Skript zur Vorlesung Zahlentheorie

Rainer Weissauer

12. September 2007

Inhaltsverzeichnis

Kapitel 1

Grundlagen

1.1 Ganze Ringerweiterungen

Sei $\varphi : R \to S$ ein Homomorphismus zwischen kommutativen Ringen mit Eins, im folgenden kurz Ringerweiterung genannt (per Definition werden Einselemente aufeinander abbildet). Wir schreiben dann $r \in S$ anstatt $\varphi(r) \in S$ für Elemente $r \in R$, obwohl φ nicht notwendigerweise injektiv sein muß.

Definition. Ein Element $s \in S$ heißt ganz über R bezüglich einer Ringerweiterung $R \to S$, wenn $r_1, .., r_n \in R$ existieren so daß s eine sogenannte GANZHEITSGLEICHUNG in S erfüllt

$$s^n + r_1 s^{n-1} + ... + r_n = 0 \, .$$

Definition. Die Ringerweiterung $R \to S$ heißt ganz, wenn jedes $s \in S$ ganz über R ist. $R \to S$ heißt endlich, wenn S als R-Modul endlich erzeugt ist.

Satz. *Sind $R \to S$, $S \to T$ endliche Ringhomomorphismen, dann ist die Zusammensetzung $R \to T$ wieder endlich.*

Beweis. Wie für Körpererweiterungen. □

Hilfssatz. *Jede endliche Ringerweiterung $R \to S$ ist ganz.*

Beweis. Seien $b_1, ..., b_n$ Erzeugende des R-Moduls S und obdA $b_1 = 1_S$. Dann gibt es $r_{ji} \in R$ mit $s \cdot b_j = \sum_{i=1}^{n} r_{ji} \cdot b_i$. Dies definiert eine Matrix $\mathbf{R} \in M_{nn}(R)$. Setzt man $\mathbf{M} = \mathbf{R} - s \cdot \mathbf{E}$ und ist $\tilde{\mathbf{M}}$ die Komplementärmatrix von $\mathbf{M} \in M_{nn}(S)$, dann gilt $\tilde{\mathbf{M}} \cdot \mathbf{M} = det(\mathbf{M}) \cdot \mathbf{E}$ (klar im Körperfall! Es genügt dies über einem Polynomring R in endlich vielen Variablen über $\mathbb{Z}$ zu beweisen, den man aber in seinen Quotientenkörper einbetten kann). Die ursprünglichen Gleichungen $\sum_i M_{ji} \cdot b_i = 0$ multipliziert mit $\tilde{M}_{kj}$ liefern daher nach Summation über j die Gleichungen $det(\mathbf{M}) \cdot b_k = 0$. Für $k = 1$ folgt wegen $b_1 = 1_S$ daraus $det(\mathbf{M}) = 0$. Dies liefert über R die Ganzheitsgleichung

$$(-1)^n det(\mathbf{M}) = s^n - spur(\mathbf{R}) s^{n-1} \pm ... + (-1)^n det(\mathbf{R}) = 0 \, .$$

Lemma. *Für $R \to S$ und $s \in S$ sind äquivalent*

a) s ist ganz über R.

b) Die von s und R in S erzeugte Teilalgebra $R[s] \subset S$ ist endlich über R.

c) $R \to S$ faktorisiert $R \to \tilde{S} \to S$, wobei $R \to \tilde{S}$ eine endliche Ringerweiterung mit $s \in \tilde{S}$ (genauer im Bild von $\tilde{S}$).

Beweis. Klar. Außer dem Hilfssatz benutzt dies nur, daß $R[s]$ als R-Modul von $1, s, s^2, ..., s^{n-1}$ erzeugt wird im Fall einer Ganzheitsgleichung vom Grad n. □

Korollar. *Sind $R \to S$ und $S \to T$ ganze Ringhomomorphismen, dann ist auch die Zusammensetzung $R \to S$ ganz.*

Beweis. Für $t \in T$ seien $s_1, ..., s_n \in S$ die Koeffizienten einer Ganzheitsgleichung. Dann gilt $t \in R[s_1, .., s_n, t]$. Da $R[s_1]$ endlich über R ist, $R[s_1, s_2] = R[s_1][s_2]$ endlich über $R[s_1]$ etc., ist am Ende $R[s_1, .., s_n, t]$ endlich über R und somit t ganz über R. Benutze Teil (c) des Lemmas. □

Ganzer Abschluß. Für eine Ringerweiterung $R \to S$ bilden die über R ganzen Elemente von S einen Teilring $Int_R(S)$ von S mit Eins, den ganzen Abschluß von R in S. [Sind s_1, s_2 ganz über R, dann sind $R[s_1]$ und $R[s_2]$ endlich über R in S. Somit ist auch $R[s_1, s_2] = R[s_1][s_2]$ endlich über R. Da $1, s_1 \cdot s_2, s_1 \pm s_2 \in R[s_1, s_2]$, sind diese Elemente wieder ganz über R wegen Teil (c) des Lemmas].

1.2 Hilbert Satz 90

Für separable endliche Körpererweiterungen K_i/K sei $L = \prod_i K_i$ eine kommutative endlich dimensionale K-Algebra. Sei $\sigma : L \to L$ Automorphismus von K-Algebren der Ordnung n mit Fixring $L^\sigma = \{x \in L \mid \sigma(x) = x\} = K$.

Satz. *Unter diesen Voraussetzungen gilt für Einheiten $x \in L^*$*

$$\prod_{i=0}^{n-1} \sigma^i(x) = 1 \iff \exists y \in L^* , \ x = y/\sigma(y) .$$

Beweis. $\Longleftarrow$ ist klar. $\Longrightarrow$. Setzt man rekursiv $x_{i+1} = x\sigma(x_i)$ mit $x_0 = 1$, gilt $x_n = 1$. Der K-Endomorphismus $f(z) = \sum_{i=0}^{n-1} x_i \sigma^i(z)$ ist nicht identisch Null (lineare Unabhängigkeit der σ^i). Sei $y = L(z) \neq 0$, dann gilt $x\sigma(y) = y$. □

Lineare Unabhängigkeit von $1, .., \sigma^{n-1}$. Durch Tensorieren mit $\overline{K}$ sind obdA alle $K_i = K = \overline{K}$ algebraisch abfgeschloßen. σ permutiert die Faktoren K_i (Idempotente oder maximale Ideale !), und zwar transitiv mit genau n Faktoren, da K der Fixring ist! Dies realisiert σ als Permutationsmatrix auf $L = K^n$ von der Ordnung n. (Siehe die Matrix auf Seite 88 für $\lambda = 1$). Also $\sum_{i=0}^{n-1} \lambda_i \sigma^i = 0 \Longleftrightarrow \lambda_i = 0 \; \forall i$, denn die zirkulare Matrix $\sum_{i=0}^{n-1} \lambda_i \sigma^i$ hat als Einträge die Zahlen λ_i (jede kommt genau n mal vor; alle Einträge der $2n-1$ Nebendiagonalen sind gleich). □

1.3 Endlich erzeugte abelsche Gruppen

Für endlich erzeugte abelsche Gruppen E gilt bekanntlich

Satz. *E ist isomorph zu einem endlichen Produkt $E = \prod_i E_i$ zyklischer Gruppen.*

Der Rang. Die Zahl r der Faktoren $E_i \cong \mathbb{Z}$ nennt man den Rang von E. Es gilt $E \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^r$. E ist endlich genau dann, wenn $r = 0$.

Charaktergruppe. Die duale Gruppe E^D von E ist die Gruppe der Homomorphismen $\eta \in E^D = Hom(E, S^1)$ von E in den komplexen Einheitskreis S^1. Die Auswertung $< \eta, x >= \eta(x)$ ist biadditiv in η und x. Da $x \in E$ auch als Charakter $\langle ., x\rangle \in (E^D)^D$ von E^D aufgefaßt werden kann, definiert $\langle ., .\rangle$ eine kanonische Abbildung $E \to (E^D)^D$.

Die Einschränkungen $\eta_i = \eta | E_i$ auf die zyklischen Faktoren E_i bestimmen einen Charakter $\eta \in E^D$. Genauer $Hom(E, S^1) \cong \prod_i Hom(E_i, S^1)$. Für zyklisches $E_i = \langle\sigma\rangle$ ist $\eta_i \in (E_i)^D$ durch den Wert $z = \eta_i(\sigma)$ des Erzeugers σ bestimmt. Ist die Ordnung n von σ endlich, gilt $z^n = 1$ wegen $\sigma^n = 1$; eine n-te Einheitswurzel $z \in \mathbb{C}$ definiert einen Charakter $\eta_i(\sigma^\nu) = z^\nu$ von E_i. Für $E_i = \mathbb{Z}$ kann $z = \eta(\sigma)$ in $S^1 \cong \mathbb{R}/\mathbb{Z}$ beliebig vorgegeben werden. Für $x_0 \neq 0$ in E gibt es daher immer ein $\eta \in E^D$ mit $\eta(x_0) \neq 1$ (Punktetrennung). Also ist $E \to (E^D)^D$ injektiv.

Endliches E. Obige Rechnung zeigt $\#(E_i)^D = n = \#E_i$, und damit $\#E^D = \prod_i \#(E_i)^D = \prod_i E_i = \#E$. Also ist $\langle ., .\rangle : E^D \times E \to S^1$ für endliches E nicht ausgeartet. Es folgt $\sum_{x \in E} \langle \eta, x\rangle = \#E \delta_{\eta 1}$ und dual

$$\sum_{\eta \in E^D} \langle \eta, x\rangle = \#E \cdot \delta_{x0} \; .$$

[Klar für $x = 0$. Für $x = x_0 \neq 0$ existiert $\eta_0(x_0) \neq 1$ (Punktetrennung). Also $\sum_\eta \langle \eta, x_0\rangle = \sum_{\eta\eta_0} \langle \eta, x\rangle = \langle \eta_0, x_0\rangle \sum_\eta \langle \eta, x\rangle$ und somit $\sum_\eta \langle \eta, x_0\rangle = 0$].

Kapitel 2

Absolute Theorie

2.1 Zahlkörper

Ganze Ringerweiterungen. Eine Ringerweiterung $R \to S$ heißt endlich, wenn S als R-Modul endlich erzeugt ist. Eine Ringerweiterung $R \to S$ heißt ganz, wenn jedes Element $s \in S$ ganz über R ist, d.h. einer Ganzheitsgleichung über R genügt. Ein Element $s \in S$ ist genau dann ganz über R, wenn der von s und R erzeugte Unterring $R[s] \subseteq S$ ein endlich erzeugter R-Modul ist, oder allgemeiner in einem Unterring $\tilde{S} \subseteq S$ liegt, der ein endlich erzeugter R-Modul ist. Daraus folgt, daß die Komposition ganzer (resp. endlicher) Ringerweiterungen wieder ganz (resp. endlich) ist. Siehe Appendix IV.

Zahlkörper. Eine endliche Körpererweiterung $K/\mathbb{Q}$ nennt man einen Zahlkörper. Zahlen $x \in K$, welche ganz über $\mathbb{Z}$ sind, heißen ganz algebraisch, und definieren einen Teilring $\mathfrak{o}_K$ in K. Beachte: Für $x, y \in \mathfrak{o}_K$ ist $\mathbb{Z}[x,y] = \tilde{S} = \mathbb{Z}[x][y]$ als Komposition ganzer endlich erzeugter Ringerweiterungen endlich erzeugt, und damit sind $x \pm y, xy \in \tilde{S}$ wieder ganz über $\mathbb{Z}$. Siehe Appendix IV.

Nenner. Für jede Zahl $x \in K$ gibt es eine natürliche Zahl $m \neq 0$ mit $mx \in \mathfrak{o}_K$. [Ist $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ ein Minimalpolynom über $\mathbb{Q}$, wähle dazu m so, daß gilt $ma_i \in \mathbb{Z}$.] Insbesondere ist daher K der Quotientenkörper von $\mathfrak{o}_K$.

Der Fall $K = \mathbb{Q}$. Ist $x = p/q \in \mathbb{Q}$ ganz über $\mathbb{Z}$, d.h. $x^n + a_1 x^{n-1} + \cdots + a_n = 0$ mit $a_i \in \mathbb{Z}$, dann gilt $x \in \mathbb{Z}$. [ObdA p und q teilerfremd. Aus $p^n = q(-a_1 p^{n-1} - \cdots - a_n q^{n-1})$ folgt $q_1 | p$ für jeden Primteiler von q. Also $q = \pm 1$].

Die Diskriminante $D_{K/\mathbb{Q}}$. Sei $[K : \mathbb{Q}] = n$ und $K = \mathbb{Q}(\alpha)$. Dann gibt es genau n verschiedene Körpereinbettungen $\sigma_i : K \to \mathbb{C}$ definiert durch $\sigma_i(\alpha) = \alpha^{(i)}$ in Termen der n komplexen Nullstellen $\alpha^{(i)}$ des Minimalpolynoms $f(X) = \prod (X - \alpha^{(i)})$ eines primitiven Elements α. Unter allen Zahlen $\omega_1, .., \omega_n$ in $\mathfrak{o}_K$ wähle solche, für die

$$D = \left| \det \begin{pmatrix} \omega_1^{(1)} & .. & \omega_n^{(1)} \\ . & . & . \\ & & \\ . & . & . \\ \omega_1^{(n)} & .. & \omega_n^{(n)} \end{pmatrix}^2 \right| \in \mathbb{Z}$$

minimal ist, aber ungleich Null. Dieses Minimum $D = D_{K/\mathbb{Q}}$ nennt man die Diskrimante der Erweiterung. Beachte: 1) Die Zahl D ist invariant unter allen Galoissubstitutionen, und liegt daher in $\mathbb{Q}$. 2) D liegt in $\mathfrak{o}_K$ (Leibnitzformel für die Determinante). Somit $D \in \mathbb{Z}$. 3) Sei α ein primitives Element der Körpererweiterung

$K/\mathbb{Q}$. Durch Multiplikation mit einem $n \in \mathbb{N}$ obdA $\alpha \in \mathfrak{o}_K$. Setzt man $\omega_j = \alpha^j$, dann ist die obige Determinante vom Vandermonde-Typ und damit nicht Null.

Der freie $\mathbb{Z}$-Modul $\mathfrak{o}_K$. Elemente $\omega_1, .., \omega_n \in \mathfrak{o}_K$, für die obiges D minimal und nicht Null ist, bilden eine $\mathbb{Z}$-Basis von $\mathfrak{o}_K$. [Beachte: Die ω_j sind linear unabhängig über $\mathbb{Q}$, bilden also ein $\mathbb{Q}$-Basis von K, da anderenfalls $D = 0$ wäre. Wäre also die Behauptung falsch, könnte man $x = \sum_j x_j\omega_j \in \mathfrak{o}_K$ finden mit $(x_1, .., x_n) \notin \mathbb{Z}^n$. ObdA kann man dann außerdem annehmen $x_1 \notin \mathbb{Z}$ (Umnummering) und $0 < x_1 < 1$ (Subtraktion einer Zahl in $\sum_j \mathbb{Z}\omega_j$). Setzt man dann $\tilde{\omega}_1 = x, \tilde{\omega}_2 = \omega_2, .., \tilde{\omega}_n = \omega_n$, dann gilt $0 < \tilde{D} = Dx_1^2 < D$ wegen

$$\begin{pmatrix} \tilde{\omega}_1^{(1)} & .. & \tilde{\omega}_n^{(1)} \\ . & . & . \\ & & \\ . & . & . \\ \tilde{\omega}_1^{(n)} & .. & \tilde{\omega}_n^{(n)} \end{pmatrix} = \begin{pmatrix} \omega_1^{(1)} & .. & \omega_n^{(1)} \\ . & . & . \\ & & \\ . & . & . \\ \omega_1^{(n)} & .. & \omega_n^{(n)} \end{pmatrix} \begin{pmatrix} x_1 & 0 & . & . & 0 \\ x_2 & 1 & . & . & 0 \\ x_3 & 0 & 1 & . & 0 \\ . & 0 & . & . & 0 \\ x_n & 0 & . & . & 1 \end{pmatrix}.$$

Widerspruch zur Minimalität von D!]

Beispiel. Für quadratfreies $D \in \mathbb{Q}^*$ und $K = \mathbb{Q}(\sqrt{D})$ ist $\mathfrak{o}_K = \mathbb{Z} + \mathbb{Z}\sqrt{D}$ mit $D_{K/\mathbb{Q}} = 4D$ für $D \equiv 2, 3 \bmod 4$, und $\mathfrak{o}_K = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{D}}{2}$ mit $D_{K/\mathbb{Q}} = D$ sonst.

Der Durchschnitt $I \cap \mathbb{Z}$. Sei I ein Ideal von $\mathfrak{o}_K$ und $0 \neq x \in I$. Dann erfüllt der Koeffizient a_0 einer Ganzheitsgleichung (von minimalem Grad) $a_0 = x(-a_1 - \cdots - x^{n-1}) \in (x) \subseteq I$. Wegen der Minimalität des Grades, und da K nullteilerfrei ist, folgt $0 \neq a_0 \in I \cap \mathbb{Z}$. [Allgemeiner: Ist $0 \neq \overline{I}$ ein Ideal in einem nullteilerfreien Ring S, und $R \hookrightarrow S$ eine ganze Ringerweiterung, dann ist $R \cap \overline{I} \neq 0$. Man zeigt leicht: Ist $\overline{I}$ Primideal von S, dann ist $R \cap \overline{I}$ Primideal in R.]

Ideale sind freie $\mathbb{Z}$-Moduln. Insbesondere also $a_0\mathfrak{o}_K \subseteq I \subseteq \mathfrak{o}_K$. Da $\mathfrak{o}_K/a_0\mathfrak{o}_K \cong (\mathbb{Z}/a_0\mathbb{Z})^n$ endlich ist, folgt: 1) I hat endlichen Index in $\mathfrak{o}_K$, 2) I ist endlich erzeugt als $\mathbb{Z}$-Modul mit $\leq (a_0)^n + n$ Erzeuger. Aus dem Hauptsatz für endlich erzeugte abelsche Gruppen folgt daher für Ideale $I \neq 0$, daß I ein freier $\mathbb{Z}$-Modul vom Rang n ist (denn wegen $I \subseteq K$ ist die Torsionsgruppe von I Null).

Primideale. Jedes Primideal $I \neq 0$ in $\mathfrak{o}_K$ ist ein maximales Ideal. [Anderenfalls sei I ein Primideal in $\mathfrak{o}_K$ und $I \subsetneq \tilde{I} \subsetneq \mathfrak{o}_K$ ein echtes Oberideal. Dann ist $0 \neq \overline{I} = \tilde{I}/I$ ein Ideal des nullteilerfreien Rings $\mathfrak{o}_K/I$, und $R = \mathbb{Z}/(\mathbb{Z} \cap I) \hookrightarrow S = \mathfrak{o}_K/I$ ist eine ganze Ringerweiterung. Der Schluß von oben zeigt $R \cap \overline{I} \neq 0$. Da $I \subseteq \mathfrak{o}_K$

ein Primideal ist, ist $\mathbb{Z} \cap I \neq 0$ ein Primideal in $\mathbb{Z}$. Das Urbild $\tilde{I} \cap \mathbb{Z}$ von $\overline{I}$ ist ein echtes Oberideal von $I \cap Z$. Da jedes nichttriviale Primideal von $\mathbb{Z}$ ein maximales Ideal ist, folgt $\mathbb{Z} \cap \tilde{I} = \mathbb{Z}$ und damit $1 \in \tilde{I}$. Widerspruch!]

2.2 Die Divisorengruppe Div_K

Idealmultiplikation. Sind I, J Ideale von $\mathfrak{o}_K$, dann ist das Produkt IJ das Ideal erzeugt von allen endlichen $\mathbb{Z}$-Linearkombinationen von Produkten $xy, x \in I, y \in J$. Sind $I = (a_1, .., a_r)$ und $J = (b_1, .., b_s)$ endlich erzeugte $\mathfrak{o}_K$-Moduln, dann gilt $IJ = (a_1b_1, a_2b_1, \cdots, a_rb_s)$. Offensichtlich gilt $(IJ)K = I(JK)$.

Teilbarkeit von Idealen. Man schreibt $I|J$, falls gilt $J \subseteq I$. Bezüglich dieser Teilerordnung gilt

$$kgV(I, J) = I \cap J \quad , \quad ggT(I, J) = I + J \; .$$

Dies sind wieder Ideale in $\mathfrak{o}_K$. Für Hauptideale $(x) = x\mathfrak{o}_K$ gilt $(x)|(y) \Longleftrightarrow (y) \subseteq (x) \Longleftrightarrow y = xz, z \in \mathfrak{o}_K \Longleftrightarrow x|y$. Zwei Hauptideale $(x) = (y)$ sind daher gleich, genau dann wenn gilt $x = yz$ mit einer Einheit $z \in \mathfrak{o}_K^*$.

Primideale. Ist P ein Primideal und gilt $P|IJ$, dann gilt $P|I$ oder $P|J$. [Andernfalls gäbe es wegen $I \nsubseteq P$ und $J \nsubseteq P$ Elemente $x \in I, x \notin P$ und $y \in J, y \notin P$. Aus $xy \in IJ \subseteq P$ folgt aber $x \in P$ oder $y \in P$, da P ein Primideal ist. Widerspruch!]

Gebrochene Ideale. Ein $\mathfrak{o}_K$-Untermodul $I \neq 0$ heißt gebrochenes Ideal in K, falls es eine Zahl $0 \neq x \in K$ gibt mit $xI = J \subseteq \mathfrak{o}_K$. Offensichtlich ist dann J ein Ideal von $\mathfrak{o}_K$ und $I = x^{-1}J$. Multipliziert man x mit einer geeigneten Zahl $n \in \mathbb{N}$, kann man obdA annehmen $x \in \mathfrak{o}_K$. Durch Multiplikation mit Elementen aus K^* übertragen sich obige Aussagen zur Multiplikation und Teilbarkeit sofort auf gebrochene Ideale.

Das inverse Ideal. Für ein gebrochenes Ideal I definieren wir den $\mathfrak{o}_K$-Modul

$$I^{-1} = \{x \in K \mid xI \subseteq \mathfrak{o}_K\} \; .$$

Für $I \subseteq \mathfrak{o}_K$ gilt $I^{-1} \supseteq \mathfrak{o}_K$. Insbesondere ist I^{-1} nicht Null, dann sogar ganz allgemein für gebrochene Ideale I. Für $0 \neq y \in I$ gilt wegen $(y) \subseteq I$ offensichtlich

$J := yI^{-1} \subseteq II^{-1} \subseteq \mathfrak{o}_K$. Also ist $I^{-1} = y^{-1}J$ ein gebrochenes Ideal. Man setzt $I^{-n} = I^{-1} \cdots I^{-1}$ (n Kopien).

Zur Teilbarkeit. Für ein Ideal $I \neq 0$ existieren endlich viele Primideale $P_1, .., P_m$ mit $I|P_1 \cdots P_m$. [Wäre die Aussage falsch, betrachte unter allen Gegenbeipielen I ein maximales. Dann ist I nicht Primideal, klar! Also existieren $x, y \in \mathfrak{o}_K$ mit $xy \in I$, aber $x \notin I$ und $y \notin I$. Also $I \subsetneq (I, x)$ und $I \subsetneq (I, y)$, und es gilt $P_1 \cdots P_m \subseteq (I, x)$ und $\tilde{P_1} \cdots \tilde{P}_{\tilde{m}} \subseteq (I, y)$ für geeignete Primideale $P_1, \cdots, P_m, \tilde{P}_1, \cdots \tilde{P}_{\tilde{m}}$ (I war maximales Gegenbeispiel). $\tilde{P}_1 \cdots \tilde{P}_{\tilde{m}} P_1 \cdots P_m \subseteq (I, y)(I, x) = I + yI + xI + xy \subseteq I$ liefert einen Widerspruch!]

Schlüssellemma. *Für ein Primideal* $0 \neq P \subseteq \mathfrak{o}_K$ *gilt* $P^{-1} \supsetneq \mathfrak{o}_K$.

Beweis. Für $0 \neq a \in P$ gilt $P|(a)|P_1 \cdots P_m$ für geeignete nichttriviale Primideale $P_1, .., P_m$. ObdA sei m minimal gewählt. Wegen $P|P_1 \cdots P_m$ gilt obdA $P|P_1$, und da P_1 maximal ist sogar $P = P_1$. Im Fall $m = 1$ folgt daher $P = (a)$ und damit $P^{-1} = (a^{-1})$. $a^{-1} \notin \mathfrak{o}_K$ ist klar, denn wäre a eine Einheit, wäre $P = (a) = \mathfrak{o}_K$. Widerspruch. Also zum Fall $m \geq 2$. Da m minimal gewählt war, gilt dann $(a) \nmid P_2 \cdots P_m$. Wähle $b \in P_2 \cdots P_m$ mit $b \notin (a)$. Dann ist $x = b/a \notin \mathfrak{o}_K$. Anderseits ist $xP \subseteq a^{-1}bP \subseteq a^{-1}P_2 \cdots P_m P = a^{-1}P_1P_2 \cdots P_m \subseteq a^{-1}(a) = \mathfrak{o}_K$. □

Folgerung. *Für jedes Primideal* $P \neq 0$ *gilt* $P^{-1}P = (1) = \mathfrak{o}_K$.

