Mitschrieb zur Vorlesung: Algebraische Zahlentheorie I

Prof. Dr. Schmidt

Vorlesung Wintersemester 2005/2006

Letzte Aktualisierung und Verbesserung: 26. April 2008

Mitschrieb der Vorlesung Algebraische Zahlentheorie I
von Herrn Prof. Dr. Schmidt im Wintersemester 2005/2006
von Marco Schreck.

Dieser Mitschrieb erhebt keinen Anspruch auf Vollständigkeit und Korrektheit.
Kommentare, Fehler und Vorschläge und konstruktive Kritik bitte an Marco.Schreck@gmx.de.

Inhaltsverzeichnis

Satz:

Es sei $A \subseteq B$ und $b_1, \ldots, b_n \in B$. Die b_i sind ganz über A genau dann, wenn $A[b_1, \ldots, b_n]$ endlich erzeugter A-Modul ist.

Beweis „⇒“:

Wir führen den Beweis mit vollständiger Induktion. Den Fall $n = 1$ haben wir letztes mal bewiesen. Wir vollziehen nun den Induktionsschritt $n - 1 \mapsto n$. $b_1, \ldots, b_n$ sind ganz über A. Hieraus folgt, dass b_n ganz über $R := A[b_1, \ldots, b_{n-1}]$ ist. Nach dem Induktionsanfang folgt, dass $R[b_n] (= A[b_1, \ldots, b_n])$ ein endlich erzeugter R-Modul ist. Die Induktionsannahme besagt, dass R endlich erzeugter A-Modul ist. Denn schreibe:

$R[b_n] = Rc_1 + \ldots + Rc_t$ und $R = A \cdot d_1 + \ldots A \cdot d_s$

Hieraus ergibt sich dann, indem wir $R = Ad_1 + \ldots + Ad_s$ in $R[b_n]$ einsetzen:

$R[b_n] = Ac_1 \cdot d_1 + \ldots + Ac_t \cdot d_s$

Die $c_i d_i$ sind ein A-Erzeugendensystem. Damit ist die Behauptung bewiesen.

Beweis „⇐“:

Sei $A[b_1, \ldots, b_n]$ ein endlich erzeugter A-Modul, etwa $A[b_1, \ldots, b_n] = A \cdot \omega_1 + \ldots + A \cdot \omega_r$. Für beliebiges $b \in A[b_1, \ldots, b_n]$ gilt:

$$\exists\, a_{ij} \in A : \; b \cdot \omega_i = \sum_{j=1}^{r} a_{ij}\omega_j \text{ für } i = 1, \ldots, r$$

Dies können wir auch in Form einer Matrizengleichung aufschreiben. Nämlich folgt mit $a := (a_{ij})$ und I_r als der r-fachen Einheitsmatrix:

$$(b \cdot I_r - a) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_r \end{pmatrix} = 0$$

Nach der Vorbemerkung gilt:

$\det(b \cdot I_r - a) \cdot \omega_i = 0$ für alle i

Stelle nun die Eins des Polynomrings $A[b_1, \ldots, b_n]$ dar als Linearkombination der ω_i, also:

$1 = \alpha_1 \cdot \omega_1 + \ldots + \alpha_r \cdot \omega_r$ mit $\alpha_i \in A$

So folgt:

$$\det(b \cdot I_r - a) = \sum_{\rho=1}^{r} \alpha_\rho \underbrace{\det(b \cdot I_r - a) \cdot \omega_\rho}_{=0} = 0$$

$\det(b \cdot I_r - a) \equiv f(b)$ ist normiertes Polynom im Polynomring $A[X]$. Daraus folgt, dass b ganz über A ist. q.e.d.

Korrolar 2.2:

Seien $b_1, \ldots, b_n$ ganz über A. Dann folgt $\forall\, b \in A[b_1, \ldots, b_n]$: b ganz über A. Insbesondere ist $b_1 + b_2$ und $b_1 \cdot b_2$ ganz über A.

Korrolar 2.3:

Seien $A \subseteq B \subseteq C$ Ringerweiterungen. Falls B ganz über A und C ganz über B, dann gilt, dass C ganz über A ist.

Beweis:

Sei $c \in C$ mit $c^n + b_1 c^{b-1} + \ldots + b_n = 0$ für $b_v \in B$. Setze $R := A[b_1, \ldots, b_n] \subseteq B$. Weiterhin ist $R[c] = \langle 1, c, c^2, \ldots, c^{n-1} \rangle_R$ insbesondere endlich erzeugter R-Modul.Da B ganz über A ist, folgt aus Satz 2.1, dass R ein endlich erzeugter A-Modul ist. Damit ist $R[c] = A[b_1, \ldots, b_n, c]$ endlich erzeugter A-Modul, womit c ganz über A ist. q.e.d.

Definition:

Der Teilring(!) $\overline{A} := \{b \in B; b \text{ ganz über } A\} \subseteq B$ heißt der „**ganze Abschluss**“ von A in B. A heißt „**ganz abgeschlossen**“ in B, falls $A = \overline{A}$ ist. Falls A Integritätsbereich ist mit Quotientenkörper $K = \text{Quot}(A)$, so heißt der ganze Abschluss $\overline{A}$ von A in K die **Normalisierung** von A. Ein solches A heißt „**ganz abgeschlossen**“, falls $A = \overline{A}$.

Bemerkungen:

1.) Faktorielle Ringe sind stets abgeschlossen.

2.) Sei A ganz abgeschlossener Integritätsbereich, $K = \text{Quot}(A)$. Ferner sei L/K eine endliche Körpererweiterung ($\dim_K L < \infty$). B sei der ganze Abschluss von A in L. Dann ist B ganz abgeschlossen. Jedes $B \in L$ lässt sich darstellen in der Form $\beta = b/a$ mit $b \in B$ und $a \in A$. Für $\beta \in L$ ist β ganz über A genau dann, wenn Minimalpolynom $f_\beta(X) \in A[X]$.

Definition:

Sie $\alpha_1, \ldots, \alpha_n \in L$ eine Basis über K und L/K separabel.

$(x, y) := \text{Tr}_{L/K}(x \cdot y)$

Die Diskriminante ist nun definiert durch $d(\alpha_1, \ldots, \alpha_n) = \det((\alpha_i, \alpha_j)) = \det(\sigma_i(\alpha_j))^2$, wobei $\sigma_i \in \text{Mono}(L, \overline{K})$. Sei nun A ein ganz abgeschlossener Integrationsbereich $K := \text{Quot}(A)$. L/K sei endlich separabel und B der ganze Abschluss von A in L. ($\Rightarrow B \cap K = A$)

Bemerkung:

Für ein $x \in B$ gilt:

a.) $\text{Tr}_{L/K}(x)$, $N_{L/K}(x) \in A$

b.) $x \in B^\times \Leftrightarrow N_{L/K}(x) \in A^\times$

Lemma 2.4:

Seien $\alpha_1, \ldots, \alpha_n \in B$ eine K-Basis von L mit Diskriminante $d := d(\alpha_1, \ldots, \alpha_n)$. Dann gilt $d \cdot B \subseteq A \cdot \alpha_1 + \ldots + A \cdot \alpha_n$.

Beweis:

Sei $\alpha = \sum_{i=1}^{n} a_i \cdot \alpha_i \in B$ mit $a_i \in K$ eine Basisdarstellung. Wir erhalten ein lineares Gleichungssystem mit Lösungsvektor $(a_1, \ldots, a_n)$:

$$A \ni \beta_j = \text{Tr}(\alpha_j \cdot \alpha) = \sum_{i=1}^{n} a_i \cdot \text{Tr}(\alpha_i \alpha_j) = \sum_{i=1}^{n} a_i \cdot ((\alpha_i, \alpha_j))$$

$T := ((\alpha_i, \alpha_j))$ ist eine Matrix $\in A^{n \times n}$. Es gilt nun nach der vorherigen Definition $\det(T) = d$. Damit gilt also die Matrixgleichung $\vec{\beta} = T \cdot \vec{a}$. Die Determinante verschwindet nicht, weil die Spurform nicht entartet ist (Separabilität). Damit existiert die inverse Matrix $T^{-1} = d^{-1} \cdot T^+$, wobei $T^+ \in A^{n \times n}$ die Adjunkte ist. Mit $a_i \in d^{-1} \cdot A$ ergibt sich:

$$d \cdot \alpha = \sum_i d \cdot a_i \cdot \alpha_i \in \sum_i A \cdot \alpha_i$$

Bemerkung:

Die Basisdarstellung der Elemente von L über K ist für die Ringe B über A **nicht** mehr generell möglich.

Definition:

Ein System von Elementen $\omega_1, \ldots; \omega_n \in B$ heißt **Ganzheitsbasis** von L (über A), falls jedes $b \in B$ eindeutig darstellbar ist als Linearkombination:

$$b = \sum_{\nu=1}^{n} a_\nu \omega_\nu \text{ mit } a_\nu \in A$$

$\Leftrightarrow B$ ist freier A-Modul vom Rang $n = (L : K)$.

Satz 2.5:

Sei L/K eine separable, endliche Erweiterung und A ein Hauptidealring. Dann ist jeder endlich erzeugte B-Teilmodul $M \neq 0$ in L ein freier A-Modul vom Rang $(L : K)$. Insbesondere hat L Ganzheitsbasis über A.

Beweis:

Sei $M = B \cdot \mu_1 + \ldots + B \cdot \mu_r \neq 0$. $\alpha_1, \ldots, \alpha_n$ sei eine K-Basis von L. Wir wissen, dass $a_\nu \neq 0 \in A$ existieren, so dass $a_\nu \cdot \alpha_\nu \in B$ und dass $a_\rho \neq 0 \in A$ existieren mit $a_\rho \cdot \mu_\rho \in B$. Also ist für

$$a := \prod_{\nu=1}^{n} a_\nu$$

$\beta_\nu := a \cdot \alpha_\nu \in B \, (\nu = 1, \ldots, n)$

K-Basis von L. Aus dem Lemma 2.4 folgt, dass für $d := d(\beta_1, \ldots, \beta_n)$ gilt: $d \cdot B \subseteq A\beta_1 + \ldots + A\beta_n =: M_0$.
Für $a' := \prod_{\rho=1}^{r} a'_\rho$ gilt:

$$a' \cdot \mu_\rho \in B \Rightarrow \boxed{a'M \subseteq B}$$

Kombinieren wir dies, so folgt, dass $a' \cdot d \cdot M \subseteq d \cdot B \subseteq M_0$ freier A-Modul ist. Hier benötigen wir den Elementarteilersatz: „Jeder A-Teilmodul M' eines freien A-Moduls M ist selbst freier A-Modul mit $\mathrm{rg}(M') \leq \mathrm{rg}(M)$."
Hieraus folgt, dass $a' \cdot d \cdot M$ freier A-Modul ist. Dies ist äquivalent dazu, dass M freier A-Modul ist.

$$\mathrm{rg}(M) = \mathrm{rg}(a' \cdot d \cdot M) \leq \mathrm{rg}(M_0) = \mathrm{rg}(M_0 \cdot \mu_1) \subseteq B \cdot \mu_1 \subseteq M \leq \mathrm{rg}(M)$$

Satz:

Seien zwei Erweiterungen L/K und L'/K beide Galois-Erweiterungen vom jeweiligen Grad $n := (L : K)$ und $n' := (L' : K)$ mit $L \cap L' = K$ mit $K = \mathrm{Quot}(A)$. Seien $\omega_1, \ldots, \omega_n$ (bzw. $\omega'_1, \ldots, \omega'_{n'}$) Ganzheitsbasen von L (bzw. L') über A mit Diskriminanten d (bzw. d'). Falls $x, x' \in A$ existieren mit $xd + x'd' = 1$ (d und d' sind teilerfremd), so ist $\omega_i \cdot \omega'_j$ ($i = 1, \ldots, n$ und $j = 1, \ldots, n'$) eine Ganzheitsbasis von LL' mit Diskriminante $d^{n'} \cdot d'^{n}$.

Beweis:

Mit etwas Galois-Theorie folgt leicht, dass $\{\omega_i \cdot \omega'_j | i = 1, \ldots, n;\ j = 1, \ldots, n'\}$ eine K-Basis von LL' ist. Sei $\alpha \in LL'$ ganz (über A) mit Basisdarstellung

$$\alpha = \sum_{i,j} \alpha_{ij} \cdot \omega_i \cdot \omega'_j \text{ mit } a_{ij} \in K$$

Zu zeigen ist nun, dass $a_{ij} \in A$. Sei $G(LL'/L') = \{\sigma_1, \ldots, \sigma_n\}$ und $G(LL'/L) = \{\sigma'_1, \ldots, \sigma'_{n'}\}$, so folgt, dass die gesamte Galois-Gruppe gegeben ist durch $G(LL'/K) = \{\sigma_k \sigma'_l | k = 1, \ldots, n; l = 1, \ldots, n'\}$ Sortiere:

$$\alpha = \sum_j \underbrace{\left(\sum_i a_{ij} \omega_i \right)}_{\in L} \cdot \omega'_j \qquad (*)$$

Betrachte nun die auftretenden Matrizen:

$$T := (\sigma'_l \omega'_j) \in L'^{n' \times n'} \text{ und } a := (\sigma'_1 \alpha, \ldots, \sigma'_{n'} \alpha)^\intercal$$

Alle Elemente sind **ganz**, weil Automorphismen die Ganzheit erhalten ($f_\alpha(X) \in A[X]$, $\sigma(f_\alpha(\alpha)) = f_\alpha(\sigma(\alpha)) = 0$)

$b := (\beta_1, \ldots, \beta_{n'})^\intercal$

Hierbei gilt nun, wenn man σ'_1, …, $\sigma'_{n'}$ auf $(*)$ anwendet:

$\det(T)^2 = d'$ und $\boxed{Tb = a}$

Erinnere: Für die adjungierte Matrix $T^\#$ zu T gilt: $T^\# \cdot T = \det(T) \cdot I$. Es gilt nun weiter:

$T^\# Tb = T^\# a \Leftrightarrow \det(T) \cdot b = T^\# a$

Nach der Definition von $T^\#$ wissen wir, dass auch $T^\#$ Einträge aus ganzen Elementen besitzt, genauso wie a. Hieraus folgt, dass auch $\det(T) \cdot b$ und damit $\det(T)^2 \cdot b = d' \cdot b$ aus ganzen Elementen besteht. Das heißt:

$$d' \cdot \beta_j = \sum_i \underbrace{d' a_{ij}}_{\in K} \omega_i \text{ ist ganz } \forall\, j$$

Da $\{\omega_i\}$ eine Ganzheitsbasis von L ist, gilt $d' \cdot a_{ij} \subset A$. Analog ist $d \cdot a_{ij} \in A$.

$$a_{ij} = 1 \cdot a_{ij} = (xd + x'd') \cdot a_{ij} = x \underbrace{(da_{ij})}_{\in A} + x' \underbrace{(d' a_{ij})}_{\in A} \in A$$

Es bleibt noch die Diskrimante der Ganzheitsbasis $\{\omega_i \cdot \omega'_j\}$ zu bestimmen.

$\Delta = \det(M)^2$ für $M = (\sigma_k \sigma'_l(\omega_i \cdot \omega'_j)) = (\sigma_k(\omega_i) \cdot \sigma'_l(\omega'_j))$

Wende nun die Determinanten-Rechenregeln an für $Q := (\sigma_k(\omega_i))$ und $Q' := (\sigma'_l(\omega'_j))$. ($I_n$ sei die n-dimensionale Einheitsmatrix.)

$$M = \begin{pmatrix} Q & & 0 \\ & Q & \\ 0 & & Q \end{pmatrix} \cdot \begin{pmatrix} \sigma'_1(\omega'_1) \cdot I_n & & \sigma'_{n'}(\omega'_1) \cdot I_n \\ & & \\ \sigma'_1(\omega'_{n'}) \cdot I_n & & \sigma'_{n'}(\omega'_{n'}) \cdot I_n \end{pmatrix}$$

Es gilt $\det(M) = \pm \det(Q)^n \cdot \det(Q')^n$, da

$$\begin{pmatrix} \sigma'_1(\omega'_1) \cdot I_n & & \sigma'_{n'}(\omega'_1) \cdot I_n \\ & & \\ \sigma'_1(\omega'_{n'}) \cdot I_n & & \sigma'_{n'}(\omega'_{n'}) \cdot I_n \end{pmatrix} \sim \begin{pmatrix} Q' & & \\ & Q' & \\ & & Q' \end{pmatrix}$$

Was sich durch Permutation von Zeilen und Spalten ergibt.

Kapitel 1

Anwendung auf Zahlkörper K

$O = O_K$ sei der ganze Abschluss von $\mathbb{Z}$ in K. Er heißt der **Ring der ganzen Elemente** von K.

Bemerkung:

Jeder endlich erzeugte O-Teilmodul $\mathfrak{a}$ in K besitzt eine $\mathbb{Z}$-Basis $\alpha_1, \ldots, \alpha_n$ und die Diskriminante $d(\alpha_1, \ldots, \alpha_n) = \det(\sigma_j(\alpha_i))$ ist unabhängig von der gewählten $\mathbb{Z}$-Basis. Insbesondere existiert eine Genzheitsbasis von K über $\mathbb{Z}$.

Beweis:

Die Existenz der $\mathbb{Z}$-Basis folgt aus Satz 2.5 für die (separable) Erweiterung $K/\mathbb{Q}$, da $A = \mathbb{Z}$ Hauptidealring ist. Sei $\alpha'_1, \ldots, \alpha'_n$ eine andere $\mathbb{Z}$-Basis von $\mathfrak{a} = \mathbb{Z}\alpha_1 + \ldots + \mathbb{Z}\alpha_n$. Für Übergangsmatrix $T = (a_{ij})$ gegeben durch Darstellung

$$\alpha'_i = \sum_j a_{ij}\alpha_j$$

gilt: $T = \mathrm{GL}_n(\mathbb{Z})$. Insbesondere folgt $\det(T) \in \mathbb{Z}^\times$. Hieraus ergibt sich:

$$d(\alpha'_1, \ldots, \alpha'_n) = \det(\mathrm{Tr}(\alpha'_\mu \cdot \alpha'_\nu)) = \det\left(\mathrm{Tr}\left(\sum_{i=1}^n a_{\mu i}\alpha_i \cdot \sum_{j=1}^n a_{\nu j}\alpha_j\right)\right) = \det\left(\sum_i a_{\mu i}\sum_j a_{\nu j}\mathrm{Tr}(\alpha_i\alpha_j)\right) =$$
$$= \det(T)^2 \cdot d(\alpha_1, \ldots, \alpha_n)$$

Definition:

Die von der speziellen Basis $\alpha_1, \ldots, \alpha_n$ unabhängige Diskriminante einer $\mathbb{Z}$-Basis von $\mathfrak{a}$ bezeichnen wir mit $d(\mathfrak{a}) := d(\alpha_1, \ldots, \alpha_n)$. Speziell die Diskriminante einer Ganzheitsbasis $d_k := d(O_k)$ heißt die **Diskriminante des Zahlkörpers** K.

Satz:

Seien $\mathfrak{a}'$, $\mathfrak{a} \neq 0$ endlich erzeugte O-Teilmoduln von K mit $\mathfrak{a} \subseteq \mathfrak{a}'$. Dann ist der Index $(\mathfrak{a}' : \mathfrak{a})$ endlich und $d(\mathfrak{a}) = (\mathfrak{a}' : \mathfrak{a})^2 \cdot d(\mathfrak{a}')$. (Der Beweis folgt in der Übung mittels des Elementarteilersatzes.)

1.1 Ideale

Sei K ein fester Zahlkörper und $O = O_K$ der Ring der ganzen Elemente von K. $O^\times$ sei die Einheitengruppe.

Bemerkung 3.1:

Jedes Element $\alpha \neq 0$ aus $O \setminus O^\times$ lässt sich in O in ein Produkt irreduzibler Elemente zerlegen.

Beweis:

Falls α selbst schon irreduzibel ist, gibt es nichts weiter zu zeigen. Existieren β; $\gamma \in O \setminus O^\times$ mit $\alpha = \beta \cdot \gamma$, so gilt für $N := N_{K/\mathbb{Q}}$: $|N(\beta)| > 1 < |N(\gamma)|$. Es gilt $N(\alpha) = N(\beta) \cdot N(\gamma)$, also $1 < |N(\beta)| < |N(\alpha)|$, wobei $N(\beta) \in \mathbb{Z}$ und $N(\alpha) \in \mathbb{Z}$. Vollständige Induktion nach $m := |N(\alpha)|$ führt zur Behauptung.
Es tritt **aber** ein neues Phänomen (im Vergleich zu $\mathbb{Q}$, $\mathbb{Q}(i)$) auf, nämlich dass die Zerlegung im allgemeinen **nicht eindeutig** ist.

Beispiel: $K = \mathbb{Q}(\sqrt{-5})$

Es gilt $O = \mathbb{Z} + \mathbb{Z}\sqrt{-5}$ (Übung!). Zerlege $\alpha = 21$ wie folgt: $\alpha = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5})$. Behauptung: Alle Faktoren sind irreduzibel in O! Damit haben wir einen Widerspruch zur Eindeutigkeit.

Ausweg: Kummer/Dedekind:

Satt ganzen Zahlen α betrachte davon erzeugte Ideale $O \cdot \alpha =: (\alpha)$ und generell alle Ideale $\mathfrak{a} \overset{\triangle}{-} G$. Verallgemeinere die Teilbarkeitsrelation auf Ideale wie folgt:

Definition:

$\mathfrak{a}|b$ ($\mathfrak{a}$ teilt b) genau dann, wenn $b \subseteq \mathfrak{a}$. Übung: Für α, $\beta \in G \setminus \{0\}$ gilt $\alpha|\beta$ in O genau dann, wenn $(\alpha)|(\beta)$.

Theorem 3.2:

Der Ring ist noethersch, ganz abgeschlossen und j als Primideal $p \neq 0$ ist maximales Ideal. (Ringe mit diesen Eigenschaften heißen „DEDEKIND-Ringe“.

Beweis:

- 1.Aussage:

  O ist noethersch (das heißt, jedes Ideal ist endlich erzeugter O-Modul), denn nach Satz 2.5 ist O freier $\mathbb{Z}$-Modul. (es existiert eine Ganzheitsbasis). Nach Elementarteilersatz ist jeder Teilmodul $\mathfrak{a} \subseteq O$ freier $\mathbb{Z}$-Modul vom Rang $\leq \operatorname{rang}(O) = (K : \mathbb{Q})$ (Dimension des Grundkörpers). Insbesondere ist jedes Ideal $\mathfrak{a}$ endlich erzeugt als $\mathbb{Z}$-Modul, also auch endlich erzeugt als O-Modul.

- 2.Aussage:

  O ist ganz abgeschlossen (als ganzer Abschluss von $\mathbb{Z}$ in K).

- 3.Aussage:

  Nun müssen wir noch einsehen, dass aus $p \neq 0$ prim folgt, dass p maximal ist. Im ersten Schritt benötigen wir, dass $\mathfrak{p} \cap \mathbb{Z}$ Primzahl ($p \neq 0$) in $\mathbb{Z}$ (insbesondere p Primzahl) ist. Dies müssen wir zunächst noch einsehen. Für a, $b \in \mathbb{Z}$ gilt $a \cdot b \in \mathfrak{p} \cap \mathbb{Z}$. Hieraus folgt, wenn $\mathfrak{p}$ prim ist, dass $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$. Also ist $\mathfrak{p} \cap \mathbb{Z}$ Primideal ist. Für $\mathfrak{p} \neq 0$ existiert ein $y \neq 0$ in $\mathfrak{p}$. Hieraus folgt für ein Minimalpolynom von y:

  $$\underbrace{y^n + a_1 y^{n-1} + \ldots}_{\in \mathfrak{p}} + a_n = 0 \text{ mit } a_\nu \in \mathbb{Z} \text{ und } a_n \neq 0$$

  Dies bedeutet, dass auch a_n in $\mathfrak{p}$ ist, da man a_n durch $y^n + a_1 y^{n-1} + \ldots$ darstellen kann. Hieraus folgt $\mathfrak{p} \cap \mathbb{Z} \neq (0)$. Jedes Primideal $\neq 0$ in $\mathbb{Z}$ ist von der Form (p) mit Primzahl p. Im zweiten Schritt zeigen wir, dass $\overline{O} := O/\mathfrak{p}$ ein Körper ist. ($\Leftrightarrow$ p maximal) Wir wissen, dass $\overline{O}$ integer ist. Es gibt eine kanonische Abbildung $\mathbb{Z} \mapsto \overline{O}$, $a \mapsto a + p$. Diese Abbildung hat den Kern $\mathbb{Z} \cap \mathfrak{p} = (p)$. Hieraus folgt $\mathbb{F}_p = \mathbb{Z}/(p)$ $\Leftrightarrow$ $\overline{O}$. $\overline{O} = \mathbb{F}_p[\overline{\alpha}; \alpha \in O]$ mit $\overline{\alpha} = \alpha + p$ ist algebraisch in $\mathbb{F}_p$. Nun wissen wir aus Algebra I, dass $\mathbb{F}_p[\overline{\alpha}] = \mathbb{F}_p(\overline{\alpha}) \subseteq \mathbb{F}_p[\overline{\alpha}; \alpha \in O]$. Damit ist $\overline{O}$ ein Körper.

Abstrahiere zunächst und betrachte einen beliebigen DEDEKIND-Ring $\mathcal{O}$ mit Quotientenkörper K. Für Ideale $\mathfrak{a}$, $\mathfrak{b}$ in diesem Ring definieren wir eine Teilbarkeitsrelation $\mathfrak{a}|\mathfrak{b}$ (teilt) genau dann, wenn $b \subseteq a$. Wir definieren neue Ideale als Summen und Produkte, nämlich

$\mathfrak{a} + \mathfrak{b} := \{a + b; a \in \mathfrak{a}, b \in \mathfrak{b}\}$

und

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_i a_i \cdot b_i \text{ mit } a_i \in \mathfrak{a} \text{ und } b_i \in \mathfrak{b} \right\}$$

$\sum_i$ sei eine endliche Summe. Es gilt offenbar, dass $\mathfrak{a} + \mathfrak{b}$ kleinstes umfassendes Ideal von $\mathfrak{a}$ und $\mathfrak{b}$ ist. Dies definieren wir als ggt($\mathfrak{a}$,$\mathfrak{b}$). Der ggT ist also ein Erzeuger dieses Ideals. (Das heißt, $\mathfrak{a} + \mathfrak{b} | \mathfrak{a}$ und $\mathfrak{a} + \mathfrak{b} | \mathfrak{b}$ und für jeden gemweinsamen Teiler $\mathfrak{t} | \mathfrak{a}$ und $\mathfrak{t} | \mathfrak{b}$ gilt $\mathfrak{t} | \mathfrak{a} + \mathfrak{b}$. Analog entspricht $\mathfrak{a} \cap \mathfrak{b}$ dem kgV($\mathfrak{a}$,$\mathfrak{b}$).

Theorem 3.3:

Jedes Ideal $\mathfrak{a} \neq (0)$, $\mathcal{O}$ besitzt eine bis auf die Reigenfolge eindeutige Zerlegung in ein Produkt von Primidealen $\mathfrak{p}_i$ von $\mathcal{O}$, nämlich $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$. (Dies nennt man die „**eindeutige Primzerlegung**“ der Ideale eines DEDEKIND-Rings.)

Lemma 3.4:

Zu jedem Ideal $\mathfrak{a} \neq (0)$ in $\mathcal{O}$ existieren Primideale $\mathfrak{p}_1$, …, $\mathfrak{p}_r$ (alle $\neq (0)$) mit $\mathfrak{p}_1 \cdot \ldots \mathfrak{p}_r \subseteq \mathfrak{a}$.

