdot|\pi_j|_L\\ &\quad \max_{i=1,\dots,m}\left\{|\alpha_{ij}|_K\right\}\cdot|\pi_j|_L\end{aligned}$$

paarweise verschieden für $j = 1, \dots, n$. Daher gilt im Folgenden bei der Dreiecksungleichung sogar Gleichheit (Lemma 3.10):

$$\begin{aligned}\left|\sum_{i=1}^{m}\sum_{j=1}^{n}\alpha_{ij}w_i\pi_j\right|_L &= \left|\sum_{j=1}^{n}\left(\sum_{i=1}^{m}\alpha_{ij}w_i\pi_j\right)\right|_L \\ &= \max_{j=1,\dots,n}\left|\sum_{i=1}^{m}\alpha_{ij}w_i\pi_j\right|_L \\ &= \max_{\substack{i=1,\dots,m\\ j=1,\dots,n}}\left\{|\alpha_{ij}|_K\cdot|\pi_j|_L\right\}.\end{aligned}$$

Um zu sehen, dass $w_i\pi_j$ linear unabhängig sind, nehmen wir an, dass

$$\sum_{i=1}^{m}\sum_{j=1}^{n}\alpha_{ij}w_i\pi_j = 0$$

ist. Dann gilt

$$\begin{aligned}0 = |0|_L &= \left|\sum_{i=1}^{m}\sum_{j=1}^{n}\alpha_{ij}w_i\pi_j\right|_L \\ &= \max_{\substack{i=1,\dots,m\\ j=1,\dots,n}}\left\{|\alpha_{ij}|_K\cdot|\pi_j|_L\right\}.\end{aligned}$$

Das impliziert für alle i, j, dass

$$|\alpha_{ij}|_K\cdot|\pi_j|_L = 0.$$

Die Werte $|\pi_j|_L$ sind nach Konstruktion ungleich Null. Daher folgt $|\alpha_{ij}|_K = 0$, also $\alpha_{ij} = 0\ \forall i, j$. □

Korollar 4.28. *Sei $(L, |\cdot|_L)/(K, |\cdot|_K)$ eine Erweiterung bewerteter Körper mit Trägheitsgrad f und Verzweigungsindex e. Dann gilt*

$$n = [L : K] \geq ef.$$

Beweis. Wir wählen Elemente $\pi_1, \dots, \pi_e \in L$, so dass die Werte $|\pi_i|_L$ ein Repräsentantensystem der Restklassen in ${}^{|L^\times|_L}\!/_{|K^\times|_K}$ bilden. Außerdem wählen wir Elemente $w_1, \dots, w_f \in \mathcal{O}_L$, deren Restklassen in ${}^{\mathcal{O}_L}\!/_{\mathfrak{m}_L} = \ell$ eine Basis von ℓ über $k = {}^{\mathcal{O}_K}\!/_{\mathfrak{m}_K}$ bilden. Dann gilt nach Lemma 4.27

$$ef \leq n = [L : K].$$

□

Bemerkung 4.29. In AZT 1 haben wir für Erweiterungen von Dedekindringen die fundamentale Gleichung bewiesen: Ist A ein Dedekindring mit Quotientenkörper K, L/K eine endliche Erweiterung, $B = A_L$ der Ganzabschluss von A in L und $\mathfrak{p} \subseteq A$ ein Primideal, so gilt

$$n = [L : K] = \sum_{i=1}^{r} e_i f_i,$$

wobei e_i und f_i die Verzweigungsindizes und Trägheitsgrade der Primideale $\mathfrak{P} \subseteq B$ über $\mathfrak{p}$ bezeichnen. Das können wir auf den Fall anwenden, in dem A ein vollständiger

diskreter Bewertungsring ist Nach Satz 4.3 entsprechen die Primideale $\mathfrak{P} \subset B$ über $\mathfrak{p}$ den Fortsetzungen von $|\cdot|_{\mathfrak{p}}$ nach L. Da K vollständig ist, gibt es nach Korollar 4.22 nur eine Fortsetzung und somit ein Primideal $\mathfrak{P} \subset B$ über $\mathfrak{p}$. Die fundamentale Gleichung nimmt dann die Form

$$n = [L : K] = ef$$

an für $e = e(\mathfrak{P}/\mathfrak{p})$ und $f = f(\mathfrak{P}/\mathfrak{p})$. Wir schließen daraus, dass in Korollar 4.28 im Falle, dass K vollständg und diskret bewertet ist, sogar Gleichheit gilt.

Beispiel 4.30. Wir betrachten für $m \in \mathbb{N}$ die Erweiterung

$$K := \mathbb{Q}_p(p^{\frac{1}{m}})/\mathbb{Q}_p.$$

Der Erweiterungsgrad ist

$$n := [K : \mathbb{Q}_p] = m.$$

Es gilt

$$|p^{\frac{1}{m}}|_K = |p|_p^{\frac{1}{m}} = \frac{1}{p^{\frac{1}{m}}}.$$

Daraus folgt

$$e = \left(|K^\times|_K : |\mathbb{Q}_p^\times|_p\right) \geq m.$$

Wegen Korollar 4.28 folgt

$$e = m, \ \ f = 1.$$

Beispiel 4.31. Wir betrachten die Kreisteilungserweiterung

$$K := \mathbb{Q}_p(\mu_{p^r})/\mathbb{Q}_p$$

für $r \in \mathbb{N}$. Sie entsteht durch Adjunktion einer primitiven p^r-ten Einheitswurzel ζ_{p^r}. Diese ist eine Nullstelle des Kreisteilungspolynoms

$$\begin{aligned}\Phi_{p^r}(T) &= \frac{T^{p^r} - 1}{T^{p^{r-1}} - 1} \\ &= T^{p^{r-1}(p-1)} + T^{p^{r-1}(p-2)} + \ldots + T^{p^{r-1}} + 1.\end{aligned}$$

Wir wollen uns davon überzeugen, dass $\Phi_{p^r}(T+1)$ ein Eisensteinpolynom ist, das heißt

$$\Phi_{p^r}(T+1) \equiv T^{p^{r-1}(p-1)} \mod p$$

und

$$\Phi_{p^r}(1) \not\equiv 0 \mod p^2.$$

In der Tat gilt

$$\Phi_{p^r}(T+1) = \frac{(T+1)^{p^r} - 1}{(T+1)^{p^{r-1}} - 1} \equiv \frac{T^{p^r}}{T^{p^{r-1}}} \equiv T^{p^{r-1}(p-1)} \mod p$$

und

$$\Phi_{p^r}(1) = 1^{p^{r-1}(p-1)} + 1^{p^{r-1}(p-2)} + \ldots + +1^{p^{r-1}} 1^{p^{r-1}} + 1 \mod p^2.$$

Nach Aufgabe 1 auf Blatt 9 der Übungen ist $\Phi_{p^r}(T+1)$ als Eisensteilpolynom irreduzibel und

$$K = \mathbb{Q}_p(\mu_{p^r}) = \mathbb{Q}_p(\zeta_{p^r}) = \mathbb{Q}_p(_{p^r}-1)$$

ist rein verzweigt von Grad $p^{r-1}(p-1)$, also

$$e = p^{r-1}(p-1), \ \ f = 1.$$

Tatsächlich sagt uns die Übungsaufgabe auch, dass $\zeta_{p^r} - 1 \in K$ eine Uniformisierende ist, also

$$|\zeta_{p^r} - 1|_K = p^{-\frac{1}{p^{r-1}(p-1)}}.$$

Bis jetzt haben wir nur Beispiele mit diskreten Bewertungen betrachtet. Aus den letzten beiden Beispielen kann man auch ein nichtdiskretes Beispiel konstruieren.

Beispiel 4.32. Sei $K = \widehat{\bigcup_{r\in\mathbb{N}} \mathbb{Q}_p(\mu_{p^r})} = \widehat{\mathbb{Q}_p(\mu_{p^\infty})}$, also die Vervollständigung der Vereinigung aller Körper $\mathbb{Q}_p(\mu_{p^r})$. Hier beachte man, dass $\bigcup_{r\in\mathbb{N}} \mathbb{Q}_p(\mu_{p^r})$ keine endliche Erweiterung von $\mathbb{Q}_p$ ist, und daher nicht automatisch vollständig. Tatsächlich kann man zeigen, dass eine unendliche algebraische Erweiterung nie vollständig ist.

Die Wertegruppe von K ist gleich

$$|K^\times| = \bigcup_{r\in\mathbb{N}} |\mathbb{Q}_p(\mu_{p^r})^\times| = \bigcup_{r\in\mathbb{N}} \left(p^{-\frac{1}{p^{r-1}(p-1)}}\right)^{\mathbb{Z}}.$$

Insbesondere ist sie eindeutig p-divisibel, das heißt für jedes $\gamma \in |K^\times|$ ist auch $\gamma^{\frac{1}{p}} \in |K^\times|$. Nun betrachten wir $L = K(\sqrt[p]{p})$. Man kann zeigen, dass $\sqrt[p]{p} \notin K$. Daher ist $[L : K] = p$. Die Wertegruppe von L ist

$$|L^\times| = |K^\times|^{\frac{1}{p}} = |K^\times|,$$

also hat die Erweiterung L/K Verzweigungsindex $e = 1$.

Der Trägheitsgrad von $\mathbb{Q}_p(\sqrt[p]{p})/\mathbb{Q}_p$ ist nach Beispiel 4.30 gleich 1. Die Erweiterung L/K bekommt man, indem man das Kompositum mit K bildet. Dabei kann der Trägheitsgrad nur abnehmen. Somit ist der Trägkeitsgrad f von L/K gleich 1. Wir sehen, dass in diesem Fall die fundamentale Gleichung nicht gilt. Es gilt nur die Ungleichung

$$ef = 1 < p = [L : K].$$

Satz 4.33 (Die fundamentale Ungleichung)**.** *Sei $(K, |\cdot|)$ ein bewerteter Körper und L/K eine endliche Körpererweiterung. Wir bezeichnen mit $|\cdot|_1, \ldots, |\cdot|_r$ die endlich vielen Fortsetzungen von $|\cdot|$ auf L. Für $i \in \{1, \ldots, r\}$ sei e_i der Verzweigungsindex und f_i der Trägheitsgrad der Erweiterung $(L, |\cdot|_i)/(K, |\cdot|)$. Dann gilt*

$$[L : K] \geq \sum_{i=1}^{r} e_i f_i$$

Beweis. [EP05, Theorem 3.3.4.] □

4.4. **Hilbertsche Verzweigungstheorie.** Ebenso wie für Zahlkörper ist die Verzweigung einer galoisschen Erweiterung $(L, |\cdot|_L)/(K, |\cdot|_K)$ bewerteter Körper in der Galoisgruppe kodiert. Die Konzepte sind analog zu denen bei Erweiterungen von Zahlkörpern, daher werden wir uns kurz fassen.