Beweis. Wegen $\mathfrak{o}_K \subseteq P^{-1}$ gilt $P \subseteq J$ für $J = P^{-1}P \subseteq \mathfrak{o}_K$. Da P prim, also maximal ist, folgt entweder $J = \mathfrak{o}_K$, was wir zeigen wollen, oder $J = P^{-1}P = P$. Den letzteren Fall kann man durch das Schlüssellemma ausschließen. Denn für ein $x \in P^{-1}, x \notin \mathfrak{o}_K$ gilt dann $xP \subseteq P$. Da $P \cong \mathbb{Z}^n \subseteq \mathbb{Q}^n = K$ ein freier $\mathbb{Z}$-Modul ist, kann man Multiplikation mit x als eine Matrix mit ganzen Koeffizienten (bezüglich der $\mathbb{Z}$-Basis von P) auffassen. Nach Cayley-Hamilton ist x dann eine Nullstelle des charakteristischen Polynoms dieser Matrix. Dies liefert eine Ganzheitsgleichung für x. Also $x \in \mathfrak{o}_K$. Ein Widerspruch! □

Folgerung. *Jedes Ideal* $I \neq (0), (1)$ *ist ein Produkt von Primidealen.*

Beweis. Wähle m minimal mit $I|P_1 \cdots P_m$. Sei $P \supseteq I$ maximal. Dann gilt wegen $P|P_1 \cdots P_m$ obdA $P = P_1$. Multiplikation mit P^{-1} gibt $(1)|P^{-1}I|P_2 \cdots P_m$. Also ist $J = P^{-1}I \subseteq \mathfrak{o}_K$ ein Ideal. Per Induktion nach m können wir außerdem bereits annehmen, daßJ ein Produkt von Primidealen ist. Durch Multiplikation mit P ist dann auch $PJ = PP^{-1}I = I$ ein Produkt von Primidealen. □

Eindeutigkeit. Aus $P_1 \cdots P_m = \tilde{P}_1 \cdots \tilde{P}_{\tilde{m}}$ folgt $m = \tilde{m}$ und $P_i = \tilde{P}_i$ für alle i (bei geeigneter Vertauschung). [Beachte $P_1 | P_1 \cdots P_m = \tilde{P}_1 \cdots \tilde{P}_{\tilde{m}}$, also obda $P_1 | \tilde{P}_1$ und damit sogar $P_1 = \tilde{P}_1$. Multiplikation mit P^{-1} und Induktion nach $max(m, \tilde{m})$ zeigt dann die Behauptung.]

Jedes gebrochene Ideal I schreibt sich obdA in der Form $I = x^{-1}J$ mit $x \in \mathfrak{o}_K$ und $J \subseteq \mathfrak{o}_K$. Zerlegt man (x) und J in ein Produkt von Primidealen, schreibt sich jedes gebrochene Ideal I als ein Produkt $I = P_1 \cdots P_1 \tilde{P}_1^{-1} \cdots \tilde{P}_{\tilde{m}}^{-1}$ von Primidealen und inversen Primidealen. Also $IJ = (1)$ für $I = P_1^{-1} \cdots P_1^{-1} \tilde{P}_1 \cdots \tilde{P}_{\tilde{m}}$. Es gilt dann übrigens $I^{-1} = J$ (mittels Induktion). Es folgt jetzt

Satz 1. *Jedes gebrochene Ideal I schreibt sich auf eindeutige Weise als ein endliches Produkt von Primidealen $\prod_{P \neq 0, prim} P^{e_P}$ für Exponenten $e_P = v_P(I) \in \mathbb{Z}$. Die Menge Div_K der gebrochenen Ideale bilden eine Gruppe unter der Multiplikation. Die Abbildung $I \mapsto (\cdots, v_P(P), \cdots)$ definiert einen Gruppenisomorphismus*

$$\boxed{Div_K \cong \bigoplus_{P \neq 0, prim} \mathbb{Z}} .$$

Der obige Isomorphismus ist zusätzlich ordnungserhaltend.

Zusatz. *Unter dem Isomorphismus $Div_K \cong \bigoplus_{P \neq 0, prim} \mathbb{Z}$ entspricht die Teilerordnung $(Div_K, |)$ der auf der direkten Summe von der Anordnung $(\mathbb{Z}, \leq)$ auf den Summanden $\mathbb{Z}$ induzierten Anordnung. Insbesondere gilt*

$$kgV(I, J) \mapsto (\cdots, max(v_P(I), v_P(J), \cdots)$$

$$ggT(I, J) \mapsto (\cdots, min(v_P(I), v_P(J), \cdots) .$$

Beweis. Dazu ist zu zeigen $\prod_P P^{\nu_P} \subseteq \prod_P P^{\mu_P} \iff \mu_P \leq \nu_P \forall P$. $\Longleftarrow$ ist trivial. Zum Beweis von $\Longrightarrow$ kann durch Multiplikation mit Primidealen obdA angenommen werden $min(\nu_P, \mu_P) = 0$. Dann benutze $P | IJ \implies P | I$ oder $P | J$ (Übungsaufgabe). □

Eine exakte Sequenz. Den Quotientengruppe $Cl(K) = Div_K / K^*$ der Gruppe aller gebrochenen Ideale modulo der Untergruppe aller gebrochenen Hauptideale

nennt man die *Klassengruppe* des Zahlkörpers K. Man erhält folgende exakte Sequenz

$$0 \to \mathfrak{o}_K^* \to K^* \to Div_K \to Cl(K) \to 0 \ .$$

Wir werden zeigen: Die Gruppe $Cl(K)$ ist endlich, und die Einheitengruppe $\mathfrak{o}_K^*$ ist endlich erzeugt als abelsche Gruppe.

Beispiel. $Cl(\mathbb{Q}) = 0$ und $\mathfrak{o}_{\mathbb{Q}}^* = \{\pm 1\}$.

2.3 Die Idealnorm $N(I)$

Wir haben gesehen, daß jedes Ideal $0 \neq I \subseteq \mathfrak{o}_K$ endlichen Index in $\mathfrak{o}_K$ besitzt. Dies definiert die Norm $N(I)$ eines solchen Ideals I als die natürliche Zahl

$$N(I) = \#(\mathfrak{o}_K/I) < \infty \ .$$

Insbesondere ist für Primideale $P \neq 0$ der Restklassenkörper (! siehe 2.1) $\kappa_P = \mathfrak{o}_K/P$ ein endlicher Körper mit $N(P)$ Elemente.

Lemma. *Für teilerfremde Ideale $I \neq 0$ und $J \neq 0$ in $\mathfrak{o}_K$ gilt $N(IJ) = N(I)N(J)$.*

Dies folgt unmittelbar aus dem folgenden Satz

Chinesischer Restsatz. *Für Ideale $I, J \subseteq \mathfrak{o}_K$ mit $ggT(I, J) = (1)$ gilt*

$$\boxed{\mathfrak{o}_K/IJ \cong \mathfrak{o}_K/I \oplus \mathfrak{o}_K/J} \ .$$

Beweis. Die natürliche $\mathfrak{o}_K$-lineare Abbildung $\mathfrak{o}_K \to \mathfrak{o}_K/I \oplus \mathfrak{o}_K/J$, definiert durch $x \mapsto (x \ mod \ I, x \ mod \ J)$, ist surjektiv. Dazu genügt, daß das Bild die Erzeuger $(1,0) = (1 \ mod \ I, 0)$ und $(0,1) = (0, 1 \ mod \ J)$ enthält. Wegen $ggT(I, J) = I + J = (1)$ gibt es $i \in I, j \in J$ mit $i + j = 1$. Das Bild von i ist $(i \ mod \ I, i \ mod \ J) = (0, i + j \ mod \ J) = (0, 1)$. Das Bild von j ist analog $(1, 0)$.

Der Kern der Abbildung besteht aus allen $x \in I \cap J$. Beachte $IJ \subseteq I \cap J$. Es gilt sogar Gleichheit, denn für $x \in I \cap J$ gilt $x = xi + xj \in JI + IJ \subseteq IJ$. □

Lemma. *Für ein Primideal $P \neq 0$ gilt $N(P^n) = N(P)^n$ für alle $n \geq 0$.*

Beweis. Wähle $x \in P^{n-1} \setminus P^n$. Dann ist $(x) \subseteq P^{n-1}$, also $(x) = P^m I$ mit $ggT(P, I) = (1)$ und $m \geq n-1$. Wäre $m \geq n$, dann folgt wegen $x \in P^m I \subseteq P^n$ ein Widerspruch. Also $(x) = P^{n-1}I$. Dies ist ein zyklischer $\mathfrak{o}_K$-Modul erzeugt von x. Also ist auch der Quotient $M = P^{n-1}I/P^nI \neq 0$ ein zyklischer $\mathfrak{o}_K$-Modul. Wegen $P \cdot M \subseteq (P \cdot P^{n-1})/P^n = 0$ ist M sogar ein zyklischer $\kappa_P = \mathfrak{o}_K/P$-Modul (also ein κ_P- Vektorraum, da P maximal ist), also ein eindimensionaler κ_P-Vektorraum. Es folgt $dim_{\kappa_P}(M) = 1$ oder $M \cong \mathfrak{o}_K/P$. Aus der exakten Sequenz

$$0 \to M = P^{n-1}I/P^nI \to \mathfrak{o}_K/P^nI \to \mathfrak{o}_K/P^{n-1}I \to 0$$

folgt daher $N(P^nI) = N(P^{n-1}I)\#M$ mit $\#M = N(P)$. Aus dem letzten Lemma folgt dann $N(P^n)N(I) = N(P^{n-1})N(I)N(P)$. Kürzt man $N(I)$, folgt sofort (Induktion nach n) die Behauptung. □

Die Zetafunktion. Die beiden letzten Lemmata zeigen $N(\prod_P P^{e_P}) = \prod_P N(P)^{e_P}$, und damit

$$N(IJ) = N(I)N(J)$$

für alle nichttrivialen Ideale $I, J \subseteq \mathfrak{o}_K$. Dies zeigt - Konvergenzfragen ignorierend - die schöne Formel

$$\boxed{\zeta(K, s) := \sum_{0 \neq I \subseteq \mathfrak{o}_K, I \ Ideal} N(I)^{-s} \ = \ \prod_{0 \neq P \ prim} (1 - N(P)^{-s})^{-1}} \ .$$

Diese Formel benutzt die Existenz und Eindeutigkeit der Zerlegung in Primideale und die Multiplikativität der Norm.

Fortsetzung der Norm auf Div_K. Man kann jetzt die Norm fortsetzen zu einem Gruppenhomomorphismus

$$N : \ Div_K \to (\mathbb{Q}^*_{>0}, \cdot) \ .$$

Für ein gebrochenes Ideal $I = I_1^{-1}I_2$ mit $I_1, I_2 \subseteq \mathfrak{o}_K$ setzt man einfach $N(I) = N(I_1)^{-1}N(I_2)$. [Dies ist wohldefiniert, denn aus $I = I_1^{-1}I_2 = I_3^{-1}I_4$ folgt $I_2I_4 = I_1I_3$ und damit $N(I_2)N(I_4) = N(I_2I_4) = N(I_1I_3) = N(I_1)N(I_3)$. Also $N(I_1)^{-1}N(I_2) = N(I_3)^{-1}N(I_4)$.]

Lemma. *Für* $0 \neq x \in K^*$ *gilt* $N((x)) = |N_{K/\mathbb{Q}}(x)|$ *für* $N_{K/\mathbb{Q}}(x) = \prod_{i=1}^n x^{(i)}$.

Beweis. ObdA $x \in \mathfrak{o}_K$ und $x : \mathfrak{o}_K \cong \mathbb{Z}^n \to \mathfrak{o}_K \cong \mathbb{Z}^n$ ist eine ganzzahlige Matrix. Nach Elementarteilertheorie[1] ist die Anzahl $\#(\mathfrak{o}_K/x\mathfrak{o}_K) = |det(x)|$. Die Determinante ist der nullte Koeffizient des charakteristischen Polynoms, also das Produkt $N_{K/\mathbb{Q}}(x)$ der Nullstellen $x^{(i)}$ (Cayley-Hamilton). □

Zerlegung von Primzahlen. Für $P \neq 0$ prim und das Primideal $p\mathbb{Z} = \mathbb{Z} \cap P$ in $\mathbb{Z}$ gilt $(p) = p\mathfrak{o}_K \subseteq P$, oder $P|(p)$. Die Primideale P über $p\mathbb{Z}$ entsprechen daher den Primteilern P_i in der Faktorisierung $(p) = \prod_i P_i^{e_i}$ des Hauptideals mit $e_i > 0$. Wegen $N(p) = p^n$ und $p^n = \prod_i N(P_i)^{e_i}$ gilt daher $n = \sum_i e_i f_i$, falls $f_i = \#\kappa_{P_i}$. Eine rationale Primzahl p zerfällt also in $\mathfrak{o}_K$ in ein Produkt von höchstens n Primidealen.

2.4 Bewertungen von K

Bewertungen. Für $x \in K^*$ und ein Primideal P bezeichne $v_P(x) = v_P((x))$ die Vielfachheit des Primideals P in der Primfaktorzerlegung des Hauptideals (x). Setzt man formal noch $v_P(0) = +\infty$, dann gilt

1. $v_P(x) \in \mathbb{Z} \cup +\infty$.
2. $v_P(xy) = v_P(x) + v_P(y)$
3. $v_P(x + y) \geq \min(v_P(x), v_P(y))$.

Zum Beweis kann man obdA annehmen $x, y \neq 0$. Dann ist 1. und 2. klar. Beachte, 3. folgt aus $(x + y) \subseteq (x) + (y) = ggT((x), (y))$.

P-adische Norm. Setzt man

$$|x|_P \;=\; N(P)^{-v_P(x)} \,,$$

dann ist $|.|_P$ eine Norm

1. $|x|_P \in \mathbb{R}_{\geq 0}$ und $|x|_P = 0 \Longleftrightarrow x = 0$.

[1] Ein anderes Argument: Sei $n = [K : \mathbb{Q}]$ und $K/\mathbb{Q}$ galoissch. Das Produkt $a = x^{(1)} \cdots x^{(n)} = N_{K/\mathbb{Q}}(x)$ liegt in $\mathbb{Q}^*$. Es gilt $N((a)) = N((x^{(1)})) \cdots N((x^{(n)})) = N((x))^n$. Anderseits $N((a)) = \#(\mathfrak{o}_K/a\mathfrak{o}_K) = \#(\mathbb{Z}/a\mathbb{Z})^n = |a|^n$. Durch Ziehen der n-ten Wurzel folgt die Behauptung! Wir werden später sehen, daß man den allgemeinen Fall auf den Galoisschen zurückführen kann.

2. $|xy|_P = |x|_P|y|_P$

3. $|x+y|_P \leq \max(|x|_P, |y|_P) \leq |x|_P + |y|_P$ (scharfe Dreiecksungleichung).

Somit definiert $d(x,y) = |x-y|_P$ eine Metrik auf K, die sogenannte P-adische Metrik auf K. $|-1|_P = 1$ (Multiplikativität) und die Dreiecksungleichung zeigen

$$\big||x|_P - |y|_P\big|_{\mathbb{R}} \leq |x-y|_P \ .$$

Approximationssatz. Gegeben seien Zahlen $x_1, .., x_r \in K$ und natürliche Zahlen $n_1, .., n_r \in \mathbb{N}$ und r paarweise verschiedene Primideale $P_1, .., P_r$ in $\mathfrak{o}_K$. Dann gibt es ein $x \in K$ mit

- $v_P(x - x_\nu) \geq n_\nu$ für $\nu = 1, \cdots, r$
- $v_P(x) \geq 0$ für alle Primideale $P \neq P_1, \cdots, P_r$

Beweis. Durch Multiplikation $x \mapsto tx$ und $x_\nu \mapsto tx_\nu$ und $n_\nu \mapsto n_\nu + v_{P_\nu}(t)$ kann obdA angenommen werden die x_ν seien alle ganz (eventuell vergrößert sich dabei r). Sind alle $x_\nu \in \mathfrak{o}_K$, folgt die Aussage aus dem chinesischen Restsatz

$$\mathfrak{o}_K \twoheadrightarrow \bigoplus_{\nu=1}^{r} \mathfrak{o}_K/P_\nu^{n_\nu} \ .$$

Äquivalent. $\forall \varepsilon > 0 \exists x \in K$ mit $|x - x_\nu|_P < \varepsilon$ für $P = P_1, .., P_r$ und $|x|_P \leq 1$ für alle $P \neq P_1, .., P_r$. Beachte außerdem $|x|_P \leq 1$ für alle P beziehungsweise $v_P(x) \geq 0$ für alle P ist gleichbedeutend mit $(1)|(x)$ oder $x \in \mathfrak{o}_K$.

2.5 Komplettierungen von K

Cauchyfolgen. In dem Ring $\mathcal{C}$ aller Cauchyfolgen in K (bzgl. der P-adischen Metrik) ist die Menge $\mathcal{N} \subseteq \mathcal{C}$ aller Nullfolgen ein Ideal.

Der Betrag einer Cauchyfolge. Für eine Folge $\xi = (x_n) \in \mathcal{C}$ bilden wegen $d(|x|_P, |y|_P) \leq |x-y|_P$ die Werte $|x_n|_P$ eine reelle Cauchyfolge. Ihr Grenzwert sei $|\xi|_P := \lim |x_n|_P$. Offensichtlich gelten für $|\xi|_P$ fast alle obigen Eigenschaften einer Norm mit einer Ausnahme: $|\xi|_P = 0 \Longleftrightarrow \xi$ ist eine Nullfolge. Dies definiert

aber eine Norm auf dem Quotientenring $K_P = \mathcal{C}/\mathcal{N}$. Die Normabbildung $|.|_P$ ist eine stetige Funktion auf K_P.

Körpereigenschaft. Der Quotientenring $K_P = \mathcal{C}/\mathcal{N}$ ist ein Körper. [Beweis: Für $\xi \notin \mathcal{N}$ gilt $|x_n|_P \to |\xi|_P \neq 0$. Daher sind fast alle $x_n \neq 0$. Also kann man $\xi = (x_n)$ so um eine Nullfolge abändern, so daß die komponentenweise inverse Folge $\xi^{-1} = (x_n^{-1})$ existiert. Wegen $|x_n^{-1} - x_m^{-1}|_P \leq |x_n|_P |x_m|_P |x_n - x_m|_P$ ist ξ^{-1} wieder eine Cauchyfolge, da $|x_n|_P$ beschränkt ist. Es gilt $\xi \cdot \xi^{-1} = 1$.]

Dichtigkeit. Die konstanten Folgen definieren eine natürliche Körpereinbettung $K \hookrightarrow K_P$. Obige Norm auf K_P ist eine Fortsetzung der Norm von K. K liegt dicht in K_P bezüglich der P-adischen Metrik auf K_P. [Für eine Cauchyfolge $\xi = (x_n)$ gilt $|x_n - x_m|_P < \varepsilon$ für alle $n, m \geq N(\varepsilon)$. Also $|\xi - x_m|_P = \lim_n |x_n - x_m|_P < \varepsilon$ für $m \geq N(\varepsilon)$. Also konvergiert die Folge $x_n \in K$ in K_P gegen ξ].

Vollständigkeit. Mit einem Diagonalschluß für Doppelreihen zeigt man, daß K_P bezüglich seiner P-adischen Metrik Cauchy-vollständig ist. [Sei (ξ_m) in K_P eine Cauchyfolge, obdA (durch Übergang zu einer Teilfolge) mit $|\xi_m - \xi_n| \leq 2^{-min(n,m)}$. Die Cauchyfolgen $\xi_m = (x_{mn})$ mögen obdA dieselbe Eigenschaft haben. Dann gilt $|x_{mn} - x_{nn}|_P \leq \lim_k |x_{mn} - x_{mk}|_P + |x_{mk} - x_{nk}|_P + |x_{nk} - x_{nn}|_P \leq 2^{-n} + 2^{-min(m,n)} + 2^{-n}$. Somit ist $\xi = (x_{nn})$ eine Cauchyfolge. Bildet man den Limes $n \to \infty$ folgt $|\xi_m - \xi|_P \leq 2^{-m}$. Also konvergiert ξ_m gegen $\xi \in K_P$.]

Man nennt den Körper $K_P := \mathcal{C}/\mathcal{N}$ die *P-adische Komplettierung von K*.

Bemerkung. Die Konstruktion ist analog zur Konstruktion von $\mathbb{R}$ als Komplettierung von $\mathbb{Q}$ bezüglich des üblichen reellen Absolutbetrags $|.|_{\mathbb{R}}$.

P-adisch ganze Zahlen. $\mathfrak{o}_P = \{x \in K_P \mid |x|_P \leq 1\}$ definiert einen Ring. Daß $\mathfrak{o}_P$ unter Addition abgeschlossen ist, benutzt die scharfe Dreiecksungleichung! Wegen der Multiplikativität der Norm ist $\mathfrak{o}_P^* = \{x \in K \mid |x|_P = 1\}$ die Einheitengruppe. Die Norm $|.|_P$ nimmt genau die Werte $N(P)^{\mathbb{Z}} \cup \{0\}$ an. Für ein beliebiges Element $\pi \in K_P$ mit $|\pi|_P = N(P)^{-1} < 1$ gilt daher

$$K_P^* \;\cong\; \pi^{\mathbb{Z}} \times \mathfrak{o}_P^* \,.$$

Der Ring $\mathfrak{o}_P$ ist ein *Hauptidealring*, und jedes nichttriviale Ideal hat die Gestalt $\pi^n \mathfrak{o}_P$ für eine natürliche Zahl n, und $(\pi) = \pi \cdot \mathfrak{o}_P$ ist das eindeutig bestimmte maximale Ideal. Der Quotientenkörper von $\mathfrak{o}_P$ ist K_P.

Der Restklassenkörper. Die natürliche Abbildung $\mathfrak{o}_K \to \mathfrak{o}_P/(\pi)$ induziert einen Isomorphismus

$$\kappa_P = \mathfrak{o}_K/P \cong \mathfrak{o}_P/(\pi) \ .$$

[Offensichtlich ist $\mathfrak{o}_K \cap (\pi)$ die Menge aller $x \in \mathfrak{o}_K$ mit $|x|_P < 1 \Longleftrightarrow v_P(x) > 0$ gleich dem Ideal $P = \{x \in \mathfrak{o}_K \mid P|(x)\}$. Die induzierte Abbildung $\mathfrak{o}_K/P \to \mathfrak{o}_P/(\pi)$ ist daher injektiv. Zur Surjektivität. Sei $\xi \in \mathfrak{o}_P$. Aus der Dichtigkeit von K in K_P folgt $\forall\, 0 < \varepsilon < 1\ \exists\, x \in K |\xi - x|_P < \varepsilon$. Aus $|\xi|_P \leq 1$ folgt $|x|_P \leq 1$. Aus dem Approximationssatz folgt $\exists\, y \in K\ |y - x|_P < \varepsilon$ und $|y|_{P'} \leq 1 \forall P' \neq P$. Beachte $|y|_P \leq \max(|x|_P, |y - x|_P) \leq 1$. Also $y \in \mathfrak{o}_K$ mit $|\xi - y|_P < \varepsilon < 1$. Also $\xi - y \in (\pi)$, und ξ und y haben dasselbe Bild in $\mathfrak{o}_P$ modulo (π).]

Analogon von Heine-Borel. Der metrische Raum K_P ist lokalkompakt. Eine Teilmenge ist kompakt genau dann wenn sie beschränkt und abgeschlossen ist. Insbesondere sind $\mathfrak{o}_P$ und die Ideale (π^n) kompakte Teilmengen. Analog ist $\mathfrak{o}_P^* = \{x \in K \mid |x|_P \leq 1\}$ kompakt in $K_P^* = K_P \setminus 0$. [Zum Beweis. Ein metrischer Raum ist kompakt genau dann, wenn er folgenkompakt ist. Wie beim klassischen Satz von Heine-Borel genügt es dann zu zeigen, daß die abgeschlossenen Quader $Q = \{x \in K \mid |x|_P \leq C\}$ folgenkompakt sind. ObdA $C = 1$ und $Q = \mathfrak{o}_P$. Der Schluß benutzt wie im reellen Fall 'Intervallschachtelung'. Wir teilen jetzt aber Q nicht zwei Teile sondern in $N(P)$ Teilquader. Seien $r_i \in R$ endlich viele Repräsentanten eines Repräsentantensystems $R \subseteq \mathfrak{o}_K$ des Restklassenkörpers κ_P. Dann gilt $Q = \biguplus_{i=1}^{|R|}(r_i + \pi \cdot Q)$. Für eine Folge $x_n \in Q$ kann man daher immer ein i finden, so daß unendlich viele Folgenglieder in $r_i + \pi \cdot Q$ liegen. Durch Iteration erhält man wie im Reellen eine Teilfolge, welche eine Cauchyfolge ist, also in Q konvergiert.]

Bemerkung. Die Beweismethode des letzten Abschnitts liefert iterativ $Q = R + \pi \cdot R + \cdots \pi^{\nu-1} \cdot R$ modulo $(\pi^\nu)Q$. Es folgt: 1) $\mathfrak{o}_K/P^\nu \cong \mathfrak{o}_P/(\pi^\nu)$. 2) Man kann jede P-adisch ganze Zahl in eine konvergente Potenzreihe $\sum_{i=0}^{\infty} r_i \pi^i$ mit Koeffizienten $r_i \in R$ entwickeln.

Der Satz von Heine-Borel beruht damit letztlich auf der Tatsache, daß ein projektiver Limes (siehe Appendix III) von endlichen Mengen kompakt ist (ein Spezialfall des Satzes von Tychonoff). In der Tat gilt

$$\mathfrak{o}_P \ = \ \lim_{\nu} \mathfrak{o}_P/(\pi^\nu) = \ \lim_{\nu} \mathfrak{o}_K/P^\nu \ .$$

2.6 Adele

Sei $[K : \mathbb{Q}] = n$ und $K = \mathbb{Q}(\alpha)$, und seien $\sigma_i : K \to \mathbb{C}$ die n verschiedenen Körpereinbettungen $\sigma_i(\alpha) = \alpha^{(i)}$ definiert durch die n komplexen Nullstellen $\alpha^{(i)}$ des Minimalpolynoms $f(X) = \prod(X - \alpha^{(i)})$ eines primitiven Elements α. Jede der Einbettungen $\sigma = \sigma_i$ definiert einen Betrag $|x|_\sigma := |\sigma(x)|_{\mathbb{C}}$ auf K.

Archimedische Stellen. Eine der Einbettungen σ heißt reell, wenn gilt $\sigma(K) \subseteq \mathbb{R}$, ansonsten heißt die Einbettung komplex. Ist r_1 die Anzahl der reellen Einbettungen, und r_2 die Anzahl der komplexen Einbettungen, und es gilt offensichtlich $n = r_1 + 2r_2$. Ist σ reell, setzen wir $K_\sigma = \mathbb{R}$. Ansonsten setzen wir $K_\sigma = \mathbb{C}$. Im letzteren Fall ist mit σ auch $\overline{\sigma} := \overline{(.)} \circ \sigma$ eine komplexe Einbettung mit demselben Betrag $|x|_\sigma = |x|_{\overline{\sigma}}$. Für jede komplexe Einbettung wählen wir einen der zwei Repräsentanten und erhalten auf diese Weise $r_1 + r_2$ archimedische Beträge $|x|_v$ auf K. Wir schreiben für diese $v|\infty$. Es gilt

$$\mathbb{R} \otimes_{\mathbb{Q}} K = \mathbb{R}[X]/(f(X)) = \prod_{v|\infty} K_v =: \mathbb{A}_\infty$$

(das Produkt läuft über die $r_1 + r_2$ archimedischen Stellen v von K).