Beweis:

Wir betrachten $\mathfrak{m} := \{\mathfrak{a} \neq (0), \text{obige Aussage falsch}\} \neq \varnothing$. Da $\mathfrak{m}$ noethersch ist, besitzt $\mathfrak{m}$ ein maximales Element $\mathfrak{a}$. Ferner gilt, dass $\mathfrak{a}$ nicht Primideal ist, da für alle Primideale $\mathfrak{p} \neq 0$ gilt, dass $\mathfrak{p} \notin \mathfrak{m}$. Das heißt, es gibt $a_i \in \mathcal{O}$, so dass $a_1 \cdot a_2 \in \mathfrak{a}$ und $a_1, a_2 \notin \mathfrak{a}$. Setze $\mathfrak{a}_i := (a_i) + \mathfrak{a} \not\supseteq A$. Es ist also $\mathfrak{a} \subsetneq \mathfrak{a}_i$, $\mathfrak{a}_1 \cdot \mathfrak{a}_2 \subseteq \mathfrak{m}$. Wegen der Maximalität von $\mathfrak{a}$ in $\mathfrak{m}$ ist $\mathfrak{a}_i \notin \mathfrak{m}$. Damit existieren Primideale $\neq (0)$: $\mathfrak{p}_1$, …, $\mathfrak{p}_r$, $\mathfrak{q}_1$, …, $\mathfrak{q}_s$ mit $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq \mathfrak{a}_1$, $\mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \subseteq \mathfrak{a}_2$. Daraus folgt, dass $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \cdot \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s \subseteq \mathfrak{a}_1 \cdot \mathfrak{a}_2 \subseteq \mathfrak{a}$. Dies ist ein Widerspruch zur Annahme.
Für ein Primideal $\mathfrak{p}$ von $\mathcal{O}$ sei $\mathfrak{p}^{-1} := \{x \in K, x \cdot \mathfrak{p} \subseteq \mathcal{O}\}$ ($\subseteq$ lins $\mathcal{O}$). Für ein Ideal $\mathfrak{a}$ sei:

$$\mathfrak{a} \cdot \mathfrak{p}^{-1} := \left\{ \sum_i a_i \cdot x_i, a_i \in \mathfrak{a}, x_i \in \mathfrak{p}^{-1} \right\}$$

Lemma 3.5:

Für jedes Ideal $\mathfrak{a} \neq (0)$ und jedes Primideal $\mathfrak{p}$ gilt $\mathfrak{a} \cdot \mathfrak{p}^{-1} \overset{(\subset l)}{\neq} \mathfrak{a}$.

Beweis:

Zeige erst, dass $\mathfrak{p}^{-1} \neq \mathcal{O}$. Klar ist dies für $p = (0)$, denn dann ist $\mathfrak{p}^{-1} = K$. Sei $x \neq 0$ und $x \in \mathfrak{p}$. Nach Lemma 3.4 existiert $\mathfrak{p}_i \neq (0)$ mit $\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r \subseteq (x) \subseteq \mathfrak{p}$. Ohne Einschränkung sei r minimal. Hieraus folgt, dass es ein i gibt mit $\mathfrak{p}_i \subseteq \mathfrak{p}$. (Wegen Maximalität des Primideals gilt sogar Gleichheit: $\mathfrak{p}_i = \mathfrak{p}$.) (Ohne Einschränkung nehmen wir $i = 1$ an, denn andernfalls gibt es $\forall i$ ein $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}$ und somit $x_1 \cdot \ldots \cdot x_r \in (x) \subseteq \mathfrak{p}$. Aus $\mathfrak{p}$ prim folgt, dass ein $x_i \in \mathfrak{p}$. Dies ist ein Widerspruch.
Ferner gilt $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \not\subseteq (x)$ (wegen Minimalität von r). Sei etwa $y \in \mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r \setminus \mathcal{O} \cdot x$. Hieraus folgt $x^{-1}y \notin \mathcal{O}$. Wegen $y \cdot \mathfrak{p} \subseteq \mathfrak{p}_1 \ldots \mathfrak{p}_r \subseteq (x)$ folgt durch Multiplikation mit x^{-1}, dass $x^{-1}y \cdot \mathfrak{p} \subseteq \mathcal{O}$. Dies ist äquivalent zu $x^{-1}y \in \mathfrak{p}^{-1}$ und daraus folgt $\mathfrak{p}^{-1} \neq \mathcal{O}$.
Nun sei $\mathfrak{a} \neq (0)$ mit $\mathfrak{a} = \mathcal{O}\alpha_1 + \ldots + \mathcal{O}a_n$. Angenommen, es gilt $\mathfrak{a} \cdot \mathfrak{p}^{-1} = \mathfrak{a}\ \forall\ x \in \mathfrak{p}^{-1}$. Damit können wir dies $\forall\ i$ schreiben als:

$$x \cdot \alpha_i = \sum_j a_{ij} \cdot \alpha_j \text{ mit } a_{ij} \in \mathcal{O}$$

Wir betrachten die Matrix $A := (x\delta_{ij} - a_{ij}) \in K^{n \times n}$. Es gilt nun:

$$A \cdot \begin{pmatrix} \alpha_1 \\ \ldots \\ \alpha_n \end{pmatrix} = 0$$

Indem wir mit $A^{\#}$ multiplizerien, finden wir für $d := \det(A)$: $d \cdot \alpha_1 = \ldots = d \cdot \alpha_n = 0$. Hieraus folgt $d = 0$. Hieraus folgt, dass x Nullstelle des charakteristischen Polynoms $f(X) := \det(X \cdot \delta_{ij} - a_{ij}) \in \mathcal{O}[X]$. Hieraus ergibt sich, dass x ganz ist in $\mathcal{O}$. Da $\mathcal{O}$ ganz abgeschlossen im Quotientenkörper ist (DEDEKIND-Eigenschaft) folgt, dass $x \in \mathcal{O}$. Damit ergibt sich $\mathfrak{p}^{-1} \subseteq \mathcal{O} (\subseteq \mathfrak{p}^{-1})$. Dies ist ein Widerspruch!

Beweis von Theorem 3.3:

A.) Existenz der Primzerlegung:

Sei $\mathfrak{m} := \{\mathfrak{a} \not\subseteq \mathcal{O}, \mathfrak{a} \neq (0) \text{ ohne Primzerlegung}\}$. Falls $\mathfrak{m} \neq \varnothing$, so folgt daraus, dass $\mathcal{O}$ noethersch ist, dass maximale Elemente $\mathfrak{a} \in \mathfrak{m}$ existieren. So findet man sicher ein maixmales Ideal $\mathfrak{p} \supseteq \mathfrak{a}$ (mittels aufsteigender Kette). Es gilt $\mathfrak{a} \subsetneqq \mathfrak{a} \cdot \mathfrak{p}^{-1} \subseteq \mathfrak{p}\mathfrak{p}^{-1} \subseteq \mathcal{O}$ (Lemma 3.5) und $\mathfrak{p} \subsetneqq \mathfrak{p}\mathfrak{p}^{-1}$ ($\subseteq \mathcal{O}$). Hieraus folgt $\mathfrak{p}\mathfrak{p}^{-1} = \mathcal{O}$. Wegen $\mathfrak{a} \in \mathfrak{m}$ ist $\mathfrak{a} \not\subseteq \subsetneqq \mathfrak{p}$. Multiplizieren wir mit $\mathfrak{p}^{-1}$, so folgt $\mathfrak{a}\mathfrak{p}^{-1} \subsetneqq \mathcal{O}$. $\mathfrak{a}$ ist maximal in $\mathfrak{m}$ und hieraus folgt, dass $\mathfrak{a}\mathfrak{p}^{-1} \notin \mathfrak{m}$. Das heißt, es existiert ein $\mathfrak{p}_i$ mit $\mathfrak{a}\mathfrak{p}^{-1} = \mathfrak{p}_1 \dots \mathfrak{p}_r$. Multiplizieren wir dies mit $\mathfrak{p}$, so folgt $\mathfrak{a} = \mathfrak{p}\mathfrak{p}_1 \dots \mathfrak{p}_r$, was ein Widerspruch darstellt.

B.) Eindeutigkeit:

Vorbemerkung: Für $\mathfrak{p}$ gilt, dass aus $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{p}$ $\mathfrak{a} \subseteq \mathfrak{p}$ oder $\mathfrak{b} \subseteq \mathfrak{p}$ folgt. Das heißt, aus $\mathfrak{p}|\mathfrak{a}\mathfrak{b}$ folgt, dass $\mathfrak{p}|\mathfrak{a}$ oder $\mathfrak{p}|\mathfrak{b}$. Denn sonst existieren $a \in \mathfrak{a} \setminus \mathfrak{p}$, $b \in \mathfrak{b} \setminus \mathfrak{p}$ oder $a \cdot b \in \mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{p}$. Hieraus folgt $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$, was ein Widerspruch darstellt.

Seien zwei Primzerlegungen gegeben, nämlich $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_1 \cdot \ldots \cdot \mathfrak{q}_s$. Aus $\mathfrak{p}_1|\mathfrak{a}$ folgt, dass es $\mathfrak{q}(= \mathfrak{q}_1$ ohne Einschränkung) existiert, so dass $\mathfrak{p}_1|\mathfrak{q}_1$. Hieraus ergibt sich $\mathfrak{p}_1 = \mathfrak{q}_1$ (wegen der Maximalität von $\mathfrak{q}_1$). Multiplizieren wir nun beide Seiten mit $\mathfrak{p}_1^{-1}$, so ergibt sich $\mathfrak{p}_2 \cdot \ldots \cdot \mathfrak{p}_r = \mathfrak{q}_2 \cdot \ldots \cdot \mathfrak{q}_s$. Hieraus ergibt sich schlussendlich $r = s$, $\mathfrak{p}_i = \mathfrak{q}_i \ \forall\ i$ nach eventuellem Umnummerieren. □

Konvention:

Schreibe die Primzerlegung der Ideale $\mathfrak{a} \neq (0)$ in der Form

$$\mathfrak{a} = \mathfrak{p}_1^{\nu_1} \cdot \ldots \cdot \mathfrak{p}_r^{\nu_r} = \prod_{\varrho=1}^{r} \mathfrak{p}_\varrho^{\nu_\varrho} \text{ mit } \nu_\varrho \in \mathbb{Z}_{>0}$$

Die $\mathfrak{p}_1$, …, $\mathfrak{p}_r$ seien alle voneinander verschieden. **Beachte**: Hierbei sind die Ideale $\mathfrak{a}_\varrho := \mathfrak{p}_\varrho^{\nu_\varrho}$ paarweise teilerfremd, also $\mathrm{ggT}(\mathfrak{a}_i\mathfrak{a}_j) = \mathfrak{a}_i + \mathfrak{a}_j = \mathcal{O}$ (mit $i \neq j$). Generell gilt für paarweise teilerfremde Ideale $\mathfrak{a}_\varrho$ ($\varrho = 1$, …, r):

$$\prod_{\varrho=1}^{r} \mathfrak{a}_\varrho = \bigcap_{\varrho=1}^{r} \mathfrak{a}_\varrho$$

(Der Beweis wird in der Übung durchgeführt.)

1.1.1 Chinesischer Restsatz

$$R/\prod_{\varrho} \mathfrak{a}_\varrho \simeq \bigoplus R/\mathfrak{a}_i$$

Wunschziel:

Wir wollen eine Gruppenstruktur auf der Menge der Ideale eines Dedekind-Rings G finden. Es fehlen noch die „Inverse“.

Definition 3.7:

Ein endlich erzeugter $\mathcal{O}$-Teilmodul $\mathfrak{a} \subseteq K(= \mathrm{Quot}(\mathcal{O}))$ mit $\mathfrak{a} \neq (0)$ heißt „**gebrochenes**“ Ideal.

Bemerkung:

1.) Für $a \in K^\times$ ist $(a) := \mathcal{O} \cdot a$ ein gebrochenes Ideal.

2.) Die gebrochenen Ideale $\mathfrak{a} \subseteq \mathcal{O}$ sind genau die Ideale von $\mathcal{O}$ und heißen auch **ganze** Ideale.

3.) Ein beliebiger $\mathcal{O}$-Teilmodul $\mathfrak{a} \subseteq K$ ist genau dann gebrochenes Ideal, falls ein $c \in \mathcal{O}$ mit $c \neq 0$ existiert mit $c \cdot \mathfrak{a} \subseteq \mathcal{O}$ (das heißt $\mathfrak{a} \subseteq 1/c\mathcal{O}$).

Satz 3.8:

Die Menge der gebrochenen Ideale bildet eine abelsche Gruppe bezüglich der Verknüpfung

$$\mathfrak{a} \cdot \mathfrak{b} := \left\{ \sum_i a_i b_i; a_i \in \mathfrak{a}, b_i \in \mathfrak{b} \right\}$$

Dies ist die sogenannte „**Idealgruppe**“ $\mathcal{J}_K$ von K. Das Einselement ist $\mathcal{O} = (1)$ und das Inverse zu $\mathfrak{a}$ ist:

$$\mathfrak{a}^{-1} := \{x \in K; x \cdot \mathfrak{a} \subseteq \mathcal{O}\}$$

Beweis:

Wir wissen bereits Assoziativität, Kommutativität und kennen das Einselement. Es bleibt nun noch das Inverse zu bestimmen! Behandle schrittweise allgemeinere $\mathfrak{a}$!

- ✳ Fall $\mathfrak{a} = \mathfrak{p}$ (prim): Wir haben gesehen, dass $\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathcal{O}$.
- ✳ Fall $\mathfrak{a}$ ganzes Ideal: Wir können $\mathfrak{a} = \mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r$ schreiben. Hier wirkt $\mathfrak{b} := \mathfrak{p}_1^{-1} \cdot \ldots \cdot \mathfrak{p}_r^{-1}$ als Inverse.

  Behauptung: $\mathfrak{b} = \mathfrak{a}^{-1}$ wie im Satz definiert. Da $\mathfrak{b} \cdot \mathfrak{a} = \mathcal{O}$ folgt, dass $\mathfrak{b} \subseteq \mathfrak{a}^{-1}$. Ist $x \in \mathfrak{a}^{-1}$, also $x \cdot \mathfrak{a} \subseteq \mathcal{O}$. Multiplizieren wir dies mit $\mathfrak{b}$, so ergibt sich $x \cdot \mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{b}$. Mit $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathcal{O}$, folgt $\mathfrak{a}^{-1} \subseteq \mathfrak{b}$. Hieraus ergibt sich die Gleichheit.
- ✳ Fall $\mathfrak{a}$ gebrochen: Es existiert ein $c \in \mathcal{O} \setminus \{0\}$, so dass $c \cdot \mathfrak{a}$ ein **ganzes** Ideal. Hieraus folgt, dass $(c \cdot \mathfrak{a})^{-1} = \{x \in K, x \cdot c \cdot \mathfrak{a} \subseteq \mathcal{O}\}$ das Inverse von $c \cdot \mathfrak{a}$ ist. Sei nun $y := x \cdot c$ und damit $x = c^{-1}y$, womit sich ergibt:

  $(c \cdot \mathfrak{a})^{-1} = c^{-1} \cdot \{y \in K, y \cdot \mathfrak{a} \subseteq \mathcal{O}\} = c^{-1} \cdot \mathfrak{a}^{-1}$ nach Definition

  Hieraus folgt $\mathcal{O} = c \cdot \mathfrak{a} \cdot c^{-1} \cdot \mathfrak{a} = \mathfrak{a} \cdot \mathfrak{a}^{-1}$. □

Korollar 3.9:

$\mathcal{J}_K$ ist freie abelsche Gruppe über die Menge aller Primideale $\mathfrak{p} \neq (0)$ von $\mathcal{O}$. Das heißt, jedes $\mathfrak{a} \in \mathcal{J}_K$ besitzt eine eindeutige Produktdarstellung

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_\mathfrak{p}} \text{ mit } \nu_\mathfrak{p} \in \mathbb{Z} \text{ und } \nu_\mathfrak{p} = 0 \text{ für fast alle } \mathfrak{p}$$

Beweis:

Zu $\mathfrak{a}$ existiert ein $c \in \mathcal{O} \setminus \{0\}$, so dass $b := c \cdot \mathfrak{a} \subseteq \mathcal{O}$. Hieraus folgt $\mathfrak{a} = \mathfrak{b}/\mathfrak{c} = \mathfrak{b} \cdot \mathfrak{c}^{-1}$ mit den ganzen Idealen $\mathfrak{b}$, $\mathfrak{c}(= (c))$. Nach Theorem 3.3 gibt es eine eindeutige Primzerlegung der $\mathfrak{b}$ und $\mathfrak{c}$, woraus die Behauptung folgt. □

Wir haben eine ausgezeichnete Untergruppe von $\mathcal{J}_K$, $\mathfrak{p}_K := \{(a) = \mathcal{O} \cdot a, a \in K^\times\}$.

Definition:

Die Faktorgruppe $\mathfrak{Cl}_K := \mathcal{J}_K/\mathfrak{p}_K$ heißt die „**Idealklassengruppe**“ von K. Man hat eine natürliche **exakte Sequenz** (von Homomorphismen abelscher Gruppen).

$$1 \mapsto \mathcal{O}^\times \xrightarrow[\text{„}\subseteq\text{“}]{} \mathcal{J}_K \mapsto \mathfrak{Cl}_K \mapsto 1$$

Bedeutung:

Die Sequenz beschreibt den „Informationsverlust“ beim Übergang von Zahlen in $K^\times$ zu Idealen einerseits und die Abweichung eines beliebigen Ideals davon, Hauptideal zu sein. Anmerkung: Für die Gruppen $\mathcal{O}^\times$ und $\mathfrak{Cl}_K$ können beliebige abelsche Gruppen vorkommen, wenn $\mathcal{O}$ alle DEDEKIND-Ringe durchläuft. Aber: Für Zahlkörper K mit $\mathcal{O} = \mathcal{O}_K$ kommen nur bestimmte Gruppen in Frage mit gewissen **Endlichkeitseigenschaften**.

Kapitel 2

Geometrie der Zahlen

2.1 Gitter

Wir erinnern uns an die Zuordnung: {GAUSSsche Zahlen} $\xrightarrow{\sim}$ Gitter $\mathbb{Z}[i] \subseteq \mathbb{R}^2$.

Definition 4.1:

Sei V ein $\mathbb{R}$-Vektorraum mit $\dim(V) = n < \infty$. Ein „**Gitter**“ $\Gamma \subseteq V$ ist eine Untergruppe der Form $\Gamma = \mathbb{Z}v_1 + \ldots + \mathbb{Z}v_m$ mit linear unabhängigen $v_1, \ldots, v_m \in V$. Die Menge $\{v_1, \ldots, v_m\}$ nennt man **Basis** des Gitters und $\Phi := \{\sum_{i=1}^{m} x_i v_i, x_i \in \mathbb{R}, 0 \leq x_i < 1\}$ heißt „**Grundmasche**“ des Gitters. Γ heißt „**vollständig**“ oder eine „***Z*-Struktur**“ auf V, falls $m = n$ ist.

Bemerkung:

Γ heißt vollständig genau dann, wenn $V = \dot{\bigcup}_{\gamma \in \Gamma} \gamma + \Phi$. (Übung!)

Unser Ziel ist die koordinatenfreie Charakterisierung von Gittern. Dazu hilft eine (metrisch-)topologische Eigenschaft.

Definition:

Eine Teilmenge $D \subseteq T$ eines topologischen Raums T heißt **diskret**, falls jeder Punkt $d \in D$ isolierter Punkt von T ist. Das heißt, es existiert eine Umgebung U von d, so dass $U \cap D = \{d\}$.

Satz 4.2:

Für eine Untergruppe $\Gamma \subseteq V$ gilt: Γ ist genau dann ein Gitter, wenn Γ diskret ist (bezüglich der Topologie des $\mathbb{R}^n \simeq V$.)

Beweis „$\Leftarrow$“:

Sei $\Gamma \subseteq V$ diskret. Betrachte einen $\mathbb{R}$-Vektorraum, wobei V_0 das Erzeugnis von Γ ist. Sei außerdem $m := \dim(V)$. Wähle in Γ ein minimales Erzeugendensystem (=Basis) von V_0, nämlich $u_1, \ldots, u_m \in \Gamma$. Mit dieser Basis spannen wir nun ein Gitter auf: $\Gamma_0 := \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_m$. Dies ist ein vollständiges Gitter in V_0, das die Zahl der Erzeugenden gleich der Dimension ist. Die Behauptung ist $(\Gamma : \Gamma_0) < \infty$. Schreibe die Nebenklassenzerlegung auf:

$$\Gamma = \dot{\bigcup_i} \gamma_i + \Gamma_0$$

Die γ_i laufen durch ein Vertretersystem von allen Klassen. V_0 lässt sich immer schreiben als Vereinigung der Translate dieser Mengen, wobei Φ_0 die Grundmasche von V_0 bezüglich Γ_0 sei:

$$V_0 = \bigcup_{\gamma \in \Gamma_0} \gamma_i + \Phi_0 \supseteq \Gamma$$

Für alle γ_i existiert dann ein $\gamma_{i0} \in \Gamma_0$ und $\mu_i \in \Phi_0$, so dass $\gamma_i = \gamma_{i0} + \mu_i$. Insbesondere gilt $\mu_i = \gamma_i - \gamma_{i0} \in \Gamma \cap \Phi_0$. Γ ist eine diskrete Menge und Φ_0 ist beschränkt. Hieraus folgt, dass die Menge endlich ist. Aus $\gamma_i + \Gamma_0 = \mu_i + \Gamma_0$ folgt die Behauptung der Endlichkeit des Index. Für $q := (\Gamma : \Gamma_0)$ gilt $q\Gamma \subseteq \Gamma_0$, also:

$$\Gamma \subseteq \frac{1}{q}\Gamma_0 = \mathbb{Z}\frac{1}{q}u_1 + \ldots + \mathbb{Z}\frac{1}{q}u_m$$

Nach dem Elementarteilersatz besitzt auch Γ eine $\mathbb{Z}$-Basis $v_1, \ldots, v_r$ ($r \leq m$) Das Erzeugnis ist $\langle v_1, \ldots, v_r \rangle_{\mathbb{R}} = V_0$. Hieraus folgt $r = m$ und dass die $v_1, \ldots, v_r$ linear unabhängig sind, das heißt, Γ ist ein Gitter. □

Lemma 4.3:

$\Gamma \leq V$ sei ein Gitter. Es gilt: Γ ist vollständig $\Leftrightarrow$ Es gibt eine beschränkte Menge $M \subseteq V$, so dass $V = \bigcup_{\gamma \in \Gamma} \gamma + M$ $(*)$.

Beweis „⇒“:

Γ ist vollständig. Wähle

$$M := \text{Grundmasche } \Phi = \left\{ \sum_{i=1}^{n} x_i v_i; 0 \leq x_i \leq 1 \right\}$$

Beweis „⇐“:

Sei $M \subseteq V$ beschränkt. V_0 definiert das $\mathbb{R}$-Erzeugnis von Γ. Zeige: $V_0 = V$. Sei $v \in V$ beliebig. Wegen $(*)$ gilt $\forall\, r \in \mathbb{N}$: Es existieren $a_r \in M$, $\gamma_r \in \Gamma$, so dass $r \cdot v = a_1 + \gamma_r$. M beschränkt impliziert, dass $1/r a_r$ Nullfolge ist. Hieraus ergibt sich:

$$v = \frac{1}{r}a_r + \frac{1}{r}\gamma_r \mapsto 0 + v = v$$

Daraus resultiert $v \in V_0$, da V_0 abgeschlossen ist. □

Sei im folgenden V ein **euklidischer** Vektorraum. Das heißt es gilt $\dim V = n < \infty$ und es existiert ein Skalarprodukt $\langle , \rangle$: $V \times V \mapsto \mathbb{R}$ (symmetrische, positiv definite Bilinearform). Dann können wir immer eine Orthonormalbasis $e_1, \ldots, e_n$ finden. Integralrechnung im $\mathbb{R}^m$: Wir haben ein „Volumen“ (oder „Inhalt“), das normiert wird durch $\text{Vol}(\Phi(e_1, \ldots, e_n)) = 1$. Φ sei ein verallgemeinerter Würfel, der Grundmasche des Gitters ist, das aus $e_1, \ldots, e_n$ erzeugt wird. Aus der Analysis wissen wir, dass beliebige linear unabhängige Vektoren $v_1, \ldots, v_n$ ein Gitter mit zugehöriger Grundmasche Φ aufspannen. Das Volumen ist dann gegeben durch:

$$\text{Vol}(\Phi) = |\det(A)| \text{ für } A = (a_{ij}) \text{ mit } v_i = \sum_k a_{ik} e_k$$

Ferner gilt $\text{Vol}(\Phi) = |\det(\langle v_i, v_j \rangle)|^{\frac{1}{2}}$. Denn:

$$\langle v_i, v_j \rangle = \sum_{k,l} a_{ik} \cdot a_{jl} \langle e_k, e_l \rangle = \sum_{k,l} a_{ik} \cdot a_{jl} \delta_{kl} = \sum_k a_{ik} \cdot a_{jk} \Rightarrow (\langle v_i, v_j \rangle) = A \cdot A^{\intercal}$$

Das Volumen der Grundmasche hängt also nur vom Gitter selbst und nicht von der $\mathbb{Z}$-Basis des Gitters $\Gamma := \mathbb{Z}u_1 + \ldots + \mathbb{Z}u_n$. Wir schreiben daher $\text{Vol}(\Gamma) := \text{Vol}(\Phi)$. Unser Nahziel ist das Auffinden von Gitterpunkten in Teilmengen von V.

Definition:

Sei $X \subseteq V$ eine Teilmenge. X heißt

a.) **zentralsymmetrisch**, wenn gilt $x \in X \Rightarrow -x \in X$. (Punktspiegelung am Ursprung)

b.) **konvex**, wenn aus x, $y \in X$ folgt, dass $\{ty + (1-t)x; 0 \leq t \leq 1\} \subseteq X$.

2.1.1 Gitterpunktsatz

Satz 4.4 (nach Minkowski):

Sei Γ ein vollständiges Gitter in einem euklidischen Raum V. Sei weiterhin $X \subseteq V$ messbar, konvex und zentralsymmetrisch. Mit $\text{Vol}(X) > 2^n \cdot \text{Vol}(\Gamma)$ existiert ein $\gamma \neq 0$ in $\Gamma \cap X$.

Beweis:

- 1.Schritt: Reduktion auf Behauptung

  Existiert $\gamma_i \in \Gamma$: $\gamma_1 \neq \gamma_2$ mit $(\gamma_1 + 1/2X) \cap (\gamma_2 + 1/2X) \neq \varnothing$. Falls dies gilt, wähle (im Durchschnitt)

  $$\frac{1}{2}x_1 + \gamma_1 = \frac{1}{2}x_2 + \gamma_2 \text{ mit } x_i \in X \text{ (auch } -x_i \in X)$$

  Hieraus folgt:

  $$\gamma := \gamma_1 - \gamma_2 = \frac{1}{2}x_2 - \frac{1}{2}x_1 \in X \cap \Gamma \text{ (da } X \text{ konvex)}$$

- 2.Schritt: Beweis der Behauptung

  Angenommen, alle $\gamma + 1/2X$ ($\gamma \in \Gamma$) sind paarweise disjunkt. Insbesondere sind alle $\Phi \cap (\gamma + 1/2X)$ paarweise disjunkt, wobei Φ die Grundmasche von Γ ist. Damit ergibt sich:

  $$\mathrm{Vol}(\Phi) \geq \sum_{\gamma \in \Gamma} \mathrm{Vol}\left(\Phi \cap \left(\gamma + \frac{1}{2}x\right)\right)$$

  Die Translationsinvarianz des Volumens hat zur Folge, dass $\mathrm{Vol}((\Phi - \gamma) \cap 1/2X) = \mathrm{Vol}(\Phi \cap (\gamma + 1/2X))$. Setzen wir dies oben ein, so folgt:

  $$\sum_{\gamma \in \Gamma} \mathrm{Vol}\left((\Phi - \gamma) \cap \frac{1}{2}X\right) = \mathrm{Vol}\left(\frac{1}{2}X\right) = 2^{-n} \cdot \mathrm{Vol}(X) \text{ da } V = \bigdot\bigcup_{\gamma} \Phi + \gamma$$

  Dies ist ein Widerspruch zur Annahme, dass alle $\gamma + 1/2X$ paarweise disjunkt sind. □

2.2 Minkowski-Theorie

Grundidee: Zahlkörper $K/\mathbb{Q}$ vom Grad n. Studium der natürlichen Einbettung $K \hookrightarrow \mathbb{R}^n$ und geometrische Eigenschaften der so als Punkte interpretieren algebraischen Zahlen. Sei zunächst

$$j : K \mapsto \prod_{\tau:\, K \hookrightarrow \mathbb{C}} \mathbb{C} =: K_{\mathbb{C}},\ \alpha \mapsto (\ldots, \tau(\alpha), \ldots)_{\text{alle } \tau}$$

Es existieren genau n Einbettungen. Erinnere: $K_{\mathbb{C}}$ hat Standard-Skalarprodukt mit der zugehörigen Metrik:

$$\langle x, y \rangle := \sum_{\tau=1}^{n} x_\tau \cdot \overline{y}_\tau \text{ mit } x = (x_\tau)$$

Erinnere: Die Galoisgruppe $G(\mathbb{C}/\mathbb{R}) = \langle F \rangle$, F: $\mathbb{C} \mapsto \mathbb{C}$, $Z \mapsto \overline{z}$. F operiert auf $\{\tau : K \hookrightarrow \mathbb{C}\}$: $\overline{\tau} := F \circ \tau$. F definiert außerdem eine Involution ($F \circ F = \mathrm{id}$) von $K_{\mathbb{C}}$ folgendermaßen:

$$F :\ K_{\mathbb{C}} \mapsto K_{\mathbb{C}},\ z = (z_\tau) \mapsto Fz \text{ mit } (Fz)_\tau := \overline{z}_{\overline{\tau}}$$

Es gilt die Invarianzeigenschaft für $x, y \in j(K)$, nämlich $\langle Fx, Fy \rangle = \langle x, y \rangle$ und ebenso für „Spur“ Tr: $K_{\mathbb{C}} \mapsto \mathbb{C}$, $x \mapsto \sum_\tau x_\tau$ ist $\mathrm{Tr}(Fx)\mathrm{Tr}(x)$.