Wir betrachten einen bewerteten Körper $(K, |\cdot|)$ und eine endliche Galoiserweiterung L/K. Dann operiert die Galoisgruppe $G := \mathrm{Gal}(L/K)$ auf der Menge der Fortsetzungen $|\cdot|'$ von $|\cdot|$ auf L. Genauer ist für eine Fortsetzung $|\cdot|'$ und $\sigma \in G$ die Abbildung

$$\begin{aligned} |\sigma(\cdot)|' : K &\to \mathbb{R}_{\geq 0} \\ x &\mapsto |\sigma(x)|' \end{aligned}$$

wieder eine Bewertung, und dies definiert die Operation.

Proposition 4.34. *Die Operation von G auf der Menge der Fortsetzungen von $|\cdot|$ auf L ist transitiv.*

Beweis. Der Beweis nutzt den schwachen Approximationssatz. Diesen haben wir nur für reelle Bewertungen bewiesen. Daher beschränken wir uns auf den Fall von reellen Bewertungen. Der allgemeine Approximationssatz gilt für Bewertungen, die nicht nur nicht äquivalent sind, sondern nicht die gleiche Topologie induzieren. Wenn man das voraussetzt, funktioniert der folgende Beweis wörtlich auch für nicht-reelle Bewertungen.

Seien $|\cdot|_1$ und $|\cdot|_2$ Fortsetzungen von $|\cdot|$ auf L. Angenommen für jedes $\sigma \in G$ sind die Bewertungen $|\cdot|_1$ und $|\sigma(\cdot)|_2$ verschieden, also nicht äquivalent.

Sei $(\mathcal{O}, \mathfrak{m})$ der Bewertungsring zu $|\cdot|$ und $\mathcal{O}_L$ sein Ganzabschluss in L. Dann gilt nach Satz 4.14

$$\mathcal{O}_L = \bigcap_{i=1}^{n} \mathcal{O}_i$$

für die endlich vielen Fortsetzungen $|\cdot|_i$ mit Bewertungsring $\mathcal{O}_i$ von L. Nach dem schwachen Approximationssatz (Satz 3.34) gibt es ein Element $x \in \mathcal{O}_L$, so dass

$$|x|_1 < 1, \ |\sigma(x) - 1|_2 < 1 \ \forall \sigma \in G.$$

Wir betrachten

$$N(x) = \prod_{\sigma \in G} \sigma x \in \mathcal{O}.$$

Alle Faktoren σx sind in $\mathcal{O}_L$ und für $\sigma = \mathrm{id}$ ist der entsprechende Faktor x in $\mathfrak{p}_1 = \{y \in \mathcal{O}_L \mid |y|_1 < 1\}$. Daher ist

$$N(x) \in \mathfrak{p}_1 \cap \mathcal{O} = \mathfrak{m}.$$

Andererseits gilt für jedes $\sigma \in G$ wegen $|\sigma(x) - 1|_2 < 1$, dass

$$\sigma(x) \notin \mathfrak{p}_2 = \{y \in \mathcal{O}_L \mid |y|_2 < 1\}.$$

Daher ist $N(x) \notin \mathfrak{p}_2$. Da $\mathfrak{m} = \mathfrak{p}_2 \cap \mathcal{O}$, ist $N(x)$ und nicht in $\mathfrak{m}$ enthalten, was im Widerspruch zum vorherigen Absatz steht. □

Definition 4.35. Für $i \in \{1, \ldots, r\}$ heißt die Standgruppe (Stabilisator) von $|\cdot|_i$ unter der Operation von G *Zerlegungsgruppe*. Wir bezeichnen sie mit

$$Z_i := \{\sigma \in G \mid |\sigma(x)|_i = |x|_i \ \forall x \in L\}.$$

Korollar 4.36. *Für $i, j \in \{1, \ldots, r\}$ sind die Zerlegungsgruppen zueinander konjugiert.*

Beweis. Das folgt direkt aus Proposition 4.34. □

Der folgende Aspekt ist neu im Vergleich zu unserer Behandlung von Zahlkörpern.

Satz 4.37 (Krasners Lemma)**.** *Sei $(K, |\cdot|)$ ein vollständiger reell bewerteter Körper und $\alpha \in K^{\mathrm{sep}}$ ein Element im separablen Abschluss. Sei $\beta \in K^{\mathrm{alg}}$ ein Element im algebraischen Abschluss, so dass für alle Einbettungen $\sigma : K(\alpha) \to K^{\mathrm{sep}}$ mit $\sigma\alpha \neq \alpha$ gilt*

$$|\alpha - \beta| < |\alpha - \sigma(\alpha)|.$$

Dann folgt $\alpha \in K(\beta)$.

Beweis. Aufgabe 1 auf Blatt 10. □

Proposition 4.38. *Ist $|\cdot|$ reell, so ist die Vervollständigung $\widehat{L_i}$ von L bezüglich $|\cdot|_i$ galoissch unter $\widehat{K}$ und wir haben einen natürlichen Isomorphismus*

$$\mathrm{Gal}(\widehat{L_i}/\widehat{K}) \simeq Z_i.$$

Beweis. Da L/K separabel ist, gibt es ein primitives Element $x \in L$, also $L = K(x)$, und x ist separabel über K. Dann ist $\widehat{K}(x)$ endlich und separabel über $\widehat{K}$. Insbesondere ist $\widehat{K}(x)$ nach Korollar 4.20 vollständig. Da

$$L = K(x) \subseteq \widehat{K}(x) \subseteq \widehat{L_i},$$

folgt daraus $\widehat{K}(x) = \widehat{L_i}$ und $\widehat{L_i}$ ist separabel über $\widehat{K}$.

Wir betrachten nun eine $\widehat{K}$-Einbettung $\sigma : \widehat{L_i} \to \widehat{K}^{\text{sep}}$. Für $\alpha \in \widehat{L_i}$ wählen wir $\beta \in L$ mit

$$|\sigma(\alpha) - \sigma(\beta)| < |\sigma(\alpha) - \tau(\alpha)| \ \forall \tau \text{ mit } \tau(\alpha) \neq \sigma(\alpha).$$

Dann folgt aus Krasners Lemma (Satz 4.37)

$$\sigma(\alpha) \in \widehat{L_i}(\sigma\beta) = \widehat{L}(\beta) = \widehat{L_i}.$$

Folglich ist $\widehat{L_i}$ galoissch.

Für $\sigma \in \mathrm{Gal}(\widehat{L_i}/\widehat{K})$ ist $\sigma\big|_L$ natürlicherweise ein Element von $\mathrm{Gal}(L/K)$. Das definiert einen Homomorphismus

$$\varphi : \mathrm{Gal}(\widehat{L_i}/\widehat{K}) \to \mathrm{Gal}(L/K).$$

φ ist injektiv: ein Element $\sigma \in \mathrm{Gal}(\widehat{L_i}/\widehat{K})$ ist auch ein $\widehat{K}$-linearer Homomorphismus $\widehat{L_i} \to \widehat{L_i}$ und somit automatisch stetig. Da L dicht in $\widehat{L_i}$ liegt, ist σ somit schon durch $\sigma\big|_L$ eindeutig festgelegt.

Das Bild von φ ist Z_i: für $\sigma \in \mathrm{Gal}(\widehat{L_i}/\widehat{K})$ ist $|\sigma(\cdot)|_{\widehat{L_i}}$ eine weitere Fortsetzung von $|\cdot|_{\widehat{K}}$ auf $\widehat{L_i}$. Da $\widehat{K}$ vollständig ist, gibt es nach Korollar 4.22 nur eine Fortsetzung und es folgt $|\cdot|_{\widehat{L_i}} = |\sigma(\cdot)|_{\widehat{L_i}}$ und somit ist $\sigma \in Z_i$.

Auf der anderen Seite ist jedes Element σ von Z_i stetig bezüglich $|\cdot|_i$, da sogar gilt

$$|\sigma(x)|_i = |x|_i \ \forall x \in L.$$

Daher setzt sich σ stetig zu einem Automorphismus von $\widehat{L_i}$ fort, und definiert somit ein Element von $\mathrm{Gal}(\widehat{L_i}/\widehat{K})$, dessen Einschränkung auf L gleich σ ist. □

Ein Element $\sigma \in Z_i$ bildet den Bewertungsring $\mathcal{O}_i$ zu $|\cdot|_i$ wieder auf $\mathcal{O}_i$ ab und das zugehörige Maximalideal $\mathfrak{m}_i$ auf $\mathfrak{m}_i$. Wir erhalten einen induzierten Homomorphismus

$$\pi : Z_i \to \mathrm{Aut}_k(\ell_i).$$

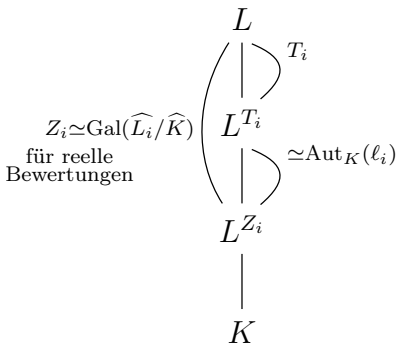
Hierbei ist $\ell_i = {}^{\mathcal{O}_i}\!/_{\mathfrak{m}_i}$ und $k = {}^{\mathcal{O}}\!/_{\mathfrak{m}}$. Genauso wie im Falle von Zahlkörpern könnte ℓ_i/k inseparabel sein. Das ist der Grund, warum wir $\mathrm{Aut}_k(\ell_i)$ statt $\mathrm{Gal}(\ell_i/k)$ schreiben.

Proposition 4.39. *(i) ℓ_i/k ist normal*
(ii) π ist surjektiv

Beweis. Das Argument ist analog zum Zahlkörperfall. □

Definition 4.40. Der Kern von π heißt *Trägheitsgruppe* und wird mit T_i bezeichnet.

Wir erhalten folgendes Bild.



In der gleichen Weise wie für Zahlkörper können wir das Zerlegungs- und Verzweigungsverhalten in den einzelnen Teilerweiterungen untersuchen. Das Ergebnis ist der folgende Satz. Die Verzweigungsindizes und Trägheitsgrade sind alle bezüglich der Bewertung $|\cdot|_i$ definiert. Mit e und f bezeichnen wir den Verzweigungsindex und Trägheitsgrad von L/K.