Adele. Im kartesischen Produkt $\prod_{v|\infty} K_v \times \prod_P K_P = \prod_v K_v$ (v durchläuft alle sogenannten Stellen von K, d.h. P durchläuft die Primideale $P \neq 0$ von $\mathfrak{o}_K$, und die $r_1 + r_2$ archimedischen Beträge $|.|_v$ für $v|\infty$) betrachten wir Quader

$$Q_C = \prod_v Q_v \quad , \quad Q_v = \{x \in K_v \mid |x|_v \leq C_v\} \, .$$

Hierbei sei $C = (C_v)_v$ für reelle Zahlen $C_v > 0$, und fast alle C_v seien gleich 1.

Wir definieren den Adelring $\mathbb{A}_K$ (als *eingeschränktes* kartesisches Produkt)

$$\mathbb{A}_K = \prod_{v|\infty} K_v \times \prod_P{}' K_P \; := \bigcup_C Q_C$$

als Teilring des kartesischen Produktes $\prod_v K_v$. Es gilt also $\mathbb{A}_K = \mathbb{A}_\infty \times \{(x_P) \mid x_P \in K_P, \text{ fast alle } x_P \in \mathfrak{o}_P\}$. Speziell $\mathbb{A} = \mathbb{A}_{\mathbb{Q}} = \mathbb{R} \times \prod_p{}' \mathbb{Q}_p$.

Restringierte Produkttopologie. Seien G_v lokalkompakte abelsche Gruppe, und seien für fast alle v offene und kompakte Untergruppen $H_v \subseteq G_v$ gegeben. Das

eingeschränkte Produkt $\prod_v' G_v = \prod_v'(G_v : H_v)$ besteht aus allen $(x_v) \in \prod_v G_v$, für die fast alle x_v in H_v liegen. Man nennt eine Teilmenge $U \subseteq \prod_v' G_v$ offen, wenn sie zu jedem Punkt auch eine Teilmenge der Gestalt $\prod_{v\in S} U_v \prod_{v\notin S} H_v$ enthält für S endlich und U_v offen in G_v für alle $v \in S$. Die Produkte $\prod_{v\notin S} H_v$ sind kompakt nach dem Satz von Tychonoff!

Adeletopologie. Wir setzen $H_v = \mathfrak{o}_v$ für alle nichtarchimedischen Stellen v von K. Beachte $\mathfrak{o}_P$ ist offen und kompakt in K_P. Wir versehen auf diese Weise $\mathbb{A}_K = \prod_v' K_v$ mit der eingeschränkten Produkttopologie der von den Normen induzierten Topologien auf den Komplettierungen K_v. Addition und Multiplikation auf $\mathbb{A}_K$ sind dann stetige Abbildungen.

Quader. Alle Quader Q_C sind kompakte Teilmengen von $\mathbb{A}_K$. [Die auf einem Quader $Q_C = \prod_v Q_v$ induzierte Teilraumtopologie ist gerade die Produkttopologie von $Q = \prod_v Q_v$. Die Quader $Q_v \subseteq K_v$ sind kompakt (Heine-Borel). Also ist Q_C kompakt nach dem Satz von Tychonoff (Produkte von Kompakta sind kompakt)]. Als Vereinigung der Quader Q_C ist daher $\mathbb{A}_K$ *lokalkompakt*.

Lemma. *$K \subseteq \mathbb{A}_K$ ist diskrete Untergruppe mit kompaktem Quotienten $K\backslash\mathbb{A}_K$.*

Beweis. *Diskretheit*. Der Körper K ist durch $x \mapsto (x)_v$ diagonal in den Ring $\mathbb{A}_K$ eingebettet. Nach 2.4 ist der Durchschnitt von K mit der offenen Teilmenge $V = \mathbb{A}_\infty \times \prod_P \mathfrak{o}_P \subseteq \mathbb{A}_K$ gerade $\mathfrak{o}_K = K \cap V$. Projektion auf den ersten Faktor $\mathbb{A}_\infty = \prod_{v|\infty} K_v = \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \cong \mathbb{R}^{r_1+2r_2} \cong \mathbb{R}^{[K:\mathbb{Q}]}$ von V definiert damit eine Inklusion in den Euklidschen $\mathbb{R}$-Vektorraum

$$\mathfrak{o}_K \hookrightarrow \mathbb{A}_\infty \cong \mathbb{R}^{[K:\mathbb{Q}]} .$$

Wie bereits in 2.1 gezeigt, ist das Bild von $\mathfrak{o}_K = \mathbb{Z}\omega_1 + \cdots \mathbb{Z}\omega_n$ ein *Gitter* in $\mathbb{A}_\infty \cong \mathbb{R}^n$ aufgespannt von $\mathbb{R}$-linear unabhängigen Vektoren ω_i (wegen $D_{K/\mathbb{Q}} \neq 0$). Also findet man eine offene Umgebung $U_\infty \subseteq \mathbb{A}_\infty$ von Null mit $\mathfrak{o}_K \cap U_\infty = \{0\}$. Es folgt $K \cap (U_\infty \times \prod_P \mathfrak{o}_P = \{0\}$. Somit ist K eine diskrete Untergruppe von $\mathbb{A}_K$, insbesondere also auch abgeschlossen.

Kokompaktheit. Wir versehen $K\backslash\mathbb{A}_K$ mit der Quotiententopologie. Insbesondere ist dann $\mathbb{A}_K \to K\backslash\mathbb{A}_K$ stetig. Es genügt daher zu zeigen, daß es einen Quader $Q_\infty \subseteq \mathbb{A}_\infty$ gibt so, daß das Kompaktum $Q = Q_\infty \times \prod_P \mathfrak{o}_P$ sich surjektiv auf den Quotienten $\mathbb{A}_K/K$ abbildet.

Konstruktion von Q_∞. Wegen dem Approximationssatz 2.4 gilt $\mathbb{A}_K = K + V$ für $V = \mathbb{A}_\infty \times \prod_P \mathfrak{o}_P$. Dann ist $K\backslash\mathbb{A}_K = V/(V \cap K) = (\mathbb{A}_\infty \times \prod_P \mathfrak{o}_P)/\mathfrak{o}_K$ und $\mathbb{A}_\infty = Q_\infty + \mathfrak{o}_K$ für einen genügend großen Quader in $\mathbb{A}_\infty$. □

Bemerkung. Letztlich zeigt der obige Beweis die Existenz eines Isomorphismus

$$\left(\mathfrak{o}_K\backslash\mathbb{A}_\infty\right) \times \prod_P \mathfrak{o}_P \xrightarrow{\sim} K\backslash\mathbb{A}_K \,.$$

Für die Gruppenstruktur ist dies bereits klar. Es stimmt aber auch in Bezug auf die natürlichen Topologien auf beiden Seiten, welche beide Seiten zu kompakten Gruppen macht. [Benutze nun: Ein bijektiver stetiger Homomorphismus $A \to B$ zwischen kompakten topologischen Gruppen, mit separiertem B, ist ein Homöomorphismus; denn man zeigt dann leicht, daß das Bild einer abgeschlossenen Menge in A abgeschlossen in B ist].

2.7 Haarmaß

Jede lokalkompakte abelsche Gruppe G besitzt ein translationsinvariantes Maß dx, d.h. ein positives $\mathbb{R}$-lineares Funktional auf $C_c(G, \mathbb{R})$ mit

$$\int_G f(x + x_0)dx = \int_G f(x)dx \,.$$

Modulus. Ein solches *Haarmaß* dx ist eindeutig bestimmt bis auf eine Konstante. Für jeden stetigen Automorphismus $\varphi : G \to G$ gibt es daher einen Modulus $\|\varphi\|$ in $\mathbb{R}_{>0}$ mit $vol(\varphi(U)) = \|\varphi\| vol(U)$ für alle $U \subseteq G$ offen.

Beispiele. Wir benötigen die Existenz des Modulus und des Haarmaßes nur in den folgenden Situationen, wo die Existenz evident ist

1. G diskret, dx diskret und $\|\varphi\| = 1$.
2. Für kompaktes G sei angenommen dx existiert und sei eindeutig. Dann ist $\|\varphi\| = 1$ (denn $\|.\|$ ist ein Homomorphismus von G nach $\mathbb{R}_{>0}$).
3. $G = \mathbb{R}$ und dx Lebesguemaß und $\|\varphi\| = |y|_\mathbb{R}$ für $\varphi(x) = yx$, $y \in \mathbb{R}^*$.
4. $G = \mathbb{C}$ und $\varphi(x) = yx, y \in \mathbb{C}^*$. Dann ist $\|\varphi\| = |y|^2_\mathbb{C}$.

5. $G = K_P$, $\varphi(x) = yx$ für $y \in K_P^*$. Dann[2] ist $\|\varphi\| = |y|_P$.

6. $G = \mathbb{A}_K$ und $dx = \prod_v dx_v$. Dann ist für $\varphi(x) = yx$ mit $y \in \mathbb{A}_K^*$ und $y = (y_v), y \in K_v$ der Modulus $\|\varphi\| = \prod_v \|\varphi_v\|$.

Für die Multiplikation $\varphi(x) = yx$ in den Fällen 3.-6. schreiben wir auch $\|y\|$ anstelle von $\|\varphi\|$. Offensichtlich gilt $\|y_1 y_2\| = \|y_1\|\|y_2\|$.

Zum Fall 5. $\|y\| = 1$ für $y \in \mathfrak{o}_P^*$ wegen $\|y\| vol(\mathfrak{o}_P) = vol(y\mathfrak{o}_P) = vol(\mathfrak{o}_P)$. Für $y = \pi$ gilt $\|\pi\| vol(\mathfrak{o}_P) = vol(\pi\mathfrak{o}_P) = N(P) vol(\mathfrak{o}_P)$, denn $\mathfrak{o}_P$ ist die disjunkte Vereinung von $N(P)$ Translaten von $\pi\mathfrak{o}_P$. Also $\|\pi\| = N(P)^{-1}$. Damit allgemein $\|y\| = N(P)^{-v_P(y)} = |y|_P$. Wir werden vorerst nur Treppenfunktionen integrieren, insofern genügt uns als Definition $\int_{K_P} 1_{a+(\pi)^n}(x)dx := |\pi^n|_P vol(\mathfrak{o}_P) = |\pi^n|_P$. Mit Hilfe des Integrals über Treppenfunktionen kann man durch den Daniell-Prozeß Lebesgue integrierbare Funktionen definieren.

Produktformel. *Für jedes* $y \in K^* \subseteq \mathbb{A}_K^*$ *gilt* $\boxed{\prod_v \|y\|_v = 1}$.

Beweis. $\prod_v \|y\|_v = \prod_{\sigma: K \hookrightarrow \mathbb{C}} |\sigma(x)| \prod_P |x|_P$ wegen 4. und 5 (das erste Produkt läuft über alle Einbettungen $\sigma : K \hookrightarrow \mathbb{C}$). Also[3] $\prod_v \|y\|_v = |N_{K/\mathbb{Q}}(x)| N(x)^{-1} = 1$ nach 2.3. □

2.8 Minkowski Lemma

Quader. Für den nicht archimedischen Quader $Q_{C,fin} = \prod_P \{x \in K_P \mid |x|_P \leq C_P\}$ und den archimedischen Quader $Q_{C,\infty} = \prod_{v|\infty} \{x \in K_v \mid |x|_v \leq C_v\}$ sei

- $Q_C = Q_{C,\infty} \times Q_{C,fin}$.
- $Q'_C = \frac{1}{2} Q_{C,\infty} \times Q_{C,fin}$.

[2]Beachte für $\lambda \in \mathbb{Q}_p$ gilt daher $|\lambda|_p^{[K_P:\mathbb{Q}_p]} = \|\lambda\|_P$ analog zu 4.

[3]Alternativ folgt aus Fubini und $0 \to K \to \mathbb{A}_K \to K\backslash A_K \to 0$ die Formel $\|y\|_{\mathbb{A}_K} = \|y\|_K \|y\|_{\mathbb{A}_K/K} = 1$ auch aus 1. und 2. oben.

Dann gilt $Q'_C - Q'_C \subseteq Q_C$.

Quadervolumina. Es gilt

$$vol(Q_C) = \|C\| vol(Q_1) \ ,$$

wobei $\|C\| = \prod_v C_v$ (komplexe Stellen wir in diesem Produkt doppelt berücksichtigt). [Für $\xi \in \mathbb{A}_K^*$ und $|\xi_v|_v = C_v$ gilt $Q_C = \xi Q_1$. Also $\|C\| = \|\xi\|$].

Lemma. *Sei $C = (C_v)$ mit $C_v > 0$ und $C_v = 1$ für fast alle v. Dann existiert ein nur von K abhängiges $\delta > 0$ so, daß gilt:* $\boxed{\|C\| > \delta \Longrightarrow Q_C \cap K \neq \{0\}}$.

Beweis. Im Fall $Q_C \cap K = \{0\}$ die Projektion $\mathbb{A}_K \to K\backslash A_K$ injektiv auf Q'_C, denn $q \in q' + K$ und $q \neq q'$ in Q'_C würde sofort $(Q'_C - Q'_C) \cap K \neq \{0\}$ und damit $Q_C \cap K \neq \{0\}$ implizieren wegen $Q'_C - Q'_C \subseteq Q_C$. Aus Fubini folgt daher

$$vol(Q'_C) = \|C\| vol(Q'_1) \leq vol(K\backslash A_K) \ .$$

Also gilt $Q_C \cap K \neq \{0\}$, falls $\|C\| > vol(K\backslash A_K)/vol(Q'_1) =: \delta$. □

Bemerkung. $\delta = (2^{-r_2}\sqrt{|D_{K/\mathbb{Q}}|})/(2^{r_1}\pi^{r_2}2^{-n}) = (\frac{2}{\pi})^{r_2}\sqrt{|D_{K/\mathbb{Q}}|}$. [4]

Endlichkeit der Klassengruppe. Für ein gebrochenes Ideal $I \in Div_K$ setze $C_P = N(P)^{-v_P(I)}$ für die Primideale $P \neq 0$ von K. Wähle C_v für $v|\infty$ mit $\|C\| > \delta$. Dann existiert $0 \neq x \in K$ mit $x \in Q_C \cap K = I$. Für das Ideal $J = xI^{-1} \subseteq \mathfrak{o}_K$ gilt dann $JI = (x)$. Also $N(J)N(I) = N((x))$. Aus $N((x)) = |N_{K/\mathbb{Q}}(x)|_{\mathbb{C}}$ (siehe 2.3) und $|N_{K/\mathbb{Q}}(x)|_{\mathbb{C}} = \prod_{v|\infty} \|x\|_v \leq \prod_{v|\infty} C_v = \|C\| N(I)$ folgt daher $N(J) \leq \|C\|$. Für die größte ganze Zahl $[\delta] \geq \delta$ gilt somit

Satz. *Die Klassengruppe $Cl(K)$ ist endlich. Jede Klasse besitzt als Repräsentanten eines der endlich vielen Ideale $J \subseteq \mathfrak{o}_K$ mit $N(J) \leq [\delta]$.*

[4] Beachte dazu $vol(K\backslash A_K) = 2^{-r_2}\sqrt{|D_{K/\mathbb{Q}}|}$. Der erste Faktor 2^{-r_2} kommt von $dxdy = \frac{1}{2}dzd\bar{z}$. Andererseits $vol(Q'_1) = 2^{-n}vol(Q_1) = 2^{-n}2^{r_1}\pi^{r_2} = (\frac{\pi}{4})^{r_2}$. Schïeßlich gilt $vol(Q_1)/vol(K\backslash A_K) = 2^{r-1+r_2}/\delta = (2\pi)^{r_2}2^{r_1}/\sqrt{|D_{K/\mathbb{Q}}|}$. Normiert man die Maße dx_v so, daß die Volumina der lokalen 1-Quader gleich $2, 2\pi, |D_{K/\mathbb{Q}}|_v^{-1/2}$ sind für $K_v = \mathbb{R}, \mathbb{C}$ und $v \nmid \infty$, folgt $vol(K\backslash A_K) = 1$.

2.9 Die Idelklassengruppe

Die Einheitengruppe $\mathbb{A}_K^*$ des Adelrings $\mathbb{A}_K$ nennt man die Idelgruppe $\mathbb{I}_K$ von K. Ein Adel $x = (x_v)$ liegt in $\mathbb{I}_K$ genau dann, wenn $|x_v|_v = 1$ gilt für fast alle v. $\mathbb{I}_K$ ist daher das eingeschränkte Produkt $\prod_v' K_v^* = \prod_v (G_v : H_v)$ für $G_v = K_v^*$ und $H_v = \mathfrak{o}_v^*$ (kompakt offen in K_v^* für alle $v \nmid \infty$). Man versieht $\mathbb{I}_K$ daher nicht mit der Einschränkungstopologie aus $\mathbb{A}_K$, sondern mit der feineren Topologie des eingeschränkten kartesischen Produktes. Nur dadurch wird $\mathbb{I}_K$ zu einer topologischen Gruppe (Stetigkeit der inversen Abbildung!) Setze $C_K = K^* \backslash \mathbb{I}_K$.

Die Idelnorm. Für $x = (x_v) \in \mathbb{I}_K$ gilt $|x_v|_v = 1$ und daher $\|x_v\|_v = 1$ für fast alle v. Daher ist das Produkt $\|x\| = \prod_v \|x_v\|_v$ wohldefiniert. Man erhält einen Homomorphismus $\|.\| : \mathbb{I}_K \to \mathbb{R}_{>0}^*$, die sogenannte Idelnorm

$$0 \to \mathbb{I}_K^1 \to \mathbb{I}_K \to \mathbb{R}_{>0}^* \to 0 \, .$$

Wir haben bereits gezeigt, daß K^* im Kern $\mathbb{I}_K^1$ der Idelnorm liegt.

Lemma. *K^* liegt diskret in $\mathbb{I}_K^1$ mit kompaktem Quotient $C_K^1 = K^* \backslash \mathbb{I}_K^1$.*

Beweis. K^* liegt diskret in $\mathbb{A}_K$, also diskret in $\mathbb{A}_K^*$ für die Einschränkungstopologie, und damit erst recht für die feinere Ideletopologie.

Der Hilfsquader Q. Wähle einen Hilfsquader $Q = Q_C$ vom Volumen $vol(Q) > \delta$. Für jedes $\xi \in \mathbb{I}_K^1$ gilt $vol(\xi Q) = vol(Q) > \delta$ wegen $\|\xi\| = 1$. Also existiert $0 \neq x \in K^* \cap (\xi Q)$, d.h. $\frac{x}{\xi} \in Q$. Wir wollen jetzt etwas analoges für den Kehrwert $\frac{\xi}{x}$ zeigen. Wegen $\|\frac{x}{\xi}\| = 1$ gibt es auch ein $0 \neq y \in K^* \cap \frac{x}{\xi} Q$. Nur endlich viele $y = y_1, .., y_r$ aus der diskreten Menge K^* liegen in dem Kompaktum Q_{C^2} von $\mathbb{A}_K$. Wegen $y \in \frac{x}{\xi} Q \subseteq Q \cdot Q = Q_{C^2}$ gilt also $y = y_i$ für ein $i = 1, .., r$.

Kokompaktheit. Es folgt $\frac{\xi}{x} \in \Omega = Q \cup \bigcup_{i=1}^r y_i^{-1} Q$. Die Menge Ω ist kompakt in $\mathbb{A}_K$ (daher obdA selbst ein Quader), und enthält $\frac{\xi}{x}$ und $\frac{x}{\xi}$. Damit liegt $\frac{x}{\xi}$ in dem Kompaktum $\Omega \cap \Omega^{-1}$ von $\mathbb{I}_K$. Der Schluß zeigt, daß $K^* \backslash \mathbb{I}_K^1$ im Bild dieses Kompaktums liegt, und daher selbst kompakt ist bezüglich der Quotiententopologie von $\mathbb{I}_K^1$. □

2.10 Idelklassencharaktere

Charaktere. Ein Quasi-Charakter einer topologische Gruppe X ist per Definition ein stetiger Homomorphismus

$$\eta : X \to \mathbb{C}^* .$$

Hat η seine Werte im komplexen Einheitskreis $S^1 \subseteq \mathbb{C}^*$, dann nennt man η einen Charakter von X. Produkte von (Quasi)charakteren sind (Quasi)charaktere. Die Charaktere von X definieren durch Multiplikation eine Gruppe X^D.

Die Gruppe Z_K. Beachte $\mathbb{I}_{\mathbb{Q}} \subseteq \mathbb{I}_K$ und damit $\mathbb{I}_{\mathbb{Q},\infty} = \mathbb{R}^*_{>0} \subseteq \mathbb{I}_K$. Wir nennen diese Untergruppe Z_K, und wählen eine konkrete Einbettung

$$\iota_K : \mathbb{R}^*_{>0} \cong Z_K \subseteq \mathbb{I}_K$$

für die gilt $\|\iota_K(t)\| = t$. Setze dazu $\iota_K(t) = (t^{1/n}, \cdots, t^{1/n}) \subseteq \mathbb{A}^*_\infty \subseteq \mathbb{I}_K$ für $t \in \mathbb{R}^*_{>0}$ und $n = [K : \mathbb{Q}]$. Die natürliche Abbildung $Z_K \times \mathbb{I}^1_K \to \mathbb{I}_K$ ist ein Isomorphismus. Der Quotient $X_K = Z_K \backslash C_K$ ist kompakt, da isomorph zu C^1_K. Jeder Quasicharakter von X_K hat daher beschränktes Bild, und ist somit ein Charakter. Jeder Quasicharakter von $\iota_K : Z_K \cong \mathbb{R}^*_{>0}$ hat die Gestalt $t \mapsto t^{(r_1+2r_2)s/n} = t^s = \|t\|^s$ für eine komplexe Zahl $s \in \mathbb{C}$.

Lemma. *Die Gruppe $X_K = Z_K \backslash C_K$ ist kompakt. Jeder Quasicharakter η von C_K besitzt eine eindeutige Zerlegung $\eta(x) = \chi(x)\|x\|^s$ in eine Potenz der Idelnorm und einen Charakter $\chi(x)$ von X_K.*

Beweis. Die Einschränkung $\eta|_{Z_K}(t)$ auf Z_K hat die Gestalt $t \mapsto t^s$ für ein $s \in \mathbb{C}$, $\chi(x) = \eta(x)\|x\|^{-s}$ ist daher trivial auf Z_K. Als Quasicharakter der kompakten Gruppe $X = Z_K \backslash C_K$ liegen die Werte von χ in S^1. □

Führer. Sei V eine Umgebung von $1 \in S^1$, welche als Untergruppe nur $\{1\}$ enthält. Für einen Charakter $\chi \in (I_K)^D$ gibt es ein Ideal $I = \prod_v P_v^{n_v} \subseteq \mathfrak{o}_K$, für das die die offene Menge $\eta^{-1}(V) \subseteq \mathbb{I}_K$ eine offene Umgebung $U = U_\infty \times U_I$ enthält mit

$$U_I = \prod_{n_v>0, v\nmid\infty} \left\{1 + \pi_v^{n_v}\mathfrak{o}_v\right\} \times \prod_{v, n_v=0} \mathfrak{o}_v^*$$

(nach Definition der Topologie von $\mathbb{I}_K$). U_I ist eine Untergruppe von $\prod_{v\nmid\infty} \mathfrak{o}_v^*$ (mit endlichem Index). Somit ist $\eta(U_I)$ eine Untergruppe von $V \subseteq S^1$, also trivial. Also

Lemma. *Jeder Charakter $\chi \in (X_K)^D$ faktorisiert über einen Quotienten*

$$\boxed{M_I = (K^* Z_K)\backslash \mathbb{I}_K / U_I} \, .$$

Das kleinste Ideal $I = \prod_{v\in S} P_v^{n_v}$ in $\mathfrak{o}_K$ mit dieser Eigenschaft ist eindeutig bestimmt und heißt FÜHRER *des Charakters χ.*

Beispiel. Der Fall $K = \mathbb{Q}$. Hier ist $\mathbb{I}_\mathbb{Q} \cong \mathbb{Q}^* \times \mathbb{R}^*_{>0} \times \prod_p \mathfrak{o}_p^*$, also $X_\mathbb{Q} = \prod_p \mathfrak{o}_p^*$. Also ist $M_I = \pi_0(M_I)$ endlich, nämlich die Einheitengruppe des Rings $\mathbb{Z}/I\mathbb{Z}$

$$M_I = \prod_p \mathfrak{o}_p^*/U_I = \prod_{v\in S} (\mathbb{Z}/p_v^{n_v}\mathbb{Z})^* = (\mathbb{Z}/I\mathbb{Z})^* \, .$$

Dies ist im allgemeinen nicht mehr richtig. Dies hat folgenden Grund.

Komponenten. Sei $U_\infty = (\mathbb{I}_{K,\infty})^+$ die topologische Zusammenhangskomponente $\mathbb{R}^{r_1}_{>0} \times \mathbb{C}^{r_2}$ von $\mathbb{I}_{K,\infty}$ (eine offene Untergruppe). Das Bild von $U_\infty U_I$ in X_K ist daher eine offene Untergruppe der kompakten Gruppe. Das Bild ist isomorph zu $(\mathfrak{o}_I^+ Z_K\backslash U_\infty U_I$ für $\mathfrak{o}_I^+ = K^* \cap (U_\infty U_I)$. Endlich viele Nebenklassen überdecken daher den Raum. Also zerfällt die kompakte Gruppe X_K in eine endliche disjunkte Vereinigung von offen-abgeschlossenen Teilmengen $X_K = \coprod_{i=1}^k (\mathfrak{o}_I^+ Z_K)\backslash U_\infty U_I$. Somit

$$M_I = \coprod_{i=1}^k (\mathfrak{o}_I^+ Z_K)\backslash U_\infty \quad , \quad \#\pi_0(M_I) = k \, .$$

Da U_∞ zusammenhängend ist, ist dies die Zerlegung von M_I in endlich viele topologische Zusammenhangskomponenten. Wir werden in 2.12 sehen, daß jede Komponente $(\mathfrak{o}_I^+ Z_K)\backslash U_\infty$ isomorph ist zu einem Produkt von Kreisringen $(S^1)^{n-1}$ für $n = [K : \mathbb{Q}]$. Also für die endliche Gruppe $\pi_0(M_I)$ der Ordnung k

$$0 \to (S^1)^{n-1} \to M_I \to \pi_0(M_I) \to 0 \, .$$

Punktetrennung. Daher gibt es jedes $1 \neq x_0 \in X_K$ einen Charakter $\chi \in (X_K)^D$ mit $\chi(x_0) \neq 1$. [Es gibt ein I mit nichttrivialem Bild von x_0 in M_I. Also genügt, daß Charaktere von endlich erzeugten abelschen Gruppen $M_I \cong \pi_0(M) \times (S^1)^{n-1}$ Punkte trennen[5](siehe 1.3)].