Definition:

Der $\mathbb{R}$-Vektorraum der F-invarianten Punkte von $K_{\mathbb{C}}$ ist der $K_{\mathbb{R}} := K_{\mathbb{C}}^{+} := (+1)$-Eigenraum des Automorphismus F. Dieser Raum zusammen mit dem durch Einschränken von $\langle , \rangle$ definierten (reellem!) Skalarprodukt $\langle , \rangle$: $K_{\mathbb{R}} \times K_{\mathbb{R}} \mapsto \mathbb{R}$ heißt der „Minkowski-Raum“.

2.2.1 Explizite Beschreibung von $K_{\mathbb{R}}$

Seien $\{\varrho_1, \ldots, \varrho_n\} := \{\tau : K \hookrightarrow \mathbb{C}; \tau(K) \subseteq \mathbb{R}\}$ die Menge der **reellen Einbettungen**. Die nicht-reellen oder „**komplexen**“ Einbettungen kommen stets als Paare von τ und $\overline{\tau}(\neq \tau)$ vor. Diese seien $\sigma_1, \ldots, \sigma_s$ und $\overline{\sigma}_1, \ldots, \overline{\sigma}_s$. Insgesamt hat man also $r + 2s = n$ Einbettungen.

Satz 5.1:

Die Zuordnung f: $K_{\mathbb{R}} \mapsto \prod_\tau \mathbb{R} = \mathbb{R}^{r+2s}$, $(z_\tau) \mapsto (x_\tau)$ mit $x_\varrho := z_\varrho$ für alle reellen ϱ, $x_\sigma := \mathrm{Re}(z_\sigma)$, $x_{\overline{\sigma}} := \mathrm{Im}(z_{\overline{\sigma}})$ für komplexe σ ist ein Isomorphismus metrischer Räume, der das Skalarprodukt $\langle , \rangle$ überführt in das Skalarprodukt $(x, y) := \sum_\tau \alpha_\tau \cdot x_\tau y_\tau$ mit $\alpha_\varrho = 1$ für reelle ϱ und $\alpha_\sigma = 2$ für komplexe σ.

Bemerkung:

Beachte dabei: Für eine messbare Menge $X \in K_{\mathbb{R}}$ gilt $\mathrm{Vol}(X) = 2^s \cdot \mathrm{Vol}(f(X))$ bezüglich des Standardmaßes auf $\mathbb{R}^n$.

Beweis:

Die explizite Beschreibung von $K_{\mathbb{R}}$ zeigt uns, dass dies ein Isomorphismus ist. Sei nun $z = (z_\tau) = (a_\tau + \mathrm{i}b_\tau)$ und $z' = (z'_\tau) = (a'_\tau + \mathrm{i}b'_\tau) \in K_{\mathbb{R}}$. Damit gilt für das Skalarprodukt:

$$\langle z, z' \rangle = \sum_{\varrho \text{ reell}} x_\varrho x'_\varrho + \sum_{\sigma \text{ komplex}} z_\sigma \overline{z}'_\sigma$$

Mit $b_{\overline{\sigma}} = -b_\sigma$ erhalten wir weiter:

$z_\sigma \overline{z}'_\sigma + z_{\overline{\sigma}} \overline{z_{\overline{\sigma}}}' = z_\sigma \cdot \overline{z_\sigma}' + \overline{z_\sigma} \cdot z'_\sigma = 2\mathrm{Re}(z_\sigma \overline{z_\sigma}') = (a_\sigma a'_\sigma + b_\sigma b'_\sigma) \cdot 2 = 2 \cdot (x_\sigma x'_\sigma + x_{\overline{\sigma}} x'_{\overline{\sigma}})$

Hieraus folgt schließlich $\langle z, z' \rangle = (f(z), f(z'))$. □

Satz 5.2:

Für jedes Ideal $\mathfrak{a} \neq (0)$ von $\mathcal{O}$ bildet $j(\mathfrak{a}) =: \Gamma$ ein vollständiges Gitter in $K_{\mathbb{R}}$ mit Grundmaschenvolumen $\mathrm{Vol}(\Gamma) = \sqrt{|d_k|} \cdot (\mathcal{O} : \mathfrak{a})$.

Beweis:

Sei $\mathfrak{a} = \mathbb{Z} \cdot \alpha_1 + \ldots + \mathbb{Z} \cdot \alpha_n$ eine $\mathbb{Z}$-Basis. Also ist $\Gamma = \mathbb{Z}j(\alpha_1) + \ldots + \mathbb{Z}j(\alpha_n)$, welches eine Basis unseres Gitters ist. Sei $\{\tau : K \hookrightarrow \mathbb{C}\} = \{\tau_1, \ldots, \tau_n\}$ und $\tau_\lambda(\alpha_\mu) =: a_{\lambda\mu}$. Dies sind Einträge der Matrix $A = (a_{\lambda\mu}) \in \mathbb{C}^{n \times n}$. Weiterhin wissen wir, dass $\det(A)^2 = |d(\alpha_1, \ldots, \alpha_n)| = d(\mathfrak{a}) = (\mathcal{O} : \mathfrak{a})^2 \cdot d_k$ ist. Hieraus ergibt sich das Volumen der Grundmasche:

$$\mathrm{Vol}(\Gamma) = |\det(\langle j(\alpha_\nu), j(\alpha_\mu) \rangle)|^{\frac{1}{2}} = \left| \left(\sum_{\lambda=1}^{n} \tau_\lambda(\alpha_\nu) \overline{\tau}_\lambda(\alpha_\mu) \right) \right|^{\frac{1}{2}} = |A \cdot \overline{A}^{\mathsf{T}}|^{\frac{1}{2}} = |\det(A) \cdot \det(\overline{A})|^{\frac{1}{2}} = |\det(A)| \qquad \square$$

Theorem 5.3:

Für $\mathfrak{a} \triangleq \mathcal{O}$, $\mathfrak{a} \neq (0)$ sei $(c_\tau) \in \mathbb{R}^{r+2s}$ gegeben mit

1.) $c_\tau > 0$

2.) $c_{\overline{\tau}} = c_\tau$

3.) $\prod_\tau c_\tau > A \cdot (\mathcal{O} : \mathfrak{a})$ mit $A := \sqrt{|d_k|} \cdot \left(\frac{2}{\pi} \right)^s$

Dann existiert ein $a \in \mathfrak{a}$, $a \neq 0$ mit $|\tau(a)| < c_\tau$ für alle τ: $K \hookrightarrow \mathbb{C}$.

Beweis:

Wende Minkowskis Gitterpunktsatz an. Betrachte $X := \{(z_\tau) \in K_{\mathbb{R}}; |z_\tau| < c_\tau\}$, welches zentralsymmetrisch und konvex ist. Zu zeigen ist, dass $\mathrm{Vol}(X) > 2^n \cdot \mathrm{Vol}(\Gamma)$ ist. Hieraus folgt dann die Behauptung. Also müssen wir das Volumen von X berechnen. Dazu wollen wir die Isometrie f: $K_{\mathbb{R}} \xrightarrow{\sim} \prod_\tau \mathbb{R}$ aus Satz 5.1 ausnutzen. Hierbei beachten wir $\mathrm{Vol}(X) = 2^s \cdot \mathrm{Vol}_{stand}(f(X))$, wobei

$$f(X) = \left\{ (x_\tau) \in \prod_\tau \mathbb{R}; |x_\varrho| < c_\varrho, x_\sigma^2 + x_{\overline{\sigma}}^2 < c_\sigma^2 \right\} = \text{„Quader“} \times \text{„Sphäre“}$$

Hieraus ergibt sich dann mit mehrdimensionaler Analysis:

$$\mathrm{Vol}(X) = 2^s \cdot \prod_\varrho (2c_\varrho) \cdot \prod_{i=1}^{s} (\pi \cdot c_\sigma^2) = 2^{r+s} \cdot \pi^s \cdot \prod_\tau c_\tau \overset{(3)}{>} 2^{r+s} \cdot \pi^s \cdot \left(\frac{2}{\pi} \right)^s \cdot (\mathcal{O} : \mathfrak{a}) \cdot \sqrt{|d_k|} = 2^n \cdot \mathrm{Vol}(\Gamma)$$

Der letzte Schritt folgt mit Satz 5.2. □

2.3 Die Klassenzahl eines Zahlkörpers

Definition:

Der Index $(\mathcal{O} : \mathfrak{a})$ eines Ideals $\mathfrak{a} \triangleq \mathcal{O}$, $\mathfrak{a} \neq (0)$ heißt „**(Absolut-)Norm**“ des Ideals: $N_\mathfrak{a} := (\mathcal{O} : \mathfrak{a})$.

Bemerkung:

Die Bezeichnung ist begründet durch die Eigenschaft $N(\mathcal{O} \cdot \mathfrak{a}) = |N_{K/\mathbb{Q}}(\alpha)$ für Hauptideale $\mathfrak{a} = \mathcal{O} \cdot \alpha \triangleq \mathcal{O}$. (Übung!)

Satz 6.1:

Die Idealnorm ist multiplikativ. Das heißt, es gilt $N(\mathfrak{a} \cdot \mathfrak{b}) = N_\mathfrak{a} \cdot N_\mathfrak{b}$ $\forall$ $\mathfrak{a}$, $\mathfrak{b} \triangleq \mathcal{O}$. Weiterhin setzt sie sich fort zu einem Gruppenhomomorphismus N: $J_K \mapsto \mathbb{Q}^\times_{>0}$.

Beweis:

Sei $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$ mit $\nu_\mathfrak{p} \geq 0$ und fast alle $\nu_\mathfrak{p} = 0$. Es genügt zu zeigen, dass $N_\mathfrak{a} = \prod_\mathfrak{p} (N_\mathfrak{p})^{\nu_\mathfrak{p}}$. (Hieraus folgt sofort die Multiplikativität.) Wir benutzen den chinesischen Restsatz für unseren Quotientenring $\mathcal{O}/\mathfrak{a}$:

$$\mathcal{O}/\mathfrak{a} = \bigoplus_\mathfrak{p} \mathcal{O}/\mathfrak{p}^{\nu_\mathfrak{p}}$$

Hieraus ergibt sich dann:

$$N_\mathfrak{a} = |\mathcal{O}/\mathfrak{a}| = \prod_\mathfrak{p} |\mathcal{O}/\mathfrak{p}^{\nu_\mathfrak{p}}| = \prod_\mathrm{P} N(\mathfrak{p}^{\nu_\mathfrak{p}})$$

Betrachte nun die Idealkette $\mathfrak{p} \supsetneqq \mathfrak{p}^2 \supsetneqq \mathfrak{p}^3 \supsetneqq \ldots \supsetneqq \mathfrak{p}^\nu$, $\mathfrak{p}^i \neq \mathfrak{p}^{i+1}$ wegen eindeutiger Primzerlegung. $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ ist ein $\mathcal{O}/\mathfrak{p}$-Vektorraum. (Zunächst ist dies ein $\mathcal{O}$-Modul. $\mathfrak{p}$ annuliert, also operiert $\mathcal{O}/\mathfrak{p}$.) Es ist $\dim_{\mathcal{O}/\mathfrak{p}}(\mathfrak{p}^i/\mathfrak{p}^{i+1}) = 1$, denn sei $\mathfrak{a} \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ und $(a) + \mathfrak{p}^{i+1} =: \mathfrak{b}$. Hieraus folgt $\mathfrak{p}^i \supseteq \mathfrak{b} \supsetneqq \mathfrak{p}^{i+1}$; das heißt, $\mathfrak{p}^i | \mathfrak{b} | \mathfrak{p}^{i+1}$ und hiermit $\mathfrak{b} = \mathfrak{p}^i$. Also erzeugt $\overline{\mathfrak{a}} := \mathfrak{a} + \mathfrak{p}^{i+1}$ $\mathfrak{p}^i/\mathfrak{p}^{i+1}$. Somit ist $\mathfrak{p}^i/\mathfrak{p}^{i+1} \simeq \mathcal{O}/\mathfrak{p}$. Mit dem Index-Multiplikationssatz erhalten wir:

$$N(\mathfrak{p}^\nu) = (O : \mathfrak{p}^\nu) = (\mathcal{O} : \mathfrak{p})(\mathfrak{p} : \mathfrak{p}^2) \ldots (\mathfrak{p}^{\nu-1}\mathfrak{p}^\nu) = (\mathcal{O} : \mathfrak{p})^\nu = (N_\mathfrak{p})^\nu$$

J_K ist die freie abelsche Gruppe über der Menge der Primideale $\mathfrak{p}$. Somit existiert ein eindeutiger Homomorphismus $J_K \mapsto$ (beliebige abelsche Gruppe) bei Vorgabe der Bilder der Basiselemente; insbesondere hier mit $J_K \mapsto \mathbb{Q}^\times$, $\mathfrak{p} \mapsto N_\mathfrak{p}$. □

Lemma 6.2:

In jedem Ideal $\mathfrak{a} \neq (0)$ von $\mathcal{O}$ existiert ein Element $a \neq 0$ mit $|N_{K/\mathbb{Q}}(a)| \leq (2/\pi)^s \cdot \sqrt{|d_k|} \cdot N_\mathfrak{a}$.

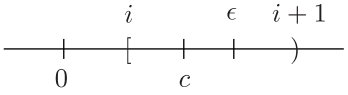
Beweis:

Zu festem $\epsilon > 0$ wähle $c_\tau > 0$ für alle Einbettungen τ: $K \hookrightarrow \mathbb{C}$ mit $c_{\overline{\tau}} = c_\tau$ und

$$\prod_\tau c_\tau = \left(\frac{2}{\pi}\right)^s \sqrt{|d_k|} \cdot N_\mathfrak{a} + \epsilon$$

Nach dem Theorem 3.5 existiert ein $a \neq 0$ in $\mathfrak{a}$, so dass $|\tau(\alpha)| < c_\tau$. Hieraus ergibt sich dann:

$$|N_{K\setminus\mathbb{Q}}(a)| = \prod_\tau |\tau(a)| < \prod_\tau c_\tau \leq \underbrace{\left(\frac{2}{\pi}\right)^s \sqrt{|d_k|} \cdot N_\mathfrak{a}}_{\text{positive Konstante } c} + \epsilon$$



Hieraus folgt $|N_{K/\mathbb{Q}}(a)| \leq i \leq c$. □

Theorem 6.3:

Die Idealklassengruppe $\mathfrak{Cl}_K = \mathcal{J}_K/\mathfrak{p}_K$ ist endlich. (Die Ordnung $h_K := |\mathfrak{Cl}_K|$ heißt die „Klassenzahl“ von K.)

Beweis:

Für ein beliebiges Primideal $\mathfrak{p} \neq (0)$ sei $\mathfrak{p} \cap \mathbb{Z} = p \cdot \mathbb{Z}$ (Hieraus folgt, dass p eine Primzahl ist.) Sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{O}/\mathfrak{p}$ (beides sind endliche Körper) insbesondere eine endliche Körpererweiterung vom Grad $f := (\mathcal{O}/\mathfrak{p} \colon \mathbb{F}_p)$. Hieraus folgt $N_\mathfrak{p} = |\mathcal{O}/\mathfrak{p}| = p^f$.

- Zu festem p existieren nur **endlich** viele Primideale $\mathfrak{p}$ mit $\mathfrak{p} \cap \mathbb{Z} = p \cdot \mathbb{Z}$. (Denn: Aus $p \in \mathfrak{p}$ ergibt sich $(p) \leq \mathfrak{p}$, also $\mathfrak{p} | (p)$)
- Zu vorgegebener Schranke S existieren nur **endlich** viele Primideale $\mathfrak{p}$ mit $N_\mathfrak{p} \leq S$ mit $p \leq p^f = N_\mathfrak{p}$ (da nur endlich viele Primzahlen $p \leq S$ existieren).
- Es existieren sogar nur **endlich** viele Ideale $\mathfrak{a} \triangleq \mathcal{O}$ mit $N_\mathfrak{a} \leq S$ (da $\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}}$). Hieraus ergibt sich $N_\mathfrak{a} = \prod_\mathfrak{p} N_\mathfrak{p}^{\nu_\mathfrak{p}} \leq S$. (Es ist $N_\mathfrak{p} \leq N_\mathfrak{a}$ für $\nu_\mathfrak{p} \geq 1$.) Damit haben nur die endlich vielen $\mathfrak{p}$ mit $N_\mathfrak{p} \leq S$ eventuell $\nu_\mathfrak{p} > 0$, wobei die $\nu_\mathfrak{p}$ beschränkt sind wegen $N_\mathfrak{p}^{\nu_\mathfrak{p}} \leq S$.

Es genügt zu zeigen, dass in jeder Klasse $[\mathfrak{a}] \in \mathfrak{Cl}_K$ ein ganzes Ideal $\mathfrak{a}_1$ mit $N_\mathfrak{a} \leq M := (2/\pi)^s \sqrt{|d_k|}$. (Hieraus folgt, dass eine **endliche** Menge von Vertretern aller Klassen existiert, also $|\mathfrak{Cl}_K| < \infty$). Dazu sei $\mathfrak{a}$ ein beliebiger Vertreter seiner Klasse $[\mathfrak{a}]$ (nicht notwendig ganz). Wir wissen, dass es ein $\gamma \in \mathcal{O}$ gibt mit $\gamma \neq 0$ und $\mathfrak{b} := \gamma \cdot \mathfrak{a}^{-1} \subseteq \mathcal{O}$. Nach Lemma 6.2 existiert ein $\beta \in \mathfrak{b}$ mit $\beta \neq 0$, wobei $|N_{K/\mathbb{Q}}(\beta)| \cdot N\mathfrak{b}^{-1} = N((\beta) \cdot \mathfrak{b}^{-1}) \leq M$. Somit ist $\mathfrak{a}_1 := \beta \cdot \mathfrak{b}^{-1} = \beta \cdot \gamma^{-1} \cdot \mathfrak{a} \in [\mathfrak{a}]$ wie behauptet. □

Bemerkung:

$h_K = 1$ bedeutet, dass $\mathcal{O}$ Hauptidealring ist, also hier, dass in $\mathcal{O}$ eindeutige Primzerlegung (der Elemente) vorliegt wie in $\mathbb{Z}$. Die Endlichkeit von h_K besagt, dass die Abweichung von der eindeutigen Primzerlegung nicht allzu groß ist. $\mathfrak{Cl}_K$ ist ein **Maß dieser Abweichung**.
Beobachtung: In der Regel ist $h_K > 1$. Offenes Problem: Gibt es unendlich viele Zahlkörper mit $h_K = 1$? Bekannt ist, dass es genau neun imaginär-quadratische Zahlkörper K gibt mit Klassenzahl $h_K = 1$. Dies sind $K = \mathbb{Q}(\sqrt{d})$ mit $d = -1, -2, -3, -7, -11, -19, -43, -67$ und -163 (Satz von Heegner-Stark). Man vermutet, dass es bereits unendlich viele reell-quadratische Zahlkörper mit $h_K = 1$ gibt.
Sei h_n mit $n \in \mathbb{N}$ die Klassenzahl des Einheitswurzelkörpers $\mathbb{Q}^{(n)} := \mathbb{Q}(\exp(2\pi \mathrm{i}/n))$. Die Klassenzahl dieses Zahlkörpers ist entscheidend für den folgenden Satz:

2.3.1 Kummerscher Satz

Für Primzahlen $p \geq 3$ mit $p \nmid h_p$ ist $X^p + Y^p = Z^p$ unlösbar ist mit $x, y, z \neq 0$. (Das heißt, Fermats Vermutung gilt für diese p mit $p \nmid h_p$.) Mehr dazu in den Übungen! Man bezeichnet solche Primzahlen als **regulär** (sonst **irregulär**). Offen ist weiterhin, ob unendlich viele p existieren.
Es ist generell schwierig, Vorhersagen über die Struktur der Klassengruppe zu machen, auch für $\mathbb{Q}^{(n)}$ oder auch nur für h_n. Die Iwasawa-Theorie beschreibt die Asymptotik von h_K für K in Körpertürmen. Es gilt $\mathrm{ord}_p(H_{a \cdot p^n}) = \lambda_p \cdot p^n + \mu_p \cdot n + \nu_p$ mit gewissen Konstanten λ_p, μ_p und ν_p. μ_p ist of gleich 0 (beispielsweise für Einheitswurzelkörper).

2.4 Der Dirichletsche Einheitensatz

Sie K ein Zahlkörper mit $(K : \mathbb{Q}) = n = r + 2s$ und $E := E_K := \mathcal{O}_K^\times$ die „Einheitengruppe“. Weiterhin sei $\mu(K)$ die Gruppe der Einheitswurzeln in K.

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_\mathbb{C}^\times & \xrightarrow{l} & \prod_\tau \mathbb{R} \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow{\scriptstyle \mathrm{Tr}} \\ \mathbb{Q}^\times & \xrightarrow[\subseteq]{} & \mathbb{C}^\times & \xrightarrow[\log|\bullet|]{} & \mathbb{R} \end{array}$$

wobei j wie früher definiert, $j \colon K^\times \mapsto K_\mathbb{C}^\times = \prod_\tau \mathbb{C}^\times$,$N \colon \prod_\tau \mathbb{C}^\times \mapsto \mathbb{C}^\times, (\ldots, z_\tau, \ldots) \mapsto \prod_\tau z_\tau$ und $l(\ldots, z_\tau, \ldots) := (\ldots, \log|z_\tau|, \ldots)$. Wir gehen nun über zu $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$-Fixmoduln. Wir finde dann folgendes kommutatives Diagramm:

$$\begin{array}{ccccc} K^\times & \xrightarrow{j} & K_\mathbb{R}^\times & \xrightarrow{l} & (\prod_\tau \mathbb{R})^+ \\ \downarrow{\scriptstyle N_{K/\mathbb{Q}}} & & \downarrow{\scriptstyle N} & & \downarrow \\ \mathbb{Q}^\times & \longrightarrow & \mathbb{R}^\times & \longrightarrow & \mathbb{R} \end{array}$$

Beachte: Hierbei nehme triviale Operation auf $K^\times$. Geraden: $j(K) \leq K_\mathbb{R}$

$$\left(\prod_\tau \mathbb{R}\right)^+ = \prod_\varrho \mathbb{R} \times \prod_\sigma (\mathbb{R}\times\mathbb{R})^+ \xrightarrow[\alpha]{\simeq} \mathbb{R}^{r+s}$$

($\mathbb{R}\times\mathbb{R} = \Delta = \{(x,x), x\in\mathbb{R}\}$ ist die sogenannte **Diagonale**.

$\alpha l(j(x)) = (\log|x_{\varrho_1}, \ldots, \log|x_{\varrho_r}|, \log|x_{\sigma_1}|^2, \ldots, \log|x_{\sigma_s}|^2)$

Erinnere:

- $E = \{\varepsilon \in \mathcal{O}_K; N_{K/\mathbb{Q}}(\varepsilon) = \pm 1\}$ und
- $S = \{y \in K_\mathbb{R}^\times, N(y) = \pm 1\}$ („**Norm-Eins-Fläche**“) und
- $H := \left\{x \in \left(\prod \mathbb{R}\right)^+, \mathrm{Tr}(x) = 0\right\}$ („**Super-Null-Hyperebene**“)

Betrachte: $E \xrightarrow{j} S \xrightarrow{l} H$ mit $E \underset{\lambda}{\to} H$ und $\lambda(E) =: \Gamma$

Satz 7.1:

Die Sequenz $1 \mapsto \mu(K) \xrightarrow{\subseteq} E_K \xrightarrow[(\ldots,\log|\tau|,\ldots)]{\lambda} \Gamma \mapsto 0$ ist exakt.

Beweis:

Zu zeigen ist, dass $\mu(K) = \mathrm{Kern}(\lambda)$. Sei $\zeta \in \mu(K)$: $\tau(\zeta)$ Einheitswurzel mit $|\tau(\zeta)| = 1$. Also folgt $\log|\tau(\zeta)| = 0$ $\forall\ \tau$, woraus sich $\lambda(\zeta) = (0,\ldots,0) \equiv \underline{0}$ ergibt. Hieraus folgt „$\subseteq$“. Zeigen wir noch, dass dies auch in der anderen Richtung gilt. Sei $\epsilon \in \mathrm{Kern}(\lambda)$, also $\underline{0} = \lambda(\epsilon) = l(j(\epsilon))$. Daraus resultiert $|\tau(\epsilon)| = 1\ \forall\ \tau$. Somit ist $j(\mathrm{Kern}(\lambda))$ beschränkt Teilmenge des Gitters $j(\mathcal{O}_K)$, also eine endliche Gruppe. Da j injektiv ist, ist auch das Urbild, also $\mathrm{Kern}(\lambda)$ endliche Untergruppe von $K^\times$. Dies sind gerade die Einheitswurzeln, also ist $\mathrm{Kern}(\lambda) \subseteq \mu(K)$. □
Die Restaufgabe ist nun, Γ zu bestimmen.

Lemma 7.2:

Zu gegebenem $a \in \mathbb{Z}_{>0}$ existieren höchstens **endlich** viele nicht assoziierte $\alpha \in \mathcal{O}_K$ mit $N_{K/\mathbb{Q}}(\alpha) = a$.

Beweis:

Wir betrachten die endlichen vielen Nebenklassen $\alpha + a\cdot\mathcal{O}$ im Restklassenring $\mathcal{O}/a\cdot\mathcal{O}$ mit $|N(\alpha)| = a$. Wir zeigen: Falls $\beta \in \alpha + a\cdot\mathcal{O}$ mit $|N(\beta)| = a$, so folgt $\beta \in \alpha\cdot E$ (oder $\alpha \sim \beta$).

$$\beta = \alpha + a\cdot\gamma \Rightarrow \frac{\alpha}{\beta} = 1 \pm \frac{N(\beta)}{\beta}\gamma \in \mathcal{O}$$

Wegen der Symmetrie gilt ach $\beta/\alpha \in \mathcal{O}$, also $\alpha/\beta \in E$. □

Satz 7.3:

Γ ist ein vollständiges Gitter in H ($\subseteq \mathbb{R}^{r+s}$).