Satz 4.41. *Es gilt:*

(i) $e(L^{Z_i}/K) = f(L^{Z_i}/K) = 1$,
(ii) $e(L^{T_i}/L^{Z_i}) = 1$,
$f(L^{T_i}/L^{Z_i}) = f_s = [L^{T_i} : L^{Z_i}]$,
(iii) $e(L/L^{T_i}) = e$,
$f(L/L^{T_i}) = f_i$,
$ef_i \leq [L : L^{T_i}]$

Beweis. [EP05, Corollary 5.3.8.] □

Wir möchten darauf hinweisen, dass in (iii) im Allgemeinen nicht $ef_i = [L : L^{T_i}]$ gilt, sondern nur $ef_i \leq [L : L^{T_i}]$. Das liegt daran, dass die fundamentale Ungleichung im Allgemeinen keine Gleichung ist. Im Falle von diskreten Bewertungen gilt $ef_i = [L : L^{T_i}]$.

5. Lokale Körper

5.1. Beschreibung von lokaler Kompaktheit.

Definition 5.1. Ein Hausdorffraum X heißt *lokal kompakt*, wenn jedes Element $x \in X$ eine offene Umgebung U besitzt, deren Abschluss $\overline{U}$ kompakt ist.

Definition 5.2. Ein *lokaler Körper* ist ein reell bewerteter Körper $(K, |\cdot|)$, der bezüglich der von $|\cdot|$ induzierten Topologie lokal kompakt ist. Außerdem soll die Bewertung nicht trivial sein.

Beispiel 5.3. $\mathbb{R}$ und $\mathbb{C}$ sind lokale Körper.

Auch $\mathbb{Q}_p$ ist ein lokaler Körper. Um das zu zeigen, reicht es einzusehen, dass $\mathbb{Z}_p$ kompakt ist. Das liegt daran, dass für jedes $x \in \mathbb{Q}_p$ die Menge $x + \mathbb{Z}_p$ eine offene Umgebung ist (und gleichzeitig auch abgeschlossen). Wir zeigen, dass $\mathbb{Z}_p$ kompakt ist, mithilfe von Intervallschachtelung:

Für $a \in \mathbb{Z}_p$ und $n \in \mathbb{N}$ betrachten wir die abgeschlossenen Bälle

$$\overline{B}(a, p^{-n}) = \left\{ x \in \mathbb{Q}_p \mid |x - a|_p \leq \frac{1}{p^n} \right\} = a + p^n \mathbb{Z}_p.$$

Sie sind offen und abgeschlossen und es gilt für $a, b \in \mathbb{Z}_p$

$$\overline{B}(a, p^{-n}) \cap B(b, p^{-n}) = \begin{cases} \overline{B}(a, p^{-n}) & a \equiv b \mod p^n \\ \varnothing & \text{sonst.} \end{cases}$$

Da $\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$ endlich ist, erhalten wir eine endliche disjunkte Zerlegung

$$\mathbb{Z}_p = \coprod_{a=0}^{p^n-1} \overline{B}(a, p^{-n}).$$

Sei nun $(x_i)_{i\in\mathbb{N}}$ eine Folge in $\mathbb{Z}_p$. Um eine konvergente Teilfolge zu finden, gehen wir folgendermaßen vor: Es gibt $a_0 \in \{0, \ldots, p-1\}$, so dass unendlich viele Folgenglieder in $\overline{B}(a, p^{-n})$ liegen. Sei $k_0 \in \mathbb{N}$ die kleinste natürliche Zahl, so dass $x_{k_0} \in \overline{B}(a_0, p^{-1})$. Dann betrachten wir die Zerlegung

$$\overline{B}(a_0, p^{-1}) = \coprod_{a=0}^{p-1} \overline{B}(a_0 + pa, p^{-2}).$$

Wieder gibt es $a_1 \in \{0, \ldots, p-1\}$, so dass unendlich viele Folgenglieder in $\overline{B}(a, p^{-2})$ liegen. Sei k_1 die kleinste natürliche Zahl größer k_0, so dass

$$x_{k_1} \in \overline{B}(a_0 + pa_1, p^{-2}).$$

Machen wir in dieser Weise weiter, erhalten wir eine Teilfolge $(x_{k_j})_{j\in\mathbb{N}}$ von $(x_i)_{i\in\mathbb{N}}$ und eine Folge von Zahlen $a_j \in \{0, \ldots, p-1\}$, so dass

$$x_{k_j} \in \overline{B}(a_0 + pa_1 + \ldots + p^j a_j, p^{-(j+1)}).$$

In $\mathbb{Z}_p$ konvergiert die Reihe $\sum_{j=0}^{\infty} a_j p^j$, und somit konvergiert x_{k_j} gegen $\sum_{j=0}^{\infty} a_j p^j$.

Ein kürzeres Argument, um die Kompaktheit von $\mathbb{Z}_p$ zu zeigen, benutzt die Darstellung als inversen Limes:

$$\mathbb{Z}_p = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p\mathbb{Z}.$$

Die Gruppen $\mathbb{Z}/p^n\mathbb{Z}$ sind endlich, also insbesondere kompakt. Der inverse Limes von kompakten Mengen ist wieder kompakt, also ist $\mathbb{Z}_p$ kompakt.

Wir wollen nun eine konkrete Beschreibung lokaler Körper erreichen. Die erste Beobachtung ist die Folgende.

Lemma 5.4. *Sei $(K, |\cdot|)$ ein lokaler Körper. Dann ist K vollständig.*

Beweis. Sei $(x_i)_{i\in\mathbb{N}}$ eine Cauchyfolge in K. Da K lokal ist, besitzt die 0 eine offene Umgebung U, so dass $\overline{U}$ kompakt ist. Da die Bälle um 0 eine Umgebungsbasis bilden, gibt es $\varepsilon > 0$, so dass

$$B(0, \varepsilon) \subseteq U.$$

Dann ist $\overline{B(0,\varepsilon)}$ abgeschlossen in der kompakten Menge $\overline{U}$ und somit selbst kompakt. Da $(x_i)_{i\in\mathbb{N}}$ eine Cauchyfolge ist, gibt es $N \in \mathbb{N}$, so dass für alle $i, j \geq N$ gilt

$$|x_i - x_j| < \varepsilon.$$

Insbesondere ist für $i \geq N$

$$x_i - x_N \in B(0, \varepsilon).$$

Nun ist $\overline{B(0,\varepsilon)}$ kompakt, also vollständig, und $(x_i - x_N)_{i\geq N}$ ist eine Cauchyfolge in $\overline{B(0,\varepsilon)}$. Daher konvergiert $(x_i - x_N)_{i\geq N}$ gegen ein Element $y \in \overline{B(0,\varepsilon)}$. Folglich konvergiert $(x_i)_{i\in\mathbb{N}}$ gegen $y + x_N \in K$. □

Lemma 5.5. *Sei $(K, |\cdot|)$ ein nichtarchimedischer Körper und $(\mathcal{O}, \mathfrak{m})$ der zugehörige Bewertungsring. Dann sind $\mathcal{O}$ und $\mathfrak{m}$ kompakt.*

Beweis. Da K lokal kompakt ist, gibt es $r > 0$, so dass

$$\overline{B}_r(0) = \{x \in K \mid |x| \leq r\}$$

kompakt ist. Sei $r' = \sup_{x\in\overline{B}(0,r)} |x|$. Dann gilt

$$\overline{B}(0,r') = \overline{B}(0,r),$$

und da diese Menge kompakt ist, wird das Supremum r' angenommen. Es gibt also $x \in \overline{B}(0,r')$ mit $|x| = r'$. Dann ist $\mathcal{O} = B(0,1)$ das Bild von $B(0,r')$ unter der stetigen Abbildung

$$\begin{aligned} K &\to K \\ y &\mapsto \frac{y}{x}. \end{aligned}$$

Folglich ist auch $\mathcal{O}$ kompakt.

Das Maximalideal

$$\mathfrak{m} = \{x \in \mathcal{O} \mid |x| < 1\}$$

ist eine offene Untergruppe von $\mathcal{O}$. Offene Untergruppen einer topologischen Gruppe sind automatisch auch abgeschlossen. Daher ist auch $\mathfrak{m}$ kompakt. □

Satz 5.6. *Sei $(K, |\cdot|)$ ein nichtarchimedischer reell bewerteter Körper mit Bewertungsring $(\mathcal{O}, \mathfrak{m})$ und Restklassenkörper $k = {}^{\mathcal{O}}/_{\mathfrak{m}}$. Dann ist K genau dann lokal, wenn*

(i) K vollständig,
(ii) k endlich und
(iii) $|\cdot|$ diskret ist.

Beweis. Wir nehmen an, dass $(K, |\cdot|)$ lokal ist. Dann ist K nach Lemma 5.4 vollständig. Der Restklassenkörper k ist ein Quotient der kompakten Gruppe $\mathcal{O}$ nach der offenen Untergruppe $\mathfrak{m}$. Da $\mathfrak{m}$ insbesondere abgeschlossen ist, ist k auch kompakt. Da $\mathfrak{m}$ offen ist, ist k außerdem diskret. Diskrete kompakte Räume sind endlich, also ist k endlich. Um zu zeigen, dass $|\cdot|$ diskret ist, betrachten wir die offene Überdeckung

$$\mathfrak{m} = \bigcup_{n\in\mathbb{N}} B(0, 1 - \frac{1}{n}).$$

Da $\mathfrak{m}$ kompakt ist, hat sie eine endliche Teilüberdeckung, was in diesem Fall bedeutet, dass es ein $n \in \mathbb{N}$ gibt mit

$$\mathfrak{m} = B(0, 1 - \frac{1}{n}).$$

Dann muss die Wertegruppe von $|\cdot|$ diskret in $\mathbb{R}_{\geq 0}$ sein, da jede nichtdiskrete Untergruppe dicht liegt. Außerdem sind alle diskreten Untergruppen von $\mathbb{R}_{\geq 0}$ von der Form $\lambda^{\mathbb{Z}}$ für ein $\lambda \in \mathbb{R}_{>0}$.