[5]Eine Gruppe M dieser Gestalt zerfällt in das Produkt von $(S^1)^{n-1}$ und der endlichen Gruppe der Komponenten. Ist $\pi_0(M)$ zyklisch von der Ordnung n, wählt man einen Erzeuger x in M. Dann ist $nx \in (S^1)^{n-1}$ gleich ny für ein $y \in (S^1)^{n-1}$. Also $M = \langle \frac{x}{y} \rangle \times (S^1)^{n-1}$. Der allgemeine Fall geht analog.

Dirichlet Charaktere. Man nennt $\chi \in (X_K)^D$ einen DIRICHLET Charakter, wenn χ auf der Zusammenhangskomponente $U_\infty = \mathbb{I}_{K,\infty}^+ \subseteq \mathbb{I}_K$ trivial ist. Äquivalent dazu ist: χ oder $\chi|_{\mathbb{I}_{K,\infty}}$ haben endliche Ordnung. Dirichlet Charaktere, deren Führer I teilt, entsprechen eineindeutig Charakteren der endlichen Gruppe $\pi_0(M_I)$.

2.11 Der modulare Turm

Wir schreiben kurz M für M_I im Fall $I = \mathfrak{o}_F$. Sei $J|I$ ein Idealteiler. Dann hat man kanonische Surjektionen

$$\begin{array}{ccc} M_I = X_K/U_I & \twoheadrightarrow & \pi_0(M_I) \\ \downarrow & & \downarrow \\ M_J = X_K/U_J & \twoheadrightarrow & \pi_0(M_J) \\ \downarrow & & \downarrow \\ M = X_K/U & \twoheadrightarrow & \pi_0(M) \end{array}$$

Wir schreiben $U_I = \prod_{v\nmid\infty} U_{I,v}$ und wieder kurz $U = U_I$ im Fall $I = \mathfrak{o}_F$. Sei S eine nichtarchimedische Stellenmenge von K, welche alle Teiler von I enthält.

Quotienten. Aus $M = M_I/U$ folgt $\pi_0(M) = \pi_0(M_I)/U$. Für $K^* \cap (U_\infty U) =: \mathfrak{o}_{K,S}^+$ gilt $Bild(U) = \mathfrak{o}_{K,S}^+ \backslash (\prod_{v\in S} U_v/U_{I,v})$ [Um das Bild von U in $\pi_0(M_I)$ zu bestimmen, muß man die Bedingung $ku_\infty u_1 u = u_2$ analysieren für $k \in K^*, u_\infty \in U_\infty, u \in U_I$ und $u_1, u_2 \in U$. Dies erzwingt $k \in K^* \cap (U_\infty U)$], also (*)

$$\boxed{0 \to \mathfrak{o}_K^+ \Big\backslash \big(U/U_I\big) \to \pi_0(M_I) \to \pi_0(M) \to 0}\,.$$

Notation. Die Untergruppen $\Gamma_I = \mathfrak{o}_K^+ \cap U_I$ definieren eine absteigende Filtration durch Kongruenzgruppen auf der arithmetischen Gruppe $\Gamma = \mathfrak{o}_K^+$. Beachte $\mathfrak{o}_K^+$ ist eine Untergruppe der Einheitengruppe $\mathfrak{o}_K^*$ (vom Index 2^l mit $l \le r_1$). Es gilt (**)

$$0 \to \mathfrak{o}_K^+/\Gamma_I \to \prod_{v\in S} U_v/U_{I,v} \to \mathfrak{o}_K^+ \Big\backslash \big(U/U_I\big) \to 0\,.$$

Für $J|I$ folgt aus (*) und (**) folgt für die Projektion $p_{IJ} : \pi_0(M_I) \twoheadrightarrow \pi_0(M_J)$

Lemma. *Für $J|I$ hat man eine exakte Sequenz*

$$0 \to \Gamma_J/\Gamma_I \to \prod_{v|I} U_{J,v}/U_{I,v} \to Kern\Big(\pi_0(M_I) \twoheadrightarrow \pi_0(M_J)\Big) \to 0\ .$$

2.12 Dirichlets Einheitensatz

Sei S eine endliche Stellenmenge von K, welche die Menge S_∞ aller archimedischen Stellen enthält. Wir betrachten die offene Untergruppe

$$U_S = \big(\prod_{v\in S} K_v^*\big)^1 \times \prod_{v\notin S} \mathfrak{o}_v^* \ \subseteq\ \mathbb{I}_K^1$$

und die kurzen exakten Sequenzen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^* & \longrightarrow & \mathbb{I}_K^1 & \xrightarrow{\pi} & C_K^1 & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & \mathfrak{o}_{K,S}^* & \longrightarrow & U_S & \longrightarrow & \mathcal{C} & \longrightarrow & 0 \end{array}$$

Das Bild $\mathcal{C} = \pi(U_S)$ ist kompakt, da abgeschlossen in dem Kompaktum C_K^1. [Beachte: $\mathcal{C}$ ist (offen) abgeschlossen in C_K^1 genau dann, wenn das Urbild $\mathcal{U} = \pi^{-1}(\mathcal{C}) = K^* \cdot U_S$ (offen) abgeschlossen in $\mathbb{I}_K^1$ ist. $\mathcal{U}$ und sein Komplement ist eine Vereinigung von Nebenklassen der offenen Untergruppe U_S, also offen. Also ist $\mathcal{U}$ offen und abgeschlossen. Somit ist auch $\mathcal{C}$ offen und abgeschlossen in C_K^1].

S-Einheiten. Bezeichne $\mathfrak{o}_{K,S}^* = K^* \cap U_S$ die Untergruppe von K^* aller S-Einheiten (für $S = S_\infty$ ist $\mathfrak{o}_{K,S}^* = \mathfrak{o}_K^*$ die Einheitengruppe), dann gilt $\mathcal{C} = U_S/\mathfrak{o}_{K,S}^*$ (siehe Diagram). Die Abbildung

$$L((x_v)) = \bigoplus_{v\in S} log(\|x_v\|_v)$$

definiert dann folgende exakte Sequenzen

$$\begin{array}{ccccc} & & \mathcal{C} & \longrightarrow\!\!\!\!\!\rightarrow & \mathcal{Q} \\ & & \uparrow & & \uparrow \\ \prod_v\{x_v \mid |x_v|_v = 1\} & \hookrightarrow & U_S & \xrightarrow{L} & (\prod_{v\in S_\infty}(\mathbb{R},+) \times \coprod_{v\in S\setminus S_\infty} \mathbb{Z}\log(P_v))^0 \\ \uparrow & & \uparrow & & \uparrow \\ \mu(K) & \hookrightarrow & \mathfrak{o}_{K,S}^* & \longrightarrow\!\!\!\!\!\rightarrow & \mathfrak{o}_{K,S}^*/\mu(K) \end{array}$$

Der Quotient Q des Kompaktums $\mathcal{C}$ ist wieder kompakt. Somit ist $L(\mathfrak{o}_{K,S}^*)$ kokompakt in$(\prod_{v\in S_\infty}(\mathbb{R},+)\times\prod_{v\in S\setminus S_\infty}\mathbb{Z}\log(P_v))^0\cong\mathbb{R}^{\#S_\infty-1}\times\mathbb{Z}^{\#S-\#S_\infty}$, also ein Gitter isomorph zu $\mathbb{Z}^{\#S-1}$.

Satz. *Die S-Einheitengruppe $\mathfrak{o}_{K,S}^*$ ist eine endliche erzeugte abelsche Gruppe*

$$\boxed{\mathfrak{o}_{K,S}^*\cong\mathbb{Z}^{\#S-1}\times\mu(K)}\,,$$

wobei $\mu(K)$ die endliche Gruppe aller Einheitswurzeln von K ist.

Beweis. Der Kern $\mu(K)$ von $L|_{\mathfrak{o}_{K,S}^*}:\mathfrak{o}_{K,S}^*\to(\prod_{v\in S}\mathbb{R})^0$ ist eine Gruppe. Als Durchschnitt der diskreten Gruppe $\mathfrak{o}_{K,S}^*\subseteq K^*$ mit der kompakten Teilmenge $\prod_v\{x_v\mid|x_v|_v=1\}$ von $\mathbb{I}_K^1$ ist sie endlich. Somit besteht $\mu(K)$ genau aus den Einheitswurzeln in K. □

Bemerkung. Der Quotient der kompakten Gruppe C_K^1 nach der offenen Untergruppe $\mathcal{C}$ ist endlich. Anderseits $C_K^1/\mathcal{C}=Div_{K,S}/K^*=:Cl(K,S)$ für $Div_{K,S}=\bigoplus_{v\notin S}\mathbb{Z}$. Für $S=S_\infty$ ist dies die Klassengruppe $Cl(K)$. Dies beweist nochmals Satz 2.8. Die endliche Klassengruppe $Cl(K)=Cl(K,S_\infty)$ (siehe 2.12) wird von endlich vielen Primidealen P erzeugt. Wählt man S so groß, daß diese endlich vielen Primideale und die Stellen $v|\infty$ in S liegen, gilt $C_K^1/U_S=Cl(K)/Bild(U_{S\setminus S_\infty})=0$ und somit

$$C_K^1=U_S/\mathfrak{o}_{K,S}^*\,.$$

Charaktere mit Führer I. ObdA $C_K^1=U_S/\mathfrak{o}_{K,S}^*$ wie oben. Für $M_I=(K^*Z_K)\backslash\mathbb{I}_K/U_I$ hat man dann die exakte Sequenz

$$0\to\frac{\prod_v\{x_v\mid|x_v|_v=1\}}{\mu(K)U_I}\to M_I\to\frac{(\prod_{v\in S_\infty}\mathbb{R}\prod_{v\in S\setminus S_\infty}\mathbb{Z})^0}{\mathfrak{o}_{K,S}^*}\to 0.$$

Links steht ein Produkt von $(S^1)^{r_2}$ und einer endlichen Gruppe, rechts ein Produkt von $(S^1)^{r_1+r_2-1}$ mit einer anderen endlichen Gruppe. $M_I\cong\pi_0(M)\times(S^1)^{n-1}$ ist also das Produkt einer endlichen Gruppe $\pi_0(M)$ mit der Zusammenhangskomponente $(S^1)^{n-1}$. Die Gruppe der Charaktere von M_I ist daher isomorph zu $\pi_0(M)^D\times\mathbb{Z}^{n-1}$. Variiert man I, folgt: Die Charaktergruppe von $X_K=(K^*Z_K)\backslash\mathbb{I}_K$ ist abzählbar.

Kapitel 3

Hecketheorie (additive Spurformel)

3.1 Normierung der Haarmaße

Sei $dx_{\mathbb{A}} = \prod_v dx_v$ ein additives Haarmaß von $\mathbb{A}_K$ mit $vol(\mathfrak{o}_v, dx_v) = 1$ für fast alle v. Die dx_v seien so normiert (etwa wie in der Fußnote von Seite 27) daß

$$vol(K\backslash\mathbb{A}_K, \frac{dx_{\mathbb{A}_K}}{d\gamma}) = 1$$

gilt für das Quotientenmaß von $dx_{\mathbb{A}_K}$ nach dem diskreten Zählmaß $d\gamma$ von K.

Wir fixieren eine globale invariante nicht verschwindende algebraische 1-Form der algebraischen Gruppe $\mathbb{G}_m = Spec(K[t, t^{-1}])$ über K. Dieser eindimensionaler K-Vektorraum wird erzeugt von der Differentialform $\frac{dt}{t}$. Jede andere Wahl unterscheidet sich daher nur um eine Konstante $\lambda \in K^*$.

Lokale Maße. Für additive Haarmaße dx_v auf K_v ist $dx_v^* = \frac{dx_v}{\|x\|_v}$ ein Haarmaß der multiplikativen Gruppe K_v^*. Sei v eine nicht archimedische Stelle von K. Nach Annahme gilt $vol(\mathfrak{o}_v, dx_v) = 1$ für fast alle v. Aus $vol(\mathfrak{o}_v, dx_v) = 1$ folgt

$$vol(\mathfrak{o}_v^*, dx_v^*) = \frac{\#\kappa_v^*}{\#\kappa_v} = \frac{N(P_v) - 1}{N(P_v)} = \lim_{s\to 1}(1 - N(P_v)^{-s})^{-1} .$$

Globale Maße. Das Produkt dieser Zahlen über alle P_v ist Null (klar im Fall $K = \mathbb{Q}$). Also ist $\mathbb{I}_K \subseteq \mathbb{A}_K$ bezüglich des additiven Maßes $\prod_v dx_v$ oder auch bezüglich $\prod_v \frac{dx_v}{\|x_v\|_v}$ eine NULLMENGE! Daher definieren wir das Haarmaß dg_K auf dem restringierten Produkt $\mathbb{I}_L$ (nach Wahl von additiven Haarmaßen dx_v auf K_v) durch die Formel

$$dg_K = \prod_{v|\infty} \frac{dx_v}{\|x\|_v} \times \prod_{v\nmid\infty} (1 - N(P_v)^{-1})^{-1} \frac{dx_v}{\|x\|_v} .$$

Jetzt gilt $vol(\mathfrak{o}_v^*, dg_v) = 1$ an allen nicht archimedischen Stellen. Eine andere Wahl $\lambda\frac{d}{t}t$ ändert die lokalen Maße um einen Faktor $\lambda \in K_v^*$. Das globale Maß ändert sich wegen $\lambda \in K^*$ wegen der Produktformel $\prod_v \|\lambda\|_v$ jedoch nicht!

Induzierte Maße. Wir definieren nun das Maß $dx_K = \frac{dg_K}{da_K}$ als das Quotientenmaß auf $X_K = Z_K\backslash C_K \cong C_K^1$ für $da_K = \iota_K^*(\frac{dt}{t})$ und $\iota_K : Z_K \cong \mathbb{R}_{>0}^*$ im Sinne von 2.10 (dx_K sollte man nicht verwechseln mit dem additiven Maß dx) nach dem diskreten Maß $d\gamma$ auf K^*. Also $dg_K = \prod_v dg_v = dx_K \cdot \frac{dt}{t} \cdot d\gamma$.

3.2 Zetafunktionen

Sei $\eta(x) = \|x\|^s \chi(x)$ ein Quasicharakter von C_K, χ ein Charakter der kompakten Gruppe $X_K = Z_K \backslash C_K$. Aufgefaßt als Charakter der Idelegruppe $\mathbb{I}_K$ gilt

$$\chi(x) = \prod_v \chi_v(x_v)$$

für die Einschränkungen $\chi_v := \chi|_{K_v^*}$ von χ auf den Faktor $K_v^* \subseteq \mathbb{I}_K$. Nach 2.10 gibt es eine endliche Stellenmenge S mit $\chi_v(\mathfrak{o}_v^*) = 1$ für $v \notin S$.

Lemma. *Sei v eine nichtarchimedische Stelle und $\chi_v : K_v^* \to S^1$ ein Charakter mit $\chi_v|_{\mathfrak{o}_v^*} = 1$. Dann gilt für $Re(s) > 0$ und $f_v(x) = 1_{\mathfrak{o}_v}(x)$*

$$\int_{K_v^*} f_v(x)\chi_v(x)\|x\|_v^s \cdot dg_v(x) = \left(1 - \chi_v(\pi_v)N(P_v)^{-s}\right)^{-1}$$

(bei der Normierung $vol(\mathfrak{o}_v^*, dg_v) = 1$ des Haarmaße dg_v^* von K_v^*).

Beweis. $K_v^* = \biguplus_i \pi_v^i \cdot \mathfrak{o}_v^*$ liefert $\int_{K_v^*} 1_{\mathfrak{o}_v}(x)\chi_v(x)\|x\|_v^s dg_v(x)$ oder die geometrische Reihe $\sum_{i=0}^{\infty} \int_{\mathfrak{o}_v^*} \chi_v(\pi_v^i x)\|\pi_v^i x\|_v^s dg_v(x) = vol(\mathfrak{o}_v^*, dg_v) \cdot \sum_{i=0}^{\infty} \chi_v(\pi_v^i)\|\pi_v\|_v^s$. Diese konvergiert für alle $Re(s) > 0$ gegen $(1 - \chi_v(\pi_v)N(P_v)^{-s})^{-1}$, denn $|\chi(\pi_v)| = 1$ und $0 < \|\pi_v\|^s = N(P_v)^{-s} < 1$. □

Bemerkung. Für $v \nmid \infty$ ist eine beliebige lokalkonstante Funktion $f_v(x)$ mit kompaktem Träger auf K_v von der Gestalt $f_v(x) = const \cdot 1_{\mathfrak{o}_v}(x) + h_v(x)$ mit einer lokalkonstanten Funktion h_v mit kompaktem Träger auf K_v^*. Das lokale Integral

$$Z_v(f_v, \chi_v, s) = \int_{K_v^*} f_v(x)\chi_v(x)\|x\|_v^s \cdot dg_v(x)$$

ist daher holomorph[1] für $Re(s) > 0$ für alle solchen Funktionen $f_v(x)$. Für gegebenes s_0 mit $Re(s_0) > 0$ ist bei geeigneter Wahl von f_v offensichtlich a $Z_v(f_v, \chi_v, s_0) \neq 0$. Dafür werden die f_v überhaupt nur eingebaut!

Der globale Fall. Sei $f(x) = \prod_v f_v(x_v)$ mit $f_v(x) = 1_{\mathfrak{o}_v}(x)$ für fast alle nichtarchimedischen Stellen v. Sei dabei $f_v(x)$ lokalkonstant mit kompaktem Träger auf

[1] Für archimedische Stellen bleibt das auch richtig. Für $K_v = \mathbb{R}$ und $\chi_v = 1$ und $f_v = exp(-\pi x^2)$ etwa $Z_v(f_v, \chi_v, s) = Z_\infty(s) = \pi^{-s/2}\Gamma(s/2)$, für $\chi_v = sign$ dagegen $Z_v(f_v, \chi_v, s) = Z_\infty(s+1)$.

K_v für alle $v \nmid \infty$. Für $v|\infty$ sei $f_v(x_v)$ eine unendlich of differenzierbare Funktion, für die alle Ableitungen schneller als jedes Polynom gegen Null konvergieren im Limes $\|x_v\|_v \to \infty$ (für jedes $v|\infty$). Solche Funktionen definieren den Raum der SCHWARTZfunktionen $S(\mathbb{A}_K)$. Für $Re(s) > 1$ existiert dann nach obigem Lemma eine endliche Stellenmenge S, so daß das Produkt

$$\boxed{Z(f,\chi,s) = \prod_{v\in S} Z_v(f_v,\chi_v,s)\ \prod_{v\notin S}\Big(1 - N(P_v)^{-s}\Big)^{-1}}$$

absolut und gleichmässig in $Re(s) > 1$ konvergiert. [Eine Majorante ist bis auf eine Konstante die Potenz $\zeta(s)^{[L:K]}$ der Riemannschen Zetafunktion $\zeta(s)$.] $Z(f,\chi,s)$ ist daher holomorph als Funktion der Variable s im Bereich $Re(s) > 1$, und besitzt dort keine Nullstellen.

3.3 Analytische Fortsetzung

Sei $Re(s) > 1$. Nach 2.10 und 3.1 gilt $\int_{\mathbb{I}_K} dg_K = \int_{\mathbb{R}^*_{>0}} \frac{dt}{t} \int_{C^1_K} dx_K \sum_{\gamma\in K^*}$. Wegen $\chi(Z_K) = \chi(K^*) = 1$ folgt

$$Z(f,\chi,s) = \int_{\mathbb{I}_K} f(g)\chi(g)\|g\|^s dg_K = \int_{\mathbb{R}^*_{>0}} \Big(\int_{C^1_K} \sum_{\gamma\in K^*} f(\gamma x t)\chi(x)dx_K\Big) t^s \frac{dt}{t}\ .$$

Wir zerlegen das t-Integral in Teilintegrale $\int_1^\infty$ und $\int_0^1$. Wir formen das zweite Integral um mit Hilfe der

Poissonformel. *Für Schwartzfunktionen $f = \prod_v f_v \in S(\mathbb{A}_K)$ gibt es Schwartzfunktionen $\widehat{f} = \prod_v \widehat{f_v} \in S(\mathbb{A}_K)$, so daß für alle $x \in \mathbb{I}_K$ gilt*

$$\boxed{f(0) - \|x\|^{-1}\widehat{f}(0) + \textstyle\sum_{\gamma\in K^*} f(\gamma x) = \|x\|^{-1} \sum_{\gamma\in K^*} \widehat{f}(\gamma x^{-1})}\ .$$

Wegen $\int_0^1 t^s \frac{dt}{t} = \frac{1}{s}$ etc. ist daher $\big(\int_{C^1_K} \chi(x)dx_K\big)\big(\frac{\widehat{f}(0)}{1-s} + \frac{f(0)}{s}\big) + Z(f,\chi,s)$ gleich

$$\int_{t\geq 1}\Big(\int_{C^1_K} \sum_{\gamma\in K^*} f(\gamma x t)\chi(x)dx_K\Big) t^s \frac{dt}{t} + \int_{t\leq 1}\Big(\int_{C^1_K} \|x^{-1}t^{-1}\| \sum_{\gamma\in K^*} \hat{f}(\gamma x^{-1}t^{-1})\chi(x)dx_K\Big) t^s \frac{dt}{t}$$

Wegen $\|x\| = 1$ für $x \in C_K^1$ liefern die Substitutionen $t \mapsto t^{-1},\ x \to x^{-1}$ somit

$$\int_{\geq 1}\Big(\int_{C_K^1}\sum_{\gamma\in K^*}(f(\gamma xt)\chi(x)dx_K\Big)t^s\frac{dt}{t} + \int_{\geq 1}\Big(\int_{C_K^1}\sum_{\gamma\in K^*}\widehat{f}(\gamma xt)\chi^{-1}(x)dx_K\Big)t^{1-s}\frac{dt}{t}$$

oder zurückverwandelt für $\mathbb{I}_K^{\geq 1} = \{x \in \mathbb{I}_K \mid \|x\| \geq 1\}$

$$\int_{(\mathbb{I}_K)^{\geq 1}} f(g)\chi(g)\|g\|^s dg_K + \int_{(\mathbb{I}_K)^{\geq 1}} \widehat{f}(g)\chi^{-1}(g)\|g\|^{1-s} dg_K\ .$$

Da f an den nichtarchimedischen Stellen kompakten Träger besitzt, klingen für $g = xt$ die Integranden beider Integrale $\widehat{f}(tx) \to 0$ und $f(tx) \to 0$ für $t \to \infty$ und $x \in C_K^1$ schneller ab als jedes Polynom in $\|tx\| = t$. (In Bezug auf $\widehat{f}$ siehe dazu Abschnitt 3.5). Daher zeigt der Satz von der dominierten Konvergenz, daß beide Integrale nicht nur für $Re(s) > 1$, sondern auf ganz $\mathbb{C}$ holomorphe Funktionen in s definieren. Also wegen $\chi^{-1} = \overline{\chi}$

Satz. $Z(f,\chi,s) + (\int_{X_K}\chi(x)dx_K)\big(\frac{\hat{f}(0)}{1-s} + \frac{f(0)}{s}\big)$ *ist holomorph auf ganz* $\mathbb{C}$*, und erfüllt die Funktionalgleichung*

$$\boxed{Z\big(f,\chi,s\big) = Z\big(\widehat{f},\overline{\chi},1-s\big)}\ .$$

3.4 Die Poissonformel

Faltung. Wir betrachten Maße wie in 3.1. Sei $f(x) = \prod_v f_v(x_v)$ und sei $f_v(x_v) \in C_c^\infty(K_v)$, wobei darunter Treppenfunktionen zu verstehen sind im Fall $v \nmid \infty$. Die Funktion f operiert durch Faltung

$$(R(fdx_{\mathbb{A}})\varphi)(x) = \int_{\mathbb{A}_K} f(x-y)\varphi(y)dy_{\mathbb{A}} = \int_{K\backslash\mathbb{A}_K} K(x,y)dy$$

auf dem Hilbertraum der quadratintegrierbaren Funktionen $L^2(\mathbb{A}_K/K, dx)$. Wegen $K(x,y) = \sum_{\xi\in K} f(x-y+\xi)$ ist die Spur von $R(fdx_{\mathbb{A}})$ daher[2]

$$Spur(R(fdx_{\mathbb{A}})) = \int_{\mathbb{A}_K/K} K(x,x)\cdot dx = vol(\mathbb{A}_K/K, dx)\cdot\sum_{\xi\in K} f(\xi)\ .$$

[2]Siehe Appendix I

Charaktergruppe. Ist $\psi(x)$ ein Charakter von $K\backslash\mathbb{A}_K$, dann auch $\psi(yx)$ für $y \in K$. Die Charaktergruppe von $K\backslash\mathbb{A}_K$ ist daher ein K-Vektorraum. Jeder Charakter $\psi(x)$ ist trivial auf einem geeigneten Quader $V_C = \prod_{v\nmid\infty} Q_{C_v}$ (analog zu 2.10). Der Approximationssatz liefert $y \in K^*$ mit $\psi(xy)|_{V_C} = 1$. Die Charaktere, welche auf V_1 trivial sind, entsprechen Charakteren von $\mathbb{A}_\infty/\mathfrak{o}_K$. Sei ψ_0 einer davon. Die Charaktere $\psi_0(xy)$ mit $y \in \mathfrak{o}_K$ bilden einen Untermodul von endlichem Index. Charaktere der Form $\psi_0(yx), y \in K$ bilden daher einen Untergruppe von endlichem Index in der Charaktergruppe von $K\backslash\mathbb{A}_K$. Der endliche Quotient ist gleichzeitig ein K-Vektorraum, also gleich Null. Wegen $K\backslash\mathbb{A}_K \cong \mathbb{A}_\infty/\mathfrak{o}_K \times \prod_P \mathfrak{o}_P$ gibt es nichttriviale Charaktere. Es folgt

Lemma. *Sei $\psi_0 \neq 1$ ein Charakter von $\mathbb{A}_K/K$. Dann durchläuft $\psi(x) = \psi_0(yx)$ für $y \in K$ alle Charaktere $\psi \in (K\backslash\mathbb{A}_K)^D$ von $K\backslash\mathbb{A}_K$.*

Spurformel. Beachte $\int_{K\backslash\mathbb{A}_K} \psi_1(x)\overline{\psi}_2(x)dx = \int_{\mathbb{A}_K/K}(\psi_1/\psi_2)(x)dx = \delta_{\psi_1,\psi_2}$, denn wegen der Translationsinvarianz des Maßes ist dieses Integral $vol(K\backslash\mathbb{A}_K)$ oder Null, je nachdem ob $\psi_1 = \psi_2$ oder nicht. Die Charaktere $\psi : K\backslash\mathbb{A}_K \to S^1$ bilden daher eine orthogonale Hilbertraumbasis (Punktetrennung!)

$$\boxed{L^2(K\backslash\mathbb{A}_K, dx) \;=\; \hat{\bigoplus}_\psi \mathbb{C}\psi}.$$

Wegen $(R(fdx_\mathbb{A})\psi)(x) = \psi(fdx_A)\cdot\psi(x)$ mit $R(fdx_\mathbb{A}) = \int_{\mathbb{A}_K} f(y)\psi(-y)dy_\mathbb{A} = \int_{A_K} f(y)\psi_0(-yx)dy_\mathbb{A} = \widehat{f}(x)$ gilt

Poissonformel. Für $\widehat{f}(y) = \prod_v \widehat{f}_v(y_v)$ mit

$$\widehat{f}_v(y_v) = \int_{K_v} f_v(x)\psi_{0,v}(-x_v y_v)dx_v$$

gilt

$$\sum_{y\in K} \widehat{f}(y) = Spur\Big(R(f, dx_\mathbb{A})\Big) = vol(K\backslash\mathbb{A}_K, dx)\sum_{\xi\in K} f(\xi) = \sum_{\xi\in K} f(\xi)\ .$$

Dies ist im Prinzip bereits die im letzten Abschnitt benutzte Poissonformel, denn für $f_v(y) = g(\eta y)$ mit $\eta \in K_v^*$ ist $(\widehat{f}_v)(x_v) = \int_{K_v} g(\eta y_v)\psi_0(-x_v y_v)dy_v = \|\eta\|^{-1}\hat{g}(x_v\eta^{-1})$. Es bleibt zu zeigen, daß die Fourier Transformation den Schwartzraum (siehe nächster Abschnitt) erhält, und die Spurformel auch für Schwartzfunktionen richtig bleibt (Übungsaufgabe). Für unsere Anwendungen reicht aus $f_v \in C_c^\infty(K_v)$, obwohl dann die Fouriertransformierte im allgemeinen für $v|\infty$ nur eine Schwartzfunktion ist.