Beweis:

a.) 1.Schritt: Γ ist ein Gitter in H (das heißt, eine diskrete Untergruppe). Es genügt zu zeigen, dass $\forall\ c > 0$ gilt:

$$\left|\left\{(x_\tau) \in \prod_\tau \mathbb{R}; |x_\tau| < c\right\} \cap \Gamma\right| < \infty \text{ mit } \left\{(x_\tau) \in \prod_\tau \mathbb{R}; |x_\tau| < c\right\} := Q_c$$

Schauen wir uns das Urbild des Quaders Q_c an:

$$l^{-1}(Q_c) = \left\{(z_\tau) \in \prod_\tau \mathbb{C}^\times; \exp(-c) < |z_\tau| < \exp(c)\right\}$$

Mit $j(E) \subseteq \text{Gitter} j(\mathcal{O}) \subseteq \left(\prod_\tau \mathbb{C}^\times\right)^+$ ergibt sich dann $|l^{-1}(Q_\tau \cap j(E)| < \infty$ (da diskret und beschränkt). Hieraus folgt dann $Q_c \cap \Gamma < \infty$.

b.) 2.Schritt: Γ ist **vollständig** in H. Wir erinnern uns an das Kriterium (Lemma 4.3): Finde eine beschränkte Menge $M \subseteq H$, so dass $H = \bigcup_{\gamma\in\Gamma} M + \gamma$. Dabei gehen wir folgendermaßen vor. Konstruiere ein beschränktes $T \subseteq S$ (Norm-Eins-Fläche) mit der Eigenschaft $S = \bigcup_{\epsilon\in E} T \cdot j(\epsilon)$ und setze $M := l(T)$. Beachte: Für $x = (x_\tau) \in T$ gilt wegen $\prod_\tau |x_\tau| = 1$ (Charakterisierung von S) und Beschränktheit von T gibt es Konstante $\delta_1 > 0$ und $\delta_2 > 0$, so dass $\delta_1 \leq |x_\tau| \leq \delta_2 \ \forall\ x \in T$. Damit ist der Logarithmus und so auch $l(T)$ beschränkt. Mit diesen Vorüberlegungen können wir T konstruieren. Wähle $c_\tau > 0$ mit der Einschränkung $c_\tau = c_{\overline{\tau}}$ und

$$C := \prod_\tau c_\tau > \left(\frac{2}{\pi}\right)^s \cdot \sqrt{|d_k|}$$

Betrachte $X := \{(z_\tau) \in K_\mathbb{R}; |z_\tau| < c_\tau\}$. Hieraus folgt für $y = (y_\tau) \in S$: $X \cdot y = \{(z_\tau) \in K_\mathbb{R}; |z_\tau| < c'_\tau\}$, wobei $c'_\tau = c_\tau \cdot |y_\tau|$ und (c'_τ) ist ebenso zulässige Wahl wie (c_τ). Denn es gilt $c'_{\overline{\tau}} = c_{\overline{\tau}} \cdot |y_{\overline{\tau}}| = c_\tau \cdot |y_\tau| = c'_\tau$ wegen $y \in K^+_\mathbb{R}$, also $y_\tau = \overline{y_\tau}$. Es gilt nämlich $y_{\overline{\tau}} \cdot \overline{y_{\overline{\tau}}} = y_{\overline{\tau}} \cdot y_\tau = \overline{y_\tau} \cdot y_\tau$.

$$\prod_\tau c'_\tau = C \cdot \prod_\tau |y_\tau| = C \text{ da } y \in S$$

Aus dem Theorem 5.3 folgt, dass wir immer ein $a \in \mathcal{O}$ mit $a \neq 0$ finden, für das $j(a) = (\ldots, \tau(a), \ldots) \in X \cdot y$ gilt. Nun wähle mit Lemma 7.2 ein Vertretersystem $\alpha_1, \ldots, \alpha_N \in \mathcal{O} \setminus \{0\}$ der $a \in \mathcal{O} \setminus \{0\}$ modulo E (das heißt bis auf Assoziativität) mit $|N_{K/\mathbb{Q}}| \leq C$. Setze $T := S \cap \bigcup_{i=1}^N X \cdot j(\alpha_i)^{-1}$. Dieses T hat die gewünschten Eigenschaften. X ist beschränkt, womit auch $X \cdot y$ beschränkt ist. Eine Vereinigung von beschränkten Mengen bleibt beschränkt, womit auch T beschränkt ist. Die Restbehauptung ist nun, dass $S = \bigcup_{\epsilon\in E} T \cdot j(\epsilon)$. Da $T \subseteq S$, so gilt also auch $S \supseteq \bigcup_{\epsilon\in E} T \cdot j(\epsilon)$. Die eigentliche Arbeit besteht also darin, die umgekehrte Richtung zu zeigen. Sei nun $y \in S$ (und damit auch $y^{-1} \in S$). Wir haben schon gesehen, dass es ein $a \in \mathcal{O} \setminus \{0\}$ gibt mit $j(a) \in X \cdot y^{-1}$. Hieraus ergibt sich, dass ein $x \in X$ existiert mit $j(a) = x \cdot y^{-1}$. Wegen $|N(a)| = |N(xy^{-1})| = N(x)| < C$. Also finden wir ein α_i mit $a = \epsilon \cdot \alpha_i$, wobei $\epsilon \in E$. So folgt $y = x \cdot j(a^{-1}) = x \cdot j(\alpha_i^{-1}\epsilon^{-1})$. Ferner gilt $y \in S$, $j(\epsilon^{-1}) \in S$, also $x \cdot j(\alpha_i^{-1}) \in S \cap X \cdot j(\alpha_i^{-1}) \subseteq T$. Somit ist $y = x \cdot j(\alpha_i^{-1}) \cdot j(\epsilon^{-1}) \in T \cdot j(\epsilon^{-1})$. □

2.4.1 Dirichletscher Einheitensatz

Theorem 7.4:

Die Einheitengruppe E_K ist das direkte Produkt der endlichen zyklischen Gruppe $\mu(K)$ und einer freien abelschen Gruppe vom Rang $r + s - 1$.
Eine alternative Formulierung dieses Theorems ist folgende:

Korollar:

Es existieren $\epsilon_1, \ldots, \epsilon_t \in E$ ($t := r + s - 1$) („**Grundeinheiten**“ von K), so dass jedes $\epsilon \in E$ eindeutig darstellbar ist als Produkt $\epsilon = \zeta \cdot \epsilon_1^{\nu_1} \cdot \ldots \cdot \epsilon_t^{\nu_t}$ mit $\zeta \in \mu(K)$ und $\nu_i \in \mathbb{Z}$.

Beweis:

Aus Satz 7.3 wissen wir, dass $\Gamma \simeq \mathbb{Z}^t$ ist. Sei $v_1, \ldots, v_t \in \Gamma$ eine $\mathbb{Z}$-Basis. Wähle Urbilder $\epsilon_i \in \lambda^{-1}(v_i)$ in der exakten Sequenz $1 \mapsto \mu(K) \mapsto E \xrightarrow{\lambda} \Gamma \mapsto 0$ Sei $A := \langle \epsilon_1, \ldots, \epsilon_t \rangle \leq E$ (A ist freier $\mathbb{Z}$-Modul) und $\lambda|_A$: $A \xrightarrow{\simeq} \Gamma$ ein Isomorphismus. Daraus folgt $\mu(K) \cap A = \{1\}$. Damit haben wir ein direktes Produkt $\mu(K) \cdot A$ und $E = \mu(K) \cdot A$. □
Zur Abrundung und Vorbereitung für später bestimmen wir nun das Grundmaschenvolumen von Γ. Seien $\lambda_1, \ldots, \lambda_{r+s}$ die Komponenten der Abbildung λ: $E \mapsto H \subseteq \mathbb{R}^{r+s}$ und $\epsilon_1, \ldots, \epsilon_t$ seien Grundeinheiten von K. Betrachte in der Matrix

$$\begin{pmatrix} \lambda_1(\epsilon_1) & \ldots & \lambda_1(\epsilon_t) \\ \vdots & \ddots & \vdots \\ \lambda_{t+1}(\epsilon_1) & \ldots & \lambda_{t+1}(\epsilon_t) \end{pmatrix}$$

Minoren M vom Rang t (das heißt: eine Zeile weglassen). Dann ist $|\det(M)|$ unabhängig von der Minorenwahl. Denn für $x \in H$ gilt $\sum_\tau x_\tau = 0$, also $0 = \sum_{j=1}^{r+s} \lambda_j(\epsilon)$, also gehen obige Minoren durch eine elementare Zeilentransformation (lineare Algebra) ineinander über.

Definition:

$|\det(M)| =: R =: R_K$ heißt der „**Regulator**“ von K.

Satz 7.5:

Die Grundmasche des Einheitengitters $\Gamma = \lambda(E)$ in dem euklidischen Raum $\text{Bild}(H) \subseteq \mathbb{R}^{r+s}$ hat den Inhalt $\text{Vol}(\Gamma) = \sqrt{r+s}R$, wobei R der Regulator ist.

Beweis:

Den Standardvektorraum $\mathbb{R}^{r+s}$ können wir zerlegen in $\text{Bild}(H) \oplus \mathbb{R} \cdot \lambda_0$ mit $\lambda_0 := 1/\sqrt{r+s}(1, \ldots, 1)$ (orthogonales Komplement), wobei $\text{Bild}(H) = \{(x_i) \in \mathbb{R}^{r+s} | \sum_i x_i = 0\}$.

$\text{Vol}(\Gamma) := \text{Vol}_{\mathbb{R}^{r+s}}(\langle \Gamma, \lambda_0 \rangle)$ da $\|\lambda_0\| = 1$

Dieses Volumen können wir nun einfacher berechnen:

$$\text{Vol}(\Gamma) = \left| \det \begin{pmatrix} \lambda_{0,1} & \ldots & \lambda_1(\varepsilon_1) & \ldots & \lambda_1(\varepsilon_t) \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \lambda_{0,r+s} & \ldots & \lambda_{r+s}(\varepsilon_1) & \ldots & \lambda_{r+s}(\varepsilon_t) \end{pmatrix} \right| \text{ mit } t := r+s-1$$

Die Summe aller Zeilen führt dazu, dass die erste Zeile folgendermaßen aussieht: $(\sqrt{r+s}, 0, \ldots, 0)$. Durch Entwickeln der Determinante nach der ersten Zeile folgt die Behauptung. □

2.5 Erweiterung von Dedekindringen

Das Ziel ist eine Übersicht über alle Primideale $\mathfrak{p} \triangleq \mathcal{O}_K$ eines Zahlkörpers K. Wir haben bereits gesehen, dass für ein Primideal $\mathfrak{p} \neq 0$ immer eine Primzahl $p \in \mathbb{Z}$ existiert, so dass $\mathfrak{p} \cap \mathbb{Z} = p \cdot \mathbb{Z}$ oder $\mathfrak{p} | p \cdot \mathcal{O}$. Gesucht ist also eine Übersicht der $\mathfrak{p} | p \cdot \mathfrak{p}$ (für festes p). Alles geht allgemein für DEDEKINDringe.

Hilfssatz:

Sei R noethersch und M Teilmodul eines endlich erzeugten R-Moduls $Rx_1 + \ldots + Rx_r$. Hieraus folgt, dass M endlich erzeugt ist.

Beweis:

Dies zeigt man durch vollständige Induktion nach r.

- Induktionsanfang $r = 1$: $M \subseteq R \cdot x$

  Wir betrachten das endlich erzeugte Ideal $\mathfrak{a} := \{a \in R; a \cdot x \in M\}$. Hieraus ergibt sich $M = \mathfrak{a} \cdot x = (a_1, \ldots, a_s) \cdot x = Ra_1 \cdot x + \ldots + Ra_s \cdot x$, womit R endlich erzeugt ist.

- Induktionsschritt $r - 1 \mapsto r$: $M \subseteq R \cdot x_1 + \ldots + R \cdot x_r$

  Sei $Y := R \cdot x_2 + \ldots + R \cdot x_r$ und $\mathfrak{a} := \{a \in R; a \cdot x_1 \in M + Y\} = (a_1, \ldots, a_s)$ mit zugehörigen $m_i = a_i \cdot x_1 + y_i$ (für $i = 1, \ldots, s$). Hieraus folgt $M = R \cdot m_1 + \ldots + R \cdot m_s + M \cap Y$. $M \cap Y$ ist selbst endlich erzeugt nach Induktionsannahme. Wir nehmen nun ein beliebiges $m \in M$ und schreiben dies in folgender Form:

  $$m = a \cdot x_1 + y \text{ mit } a = \sum_i r_i a_i$$

  $$m = \sum_i r_i(a_i x_1) + y = \sum_i r_i(m_i - y_i) + y = \underbrace{\sum_i r_i m_i}_{\in M} - \underbrace{\sum r_i y_i + y}_{\in M \cap Y}$$

  □

Satz 8.1:

Sei $\mathfrak{o}$ ein DEDEKINDring mit $\text{Quot}(\mathfrak{o}) = K$, L/K eine endliche Körpererweiterung und $\mathcal{O}$ der ganze Abschluss von $\mathfrak{o}$ in L. Dann ist auch $\mathcal{O}$ ein DEDEKINDring.

Beweis:

Wir müssen die Bedingungen für einen DEDEKINDring überprüfen:

a.) Da $\mathcal{O}$ ganzer Abschluss von $\mathfrak{o}$ ist, ist $\mathcal{O}$ ganz abgeschlossen. (Dies hatten wir in eine der Übungsaufgaben gezeigt.)

b.) Zu zeigen ist, dass Primideale $\mathfrak{P} \neq 0$ maximal sind. Denn (wie im Fall $\mathfrak{o} = \mathbb{Z}$ folgt) $\mathfrak{P} \cap \mathfrak{o} =: \mathfrak{p} \neq 0$ ist Primideal in $\mathfrak{o}$ und $\mathcal{O}/\mathfrak{P}$ ist eine **Körper**erweiterung von $\mathfrak{o}/\mathfrak{p}$. Damit ist $\mathfrak{P}$ maximal.

c.) Es bleibt zu zeigen, dass O noethersch ist. (Wir werden dies hier nur für separable Erweiterungen L/K beweisen. Dies genügt für Zahlkörper.) Sei $\alpha_1, \ldots, \alpha_n \in \mathcal{O}$ eine K-Basis von L.Es gilt $d := d(\alpha_1, \ldots, \alpha_n) \neq 0$ aufgrund der Seperabilität und ach Lemma 2.4 $d \cdot \mathcal{O} \subseteq \mathfrak{o} \cdot \alpha_1 + \ldots + \mathfrak{o} \cdot \alpha_n$. Für alle Ideale $\mathfrak{a}$ (wobei $\mathfrak{a}$ insbesondere $\mathfrak{o}$-Moduln sind) folgt:

$$\mathfrak{a} \triangleq O \subseteq \mathfrak{o} \cdot \frac{\alpha_1}{d} + \ldots + \mathfrak{o} \cdot \frac{\alpha_n}{d}$$

Auf der rechten Seite steht ein endlich erzeugter o-Modul. Daraus folgt mit dem Hilfssatz, dass $\mathfrak{a}$ auch **endlich** erzeugter $\mathfrak{o}$-Modul ist und insbesondere ein endlich erzeugter $\mathcal{O}$-Modul, womit $\mathcal{O}$ noethersch ist.

Bemerkung 1:

Sei $\mathfrak{p} \triangleq \mathfrak{o}$ Primideal. Hieraus folgt $\mathfrak{p}\mathcal{O} \neq \mathcal{O}$.

Beweis:

Klar ist dies für $\mathfrak{p} = 0$. Sei also $\mathfrak{p} \neq 0$. Aus $\pi \in \mathfrak{p} \setminus \mathfrak{p}^2$ folgt $\pi \cdot \mathfrak{o} = \mathfrak{p} \cdot \mathfrak{a}$ mit $\mathfrak{p} \nmid \mathfrak{a}$, also $\mathfrak{p} + \mathfrak{a} = o$. Hieraus folgt, dass $b \in \mathfrak{p}$ und $s \in \mathfrak{a}$ existieren, so dass $1 = b + s$, wobei jedoch $1 \notin \mathfrak{p}$ und $\mathfrak{s} \cdot \mathfrak{p} \subseteq \mathfrak{p} \cdot \mathfrak{a} = \pi \cdot \mathfrak{o}$. Wäre $\mathfrak{p}\mathcal{O} = \mathcal{O}$,so folgt $\mathfrak{s} \cdot \mathcal{O} = \mathfrak{s} \cdot \mathfrak{p}\mathcal{O} \subseteq \pi\mathcal{O}$. Also existiert ein $x \in \mathcal{O} \cap K = \mathfrak{o}$ mit $\mathfrak{s} = \pi \cdot x \in \mathfrak{p}$. Dies ist ein Widerspruch zur Annahme, dass $\mathfrak{s} \notin \mathfrak{p}$ ist. □

Bemerkung 2:

Jedes Primideal $\mathfrak{p} \neq 0$ in $\mathfrak{o}$ zerfällt in $\mathcal{O}$ eindeutig als Produkt $\mathfrak{p} \cdot \mathcal{O} = \mathfrak{P}_1^{e_1} \ldots \mathfrak{P}_r^{e_r}$.(Man schreibt kurz $\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}}$.) Die Primideale $\mathfrak{P}_i$ (mit $e_i \geq 1$) sind genau die mit $\mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$.

Definition:

Der Exponent $e_\mathfrak{P} = e(\mathfrak{P}, \mathfrak{p})$ heißt „**Verzweigungsindex**“ von $\mathfrak{P}$ über $\mathfrak{p}$. Der Körpergrad $f_\mathfrak{P} := f(\mathfrak{P}, \mathfrak{p}) := (\mathcal{O}/\mathfrak{P} : \mathfrak{o}/\mathfrak{p})$ heißt „**Trägheitsgrad**“ von $\mathfrak{P}$ über $\mathfrak{p}$.

Satz 8.2:

Ist L/K separabel vom Grad $n = (L : K)$, so gilt für jedes Primideal $\mathfrak{p} \neq 0$ von $\mathfrak{o}$:

$$\boxed{\sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}, \mathfrak{p}) \cdot f(\mathfrak{P}, \mathfrak{p}) = n} \text{ oder kurz: } \sum_i e_i f_i = n$$

Beweis:

Nach dem chinesischen Restsatz gilt:

$$\mathcal{O}/\mathfrak{p}\mathcal{O} \simeq \bigoplus_{i=1}^{r} \mathcal{O}/\mathfrak{P}_i^{e_i}$$

Beides sind $\mathfrak{o}$-Moduln, annuliert von $\mathfrak{p}$, also Vektorräume über $k = \mathfrak{o}/\mathfrak{p}$. Zu zeigen ist nun:

a.) $\dim_k(\mathcal{O}/\mathfrak{p}\mathcal{O}) = n$

Seien $\omega_1, \ldots, \omega_m \in \mathcal{O}$, so dass $\overline{\omega}_1, \ldots, \overline{\omega}_m$eine k-Basis von $\mathcal{O}/\mathfrak{p}\mathcal{O}$ ist. (Die Dimension dieses Vektorraum ist endlich, da $\mathcal{O}$ endlich erzeugter $\mathfrak{o}$-Modul ist. (siehe oben)) Zu zeigen ist, dass $\omega_1, \ldots, \omega_m$ K-Basis von L ist (insbesondere $m = n$). Angenommen, $\omega_1, \ldots, \omega_m$ sind linear abhängig über k. (Hieraus folgt, dass diese über $\mathfrak{o}$ linear abhängig sind, nach Multiplikation mit dem Hauptnenner.) Es existieren $a_1, \ldots,$

$a_m \in \mathfrak{o}$ mit $\sum_{i=1}^{n} a_i\omega_i = 0$ (wobei nicht alle $a_i = 0$ sind). Betrachte nun das Ideal $\mathfrak{a} := (a_1, \ldots, a_m) \triangleq \mathfrak{o}$. Wähle $a \in \mathfrak{a}^{-1} \setminus \mathfrak{p}\mathfrak{a}^{-1}$. (Hieraus folgt insbesondere $a \cdot \mathfrak{a} \subseteq \mathfrak{o} \setminus \mathfrak{p}$.) Damit resultiert modulo $\mathfrak{p}$:

$$\sum_i \overline{a \cdot a_i} \cdot \overline{\omega}_i = \overline{0}$$

Es sind nicht alle $\overline{a \cdot a_i} = \overline{0}$ wegen $a \cdot \mathfrak{a} \subseteq \mathfrak{o} \setminus \mathfrak{p}$. Dies ist ein Widerspruch zur linearen Abhängigkeit der $\overline{\omega}_i$ über k. Damit sind $\omega_1, \ldots, \omega_m$ linear unabhängig über K. Diese Elemente erzeugen also L/K.

b.) $\dim_k(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i \cdot f_i$

Behauptung: $\omega_1, \ldots, \omega_m$ erzeugen den Vektorraum L. Um das zu zeigen, betrachten wir die folgenden $\mathfrak{o}$-Moduln, nämlich $M := \mathfrak{o} \cdot \omega_1 + \ldots + \mathfrak{o} \cdot \omega_m$ und $N := \mathcal{O}/M$. Es gilt $\mathcal{O} = M + \mathfrak{p}\mathcal{O}$, da $\overline{\omega}_i$ eine Basis von $\mathcal{O}/\mathfrak{p}\mathcal{O}$ über $\mathfrak{o}/\mathfrak{p}$ sind. Daraus folgt $N = \mathfrak{p} \cdot N$, denn es gilt, da $M \in \mathcal{O}$:

$$\mathfrak{p}N = \mathfrak{p}\,[(\mathcal{O} + M)/M] = (\mathfrak{p} \cdot \mathcal{O} + M)/M = \mathcal{O}/M = N$$

Wir haben gesehen, dass $\mathcal{O}$ endlich erzeugter $\mathfrak{o}$-Modul ist. Damit ist der Quotient $N = \mathcal{O}/M$ erst recht endlich erzeugt: $N = \mathfrak{o} \cdot \alpha_1 + \ldots + \mathfrak{o} \cdot \alpha_s$. Mit $N = \mathfrak{p} \cdot N$ finden wir Koordinaten $a_{ij} \in \mathfrak{p}$, so dass $\alpha_i = \sum_{j=1}^{s} a_{ij} \cdot \alpha_j$. Für $A := (a_{ij}) - I$ sei $B := A^{\#}$, also $B \cdot A = d \cdot I$ mit $d := \det(A)$. In Matrizenschreibweise lautet die obige Identität:

$$A \cdot \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_s \end{pmatrix} = 0$$

Multiplizieren wir dies mit der Adjunkten B, so folgt $d \cdot \alpha_i = 0 \;\forall\; i$. Hieraus ergibt sich $d \cdot N = 0$, also $d \cdot \mathcal{O} \subseteq M = \mathfrak{o} \cdot \omega_1 + \ldots + \mathfrak{o} \cdot \omega_m$. Dabei ist $d \neq 0$, denn mod $\mathfrak{p}$ gilt: $A \equiv -I$ (da alle $a_{ij} \equiv 0(\mathfrak{p})$). So gilt $d \equiv (-1)^s$ mod $\mathfrak{p}$und wir können durch d dividieren:

$$\mathcal{O} \subseteq \mathfrak{o}d^{-1}\omega_1 + \ldots + \mathfrak{o} \cdot d^{-1}\omega_m$$

Wir erinnern uns daran, dass für alle $\beta \in L$ ein $b \in \mathcal{O}$ und $a \in \mathfrak{o}$ existieren, so dass $\beta = b/a$. Damit ist $L \subseteq \langle \omega_1, \ldots, \omega_m \rangle_K \subseteq L$. Nun kommen wir zum eigentlichen Beweis, nämlich $\dim_k(\mathcal{O}/\mathfrak{P}_i^{e_i}) = e_i \cdot f_i$. Dazu betrachten wir eine Kette von k-Vektorräumen $\mathcal{O}/\mathfrak{P}^e \supsetneqq \mathfrak{P}/\mathfrak{P}^e \supsetneqq \ldots \supsetneqq \mathfrak{P}^{e-1}/\mathfrak{P}^e \neq 0$. Schauen wir uns nun den jeweiligen Quotienten zweier Vektorräume, also den Faktorraum an. Nach dem Homomorphiesatz von Vektorräumen gilt:

$$(\mathfrak{P}^\nu/\mathfrak{P}^e)/(\mathfrak{P}^{\nu+1}/\mathfrak{P}^e) \simeq \mathfrak{P}^\nu/\mathfrak{P}^{\nu+1} \simeq \mathcal{O}/\mathfrak{P}$$

Um dies einzusehen, betrachten wir den Isomorphismus von $\mathcal{O}/\mathfrak{P}$ nach $\mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$. Dazu fixieren wir ein $\alpha \in \mathfrak{P}^\nu \setminus \mathfrak{P}^{\nu+1}$ und definieren eine Abbildung φ: $\mathcal{O} \mapsto \mathfrak{P}^\nu/\mathfrak{P}^{\nu+1}$, $a \mapsto a \cdot \alpha$ mod $\mathfrak{R}^{\nu+1}$. φ ist surjektiv, da $\mathfrak{P}^{\nu+1} + \alpha \cdot \mathcal{O} = \mathrm{ggT}(\mathfrak{P}^{\nu+1}, \alpha \cdot \mathcal{O}) = \mathfrak{P}^\nu$. Ist die Abbildung auch injektiv? Dazu betrachten wir $\mathrm{Kern}(\varphi) = \{a \in \mathcal{O}, a \cdot \alpha \in \mathfrak{P}^{\nu+1}\} = \mathfrak{P}$, da $\alpha = \mathfrak{P}^\nu \cdot \mathfrak{a}$ mit $\mathfrak{P} \nmid \mathfrak{a}$. Mit $f := \dim_k(\mathcal{O}/\mathfrak{P})$ gilt: $\dim_k(\mathfrak{P}^\nu/\mathfrak{P}^e) = f + \dim_k(\mathfrak{P}^{\nu+1}/\mathfrak{P}^e)$ (nach der linearen Algebra). Insgesamt folgt $\dim_k(\mathcal{O}/\mathfrak{P}^e) = e \cdot f$. □

Problem:

Wie bestimmt man das Zerlegungsverhalten $\mathfrak{p} = \prod_{\mathfrak{P}} \mathfrak{P}^{\nu_\mathfrak{P}}$? Die Situation ist dabei folgende: L/K sei separabel und $\theta \in \mathcal{P}$ mit $L = K(\theta)$. Das zugehörige Minimalpolynom von θ sei $p(X) \in \mathfrak{o}[X]$.

Definition:

Das Ideal $\mathfrak{F} := \{\alpha \in \mathcal{O}; \alpha \cdot \mathcal{O} \subseteq \mathfrak{o}[\theta]\}$ heißt der **Führer** des Rings $\mathfrak{o}[\theta]$. (Es ist $\mathfrak{F} \neq 0$, da $d(1, \theta, \ldots, \theta^{n-1}) \cdot \mathcal{O} \subseteq \mathfrak{o} \cdot 1 + \mathfrak{o} \cdot \theta + \ldots + \mathfrak{o} \cdot \theta^{n-1} = \wr[\theta]$.) Beachte: $\mathfrak{F}$ ist das größte $\mathcal{O}$-Ideal, dass im Ring $\mathfrak{o}[\theta]$ liegt.

Satz 8.3:

Sei $\mathfrak{p} \lhd \mathfrak{o}$ Primideal, das teilerfremd zum Führer $\mathfrak{F}$ von $\mathfrak{o}[\theta]$ ist. Ferner sei über dem Restklassenkörper $k = \mathfrak{o}/\mathfrak{p}$ die Primzerlegung in ein Produkt von irreduziblen Polynomen gegeben durch $\overline{p}(X) = \prod_{i=1}^{r} \overline{p}_i(X)^{e_i}$ mit normierten Vertretern $p_i(X) \in \mathfrak{o}[X]$. Dann sind die Ideale $\mathfrak{P}_i := \mathfrak{p}\mathcal{O} + p_i(\theta) \cdot \mathcal{O}$ (für $i = 1, \ldots, r$) Primideale mit $\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ und $f(\mathfrak{P}_i/\mathfrak{p}) = \mathrm{Grad}(\overline{p}_i(X))$.

Beweis:

Setze $\mathcal{O}' = \mathfrak{o}[\theta]$. Zu zeigen ist, dass der Restklassenring $\mathcal{O}/\mathfrak{p}\mathcal{O}$ erstens isomorph ist zu $\mathcal{O}'/\mathfrak{p}\mathcal{O}'$ und zweitens $\mathcal{O}'/\mathfrak{p}\mathcal{O}'$ isomorph ist zu $k[X]/(\overline{p}(X))$ $(*)$.

1.) Es gilt $\mathfrak{p}\mathcal{O}+\mathfrak{F} = \mathcal{O}$ weil $\mathfrak{p}$ teilerfremd zu $\mathfrak{F}$ ist. Aus $\mathfrak{F} \subseteq \mathcal{O}'$ folgt $\mathfrak{p}\mathcal{O}+\mathcal{O}' = \mathcal{O}$. Die kanonische Abbildung $\mathcal{O}' \hookrightarrow \mathcal{O}/\mathfrak{p}\mathcal{O}$ ist surjektiv mit Kern $= \mathcal{O}' \cap \mathfrak{p}\mathcal{O} \stackrel{!}{=} \mathfrak{p}\mathcal{O}'$, da die Teilerfremdheit $\mathfrak{p}\mathcal{O}+\mathfrak{F} = \mathcal{O}$ impliziert, dass $\mathfrak{p} + (\mathfrak{F} \cap \mathfrak{o}) = \mathfrak{o}$, da die Teilerfremdheit erhalten bleibt. Also gilt:

$\mathfrak{p}\mathcal{O} \cap \mathcal{O}' = (\mathfrak{p}+\mathfrak{F}) \cdot (\mathfrak{p}\mathcal{O} \cap \mathcal{O}') \subseteq \mathfrak{p}\mathcal{O}'$ da $\mathfrak{F} \cdot \mathcal{O} \subseteq \mathcal{O}'$

2.) Betrachte die natürliche Surjektion $\sigma[X] \mapsto k[X] \mapsto k[X]/(\overline{p}(X))$ mit dem Kern $\mathfrak{p} \cdot \mathfrak{o}[X] + (p(X)) =: (\mathfrak{p}, p(X))$. Wegen $\mathcal{O}' = \mathfrak{o}[\theta] = \mathfrak{o}[X]/(p(X))$ folgt: $\mathcal{O}'/\mathfrak{p}\mathcal{O}' \simeq \mathfrak{o}[X]/(\mathfrak{p}, p(X))$.