Nun wollen wir aus den Eigenschaften (i)-(iii) folgern, dass $(K, |\cdot|)$ lokal ist. Nach Voraussetzung ist $\mathcal{O}$ ein diskreter Bewertungsring. Wir wählen eine Uniformisierende $\pi \in \mathfrak{m}$. Dann können wir genau so wie in Beispiel 5.3 durch Intervallschachtelung zeigen, dass

jede Folge $(x_i)_{i\in\mathbb{N}} \subseteq \mathcal{O}$ eine konvergente Teilfolge hat. Dafür wählen wir ein Repräsentantensystem $\mathcal{M} \subset \mathcal{O}$ des Restklassenkörpers k. Da k endlich ist, ist $\mathcal{M}$ endlich. Wir konstruieren induktiv eine Teilfolge $(x_{k_j})_{j\in\mathbb{N}}$ und $(a_j)_{j\in\mathbb{N}}$ in $\mathcal{M}$, so dass

$$x_{k_j} \in B(a_0 + a_1\pi + \ldots + a_j\pi^j, |\pi|^{j+1})$$

wie in Beispiel 5.3. Da K vollständig ist, konvergiert die Reihe $\sum_{j=0}^{\infty} a_j\pi^j$, und $(x_{k_j})_{j\in\mathbb{N}}$ konvergiert gegen den selben Grenzwert. Genauso wie in Beispiel 5.3 kann man ein schnelleres Argument benutzen, wenn man mit dem Konzept des inversen Limes vertraut ist. Für den vollständigen diskreten Bewertungsring $\mathcal{O}$ gilt nämlich

$$\mathcal{O} \cong \varprojlim_{n\in\mathbb{N}} {}^{\mathcal{O}}\!/_{\pi^n\mathcal{O}}.$$

Um zu zeigen, dass $\mathcal{O}$ kompakt ist, müssen wir uns nur noch davon überzeugen, dass ${}^{\mathcal{O}}\!/_{\pi^n\mathcal{O}}$ endlich und somit kompakt ist. Das zeigen wir per Induktion mithilfe der kurzen exakten Folge

$$0 \longrightarrow {}^{\mathcal{O}}\!/_{\pi^{n-1}} \xrightarrow{x\mapsto\pi x} {}^{\mathcal{O}}\!/_{\pi^n\mathcal{O}} \longrightarrow \underbrace{{}^{\mathcal{O}}\!/_{\pi\mathcal{O}}}_{=k} \longrightarrow 0$$

und der Voraussetzung, dass k endlich ist. □

Beispiel 5.7. Sei K ein Zahlkörper und $\mathfrak{p} \subset \mathcal{O}_K$ ein Primideal. Dann definiert $\mathfrak{p}$ eine diskrete Bewertung $|\cdot|_{\mathfrak{p}}$. Man bekommt sie entweder durch die Beobachtung, dass die Lokalisierung $\mathcal{O}_{K,\mathfrak{p}}$ ein diskreter Bewertungsring ist, oder indem man für $a \in K^\times$ die Primfaktorzerlegung

$$(a) = \mathfrak{p}^e \cdot \mathfrak{p}_2^{e_2} \cdot \ldots \cdot \mathfrak{p}_n^{e_n}$$

mit $e, e_i \in \mathbb{Z}$ betrachtet, und

$$|a|_{\mathfrak{p}} = q^{-e}$$

setzt. Hierbei ist q die Kardinalität des Restklassenkörpers $k(\mathfrak{p}) = {}^{\mathcal{O}_K}\!/_{\mathfrak{p}}$. Vervollständigen wir K bezüglich $|\cdot|_{\mathfrak{p}}$, so erhalten wir nach Satz 5.6 einen lokalen Körper $K_{\mathfrak{p}}$. Hierbei beachte man, dass die Vervollständigung den Restklassenkörper und die Wertegruppe erhält (Lemma 4.25).

5.2. **Klassifikation lokaler Körper.** In Beispiel 5.3 haben wir gesehen, dass $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{Q}_p$ lokale Körper sind. Ebenso ist $\mathbb{F}_p(\!(T)\!)$ ein lokaler Körper. Das sieht man zum Beispiel durch anwenden von Satz 5.6, oder man imitiert das Argument für $\mathbb{Q}_p$.

Ziel dieses Abschnittes ist es, zu zeigen, dass die oben genannten Körper die Prototypen für lokale Körper sind. Alle anderen sind endliche Erweiterungen eines solchen Körpers. Zentral ist hierfür folgende Folgerung aus der Betrachtung von normierten Vektorräumen über einem vollständigen reell bewerteten Körper.

Satz 5.8. *Sei $(K, |\cdot|)$ ein lokaler Körper und $(V, \|\cdot\|)$ ein normierter K-Vektorraum. Dann ist V genau dann lokal kompakt, wenn er endlich dimensional ist.*

Beweis. Wenn V endlich dimensional ist, ist seine Norm nach Korollar 4.20 äquivalent zur Supremumsnorm sobald wir einen Isomorphismus $V \simeq K^n$ gewählt haben. Für $x = (x_1, \ldots, x_n) \in K^n$ betrachten wir die offene Umgebung

$$U = U_1 \times \ldots \times U_n,$$

wobei $U_i \subset K$ eine offene Umgebung von x_i ist, so dass $\overline{U_i}$ kompakt ist. Dann ist

$$\overline{U} = \overline{U_1} \times \ldots \times \overline{U_n}$$

kompakt, und V somit lokal kompakt.

Wir nehmen nun an, dass V lokal kompakt ist. Dann ist

$$\overline{B}(0,1) = \{x \in V \mid \|x\| \leq 1\}$$

kompakt. Wir wählen $r \in \mathbb{R}$ und $\alpha \in K$ mit

$$0 < r < |\alpha| < 1.$$

Da $\overline{B}(0,1)$ kompakt ist, gibt es endlich viele Vektoren $w_1, \ldots, w_m \in \overline{B}(0,1)$, so dass

$$\overline{B}(0,1) = \bigcup_{i=1}^{m} B(w_i, r).$$

Wir betrachten den Untervektorraum

$$W := Kw_1 + \ldots + Kw_m \subseteq V$$

und wollen zeigen, dass $W = V$ ist. Gäbe es $x \in V \setminus W$, so wäre nach Satz 4.19 $d(x,W) > 0$. Für $c > d(x,W)$ ist der Schnitt

$$W_c := \overline{B}(x,C) \cap W$$

nicht leer. Außerdem ist $\overline{B}(x,C)$ kompakt, und W ist abgeschlossen in V (nach Korollar 4.21). Daher ist W_c abgeschlossen in $\overline{B}(x,C)$ und somit kompakt. Das Infimum

$$d(x,W) = d(x,W_c) = \inf_{y \in W_c} d(x,y)$$

wird daher angenommen, und es gibt $w \in W_c$ mit

$$d(x,w) = d(x,W) > 0.$$

Wir reskalieren nun um x nach $\overline{B}(0,1)$ zu verschieben. Für ein geeignetes $N \in \mathbb{Z}$ ist

$$x' := \alpha^N (x - w) \in \overline{B}(0,1) \setminus \overline{B}(0,|\alpha|),$$

das heißt

$$|\alpha| < \|x'\| \leq 1.$$

Außerdem ist dann

$$d(x',W) = d(x',0) = \|x'\| > |\alpha|.$$

Insbesondere gilt für die Basisvektoren w_i

$$d(x',w_i) > |\alpha| > r.$$

Doch das steht im Widerspruch zu $x' \in \overline{B}(0,1)$, da $\overline{B}(0,1) = \bigcup_{i=1}^{m} B(w_i,r)$. □

Jetzt sind wir bereit für die Klassifikation lokaler Körper.

Satz 5.9. *Sei $(K, |\cdot|)$ ein lokaler Körper.*

(i) Ist $|\cdot|$ archimedisch, so ist $K = \mathbb{R}$ oder $K = \mathbb{C}$.

(ii) Ist $|\cdot|$ nichtarchimedisch und $\mathrm{char}(K) = 0$, so ist K eine endliche Erweiterung von $\mathbb{Q}_p$ für eine Primzahl p.

(iii) Ist $\mathrm{char}(K) = p > 0$, so ist K eine endliche Erweiterung von $\mathbb{F}_p(\!(T)\!)$.

Beweis. Wir betrachten zunächst den Fall, dass $\mathrm{char}(K) = 0$ ist. Dann gibt es eine natürliche Inklusion $\mathbb{Q} \subseteq K$. Die Einschränkung $|\cdot|_Q$ von $|\cdot|$ auf $\mathbb{Q}$ ist nach dem Satz von Ostrowski (Satz 3.24) entweder äquivalent zum Standardabsolutbetrag $|\cdot|_\infty$ oder zu einer p-adischen Bewertung $|\cdot|_p$. Da K vollständig ist, enthält K auch die Vervollständigung $\mathbb{R}$, beziehungsweise $\mathbb{Q}_p$.

Nun sind $\mathbb{Q}_p$ und $\mathbb{R}$ lokale Körper, und K ist ein lokal kompakter normierter $\mathbb{Q}_p$- oder $\mathbb{R}$-Vektorraum. Nach Satz 5.8 muss $K/\mathbb{Q}_p$ beziehungsweise $K/\mathbb{R}$ eine endliche Erweiterung sein. Damit haben wir die Fälle (i) und (ii) abgearbeitet.

Nehmen wir nun an, dass $\mathrm{char}(K) = p > 0$. Dann haben wir eine Einbettung $\mathbb{F}_p \subseteq K$. Sei $t \in K$ ein Element mit $|t| < 1$. Dann ist t nicht algebraisch über $\mathbb{F}_p$, da sonst $\mathbb{F}_p(t)$ ein endlicher Körper wäre, und auf solchen ist jede Bewertung trivial (Proposition 3.18).

Da nun t transzendent über $\mathbb{F}_p$ ist, erhalten wir eine Körpererweiterung.

$$\begin{aligned} \mathbb{F}_p(T) &\hookrightarrow K \\ T &\mapsto t \end{aligned}$$

Die Einschränkung $|\cdot|_{\mathbb{F}_p(T)}$ erfüllt

$$|T|_{\mathbb{F}_p(T)} = |t| < 1.$$

Nach dem Satz von Ostrowski für Funktionenkörper (Satz 3.29) muss $|\cdot|_{\mathbb{F}_p(T)}$ die T-adische Bewertung sein. Die Vervollständigung von $\mathbb{F}_p(T)$ bezüglich dieser ist $\mathbb{F}_p(\!(T)\!)$, und da K vollständig ist, erhalten wir eine Inklusion

$$\mathbb{F}_p(\!(T)\!) \hookrightarrow K.$$

Nun argumentieren wir wie zuvor, dass $\mathbb{F}_p(\!(T)\!)$ ein lokaler Körper ist, und dass K ein lokal kompakter normierter $\mathbb{F}_p(\!(T)\!)$-Vektorraum ist, um mit Satz 5.8 zu schließen, dass $K/\mathbb{F}_p(\!(T)\!)$ endlich ist. □

Im Fall von Funktionenkörpern können wir die Beschreibung noch verfeinern.

Satz 5.10. *Sei K ein lokaler Körper von Charakteristik $p > 0$ mit Restklassenkörper $\mathbb{F}_q$ für $q = p^f$. Dann gibt es einen Isomorphismus*

$$K \cong \mathbb{F}_q(\!(T)\!).$$

Beweis. Da $\mathrm{char}(K) = p > 0$ ist, haben wir $\mathbb{F}_p \subseteq K$. Die Elemente $\overline{x} \neq 0$ im Restklassenkörper $\mathbb{F}_q$ erfüllen $\overline{x}^{q-1} = 1$. Mit anderen Worten enthält $\mathbb{F}_q$ die $(q-1)$-ten Einheitswurzeln. Daher impliziert das Henselsche Lemma, dass auch K die $(q-1)$-ten Einheitswurzeln enthält, also

$$\mathbb{F}_q(\mu_{q-1}) \subseteq K.$$

Aber $\mathbb{F}_q(\mu_{q-1}) = \mathbb{F}_q$, so dass $\mathbb{F}_q \subseteq K$. Sei π eine Uniformisierende des Bewertungsrings $\mathcal{O}$ von K. Wie im Beweis von Satz 5.9 erhalten wir eine Körpererweiterung

$$\begin{aligned} \mathbb{F}_q(\!(T)\!) &\hookrightarrow K \\ T &\mapsto \pi. \end{aligned}$$

Behauptung. *Die Elemente der Form*

$$\sum_{i=r}^{s} \alpha_i \pi^i, \;\; r < s \in \mathbb{Z}, \;\; \alpha_i \in \mathbb{F}_q$$

liegen dicht in K.