3.5 Fourier Transformation

Zur Bezeichnung. Wir fixieren jetzt eine Stelle v des Zahlkörpers K, und betrachten für den Körper K_v die (lokale) Fourier Transformation

$$\widehat{f}(y) = \int_{K_v} f(x)\psi_0(-xy)dx = \int_{K_v} f(x)\overline{\psi}_0(xy)dx \ .$$

Ist der globale Charakter ψ_0 nichttrivial, dann auch $\psi_{0,v} = \psi_0|K_v$ (Approximation !). In den Bezeichnungen lassen wir jetzt die Indizes v weg.

Eigenschaften der Fourier Transformation. Für $f \in C_c^\infty(K_v)$ und $\eta \in K_v$ sei $(T_\eta f)(x) = f(x+\eta)$, $(M_\eta f)(x) = \psi_0(\eta x)f(x)$ sowie $(R_\eta f)(x) = f(\eta x)$ im Fall $\eta \neq 0$. Es gilt

1. $\widehat{T_\eta f}(y) = \psi_0(\eta y) \cdot \hat{f}(y) = M_\eta \hat{f}(y)$
2. $\widehat{M_\eta f}(y) = \hat{f}(y-\eta) = T_{-\eta}\hat{f}(y)$.
3. $\widehat{R_\eta f}(y) = \|\eta\|^{-1} \cdot \hat{f}(\eta^{-1}y) = \|\eta\|^{-1} \cdot R_{\eta^{-1}} f(y)$.

Beweis. $\widehat{T_\eta f}(y) = \int_{K_v} f(x+\eta)\overline{\psi}_0(xy)dx = \int_{K_v} f(x)\overline{\psi}_0(xy-\eta y)dx = \psi_0(\eta y)\hat{f}(y)$. Analog $\widehat{M_\eta f}(y) = \int_{K_v} \psi_0(\eta x)f(x)\overline{\psi}_0(xy)dx = \int_{K_v} f(x)\overline{\psi}_0(x(y-\eta))dx = \hat{f}(y-\eta)$. Wie bereits im letzten Abschnitt gezeigt, gilt $\widehat{R_\eta f}(y) = \int_{K_v} f(\eta x)\overline{\psi}_0(xy)dx = \|\eta\|^{-1}\int_{K_v} f(x)\overline{\psi}_0(x\eta^{-1}y)dx = \|\eta\|^{-1}\hat{f}(\eta^{-1}y)$. □

Sei $K_v = \mathbb{R}$ oder $\mathbb{C}$. Der Schwartzraum $S(K_v)$ ist dann der Raum aller C^∞-Funktionen auf K_v, deren Ableitungen schneller als jedes Polynom gegen Null geht für $|x|_v \to \infty$. Die Fourier Transformation ist für alle $f \in S(K_v)$ erklärt. Obige Identitäten bleiben richtig. Man kann die Identitäten nach η Ableiten. Dies zeigt, daß Fourier Transformation Polynom-Multiplikation transferiert in eine iterierte Ableitung. Daraus folgt sofort

$$f \in S(K_v) \Longrightarrow \widehat{f} \in S(K_v) \ .$$

Im nichtarchimdischen Fall ist $S(K_v) = C_c^\infty(K_v)$ der Raum der lokalkonstanten $\mathbb{C}$-wertigen Funktionen auf K_v mit kompaktem Träger (Treppenfunktionen). Beispiel: $f(x) = 1_{\mathfrak{o}_v}(x)$ in $S(K_v)$. Dieser Raum ist invariant unter den R_η, M_η, T_η.

Die Bilder von $1_{\mathfrak{o}_v}(x)$ erzeugen $S(K_v)$ als $\mathbb{C}$-Vektorraum, und $\widehat{f} \in S(K_v)$ folgt aus $f \in S(K_v)$. Dazu genügt

$$\widehat{1}_{\mathfrak{o}_v} = 1_{\pi_v^m \mathfrak{o}_v} = R_{\pi_v^{-m}} 1_{\mathfrak{o}_v} \ .$$

Hierbei ist $m = m_v$ der Führer von ψ_0, die kleinste Zahl $m \in \mathbb{Z}$ mit $\psi_0 | \pi_v^m \mathfrak{o}_v \equiv 1$. Beachte $\int_{\mathfrak{o}_v} \psi_0(yx)dx = 0$, falls $\psi_0(x)|y\mathfrak{o}_v \neq 1$, und $\int_{\mathfrak{o}_v} \psi_0(yx)dx = vol(\mathfrak{o}_v) = 1$ sonst. Zweimaliges Anwenden der Fourier Transformation liefert daher

$$\widehat{\widehat{1}}_{\mathfrak{o}_v} = \widehat{1}_{\pi_v^m \mathfrak{o}_v} = \|\pi_v\|_v^m \cdot R_{\pi_v^m} 1_{\pi_v^m \mathfrak{o}_v} = N(P_v)^{-m} \cdot 1_{\mathfrak{o}_v} \ .$$

Daraus folgt $\widehat{\widehat{\mathrm{f}}}(x) = N(P_v)^{-m} \cdot \mathrm{f}(-x)$ für alle $\mathrm{f} \in S(K_v)$. An der archimedischen Stelle sind $exp(-\pi x^2)$ und $exp(-\pi z\overline{z})$ die Analoga der Funktionen $1_{\mathfrak{o}_v}$.

Globaler Führer. $\psi_0 \in (K \backslash \mathbb{A}_K)^D$ ist konstant 1 auf einer Menge $Q = \prod_{v \nmid \infty} \pi_v^{C_v} \mathfrak{o}_v$ mit $C_v = 1$ für fast alle v (wie in 2.10). Also $m_v \leq 0$ für fast alle v. Beachte $\widehat{1_Q} = 1_{\prod_v \pi_v^{m_v} Q}$. Es folgt dann aber $m_v = 0$ für fast alle v [Sonst wäre $\gamma \in K \cap \prod_v \pi_v^{m_v} Q$ nicht diskret in $\mathbb{A}_\infty$ und $\sum_{\gamma \in K} \widehat{f_\infty 1_Q}(\gamma)$ divergent für geeignetes $f_\infty \in C_c^\infty(\mathbb{A}_\infty)$. Widerspruch!]

Korollar. *Der lokale Führer m_v von ψ_0 erfüllt $m_v = 0$ für fast alle Stellen v.*

Für globales $f(x) = \prod_v f_v(x_v)$ mit $f_v(x_v) = 1_{\mathfrak{o}_v}(x_v)$ für fast alle v (wie in 3.2) impliziert dies $\widehat{f_v} = 1_{\mathfrak{o}_v}$ für fast alle v.

Mit anderen Worten. Sei $S(\mathbb{A}_K)$ der Raum der endlichen Linearkombinationen von Funktionen $f = \prod_v f_v$ mit $f_v \in S(K_v)$ und $f_v = 1_{\mathfrak{o}_v}$ für fast alle Stellen v. Dann gilt

$$f \in S(\mathbb{A}_K) \Longrightarrow \widehat{f} \in S(\mathbb{A}_K) \ .$$

Diese Eigenschaft ist wesentlich (!) für die Existenz einer holomorphen Fortsetzung des Integrals

$$Z^{\geq 1}(\widehat{f}, \overline{\chi}, s) \ := \ \int_{\mathbb{I}_K^{\geq 1}} \widehat{f}(g)\overline{\chi}(g)\|g\|^{1-s} dg_K$$

auf ganz $\mathbb{C}$ im Beweis des Heckeschen Satzes 3.3.

3.6 Das Tamagawa Maß

Der Fall $\chi \neq 1$. Nach 3.3 sind die Funktionen $Z(f, \chi, s)$ holomorph bei $s = 1$ für alle nichttrivialen Charaktere $\chi : C_K \to S^1$ der Ideleklassengruppe C_K ist. [$\chi \neq 1$ impliziert $\int_X \chi(x)dx_K = 0$ wegen $\int_X \chi(x)dx_K = \int_X \chi(xx_0)dx_K = \chi(x_0)\int_X \chi(x)dx_K$.] Durch geeignete Wahl von $f_v, v \in S$ folgt:

$$\prod_{v \notin S}(1 - \chi_v(\pi_v)N(P_v)^{-s})^{-1}$$

ist holomorph bei $s = 1$ für $\chi \neq 1$.

Der Fall $\chi = 1$. Die Funktion $Z(f, 1, s)$ hat bei $s = 1$ höchstens einen einfachen Pol mit dem Residuum $vol(X, dx) \cdot \hat{f}(0)$ für $\hat{f}(0) = \int_{\mathbb{A}_K} f(x)dx_{\mathbb{A}} = \prod_v \int_{K_v} f_v(x_v)dx_v$. Siehe 3.3. Wähle alle f_v mit $\int_{K_v^*} f_v(x_v)dx_v \neq 0$. 3.3 zeigt dann $\lim_{s\to 1} Z_v(f_v, 1, s) = (1 - N(P_v)^{-1})^{-1} \int_{K_v^*} f_v(x)dx_v$. Diese Terme kürzen sich weg. Es folgt

Satz. *Die Zetafunktion* $\zeta(K, s)$ *des Zahlkörpers* K

$$\zeta(K, s) = \prod_{0 \neq P \text{ prim}} (1 - N(P)^{-s})^{-1} = \sum_{I \neq 0} N(I)^{-s}$$

hat einen einfachen Pol bei $s = 1$. *Für* $dx_{\mathbb{A}} = \prod_v dx_v$ *und das Zählmaß* $d\gamma$ *von* K *sei* dx_K *das Quotientenmaß auf* $X_K = K^* Z_K \backslash \mathbb{I}_K$ *von* dg_K/da_K *nach dem Zählmaß von* K^*, *wobei* $da_L = \iota^*(\frac{dt}{t})$ *und*

$$dg_K = \prod_{v|\infty} \frac{dx_v}{\|x_v\|_v} \prod_{0 \neq P \text{ prim}} (1 - N(P)^{-1})^{-1} \frac{dx_v}{\|x_v\|_v} .$$

Dann gilt[3]

$$\frac{vol(X, dx_K)}{vol(K\backslash \mathbb{A}_K, dx_{\mathbb{A}}/d\gamma)} = res_{s=1}\Big(\prod_{v \nmid \infty}(1 - N(P_v)^{-s})^{-1}\Big) = res_{s=1}\Big(\zeta(K, s)\Big) .$$

[3]Das zeigt $vol(X) = 1$ für das regularisierte Maß $(dx_{\mathbb{A}}/\|x_{\mathbb{A}}\|)_{reg} = dg_K/res_{s=1}\zeta(K, s)$, das sogenannte Tamagawa Maß.

3.7 Dirichlet Dichte

Einer Menge von nichtarchimedischen Primstellen Σ des Zahlkörpers K läßt sich die Größe unter dem reellen Limes

$$m_K(\Sigma) = \limsup_{s\to 1^+} \frac{\sum_{w\in\Sigma} N(P_w)^{-s}}{-\log(s-1)} \leq 1$$

zuordnen. Konvergiert die rechte Seite, sagt man Σ besitzt die Dirichletsche K-Dichte $m_K(\Sigma)$. Es gilt

$$-\log(\zeta(K,s)) = \sum_{P\neq 0} log(1-N(P)^{-s}) = \sum_{P\neq 0} N(P)^{-s} + \dots ,$$

bis auf die Summanden $\sum_{m\geq 2}\sum_{P\neq 0} N(P)^{-ms}/m$, der Teilsumme aber im Limes $s\to 1^+$ beschränkt bleibt[4]. Wie wir im letzten Abschnitt gesehen haben ist die Dichte aller Primstellen von K gleich 1, da $\zeta(K,s)$ bei $s=1$ eine einfache Polstelle besitzt! Allgemeiner, läßt man Primstellen aus einer endlich Stellenmenge S weg, gilt immer noch

$$\#S<\infty \implies d_K\Big(\big\{v \;\big|\; v\notin S\big\}\Big) = 1 .$$

Ein analoges Argument zeigt

Satz. *Die Menge aller Primstellen P_v von K, für die K_v nicht isomorph ist zu einem der Körper $\mathbb{Q}_p$, besitzt die K-Dichte Null besitzt. Die komplementäre Menge Σ_K der total zerfallenden Stellen v hat daher die K-Dichte 1*

$$d_K\left(\Big\{v \;\Big|\; K_v\cong\mathbb{Q}_p \text{ für } v|p \text{ und } p\in\mathbb{N}\Big\}\right) = 1 .$$

[4] $\sum_{m\geq 2}\sum_{P\neq 0} N(P)^{-ms}/m \leq [L:K]\sum_{m\geq 2}\sum_p p^{-ms}/m \leq [L:K]\sum_{m\geq 2}\sum_p p^{-ms} \leq [L:K]\sum_p p^{-2}\frac{1}{1-p^{-s}} \leq 2[L:K]\sum_p p^{-2} \leq 2[L:K]\zeta(2)$.

Kapitel 4

Relative Theorie

4.1 Divisoren in Erweiterungskörpern

Für Zahlkörper $\mathbb{Q} \subseteq K \subseteq L$ definiert $i(I) = \mathfrak{o}_L I$ einen ordnungserhaltenden Homomorphismus

$$\boxed{i : \ Div_K \hookrightarrow Div_L}\,.$$

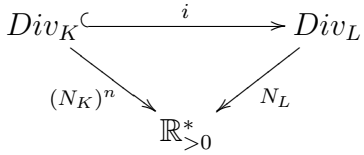
Beachte $i(IJ) = \mathfrak{o}_L IJ = \mathfrak{o}_L \mathfrak{o}_L IJ = \mathfrak{o}_L I \mathfrak{o}_L J = i(I)i(J)$. Wir behaupten

Lemma. *Es gilt* $i(I) \cap K = I$.

Folgerung. i *ist injektiv und* $i(I) \subseteq i(J) \iff I \subseteq J$.

Beweis. $I \subseteq i(I) \cap K$ ist klar. Andererseits gilt $J = i(I) \cap K \in Div_K$ mit $I \subseteq J$. Also $i(I) \subseteq i(J) = \mathfrak{o}_L(K \cap i(I)) \subseteq \mathfrak{o}_L I = i(I)$, und damit $i(I) = i(J)$. Wäre $I \neq J$, kann man durch Multiplikation mit $i(I^{-1})$ obdA $I = \mathfrak{o}_K$ und $\mathfrak{o}_K \subsetneqq J$ mit $\mathfrak{o}_L = i(I) = i(J)$ erreichen. Für jedes $x \in J$ gilt damit $x \in i(J) = \mathfrak{o}_L$. Da x somit einer Ganzheitsgleichung über $\mathbb{Z}$ genügt, folgt wegen $x \in K$ daraus $x \in \mathfrak{o}_L = I$. Also $I = J$ im Widerspruch zur Annahme $I \neq J$. □

Man hat die Normhomomorphismen, und folgendes kommutatives Diagram



Relativnormgesetz. $\boxed{N_L(i(I)) = N_K(I)^n}$ für $n = [L : K]$.

Beweis. $N_L(i(x)) = N_L((x)) = |N_{L/\mathbb{Q}}(x)| = |N_{K/\mathbb{Q}}(x)|^n = N_K((x))^n$ gilt für Hauptideale $I = (x)$ nach 2.3. Dies genügt wegen der Endlichkeit von $Cl(K)$. [Sind die h-ten Potenzen zweier Zahlen in $\mathbb{R}^*_{>0}$ gleich, dann die Zahlen selbst.]

4.2 Primidealzerlegung

Sei $P \neq 0$ ein Primideal in Div_K und sei

$$\boxed{i(P) = P_1^{e_1} \cdots P_g^{e_g}}$$

die Produktzerlegung von $i(P) \subseteq \mathfrak{o}_L$ in Potenzen paarweise verschiedener Primideale P_i in Div_L. ObdA $e_i > 0$. Man nennt P in $\mathfrak{o}_K$ *verzweigt* in L/K, wenn eine der Zahlen $e_i > 1$ ist, ansonsten *unverzweigt*.

Die Teiler von $i(P)$. Wegen $P_\nu | i(P)$ gilt $P \subseteq i(P) \subseteq P_\nu$, und damit $P = P_\nu \cap \mathfrak{o}_K$, da P maximal ist. Ist umgekehrt P' ein Primideal von $\mathfrak{o}_L$ mit $P = P' \cap \mathfrak{o}_K$, dann gilt $\mathfrak{o}_L P \subseteq P'$, also $P' | i(P)$ und damit $P' = P_\nu$ für ein $\nu = 1, .., g$.

Für ein Primideal $P' \in Div_L$ sind also äquivalent

1. $P' = P_i$ für ein $i = 1, .., g$
2. $P' \cap \mathfrak{o}_K = P$.

Insbesondere gilt $\mathfrak{o}_K/P \hookrightarrow \mathfrak{o}_L/P_i$. Das heißt der endliche Restklassenkörper κ_{P_i} ist ein Erweiterungskörper von κ_P.

Die Gradformel. Mit folgenden Bezeichnungen

- $f_i = f_{P_i/P} = dim_{\kappa_P}(\kappa_{P_i})$, die sogenannten Restklassengrade von P
- $e_i = e_{P_i/P}$, die sogenannten Verzweigungsgrade von P
- g, der Zerlegungsgrad von P

gilt die Formel

$$\boxed{[L : K] \; = \; \sum_{i=1}^{g} e_i f_i}\,.$$

Beweis. Wegen $N_L(i(P)) = \prod_i N_L(P_i)^{e_i}$ folgt die Behauptung aus dem Relativnormgesetz und $N_L(P_i) = \#\kappa_{P_i} = (\#\kappa_P)^{f_i} = N_K(P)^{f_i}$. □

Transitivität. Für einen Körperturm $k \subseteq K \subseteq L$ und primes $Q \in Div_k$ gilt offensichtlich durch Einsetzen $i_{L/k}(Q) = i_{L/K}(P^{e_{P/Q}} \ \ldots) = (P_1^{e_{P_1/P}})^{e_{P/Q}} \ \ldots$. Es folgt $e_{P_1/Q} = e_{P_1/P} e_{P/Q}$. Analog gilt $f_{P_1/Q} = f_{P_1/P} f_{P/Q}$.

4.3 Der galoissche Fall

Sei L/K eine galoissche Körpererweiterung mit Galoisgruppe G. Dann gilt

$$\sigma(\mathfrak{o}_L) = \mathfrak{o}_L$$

für alle $\sigma \in G$. [Elemente $x \in L$, welche eine Ganzheitsgleichung über $\mathbb{Z}$ erfüllen, werden auf ebensolche Elemente unter σ abgebildet].

Insbesondere bildet $\sigma \in G$ (Prim)ideale I auf (Prim)ideale $\sigma(I)$ ab. Analog für gebrochene Ideale aus Div_L. Außerdem gilt $\sigma(IJ) = \sigma(I)\sigma(J)$ sowie $\sigma(i(I)) = \sigma(\mathfrak{o}_L I) = \sigma(\mathfrak{o}_L)\sigma(I) = \mathfrak{o}_L I = i(I)$ für alle $I \in Div_K$.

Sei $i(P) = \prod_{i=1}^{g} P_i^{e_i}$ die Faktorierung eines Primideals $P \in Div_K$ in Div_L. Wegen $\sigma(i(P)) = i(P)$ gilt $i(P) = \prod_{i=1}^{g} \sigma(P_i)^{e_i}$. Wegen der Eindeutigkeit der Faktorisierung permutiert $\sigma \in G$ die g Primteiler $P_1, .., P_g$ von $i(P)$. Primideale P_i im selben Orbit haben denselben Exponenten e_i.

Lemma. *Die Galoisgruppe G operiert transitiv auf den Primteilern $P_1, \cdots, P_g$.*

Beweis. Angenommen es gäbe zwei disjunkte nichtleere Orbiten X und Y. Auf Grund des Approximationssatzes findet man ein $x \in \mathfrak{o}_L$ mit $x \in P_i$ für $P_i \in X$ und $x \notin P_j$ für $P_j \in Y$. Dann gilt $P_j \nmid \prod_{\sigma \in G}(\sigma(x)) = (y)$ für $y = \prod_{\sigma \in G} \sigma(x)$. Beachte $y \in \mathbb{Z}$ und $p|y$ wegen $y \in P_i, i \in X$ und $P_i \cap \mathbb{Q} = P \cap \mathbb{Q} = (p)$. Dies liefert wegen $P_j|(p)|(y)$ dann einen Widerspruch. □

Restklassenkörper. Da σ einen Ringisomorphismus $\mathfrak{o}_L/P \to \sigma(\mathfrak{o}_L)/\sigma(P)$ induziert, folgt wegen $\sigma(\mathfrak{o}_L) = \mathfrak{o}_L$ und $\kappa_{\sigma(P)} = \mathfrak{o}_L/\sigma(P)$ daher $\kappa_P \cong \kappa_{\sigma(P)}$. Insbesondere hängt der Restklassengrad $f = f_i$ wegen dem letzten Lemma nicht von i ab. Es folgt

Korollar. *Sei L/K galoissch mit Galoisgruppe G. Sei $P \in Div_K$ prim und P_1 einer der Primteiler von $i(P) \in Div_L$, und G_{P_1} der Stabilisator von P_1 in G (der sogenannten Zerlegungsgruppe). Dann gilt $i(P) = \prod_{\sigma \in G/G_{P_1}} \sigma(P_1)^e$ sowie*

$$\boxed{[L:K] = efg},$$

wobei e der Verzweigungsgrad, f der Restklassenkörpergrad $[\kappa_{P_1} : \kappa_P]$ von P_1 ist, und $g = \#(G/G_{P_1})$.

4.4 Limiten und Tensorprodukte

Sei K/L eine Erweiterung von Zahlkörpern und $P \neq 0$ ein Primideal von $\mathfrak{o}_K$.

Projektive Limiten. Wir betrachten den projektiven Limes $R = \mathfrak{o}_P$

$$\mathfrak{o}_P = \lim_{\nu} R_\nu \quad , \quad R_\nu = \mathfrak{o}_P/(\pi^\nu)$$

bezüglich der kanonischen Abbildungen $\varphi_\nu : R_\nu \to R_{\nu-1}$ definiert durch die Ringhomomorphismen $x \bmod (\pi^\nu) \mapsto x \bmod (\pi^{\nu-1})$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathfrak{o}_P & \xrightarrow{\pi^\nu} & \mathfrak{o}_P & \longrightarrow & R_\nu & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \varphi_\nu} & & \\ 0 & \longrightarrow & \mathfrak{o}_P & \xrightarrow{\pi^{\nu-1}} & \mathfrak{o}_P & \longrightarrow & R_{\nu-1} & \longrightarrow & 0 \end{array}$$

Alternative Beschreibung. Wegen $R_\nu = \mathfrak{o}_K/P^\nu \cong \mathfrak{o}_P/(\pi^\nu)$ hat man

$$\begin{array}{ccccccccc} 0 & \longrightarrow & P^\nu & \hookrightarrow & \mathfrak{o}_K & \longrightarrow & R_\nu & \longrightarrow & 0 \\ & & \downarrow & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \varphi_\nu} & & \\ 0 & \longrightarrow & P^{\nu-1} & \hookrightarrow & \mathfrak{o}_K & \longrightarrow & R_{\nu-1} & \longrightarrow & 0 \end{array}$$

Also $R = \lim_\nu \mathfrak{o}_K/P^\nu$ definiert durch die Ringhomomorphismen $x \bmod P^\nu \mapsto x \bmod P^{\nu-1}$.