Nach dem chinesischen Restsatz gilt

$$R := k[X]/(\overline{p}(X)) = \bigoplus_{i=1}^{r} k[X]/(\overline{p}_i(X)^{e_i})$$

wobei die Primideale von R gegeben sind durch die Hauptideale $R \cdot \overline{p}_i$ mit $\overline{p}_i := \overline{p}_i(X) \bmod \overline{p}(X)$ (Algebra Übung!) und $R/R \cdot \overline{p}_i = k[X]/(\overline{p}_i(X))$, also $(R/(\overline{p}_i) : h) = \mathrm{Grad}(\overline{p}_i(X))$. Die Isomorphie $(*)$ $k[X]/(\overline{p}(X)) \xrightarrow{\sim} \mathcal{O}/\mathfrak{p}\mathcal{O} =: \overline{\mathcal{O}}$, $f(X) \mapsto f(\theta)+\mathfrak{p}\mathcal{O}$ liefert die analoge Aussage für $\overline{\mathcal{O}}$. Die Primideals $\overline{\mathfrak{P}_i}$ sind die $\overline{\mathcal{O}} \cdot (p_i(\theta)) \bmod \mathfrak{p}\mathcal{O})$ $(\overline{\mathcal{O}}/\overline{\mathfrak{P}}_i : k) = \mathrm{Grad}(\overline{p}_i(X))$. Setze $\mathfrak{P}_i := \kappa^{-1}(\overline{\mathcal{P}}_i)$ bei κ: $\mathcal{O} \mapsto \mathcal{O}/\mathfrak{p}\mathcal{O}$. Hieraus folgt, dass die $\mathfrak{P}_i = \mathfrak{p}\mathcal{O} + p_i(\theta)\mathcal{O}$ alle Primideale $\mathfrak{P}|\mathfrak{p}$ $(\mathfrak{p}\mathcal{O} \subseteq \mathfrak{P})$ mit $f_i := (\mathcal{O}/\mathfrak{P}_i : k) = \mathrm{Grad}(\overline{p}_i(X))$. Ferner gilt:

$$\prod_{i=1} \mathfrak{P}_i^{e_i} = \bigcup \mathfrak{P}_i^{e_i} \subseteq \mathfrak{p}\mathcal{O} \text{ mit } \mathfrak{p} = \mathrm{Kern}(\kappa)$$

Hieraus folgt:

$$\mathfrak{p}\mathcal{O} | \prod_i \mathfrak{P}_i^{e_i} \Rightarrow \mathfrak{p} = \prod_i \mathfrak{P}_i^{e_i'} \text{ mit } e_i' \leq e_i$$

Wegen $\sum_i e_i f_i = \mathrm{Grad}(\overline{p}) = n$ und $\sum_i e_i' f_i = n$ folgt, dass alle $e_i' = e_i$ sind. □

Definition:

Ein Primideal $\mathfrak{p} = \prod_{i=1}^{r} \mathfrak{P}_i^{e_i}$ heißt

a.) „**voll zerlegt**“ oder **total zerlegt** in L, falls $r = n$ ist (also gilt $e_i = f_i = 1 \; \forall \; i$).

b.) „**unzerlegt**“, falls $r = 1$ ist. Ein $\mathfrak{P}_i|\mathfrak{p}$ heißt **unverzweigt**, falls $e_i = 1$ und die Restklassenkörpererweiterung $\mathcal{O}/\mathfrak{P}_i$ über $\mathfrak{o}/\mathfrak{p}$ separabel ist. (Die Minimalpolynome haben alle nur einfache Nullstellen.) Andernfalls heißt $\mathfrak{P}_i/\mathfrak{p}$ **verzweigt**. Falls $f_i = 1$ und $e_i > 1$, so heißt $\mathfrak{P}_i/\mathfrak{p}$ **rein verzweigt**. $\mathfrak{P}$ heißt „**unverzweigt**“, falls alle $\mathfrak{P}_i|\mathfrak{p}$ unverzweigt sind. L/K heißt **unverzweigt**, wenn alle Primideale $\mathfrak{p}$ von $\mathfrak{o}$ in $\mathfrak{O}$ unverzweigt sind.

Frage: Wie viele verzweigte $\mathfrak{p}$ existieren? (Später: Verzweigte $\mathfrak{p}$ sind ablesbar an der Diskriminante).

Satz 8.4:

Ist L/K separabel, so sind nur **endlich** viele $\mathfrak{p}$ verzweigt.

Beweis:

Sei $\theta \in \mathcal{O}$ mit $L = K(\theta)$. $p(X) \in \mathfrak{o}[X]$ heißt Minimalpolynom von θ. Dies zerfällt in Linearfaktoren:

$$p(X) = \prod_i (X - \theta_i)$$

Betrachte die Diskriminante dieses Polynoms (Elementsystem-Determinante der aufsteigenden θ-Potenzen). Dabei handelt es sich um die aus der linearen Algebra bekannten Van der Monde-Determinante:

$$d = d(1, \theta, \theta^2, \ldots, \theta^{n-1}) = \prod_{i<j} (\theta_i - \theta_j)^2 \in \mathfrak{o}$$

Setze $\mathfrak{F}$:=Führer $\mathfrak{o}[\theta]$. Behauptung: Alle Primideale $\mathfrak{p}$ sind unverzweigt, falls $\mathrm{ggT}(\mathfrak{p}, d \cdot \mathfrak{F}) = 1$ gilt, denn $\overline{d} := d \bmod \mathfrak{p}$ ist $\neq \overline{0}$. Hieraus folgt, dass $\overline{p}(X)$ keine mehrfachen Nullstellen in $\mathfrak{o}/\mathfrak{p}[X]$ hat. Aus Satz 8.3 folgt, dass alle $e_i = 1$ sind. Ferner gilt für die Restklassenkörperweiterung $\mathcal{O}/\mathfrak{P}_i = \mathfrak{o}/\mathfrak{p}[\overline{\theta}]$ für $\overline{\theta} = \theta \bmod \mathfrak{P}_i$, da $\mathfrak{o}[\theta] + \mathfrak{P}_i = \mathcal{O}$ gilt, weil $\mathrm{ggT}(\mathfrak{P}_i, \mathfrak{F}) = 1$ (das heißt, $\mathfrak{P}_i + \mathfrak{F} = \mathcal{O}$). Also ist die Erweiterung separabel und $\mathfrak{p}$ ist unverzweigt. □

Definition:

Das Ideal $\vartheta \triangleq \mathfrak{o}$, erzeugt von allen Diskriminanten $d(\omega_1, \ldots, \omega_n)$ mit $\omega_i \in \mathcal{O}$, K-Basis von L, heißt die „**Diskriminante der Erweiterung**“ $\mathcal{O}/\mathfrak{o}$. (Später: $\mathfrak{p}|\vartheta \Leftrightarrow \mathfrak{p}$ verzweigt)

2.6 Hilbertsche Verzweigungstheorie

Situation: Sei L/K galoisch und $G = \mathrm{Gal}(L/K)$. Zuerst kommen wir zu einigen grundsätzlichen Beobachtungen:

a.) G operiert auf $\mathcal{O}$, da für $a \in \mathcal{O}$ und $\sigma \in G$ auch $\sigma(a) \in \mathcal{O}$ ist (betrachte das Minimalpolynom).

b.) Sei $\mathfrak{P}$ Primideal von $\mathcal{O}$ mit $\mathfrak{P}|\mathfrak{p}$, dann gilt $\sigma\mathfrak{P}|\mathfrak{p}$. Das heißt, G operiert auf der Menge aller Teiler $\mathfrak{P}|\mathfrak{p}$ (für festes $\mathfrak{p}$). Denn es gilt $\sigma\mathfrak{P} \cap \mathfrak{o} = \sigma\mathfrak{P} \cap \sigma(\mathfrak{o}) = \sigma(\mathfrak{P} \cap \mathfrak{o}) = \sigma(\mathfrak{p})$. Schreibe auch $\mathfrak{P}^\sigma := \sigma\mathfrak{P}$. Diese heißen zu $\mathfrak{P}$ **konjugierte** Primideale.

Satz 9.1:

G operiert transitiv auf der Menge der Teiler $\mathfrak{P}|\mathfrak{p}$ (für $\mathfrak{p}$ fest). (Ausgehend von einem beliebigem $\mathfrak{P}$ erreicht man durch Operation alle anderen.)

Beweis:

Seien $\mathfrak{P}|\mathfrak{p}$ und $\mathfrak{P}'|\mathfrak{p}$. Angenommen, es ist $\mathfrak{P}' \neq \mathfrak{P}^\sigma \ \forall\ \sigma \in G$. Wir nutzen den chinesischen Restsatz aus:

$$\mathcal{O}/(\mathfrak{P}' \cdot \prod_\sigma \mathfrak{P}^\sigma) \simeq \mathcal{O}/\mathfrak{P}' \oplus \ldots \oplus \mathcal{O}/\mathfrak{P}^\sigma$$

Es existiert ein $x \in \mathcal{O}$ mit $x \equiv \sigma(\mathfrak{P}')$ und $x \equiv 1(\mathfrak{P}^\sigma)\ \forall\ \sigma \in G$. Weil einer der Faktoren in $\mathfrak{P}'$ ist, gilt für die Norm:

$$N(x) = \prod_{\sigma \in G} \sigma(x) \in \mathfrak{P}' \cap \mathfrak{o} = \mathfrak{p}$$

Aber es ist $x \notin \mathfrak{P}^\sigma\ \forall\ \sigma$, also $\sigma(x) \notin \mathfrak{P}\ \forall\ \sigma$. Daraus folgt:

$$\prod_{\sigma \in G} \sigma(x) \notin \mathfrak{P} \cap \mathfrak{o} = \mathfrak{p}$$

Dies ist also ein Widerspruch zu unserer Annahme. □

Definition:

Sei $\mathfrak{P}$ Primideal von $\mathcal{O}$. Die Fixgruppe $G_\mathfrak{P} := \{\tau \in G; \mathfrak{P}^\tau = \mathfrak{P}\}$ heißt „**Zerlegungsgruppe**“ von $\mathfrak{P}$ über K. Der Fixkörper $Z_\mathfrak{P} := L^{G_\mathfrak{P}}$ heißt „**Zerlegungskörper**“ von $\mathfrak{P}$ über K.

Bemerkungen 9.2:

1.) Die Abbildung (bei festem $\mathfrak{P}/\mathfrak{p}$) $G/G_\mathfrak{P} \mapsto \{\mathfrak{P}'; \mathfrak{P}'|\mathfrak{p}\}$, $\sigma \mapsto \mathfrak{P}^\sigma$ ist bijektiv. (Die ist klar nach 9.1 wegen der „Bahnbilanz“. Die Elementanzahl einer Bahn, also die Bahnlänge, ist gleich dem Index der Fixgruppe.)

2.) $G_\mathfrak{P} = 1$ ist äquivalent zu $Z_\mathfrak{P} = L$ und dies wiederum äquivalent dazu, dass $\mathfrak{p}$ voll zerlegt. Ist die Zerlegungsgruppe die volle Gruppe, also $G_\mathfrak{P} = G$, so ist dies äquivalent zu $Z_\mathfrak{P} = K$ und dies wiederum dazu, dass $\mathfrak{P}$ unzerlegt ist.

3.) Es ist $G_{\sigma\mathfrak{P}} = \sigma G_\mathfrak{P} \sigma^{-1}$, da:

$$\tau \in G_{\sigma\mathfrak{P}} \Leftrightarrow \tau(\sigma\mathfrak{P}) = \sigma\mathfrak{P} \Leftrightarrow \sigma^{-1}\tau\sigma\mathfrak{P} = \mathfrak{P} \Leftrightarrow \sigma^{-1}\tau\sigma \in G_\mathfrak{P} \Leftrightarrow \tau \in \sigma G_\mathfrak{P} \sigma^{-1}$$

4.) In der Zerlegung $\mathfrak{p} = \prod_{i=1}^r \mathfrak{P}_i^{e_i}$ gilt, dass alle e_i gleich sind (=: e) und außerdem dass alle f_i gleich sind (:= f) und $n = r \cdot e \cdot f$.

Beweis:

Sei $\mathfrak{P} := \mathfrak{P}_1$ und $\mathfrak{P}_i = \sigma_i\mathfrak{P}$ für geeignete $\sigma_i \in G$. Wir haben den Isomorphismus σ_i: $\mathcal{O} \xrightarrow{\sim} \mathcal{O}$, also auch $\mathcal{O}/\mathfrak{P} \xrightarrow{\sim} \mathcal{O}/(\sigma_i\mathfrak{P})$, $a + \mathfrak{P} \mapsto \sigma_i(a) + \sigma_i\mathfrak{P}$. Insbesondere:

$f_i = (\mathcal{O}/\sigma_i\mathfrak{P} : \mathfrak{o}/\mathfrak{p}) = (\mathcal{O}/\mathfrak{P} : \mathfrak{o}/\mathfrak{p})$ für $i = 1, \ldots, r$

Für alle ν gilt:

$\mathfrak{P}^\nu|\mathfrak{p}\mathcal{O} \Leftrightarrow \sigma_i(\mathfrak{P}^\nu)|\sigma_i(\mathfrak{p}\mathcal{O}) = \mathfrak{p}\mathcal{O}$

Hiermit sind alle e_i gleich. □

Satz 9.3:

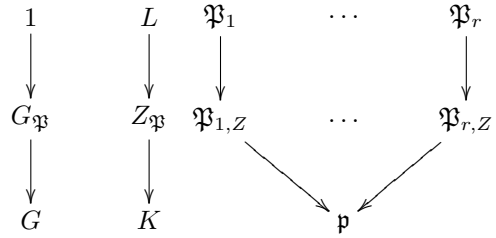
Sei $\mathfrak{P} \cap Z_\mathfrak{P} =: \mathfrak{P}_Z$ das Primideal von $Z_\mathfrak{P}$ unter $\mathfrak{P}$. Es gilt:

i.) $\mathfrak{P}_z$ ist unzerlegt in L, also ist $\mathfrak{P}$ das einzige über $\mathfrak{P}_Z$ liegende Primideal von L.

ii.) $e(\mathfrak{P}/\mathfrak{P}_Z) = e(\mathfrak{P}|\mathfrak{p}) = e$ und $f(\mathfrak{P}/\mathfrak{P}_Z) = f(\mathfrak{P}/\mathfrak{p}) = f$

iii.) $e(\mathfrak{P}_Z/\mathfrak{p}) = 1 = f(\mathfrak{P}_Z/\mathfrak{p})$

Merkschema:



Beweis:

i.) $G_\mathfrak{P} = G(L/Z_\mathfrak{P})$
Alle $\mathfrak{P}'|\mathfrak{P}_Z$ sind konjugiert unter $G_\mathfrak{P}$ (nach Satz 9.2), also von der Form $\sigma\mathfrak{P}|\mathfrak{P}_Z$ mit $\sigma \in G_\mathfrak{P}$. Hieraus folgt $\sigma\mathfrak{P} = \mathfrak{P}$, also nun $\mathfrak{P}|\mathcal{P}_Z$.

ii.) $n = r \cdot e \cdot f$ mit $r = (G : G_\mathfrak{P})$. Damit ergibt sich $|G_\mathfrak{P}| = e \cdot f$. Sei $e(\mathfrak{P}|\mathfrak{P}_Z) = e'$ und $e(\mathfrak{P}_Z|\mathfrak{p}) = e''$. Also gilt $\mathfrak{p} = \mathfrak{P}_Z^{e''} \cdot \ldots$, $\mathfrak{P}_Z = \mathfrak{P}^{e'}$. Hieraus folgt $\mathfrak{p} = \mathfrak{P}^{e' \cdot e''} \cdot \ldots$ und somit $e = e' \cdot e''$. (Dies ist klar entsprechend der Restklassengrade). Analog gilt $f = f' \cdot f''$. Es gilt $L : Z_\mathfrak{P} = e' \cdot f'$ und $(L : Z_\mathfrak{P}) = |G_\mathfrak{P}| = e \cdot f$, womit sich $e = e'$ und $f = f'$ ergibt.

Wir setzen im folgenden $\kappa(\mathfrak{P}) := \mathcal{O}/\mathfrak{P}$ und $\kappa(\mathfrak{p}) := \mathfrak{o}/\mathfrak{p}$. Beachte: Für alle $\sigma \in G_\mathfrak{P}$ induziert der Isomorphismus σ: $\mathcal{O} \xrightarrow{\sim} \mathcal{O}$ (mit $\sigma|_\mathfrak{P}$: $\mathfrak{P} \mapsto \mathfrak{P}$) den folgenden Automorphismus: $\overline{\sigma}$: $\kappa(\mathfrak{P}) \mapsto \kappa(\mathfrak{P})$, $\alpha + \mathfrak{P} \mapsto \sigma(\alpha) + \mathfrak{P}$.

Satz 9.4:

Die Erweiterung $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ ist normal und $\sigma \mapsto \overline{\sigma}$ definiert einen surjektiven Gruppenhomomorphismus $G_\mathfrak{P} \mapsto \mathrm{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}))$.

Beweis:

Wegen $f(\mathfrak{P}_Z/\mathfrak{p}) = 1$ ist $\kappa(\mathfrak{P}_Z) = \kappa(\mathfrak{p})$. Sei also ohne Einschränkung $Z_\mathfrak{P} = K$, $G_\mathfrak{P} = G$. Insbesondere haben wir nun ein Zerlegungsgesetz von einer sehr einfachen Bauart, nämlich $\mathfrak{p} = \mathfrak{P}^e$. Für $\theta \in \mathcal{O}$ sei $f(X)$ Minimalpolynom von θ über K. (Die Koeffizienten liegen in $\mathfrak{o}$.) Sei $\overline{g}(X)$ das Minimalpolynom von $\overline{\theta} \in \kappa(\mathfrak{P})$ über $\kappa(\mathfrak{p})$. Somit ist $\overline{\theta}$ Nullstelle von $\overline{f}(X) := f(X) \bmod \mathfrak{p}$ und außerdem $\overline{g}|\overline{f}$. Nach Voraussetzung ist L/K normal. Dies impliziert insbesondere $f(X) = \prod_i (X - \theta_i)$ mit $\theta_i \in \mathcal{O}$ für alle i. Hieraus folgt $\overline{f}(X) = \prod_i (X - \overline{\theta}_i) \in \kappa(\mathfrak{P})[X]$. Insbesondere zerfällt $\overline{g}$ in Linearfaktoren in $\kappa(\mathfrak{P})[X]$, das heißt, die Erweiterung $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ ist normal. (Für Zahlkörper ist die Erweiterung sogar galoisch.) Sei $\kappa(\mathfrak{P})_{sep}$ die maximal separable Teilerweiterung und hat nach dem Satz vom primitiven Element ein solches Element $\overline{\theta}$. Also ist $\mathrm{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) = \mathrm{Gal}(\kappa(\mathfrak{p})(\overline{\theta})/\kappa(\mathfrak{p}))$. (Zur Erinnerung: Wenn p Charakteristik ist, gilt $X^{p^\nu} - 1 = (X-1)^{p^\nu}$.) Sei $\overline{\sigma} \in \mathrm{Gal}(\kappa(\mathfrak{p})(\overline{\theta})/\kappa(\mathfrak{p}))$. Dann ist $\widetilde{\sigma}\overline{\theta}$ Nullstelle von $\overline{g}(|\overline{f})$. Damit existiert eine Nullstelle θ' von f mit $\widetilde{\sigma}\overline{\theta} = \theta' \bmod \mathfrak{P}$. Da θ' konjugiert ist zu θ, gibt es ein $\sigma \in G(L/K)$: $\theta' = \sigma\theta$. Nun gilt $\overline{\sigma}\overline{\theta} = \sigma\theta \bmod \mathfrak{P} = \overline{\theta}' = \widetilde{\sigma}\overline{\theta}$. Also ist $\widetilde{\sigma} = \overline{\sigma}$ und daraus folgt die Surjektivität. □

Definition:

Der Kern $\mathrm{Ker}(G_\mathfrak{P} \mapsto \mathrm{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}), \sigma \mapsto \overline{\sigma}) = I_\mathfrak{P}$ heißt die „**Trägheitsgruppe**“ von $\mathfrak{P}$ über K. Der zugehörige Fixkörper $T_\mathfrak{P} := L^{I_\mathfrak{P}}$ heißt der „**Trägheitskörper**“ von $\mathfrak{P}$ über K. Wir erhalten somit eine exakte Sequenz von Gruppenhomomorphismen $1 \mapsto I_\mathfrak{P} \xrightarrow{\subseteq} G_\mathfrak{P} \mapsto \mathrm{Aut}(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})) \mapsto 1$.

Satz 9.6:

Die Erweiterung $I_\mathfrak{P}/Z_\mathfrak{P}$ ist galoisch mit Galoisgruppe $G(T_\mathfrak{P}/Z_\mathfrak{P}) \simeq \mathrm{Aut}(\kappa(\mathfrak{P}/\kappa(\mathfrak{p}))$ und $G(L/T_\mathfrak{P}) = I_\mathfrak{P}$. Falls $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ separabel (also galoisch) ist, so gilt $|I_\mathfrak{P}| = e$, $(G_\mathfrak{P} : I_\mathfrak{P}) = (T_\mathfrak{P} : Z_\mathfrak{P}) = f$ und für das Primideal $\mathfrak{P}_T := \mathfrak{P} \cap T_\mathfrak{P}$ gilt:

i.) $e(\mathfrak{P}/\mathfrak{P}_T) = e$, $f(\mathfrak{P}/\mathfrak{P}_T) = 1$

ii.) $e(\mathfrak{P}_T/\mathfrak{P}_Z) = 1$, $f(\mathfrak{P}_T/\mathfrak{P}_Z) = f$

Beweis:

Die exakte Sequenz reproduziert die erste Aussage mittels Galoistheorie. Falls die Erweiterung $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ separabel ist, dann gilt $(T_\mathfrak{P} : Z_\mathfrak{P}) = (\kappa(\mathfrak{P}) : \kappa(\mathfrak{p})) = f$ (aufgrund der gleichen Elementanzahl). Hieraus ergibt sich:

$$e = \frac{|G_\mathfrak{P}|}{f} = \frac{|G_\mathfrak{P}|}{(G_\mathfrak{P} : I_\mathfrak{P})} = |I_\mathfrak{P}|$$

Wir zeigen nun den Punkt (i). (Dies ist äquivalent zu (ii), da $e \cdot f = |G_\mathfrak{P}|$.) Dazu ist zuerst $\kappa(\mathfrak{P}) = \kappa(\mathfrak{P}_T)$ zu beweisen. Dies wollen wir durch Vergleich von Trägheitsgruppen bewerkstelligen.

$I_\mathfrak{P} = \mathrm{Ker}(G_\mathfrak{P} \mapsto G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p})))$

$I(L/T_\mathfrak{P})_\mathfrak{P} = \mathrm{Ker}(G(L/T_\mathfrak{P})_\mathfrak{P} \mapsto G(\kappa(\mathfrak{P})/\kappa(\mathfrak{P}_T)))$

Das Ziel ist einzusehen, dass diese beiden Trägheitsgruppen gleich sind. Wir betrachten $\sigma \in I_\mathfrak{P}$. $\overline{\sigma}$ fixiert $\kappa(\mathfrak{P})$, also $\kappa(\mathfrak{P}_T)$ elementweise. Mit $G(L/T_\mathfrak{P})_\mathfrak{P} = I_\mathfrak{P}$ folgt $\sigma \in I(L/T_\mathfrak{P})_\mathfrak{P}$ und $I_\mathfrak{P} = I(L/T_\mathfrak{P})_\mathfrak{P}$. Somit ist $e = |I_\mathfrak{P}| = e(\mathfrak{P}/\mathfrak{P}_T)$. □

Korollar:

Falls $\kappa(\mathfrak{P})/\kappa(\mathfrak{p})$ separabel ist, gilt:

$I_\mathfrak{P} = 1 \Leftrightarrow T_\mathfrak{P} = L \Leftrightarrow \mathfrak{p}$ ist unverzweigt in L

In diesem Fall ist $G(\kappa(\mathfrak{P})/\kappa(\mathfrak{p}) \hookrightarrow G(L/K)$. (Sonst ist es nur ein „Subquotient“ $G_\mathfrak{P}/I_\mathfrak{P}$.)

Beweis:

Dies folgt aus dem vorherigen Satz.

2.7 Kreisteilungskörper

Sei $\zeta \in \mathbb{C}$ primitive n-te Einheitswurzel, etwa $\zeta = \exp(2\pi\mathrm{i}/n)$ (wobei n beliebig). Sei $\mathfrak{o}$ der Ring der ganzen Zahlen im Kreisteilungskörper $\mathbb{Q}(\zeta)$. Wie sieht die explizite Gestalt dieses Rings aus? Als Vorbemerkung wollen wir den Spezialfall von Primpotenzen $n = l^\nu$ betrachten.

Lemma 10.1:

Sei $n = l^\nu$ mit Primzahl l und $\lambda := 1 - \zeta$. Dann ist das Hauptideal $(\lambda) \in \mathfrak{o}$ Primideal vom Grad 1 (Restklassengrad) und es gilt $(l) = (\lambda)^d$ mit $d := \varphi(l^\nu) = (\mathbb{Q}(\zeta) : \mathbb{Q})$. Ferner hat die Körperbasis $\{1, \zeta, \ldots, \zeta^{d-1}\}$ von $\mathbb{Q}(\zeta)$ die Diskriminante $d(1, \zeta, \ldots, \zeta^{d-1}) = \pm l^s$ mit $s := l^{\nu-1}(\nu(l-1) - 1)$.

Beweis:

Wir gehen aus vom Minimalpolynom von ζ über $\mathbb{Q}$ („n-tes Kreisteilungspolynom“).

$$\prod_{\sigma\in G}(X-\zeta^\sigma)=\phi_n(X)=\frac{X^{l^\nu}-1}{X^{l^{\nu-1}}-1}=X^{l^{\nu-1}(l-1)}+\ldots+X^{l^{\nu-1}\cdot 2}+X^{l^{\nu-1}}+1$$

Dies folgt aus der geometrischen Reihe mit $q=X^{l^{\nu-1}}$. Setzen wir $X=1$, so ergibt sich:

$l=\prod_{\sigma\in G}(1-\zeta^\sigma)$ wobei $G=G(\mathbb{Q}(\zeta)/\mathbb{Q})\overset{\sim}{\leftarrow}(\mathbb{Z}/n\mathbb{Z})^\times$, $(\zeta\mapsto\zeta)=:\sigma_a\leftarrow a \bmod n$

Schauen wir uns nun einen Einzelfaktor $1-\zeta^a$ an.

$$1-\zeta^a=\varepsilon_a\cdot(1-\zeta)\text{ mit }\varepsilon_a=\frac{1-\zeta^a}{1-\zeta}=1+\zeta+\ldots+\zeta^{a-1}\in\mathfrak{o}$$

Behauptung: ε_a ist eine Einheit, also $\in\mathfrak{o}^\times$. Sei nämlich $a'\in\mathbb{Z}$ mit $a\cdot a'\equiv 1\,(n)$. Damit folgt:

$$\varepsilon_a^{-1}=\frac{1-\zeta^1}{1-\zeta^a}=\frac{1-(\zeta^a)^{a'}}{1-\zeta^a}=1+\zeta^a+\ldots+\zeta^{a(a'-1)}\in\mathfrak{o}$$

Damit existiert $\varepsilon\in\mathfrak{o}^\times$, so dass $l=\varepsilon(1-\zeta)^d$. Also ist $(l)=(\lambda)^d$ mit $d=(l:\mathbb{Q})$. Aus $e\cdot f\cdot r=d$ folgt, dass $(1-\zeta)$ Primideal ist und $f=r=1$. Kommen wir nun zur Bestimmung der Diskriminanten.

$$\phi_n(X)=\prod_{j=1}^{d}(X-\zeta_j)$$

Wir leiten $\phi_n(X)$ mittels der Produktregel ab und setzen dann ζ_i ein:

$$\phi_n'(\zeta^i)=\prod_{\substack{j=1\\ j\neq i}}^{d}(\zeta_i-\zeta_j)$$

Wir haben früher schon gesehen, dass wir die Diskriminante in folgender Form schreiben können:

$$\pm d(1,\zeta,\ldots,\zeta^{d-1})=\prod_{i\neq j}(\zeta_i-\zeta_j)=\prod_{i=1}^{d}\phi_n'(\zeta_i)=N_{L/\mathbb{Q}}(\phi_n'(\zeta))$$

Schauen wir uns die Ableitung von $(X^{l^{\nu-1}}-1)\phi_n(X)=X^{l^\nu}-1$ an:

$$l^{\nu-1}X^{l^{\nu-1}-1}\phi_n(X)+(X^{l^{\nu-1}}-1)\phi_n'(X)=l^\nu X^{l^\nu-1}$$

An der Stelle $X=\zeta$ ausgewertet, lautet dies:

$(\zeta^{l^\nu-1}-1)\phi_n'(\zeta)=l^\nu\zeta^{l^\nu-1}=l^\nu\zeta^{-1}$ da l^ν-te Einheitswurzel

Mit $\xi:=\zeta^{l^{\nu-1}}$ als primitive l-te Einheitswurzel, ergibt sich weiter:

$$N_{\mathbb{Q}(\xi):\mathbb{Q}}(\xi-1)=\prod_{x=1}^{l-1}(\zeta^x-1)=\pm\phi_l(1)=\pm(X^{l-1}+\ldots+X+1)|_{X=1}=\pm l$$

Hieraus folgt $N_{L/\mathbb{Q}}(\xi-1)=\pm l^{(L:\mathbb{Q}(\xi))}=\pm l^{l^{\nu-1}}$. Wegen $N_{L/\mathbb{Q}}(\zeta)=\pm1$ folgt für die Diskriminante:

$$d(1,\zeta,\ldots,\zeta^{d-1})=\pm N_{L/\mathbb{Q}}=\pm N_{L/\mathbb{Q}}\left(\frac{l^\nu\cdot\zeta^{-1}}{\xi-1}\right)=\pm l^{\nu\cdot d-e^{\nu-1}}=\pm l^s$$ □

Satz 10.2:

Eine Ganzheitsbasis von $\mathfrak{o}$ ist gegeben durch die aufsteigenden Potenzen 1, ζ, …, ζ^{d-1} zu einer fest gewählten n-ten Einheitswurzel. d ist der Körpergrad, also $d=\varphi(n)=(\mathbb{Q}(\zeta):\mathbb{Q})$. Das heißt, $\mathfrak{o}$ wird durch alle ζ-Potenzen erzeugt: $\mathfrak{o}=\mathbb{Z}[\zeta]$.