Um die Behauptung zu zeigen, müssen wir für $x \in K$ und eine offene Umgebung U von x ein Element x_0 von der oben beschriebenen Form finden, das in U liegt. Ohne Beschränkung der Allgemeinheit können wir annehmen, dass U von der Form

$$U = x + \pi^N \mathcal{O}$$

ist, für $N \in \mathbb{N}$. Zunächst schreiben wir x in der Form $x = u\pi^r$, für $r \in \mathbb{Z}$ und eine Einheit $u \in \mathcal{O}^\times$. Wir konstruieren x_0 per Induktion über N, angefangen bei $N = r + 1$. Sei u_0 das Bild von u unter der Komposition

$$\mathcal{O} \twoheadrightarrow \mathbb{F}_q \hookrightarrow K.$$

Dann ist für $N = r + 1$ das Element $x_0 = u_0\pi^r$ das gesuchte:

$$\begin{aligned} x - x_0 &= u\pi^r - u_0\pi^r \\ &= \underbrace{(u - u_0)}_{\in \pi\mathcal{O}}\pi^r \in \pi^{r+1}\mathcal{O}. \end{aligned}$$

Nun nehmen wir an, dass es $y_0 = \sum_{i=r}^{s} \alpha_i \pi^i$ gibt mit $x - y_0 \in \pi^{N-1}\mathcal{O}$, also

$$x = \sum_{i=r}^{s} \alpha_i \pi^i + \pi^{N-1}\beta, \ \beta \in \mathcal{O}.$$

Sei β_0 das Bild von β unter

$$\mathcal{O} \twoheadrightarrow \mathbb{F}_q \hookrightarrow K.$$

Dann ist $x_0 := y_0 + \pi^{N-1}\beta_0$ das gesuchte Element, da

$$x - x_0 = \pi^{N-1}\underbrace{\beta - \beta_0}_{\in \pi\mathcal{O}} \in \pi^N \mathcal{O}.$$

Damit haben wir die Behauptung bewiesen. Die Elemente $\sum_{i=r}^{s} \alpha_i \pi^i$ liegen im Bild von $\mathbb{F}_q(T)$. Daher ist $\mathbb{F}_q(T)$ diskret in K. Daher folgt für die Vervollständigung $\mathbb{F}_q(\!(T)\!) = K$. □

5.3. **Die maximale abelsche Erweiterung.** Für lokale und globale Körper gibt es eine Maschinerie um die maximale abelsche Erweiterung zu untersuchen, genannt Klassenkörpertheorie. Diese zu entwickeln würde ein ganzes Semester in Anspruch nehmen. Wir wollen in diesem Abschnitt aber im Falle der lokalen Klassenkörpertheorie die Ergebnisse zusammenstellen.

Satz 5.11. *Sei L/K eine endliche galoissche Erweiterung nichtarchimedisch bewerteter Körper. Dann gibt es eine exakte Folge*

$$1 \longrightarrow N_{L/K}L^\times \longrightarrow K^\times \xrightarrow{(\,\cdot\,, L/K)} G_{L/K}^{\mathrm{ab}} \longrightarrow 1.$$

Hierbei ist $G_{L/K}^{\mathrm{ab}}$ die Abelisierung der Galoisgruppe $G_{L/K}$, also

$$G_{L/K}^{\mathrm{ab}} = {}^{G_{L/K}}\!/_{[G_{L/K}, G_{L/K}]},$$

und $N_{L/K} : L^\times \to K^\times$ ist die Norm. Die Abbildung $(\,\cdot\,, L/K)$ nennt man das Normrestsymbol.

Wir erhalten dadurch einen Isomorphismus

$$G_{L/K}^{\mathrm{ab}} \simeq {}^{K^\times}\!/_{N_{L/K}L^\times}$$

Beweis. Siehe [Neu11, Satz 5.9.] □

Gehen wir zum Limes über alle endlichen galoisschen Erweiterungen über, erhalten wir:

Satz 5.12. *Sei K ein nichtarchimedischer lokaler Körper. Dann erhalten wir eine Injektion*

$$K^\times \overset{(\cdot,K)}{\hookrightarrow} G_k^{\mathrm{ab}}$$

mit dichtem Bild.

Man kann das so interpretieren, dass die Galoisgruppe der maximalen abelschen Erweiterung eines lokalen Körpers K durch die multiplikative Gruppe $K^\times$ parametrisiert wird. Ist π die Uniformisierende des Bewertungsrings $\mathcal{O}$ von K, so gilt

$$K^\times = \pi^{\mathbb{Z}} \times \mathcal{O}^\times.$$

Man kann zeigen, dass die Elemente $(\pi^k, K^\times)$ gerade die maximale unverzweigte Teilerweiterung parametrisieren. $(\pi, K^\times) = \mathrm{Frob}$

Wir wollen sehen, dass die maximale unverzweigte Erweiterung isomorph ist zur absoluten Galoisgruppe des Restklassenkörpers, also zu $\widehat{\mathbb{Z}}$. Um die verzweigten Erweiterungen zu verstehen, müssten wir uns die Struktur von $\mathcal{O}^\times$ anschauen. Wir wissen schon, dass $\mathcal{O}^\times$ die $(q-1)$-ten Einheitswurzeln enthält, falls $\mathbb{F}_q$ der Restklassenkörper ist. Es gilt

$$\mathcal{O}^\times = \mu_{q-1} \times U^{(1)},$$

wobei $U^{(1)} = 1 + \pi\mathcal{O}$ die *Einseinheiten* sind. Bis hierhin ist die Struktur von lokalen Körpern in Charakteristik 0 oder $p > 0$ analog. Schaut man sich $U^{(1)}$ genauer an, gibt es aber große Unterschiede.

Satz 5.13. *(i) Sei $K/\mathbb{Q}_p$ eine endliche Erweiterung von Grad d mit Restklassenkörper $\mathbb{F}_q$. Dann gilt*

$$K^\times = \pi^{\mathbb{Z}} \times \mu_{q-1} \times \underbrace{\mu_{p^a} \times \mathbb{Z}_p^d}_{U^{(1)}},$$

wobei a maximal ist, so dass $\mu_{p^a} \subseteq K$.

(ii) Ist $K = \mathbb{F}_q(\!(T)\!)$, so gilt

$$K^\times = T^{\mathbb{Z}} \times \mu_{q-1} \times \underbrace{\mathbb{Z}_p^{\mathbb{N}}}_{U^{(1)}}.$$

6. Perfektoide Körper

6.1. **Das Theorem von Fontaine und Wintenberger.** Im letzten Abschnitt haben wir gesehen, dass für nichtarchimedische lokale Körper K die Struktur der absoluten Galoisgruppe $G_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ immer ähnlich aussieht, aber immer davon abhängt, ob K Charakteristik 0 (beispielsweise wenn K eine endliche Erweiterung von einem $\mathbb{Q}_p$ ist) oder Charakteristik $p > 0$ (beispielsweise wenn K eine endliche Erweiterung von $\mathbb{F}_p(\!(T)\!)$ ist) hat. In diesem Abschnitt sehen wir, dass man zu einer passenden unendlichen Erweiterung von $\mathbb{Q}_p$ übergehen kann, um tatsächlich eine Korrespondenz der Galoisgruppen in Charakteristik 0 und p zu erhalten.

Das erste Resultat in diese Richtung ist das folgende Theorem von Fontaine und Wintenberger ([FW79]).

Theorem 6.1 (Fontaine und Wintenberger)**.** *Für p prim gilt*

$$G_{\mathbb{Q}_p(\mu_{p^\infty})} \simeq G_{\mathbb{F}_p(\!(T)\!)}.$$

Wie sich herausstellt hat diese Korrespondenz eine starke Verallgemeinerung auf sogenannte perfektoide Körper.

Definition 6.2. Ein *perfektoider Körper* ist ein vollständiger nichtarchimedischer reell bewerteter Körper $(K, |\cdot|)$, dessen Bewertung $|\cdot|$ nicht diskret ist und dessen Restklassenkörper k Charakteristik $p > 0$ hat, so dass der Frobenius

$$\begin{aligned} \mathcal{O}_K/_{(p)} &\to \mathcal{O}_K/_{(p)} \\ x &\mapsto x^p \end{aligned}$$

surjektiv ist.

Ist $(K, |\cdot|)$ ein vollständiger nichtarchimedisch reell bewerteter Körper von positiver Charakteristik $p > 0$ mit $|\cdot|$ einer nichtdiskreten Bewertung, so ist die Bedingung, dass der Frobenius surjektiv ist, äquivalent dazu, dass K perfekt ist.

Der Körper $\mathbb{F}_p(\!(T)\!)$ ist nicht perfekt, da T keine p-te Wurzel besitzt. Wir können aber seine Vervollkommnung (auch Perfektion) betrachten:

$$\widehat{\mathbb{F}_p(\!(T^{1/p^\infty})\!)} := \bigcup_{n=0}^{\infty} \widehat{\mathbb{F}_p(\!(T^{1/p^n})\!)}.$$

Die Körper $\mathbb{F}_p(\!(T^{1/p^n})\!)$ sind alle isomorph zu $\mathbb{F}_p(\!(T)\!)$:

$$\begin{aligned} \mathbb{F}_p(\!(T^{1/p^n})\!) &:= \mathbb{F}_p(\!(T)\!)[S]/_{(S^p - T)} \\ &= \mathbb{F}_p(\!(S)\!). \end{aligned}$$

Mit dieser Betrachtung sind aber die Übergangsabbildungen gegeben durch $x \mapsto x^p$. Die Erweiterung $\mathbb{F}_p(\!(T^{1/p^\infty})\!)/\mathbb{F}_p(\!(T)\!)$ ist rein inseparabel. Darum erhalten wir einen Isomorphismus der absoluten Galoisgruppen

$$G_{\mathbb{F}_p(\!(T^{1/p^\infty})\!)} \simeq G_{\mathbb{F}_p(\!(T)\!)}.$$

Lemma 6.3. *Sei $(K, |\cdot|)$ ein vollständiger bewerteter Körper und L/K eine algebraische Erweiterung. Dann gilt*

$$G_{\widehat{L}} \simeq G_L.$$

Beweis. Die Bewertung $|\cdot|$ hat nach Korollar 4.22 eine eindeutige Fortsetzung auf jede endliche Erweiterung von K, also auch auf jede algebraische Erweiterung von K. Ist M/L endlich und galoissch, dann ist $\mathrm{Gal}(\widehat{M}/\widehat{L})$ nach Proposition 4.38 identisch mit der Zerlegungsgruppe der Bewertung auf M. Aber da die Fortsetzungen der Bewertungen in diesem Kontext eindeutig sind, ist die Zerlegungsgruppe bereits die gesamte Galoisgruppe $\mathrm{Gal}(M/L)$. □

Eine direkte Folgerung des Lemmas ist, dass

$$G_{\widehat{F_p(\!(T^{1/p^\infty})\!)}} \simeq G_{F_p(\!(T^{1/p^\infty})\!)} \simeq G_{F_p(\!(T)\!)}.$$

Bisher haben wir eine Seite des Theorems von Fontaine und Wintenberger als die Galoisgruppe des perfektoiden Körpers $\widehat{F_p(\!(T^{1/p^\infty})\!)}$ identifiziert. Nun betrachten wir $\mathbb{Q}_p(\mu_{p^\infty})$.