Endlich erzeugte R-Moduln. Wegen $\mathfrak{o}_P/(\pi^\nu) \cong \mathfrak{o}_K/P^\nu = R_\nu$ ist die natürliche Abbildung $S \to \lim_\nu S_\nu = S/\pi^\nu S$ ein Isomorphismus für $S = R$ oder Quotienten von R. Da $R = \mathfrak{o}_P$ ein Hauptidealring ist jeder endliche erzeugte R-Modul S isomorph zu einer direkte Summe von Quotienten von R. Es folgt

Lemma. *Für jeden endlich erzeugten $\mathfrak{o}_P$-Modul S ist die kanonische Abbildung $S \to \lim_\nu S_\nu$, $S_\nu = S/\pi^\nu S$ ein Isomorphismus.*

Beispiel. $\mathfrak{o}_L$ ist endlich erzeugt als $\mathbb{Z}$-Modul, daher endlich erzeugt als $\mathfrak{o}_K$-Modul. Also ist der $\mathfrak{o}_P$-Modul $S = \mathfrak{o}_P \otimes_{\mathfrak{o}_K} \mathfrak{o}_L$ endlich erzeugt als $\mathfrak{o}_P$-Modul. Es folgt $S \xrightarrow{\sim} \lim S_\nu$. Beachte, S ist als Tensorprodukt von Ringen sogar ein Ring.

Berechnung von S_ν. Das Tensorprodukt ist rechtsexakt, d.h.: Ist $M \xrightarrow{\varphi} M'$ surjektiver Homomorphismus von R-Moduln, dann ist auch $M \otimes_R N \xrightarrow{\varphi\otimes id_N} M' \otimes_R N$ surjektiv. Es folgt $(M'/M) \otimes_R N \cong (M' \otimes_R N)/(M \otimes_R N)$. Also

$$\begin{array}{ccccccc}
S = \mathfrak{o}_P \otimes_{\mathfrak{o}_K} \mathfrak{o}_L & \xrightarrow{\pi^\nu} & S = \mathfrak{o}_P \otimes_{\mathfrak{o}_K} \mathfrak{o}_L & \longrightarrow & S_\nu = R_\nu \otimes_{\mathfrak{o}_K} \mathfrak{o}_L & \longrightarrow & 0 \\
\downarrow{\scriptstyle \pi} & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \varphi_\nu\otimes id} & & \\
S = \mathfrak{o}_P \otimes_{\mathfrak{o}_K} \mathfrak{o}_L & \xrightarrow{\pi^{\nu-1}} & S = \mathfrak{o}_P \otimes_{\mathfrak{o}_K} \mathfrak{o}_L & \longrightarrow & S_{\nu-1} = R_{\nu-1} \otimes_{\mathfrak{o}_K} \mathfrak{o}_L & \longrightarrow & 0
\end{array}$$

Alternative Beschreibung. Beachte $\mathfrak{o}_K \otimes_{\mathfrak{o}_K} \mathfrak{o}_L = \mathfrak{o}_L$. Das Bild der Abbildung $P^n \otimes_{\mathfrak{o}_K} \mathfrak{o}_L \to \mathfrak{o}_K \otimes_{\mathfrak{o}_K} \mathfrak{o}_L = \mathfrak{o}_L$ gegeben durch $x \otimes_K \lambda \mapsto x\lambda$ ist $\mathfrak{o}_L P^n = i(P^n) \subseteq \mathfrak{o}_L$. Man erhält

$$\begin{array}{ccccccc}
i(P^\nu) & \hookrightarrow & \mathfrak{o}_L & \longrightarrow & S_\nu = R_\nu \otimes_{\mathfrak{o}_K} \mathfrak{o}_L & \longrightarrow & 0 \\
\downarrow & & \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \varphi_\nu\otimes id} & & \\
i(P^{\nu-1}) & \hookrightarrow & \mathfrak{o}_L & \longrightarrow & S_{\nu-1} = R_{\nu-1} \otimes_{\mathfrak{o}_K} \mathfrak{o}_L & \longrightarrow & 0
\end{array}$$

Wegen dem letzten Lemma also

$$S \xrightarrow{\sim} \lim_\nu \mathfrak{o}_L/i(P^\nu)$$

bezüglich der kanonischen Abbildungen $\mathfrak{o}_L/i(P^\nu) \to \mathfrak{o}_L/i(P^{\nu-1})$ induziert von $x \bmod i(P^\nu) \mapsto x \bmod \mathfrak{o}_L/i(P^{\nu-1})$.

Chinesischer Restsatz. Aus $i(P^\nu) = P_1^{\nu e_1} \cdots P_g^{\nu e_g}$ und dem chinesischen Restsatz folgt die Existenz von Ringisomorphismen $S_\nu \cong \prod_{i=1}^g \mathfrak{o}_L/P_i^{\nu e_i}$. Die explizite Beschreibung dieses Isomorphismus hatte uns gezeigt, daß es sich hierbei auch um die kanonischen Projektionen handelt, und daß die Abbildungen $\varphi_\nu : S_\nu \to S_{\nu-1}$ unter dem obigen Isomorphismus das Produkt der entsprechenden kanonischen Abbildungen $\mathfrak{o}_L/P_i^{\nu e_i} \to \mathfrak{o}_L/P_i^{(\nu-1)e_i}$ sind. Also $S \xrightarrow{\sim} \lim_\nu S_\nu \cong \prod_{i=1}^g \lim_\nu(\mathfrak{o}_L/P_i^{\nu e_i}) = \prod_{i=1}^g \mathfrak{o}_{P_i}$. Das heißt $S = \mathfrak{o}_P \otimes_{\mathfrak{o}_K} \mathfrak{o}_L \xrightarrow{\sim} \lim_\nu S_\nu \cong \prod_{i=1}^g \mathfrak{o}_{P_i}$. Der kanonische Ringhomomorphismus

$$\mathfrak{o}_P \otimes_{\mathfrak{o}_K} \mathfrak{o}_L \xrightarrow{\sim} \prod_{i=1}^g \mathfrak{o}_{P_i}$$

induziert von den kanonischen Abbildungen $\mathfrak{o}_P \hookrightarrow \mathfrak{o}_{P_i}$ und den natürlichen Abbildungen $\mathfrak{o}_L \hookrightarrow \mathfrak{o}_{P_i}$ ist daher ein Isomorphismus!

4.4.1 Körperfall

Bezüglich der Inklusionen $K \hookrightarrow L \hookrightarrow L_{P_1}$ besitzt jede Cauchyfolge aus $(K, |.|_P)$ einen Limes in der Komplettierung L_{P_1}. Man erhält eine Einbettung $K_P \hookrightarrow L_{P_1}$. Anderseits hat man die natürliche Einbettung $L \to L_{P_1}$. Zusammen definiert dies einen natürlichen Ringhomomorphismus

$$K_P \otimes_K L \to \prod_{i=1}^{g} L_{P_i} \ .$$

Wegen dem Approximationssatz ist das Bild von L dicht in $\bigoplus_{i=1}^{g} L_{P_i}$. Also erzeugen $Bild(1 \otimes_K L)$ und $\prod_{i=1}^{g} \mathfrak{o}_{P_i}$ die rechte Seite $\prod_{i=1}^{g} L_{P_i}$. Aus der Surjektivität $\mathfrak{o}_P \otimes_{\mathfrak{o}_K} \mathfrak{o}_L \twoheadrightarrow \prod_{i=1}^{g} \mathfrak{o}_{P_i}$ folgt daher die Surjektivität

$$K_P \otimes_K L \ \twoheadrightarrow \ \prod_{i=1}^{g} L_{P_i} \ .$$

Injektivität. Wir wollen nun zeigen, daß diese Abbildung injektiv ist. Dazu können wir L durch seine galoissche Hülle $\tilde{L}$ ersetzen, also obdA annehmen L/K sei galoissch mit Galoisgruppe G, da $K_P, K, L, \tilde{L}$ Körper sind.

4.4.2 Der galoissche Fall

Die $\sigma \in G_{P_1}$ definieren stetige Körperautomorphismen von $(L, |.|_{P_1})$, welche sich zu (verschiedenen) Automorphismen von L_{P_1}/K_{P_1} fortsetzen. Also gilt $\#G_{P_1} \leq dim_{K_P}(L_{P_1})$ mit Gleichheit nur im Fall $L_{P_1}^{G_{P_1}} = K_P$ (Artin's Lemma). Aber Gleichheit tritt genau dann ein, wenn L_{P_1}/K_P galoissch mit Galoisgruppe G_{P_1} ist. Andererseits: Da G transitiv auf den Primidealen $P_1, .., P_g$ operiert, gilt $L_{P_i} \cong L_{P_1}$ für alle $i = 1, .., g$ und somit die linke Gleichung

$$\#G = g \cdot \#G_{P_1} \leq dim_{K_P}(\prod_{i=1}^{g} L_{P_i}) \leq dim_{K_P}(K_P \otimes_K L) = [L : K] \ .$$

Wegen $g\#G_{P_1} = \#G = [L : K]$ hat man also in allen obigen Ungleichungen Gleichheit. Also $dim_{K_P}(K_P \otimes L) = dim_{K_P}(\prod_{i=1}^{g} L_{P_i})$, und somit folgt die Injektivität der betrachteten Abbildung aus Dimensionsgründen. Zusätzlich haben wir gezeigt

$$\boxed{L_{P_1}^{G_{P_1}} = K_P} \ .$$

Zurück zum allgemeinen Fall. Wir fassen zusammen

Satz. *Sei L/K eine Erweiterung von Zahlkörpern und $i(P) = \prod_{i=1}^{g} P_i^{e_i}$. Dann induzieren die kanonischen Abbildungen Ringisomorphismen*

$$\boxed{K_P \otimes_K L \;\cong\; \prod_{i=1}^{g} L_{P_i} \quad , \quad \mathfrak{o}_P \otimes_{\mathfrak{o}_K} \mathfrak{o}_L \;\cong\; \prod_{i=1}^{g} \mathfrak{o}_{P_i}} \; .$$

Ist L/K galoissch mit Galoisgruppe G und dem Stabilisator $G_{P_1} \subseteq G$ von P_1, dann ist die Erweiterung L_{P_1}/K_P galoissch mit Galoisgruppe G_{P_1}.

Bemerkung. Der erste Aussage des letzten Satzes schreiben wir kurz in der Form

$$\boxed{K_v \otimes_K L \cong \prod_{w|v} L_w} \; .$$

Diese Schreibweise zeigt (im Fall $K = \mathbb{Q}$ und $K_v = \mathbb{R}$, dann aber auch allgemein) die Analogie zur archimedischen Stelle $\mathbb{A}_\infty = \mathbb{R} \otimes_K L = \prod_{w|\infty} L_w$.

Bemerkung. In Analogie zur archimedischen Stelle kann man das umformulieren. Sei $L = K[X]/(f(X))$ nach dem Satz vom primitiven Element. Dann gilt $K_P \otimes_K L = K_P[X]/(f(X)) \cong \prod_i L_i$ mit $L_i = K_P[x]/(f_i(X))$ wegen des chinesischen Restsatzes, wenn $f(X) = \prod_i f_i(X)$ die Zerlegung des über K irreduziblen Polynoms f in irreduzible Faktoren $f_i(X)$ über dem Erweiterungskörper K_P ist. Die Zahl der Körper L_i resp. irreduziblen Faktoren $f_i(X)$ ist daher genau der Zerlegungsgrad g, und bei geeigneter Nummerierung gilt

$$L_{P_i} \cong K_P[x]/(f_i(x)) \; .$$

4.5 Der Frobenius

Sei L/K galoissch mit Galoisgruppe G und dem Stabilisator $G_{P_1} \subseteq G$ von P_1. Dann ist die Erweiterung L_{P_1}/K_P galoissch mit Galoisgruppe G_{P_1}. Jedes $\sigma \in G_{P_1}$ operiert normerhaltend auf L_{P_1}. Insbesondere bleiben die Ideale (π_1^n) und $\mathfrak{o}_{P_1}$ invariant unter σ. Dies induziert eine Operation von G_{P_1} auf $\kappa_{P_1} = \mathfrak{o}_L/(\pi_1)$. Man erhält also kommutative Diagramme von G_{P_1}-Moduln

$$\begin{array}{ccc} \mathfrak{o}_L & \twoheadrightarrow & \kappa_{P_1} \\ \uparrow & & \uparrow \\ \mathfrak{o}_K & \twoheadrightarrow & \kappa_P \end{array} \qquad \begin{array}{ccc} \mathfrak{o}_{P_1} & \twoheadrightarrow & \kappa_{P_1} \\ \uparrow & & \uparrow \\ \mathfrak{o}_P & \twoheadrightarrow & \kappa_P \end{array}$$

und dies induziert einen Gruppenhomomorphismus

$$\boxed{G_{P_1} \twoheadrightarrow Gal(\kappa_{P_1}/\kappa_P)}\,.$$

Lemma. *Dieser Homomorphismus ist surjektiv.*

Der Kern dieses Homomorphismus ist die sogenannte *Verzweigungsgruppe* I.

Zur Erinnerung. Die Gruppe G_{P_1} hat die Ordnung ef. Die Körpererweiterung der endlichen Körper κ_{P_1}/κ_P ist vom Grad f. Also gilt bekanntlich

$$Gal(\kappa_{P_1}/\kappa_P) \cong \mathbb{Z}/f\mathbb{Z}\,.$$

Somit ist die Verzweigungsgruppe I ein Normalteiler von G_{P_1} der Ordnung e.

Diagram. Für den Fixkörper $(L_{P_1})^I$ folgt

$$\begin{array}{ccc} L_{P_1} & & \\ \Big| e & & \\ (L_{P_1})^I & & \kappa_{P_1} \\ \Big| f & & \Big| f \\ K_P & & \kappa_P \end{array}$$

mit $Gal((L_{P_1})^I/K_P) \cong Gal(\kappa_{P_1}/\kappa_P) \cong \mathbb{Z}/f\mathbb{Z}$.

Sei $q = \#\kappa_P$. Die Galoisgruppe $Gal(\kappa_{P_1}/\kappa_P)$ wird von dem Automorphismus $x \mapsto x^q$ des Körpers κ_{P_1} erzeugt. Die inverse Substitution nennen wir den geometrischen **Frobenius**

$$\boxed{F_{P_1} \in Gal(\kappa_{P_1}/\kappa_P)}\,.$$

Sein Urbild in G_{P_1} ist eine wohldefinierte I-Nebenklasse in G_{P_1}, kurz:

$$F_{P_1} \cdot I \subseteq G_{P_1} \subseteq G\,.$$

Beweis des Lemmas. Wir müßen zeigen: unter den Automorphismen $\sigma \in G_{P_1}$ invariante Elemente aus $\kappa_{P_1}^*$ liegen in κ_P^*. Wegen $(L_{P_1})^{G_{P_1}} = K_P$ genügt dazu das Lemma des nächsten Abschnitts

4.6 Der lokale Einheitensatz

Lemma. *Sei $\mu^p = \mu^p(L_{P_1})$ die Gruppe der Einheitswurzeln mit zu p teilerfremder Ordnung in L_{P_1}. Dann gibt es eine $G_{L_{P_1}}$-invariante Zerlegung*

$$\boxed{\mathfrak{o}_{P_1}^* \;\cong\; \mu^p \times U_{P_1}^1}\,.$$

$U_{P_1}^1 = \{x \in \mathfrak{o}_{P_1} \mid x \in 1 + (\pi_1)\}$ ist die Untergruppe der 1-Einheiten in $\mathfrak{o}_{P_1}^*$. Der Restklassenhomomorphismus π induziert einen Isomorphismus $\mu^p(L_{P_1}) \cong \kappa_{P_1}^*$. Die G_{P_1}-äquivariante Umkehrabbildung

$$t : \kappa_{P_1}^* \cong \mu^p$$

nennt man den Teichmüller Lift.

Beweis. Sei $q = \#\kappa_{P_1}$, $a \in \mathfrak{o}_{P_1}^*$ mit Restklasse $\overline{a} = \pi(a)$ in $\kappa_{P_1}^*$. Beachte $\overline{a}^q = \overline{a}$. Für $X = \pi^{-1}(\overline{a}) \subseteq \mathfrak{o}_{P_1}^*$ gilt daher für die Abbildung $F(y) = y^q$

$$F : X \to X\ .$$

F ist kontraktiv. Wegen $|x^q - y^q|_{P_1} = |x - y|_{P_1}|x^{q-1} + yx^{q-2} + \cdots + y^{q-1}|_{P_1}$ genügt dazu, daß der P_1-adische Betrag der folgenden Zahl < 1 ist

$$x^{q-1} + yx^{q-2} + \cdots + y^{q-1} \equiv a^{q-1} + \cdots + a^{q-1} \equiv\ qa^{q-1} \mod\ (\pi_1)\,.$$

Somit besitzt F nach dem Banachschen Fixpunktsatz einen eindeutig bestimmten Fixpunkt. Dieser Fixpunkt ist eine $(q-1)$-ste Einheitswurzel, also der gesuchte Teichmüller-Repräsentant $t(\overline{a})$.

Bestimmung von μ^p. Sei schließlich $a \in \mu^p$ und obdA $\overline{a} = 1$. Dann gilt $a^N = 1$ mit $(N, q) = 1$. Also $a = F(a^u)$ für $1 = uq + vN$. Somit gilt $u^r \equiv 1(N)$ für geeignetes r, und damit $a = F^r(a)$, wegen $(u, N) = 1$. Als Fixpunkt der kontraktiven Abbildung F^r ist a eindeutig bestimmt in X. Also $a = 1$. □

4.7 Unverzweigte Stellen

Das fundamentale Lemma. *Sei w eine nicht archimedische und in L/K (obdA galoissch) unverzweigte Stelle, dann gilt für die Norm $N_{L_v/K_w}(x) = \prod_{\sigma\in G_v}\sigma(x)$*

$$\boxed{N_{L_v/K_w}(\mathfrak{o}_v^*) = \mathfrak{o}_w^*}\,.$$

Beweis. Wir wählen ein Primelement $\pi_K \in K$, welches das maximale Ideal von $\mathfrak{o}_w$ erzeugt. Da die Erweiterung L/K unverzweigt ist, ist $\pi_K = \pi_L$ auch ein Erzeuger des maximalen Ideals von $\mathfrak{o}_v$.

Die lokale Einheitengruppe $\mathfrak{o}_K^*$ besitzt eine absteigende Kette von Untergruppen

$$\mathfrak{o}_K^* \supseteq 1+\pi_K\mathfrak{o}_w \supseteq 1+\pi_K^2\mathfrak{o}_w \supseteq \cdots\,.$$

Analoges gilt für $\mathfrak{o}_v^*$. Die sukzessiven Quotienten sind $\mathfrak{o}_w^*/(1+\pi_K\mathfrak{o}_w) \cong \kappa_w^*$ sowie $(1+\pi_w^{m-1}\mathfrak{o}_w)/(1+\pi_w^m\mathfrak{o}_w) \cong \mathfrak{o}_w/\pi_w\mathfrak{o}_w = \kappa_w$. Letzteres kommt von den Bijektionen $(1+x\pi_w^{m-1})$ mod $(1+\pi_w^m\mathfrak{o}_w) \mapsto x$ mod $\pi_w\mathfrak{o}_w$. Dies sind Homomorphismen wegen

$$(1+x\pi_w^{m-1})(1+y\pi_w^{m-1}) \in 1+(x+y)\pi_w^{m-1}+\pi_w^m\mathfrak{o}_w\,.$$

Somit schreibt sich jedes $x \in \mathfrak{o}_w^*$ als ein konvergentes Produkt

$$x = \lim_{m\to\infty} \zeta\cdot\prod_{i=1}^{m}(1+x_i\pi^i)$$

für gewisse $x_i \in \mathfrak{o}_w$. Hierbei ist ζ ein Teichmüller Repräsent des Bildes von x im Restklassenkörper κ_w. Man zeigt nun leicht durch Induktion nach m die Existenz von $\tilde{\zeta}$ und $y_m \in \mathfrak{o}_v$ mit $N(\tilde{\zeta}\cdot\prod_{i=1}^m(1+\pi_w y_i)) = \lim_{m\to\infty}\ \zeta\cdot\prod_{i=1}^m(1+x_i\pi^i)$. Der Limes $y \in \mathfrak{o}_v^*$ ist das gesuchte Element mit $N(y) = x$.

Induktionsbeginn. Zur Konstruktion von $\tilde{\zeta}$ mit $N(\tilde{\zeta}) = \zeta$ genügt, daß die Norm $N : \kappa_v^* \to \kappa_w^*$ surjektiv ist. [Der Kern der Norm ist gegeben durch die Gleichung $X^{1+q+\cdots+q^{n-1}} = 1$, enthält also höchsten $(q^n-1)/(q-1)$ Elemente. Wegen $\#\kappa_v^* = q^n-1$ folgt $\#N(\kappa_v^*) \geq q-1 \geq \#(\kappa_w^*)$].

Der Induktionsschritt auf m führt auf eine Lösung der Gleichung $S(y_m) = b_m$ für $b_m \in \kappa_w$, welche lösbar ist, da die Spur $S = Sp_{\kappa_v/\kappa_w}$ surjektiv ist. [Der Kern der Spur ist gegeben durch die Gleichung $X + X^q + \cdots X^{q^{n-1}} = 0$, enthält also höchstens q^{n-1} Elemente. Also $dim_{\kappa_w}(Kern(S)) \leq n-1$. Die Spur $S : \kappa_v \to \kappa_w$ ist κ_w-linear, also surjektiv wegen $dim_{\kappa_w}(Bild(S)) \geq 1$.] □

Analog zeigt man

Lemma. *Für einen nicht archimedischen lokalen Körper K_w und $r \geq v_{P_w}(q)+1$ induziert Potenzierung mit $q \in \mathbb{N}$ einen Isomorphismus*

$$1+\pi_w^r \mathfrak{o}_w \xrightarrow[\sim]{q-Potenz} 1+\pi_w^r q\mathfrak{o}_w \ .$$

Insbesondere bildet dann $x \mapsto x^q$ offene Teilmengen von K_w^* auf offene Teilmengen von K_w^* ab, und die Gruppe aller Einheitswurzel von K_w^* ist endlich[1].

Beweis. Wegen $q \in \pi_K^s \mathfrak{o}_w^*$ und $x \in \mathfrak{o}_w$ gilt $(1+x\pi_w^r)^q \equiv 1+xq\pi_K^r \mod xq\pi_w^{r+1}\mathfrak{o}_w$ im Fall $s+1 \leq r$ (Binomische Entwicklung). Für $r \geq s+1$ zeigt dies $\mu_q(K_w) \cap (1+\pi_w^r\mathfrak{o}_w) = 1$ (Injektivität), und obige Produktdarstellung liefert die Surjektivität. □

4.8 Verzweigte Stellen

Die nilpotenten Elemente eines kommutativen Rings R bilden ein Ideal, das Nilradikal N des Rings. Ringhomomorphismen $R \to S$ bildet nilpotente Elemente auf nilpotente Elemente ab. Teilt man R durch sein Nilradikal N, so erhält man einen reduzierten (d.h. nilpotenzfreien) Ring $R_{red} = R/N$.

Beispiel. Ist P ein Primideal in $\mathfrak{o}_K$, dann ist $R_\nu = \mathfrak{o}_K/(P^\nu)$ nur für $\nu = 1$ reduziert. Genauer: Das Nilradikal ist

$$N = P/P^\nu$$

und $(R_\nu)_{red} = R_1 = \kappa_P$.

Kriterium. Sei L/K ein Erweiterung von Zahlkörpern und sei P prim in Div_K. Der Restklassenring $\mathfrak{o}_L/i(P) \cong \prod_{i=1}^g \mathfrak{o}_L/P_i^{e_i}$ ist genau dann reduziert, wenn das Primideal P in der Erweiterung L/K unverzweigt ist.

Lemma. *Nur endlich viele Primideale $P \in Div_K$ sind verzweigt in L/K.*

Beweis. Ist P verzweigt in L/K und $(p) = P \cap \mathbb{Z}$, dann ist p verzweigt in $L/\mathbb{Q}$. Wegen der Transitivität der Verzweigungszahlen ist obdA $K = \mathbb{Q}$. Für ein ganzes

[1] $1+\pi_w^r\mathfrak{o}_w$ enthält keine p-ten Einheitswurzeln mehr. Als bildet sich die Gruppe der der p-Potenz Einheitswurzeln injektiv ab in die endliche Gruppe $\mathfrak{o}_w^*/(1+\pi_w^r\mathfrak{o}_w)$.

α mit $L = \mathbb{Q}(\alpha)$ und Minimalpolynom $f(x) \in \mathbb{Z}[x]$ ist $N = [\mathfrak{o}_L : \mathfrak{o}_K[\alpha]] < \infty$ nach 2.1. Sei $M \in \mathbb{Z}$ der Nenner von $g, h \in \mathbb{Q}[x]$ mit $gf + hf' = 1$. Für $p \nmid NM$ ist $\mathfrak{o}_L/p$ reduziert und damit p unverzweigt in $L/\mathbb{Q}$. □

Variante. Sei $f(x) \in \mathfrak{o}_K[x]$ Ganzheitspolynom und $T = \mathfrak{o}_K[x]/(f) \hookrightarrow \mathfrak{o}_L$ habe endlichen Index in dem Ring $\mathfrak{o}_L$ (gleichbedeutend $L = Quot(T)$). Für eine Primstelle w von $\mathfrak{o}_K$ erhalten wir eine induzierte endliche Ringerweiterung ι, sowie

$$\mathfrak{o}_w \subseteq \mathfrak{o}_w[x]/(f(x)) = T \otimes_{\mathfrak{o}_K} \mathfrak{o}_w \xrightarrow{\iota} \mathfrak{o}_L \otimes_{\mathfrak{o}_K} \mathfrak{o}_w = \prod_{v|w} \mathfrak{o}_v \overset{pr_v}{\twoheadrightarrow} \mathfrak{o}_v$$

ι ist injektiv (betrachte die analoge Abbildung für die Körper!).