Beweis:

a.) Fall $n = l^\nu$ Primpotenz:

Wir erinnern uns an das Lemma 2.9. Dies besagte $l^s \cdot \mathfrak{o} = \mathbb{Z}[\zeta] \subseteq \mathfrak{o}$, wobei in unserem Falle hier $d(1, \zeta, \ldots, \zeta^{d-1}) = \pm l^s$ ist. Für $\lambda = 1-\zeta$ gilt nach Lemma 10.1 $\mathfrak{o}/(\lambda) = \mathbb{Z}/l\mathbb{Z}$, also lässt sich jedes Element von $\mathfrak{o}$ schreiben als $\mathfrak{o} = \mathbb{Z} + \lambda\mathfrak{o}$. Wir multiplizieren diese Gleichheit (in der Schreibweise $\mathfrak{o} = \mathbb{Z}[\zeta] + \lambda\mathfrak{o}$) mit λ und erhalten $\lambda\mathfrak{o} = \lambda\mathbb{Z}[\zeta] + \lambda^2\mathfrak{o}$. Setzen wir nun die vorige Gleichung für $\lambda\mathfrak{o}$ ein, so folgt $\mathfrak{o} = \mathbb{Z}[\zeta] + \lambda^2\mathfrak{o}$. Dies führt zu einem iterativen Prozess und damit zu $\mathfrak{o} = \mathbb{Z}[\zeta] + \lambda^t\mathfrak{o}\ \forall\ t \geq 1$. Insbesondere für $t := s \cdot \varphi(l^\nu)$ folgt, indem wir $l \cdot \mathfrak{o} = \lambda^{\varphi(l^\nu)} \cdot \mathfrak{o}$ mit s multiplizieren: $\mathfrak{o} = \mathbb{Z}[\zeta] + l^s \cdot \mathfrak{o} = Z[\zeta]$, da $l^s \cdot \mathfrak{o} \subseteq \mathbb{Z}[\zeta]$.

b.) Allgemeiner Fall:

Sei $n = l_1^{\nu_1} \ldots l_r^{\nu_r}$ eine Primzerlegung und $\zeta^{n/l_i^{\nu_i}} =: \zeta_i$ primitive $l_i^{\nu_i}$-te Einheitswurzel. Das Körperkompositum ist $\mathbb{Q}(\zeta) = \mathbb{Q}(\zeta_1) \ldots \mathbb{Q}(\zeta_r)$. Für dieses gilt $(\mathbb{Q}(\zeta_1) \ldots \mathbb{Q}(\zeta_{i-1})) \cap \mathbb{Q}(\zeta_i) = \mathbb{Q}$. (Die Verifizierung davon erfolgt mittels GALOIStheorie.) Für alle $i = 1, \ldots, r$ wissen wir, dass $1, \zeta_i, \ldots, \zeta_i^{d_i - 1}$ mit $d_i = \varphi(l_i^{\nu_i})$ eine Ganzheitsbasis von $\mathbb{Q}(\zeta_i)$ bildet (nach (a)). Alle Diskriminanten $d(1, \zeta_i, \ldots, \zeta_i^{d_i-1}) = \pm l_i^{s_i}$ sind paarweise teilerfremd. Nach Satz 2.6 ist $\{\zeta_i^{j_1} \cdot \ldots \cdot \zeta_r^{j_r} | j_i = 1, \ldots, d_{i-1}\}$ Ganzheitsbasis von $\mathbb{Q}(\zeta)/\mathbb{Q}$. Hieraus folgt $\mathfrak{o} \subseteq \mathbb{Z}[\zeta]$ und außerdem $\mathfrak{o} = \mathbb{Z}[\zeta]$. Aus „Reduktion modulo $\phi_n(X) \in \mathbb{Z}[X]$“ folgt $\mathfrak{o} = \mathbb{Z} + \mathbb{Z}\zeta + \ldots + \mathbb{Z}\zeta^{\varphi(n)-1}$. □

Satz 10.3 (Zerlegungsgesetz):

Sei $n = \prod_{p \text{ prim}} p^{\nu_p}$ und für jedes p sei f_o die kleinste natürliche Zahl mit $p^{f_p} \equiv 1 \bmod n/p^{\nu_p}$. Dann zerfällt die Primzahl p in $\mathbb{Q}(\zeta)$ in der Form $(p) = (\mathfrak{p}_1 \cdot \ldots \cdot \mathfrak{p}_r)^{\varphi(p^{\nu_p})}$ mit $r := \frac{\varphi(n/p^{\nu_p})}{f_p}$ verschiedenen Primidealen $\mathfrak{p}_1$, …, $\mathfrak{p}_r$ vom Grad f_p.

Beweis:

Wir wenden das Kriterium Satz 8.3 an auf $\mathbb{Z}[\zeta]$. Wegen $\mathfrak{o} = \mathbb{Z}[\zeta]$ ist Führer$(\mathbb{Z}[\zeta]) = 1$. Daraus folgt, dass ein p zerfällt wie $\phi_n(X)$ mod p. Zu zeigen ist:

$$\phi_n(X) \equiv (p_1(X) \cdot \ldots \cdot p_r(X))^{\varphi(p^{\nu_p})}_{\bmod p}$$

mit $\overline{p}_\varrho(X) \in \mathbf{F}_p[X]$ irreduzibel vom Grad f_p. Fixiere p und zerlege $n = p^\nu \cdot m$ mit $p \nmid m$. Sei nun $\phi_{p^\nu}(X) = \prod_j (X - \eta_j)$, $\phi_m(X) = \prod_i (X - \xi_i)$. Also gilt $\phi_n(X) = \prod_{i,j}(X - \eta_j \cdot \xi_i)$ Da $(X-1)^{p^\nu} \equiv X^{p^\nu} - 1 \bmod p$ ist, folgt für alle $\mathfrak{p}|p$, dass $\eta_i \equiv 1\,(\mathfrak{p})$. Also ist $\phi_n(X) \equiv \prod_i (X - \xi_i)^{\varphi(p^\nu)} \bmod \mathfrak{p}$. Aus $\prod_i (X - \xi_i)^{\varphi(p^\nu)} = \phi_m(X)^{\varphi(p^\nu)}$ folgt:

$$\boxed{\phi_m(X) \equiv \phi_m(X)^{\varphi(p^\nu)} \bmod p}$$

Die Restbehauptung ist $\phi_m \equiv \prod_{\varrho=1}^r p_\varrho(X) \bmod p$ mit $p_\varrho(X)$ irreduzibel vom Grad f_p. Dies ist äquivalent zur Behauptung für $p \nmid n$. Sei also ab jetzt ohne Einschränkung $p \nmid n$. Hieraus folgt, dass $X^n - 1 \bmod p$ keine mehrfache Nullstelle hat, denn $\mathrm{ggT}(\overline{n \cdot X^{n-1}}, \overline{X^n - 1}) = 1$, da $p \nmid n$. Die Restklassenabbbildung $\mathfrak{o} \mapsto \mathfrak{o}/\mathfrak{p}$ (mit $\mu_n = \langle\zeta\rangle \subseteq \mathfrak{o}$) eingeschränkt auf μ_n ist **injektiv**. Insbesondere ist $\zeta \bmod \mathfrak{p}$ von der Ordnung $n || \mathfrak{o}/\mathfrak{p}| - 1$. Der kleinste Erweiterungskörper $\mathbf{F}_q/\mathbf{F}_p$ mit Element der Ordnung n ist $\mathbb{F}_q = \mathbb{F}_{p^{f_p}}$ (f_p minimal mit $n || \mathbb{F}_{p^f}^\times| = p^f - 1$). Dies verrät uns, dass $\mathbb{F}_{p^{f_p}}$ Zerfällungskörper ist von $\overline{\phi}_n(X) := \phi_n \bmod p$ (kleinster Körper, der die Nullstellen ζ enthält). $\overline{\phi}_n$ hat keine mehrfachen Nullstellen (wegen $\overline{\phi}_n | \overline{X^n - 1}$) und zerfällt daher in ein Produkt **verschiedener** irreduzibler Polynome. Also ist $\overline{\phi}_n = \overline{p}_1 \cdot \ldots \cdot \overline{p}_r$ in $\mathbb{F}_p[X]$. Daher ist jedes $\overline{p}_i$ Minimalpolynom einer primitiven n-ten Einheitswurzel $\overline{\xi}_i \in \mathbb{F}_{p^{f_p}}$. Insbesondere ist Grad$(\overline{p}_i) = f_p$. □

Korollar 10.4:

Falls $p = 2 = (4, n)$, ist $p = 2$ unverzweigt. Sonst gilt, dass p verzweigt ist genau dann, wenn $n \equiv \mathfrak{o}(p)$. Für $p \neq 2$ ist p voll zerlegt genau dann, wenn $p \equiv 1\ (n)$.

Kapitel 3

Bewertungstheorie

3.1 Bewertungen

Definition 1.1:

Eine „**Bewertung**“ oder in „**Betrag**“ eines Körpers K ist eine Funktion $|\bullet| \; K \mapsto \mathbb{R}$ mit den folgenden Eigenschaften:

1.) Positiv Definitheit: $|x| \geq 0$, $|x| = 0 \Leftrightarrow x = 0$

2.) $|x \cdot y| = |x| \cdot |y|$

3.) Dreiecksungleichung: $|x + y| \leq |x| + |y|$

Beispiel:

Der **triviale Betrag** ist definiert durch $|x| := 1 \; \forall \; x \neq 0$. (Diesen wollen wir jedoch im folgenden ausschließen.)

Bemerkung:

Eine Bewertung $|\bullet|$ macht K zu einem **metrischen** Raum mit der Metrik $d(x, y) := |x - y|$. Diese Metrik macht einen Körper insbesondere zum topologischen Raum.

Definition 1.2:

Zwei Bewertungen des Körpers K heißen „**äquivalent**“, wenn sie die gleiche Topologie auf K definieren ($|\bullet|_1 \sim |\bullet|_2$).

Satz 1.3:

Es gilt $|\bullet|_1 \sim |\bullet|_2$ genau dann, wenn ein $s > 0$ existiert, so dass für alle $x \in K$ gilt: $|x|_1 = |x|_2^s$ ($|\bullet|_1 = |\bullet|_2^s$).

Beweis „⇐“:

Dies ist deshalb klar, weil $|\bullet|_1$ und $|\bullet|_1^s$ die gleiche Menge von ε-Umgebungen eines Punktes definieren, also die gleiche Topologie.

Beweis „⇒“:

Vorbemerkung: Geben wir eine Bewertung $|\bullet|$ vor. Dann gilt für $x \in K$: $|x| < 1 \Leftrightarrow \{x^n\}_{n \in \mathbb{N}}$ ist Nullfolge bezüglich der durch $|\bullet|$ definierten Topologie. (Begründung: In der Richtung „⇒“ ist die Behauptung klar. „⇐“: Sei $\{x^n\}$ Nullfolge, das heißt $|x|^n \mapsto 0$, also $|x| < 1$.) Sei $|\bullet|_1 \sim |\bullet|_2$. Aus der Vorbemerkung folgt $\forall$ $x \in K$: $|x_1| < 1 \Leftrightarrow |x_2| < 1$ $(*)$. Da $|\bullet|_1$ nichttrivial ist, existiert ein $y \in K$ mit $|y_1| > 1$. Für alle $x \neq 0$ in K finden wir ein $\alpha = \alpha(x) \in \mathbb{R}$, so dass $|x|_1 = |y|_1^\alpha$. Wähle eine Folge $m_i/n_i \in \mathbb{Q}$ mit $m_i/n_i > \alpha$ und $\lim m_i/n_i = \alpha$. Damit gilt wegen der Monotonie der Potenzfunktion:

$$|x|_1 = |y|_1^\alpha < |y_1|^{\frac{m_i}{n_i}} \text{ also } \left|\frac{x^{n_i}}{y^{m_i}}\right|_1 < 1$$

Mittels $(*)$ folgt $|x^{n_i}/y^{m_i}|_2 < 1$, also $|x|_2 < |y|_2$. Im Limes finden wir $|x|_2 \leq |y|_2^\alpha$. Die gleiche Schlussweise für eine Folge mit $m_i/n_i < \alpha$ liefert uns die entsprechende Ungleichung $|x|_2 \geq |y|_2^\alpha$, also $|x|_2 = |y|_2^\alpha$. Durch Logarithmieren folgt:

$$\frac{\log|x|_1}{\log|x|_2} = \frac{\log|y|_1}{\log|y|_2} =: s \text{ und damit } |x|_1 = |x|_2^s$$

Wegen $|y|_1 > 1$ folgt wegen der Äquivalenz $(|\bullet|_1 \sim |\bullet|_2)$ $|y|_2 > 1$, also $s > 0$. □

Korollar:

Zwei Beträge sind äquivalent $(|\bullet|_1 \sim |\bullet|_2)$ genau dann, wenn für alle $x \in K$ aus $|x|_1 < 1$ folgt, dass $|x|_2 < 1$ ist.

3.1.1 Verallgemeinerte Variante des chinesischen Restsatzes

Satz 1.4 (Approximationssatz):

Seien $|\bullet|_1, \ldots, |\bullet|_n$ paarweise inäquivalente Bewertungen von K und $a_1, \ldots, a_n \in K$. Dann existiert zu jedem $\varepsilon > 0$ ein $x \in K$ mit $|x - a_i|_i < \varepsilon$ für $i = 1, \ldots, n$. (Man spricht von einer **simultanen Approximation**.)

Beweis:

Wir zeigen dies zuerst für zwei inäquivalente Bewertungen und zwar die erste und letzte. Aus dem Korollar folgt, dass $|\bullet|_1 \not\sim |\bullet|_n$ genau dann, wenn ein $a \in K$ existiert, so dass $|a|_1 < 1$, $|a|_n \geq 1$ (und ebenso dass ein $b \in K$ existiert, so dass $|b|_n < 1$ und $|b|_1 \geq 1$). Setze $y := b/a$, so gilt $|y|_1 > 1$ und $|y|_n < 1$. Behauptung: Es gibt ein $z \in K$ mit $|z|_1 > 1$ und $|z|_j < 1$ (für $j = 2, \ldots, n$). Dies zeigen wir mittels vollständiger Induktion nach n. Den Induktionsanfang für $n = 2$ haben wir schon oben gezeigt. Führen wir nun den Induktionsschritt $n-1 \mapsto n$. Sei z so, dass die Behauptung gilt für $j = 2, \ldots, n-1$. Fall $|z|_n \leq 1$ ist, so erfüllt $z' := z^m \cdot y$ die Behauptung, wenn m nur groß genug ist. Für den Fall $|z|_n > 1$ betrachten wir die konkrete Folge $t_m := z^m/(1+z^m) \mapsto 1$ bezüglich $|\bullet|_1$ und $|\bullet|_n$ und $\mapsto 0$ bezüglich $|\bullet|_2, \ldots, |\bullet|_{n-1}$. Damit konstruieren wir ein $z'' := t_m \cdot y$. Dies erfüllt die Bedingung für m, die groß genug sind. Für das z aus der Behauptung bilde

$$w_{1,m} := \frac{z^m}{1+z^m} \mapsto \begin{cases} 1 & \text{bezüglich } |\bullet|_1 \\ 0 & \text{bezüglich } |\bullet|_2, \ldots, |\bullet|_n \end{cases}$$

Ersetze $|\bullet|_1$ durch anderes festes $|\bullet|_i$. Damit existiert für alle i ein $w_{i,m}$ mit $|w_{i,m} - 1|_i \mapsto 0$ und $|w_{i,m}|_j \mapsto 0$. Aus diesen Folgen setzt man das gesuchte Element zusammen. Nehme $x := a_1 \cdot w_{1,m} + \ldots + a_n \cdot w_{n,m}$. Dies hat die gewünschten Eigenschaften:

$$|x - a_i|_i \leq |a_i(w_{i,m} - 1)|_i + \sum_{j \neq i} |a_j w_{j,m}|_i \mapsto 0$$ □

Definition 1.5:

Eine Bewertung heißt **nicht-archimedisch** oder „**ultrametrisch**“, falls $|n|$ für alle $n \in \mathbb{N}$ beschränkt ist. Sonst heißt $|\bullet|$ **archimedisch**.

Satz 1.6:

$|\bullet|$ ist nicht-archimedisch, genau dann wenn die „**verschärfte Dreiecksungleichung**“ $|x+y| \leq \max(|x|, |y|)$ $\forall\, x, y \in K$ gilt.

Beweis „⇐“:

Es gilt $|n| = |1 + \ldots + 1| \leq |1|$. Damit ist $|n|$ beschränkt.

Beweis „⇒“:

Sei $|n| \leq C$ für alle $n \in \mathbb{N}$. Sei für $x, y \in K$ ohne Einschränkung $|x| \geq |y|$. Hieraus ergibt sich $|x|^\nu |y^{n-\nu}| \leq |x|^n$ für alle $\nu = 0, \ldots, n$.

$$|x+y|^n \leq \sum_{\nu=0}^{n} \underbrace{\left|\binom{n}{\nu}\right|}_{\leq C} \cdot |x|^\nu \cdot |y|^{n-\nu} C \cdot (n+1)|x|^n$$

Nun ziehen wir die n-te Wurzel davon und erhalten:

$|x+y| \leq C^{\frac{1}{n}}(1+n)^{\frac{1}{n}} \cdot \max\{|x|,|y|\} = \max\{|x|,|y|\}$ da $C^{\frac{1}{n}} \mapsto 1$ und $(1+n)^{\frac{1}{n}} \mapsto 1$

Damit folgt die Behauptung. □

Bemerkung:

a.) Die verschärfte Dreiecksungleichung liefert sogar, dass auch $|x| \neq |y|$ folgt, dass $|x+y| = \max\{|x|,|y|\}$ ist. (Übung!)

b.) Jede nicht-archimedische Bewertung $|\bullet|$ von K lässt sich fortsetzen auf den rationalen Funktionenkörper $K(t) = \mathrm{Quot}(K[t])$ vermöge $|a_0 + a_1 t + \ldots + a_n t^n| := \max\{|a_0|, \ldots, |a_n|\}$.

Beispiele:

1.) Der gewöhnliche Absolutbetrag $|\bullet|_\infty$ von $\mathbb{Q}$ ist archimedisch. Für jede Primzahl p ist die „**p-adische Bewertung**“ $|\bullet|_p$ von $\mathbb{Q}$ nicht-archimedisch.

$$\Big|\pm \prod_{l \text{ prim}} l^{\nu_l}\Big|_p := p^{-\nu_p}$$

Satz 1.7:

Jede (nichttriviale) Bewertung von $\mathbb{Q}$ ist äquivalent zu einem $|\bullet|_p$ oder zu $|\bullet|_\infty$.

Beweis:

Sei $|\bullet|$ nicht-archimedisch, also $|n| \leq |1| = 1$. Daraus folgt, dass eine Primzahl p existiert mit $|p| < 1$. (Andernfalls wäre $|x| = 1$ für alle $x \in \mathbb{Q}^\times$.) $\mathfrak{a} := \{a \in \mathbb{Z}; |a| < 1\}$ ist Ideal von $\mathbb{Z}$ und $p \cdot \mathbb{Z} \subseteq \mathfrak{a} \neq \mathbb{Z}$. Hieraus ergibt sich $\mathfrak{a} = p \cdot \mathbb{Z}$ wegen der Maximalität von $p\mathbb{Z}$. Für $a \in \mathbb{Z}$ sei $a = p^m \cdot b$ mit $p \nmid b$ (also $b \notin \mathfrak{a}$). Damit folgt $|b| = 1$. Also ist $|a| = |p|^m = |a|_p^s$ mit $s := \log|p| / \log p$.

3.2 Komplettierung und projektiver Limes

Sei $K \supseteq \mathcal{O} \supseteq \mathfrak{p}$ vollständig bezüglich einer diskreten Bewertung v. Haben natürliche Abbildungen $\mathcal{O} \mapsto \mathcal{O}/\mathfrak{p}^n$ $\forall\, n \geq 1$ und $\mathcal{O}/\mathfrak{p} \xleftarrow{\lambda_1} \mathcal{O}/\mathfrak{p}^2 \xleftarrow{\lambda_2} \mathcal{O}/\mathfrak{p}^3$ (λ_ν: $\mathcal{O}/\mathfrak{p}^{\nu+1} \mapsto \mathcal{O}/\mathfrak{p}^\nu$, $x + \mathfrak{p}^{\nu+1} \mapsto x + p^\nu$). Im kartesischen Produkt der Faktorringe $\mathcal{O}/\mathfrak{p}^n$ liegt der Teilring (!) $\{(x_n) \in \prod_{n=1}^\infty \mathcal{O}/\mathfrak{p}^n; \lambda_n(x_{n+1}) = x_n\} =: \lim\limits_{\leftarrow\, n} \mathcal{O}/\mathfrak{p}^n$. Man bezeichnet diesen als „**projektiven Limes**“ der $\mathcal{O}/\mathfrak{p}^n$.

3.2.1 Topologie auf dem projektiven Limes

Zunächst definieren wir eine Topologie auf den einzelnen Quotienten. Jedes $\mathcal{O}/\mathfrak{p}^n$ trage die diskrete Topologie (jede Teilmenge ist offen). $\prod_{n=1}^\infty \mathcal{O}/\mathfrak{p}^n$ trage die Produkttopologie (größte Topologie, so dass die Projektionen auf einen Einzelfaktor stetig sind).

Satz 2.5:

Die natürliche Abbildung α: $\mathcal{O} \mapsto \lim\limits_{\leftarrow\, n} \mathcal{O}/\mathfrak{p}^n$, $x \mapsto (x + \mathfrak{p}^n)$ ist eine Isomorphismus und Homöomorphismus (Bijektion, die in beiden Richtungen stetig ist), ebenso die natürliche Abbildung β: $\mathcal{O}^\times \mapsto \lim\limits_{\leftarrow\, n} \mathcal{O}^\times/U^{(n)}$ mit $U^{(n)} = 1 + \mathfrak{p}^n$.

Beweis:

1.) Injektivität:
Wir betrachten den Kern(α). Dieser ist gegeben durch Kern(α) $= \bigcap_n \mathfrak{p}^n = \{0\}$.

2.) Surjektivität:
Sei $\mathfrak{p} = \pi \cdot \mathcal{O}$ und $\mathfrak{R} \subseteq \mathcal{O}$ ein Restsystem mit $0 \in \mathfrak{R}$. Für alle $a + \mathfrak{p}^n \in \mathcal{O}/\mathfrak{p}^n$ existiert eine eindeutige Darstellung $a \equiv a_0 + a_1\pi + \ldots + a_{n-1}\pi^{n-1} \bmod \mathfrak{p}^n$ mit $a_i \in \mathfrak{R}$, wobei $\lambda_n(a_0 + \ldots + a_n\pi^n + \mathfrak{p}^{n+1}) = a_0 + \ldots + a_{n-1}\pi^{n-1} + \mathfrak{p}^n$, da $\lambda_n(a_n\pi^n) \equiv 0$. Daraus ergibt sich, dass für alle $s \in \lim_{\leftarrow} \mathcal{O}/\mathfrak{p}^n$ eine Folge $(a_i) \subseteq \mathfrak{R}$ existiert mit $s_n = a_0 + a_1\pi + \ldots + a_{n-1}\pi^{n-1} + \mathfrak{p}^n$. Damit hat s ein Urbild (bei α) mit $x := \lim_{n \mapsto \infty} a_0 + \ldots + a_n\pi^n \in \mathcal{O}$.

3.) Homöomorphie

Man vergleiche Umgebungsbasen der Null. (Dies wollen wir nicht weiter verfolgen.)

Definition:

Sei (K, v) vollständig und nicht-archimedesch. Für $f(X) = \sum_{\nu=0}^{n} a_\nu X^\nu$ sei $|f| := \max\{|a_0|, \ldots, |a_n|\}$. $f(X) \in \mathfrak{o}[X]$ heißt „**primitiv**“, wenn nicht alle Koeffizienten in $\mathfrak{p}$ liegen; das heißt, $f(X) \not\equiv 0 \bmod \mathfrak{p}$ oder $|f| = 1$.

3.2.2 Henselsches Lemma

Sei $f \in \mathfrak{o}[X]$ primitiv und besitze mod $\mathfrak{p}$ eine Zerlegung $\overline{f}(X) = \overline{g}(X) \cdot \overline{h}(X)$ mit teilerfremden Polynomen $\overline{g}$, $\overline{h} \in k[X]$. Dann zerfällt f als $f = g \cdot h$ mit g, $h \in \mathfrak{o}[X]$, $\mathrm{Grad}(g) = \mathrm{Grad}(\overline{g})$ und $g \bmod \mathfrak{p} = \overline{g}$, $h \bmod \mathfrak{p} = \overline{h}$.

Beweis:

Sei $d := \mathrm{Grad}(f)$, $m := \mathrm{Grad}(\overline{g})$. Dann gilt $d \geq \mathrm{Grad}(\overline{f}) = m + \mathrm{Grad}(\overline{h})$. Wähle g_0, $h_0 \in \mathfrak{o}[X]$ mit $\overline{g}_0 = \overline{g}$, $\overline{h}_0 = \overline{h}$ und außerdem $\mathrm{Grad}(g_0) = \mathrm{Grad}(\overline{g}) = m$, $\mathrm{Grad}(h_0) = \mathrm{Grad}(\overline{h}) \leq d - m$. Wegen $\mathrm{ggT}(\overline{g}, \overline{h}) = 1$ existieren a, $b \in \mathfrak{o}[X]$ mit $a \cdot g_0 + b \cdot h_0 \equiv 1\,(\mathfrak{p})$ (koeffizientenweise). Hieraus folgt $ag_0 + bh_0 - 1$, $f - g_0 h_0 \in \mathfrak{p}[X]$. Sei $\omega \in \mathfrak{p}$ ein Koeffizient mit minimalem v-Wert. Wir machen nun einen Ansatz für die gesuchten Polynome g und h und zwar $g = g_0 + \omega p_1 + \omega^2 p_2 + \ldots$ und $h = h_0 + \omega q_1 + \omega^2 q_2 + \ldots$ (koeffizientenweise konvergente Folgen in $\mathfrak{o}$) mit p_i, $q_i \in \mathfrak{o}[X]$, $\mathrm{Grad}(p_i) < m$, $\mathrm{Grad}(q_i) \leq d - m$. Konstruiere rekursiv Polynomfolgen $g_n = g_0 + \omega p_1 + \ldots + \omega^n p^n$ und $h_n = h_0 + \omega q_1 + \ldots + \omega^n q_n$ mit der Eigenschaft $f \equiv g_n \cdot h_n \bmod \omega^{n+1}$ $(*)$. Im Limes gilt $f = g \cdot h$. Wir zeigen dies durch vollständige Induktion. Der Fall $n = 0$ ist klar. Machen wir nun den Induktionsschritt $n - 1 \mapsto n$. Dazu betrachten wir $g_n = g_{n-1} + p_n \omega^n$ und $h_n = h_{n-1} + q_n \omega^n$ mit zu findenden p_n und q_n, so dass $(*)$ gilt. $(*)$ ist äquivalent zu:

$$f - g_n h_n \left(= f - g_{n-1} h_{n-1} - (p_n h_{n-1} + q_n g_{n-1})\omega^n - p_n q_n \omega^{2n}\right) \equiv O(\omega^{n+1})$$

$$\Leftrightarrow p_n \underbrace{h_{n-1}}_{\equiv h_0} + q_n \underbrace{g_{n-1}}_{\equiv g_0} \equiv \underbrace{\frac{f - g_{n-1} h_{n-1}}{\omega^n}}_{= f_n \in \mathfrak{o}[X]} \bmod \omega$$

Wegen $g_0 a + h_0 b \equiv 1\ (\omega)$ gilt, indem wir mit f_n multiplizieren:

$$\underbrace{(bf_n)}_{=:p'_n} h_0 + \underbrace{(af_n)}_{=:q'_n} g_0 \equiv f_n$$

p'_n und q'_n erfüllen $(*)$. Nun bleibt noch als Restproblem die Gradbeschränkung zu verifizieren. Mache dazu „Division mit Rest“ in $k[X]$.