Beispiel 6.4. Wir betrachten den Körper

$$K = \widehat{\mathbb{Q}_p(\mu_p^\infty)}.$$

Er trägt die eindeutige Fortsetzung der p-adischen Bewertung $|\cdot|_p$ von $\mathbb{Q}_p$. Offensichtlich ist K vollständig, und wir haben in Beispiel 4.32 gesehen, dass die Bewertung auf $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ nicht diskret ist. Es bleibt zu zeigen, dass der Frobenius modulo p ein surjektiver Endomorphismus ist.

Der Bewertungsring $\mathcal{O}_K$ ist die Vervollständigung von

$$\mathbb{Z}_p[\zeta_p, \zeta_{p^2}, \zeta_{p^3}, \ldots]$$

für ein kompatibles System $(\zeta_{p^n})_{n\in\mathbb{N}}$ von primitiven p^n-ten Einheitswurzeln. Mit kompatibel meinen wir, dass

$$(\zeta_{p^n})^p = \zeta_{p^{n-1}}$$

für alle $n \in \mathbb{N}$. Wir können diesen Ring folgendermaßen als Quotienten des Polynomrings in unendlich vielen Variablen schreiben:

$$\mathbb{Z}_p[\zeta_p, \zeta_{p^2}, \ldots] = \mathbb{Z}_p[X_1, X_2, \ldots] \Big/ \left(\tfrac{X_1^p-1}{X_1-1}, X_2^p - X_1, X_3^p - X_2, \ldots\right).$$

Modulo p erhalten wir

$$\begin{aligned}\mathcal{O}_K \big/ (p) &= \mathbb{Z}_p[\zeta_p, \zeta_{p^2}, \ldots] \big/ (p) \\ &= \mathbb{F}_p[X_1, X_2, \ldots] \Big/ \left(\tfrac{X_1^p-1}{X_1-1}, X_2^p - X_1, X_3^p - X_2, \ldots\right).\end{aligned}$$

Da wir uns nun in Charakteristik p befinden, gilt

$$\frac{X_1^p - 1}{X_1 - 1} = \frac{(X_1-1)^p}{X_1-1} = (X_1-1)^{p-1}.$$

Da der Frobenius ein Homomorphismus ist, reicht es zu zeigen, dass die Erzeuger x_i alle p^n-ten Wurzeln besitzen. Das stimmt aber nach Konstruktion durch die Relationen $X_{i+1}^p - X_i$.

Jetzt wissen wir, dass auch $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ perfektoid ist. Weiterhin wissen wir, da die Vervollständigung die Galoisgruppe nicht verändert, dass

$$G_{\widehat{\mathbb{Q}_p(\mu_{p^\infty})}} \simeq G_{\mathbb{Q}_p(\mu_{p^\infty})}.$$

Wir können das Theorem von Fontaine und Wintenberger also umformulieren als

$$G_{\widehat{\mathbb{Q}_p(\mu_{p^\infty})}} \simeq G_{\widehat{F_p(\!(T^{1/p^\infty})\!)}},$$

wobei beide Seiten absolute Galoisgruppen perfektoider Körper sind.

6.2. **Der Tilting-Funktor.** Wir wollen zu einer Verallgemeinerung des Theorems von Fontaine und Wintenberger kommen, die $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ mit einem beliebigen perfektoiden Körper der Charakteristik 0 ersetzt. Dann kommt aber die Frage auf, wie man sein Äquivalent in Charakteristik p konstruiert. Die Antwort ist durch den Tilting-Funktor gegeben, den wir in diesem Abschnitt konstruieren.

Zur Vorbereitung erinnern wir uns an das Konzept des inversen (auch „projektiven“) Limes. Der Einfachheit halber betrachten wir nur Indexmengen, die zu $\mathbb{N}$ isomorph sind. (Allgemeiner können wir eine orientierte partiell geordnete Menge oder sogar eine cofiltrierte Kategorie betrachten.)

Definition 6.5. Sei $\mathcal{C}$ eine Kategorie und $(X_i)_{i\in\mathbb{N}}$ Objekte in $\mathcal{C}$, die durch Morphismen

$$\ldots \xrightarrow{f_4} X_4 \xrightarrow{f_3} X_3 \xrightarrow{f_2} X_2 \xrightarrow{f_1} X_1$$

verbunden sind. Ein *inverser Limes* von $(X_i)_{i\in\mathbb{N}}$ in $\mathcal{C}$ ist ein Objekt X in $\mathcal{C}$ zusammen mit Morphismen

$$X \xrightarrow{\pi_i} X_i$$

so dass die Diagramme

$$\begin{array}{ccc} X & \xrightarrow{\pi_{i+1}} & X_{i+1} \\ & \searrow^{\pi_i} & \downarrow{\scriptstyle f_i} \\ & & X_i \end{array}$$

kommutieren, und X ist universell mit dieser Eigenschaft. Wir verwenden die Notation

$$\varprojlim_{i\in\mathbb{N}} X_i$$

für den inversen Limes. Die Sammlung der $(X_i)_{i\in\mathbb{N}}$ zusammen mit den Morphismen f_i heißt *inverses System* in $\mathcal{C}$.

Lemma 6.6. *Sei $(X_i)_{i\in\mathbb{N}}$ ein inverses System in der Kategorie der Mengen/Gruppen/Ringe/topologischen Räume/topologischen Ringe. Dann existiert der inverse Limes der $(X_i)_{i\in\mathbb{N}}$ und ist gegeben durch*

$$\varprojlim_{i\in\mathbb{N}} X_i = \left\{ (x_i)_{i\in\mathbb{N}} \in \prod_{i=1}^{\infty} X_i \mid f_i(x_{i+1}) = x_i \right\}.$$

Die Gruppen-/Ring-Struktur kommt von der entsprechenden Struktur auf dem Produkt, und die Topologie ist die Unterraum-Topologie von der Produkt-Topologie auf $\prod_{i=1}^{\infty} X_i$.

Beispiel 6.7. Für p prim ist

$$\mathbb{Z}_p \simeq \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z}.$$

Um das zu sehen, betrachten wir die Projektion

$$\mathbb{Z}_p \overset{\pi_n}{\twoheadrightarrow} \mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Nach der universellen Eigenschaft des inversen Limes bekommen wir einen Homomorphismus

$$f : \mathbb{Z}_p \to \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \left\{ (x_i)_{i\in\mathbb{N}} \in \prod_{i=1}^{\infty} \mathbb{Z}/p^n\mathbb{Z} \mid x_{n+1} \equiv x_n \mod p^n \right\}.$$

f ist injektiv: ist $f(x) = 0$, so bedeutet das, dass

$$x \equiv 0 \mod p^n\mathbb{Z}_p$$

für alle $n \in \mathbb{N}$. In der Sprache von Bewertungen bedeutet das

$$|x|_p \leq p^{-n}$$

für alle $n \in \mathbb{N}$. Aber das impliziert $|x|_p = 0$, also $x = 0$.

f ist surjektiv: für ein Element $(x_n)_{n\in\mathbb{N}} \in \varprojlim_{n\in\mathbb{N}}$ wählen wir Lifts $y_n \in \mathbb{Z}$ von x_n. Dann gilt für $m \geq n$

$$y_m \equiv y_n \mod p^n,$$

oder anders ausgedrückt,

$$|y_m - y_n|_p \leq p^{-n}.$$

Darum ist $(y_n)_{n\in\mathbb{N}}$ eine Cauchyfolge in $\mathbb{Z}$, die gegen ein $x \in \mathbb{Z}_p$ konvergiert. Dann ist $f(x) = (x_n)_{n\in\mathbb{N}}$. Natürlich muss man noch prüfen, dass dieser Isomorphismus topologisch ist.

Nun kommen wir zurück zur Konstruktion des Tilting-Funktors. Sei $(K, |\cdot|)$ ein vollständiger nichtarchimedisch reell bewerteter Körper von gemischter Charakteristik $(0, p)$, das heißt K hat Charakteristik 0 und der Restklassenkörper $k = {}^{\mathcal{O}_K}/_{\mathfrak{m}_K}$ hat Charakteristik $p > 0$.

Der Frobenius-Homomorphismus

$$\begin{aligned}\Phi : {}^{\mathcal{O}_K}/_{(p)} &\to {}^{\mathcal{O}_K}/_{(p)}\\ x &\mapsto x^p\end{aligned}$$

definiert ein inverses System

$$\ldots \xrightarrow{\Phi} {}^{\mathcal{O}_K}/_{(p)} \xrightarrow{\Phi} {}^{\mathcal{O}_K}/_{(p)} \xrightarrow{\Phi} {}^{\mathcal{O}_K}/_{(p)}.$$

Definition 6.8. Der *Tilt* von $\mathcal{O}_K$ ist

$$\begin{aligned}\mathcal{O}_K^\flat &:= \varprojlim_{n\in\mathbb{N}} {}^{\mathcal{O}_K}/_{(p)}\\ &= \left\{(x_n)_{n\in\mathbb{N}} \in \prod_{n\in\mathbb{N}} {}^{\mathcal{O}_K}/_{(p)} \mid x_{n+1}^p = x_n\right\}.\end{aligned}$$

Um $\mathcal{O}_K^\flat$ zu verstehen, ist der folgende Isomorphismus nützlich.