Das Bild von $pr_v \circ \iota$. Für $x_v \in \mathfrak{o}_v$, welches nicht im Bild von $pr_v \circ \iota$ liegt, gibt es $r, s \in R = \mathfrak{o}_w[x]/(f(x))$ mit $x = r/s$ (denn $L = Quot(T)$). Die Klasse $[r]$ von $r = xs$ in $R/(s)$ ist dann von Null verschieden $[r] \neq 0$ [Andernfalls gäbe es $\tilde{r} \in R$ mit $xs = \tilde{r}s$ in $\mathfrak{o}_v$. Da $\mathfrak{o}_v$ nullteilerfrei ist, wäre $x = \tilde{r}$ im Widerspruch zur Annahme.] x erfüllt eine Ganzheitsgleichung $x^n + .. = 0$ über R. Multiplikation mit s^n gibt $r^n + s \cdot [...] = 0$ in $\mathfrak{o}_v$, und damit wegen der Injektivität von ι auch in R. Also $[r]^n = 0$ in $R/(s)$, d.h. $R/(s)$ besitzt nilpotente Elemente. Das Ideal $(s) \cap \mathfrak{o}_w$ ist verschieden von $\mathfrak{o}_w$, da sonst $(s) = R$ und damit $[r] = 0$. Also $(\pi_w) \subseteq (s) \cap \mathfrak{o}_w$, und damit $\pi_w \in (s) \subseteq R$. Damit ist erst recht die Restklasse von r in $R/(\pi_w) = \kappa_w[x]/\overline{f}(x)$ ungleich Null (und ist nilpotent modulo (s). In der Situation des nächsten Lemmas ist so etwas unmöglich. Unter den Bedinungen des Lemmas ist also $pr_v \circ \iota$ surjektiv und $\mathfrak{o}_v$ ein Quotient von R, insbesondere also $\mathfrak{o}_v/P_v^{e_v}$ ein Quotient von $\overline{R} = R/(\pi_w)$. Das Lemma erzwingt dann die Reduziertheit mit der Konsequenz $e_v = 1$.

Korollar. *Sei $f(x) \in \mathfrak{o}_X[x]$ ein Ganzheitspolynom, dessen Restklassenpolynom $\overline{f}(x) \in \kappa_w[x]$ keine doppelten Nullstellen besitzt, und es gelte $K[x]/f(x) = L$. Dann ist w unverzweigt in L/K.*

Lemma. *Für ein Ganzheitspolynom $f(x) \in \mathfrak{o}_K[x]$, dessen Restklassenpolynom $\overline{f}(x) \in \kappa_w[x]$ keine doppelten Nullstellen besitzt, ist jeder Quotientenring von $\overline{R} = \kappa_w[x]/\overline{f}(x)$ reduziert.*

Beweis. Aus der Annahme folgt, daß die κ_w-Algebra $\overline{R} = \kappa_w[x]/\overline{f}(x)$ ein Produkt von Körpern ist. Dann ist aber jeder Quotientenring von $\overline{R}$ ein Produkt von Körpern, also reduziert. □

Wir benutzen diese Variante nur in dem folgendem Spezialfall

Abhyankars Lemma. *Sei* $L = K(\alpha^{1/q})$. *Für* $w \nmid q$ *sowie* $\alpha \in \mathfrak{o}_w^*$ *ist dann* w *unverzweigt in* L/K.

Beweis. Die Reduktion $\overline{f} \in \kappa_w[x]$ des Polynoms $f(x) = X^q - \alpha$ hat ist separabel wegen

$$\overline{f}' = q \cdot x^{q-1} \neq 0 \; .$$

Wegen $\overline{\alpha} \neq 0$ ist daher $ggT(\overline{f}, \overline{f}') = 1$. Benutze dann Korollar 4.8. □

Appendix

Eine quadratische Form. Beachte $Sp_{L/\mathbb{Q}}(x) = \sum_{i=1}^{n} x^{(i)} \in \mathbb{Z}$ für $x \in \mathfrak{o}_L$. Somit definiert $Sp_{L/\mathbb{Q}}(xy)$ eine $\mathbb{Z}$-Bilinearform auf dem $\mathbb{Z}$-Gitter $\mathfrak{o}_L$. Die zugehörige ganzzahlige symmetrische Matrix $S = (Sp_{L/\mathbb{Q}}(\omega_i\omega_j))$ hat die Determinante

$$det(S) = det \begin{pmatrix} \omega_1^{(1)} & .. & \omega_1^{(n)} \\ . & . & . \\ & & \\ . & . & . \\ \omega_n^{(1)} & .. & \omega_n^{(n)} \end{pmatrix} \begin{pmatrix} \omega_1^{(1)} & .. & \omega_n^{(1)} \\ . & . & . \\ & & \\ . & . & . \\ \omega_1^{(n)} & .. & \omega_n^{(n)} \end{pmatrix} = \pm D_{L/\mathbb{Q}} \; .$$

Für $K = \mathbb{Q}$ gilt $Sp_{L/\mathbb{Q}} : \mathfrak{o}_L \to \mathfrak{o}_{\tilde{L}}$ (für die Galoishülle $\tilde{L}$). Nilpotente Elemente von $\mathfrak{o}_L/p$ werden daher von $Sp_{L/\mathbb{Q}}$ auf nilpotente Elemente in $\mathfrak{o}_{\tilde{L}}/p$ abgebildet; da die Werte aber bereits in $\mathbb{Z}/p\mathbb{Z}$ liegen, somit auf Null. Das zeigt, daß die Form $Sp_{L/\mathbb{Q}}(xy)$ auf $\mathfrak{o}_L/p$ eine ausgeartete $\mathbb{F}_p$-Bilinearform mit Werten in $\mathbb{F}_p$ induziert, wenn $\mathfrak{o}_L/p$ nicht reduziert ist. Es folgt $p|D_{L/\mathbb{Q}}$, falls p in $L/\mathbb{Q}$ verzweigt.

Übungsaufgabe. Zeige umgekehrt, daß jede Primzahl $p|D_{L/\mathbb{Q}}$ in $L/\mathbb{Q}$ verzweigt.

Kapitel 5

Das Yoga der zerfallenden Stellen

5.1 Die zerfallenden Stellen $\Sigma_{L/K}$

Man sagt, eine Stelle w eines Zahlkörpers K zerfällt in der Erweiterung L/K, wenn eine der folgenden äquivalenten Eigenschaften erfüllt ist

1. $L \otimes_K K_w$ und $\prod_{v|w} K_w$ sind isomorph als Ringe.
2. $L_v = K_w$ für alle $v|w$
3. Über w liegen genau $g = [L : K]$ Stellen v von L.

Sei $\Sigma_{L/K}$ die Menge der in L/K zerfallenden Stellen von K.

Vererbung. Gegeben seien Zahlkörper $K \subseteq K' \subseteq L$. Für $w \in \Sigma_{L/K}$ und Stellen $v|w'|w$ gilt wegen $L_v = K_w$ (siehe 2. oben) sofort $L_v = K_{w'}$ und $K_{w'} = K_w$. Dies zeigt die Implikation $\Longrightarrow$

$$\boxed{w \in \Sigma_{L/K} \iff w' \in \Sigma_{L/K'} \ (\forall w'|w) \ , \ w \in \Sigma_{L'/K}} \ .$$

Die Rückrichtung folgt aus $L \otimes_K K_w \cong L \otimes_{K'} K' \otimes K_w \cong L \otimes_{K'} \prod_{w'|w} K_w \cong \prod_{w'|w} \prod_{v|w'} K_w$ wegen $K_{w'} = K_w$ und $L_v = K_{w'}$. (Benutze dann 1. von oben).

Isomorphe Erweiterungen. Angenommen w zerfällt in L/K. Ist $L' \cong L$ ein K-Isomorphismus, dann gilt ebenfalls $L' \otimes_K K_w \cong \prod K_w$. Also zerfällt w auch in L'/K. Also gilt

$$\Sigma_{L/K} = \Sigma_{L'/K} \ .$$

Komposita. Zerfällt w in zwei Erweiterungen L/K und L'/K, dann auch in LL'/K. [Benutze: Das Kompositum ist ein Summand von $L \otimes_K L'$. Es gilt $K_w \otimes_K (L \otimes_K L') = (K_w \otimes_K L) \otimes_K L' = (\prod K_w) \otimes_K L' = \prod \prod K_w$.] Die Umkehrung folgt aus den oben formulierten Vererbungseigenschaften. Somit gilt

$$\boxed{\Sigma_{LL'/K} = \Sigma_{L/K} \cap \Sigma_{L'/K}} \ .$$

Galoishülle. Aus den beiden letzten Bemerkungen folgt für die Galoishülle $\tilde{L}/K$ von L/K, welche ein Kompositum zu L/K isomorpher Erweiterungen L'/K ist

$$\boxed{\Sigma_{\tilde{L}/K} = \Sigma_{L/K}} \ .$$

5.2 Der Dichtesatz

Satz. *Sei L/K galoissch. Dann gilt für die K-Dichte (siehe 3.7)*

$$\boxed{d_K(\Sigma_{L/K}) = [L:K]^{-1}} .$$

Beweis. Sei $S = S_{L/K}$ die endliche Menge der archimedischen und in L/K verzweigten Stellen w von K. Da L/K galoissch ist, gilt für unverzweigte Stellen daher

$$w \notin \Sigma_{L/K} \Longleftrightarrow \forall\, v|w\ f_{v|w} \geq 2 .$$

Außerdem

$$w \in \Sigma_{L/K} \Longleftrightarrow N(P_w) = N(P_v)\ ,\ \forall\, v|w \iff f_{v|w} = 1\ \ ,\ \forall\, v|w\ \ .$$

Da obendrein jedes $w \in \Sigma_{L/K}$ genau $[L:K]$ Fortsetzung besitzt, gilt für das Produkt über die nichtarchimedischen Stellen aus $\Sigma_{L(K}$ daher

$$\prod_{v|w, w\in\Sigma_{L/K}} (1 - N(P_v)^{-s})^{-1} = \prod_{w\in\Sigma_{L/K}} (1 - N(P_w)^{-s})^{-[L:K]} .$$

Nach der Vererbungseigenschaft 5.1 enthalten links die Stellen $v|w$ mit $w \in \Sigma_{L/K}$ alle total zerfallenden Stellen $v \in \Sigma_L$ im Sinne von Satz 3.7. Nach Satz 3.7 hat daher die linke Seite einen einfachen Pol bei $s = 1$. Bildet man daher von obiger Identität den Logarithmus und berechnet die Dichte, folgt sofort die Behauptung. □

Korollar. *Für L/K (nicht notwendig galoissch) gilt*

$$\boxed{d_K(\Sigma_{L/K}) = 1 \implies L = K} .$$

Beweis. Für die Galoishülle $\tilde{L}/K$ folgt $d_K(\Sigma_{\tilde{L}/K}) = 1$ wegen $\Sigma_{\tilde{L}/K} = \Sigma_{L/K}$. Der letzte Satz zeigt daher $[\tilde{L}:K] = 1$, und somit $L = K$. □

Proposition. *(1) Die Zuordnung*

$$\boxed{\text{Galoiserweiterungen } L/K \;\; \mapsto \;\; \Sigma_{L/K}}$$

definiert eine Injektion der Isomorphieklassen von Galoiserweiterungen L/K in die Teilmengen der Primideale von K (modulo Mengen der K-Dichte Null).

(2) Für galoissche Erweiterungen L_1/K und L_2/K gilt

$$\boxed{L_1 \subseteq L_2 \Longleftrightarrow \Sigma_{L_2/K} \subseteq \Sigma_{L_1/K}}\,.$$

Beweis. (1) Angenommen $\Sigma_{L/K}$ und $\Sigma_{L'/K}$ stimmen überein, dann gilt dies auch für $\Sigma_{L/K}$ und $\Sigma_{LL'/K} = \Sigma_{L/K} \cap \Sigma_{L'/K}$ (bis auf Mengen der K-Dichte Null). Da LL'/K und L/K galoissch sind, folgt daher aus dem Dichtesatz $[LL' : K]^{-1} = [L : K]^{-1}$ und damit $[LL' : L] = 1$ oder $L = L'$. Aussage (2) zeigt man analog. □

Korollar. *Sei L/K galoissch und S eine endliche Menge von Stellen von K, welche alle archimedischen und verzweigten Stellen enthalte. Dann erzeugen die Frobeniuselemente $F_v, v|w$ für $w \notin S$ die Galoisgruppe $G = Gal(L/K)$*

$$\boxed{\langle F_v, v \nmid S \rangle = Gal(L/K)}\,.$$

Beweis. Sei H die von den $F_v, v \notin S$ erzeugte Untergruppe. Jede Stelle von L^H/K, die nicht über S liegt, zerfällt. Aus dem letzten Korollar folgt $L^H = K$. Also $H = Gal(L/K)$. □

5.3 Die automorphe Menge $\mathcal{N}_{L/K} \supseteq \Sigma_{L/K}$

Lemma. *Sei L/K eine galoissch und $S = S_{L/K}$ die endliche Menge der archimedischen und in L/K verzweigten Stellen w von K. Für $w \notin S_{S/K}$ sind dann äquivalent*

(1) $w \in \Sigma_{L/K}$

(2) $ord(F_v) = 1$ *oder* $[L_v : K_w] = 1$.

(3) π_w *ist im Bild der Norm* $N : L_w^* := \prod_{v|w} L_v^* \to K_w^*$.

(4) π_w *ist im Bild der Norm* $N_{L^v/K_w} : L_v^* \to K_w^*$.

(5) $N : L_w^* := \prod_{v|w} L_v^* \to K_w^*$ *ist surjektiv.*

Beweis. Die Eigenschaften (1) und (2) respektive (3) und (4) sind offensichtlich äquivalent. Angenommen es gilt (2). Aus $ord(F_v) = 1$ folgt dann $L_v^* \cong K_w^*$ und damit (3) und (4). Angenommen es gilt (3). Wegen $w \notin S_{L/K}$ gilt $N(L_w^*) = N(\pi_w^{\mathbb{Z}} \cdot \mathfrak{o}_v^*) = \pi_w^{[L_v:K_w]\mathbb{Z}} \cdot N(\mathfrak{o}_v^*) \subseteq \pi_w^{[L_v:K_w]\mathbb{Z}} \cdot \mathfrak{o}_w^*$. Gilt daher (3) oder äquivalent dazu (4), d.h. $\pi_w \in N(L_w^*)$, so folgt für den Exponenten $[L_v : K_w] = 1$, d.h. (2). Die Äquivalenz von (4)mund (5) folgt aus dem fundamentalen Lemma. □

Aus den obigen Äquivalenzen folgt insbesondere

$$\boxed{w \in \Sigma_{L/K} \Longrightarrow \pi_w \in K^* \cdot N(\mathbb{I}_L)}\,.$$

Bezeichne wir die Stellen w von K mit $\pi_w \in K^* N(\mathbb{I}_L)$ mit

$$\mathcal{N}_{L/K} \;=\; \left\{ w \;\middle|\; \pi_w \in K^* \cdot N(\mathbb{I}_L) \right\},$$

so bedeutet dies

$$\boxed{\mathcal{N}_{L/K} \supseteq \Sigma_{L/K}}\,.$$

Also nach dem Dichtesatz $d_K(\mathcal{N}_{L/K}) \geq [L : K]^{-1}$.

5.4 Der Normenindex

Satz. *Sei L/K galoissch und die Ordnung m der Gruppe $E = \mathbb{I}_K/(K^* N(\mathbb{I}_L))$ sei endlich, dann gilt*

$$\boxed{m \leq [L:K]}\,.$$

Zusatz. *Gilt $m = [L:K]$, dann auch $d_K(\mathcal{N}_{L/K}) = [L:K]^{-1}$ oder*

$$\boxed{d_K(\mathcal{N}_{L/K}) = d_K(\Sigma_{L/K})}\,.$$

Beweis. Seien $\chi_1, ..., \chi_m \in E^D$ die Charaktere von E, aufgefaßt als Charaktere von C_K. Nach Annahme ist E endlich, also $E^D \cong E$ (siehe 1.3). Wähle S endlich und genügend groß , so daß S den Führer (siehe 2.10) der Charaktere $\chi_i \in E^D$ enthält. Dann gilt asymptotisch[1] bei $s \to 1^+$

$$-\sum_{\chi\in E^D}^{m} \log(Z(K,\chi,s)) \;\sim\; \sum_{\chi\in E^D}\sum_{w\notin S} \frac{\chi(P_w)}{N(P_w)^s} \;\sim\; m \sum_{w\notin S, \pi_w \in K^* N(\mathbb{I}_L)} \frac{1}{N(P_w)^s}\,,$$

denn die Summe über alle Charaktere einer endlichen Gruppe E ist nach 1.3 nur auf dem trivialen Element von Null verschieden und dort gleich $m = \#E$. Beachte, für $w \in \mathcal{N}_{L/K} \iff \pi_w \in \mathbb{I}_K$ wird π_w Null im Quotient $\mathbb{I}_K \twoheadrightarrow E$, und damit $\chi_i(\pi_w) = 1$. Da $L(K,\chi_i,s)$ nach 3.6 nur für den trivialen Charakter $\chi_1 = 1$ einen Pol bei $s = 1$ besitzt, folgt nach Teilen durch $-\log(s-1)$ im Limes $s \to 1^+$

$$1 \geq \sum_{\chi\in E^D} ord_{s=1}(L(K,\chi,s)) \;\geq\; \limsup_{s\to 1^+} \sum_{\chi\in E^D} \frac{-\log(Z(K,\chi,s))}{\log(\frac{1}{s-1})} \;\geq\; m{\cdot}d_K(\mathcal{N}_{L/K})\,,$$

und damit $\frac{1}{m} \geq d_K(\mathcal{N}_{L/K})$. Wegen $\mathcal{N}_{L/K} \supseteq \Sigma_{L/K}$ liefert der Dichtesatz

$$d_K(\mathcal{N}_{L/K}) \;\geq\; d_K(\Sigma_{L/K}) = \frac{1}{[L:K]}$$

dann die Abschätzung $1 \geq m/[L:K]$, und damit $m \leq [L:K]$. Ist zusätzlich $m = [L:K]$, gilt Gleichheit und es folgt $d_K(\mathcal{N}_{L/K}) = d_K(\Sigma_{L/K})$. □

[1] Summen vom Typ $\sum_p (p^{2s}/2 + p^{3s}/3 + \cdots)$ bleiben beschränkt bei $s \to 1^+$

Kapitel 6

Die multiplikative Spurformel

6.1 Spektralzerlegung von $L^2(X)$

Sei L/K galoissch mit zyklischer Gruppe $G = \langle\sigma\rangle$. Sei $L^2(X)$ der Hilbertraum[1] der kompakten Gruppe $X = (L^*Z_L\backslash\mathbb{I}_L, dx_L)$ mit dem Skalarprodukt $\langle f, g\rangle = \int_X f(x)\overline{g}(x)$. Jedes $\kappa \in \mathbb{I}_L$ mit $N(\kappa) \in K^*$ induziert einen Automorphismus $\theta(x) = \kappa \cdot \sigma(x)$ von X der Ordnung $n = \#G$.

Charaktere. Die Charaktere $\eta : X \to S^1$ von X bilden eine Hilbertraumbasis

$$\boxed{L^2(X) = \hat{\oplus}_\eta\, \mathbb{C} \cdot \eta}\,,$$

d.h. sie spannen einen dichten Teilraum von $L^2(X)$ auf (Satz von Stone-Weierstraß und Punktetrennung 2.10), und man hat Orthogonalität $\langle\eta', \eta\rangle = 0$ für $\eta' \neq \eta$ [Benutze $\langle\eta', \eta\rangle_X = \int_X(\eta'/\eta)(x) = (\eta'/\eta)(x_0)\int_X(\eta'/\eta)(x)$ wegen der Translationsinvarianz von dx_L].

Testfunktionen. Betrachte Funktionen $f(x) = \prod_v f_v(x)$ auf $\mathbb{I}_L$ mit $f_v \in C_c^\infty(L_v^*)$ an den unendlichen Stellen, für die f_v an den Stellen $v \nmid \infty$ Treppenfunktion (lokal konstant mit kompaktem Träger) sind mit $f_v(x) = 1_{\mathfrak{o}_v}(x)$ für fast alle v. Integriert über Z_L spannen diese f einen Raum $C_c^\infty(Z_L\backslash\mathbb{I}_L)$ auf.

Faltung. Für $f \in C_c^\infty(Z_L\backslash\mathbb{I}_L)$ und $\varphi \in L^2(X)$ ist

$$(R\varphi)(y) = \int_{Z_L\backslash\mathbb{I}_L} f\big(y^{-1}\theta(g)\big)\varphi(g)\,\frac{dg_L}{da_L}\,.$$

wieder in $L^2(X)$ wegen $\|R\varphi\|_X^2 \leq (\int_{Z_L\backslash\mathbb{I}_L}|f(g)|^2\frac{dg_L}{da_L}) \cdot \|\varphi\|_X^2$. Wegen Fubini $\int_{Z_L\backslash\mathbb{I}_L} = \int_{L^*Z_L\backslash\mathbb{I}_L}\sum_{\delta\in L^*}$ gilt für den Integralkern $K(y,x) = \sum_{\delta\in L^*} f\big(y^{-1}\delta\theta(x)\big)$

$$(R\varphi)(y) = \int_X K(y,x)\varphi(x)\,.$$

Eigenvektoren. Für Charaktere $\eta(x)$ von X gilt $R\eta(x) = \eta(f)\cdot\eta^\theta(x)$ mit der Konstante

$$\eta(f) = \int_{Z_L\backslash\mathbb{I}_L} f\big(\theta(g)\big)\eta(g)\,\frac{dg_L}{da_L}\,.$$

Hierbei ist $\eta^\theta(x) = \eta(\sigma^{-1}(x))$ wieder ein Charakter von X.

[1] Fixiere Haarmaße dg_L auf $\mathbb{I}_L$, $da_L = \iota_L^*(\frac{dt}{t})$ auf Z_L (letzteres wie in 2.10 und 3.3). Sei dx_L das Quotientenmaß von dg_L/da_L nach dem diskreten Maß auf L^*. ObdA $vol(X, dx_L) = 1$. Dadurch weicht jetzt dg_L von der Wahl in 3.1 ab, und ist ein Tamagawamaß.

6.2 Die Spur des Operators R

Spektrale Seite. Bezüglich der Basis $L^2(X) = \hat{\oplus}_\eta \, \mathbb{C}\cdot\eta$ schreibt sich R als Summe (im Hilbertraum-Sinn) endlicher Permuationsmatrizen. Nur die invarianten Charaktere $\eta = \eta^\theta$ liefern nichttriviale Beiträge zur Spur, d.h.

$$Spur(R) \;=\; \sum_{\eta=\eta^\theta} \eta(f dg_L) \; .$$

Geometrische Seite. R ist von der Spurklasse[2] mit $Spur(R) = \int_X K(x,x)$, d.h.

$$Spur(R) = \int_X \sum_{\delta\in L^*} f\big(x^{-1}\delta\theta(x)\big) \; .$$

Die Abbildung $x \mapsto \sigma(x)/x$ definiert eine Injektion $(\sigma-1) : K^*\backslash L^* \cong (\sigma-1)L^*$. Beppo Levi (obdA ist $f \geq 0$) liefert daher

$$\sum_{\delta\in L^*/(\sigma-1)L^*} \int_X \sum_{\lambda\in(\sigma-1)L^*} f\big(x^{-1}\delta\lambda\theta(x)\big) = \sum_{\delta\in L^*/(\sigma-1)L^*} \int_{Z_L K^*\backslash\mathbb{I}_L} f\big(x^{-1}\delta\theta(x)\big) \; .$$

Benutzt man nun Fubini $\int_{Z_L K^*\backslash\mathbb{I}_L} = \int_{\mathbb{I}_K\backslash\mathbb{I}_L} \int_{Z_L K^*\backslash\mathbb{I}_K}$ und $Z_K = Z_L$, gibt das innere Integral $\int_{Z_L K^*\backslash\mathbb{I}_K}$ nur einen konstanten Faktor, und es bleiben

Orbitalintegrale. Für $\prod_w f_w$ mit $f_w = \prod_{v|w} f_v$ setze $L^*_w = \prod_{v|w} L^*_v$ und

$$O^L_\delta(f_w) = \int_{K^*_w\backslash L^*_w} \Big(\prod_{v|w} f_v\big(g_v^{-1}\delta\theta(g_v)\big) dg_v\Big)/dg_w \; ,$$

sowie $O^L_\delta(f) = \prod_w O^L_\delta(f_w)$. Mit diesen Bezeichnungen gilt dann[3]

Spurformel. *Für* $\prod_w f_w \in C^\infty_c(Z_L\backslash\mathbb{I}_L)$ *und* $O^L_\delta(f) = \prod_w O^L_\delta(f_w)$ *ist*

$$\boxed{\sum_{\eta=\eta^\theta\in(X_L)^D} \eta(f) \;=\; \tfrac{1}{[L:K]} \sum_{\delta\in L^*/(\sigma-1)L^*} O^L_\delta(f)} \; .$$

---

[2] Siehe Appendix I

[3] Der natürliche Isomorphismus $i(t) = \iota_L \circ (\iota_K)^{-1}(t^{[L:K]})$, d.h. $i : Z_K \hookrightarrow Z_L$, liefert einen Volumenfaktor $i^*(da_L)/da_K = [L : K]$. Hierbei sei $dg_K = \prod_w dg_w$ analog normiert mit $vol(dx_K, Z_K K^*\backslash\mathbb{I}_K) = 1$.

6.3 Matching

Die Norm. Sei w eine Stelle von K. Für $K_w \otimes_K L = \prod_{v|w} L_v$ (siehe 4.4) gilt $(K_w \otimes_K L)^* = \prod_{v|w} L_v^* = L_w^*$. Der Automorphismus $\sigma = id_{K_w} \otimes \sigma$ operiert auf $L_w^* = \prod_{v|w} L_v^*$. Für Elemente $\delta_w = (\delta_v)_{v|w}$ in diesem Produkt definiert $N(\delta_w) = \prod_{v|w} N_{L_v/K_w}(\delta_v)$ einen stetigen Homomorphismus $N : L_w^* \to K_w^*$. Für δ in L^* gilt

$$N(\delta) = N_{L/K}(\delta) \ .$$

Wegen $Kern(N : L_w^* \to K_w^*) = (\sigma - 1)L_w^*$ (Hilbert Satz 90 nach 1.2) definiert N einen Isomorphismus

$$N: \quad L_w^* / (\sigma - 1) L_w^* \quad \xrightarrow[\sim]{N} \quad N(L_w^*) \quad \subseteq K_w^* \ .$$

Matching. Für Haarmaße dg_v auf L_v^*, dg_w auf K_w^* und Funktionen $f_v \in C_c^\infty(L_v^*)$ für $v|w$ und $h_w \in C_c^\infty(K_w^*)$ nennen wir $f_w = \prod_{v|w} f_v$ und h_w assoziiert, falls

- $h_w(\gamma_w) = 0$ für $\gamma_w \notin N(L_w^*)$
- $h_w(\gamma_w) = O_{\delta_w}^L(f_w)$ für $\gamma_w = N(\delta_w)$ und $\delta_w \in L_w^*$.