$b \cdot f_n = q \cdot g_0 + r$ mit $\mathrm{Grad}(r) < m = \mathrm{Grad}(g_0)$

Setze $p_n := r$. g_0 hat den höchsten Koeffizienten $\in \mathfrak{o}^\times$ (da $g_0 \bmod \mathfrak{p} = \overline{g}$ und die Grade **gleich** m sind). Dann geht die Division schon in $\mathfrak{o}[X]$, also $q \in \mathfrak{o}[X]$. Mit $b \cdot f_m = q \cdot g_0 + r$ und $(bf_n)h_0 + (af_n)g_0 \equiv f_n$ ergibt sich:

$g_0(af_n + h_0 q) + h_0 p_n \equiv f_n\ (\omega)$

Wir lassen die Koeffizienten $\equiv 0\ (\omega)$ weg! Damit folgt $q_n \in \mathfrak{o}[X]$ mit $g_0 q_n + h_0 p_n \equiv f_n\ (\omega)$. (also gilt $(*)$), wobei $\mathrm{Grad}(h_0 p_n) < (d - m) + m = d$ und $\mathrm{Grad}(f_n) \leq d$, $\mathrm{Grad}(g_0) = m$. Damit ist $\mathrm{Grad}(q_n) = \mathrm{Grad}(\overline{q}_m \bmod \omega) \leq d - m$. □

Beispiel:

Sei $K \in \mathbb{Q}_p$ und $\mathfrak{o} = \mathbb{Z}_p$ und $f := X^{p-1} - 1$. Der Restklassenkörper ist $k = \mathbb{Z}_p / p \cdot \mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$. $\mathbb{F}_p^\times$ ist zyklisch der Ordnung $p - 1$. Wir wissen, dass $\overline{f} = \prod_{i=1}^{p-1}(X - \overline{i})$. Das HENSELsche Lemma sagt uns nun, dass $\zeta_i \in \mathfrak{o}$ existieren mit $f = \prod_{i=1}^{p-1}(X - \zeta_i)$. $f(\zeta_i) = 0$ ist äquivalent zu $\zeta_i^{p-1} = 1$ ($p - 1$-te Einheitswurzeln). Damit enthält $\mathbb{Z}_p$ die $(p-1)$-ten Einheitswurzeln. Beachte: Diese Einheitswurzeln bilden mit 0 ein vollständiges Restsystem, das sogar abgeschlossen unter Multiplikation ist.

Korollar 2.7:

Sei $f = a_0 + a_1 X + \ldots + a_n X^n \in K[X]$ irreduzibel. Hieraus folgt $|f| = \max\{|a_0|, |a_n|\}$. Insbesondere ergibt sich für $a_n = 1$, $a_0 \in \mathfrak{o}$, dass $f \in \mathfrak{o}[X]$ ist.

Beweis:

Ohne Einschränkung sei $f \in \mathfrak{o}[X]$ mit $|f| = 1$. (Multipliziere mit geeignetem $\gamma \in K$.) Sei $r := \min\{\nu = 0, \ldots, n; |a_\nu| = 1\}$. Hieraus folgt $f \equiv X^r \cdot (a_r + a_{r+1}X + \ldots + a_nX^n) \bmod \mathfrak{p}$. Wenn man annimmt, dass $\max\{|a_0|, |a_n|\} < 1$ ist, hat dies zur Folge, dass $0 < r < n$ ist. Dies widerspricht dem HENSELschen Lemma, womit f reduzibel ist.

Theorem 2.8:

Sei K vollständig bezüglich einer Bewertung $|\bullet|$ und L/K sei algebraisch. Dann gilt:

a.) $|\bullet|$ besitzt eine eindeutige Fortsetzung zu einer Bewertung von L.

b.) Falls $(L : K) =: n$ endlich ist, so ist die Fortsetzung durch folgende Formel gegeben:

$$|\alpha| = \sqrt[n]{|N_{L/K}(\alpha)|}$$

Man nimmt **die** positive reelle Wurzel. Zusätzlich ist L wieder vollständig bezüglich dieser Fortsetzung.

Beweis:

1.) Archimedischer Fall:

Der einzige nichttriviale Fall ist $K = \mathbb{R}$ und $\mathbb{C} = L$. Die Norm ist dann gegeben durch $N_{\mathbb{C}/\mathbb{R}}(z) = z \cdot \overline{z} = |z|_\infty^2$. Die Eindeutigkeit kann als Übung gezeigt werden!

2.) Nichtarchimedischer Fall:

O.B.d.A. nehmen wir an, dass der Grad endlich ist, also $n < \infty$.

a.) Existenz: Sei $\mathfrak{o}$ der Bewertungsring von K, also die Kreisscheibe ≤ 1. Sei außerdem $\mathcal{O}$ der ganze Abschluss von $\mathfrak{o}$ in L. $\mathcal{O}$ lässt sich als folgende Weise charakterisieren, nämlich $\mathcal{O} = \{\alpha \in L; N_{L/K}(\alpha) \in \mathfrak{o}\}$ $(*)$. „$\subseteq$“: Mit der Norm kommt man in den ganzen Abschluss. Dies hatten wir früher schon gesehen. „$\supseteq$“: Sei $\alpha \neq 0$, $N_{L/K}(\alpha) \in \mathfrak{o}$. Unser Ziel ist zu zeigen, dass alle Koeffizienten des Minimalpolynoms

$$f(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0 \in K[X] = \prod_i (X - \alpha_i) \text{ mit } \pm a_0 = \prod_i \alpha_i$$

$\in \mathfrak{o}$ sind. Ohne Einschränkung nehmen wir an, dass $\alpha = \alpha_1$ ist. Damit existiert ein m_i, so dass $a_0^m = N_{L/K}(\alpha)$ ist. (Dies gilt wegen $N_{K(\alpha)/K}N_{L/K(\alpha)}(\alpha) = N_{K(\alpha)/K}\alpha^{(L:K(\alpha))}$.) $N_{L/K}(\alpha)$ ist aber nun $\in \mathfrak{o}$, also ist $|a_0| \leq 1$; das heißt, es ist $a_0 \in \mathfrak{o}$. Nach Korollar 2.7 ist $f(X) \in \mathfrak{o}[X]$, also $\alpha \in \mathcal{O}$. Jetzt zeigen wir, dass die Funktion $|\alpha| := \sqrt[n]{|N(\alpha)|}$ eine Bewertung des Erweiterungskörpers L ist.

- Positive Definitheit: Es gilt $|\alpha| = 0$ genau dann, wenn $N(\alpha) = 0$ ist. Die ist genau dann der Fall, wenn $\alpha = 0$ ist.
- Multiplikativität: Norm, Betrag und Wurzel sind multiplikativ!
- Dreiecksungleichung (verschärft): Es genügt zu zeigen, dass $|\alpha + 1| \leq 1$ ist für $|\alpha| \leq 1$. Wieso gilt dies? Betrachten wir dazu:

  $$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$$

  Wir dividieren durch $|\beta| \geq |\alpha|$, womit sich $|\alpha/\beta + 1| \leq \max\{|\alpha/\beta|, 1\}$ ergibt. Damit ist dies gezeigt. Nun wieder zurück zum eigentlichen Beweis. Aus $(*)$ folgt $\mathcal{O} = \{\alpha \in L; |\alpha| \leq 1\}$. Es ist $\alpha + 1 \in \mathcal{O}$, wenn $\alpha \in \mathcal{O}$ liegt.

Insbesondere haben wir also gezeigt, dass $|\bullet|$ Bewertungsfortsetzung mit Bewertungsring $\mathcal{O}$ ist.

Schließe zunächst **Vollständigkeit** mit:

Hilfssatz 2.9:

Sei $(K, |\bullet|)$ vollständig und V ein n-dimensionaler Vektorraum über K. Dann sind alle Normen $\|\bullet\|$ auf V äquivalent, das heißt, zu zwei Normen $\|\bullet\|_1$, $\|\bullet\|_2$ existieren ϱ, $\varrho' > 0$, so dass $\forall\, x \in V$ gilt: $\varrho \cdot \|x\|_1 \leq \|x\|_2 \leq \varrho'\|x\|_1$. Insbesondere ist V homöomorph zu K^n, versehen mit der Maximumsnorm $\|(x_1, \ldots, x_n)\|_{max} := \max\{|x_i|\}$ und somit vollständig.

Beweis:

Dieser funktioniert analog wie in der reellen Analysis und kann als Übung durchgeführt werden.
Was also nun noch im Beweis des Theorems 2.8 fehlt, ist die Eindeutigkeit. Sind $|\bullet|$ und $|\bullet|'$ zwei Betragsfortsetzungen auf L. Die Normen auf $V = L$ sind äquivalent, womit sie gleiche Topologie definieren. Damit sind die Beträge äquivalent und somit gleich, da $|\bullet|_K = |\bullet|'_K$. □

3.3 Lokale Körper

Der Hintergrund ist, dass die Zahlentheorie „**globale Körper**“ beschreibt, also:

a.) $K/\mathbb{Q}$ endliche Erweiterungen

b.) $K/\mathbb{F}_p(t)$ endliche Erweiterungen für den rationalen Funktionenkörper über $\mathbb{F}_p$.

Dazu werden die Komplettierungen $\widehat{K}$ von K bezüglich der verschiedenen nicht-archimedischen Bewertungen v betrachtet. Für diese komplettierten Körper $(\widehat{K}, v)$ gilt:

1.) Die Bewertungen v sind diskret.

2.) Der Restklassenkörper $k = \mathfrak{o}/\mathfrak{p}$ ist **endlich**.

Abstrahiere zu:

Definition:

Ein Körper K mit (nicht-archimedischer) Bewertung v heißt „**lokaler Körper**“, falls gilt:

1.) K ist **vollständig** bezüglich v.

2.) v ist **diskret**.

3.) Der Restklassenkörper $k = \mathfrak{o}/\mathfrak{p}$ ist **endlich**.

Die (vermöge $v_\mathfrak{p}(K^\times) = \mathbb{Z}$) normierte Exponentialbewertung sei $v_\mathfrak{p}$ mit dem zugehörigen durch $q := |k|$ definierten normierten Betrag $|x|_\mathfrak{p} := q^{-v_\mathfrak{p}(x)}$.

Satz 3.1:

Ein lokaler Körper K ist lokal kompakt und sein Bewertungsring ist kompakt.

Beweis:

Gegeben ist $\mathfrak{o} \simeq \lim_{\leftarrow} \mathfrak{o}/\mathfrak{p}^n$ (algebraisch und topologisch) $\subseteq \prod_n \mathfrak{o}/\mathfrak{p}^n$. $\mathfrak{o}/\mathfrak{p}^n$ ist endlich und damit kompakt. Damit ist auch das Produkt kompakt. Die Teilmenge $\lim_{\leftarrow} \mathfrak{o}/\mathfrak{p}^n$ ist abgeschlossen und damit auch kompakt. Für alle $a \in K$ ist $a + \mathfrak{o}$ offen und kompakte Umgebung, also ist K lokal kompakt. □

Satz 3.2:

Ein Körper K ist genau dann lokal, wenn er endliche Erweiterung eines p-adischen Körpers $\mathbb{Q}_p$ oder eines rationalen Funktionenkörpers $\mathbb{F}_p((t))$ ist.

Beweis „⇐“:

Sei K/k endliche Erweiterung für $l = \mathbb{Q}_p$ oder $\mathbb{F}_p((t))$. Mit dem Fortsetzungssatz 2.8 folgt, dass K vollständig bezüglich der eindeutig bestimmten Bewertungsfortsetzung $|\alpha| = \sqrt[n]{|N(\alpha)|}$ und $|\bullet|$ ist wieder diskret. Bemerkung: Ist K/k endlich, so ist auch die Restklassenkörpererweiterung $k/\mathbb{F}_p$ endlich, denn $\overline{x}_1, \ldots, \overline{x}_m \in k$ ist linear unabhängig $/\mathbb{F}_p$. Damit ist die beliebige Vertreterwahl $x_1, \ldots, x_m \in K$ linear unabhängig $/k$, da $\lambda_1 x_1 + \ldots + \lambda_m x_m = 0$ mit $\lambda_i \in k$ und nicht alle $\lambda_i \neq 0$. Multiplizieren wir mit den Hauptnenner der λ_i:

$\lambda_1 x_1 + \ldots = 0$ mit $\lambda_i \in \mathfrak{o}$, nicht alle $\equiv \mathfrak{o}(\mathfrak{p})$

Dies ist ein Widerspruch zur Annahme! Damit sind die K lokale Körper.

Beweis „⇒“:

Sei (K, v) lokaler Körper mit $p := \mathrm{char}(k)$ ($\Leftrightarrow p \cdot 1 \in \mathfrak{p}$).

1.) Fall $\mathrm{char}(K) = 0$: Hieraus folgt $\mathbb{Q} \subseteq K$ und $v|_{\mathbb{Q}} \sim \mathrm{ord}_p$, da $v(p) > 0$ ist. K ist vollständig und damit ist $\mathbb{Q}_p \subseteq K$.

Allgemeiner Satz (über topologische Vektorräume):

Sei V ein $\mathbb{Q}_p$-Vektorraum, normiert. V ist genau dann lokal kompakt, wenn $\dim_{\mathbb{Q}_p} V < \infty$. (Der Beweis dieses Satzes ist als Übung gedacht.)

Oder man verwendet $e := v(p)$ mit $\overline{x}_1, \ldots, \overline{x}_f$ als $\mathbb{F}_p$-Basis von $k/\mathbb{F}_p$. Mit Satz 2.4 folgt, dass $\{x_i \cdot \pi^j; i = 1, \ldots, f;\ j = 1, \ldots, e\}$ eine $\mathbb{Q}_p$-Basis von K ist.

2.) Fall $\mathrm{char}(K) \neq 0$: Hierbei gilt $\mathrm{char}(K) = \mathrm{char}(k) = p$, da $l \cdot 1 = 0$ in K. Daraus folgt $l \cdot 1 = 0$ in k, das heißt $p|l$. Weil die Restklassenkörpererweiterung endlich ist, existiert ein $\alpha \in k$, so dass $k = \mathbb{F}_p(\alpha)$ mit Minimalpolynom $p(X) \in \mathbb{F}_p[X] \subseteq K[X]$. An dieser Stelle greift nun das HENSELsche Lemma. Diese besagt, dass $p(X)$ über K in Linearfaktoren zerfällt. Damit ist $\alpha \in K$ und $k \subseteq K$. Insbesondere ist k Restsystem. Sei $t \in K^\times$ Primelement. Notwendig ist t transzendent $/k$. (Sonst wäre t algebraisch $/\mathbb{F}_p$, also existiere ein q, so dass $t^{q-1} = 1$, woraus $v(t) = 0$ folgen würde.) Nach Satz 2.4 ist $K = k((t)) \supseteq \mathbb{F}_p((t))$, womit $K/\mathbb{F}_p((t))$ endlich ist! (Basis etwa $\mathbb{F}_p$-Basis von k) □

Definition:

Die lokalen Körper der Charakteristik p ($\neq 0$) heißen „**Potenzreihenkörper**“ ($\mathbb{F}_p((t))$ mit $q = p^f$). Die lokalen Körper der Charakteristik 0 heißen die „**$\mathfrak{p}$-adischen (Zahl-)körper**“ ($K/\mathbb{Q}_p$ endliche Erweiterungen).
Wir wollen nun **Exponentialfunktion** und **Logarithmus** studieren für die $\mathfrak{p}$-adischen Zahlkörper. Als Vorarbeit schauen wir uns die Gruppenstruktur der multiplikativen Gruppe von K an.

Satz 3.3:

Die multiplikative Gruppe eines lokalen Körpers besitzt die folgende Zerlegung (direktes Produkt): $K^\times = \pi^{\mathbb{Z}} \cdot \mu_{q-1} \cdot U^{(1)}$. μ_{q-1} sei die Gruppe der $(q-1)$-ten Einheitswurzeln und $U^{(1)}$ sind die Nebenklassen des maximalen Ideals $\mathfrak{p}$ zu der Bewertung, also $U^{(1)} = 1 + \mathfrak{p} \leq \mathcal{O}^\times$ („**Einseinheiten**“ (Einheiten, die kongruent zur Eins sind)). π sei festes Primelement.

Beweis:

Jedes $\alpha \in K^\times$ besitzt eine eindeutige Darstellung $\alpha = \pi^n \cdot n$ mit $n \in \mathbb{Z}$ und $u \in \mathcal{O}^\times$, also $K^\times = \langle \pi \rangle \cdot \mathcal{O}^\times$. ($\langle \pi \rangle$ ist die von π erzeugte zyklische Gruppe.) Wir schauen uns wie früher das Polynom $X^{q-1} - 1$ an. Dieses zerfällt in Linearfaktoren, nämlich $X^{q-1} - 1 = \prod_{\nu=1}^{q-1}(X - \zeta_\nu)$ in $K[X]$ wobei ζ_ν die Nullstellen des Polynoms sind (Einheitswurzeln). Nach dem HENSELschen Lemma ist $k^\times \simeq \mathbb{Z}/(q-1)\mathbb{Z}$, also isomorph zu einer zyklischen Gruppe der Ordnung $q - 1$. Damit ist die Gruppe der $(q-1)$-ten Einheitswurzeln μ_{q-1} eine Untergruppe von $\mathcal{O}^\times$ und ist mit 0 ein multiplikatives vollständiges Restsystem. So erhalten wir einen Isomorphismus $O^\times \xrightarrow{\sim} \mu_{q-1} \times U^{(1)}$, $u \mapsto (\zeta_{(u)}, u \cdot \zeta_{(u)}^{-1}$ mit $\zeta_{(u)} \in \mu_{q-1}$ eindeutig bestimmt durch $u \equiv \zeta_{(u)} \bmod \mathfrak{p}$. □

Satz 3.4:

Sei K ein $\mathfrak{p}$-adischer Zahlkörper. Dann existiert ein eindeutig bestimmter stetiger Homomorphismus log: $K^\times \mapsto K$ mit $\log(p) = 0$, der für $1 + x \in U^{(1)}$ mit $x \in \mathfrak{p}$ durch die übliche Potenzreihe des Logarithmus gegeben ist, also

$$\log(1 + x) = \sum_{\nu=1}^{\infty} (-1)^{\nu+1} \frac{x^\nu}{\nu}$$

(Diese Reihe konvergiert $\mathfrak{p}$-adisch.)

Beweis:

Sei $|\bullet|_p$ von $\mathbb{Q}_p$ auf K fortgesetzt wie in Satz 2.8. Behauptung: $\forall\ x \in \mathfrak{p}$ ist die Folge $\{x^\nu/\nu\}$ eine Nullfolge bezüglich $|\bullet|_p$, denn $v(x) > 0$, womit wir eine Konstante $c := p^{v(x)} > 1$ definieren. Das heißt, $v(x) = \ln(c)/\ln(p)$ (gewöhnlicher Logarithmus). Ferner ist $p^{v(\nu)} = p^{\mathrm{ord}_p(\nu)} \leq \nu$ also $v(\nu) \leq \ln(\nu)/\ln(p)$. Uns interessiert nun:

$$v\left(\frac{x^\nu}{\nu}\right) = \nu \cdot v(x) - v(\nu) \geq \nu\frac{\ln(c)}{\ln(p)} - \frac{\ln(\nu)}{\ln(p)} = \frac{\ln\left(\frac{c^\nu}{\nu}\right)}{\ln(p)} \xrightarrow[\nu\mapsto\infty]{} \infty$$

Also ist $\log(1+x)$ konvergent für alle $x \in \mathfrak{p}$. log: $U^{(1)} \mapsto K$ ist ein Homomorphismus, denn für unbestimmte X, Y gilt die Identität formaler Potenzreihen:

$$\log((1+X)(1+Y)) = \log(1+X) + \log(1+Y)$$

Für $x, y \in \mathfrak{p}$ konvergieren alle Reihen. **Ausdehnung** auf $K^\times$: Nehme die eindeutige Darstellung von $\alpha \in K^\times$, $\alpha = \pi^{\mathrm{ord}_\mathfrak{p}(\alpha)} \cdot \omega(\alpha) \cdot \langle\alpha\rangle$ mit $\omega(\alpha) \in \mu_{q-1}$ und $\langle\alpha\rangle \in U^{(1)}$ (mit $\pi^{\mathrm{ord}_\mathfrak{p}(x)} \in \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\alpha)} \setminus \mathfrak{p}^{\mathrm{ord}_\mathfrak{p}(\alpha)+1}$). Insbesondere sei ($\alpha = p$): $p = \pi^e \cdot \omega(p) \cdot \langle p\rangle$. Setze $\log(\pi) := -1/e \log\langle p\rangle$ und definieren damit einen Homomorphismus $K^\times \mapsto K$, $\log(\alpha) := \mathrm{ord}_\mathfrak{p}(\alpha) \cdot \log(\pi) + \log\langle\alpha\rangle$. Wegen der Struktur von $K^\times$ lässt sich ein Homomorphismus immer stets so festlegen. log ist $\mathfrak{p}$-adisch stetig und $\log(p) = 0$. Was uns nun noch fehlt, ist die **Eindeutigkeit**. Sei λ: $K^\times \mapsto K$ eine beliebige Ausdehnung von log: $U^{(1)} \mapsto K$ mit $\lambda(p) = 0$. Somit ist für alle $\zeta \in \mu_{q-1}$ $\lambda(\zeta) = 1/(q-1)\lambda(\zeta^{q-1}) = 0$ mit $\zeta^{q-1} = 1$ und

$$0 = \lambda(p) = \lambda(\pi^e \cdot \omega(p) \cdot \langle p\rangle) = e \cdot \lambda(\pi) + \underbrace{\lambda(\langle p\rangle)}_{\log\langle p\rangle} \Rightarrow \lambda(\pi) = -\frac{1}{e}\log\langle p\rangle = \log(\pi)$$

Für alle $\alpha \neq 0$ ist $\lambda(\alpha) = \log(\alpha)$ (insbesondere unabhängig von der Wahl von π).

Satz 3.5:

Sei $K/\mathbb{Q}_p$ ein $\mathfrak{p}$-adischer Zahlkörper mit $p \cdot \mathcal{O} = \mathfrak{p}^e$. Dann konvergiert die Potenzreihe

$$\exp(x) := \sum_{\nu=0}^{\infty} \frac{x^\nu}{\nu!}$$

für alle $x \in \mathfrak{p}^n$ mit $n > e/(p-1)$ und definiert dann einen Isomorphismus und Homöomorphismus

$$\exp:\ \mathfrak{p}^n \xrightarrow{\sim} U^{(n)} (= 1 + \mathfrak{p}^n)$$

Die inverse Abbildung ist gegeben durch $\exp^{-1} = \log$.

Beweis:

Dazu benötigen wir eine Formel für die p-Bewertung von $\nu!$. Betrachten wir also zuerst folgendes Lemma:

Lemma 3.6:

Sei $\nu \in \mathbb{N}$ mit p-adischer Entwicklung $\nu = \sum_{i=0}^r a_i p^i$, wobei $0 \leq a_i < p$. Dann gilt mit der p-adischen Quersumme $S_\nu := \sum_{i=0}^r a_i$:

$$\mathrm{ord}_p(\nu!) = \frac{1}{p-1}\sum_{i=0}^{r} a_i(p^i - 1) = \frac{\nu - s_\nu}{p-1}$$

Beweis des Lemmas:

Für $c \in \mathbb{R}$ sei $[c] \in \mathbb{Z}$ die größte ganze Zahl $\leq c$ (Gauss-Klammer).

$$\left[\frac{\nu}{p}\right] = a_1 + a_2 p + \ldots + a_r p^{r-1} = \text{Anzahl}\{\mu \leq \nu; p|\mu\} =: \alpha_1$$

$$\left[\frac{\nu}{p^2}\right] = a_2 + \ldots + a_r p^{r-2} = \text{Anzahl}\{\mu \leq \nu; p^2|\mu\} =: \alpha_2$$

$$\vdots$$

$$\left[\frac{\nu}{p^\nu}\right] = a_r = \text{Anzahl}\{\mu \leq \nu; p^\nu | \mu\} =: \alpha_r$$

Damit ergibt sich (Teleskopsumme!):

$$\text{ord}_p(\nu!) = (\alpha_1 - \alpha_2) + 2 \cdot (\alpha_2 - \alpha_3) + \ldots + r \cdot \alpha_r = \sum_{\varrho=1}^{r} \alpha_\varrho = a_1 + a_2(p+1) + \ldots + a_r(p^{r-1} + \ldots + p + 1)$$

Mittels der geometrischen Reihe folgt die Behauptung. □

Nun kommen wir zum eigentlichen Beweis des Satzes 3.5. Setze ord_p fort von $\mathbb{Q}_p$ auf K. Normierte Exponentialbewertung von K: $v_\mathfrak{p} = e \cdot \text{ord}_p$. Für alle $\nu > 1$ gilt:

$$\frac{\text{ord}_p(\nu)}{\nu - 1} \leq \frac{1}{p-1}$$

Dies können wir folgendermaßen einsehen:

$\nu = p^a \cdot \nu_0$ mit $p \nmid \nu_0$, $a \geq 1$

Für $a = 0$ sind wir fertig! Sonst gilt wieder mit der geometrischen Reihe:

$$\frac{\text{ord}_p(\nu)}{\nu - 1} = \frac{a}{p^a \cdot \nu_0 - 1} \leq \frac{a}{p^a - 1} = \frac{1}{p-1} \cdot \underbrace{\frac{a}{p^{a-1} + \ldots + p + 1}}_{\leq 1}$$

Für alle $x \in K$ mit $\text{ord}_p(x) > 1/(p-1)$ gilt also:

$$\text{ord}_p\left(\frac{x^\nu}{\nu}\right) - \text{ord}_p(x) = (\nu - 1)\text{ord}_p(x) - \text{ord}_p(\nu) > (\nu - 1) \underbrace{\left(\frac{1}{p-1} - \frac{\text{ord}_p(\nu)}{\nu - 1}\right)}_{\geq 0}$$

$$\Rightarrow \boxed{v_\mathfrak{p}(\log(1+x)) = v_\mathfrak{p}(x)} \text{ falls } v_\mathfrak{p}(x) > \frac{e}{p-1}$$

Das heißt, für alle $n > e/(p-1)$ gilt:

$$\boxed{\log(U^{(n)}) \subseteq \mathfrak{p}^n}$$

Für alle $\nu > 0$ gilt außerdem nach dem Lemma 3.6:

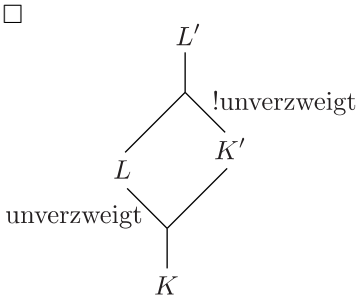
$$\text{ord}_p\left(\frac{x^\nu}{\nu!}\right) = \nu \cdot \text{ord}_p(x) - \frac{\nu - S_\nu}{p-1} = \nu\left(\text{ord}_p(x) - \frac{1}{p-1}\right) + \frac{S_\nu}{p-1}$$

Also konvergiert $\exp(x)$ $\forall$ $x \in K$ mit $\text{ord}_p(x) > 1/(p-1)$. Für $x \neq 0$ und $\nu > 1$ gilt außerdem:

$$\text{ord}_p\left(\frac{x^\nu}{\nu!}\right) - \text{ord}_p(x) = \underbrace{(\nu - 1)\text{ord}_p(x) - \frac{\nu - 1}{p-1}}_{>0} + \underbrace{\frac{S_\nu - 1}{p-1}}_{\geq 0} > 0$$

$$\boxed{\text{ord}_p(\exp(x) - 1) = \text{ord}_p(x)} \text{ für } v_\mathfrak{p}(x) > \frac{e}{p-1}$$

Das heißt, für alle $n > e/(p-1)$ gilt $\exp(\mathfrak{p}^n) \subseteq U^{(n)}$. Ferner ist $\exp(\log(1+X)) = 1+X$ und $\log(\exp(X)) = X$. □



Beweis:

Sei ohne Einschränkung L/K endlich. Daraus folgt, das l/k endlich ist (wie beim Beweis von Satz 3.2). Aufgrund der Separabilität existiert ein primitives Element $\overline{\alpha} \in l$ mit $l = k(\overline{\alpha})$. Der Vertreter $\alpha \in \mathcal{O}$ habe das Minimalpolynom $f(X) \in \mathfrak{o}[X]$. Setze $\overline{f} := f \bmod \mathfrak{p} \in k[X]$. $f(\alpha) = 0$ impliziert $\overline{f}(\overline{\alpha}) = 0$.