Lemma 6.9. *Sei R ein p-adisch vollständiger Ring (beispielsweise $R \simeq \varprojlim_{n\in\mathbb{N}} {}^{R}/_{p^n R}$). Die Projektion $\pi : R \to {}^{R}/_{(p)}$ induziert dann einen Isomorphismus multiplikativer Monoide*

$$\varprojlim_{\Phi} R \xrightarrow{\sim} \varprojlim_{\Phi} {}^{R}/_{(p)}.$$

Mit Φ meinen wir die Abbildung

$$\begin{aligned}\Phi : R &\to R\\ x &\mapsto x^p.\end{aligned}$$

Das ist kein Ringhomomorphismus. Er respektiert nur die Multiplikation, aber nicht die Addition.

Lemma 6.10. *$\mathcal{O}_K^\flat$ ist ein Bewertungsring.*

Beweis. Zuerst zeigen wir, dass $\mathcal{O}_K^\flat$ ein Integritätsring ist, also dass es keine Nullteiler gibt. Nach Lemma 6.9 reicht es zu prüfen, dass für $(x_n)_{n\in\mathbb{N}}, (y_n)_{n\in\mathbb{N}} \in \varprojlim_{\Phi} \mathcal{O}_K$ mit $x_n y_n = 0\ \forall n \in \mathbb{N}$ gilt, dass entweder $(x_n)_{n\in\mathbb{N}} = 0$ oder $(y_n)_{n\in\mathbb{N}} = 0$. Aber das ist klar, da $\mathcal{O}_K$ nullteilerfrei ist.

Sei $x \in K(\mathcal{O}_K^\flat)^\times$ nicht in $\mathcal{O}_K^\flat$. Wir wollen zeigen, dass $x^{-1} \in \mathcal{O}_K^\flat$. Das Element x hat eine Darstellung als

$$x = \frac{(a_n)_{n\in\mathbb{N}}}{(b_n)_{n\in\mathbb{N}}},$$

für $(a_n)_{n\in\mathbb{N}}, (b_n)_{n\in\mathbb{N}} \in \varprojlim_\Phi \mathcal{O}_K$ und $b_n \neq 0$. Ist $\frac{a_n}{b_n} \in \mathcal{O}_K$, dann ist auch $\frac{a_{n+1}}{b_{n+1}} \in \mathcal{O}_K$, da $\left(\frac{a_{n+1}}{b_{n+1}}\right)^p = \frac{a_n}{b_n}$. Also ist $x \in \mathcal{O}_K$ genau dann, wenn $\frac{a_1}{b_1} \in \mathcal{O}_K$. Aber da $\mathcal{O}_K$ ein Bewertungsring ist, ist $\frac{b_1}{a_1} \in \mathcal{O}_K$, und daher $\frac{1}{x} \in \mathcal{O}_K$. □

Definition 6.11. Der *Tilt* $K^\flat$ von K ist der Quotientenkörper $K(\mathcal{O}_K^\flat)$ von $\mathcal{O}_K^\flat$. Er ist ein bewerteter Körper mit Bewertungsring $\mathcal{O}_{K^\flat} = \mathcal{O}_K^\flat$. Weiter ist $K^\flat$ von Charakteristik p.

Beispiel 6.12. Wir wollen den Tilt von $\widehat{\mathbb{Q}_p(\mu_{p^\infty})}$ berechnen. Sein Bewertungsring ist $\widehat{\mathbb{Z}_p(\mu_{p^\infty})}$, und nach Beispiel 6.4 ist

$$\begin{aligned}\widehat{\mathbb{Z}_p(\mu_{p^\infty})} &= \mathbb{F}_p[X_1, X_2, X_3, \ldots]/((X_1-1)^{p-1}, X_2^p - X_1, X_3^p - X_2, \ldots)\\ &= \mathbb{F}_p[X_1^{1/p^\infty}]/(X_1-1)^{p-1}\\ &= \mathbb{F}_p[(T+1)^{1/p^\infty}]/(T^{p-1})\\ &= \mathbb{F}_p[T^{1/p^\infty}]/(T^{p-1})\end{aligned}$$

Der Tilt von $\widehat{\mathbb{Z}_p(\mu_{p^\infty})}$ ist also

$$\begin{aligned}\varprojlim_\Phi \widehat{\mathbb{Z}_p(\mu_{p^\infty})}/(p) &= \varprojlim_\Phi \mathbb{F}_p[T^{1/p^\infty}]/(T^{p-1})\\ &= \widehat{\mathbb{F}_p[\![T^{1/p^\infty}]\!]}\end{aligned}$$

Insbesondere ist

$$\left(\widehat{\mathbb{Q}_p(\mu_{p^\infty})}\right)^\flat = \widehat{F_p(\!(T^{1/p^\infty})\!)}.$$

6.3. **Strikte p-Ringe.** In Abschnitt 6.2 haben wir für einen perfektoiden Körper K den Tilt $K^\flat$ untersucht. Das ist ein Körper der Charakteristik $p > 0$. Wir wollen uns nun der Frage widmen, wie man andererseits aus einem perfektoiden Körper der Charakteristik $p > 0$ einen perfektoiden Körper der Charakteristik $(0, p)$ konstruieren kann.

Lemma 6.13. *Sei R ein Ring und $n \in \mathbb{N}$. Dann ist*

$$\begin{aligned}\theta_n : R/(p) &\to R/(p^{n+1})\\ x &\mapsto x^{p^n}\end{aligned}$$

eine wohldefinierte Monoidabbildung.

Beweis.

$$\begin{aligned}R &\to R/(p^{n+1})\\ x &\mapsto x^{p^n}\end{aligned}$$

ist eine wohldefinierte Abbildung multiplikativer Monoide. Wir müssen noch zeigen, dass für $x, y \in R$ mit $x \equiv y \mod p$ folgt, dass $x^{p^n} \equiv y^{p^n}$. Dann faktorisiert die Abbildung über $R/(p)$. Das sieht man per Induktion über n indem man die Binomialkoeffizienten in $(x-y)^p$ untersucht. □

Wir wollen eine Klasse von Ringen R definieren, für die wir R aus ${}^{R}/_{(p)}$ rekonstruieren können. Es ist naheliegend, zu fordern, dass R p-adisch vollständig sein soll, also

$$R = \varprojlim_{n\in\mathbb{N}} {}^{R}/_{(p^n)}.$$

Dann wäre die Strategie, schrittweise ${}^{R}/_{(p^n)}$ aus ${}^{R}/_{(p^{n-1})}$ zu rekonstruieren. Insbesondere sollte für zwei solcher Ringe R und S gelten

$$\operatorname{Hom}\left({}^{R}/_{(p^{n+1})}, {}^{S}/_{(p^{n+1})}\right) \simeq \operatorname{Hom}\left({}^{R}/_{(p)}, {}^{S}/_{(p)}\right).$$

Mithilfe des letzten Lemmas könnten wir folgendermaßen vorgehen. Für

$$\varphi_1 : {}^{R}/_{(p)} \longrightarrow {}^{S}/_{(p)}$$

wollen wir einen Lift

$$\varphi_n : {}^{R}/_{(p^n)} \longrightarrow {}^{S}/_{(p^n)}$$

konstruieren. Dann schauen wir uns das folgende Diagramm an.

$$\begin{array}{ccc} {}^{R}/_{(p)} & \xrightarrow{\varphi_1} & {}^{R}/_{(p)} \\ \downarrow{\scriptstyle \theta_n} & & \downarrow{\scriptstyle \theta_n} \\ {}^{R}/_{(p^{n+1})} & \overset{\varphi_n}{\dashrightarrow} & {}^{R}/_{(p^{n+1})} \end{array}$$

Um φ_n zu konstruieren, so dass das Diagramm kommutiert, würde man mit $x \in R$ anfangen und dann $y \in R$ finden mit $y^{p^n} \equiv x \mod p$. Dann setzt man $\varphi_n([x]) := \theta_n \circ \varphi_1([y])$. Damit das faktorisiert, sollte der Frobenius

$$\begin{aligned} \Phi : {}^{R}/_{(p)} &\to {}^{R}/_{(p)} \\ x &\mapsto x^p \end{aligned}$$

ein Isomorphismus sein, ${}^{R}/_{(p)}$ sollte also perfekt sein. Das motiviert folgende Definition.

Definition 6.14. Ein Ring R ist ein *strikter p-Ring*, wenn er p-torsionsfrei und p-adisch vollständig ist, und ${}^{R}/_{(p)}$ perfekt ist.

Beispiel 6.15. $\mathbb{Z}_p$ ist ein perfekter p-Ring, aber $\mathbb{Z}_p[\sqrt{p}]$ ist kein perfekter p-Ring, da

$$\begin{aligned} {}^{\mathbb{Z}_p[\sqrt{p}]}/_{(p)} &= {}^{\mathbb{Z}_p[T]}/_{(p, T^2-p)} \\ &= {}^{\mathbb{F}_p[T]}/_{(T^2)} \end{aligned}$$

nicht perfekt ist. Das kann man ganz schnell daran sehen, dass perfekte Ringe immer reduziert sind, also keine nilpotenten Elemente haben. Explizit kann man es daran sehen, dass $[T]^p = 0$ gilt in ${}^{\mathbb{F}_p[T]}/_{(T^2)}$, und damit der Frobenius nicht injektiv ist.

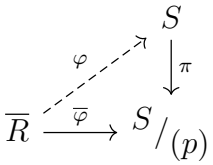
Lemma 6.16. *Sei $\overline{R}$ ein perfekter Ring der Charakteristik p, S ein p-adisch vollständiger Ring mit kanonischer Projektion $\pi : S \to {}^{S}/_{(p)}$ und*

$$\overline{\varphi} : \overline{R} \to {}^{S}/_{(p)}$$

ein Ringhomomorphismus. Dann gibt es eine eindeutig bestimmte multiplikative Abbildung

$$\varphi : \overline{R} \to S,$$

so dass das Diagramm



kommutiert.

Explizit ist φ folgendermaßen definiert: Für $x \in \overline{R}$ und $n \in \mathbb{N}$ wählen wir $x_n \in S$ mit

$$x_n \equiv \overline{\varphi}(\overline{x}^{p^{-n}}) \mod p.$$

Dann gilt

$$\varphi(\overline{x}) \equiv x_n^{p^n} \mod p^{n+1}$$

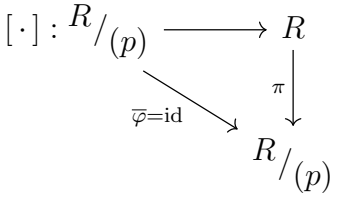
und folglich

$$\varphi(\overline{x}) = \lim_{n\to\infty} x_n^{p^n}.$$

Insbesondere können wir Lemma 6.16 für einen strikten p-Ring R auf die Identität

$$\overline{\varphi} = \mathrm{id} : {}^{R}/_{(p)} \to {}^{R}/_{(p)}$$

anwenden, und erhalten eine eindeutig bestimmte multiplikative Abbildung



Definition 6.17. Die Abbildung $[\,\cdot\,]$ heißt *Teichmüller-Lift.*

Beispiel 6.18. Wir wollen den Teichmüller-Lift von $\mathbb{Z}_p$ bestimmen. Dazu erinnern wir uns daran, dass die Projektion $\mathbb{Z}_p \to \mathbb{F}_p$ einen Isomorphismus

$$\psi : \mu_{p-1}(\mathbb{Z}_p) \xrightarrow{\sim} \mu_{p-1}(\mathbb{F}_p) = \mathbb{F}_p^\times$$

definiert. Dann ist für $\overline{x} \in \mathbb{F}_p^\times$

$$[\overline{x}] = \psi^{-1}(\overline{x})$$

und $[0] = 0$. Jedes Element x eines strikten p-Rings R hat eine eindeutige Darstellung

$$x = \sum_{n=0}^{\infty} [x_n] p^n, \quad x_n \in {}^{R}/_{(p)}.$$

Diese erhält man folgendermaßen: Sei $x_0 = \pi(x)$ für die kanonische Projektion $\pi : R \to {}^{R}/_{(p)}$. Angenommen wir haben $x_0, \ldots, x_N \in {}^{R}/_{(p)}$ gefunden, so dass

$$x - \sum_{n=0}^{N} [x_n] p^n \in p^{n+1} R.$$

Dann setzen wir

$$x_{N+1} := \pi\left(\frac{x - \sum_{n=0}^{N}[x_n]p^n}{p^{n+1}}\right).$$

Satz 6.19. *Der Funktor*

$$\{ \textit{ strikte } p\textit{-Ringe } \} \to \{ \textit{ perfekte Ringe in } \operatorname{char} p \}$$
$$R \mapsto {}^{R}\!/_{(p)}$$

ist eine Kategorienäquivalenz.

Beweisidee. Um zu zeigen, dass der Funktor volltreu ist, müssen wir für strikte p-Ringe R und S überprüfen, dass

$$\operatorname{Hom}(R,S) \xrightarrow{\sim} \operatorname{Hom}\left({}^{R}\!/_{(p)}, {}^{S}\!/_{(p)}\right).$$

Für $\overline{\varphi} : {}^{R}\!/_{(p)} \to {}^{S}\!/_{(p)}$ brauchen wir einen eindeutig bestimmten Homomorphismus $\varphi : R \to S$, dessen Reduktion modulo p gleich $\overline{\varphi}$ ist. Mithilfe von Lemma 6.16 finden wir zunächst

$$\varphi' : {}^{R}\!/_{(p)} \to S,$$

so dass das Diagramm

$$\begin{array}{ccc} & & S \\ & \overset{\varphi'}{\nearrow} & \downarrow \pi \\ \overline{R} & \xrightarrow{\overline{\varphi}} & {}^{S}\!/_{(p)} \end{array}$$

kommutiert. Dann setzen wir für $x = \sum_{n=0}^{\infty}[x_n]p^n \in R$:

$$\varphi(x) = \varphi\left(\sum_{n=0}^{\infty}[x_n]p^n\right) = \sum_{n=0}^{\infty}\varphi'(x_n)p^n.$$

Jetzt müsste man noch nachrechnen, dass φ tatsächlich das eindeutig bestimmte Urbild von $\overline{\varphi}$ ist. Das aufwändigste daran ist, zu zeigen, dass φ verträglich mit der Addition ist.

Als zweites ist die wesentliche Surjektivität zu zeigen. Wir müssen also für einen perfekten Ring $\overline{R}$ der Charakteristik p einen strikten p-Ring finden, so dass ${}^{R}\!/_{(p)} \simeq \overline{R}$. Dafür wählen wir eine Surjektion

$$\psi : \mathbb{F}_p[M] \to \overline{R}$$

für eine geeignete Menge M[1] und setzen $\overline{I} := \ker(\psi)$. Da $\overline{R}$ perfekt ist, faktorisiert ψ über

$$\psi_\infty : \mathbb{F}_p[M^{-p^\infty}] \to \overline{R}.$$

Sei R_0 die p-adische Vervollständigung von $\mathbb{Z}_p[M^{-p^\infty}] = \bigcup_{n=0}^{\infty}\mathbb{Z}[M^{-p^n}]$. Das ist ein strikter p-Ring mit

$${\mathbb{Z}_p[M^{-p^\infty}]}\!/_{(p)} = \mathbb{F}_p[M^{-p^\infty}].$$

Wir setzen

$$I = \left\{\sum_{n=0}^{\infty}[\overline{x}_n]p^n \;\middle|\; \overline{x}_i \in \overline{I}\right\}.$$

[1] $\mathbb{F}_p[M]$ ist der Polynomring mit einer Variable für jedes Element von M.

Dann ist $R := {}^{R_0}/_I$ der Ring, den wir suchen. □

Definition 6.20. Für einen perfekten Ring $\overline{R}$ heißt der Ring R aus Satz 6.19 *Wittring* von $\overline{R}$. Wir schreiben dafür $R = W(\overline{R})$.

Somit haben wir zueinander äquivalente Kategorienäquivalenzen

$$\begin{aligned} \{ \text{ strikte } p\text{-Ringe } \} &\to \{ \text{ perfekte Ringe in char } p \} \\ R &\mapsto {}^{R}/_{(p)} \\ W(\overline{R}) &\leftarrow\!\shortmid \overline{R}. \end{aligned}$$

Wir können das Gelernte nun anwenden auf einen perfektoiden Körper $(K, \mathcal{O}_K)$ mit Tilt $(K^\flat, \mathcal{O}_{K^\flat})$. Wir betrachten die Projektion

$$\begin{aligned} pr_0 : \mathcal{O}_{K^\flat} = \varprojlim_{\Phi} {}^{\mathcal{O}_K}/_{(p)} &\to {}^{\mathcal{O}_K}/_{(p)} \\ (\dots, x_2, x_1, x_0) &\mapsto x_0 \end{aligned}$$

und die natürliche Projektion

$$\pi : \mathcal{O}_K \to {}^{\mathcal{O}_K}/_{(p)}.$$

Dann gibt es nach Lemma 6.16 eine Abbildung $(\cdot)^\sharp$, so dass folgendes Diagramm kommutiert.

$$\begin{array}{ccc} & & \mathcal{O}_K \\ & \overset{(\cdot)^\sharp}{\nearrow} & \big\downarrow \pi \\ \mathcal{O}_{K^\flat} & \xrightarrow[pr_0]{} & {}^{\mathcal{O}_K}/_{(p)} \end{array}$$

Dann konstruieren wir einen Homomorphismus

$$\begin{aligned} \theta : W(\mathcal{O}_K^\flat) &\to \mathcal{O}_K \\ \sum_{n=0}^{\infty} [x_n] p^n &\mapsto \sum_{n=0}^{\infty} x_n^\sharp p^n. \end{aligned}$$

Wir definieren

$$\begin{aligned} |\cdot|^\flat : \mathcal{O}_{K^\flat} &\to \mathbb{R}_{\geq 0} \\ x &\mapsto |x^\sharp|. \end{aligned}$$

Satz 6.21. *(i)* $|\cdot|^\flat$ *ist die zu* $\mathcal{O}_{K^\flat}$ *gehörige Bewertung auf* $K^\flat$.
(ii) $K^\flat$ *ist vollständig.*
(iii) $|K^\times| = |(K^\flat)^\times|^\flat$
(iv) $pr_0 : \mathcal{O}_{K^\flat} \to {}^{\mathcal{O}_K}/_{(p)}$ *induziert einen Isomorphismus*

$$ {}^{\mathcal{O}_{K^\flat}}/_{(z)} \simeq {}^{\mathcal{O}_K}/_{(p)}.$$

für alle $z \in \mathcal{O}_{K^\flat}$ *mit* $|z|^\flat = |p| = p^{-1}$. *Insbesondere sind die Restklassenkörper von* $\mathcal{O}_K$ *und* $\mathcal{O}_{K^\flat}$ *isomorph.*
(v) $\theta : W(\mathcal{O}_{K^\flat}) \to \mathcal{O}_K$ *ist surjektiv.*

6.4. **Die Tilting-Äquivalenz.** Hier könnte man eventuell noch etwas zu den Resultaten sagen. Z.B. zum Thm 6.24 Nun können wir die angekündigte Verallgemeinerung des Theorems von Fontaine und Wintenberger formulieren. Diese sagt aus, dass der Tilting-Funktor uns für einen perfektoiden Körper K eine Kategorienäquivalenz von endlichen Erweiterungen perfektoider Körper L/K und endlichen Erweiterungen des Tilts $K^\flat$ gibt.

Definition 6.22. $z = \sum_{n=0}^{\infty}[z_n]p^n \in W(\mathcal{O}_F)$ heißt *primitiv*, falls $|z_n|^\flat = p^{-1}$ und $p^{-1}(z-[z_0]) \in W(\mathcal{O}_F)^\times$, also $z = [z_0] + up$, $u \in W(\mathcal{O}_F)^\times$.

Satz 6.23.

$$\{ \text{ perfektoide Körper } \} \overset{\sim}{\leftrightarrow} \{(F, I) \mid F \text{ perfektoid von char } p,\ I = (z) \text{ für } z \text{ primitiv}\}$$

$$K \mapsto \left(K^\flat, \ker\left(\theta : W(\mathcal{O}_{K^\flat}) \to \mathcal{O}_K\right)\right)$$

$$\left(W(\mathcal{O}_K)/I\right)[p^{-1}] \mapsfrom (F, I)$$

Theorem 6.24. *([Sch12, Theorem 3.7.].) Sei K perfektoid und L/K endlich. Dann ist L perfektoid und*

$$\{ \ L/K \text{ endlich } \} \xrightarrow{\sim} \left\{ F/K^\flat \text{ endlich} \right\}$$

$$L \mapsto L^\flat.$$

Insbesondere ist $G_K \simeq G_{K^\flat}$. Hier wurde nicht erwähnt, dass $(\cdot)^\flat$ den Grad der Erweiterung erhält.

Literatur

[EP05] Antonio J. Engler and Alexander Prestel. *Valued fields*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2005.

[FW79] Jean-Marc Fontaine and Jean-Pierre Wintenberger. Le "corps des normes" de certaines extensions algébriques de corps locaux. *CR Acad. Sci. Paris Sér. AB*, 288(6):367–370, 1979.

[Neu11] Jürgen Neukirch. *Klassenkörpertheorie*. Springer-Lehrbuch. Springer, Heidelberg, 2011.

[Sch12] Peter Scholze. Perfectoid spaces. *Publications mathématiques de l'IHÉS*, 116(1):245–313, 2012.

Email address: huebner@math.uni-frankfurt.de

Robert Mayer Strasse 6-8, 60325 Frankfurt