$[l : k] \leq \mathrm{Grad}(\overline{f}) = \mathrm{Grad}(f) = [K(\alpha) : K] \leq [L : K] = [l : k]$

Dies folgt aus der Unverzweigtheit. Damit ist insbesondere $L = K(\alpha)$ und $\overline{f}$ das Minimalpolynom von $\overline{\alpha}$. Daraus folgt $L' = LK' = K(\alpha)K' = K'(\alpha)$.

a.) Zu zeigen ist, dass L'/K' unverzweigt ist. Sei $g(X) \in \mathfrak{o}'[X]$ Minimalpolynom von α über K' und $\overline{g} := g \bmod \mathfrak{p}' \in k'[X]$, $f = g \cdot h \in \mathfrak{o}'[X]$. Hieraus folgt $\overline{f} = \overline{g} \cdot \overline{h}$ in $k'[X]$. Da $\overline{f}$ separabel ist, folgt insbesondere auch, dass $\overline{g}$ separabel ist. $\overline{g}$ ist irreduzibel in $k'[X]$. (Denn sonst wäre g reduzibel nach dem Hensel-Lemma.) Also gilt:

$[l' : k'] \leq [L' : K'] = \mathrm{Grad}(g) = \mathrm{Grad}(\overline{g}) = [k'(\overline{\alpha}) : k'] \leq [l' : k']$

Damit ist wieder alle gleich, insbesondere also $[l' : k'] = [L' : K']$. l'/k' ist separabel, also ist L'/K' unverzweigt.

b.) Sei nun L/K unverzweigt und $L \supseteq K' \supseteq K$. Hieraus folgt $l \supseteq k' \supseteq k$ und damit ist L/K' nach (a) unverzweigt. Das heißt, l/k' ist separabel und $(L : K') = (l : k')$. Auch ist L/K unverzweigt, also l/k separabel und $(L : K) = (l : k)$. Somit ist k'/k separabel und

$$[K' : K] = \frac{[L : K]}{[L : K']} = \frac{[l : k]}{[l : k']} = [k' : k]$$

Damit ist die Unverzweigtheit gezeigt. □

Korollar 4.3:

Das Kompositum zweier unverzweigter Erweiterungen von K ist selbst wieder unverzweigt (über K).

Beweis:

Ohne Einschränkung seien L/K und L'/K endlich und unverzweigt. Nach dem Satz 4.2 ist LL'/L' unverzweigt und nach Voraussetzung auch L'/K. Damit ist LL'/K unverzweigt wegen der Transitivität der Separabilität und Multiplikativität der Körpergrade. □

Definition 4.4:

Sei L/K algebraische Erweiterung und $L \supseteq T \supseteq K$, wobei T das Kompositum aller unverzweigten Teilerweiterungen ist. T heißt die „**maximale unverzweigte Teilerweiterung** von L/K. L/K heißt „**rein verzweigt**“, falls $T = K$ ist.

Satz 4.5:

Der Restklassenkörper von T ist der separable Abschluss l_{sep} von k in l/k. Die Wertegruppe von T ist gleich der von K.

Beweis:

Sei $l_0 := \mathcal{O}_T/\mathfrak{P}_T$. Es ist klar, dass die Restklassenkörpererweiterung l_0/k separabel ist. Sei $\overline{\alpha} \in l$ separabel über k. Zu zeigen ist, dass $\overline{\alpha} \in l_0$ liegt. Sei $\overline{f}(X)$ in $k[X]$ Minimalpolynom von $\overline{\alpha}$. Wähle $f \in \mathfrak{o}[X]$ normiert mit $f \bmod \mathfrak{p} = \overline{f}$. Somit ist f irreduzibel und nach dem Hensel-Lemma existiert eine Nullstelle $\alpha \in L$ mit $\alpha \in \mathcal{O}$ mit $\alpha \bmod \mathfrak{p} = \overline{\alpha}$. Hieraus folgt $[K(\alpha) : K] = [k(\overline{\alpha}) : k]$, also insbesondere ist $K(\alpha)/K$ unverzweigt und $K(\alpha) \subseteq T$ und $\overline{\alpha} \in l_0$. Restbehauptung: $w(T^\times) = v(K^\times)$. Ohne Einschränkung ist L/K endlich.

$[T : K] \geq [w(T^\times) : v(K^\times)] \cdot [l_0 : k] = [w(T^\times) : v(K^\times)] \cdot [T : K]$

Diese Abschätzung folgt für beliebiges T/K wie früher skizziert. Man wählt Vertreter $\pi_1, \ldots, \pi_e \in T^\times$ mit $w(\pi_i)$ als Vertreter verschiedener Nebenklassen in $w(T^\times)/v(K^\times)$ und $\omega_1, \ldots, \omega_f \in \mathcal{O}_T$ Vertreter einer k-Basis von l_0. Dann folgt leicht, dass die $\omega_j\pi_i$ $(j = 1, \ldots, f;\ i = 1, \ldots, e)$ linear unabhängig sind. Damit folgt die Behauptung. □

Im folgenden sei nun $\mathrm{char}(k) = p$.

Definition 4.6:

L/K heißt **zahm-verzweigt**, wenn l/k separabel ist und $p \nmid [L : T]$, das heißt der Grad jeder endlichen Teilerweiterung ist nicht durch p teilbar. T ist wie zuvor der maximal unverzweigte Zwischenkörper.

Satz 4.7:

Eine endliche Erweiterung L/K ist genau dann **zahm-verzweigt**, wenn die Erweiterung L/T eine Radikalerweiterung der Form $L = T(\sqrt[m_1]{a_1}, \ldots, \sqrt[m_r]{a_r})$ ist mit $p \nmid m_i$. In diesem Fall gilt $[L : K] = e(L/K) \cdot f(L/K)$ mit $e := e(L/K) := [\omega(L^\times) : v(K^\times)]$ der Verzweigungsordnung und dem Restklassengrad $f := f(L/K) := [l : k]$.

Beweis:

Ohne Einschränkung sei $K = T$, denn L/K ist genau dann zahm-verzweigt, wenn L/T zahm-verzweigt ist. Dann ist $[T : K] = [l : k] = f$.

- „$\Rightarrow$“: Sei $L/K(= T)$ zahm-verzweigt, also $l = k(= l_0)$ und $p \nmid [L : K]$. Vorbemerkung: Falls $e = 1$ (gleiche Wertegruppe!) ist, folgt $L = K$, denn für $\alpha \in L \setminus K$ existieren Konjugierte α_1, …, α_m und

  $$a := \mathrm{Sp}(\alpha) = \sum_{\mu=1}^{m} \alpha_\mu \in K$$

  Damit folgt $\beta := \alpha - 1/ma \in L \setminus K$ mit $\mathrm{Sp}(\beta) = 0$. Wegen $v(K^\times) = w(L^\times)$ existiert ein $b \in K^\times$ mit der Eigenschaft $v(b) = w(\beta)$, also ist $\varepsilon := \beta/b$ Einheit in $L \setminus K$ mit $\mathrm{Sp}(\varepsilon) = 0$. Aber alle Konjugierten ε_i haben alle gleiche Restklasse in $l = k$. Somit folgt $\overline{0} = \overline{\mathrm{Sp}(\varepsilon)} = m \cdot \overline{\varepsilon}$, also $m \equiv o(p)$ (Vielfaches der Charakteristik), das heißt $p|m = [K(\alpha) : K]|[L : K]$, was ein Widerspruch zur Annahme darstellt. Nun sei $w_1, \ldots, w_r \in w(L^\times)$ ein Vertretersystem von Erzeugenden von $w(L^\times)/v(K^\times)$ mit m_i als Ordnung von w_i mod $v(K^\times)$. Wegen $w(L^\times) = 1/nv(N_{L/K}(L^\times)) \subseteq 1/nv(K^\times)$ mit $n := [L : K]$ gilt $m_i|n$, also insbesondere $p \nmid m_i$. Wähle $\gamma_i \in L^\times$ mit $w(\gamma_i) = w_i$. Damit existiert ein $c_i \in K$, so dass $w(\gamma_i^{m_i}) = v(c_i)$ ist. Weiterhin gibt es also eine Einheit $\varepsilon_i \in L$ mit $\gamma_i^{m_i} = c_i \cdot \varepsilon_i$. Wegen $l = k$ findet man $b_i \in K$ mit $\varepsilon_i = b_i \cdot u_i$ mit $\overline{u}_i = \overline{1}$ in l. Die Gleichung $X^{m_i} - u_i$ hat eine Nullstelle $\beta_i \in L$ (nach dem HENSEL-Lemma). Setze $\alpha_i := \gamma_i \beta_i^{-1}$ und damit $w(\alpha_i) = w(\gamma_i) = w_i$ und $\alpha_i^{m_i} = c_i \cdot b_i =: a_i \in K$. Also ist $K(\sqrt[m_1]{a_1}, \ldots, \sqrt[m_r]{a_r}) \subseteq L$ mit gleicher Wertgruppe und gleichem Restklassenkörper. Die Restbehauptung ist nun $[L : K] \leq e$. Um dies zu zeigen, führen wir eine Induktion nach r durch.

  a.) $L_1 := K(\sqrt[m_1]{a_1})$
  Hieraus ergibt sich $w_1 \in w(L_1^\times)$. Dies liefert uns eine Ungleichungskette:

  $$e(L_1/K) = (w(L_1^\times) : v(K^\times)) \geq m_1 \geq [L_1 : K]$$

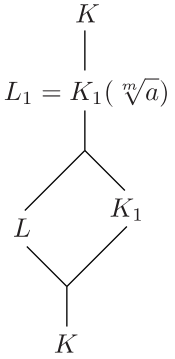
  b.) Nach Induktionsvoraussetzung gilt $e(L/L_1) \geq [L : L_1]$. Aufgrund der Multiplikativität der Körpergrade und der Wertegruppen gilt:

  $$e = e(L/L_1) \cdot e(L_1/K) \geq [L : L_1] \cdot [L_1 : K] = [L : K]$$

- „$\Leftarrow$“: Nun sei L Erweiterung der Form $L = K(\sqrt[m_1]{a_1}, \ldots, \sqrt[m_r]{a_r})$ mit $p \nmid m_i$. Zu zeigen ist, dass dann L/K zahm-verzweigt ist. Dies tun wir mit vollständiger Induktion nach r. Es genügt, den Fall $r = 1$ zu betrachten, da Induktionsanfang und Induktionsschritt analog funktioniert.

  $L = K(\sqrt[m]{a})$ mit $p \nmid m$

  Wir können K ersetzen durch $K_1 := K_{nr} :=$ maximal unverzweigte Erweiterung von K in $\overline{K}$, wobei wegen Satz 4.5 der zugehörige Restklassenkörper $k_1 = \overline{k}_s :=$ separable algebraische Hülle von k in $\overline{k}$ mit $L \cap K_1 = T$ $(= K$ nach genereller Annahme).



Ist L_1/K_1 zahm-verzweigt, so ist auch L/K zahm-verzweigt, denn aus der Separabilität l_1/k_1 folgt $l_1 = k_1$. Weiterhin gilt $p \nmid [L_1 : K_1] = [L : K] = [L : T]$. Da $l_1 \supseteq l$ ($k_1 \supseteq l$) ist l/k separabel, also L/K zahm-verzweigt. Wir können also ohne Einschränkung annehmen, dass k separabel abgeschlossen ist. Sei $\alpha := \sqrt[m]{a}$. Das Polynom $X^m - a \in K[X]$ ist ohne Einschränkung irreduzibel. Dies gilt wegen der KUMMER **Theorie**, da $\mu_m \subseteq k^\times$. Wegen dem HENSELschen Lemma gilt $\mu_m \subseteq K^\times$ und damit ist L/K zyklisch. Sei n die Ordnung von $w(\alpha)$ mod $v(K^\times)$, etwas $n \cdot w(\alpha) = v(b)$ mit $b \in K^\times$. Da $m \cdot w(\alpha) = v(a) \in v(K^\times)$ gilt $n|m$. Setze $d := m/n$. Damit gilt $w(\alpha^m) = v(b^d) = v(a)$ und $\alpha^m = \varepsilon \cdot b^d$ mit Einheit $\varepsilon \in K$. Wegen $p \nmid d$ und weil k separabel abgeschlossen ist, zerfällt $X^d - \overline{\varepsilon}$ in verschiedene Linearfaktoren, nämlich $X^d - \overline{\varepsilon} = \prod_{i=1}^{d}(X - \overline{\theta}_i)$ in $k[X]$. Nach dem HENSELschen Lemma zerfällt schon das ursprüngliche Polynom $X^d - \varepsilon$, also $X^d - \varepsilon = \prod_i (X - \theta_i)$ in $K[X]$. Das heißt, es existiert ein $\theta \in K$ mit $\theta^d = \varepsilon$ und dann gibt es ein $b \in K^\times$ mit $\alpha^m = b^d = a$.

$$X^m - a = X^m - b^d \underset{m=nd}{=} (X^n - b)\left(b^{d-1} + \ldots + X^{n(d-1)}\right)$$

Da wir von einem irreduziblen Polynom ausgegangen sind, muss einer der beiden Faktoren das triviale Polynom sein. Dies funktioniert nur für $d = 1$. Somit ist $m = n$ und $e \geq n = m = [L : K] \geq e \cdot f \geq e$. Also ist $f = 1$ und $l = k$ und nach Voraussetzung $p \nmid n = [L : T]$. □

Korollar 4.8:

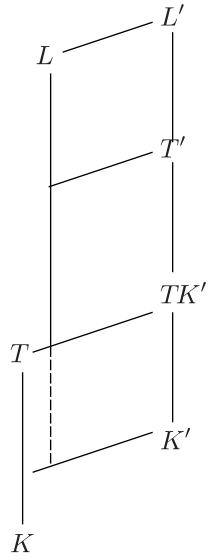
Seien L/K und K'/K algebraische Erweiterungen mit L, $K' \subseteq \overline{K}$ und $L' = LK'$. Dann gilt:

a.) Ist L/K zahm-verzweigt, so ist auch L'/K' zahm-verzweigt.

b.) Jede Teilerweiterung einer zahm-verzweigten Erweiterung ist zahm-verzweigt.

Beweis:

a.) Ohne Einschränkung ist L/K endlich.



Nach Satz 4.2 folgt $T \subseteq T'$ und da L/K zahm-verzweigt ist, nach Satz 4.7: $L = T(\sqrt[m_1]{a_1}, \ldots)$ mit $p \nmid m_i$. Daraus folgt $L' = LK' = LT' = T'(\sqrt[m_1]{a_1}, \ldots)$. Also ist L'/K' zahm-verzweigt nach Satz 4.7.

b.) Dies folgt aus (a) für speziell $L \supseteq K' \supseteq K$, dass L/K' zahm-verzweigt ist und somit auch K'/K (analog zum Beweis von Satz 4.2 (b)). □

Korollar 4.9:

Das Kompositum von zahm-verzweigten Erweiterungen ist wieder zahm-verzweigt.

Beweis:

Das resultiert analog wie 4.3 aus 4.2 aus dem Korollar 4.8.

Definition 4.10:

Sei L/K algebraische Erweiterung. Das Kompositum V/K aller zahm-verzweigten Teilerweiterungen von L/K heißt die „**maximale zahm-verzweigte**“ Teilerweiterung von L/K. Setze $w(L^\times)^{(p)} := \{w \in w(L^\times); \exists m \in \mathbb{N} : p \nmid m, m \cdot w \in v(K^\times)\}$.

Übung:

$w(L^\times)^{(p)}/v(K^\times) = \{\overline{w} \in w(L^\times)/v(K^\times); p \nmid \text{Ordnung}(\overline{w})\}$

Satz 4.11:

Die maximal zahm-verzweigte Teilerweiterung V/K von L/K hat die Wertegruppe $w(V^\times) = v(L^\times)^{(p)}$ und als Restklassenkörper den separablen Abschluss l_{sep} von k in l.

Beweis:

Ohne Einschränkung sei L/K endlich und $e(T/K) = 1$. Es gilt $K \subseteq T \subseteq V \subseteq L$ und $k \subseteq l_{sep} = l_v \subseteq l$. Die Gleichheit $l_{sep} = l_v$, da l_v/K separabel ist.

$p \nmid [V : T] = e(V/K) = |w(V^\times)/v(K)| \Rightarrow w(V^\times) \subseteq w(L^\times)^{(p)}$

„$\supseteq$“: Sei $w \in w(L^\times)^{(p)}$ wie im Beweis von Satz 4.7. Es existiert ein $\alpha \in \sqrt[m]{a} \in L$ mit $a \in K$, $p \nmid m$, $w(\alpha) = w$. Nach Satz 4.7 ist $\alpha \in V$, also $w \in w(V^\times)$. □

Definition:

L/K heißt „**rein verzweigt**“, wenn $T = K$ ist. L/K heißt „**wild verzweigt**“, wenn $V \neq L$ ist.

3.3.1 Beispiel: Einheitswurzelkörper

Satz 4.12:

Sei K beliebiger lokaler Körper und $k = \mathbb{F}_q (q = p^r)$ und $p \nmid n$. Sei $\zeta \in \overline{K}$ primitive n-te Einheitswurzel, $L := K(\zeta)$. Dann gilt:

a.) L/K ist unverzweigt vom Grad f, wobei $f := \min\{m \in \mathbb{N}; q^m \equiv 1 \bmod n\}$.

b.) $\text{Gal}(L/K)$ ist kanonisch isomorph zu $\text{Gal}(l/k) = \langle \text{Frob}_q \rangle$ mit Frob_q: $l \mapsto l$, $a \mapsto a^q$.

c.) $\mathcal{O} = \mathfrak{o}[\zeta]$.

Satz 4.13:

Sei ζ primitive p^m-te Einheitswurzel in $\overline{\mathbb{Q}}_p$. Dann gilt:

a.) $L = \mathbb{Q}_p(\zeta)$ ist rein verzweigt über $\mathbb{Q}_p$ vom Grad $\varphi(p^m)$.

b.) $\text{Gal}(L/\mathbb{Q}_p) \simeq (\mathbb{Z}/p^m\mathbb{Z})^\times$

c.) Der Bewertungsring $\mathcal{O}$ von L ist $\mathbb{Z}_p[\zeta]$.

d.) $\pi = 1 - \zeta$ ist Primelement von $\mathcal{O}$ mit Norm $N_{L/\mathbb{Q}_p}(\pi) = p$.

Beweis:

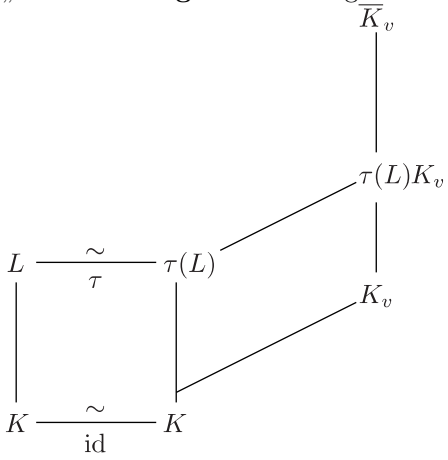
Dieser wird in der Übung diskutiert.

3.4 Fortsetzung von Bewertungen

Situation: Sei K ein beliebiger Körper mit einer Bewertung v von K (archimedisch oder nicht archimedisch). Für die archimedischen Betragsbewertungen $|\bullet|$ von K bezeichnet v **nur ein Index** zur Unterscheidung der verschiedenen Äquivalenzklassen von Beträgen $|\bullet|_v$, also keine Exponentbewegung! K_v sei die Komplettierung von K bezüglich v und $\overline{K}_v$ sei der algebraische Abschluss der Komplettierung K_v. Erinnere: Die Bewertung v hat eine natürliche Fortsetzung v auf K_v und hat daher eine eindeutige Fortsetzung auf $\overline{K}_v$. Sei nun L/K eine algebraische Erweiterung. Wähle eine K-Einbettung τ: $L \hookrightarrow \overline{K}_v$. Erhalte Bewertungsfortsetzung w von v auf L vermöge $w := \overline{v} \circ \tau$. Das heißt, für alle $x \in L$ gilt: $|x|_w = |\tau(x)|_{\overline{v}}$.

Definition:

Sei L_w die Komplettierung von L bezüglich w, falls L/K eine endliche algebraische Erweiterung ist. Sonst sei $L_w := \bigcup_i L_{i,w_i}$, wobei L_i über alle endlichen Teilerweiterungen von L/K läuft. L_w bezeichnet man als „**Lokalisierung**“ von L bezüglich w.



Auch $\tau = id$ ist möglich. Für alle $\sigma \in \mathrm{Aut}(\overline{K}_v/K_v)$ gibt es ein $\tau' = \sigma \circ \tau$ als „K-Einbettung von L zu τ über K_v konjugiert“.

3.4.1 Fortsetzungssatz (abstrakt)

Satz 5.1:

Sei L/K algebraische Körpererweiterung und v eine Bewertung von K. Dann gilt:

a.) Für alle Bewertungsfortsetzungen w existiert eine K-Einbettung $\tau\colon L \hookrightarrow \overline{K}_v$ mit $w = \overline{v} \circ \tau$.

b.) Für $w' = \overline{v} \circ \tau'$ gilt $w' = w$ genau dann, wenn τ und τ' über K_v konjugiert sind.

Beweis:

a.) Sei $w|_K = v$ mit der zugehörigen Lokalisierung L_w. $K_v \subseteq L_w$ ist nach wie vor algebraisch, also existiert eine K_v-Einbettung $\tau\colon L_w \hookrightarrow \overline{K}_v$. Aus der Eindeutigkeit von $\overline{v}$ ergibt sich $\overline{v} \circ \tau = w$. Somit ist $\tau|_L\colon L \mapsto \overline{K}_v$ eine K-Einbettung wie behauptet.

b.) „$\Leftarrow$“: Sei $\sigma \in \mathrm{Aut}(\overline{K}_v/K_v)$ mit $\tau' = \sigma \circ \tau$. $\overline{v}$ ist eindeutig bestimmte Fortsetzung von v von K_v auf $\overline{K}_v$. Auch ist $\overline{v} \circ \sigma$ Fortsetzung von v von K_v auf $\overline{K}_v$. Hieraus ergibt sich $\overline{v} = \overline{v} \circ \sigma$.

$$w = \overline{v} \circ \tau = (\overline{v} \circ \sigma) \circ \tau = \overline{v} \circ \tau' = w'$$

„$\Rightarrow$“: Seien τ und τ' Einbettungen von $L \mapsto \overline{K}_v$ mit $\overline{v} \circ \tau = \overline{v} \circ \tau'$. Setze $\sigma := \tau' \circ \tau^{-1}\colon \tau L \xrightarrow{\sim} \tau' L$. Dies ist ein K-Isomorphismus. Setze σ fort zu einem K_v-Isomorphismus, also $\sigma\colon \tau(L)K_v \xrightarrow{\sim} \tau'(L)K_v$. (Dies funktioniert; siehe Algebra!) Nun setze σ fort zu $\widetilde{\sigma} \in \mathrm{Aut}(\overline{K}_v/K_v)$. Damit gilt $\tau' = \widetilde{\sigma} \circ \tau$. □

3.4.2 Fortsetzungssatz (konkrete Fassung)

Satz 5.2:

Sei $f(X) \in K[X]$ irreduzibel und $L = K(\alpha)$ mit $f(\alpha) = 0$. Ferner sei $f(X) = \prod_{\varrho=1}^{r} f_\varrho(X)^{m_\varrho}$ in $K_v[X]$ mit $f_\varrho(X)$ irreduzibel in $K_v[X]$. Dann entsprechen die Faktoren $f_1, \ldots, f_r$ bijektiv den Fortsetzungen $w_1, \ldots, w_r$ von v auf L.

Beweis:

Die K-Einbettungen $\tau\colon L \hookrightarrow \overline{K}_v$ entsprechen den Nullstellen von f in $\overline{K}_v$: $\tau(\alpha) = \beta$. Dabei gilt: τ und τ' sind konjugiert über K_v genau dann, wenn ein $\sigma \in \mathrm{Aut}(\overline{K}_v/K_v)$ existiert mit $\tau' = \sigma \circ \tau$. Dies ist äquivalent dazu, dass ein σ existiert, so dass $\beta' = \sigma(\beta)$ ist mit $\beta' = \tau'(\alpha)$ und das ist wieder äquivalent zur Existenz eines ϱ mit $f_\varrho(\beta) = f_\varrho(\beta') = 0$. Damit ergibt sich die Behauptung nach Satz 5.1. □

Definition:

Sei L/K endlich und v bzw. w Bewertungen von K bzw. L. Schreibe: $w|v$ („teilt“), falls $w|_K = v$ ist. Betrachte den Homomorphismus (für $w|v$) φ_w: $L \otimes_K K_v \mapsto L_w$ (Tensorprodukt von Vektorräumen), $a \otimes b \mapsto \tau(a) \cdot b$ ($w = \overline{v} \circ \tau$) und definiere damit die Abbildung $\varphi = \prod_{w|v} \varphi_w$: $L \otimes_K K_v \mapsto \overline{|\times|}_{w|v} L_w$.
Erinnere: Der K-Vektorraum $L \otimes_K K_v$ ist K_v-Vektorraum vermöge

$$K_v \times L \otimes_K K_v \mapsto L \otimes_K K_v,\ (\lambda, a \otimes b) \mapsto a \otimes \lambda \cdot b$$

und sogar eine K_v-Algebra mit der Multiplikation

$$(a \otimes b) \cdot (a' \times b') := a \cdot a' \otimes b \cdot b'$$

Damit ist φ ein Homomorphismus von K_v-Algebren.

Satz 5.3:

Ist L/K separabel, so definiert φ einen Isomorphismus

$$L \times_K K_v \xrightarrow[\varphi]{\sim} \prod_{w|v} L_w$$

(Auf der rechten Seite steht das kartesische Produkt!)

Beweis:

Aus der Separabilität folgt $L = K(\alpha)$. $f \in K[X]$ sei Minimalpolynom $f = \prod_\varrho f_\varrho$ mit verschiedenen irreduziblen Faktoren f_ϱ in $K_v[X]$. (Alle m_ϱ sind $= 1$, da f separabel ist.) Nach Satz 5.2 können wir die f_ϱ indizieren durch die $w|v$: $f = \prod_{w|v} f_w$. Seien alle L_w in einem festen algebraischen Abschluss $\overline{K}_v$ eingebettet und sei $L_w = K_v(\alpha_w)$ mit $f_w(\alpha_w) = 0$. Wir erhalten ein kommutatives Diagramm:

$$\begin{array}{ccccc}
\overline{x} \in K_v[X]/(ff) & & K_v[X]/(f) & \xrightarrow[\sim]{\text{C.R.}} & \prod_{w|v} K_v[X]/(f_w) \\
\downarrow & & \sim\downarrow\theta & & \downarrow\sim \\
\alpha \circ 1 \in L & & L \times_K K_v & \xrightarrow[\varphi]{} & \prod_{w|v} L_w \\
 & & & & \overline{X} \\
 & & & & \downarrow \\
 & & & & \alpha_w
\end{array}$$

θ ist Isomorphismus, da $K[X]/(f) \xrightarrow{\sim} K(\alpha) = L$ und bleibt Isomorphismus nach Tensorieren mit K_v. Dies führt zu dem gesuchten Isomorphismus φ. □

Korollar 5.4:

Sei L/K separabel und v fest. Dann gilt

$$[L : K] = \sum_{w|v} [L_w : K_v]$$

und für alle $\alpha \in L$:

$$N_{L/K}(\alpha) = \prod_{w|v} N_{L_w/K_v}(\alpha) \text{ und entsprechend } \mathrm{Tr}_{L/K}(\alpha) = \sum_{w|v} \mathrm{Tr}_{L_w/K_v}(\alpha)$$

Beweis:

Wir gehen aus von

$$[L : K] = \dim_K L = \dim_{K_v}(L \times_K K_v) \overset{Satz 5.3}{=} \sum_{w|v} [L_w : K_v]$$

Betrachte Multiplikation mit α als K_v-Endomorphismus $\theta := \prod_w \theta_w$ von $L \otimes_v K_v \xrightarrow{\sim} \overline{|\times|}_{w|v} L_w$. Betrachte charakteristisches Polynom:

$$g_\theta = \det(\theta - t \cdot \mathrm{id}, L/K) = \det(\theta - t \cdot \mathrm{id}, L \times_K K_v/K_v) = \prod_{w|v} g_{\theta_w}$$

Vergleiche bestimmte Koeffizienten. □