Man kann dabei f_w vorschreiben. Die dazu durch obige Bedingungen eindeutig bestimmte Funktion h_w liegt nämlich in $C_c^\infty(K_w^*)$. [Benutze, daß das Bild $N(L_w^*)$ offen und abgeschlossen in K_w^* ist. Beachte, bereits die Untergruppe $(K_w^*)^n$ des Bildes hat endlichen Index in K_w^*. Zum Beweis benutze 4.7]. Umgekehrt legt h_w aber f_w nicht fest.

Idelsituation. Für $N: \ \mathbb{I}_L/(\sigma - 1)\mathbb{I}_L \ \cong N(\mathbb{I}_L) \ \subseteq \mathbb{I}_K$ heißen $f = \prod_v f_v$ und $h = \prod_w h_w$ assoziiert, wenn $\prod_{v|w} f_v$ und h_w assoziiert sind für alle w. Man kann f vorschreiben mit $f_v = 1_{\mathfrak{o}_v}$ für fast alle v.

Zur Existenz. Wesentlich für die Existenz assoziierter Funktionen $f \in C_c^\infty(Z_L \backslash \mathbb{I}_L)$ und $h \in C_c^\infty(Z_K \backslash \mathbb{I}_K)$ ist Lemma 4.7. Es zeigt

Fundamentales Lemma. $\prod_{v|w} 1_{\mathfrak{o}_v^*}$ *und* $1_{\mathfrak{o}_w^*}$ *sind assoziiert für unverzweigte* w.

Beweis. Benutze die triviale Aussage $F_w^* \backslash L_w^* \cong (\sigma - 1)L_w^*$ sowie dann auch die Aussage $(1 - \sigma)\delta_w \in \prod_{v|w} \mathfrak{o}_v^* \iff \delta_w \in F_w^* \prod_{v|w} \mathfrak{o}_v^*$. ObdA sei dabei an den unverzweigten Stellen $\int_{F_w^* \backslash F_w^* \prod_{v|w} \mathfrak{o}_v^*} (\prod_{v|w} dg_v)/dg_w = 1$. □

6.4 Spurformelvergleich

Wir betrachten nun die getwistete Spurformel einerseits für L/K, und andererseits im trivialen Fall $L = K$. Für assoziierte f und h wollen wir die 'getwistete' Spurformel für den Operator $R = R(fdg_L)$ (Körpererweiterung L/K) mit der Spurformel für den Operator $R(hdg_K)$ (triviale Körpererweiterung K/K) vergleichen. Wegen der Assoziiertheit von f und h gilt

Trägerbedingung. h hat Träger in $N(Z_L\backslash\mathbb{I}_L) \subseteq Z_K\backslash\mathbb{I}_L$. Für das Bild $Y^\flat$ von $N(Z_L\backslash\mathbb{I}_L)$ in $X_K = Z_K K^*\backslash\mathbb{I}_K$ hat man eine exakte Sequenz

$$0 \to K^* \cap N(\mathbb{I}_L) \to N(Z_L\backslash\mathbb{I}_L) \to Y^\flat \to 0\ .$$

Wegen $0 \to L^* \to (Z_L\backslash\mathbb{I}_L) \stackrel{N}{\to} N(L^*)\big\backslash N(Z_L\backslash\mathbb{I}_L) \to 0$ liefert dies daher für $Y^\sharp = N(L^*)\big\backslash N(Z_L\backslash\mathbb{I}_L) = (\sigma-1)X_L$ die exakte Sequenz

$$0 \to \frac{K^* \cap N(\mathbb{I}_L)}{N(L^*)} \to Y^\sharp \to Y^\flat \to 0\ .$$

Spurformel für h. Für $L = K$ und $\kappa = 1$ gilt $O_\gamma(hdg_K) = h(\gamma)$, und damit $Spur(R(h)) = \sum_{\gamma\in K^*} h(\gamma)$. Für die Berechnung von $\chi(h)$ sind die Charaktere $\chi \in (X_K)^D$, über die auf der linken Seite der Spurformel summiert wird, nur relevant auf dem Träger $Y^\flat \subseteq X_K$ von h. Gilt $\chi|_{Y^\flat} = \chi'|_{Y^\flat} \iff \chi'/\chi = 1$ auf $Y^\flat$, nennen wir χ und χ' äquivalent. $\chi'/\chi(Y^\flat) = 1$ bedeutet, daß χ' und χ sich nur um einen Charakter der endlichen Faktorgruppe $C_K/Y^\flat$ der Kardinalität $m = [X_K : Y^\flat] = [C_K : N(C_L)]$ unterscheiden. Es gibt also genau m Elemente in jeder Äquivalenzklasse. Die Einschränkungen $\chi|Y^\flat$ durchlaufen andererseits alle (!) Charaktere $\chi^\flat$ von $Y^\flat$. Setzt man $\chi^\flat(h) := \int_{Z_K\backslash N(\mathbb{I}_L)} \chi^\flat(t)h(t)\frac{dg_K}{da_K}$, ist daher

$$m \cdot \sum_{\chi^\flat\in(Y^\flat)^D} \chi^\flat(h) = Spur\big(R(h)\big) = \sum_{\gamma\in K^*\cap N(\mathbb{I}_L)} h(\gamma)\ .$$

Insbesondere also $m < \infty$.

Spurformel für f. Im einfachsten Fall ist $\kappa = 1$ und $\theta = \sigma$. Die rechte Seite der Spurformel $Spur(R(f)) = \frac{1}{[L:K]}\sum_{\delta\in L^*/(\sigma-1)} O_\delta^L(f)$ ist wegen der Assoziiertheit von f und h gleich $\frac{1}{[L:K]}\sum_{\gamma\in N(L^*)} h(\gamma)$. Hilbert Satz 90 zeigt nämlich $N : L^*/(\sigma-1)L^* \cong N(L^*)$. Die linke Seite der Spurformel ist $\sum_{\eta=\eta^\sigma} \eta(f)$. Hierbei bedeutet $\eta = \eta^\sigma$, daß η als Charakter von $\mathbb{Z}_L\backslash\mathbb{I}_L$ auf $(\sigma-1)\mathbb{I}_L = Kern(N)$,

genauer $Kern(N : \mathbb{I}_L \to \mathbb{I}_L)$, verschwindet. [Benutze Hilbert Satz 90 für $L_w = \prod_{v|w} L_v$]. Somit ist $\eta = \eta^\sigma$ ein Charakter des Quotienten $\mathbb{I}_L/L^* Z_L Kern(N)$. Die Norm N definiert eine Bijektion zwischen $Z_L Kern(N)\backslash\mathbb{I}_L$ und $Z_K\backslash N(\mathbb{I}_L)$. Man kann daher $\eta = \tilde{\chi}^\sharp \circ N$ als einen Charakter $\chi^\sharp$ der Gruppe $Z_K\backslash N(\mathbb{I}_L)$ auffassen, der auf $N(L^*)$ verschwindet. Jeder solche Charakter $\chi^\sharp$ definiert umgekehrt einen Charakter $\eta = \chi^\sharp \circ N$ von $\mathbb{I}_L$, welcher auf L^* und $Kern(N)$ verschwindet. Der Summand $\eta(f) = \int_{Z_L\backslash\mathbb{I}_L} \eta(g) f(g)\, \frac{dg_L}{da_L}$ zum Charakter $\eta = \eta^\sigma$ ist nach Fubini

$$\int_{Z_L Kern(N)\backslash\mathbb{I}_L} \eta(g) \Big(\int_{Kern(N)} f(gn) dn \Big) \frac{dg_L}{dn da_L}$$

$$= \int_{Z_L Kern(N)\backslash\mathbb{I}_L} \eta(g) \Big(\int_{\mathbb{I}_K\backslash\mathbb{I}_L} f(h^{-1} g \sigma(h)) \frac{dg_L(h)}{dg_K} \Big) \frac{dg_L}{dn da_L}$$

für $\frac{dg_L}{dg_K} = dn$. Assoziiertheit von h und f impliziert daher

$$\eta(f) = \int_{Z_L Kern(N)\backslash\mathbb{I}_L} \eta(g) h(N(g))\, \frac{dg_L}{dn da_L} = c \cdot \int_{Z_K\backslash N(\mathbb{I}_L)} \chi^\sharp(t) h(t)\, \frac{dg_K}{da_K}\ .$$

für einen Volumenfaktor c definiert durch $c \cdot \frac{da_L}{da_K} = \frac{dg_L}{dn dg_K}$. Also liefert uns die Spurformel

$$c \cdot \sum_{\chi^\sharp \in (Y^\sharp)^D} \chi^\sharp(h) = \sum_{\eta = \eta^\sigma} \eta(f) = \frac{1}{[L:K]} \sum_{\gamma \in N(L^*)} h(\gamma)\ .$$

Für $\kappa \neq 1$ erhält man (bis auf eine Translation von f und h) im Prinzip dieselbe Formel. Summiert man über Repräsentanten aller möglichen $\kappa \in \mathbb{I}_L$ modulo L^* mit $\gamma = N(\kappa) \in K^*$, welche zu den $\tilde{m}$ Nebenklassen $(K^* \cap N(\mathbb{I}_L))/N(L^*)$ korrespondieren, erhält man

$$c\tilde{m} \cdot \sum_{\chi^\flat \in (Y^\flat)^D} \chi^\flat(h) = \sum_{\kappa} Spur_\kappa(R(f)) = \frac{1}{[L:K]} \sum_{\gamma \in K^* \cap N(\mathbb{I}_L)} h(\gamma)\ .$$

Für geeignetes f mit Träger in einer genügend kleinen Umgebung der 1 verschwindet $h(\gamma)$ außer für $\gamma = 1$. Der Vergleich der letzten Formel mit der Spurformel für $L = K$ zeigt daher $[L:K] c\tilde{m} = m$, also

Korollar.

$$[L:K] \cdot c = \frac{[C_K : N(C_L)]}{[(K^* \cap N(\mathbb{I}_L)) : N(L^*)]}\ .$$

6.5 Der Volumenfaktor

Um den Volumenfaktor c aus den Formeln $c \cdot \frac{da_L}{da_K} = \frac{dg_L}{dndg_K}$ und $\frac{dg_L}{dg_K} = dn$ zu berechnen, kann man jetzt die bisherigen Normierungsbedingungen an die Maße dg_L und dg_K ignorieren. Im Abschnitt 6.2 haben wir benutzt, daß die Inklusion $\mathbb{I}_K \hookrightarrow \mathbb{I}_L$ die Untergruppen $Z_K = Z_L$ und Maße da_L und da_K bis auf den Faktor $[L : K]$ identifiziert. Der Quotient da_L/da_K im Abschnitt 6.4 entstand dagegen durch den Isomorphismus $N : Z_L \cong Z_K$. Wegen $N \circ \iota_L = \iota_K$ ist jetzt der Faktor $\frac{da_K}{da_L} = 1$. Der verbleibende Term $c = \frac{dg_L}{dndg_K}$ dagegen entsteht durch die Abbildungen der exakten Sequenz

$$0 \to \mathbb{G}_m \xrightarrow{i} Res_{L/K}(\mathbb{G}_m) \xrightarrow{\sigma-1} Kern(N) \to 0$$

$$0 \to Kern(N) \to Res_{L/K}(\mathbb{G}_m) \xrightarrow{p} \mathbb{G}_m \to 0$$

zwischen den algebraischen Gruppen $\mathbb{G}_m$ und $T = Res_{L/K}(\mathbb{G}_m)$ und $V = Kern(N)$ über K. Fixiert man Haarmaße dg_K und dn auf $\mathbb{I}_K$ und $(1-\sigma)(\mathbb{I}_K)$, werden durch beide Sequenzen Haarmaße auf $\mathbb{I}_L$ induziert. Wir behaupten, diese stimmen überein, d.h. es gilt

$$c = 1 \ .$$

Dazu genügt es algebraische Differentialformen höchsten Grades auf den Gruppen zu vergleichen, denn diese definieren Maße dg_L resp. dg_K und dn (welche allerdings an fast allen Stellen mit Konvergenz erzeugenden Faktoren normalisiert werden müssen nach dem Rezept von 3.1). Da sich diese Konvergenz erzeugenden Faktoren beim Vergleich aber wegkürzen, genügt es zum Beweis den Tangentialraum[4] der algebraischen Gruppen im Nullpunkt zu betrachten!

Wegen $c = 1$ liefert somit Korollar 6.4 zusammen mit Satz 5.4

Normensatz von Hasse. *Für zyklische Erweiterungen L/K gilt*

$$\boxed{K^* \cap N(\mathbb{I}_L) = N(L^*)}$$

Normenindexsatz. *Für zyklische Erweiterungen L/K gilt*

$$\boxed{[C_K : N(C_L)] = [\mathbb{I}_L : K^* N(\mathbb{I}_L)] = [L : K]}$$

[4]Für geeignete 1-Formen $A = i^*(e_1^*)$ auf $\mathbb{G}_m$ und $(n-1)$-Formen B auf $V = (1-\sigma)T = Kern(p)$ reduziert man dann auf die Formel $e_1^* \wedge (1-\sigma)^*(B) = e_1^* \wedge (e_2^* - e_1^*) \wedge \cdots (e_n^* - e_{n-1}^*) = e_1^* \wedge \cdots \wedge e_n^* = [e_1^* \wedge \cdots e_{n-1}^*] \wedge (e_1^* + \cdots + e_n^*) = B \wedge p^*(A)$.

6.6 Zyklischer Basiswechsel

Sei L/K zyklisch mit $G = Gal(L/K) = \langle\sigma\rangle$. Der Spurformelvergleich im letzten Abschnitt ergab den Normensatz $\tilde{m} = 1$, und damit a posteriori $Y^\flat = Y^\sharp$. Ebenfalls folgt dann: Die Äquivalenzklassen $\chi \sim \chi'$ der Charaktere von X_K enthalten genau $m = [L : K]$ Elemente. Also wegen $(X_K)^D = (C_K)^D$ dann

Satz. *Die durch $\chi \mapsto \eta = \chi \circ N$ definierte Zuordnung*

$$\Big\{\chi \in (C_K)^D\Big\}\Big/ \sim \quad \xrightarrow{\sim} \quad \Big\{\eta \in (C_L)^D \mid \eta = \eta^\theta\Big\}$$

induziert eine kanonische Bijektion (und erhält Charakter endlicher Ordnung).

Eine analoge Eigenschaft besitzen die Charaktere der absoluten Galoisgruppe $G_K = \lim_{\tilde{L}/K} Gal(\tilde{L}/K)$ von K (siehe Appendix).

Satz. *Die durch $\rho_K \mapsto \rho = \rho_K|G_L$ definierte Zuordnung*

$$\Big\{\rho_K \in (G_K)^D\Big\}\Big/ G^D \quad \xrightarrow{\sim} \quad \Big\{\rho \in (G_L)^D \mid \rho = \rho^\theta\Big\}$$

induziert eine kanonische Bijektion von Charakteren endlicher Ordnung.

Beweis. Diese Aussage gilt für beliebige[5] Körper K, also nicht nur für Zahlkörper. Klar, zwei Charaktere ρ'_K, ρ_K werden nur gleich auf G_L, wenn ihr Quotient trivial auf G_L und damit ein Charakter von $G = G_K/G_L$ ist. Umgekehrt sei ρ ein σ-invarianter Charakter von $Gal(\tilde{L}/L)$ für eine endliche Galois Erweiterung $\tilde{L}/K$ (Stetigkeit). Wähle $\sigma \in Gal(\tilde{L}/K)$, das G erzeugt. Setze $\rho_K(\theta^\nu g) = A^\nu \rho(g)$ für $\nu \in \mathbb{Z}$ und $g \in Gal(\tilde{L}/L)$, wobei $A^n = \rho(\theta^n)$ für $n = [L : K]$. [6]. □

[5]Für nicht zyklisches L/K kann man etwas ähnliches nur für projektive irreduzible Darstellungen ρ der Gruppen G_K machen, sagen wir die bei Einschränkung irreduzibel bleiben. Für Zahlkörper K kommt nach einem Satz von Serre/Tate wenigstens jede projektive endlich dimensionale komplexe Darstellung von G_K von einer echten Darstellung ρ.

[6]Sei $\rho : Gal(\tilde{L}/L) \to Gl(V)$ sogar eine beliebige σ-invariante komplexe Darstellung des Normalteilers $Gal(\tilde{L}/L)$ von $Gal(\tilde{L}/K)$, d.h. $\rho(\theta g \theta^{-1}) = A_\theta \rho(g) A_\theta^{-1}$ für eine Matrix $A_\theta \in Gl(V)$. Dann definiert $\rho_K(\theta^\nu g) = A_\theta^\nu \rho(g)$ für $\nu \in \mathbb{Z}$ und $g \in Gal(\tilde{L}/L)$ eine Darstellung von $Gal(\tilde{L}/K)$, deren Einschränkung ρ ist, wenn man A_θ durch eine Konstante so normieren kann, daß $(A_\theta)^n = \rho(\theta^n)$ gilt für $n = [L : K]$. Dies ist immer möglich, wenn ρ irreduzibel ist, wegen dem Schurschen Lemma $\rho(\theta) = \lambda A_\theta$ für $\lambda \in \mathbb{C}^*$ (und in unserem Fall trivial wegen $dim_{\mathbb{C}}(V) = 1$)

Kapitel 7

Abelsche Erweiterungen

7.1 Anwendungen vom Normenindexsatz

Wir wenden den Normenindexsatz (siehe Abschnitt 6.5)

$$[C_K : N(C_L)] = [L : K]$$

für zyklische Erweiterungen L/K von Zahlkörpern an, und erhalten

Satz. *Die Gruppe*

$$N(C_L) \subseteq C_K$$

bestimmt die zyklische Erweiterungen L/K in $\overline{K}/K$ eindeutig. Es gilt

$$\Sigma_{L/K} \equiv \mathcal{N}_{L/K}$$

(Gleichheit bis auf Mengen der K-Dichte Null).

Beweis. Dies gilt für $\Sigma_{L/K}$ (Proposition 5.2). Da wegen dem Normenindexsatz die Vorraussetzungen des Zusatzes von Satz 5.4 für zyklische Erweiterungen erfüllt sind, gilt $\Sigma_{L/K} \equiv \mathcal{N}_{L/K}$ (Gleichheit bis auf eine Menge der K-Dichte Null). Die K-Dichte von $\Sigma_{L/K}$ ist aber nicht Null nach dem Dichtesatz. Daher bestimmt $\mathcal{N}_{L/K}$ den Körper $L \subseteq \overline{K}$, und $\mathcal{N}_{L/K}$ wiederum ist eindeutig bestimmt durch die Gruppe $N(C_L) \subseteq C_K$. □

Bemerkung. Wie wir in 2.12 gesehen haben gibt es für jeden Zahlkörper K eine endliche Menge S von Stellen von K mit $S \supseteq S_\infty$ und der Eigenschaft $Cl(K,S)/n = 0$ (Endlichkeit der Klassenzahl). Gleichbedeutend damit ist

$$\mathbb{I}_K = K^* \cdot (\mathbb{I}_K)^n \cdot \Big(\prod_{w \in S} K_w^*) \times \prod_{w \notin S} \mathfrak{o}_w^* \Big) .$$

Unter dieser Voraussetzung an S folgt aus dem Normenindexsatz

Proposition. *Sei L/K zyklisch von der Ordnung n, unverzweigt außerhalb von S und zerfalle an allen Stellen $v \in S$. Dann gilt $L = K$.*

Beweis. Aus den Annahmen folgt $N(\mathbb{I}_L) \supseteq (\mathbb{I}_K)^n \cdot (\prod_{w \in S} K_w^* \times \prod_{w \notin S} \mathfrak{o}_w^*)$ wegen dem fundamentalen Lemma (für $v \notin S$) und wegen 5.3 (für $v \in S$). Aus der Annahme an S folgt daher $K^* \cdot (\mathbb{I}_K)^n \cdot N(\mathbb{I}_L) = \mathbb{I}_K$. Das heißt L/K ist eine zyklische Erweiterung mit $m = [C_K : N(C_L)] = 1$. Aus dem Normenindexsatz 6.5 folgt $L = K$. □

7.2 Das Potenzkriterium

Die wichtigsten Beispiele abelscher Erweiterungen entstehen durch Ziehen von Wurzeln aus einer Zahl. Entscheidend ist daher ein lokales Kriterium zu besitzen, wann eine Zahl $\alpha \in K$ eine q-te Potenz in K ist.

Vorbemerkung. Wie wir in 2.12 gesehen haben gibt es für jeden Zahlkörper K eine endliche Menge S von Stellen von K mit $S \supseteq S_\infty$ und der Eigenschaft $Cl(K,S)/n = 0$ (Endlichkeit der Klassenzahl). Gleichbedeutend damit ist

$$\mathbb{I}_K = K^* \cdot (\mathbb{I}_K)^n \cdot \Big(\prod_{w \in S} K_w^* \times \prod_{w \notin S} \mathfrak{o}_w^* \Big) .$$

Unter dieser Voraussetzung an S folgt als Anwendung vom NORMENINDEXSATZ das folgende

Potenzkriterium. *Sei K ein Zahlkörper, der eine primitive q-te Einheitswurzeln enthalte, und $S \supseteq S_\infty \cup \{v|p\}$ eine endliche Stellenmenge mit $Cl(K,S)/q = 0$. Für eine Zahl α in K^* sind dann äquivalent*

1. *α ist lokal eine q-te Potenz*
$$\alpha \in (K_w^*)^q$$
für $w \in S$ und alle (nichtarchimedischen) Stellen w mit der Eigenschaft $\alpha \notin \mathfrak{o}_w^*$.

2. *α ist eine q-te Potenz $\alpha \in (K^*)^q$ global.*

Beweis. Wegen $\mu_q \subseteq K$ ist $L = K(\alpha^{1/q})/K$ zyklisch von der Ordnung q. Nach Abhyankars Lemma (siehe 4.8) sind alle $w \notin S$ unverzweigt in L/K, und die Stellen von S zerfallen (unter der Voraussetzung 1.). Die Proposition 7.1 impliziert daher $L = K$, und damit $\alpha \in (K^*)^q$. □

Beispiel. In elementarer Form ist der Fall $K = \mathbb{Q}$ und $q = 2$ wohlvertraut. Hier ist obdA $S = S_\infty$.

Bemerkung. Im Fall $q > 2$ ist wegen $K_w = L_v = \mathbb{C}$, also ist für alle $w|\infty$ die Bedingung $\alpha \in (K_w)^q$ automatisch erfüllt.

7.3 Das Abzählargument

Annahmen an K. *Sei K ein Zahlkörper. Wir nehmen an p sei eine Primzahl und die p-ten Einheitswurzeln seien in K.*

Annahmen an S (für Lemma 1). *S sei eine endliche Menge S von Stellen von K mit $S \supseteq S_\infty$ und $S \supseteq \{v|p\}$ sowie der Eigenschaft $Cl(K,S)/p = 0$.*

Zur Erinnerung. Wir haben in 7.1 die Existenz einer Injektion gezeigt

$$(L/K)/\sim \quad \mapsto \quad N(C_L)$$

von der Menge der Isomorphieklassen von galoisschen Körpererweiterungen L/K in die Menge der Untergruppen von endlichem Index in C_K.

Spezialfall. Wir beschränken uns jetzt darauf, diese Abbildung auf Klassen primzyklischer Erweiterungen L/K vom Grad p zu betrachten. Wir wissen bereits

1. Für unverzweigtes w in L/K enthält $N(C_L)$ die Untergruppe $\mathfrak{o}_w^* \subseteq \mathbb{I}_K$ (fundamentales Lemma).
2. Die Normgruppe $N(C_L)$ einer Erweiterung L/K vom Grad $[L:K] = p$ enthält immer $(K_w^*)^p$ für alle Stellen w (dies ist trivial).
3. Nach dem Normenindexsatz 6.5 gilt $[C_K : N(C_L)] = p$ für primzyklisches L/K vom Grad p.

S-Erweiterungen. Wir beschränken wir uns jetzt außerdem darauf nur solche zyklische Körpererweiterungen L/K mit $Gal(L/K) \cong \mathbb{F}_p$ zu betrachten, welche unverzweigt außerhalb der oben fest gewählten Menge S sind (da S ja beliebig vergrößert werden kann, stellt dies letztlich keine echte Einschränkung dar). Dann gilt für die Normengruppe $N(C_L)$ wegen der obigen Aussagen 1.–3.

$$\mathbb{I}_K \supseteq N(C_L) \supseteq K^* \cdot (\mathbb{I}_K)^p \cdot N_S \ ,$$

wobei

$$N_S = \prod_{w \in S} (K_w^*)^p \times \prod_{v \notin S} \mathfrak{o}_w^* \ \subseteq \ \mathbb{I}_K \ .$$

Lemma 1.

$$\boxed{\mathbb{I}_K / K^* (\mathbb{I}_K)^p N_S \cong (\mathbb{F}_p)^{\#S}} \ .$$

Also gibt es nach Satz 7.1 höchstens $(p^{\#S}-1)/(p-1)$ Erweiterungen L/K mit obigen Eigenschaften (bis auf Isomorphie):

$$\sim \Big\backslash \left\{ \begin{matrix} \text{L/K mit Gal(L/K)}\cong \mathbb{F}_p \\ \text{unverzweigt für } w \notin S \end{matrix} \right\} \hookrightarrow \mathbb{P}^{\#S-1}(\mathbb{F}_p) = \mathbb{P}\big(\mathbb{I}_K/K^*(\mathbb{I}_K)^p N_S\big)\,.$$

Diese Inklusion ist sogar eine Bijektion wegen

Lemma 2. *Es gibt genau $(p^{\#S}-1)/(p-1)$ verschiedene Erweiterungen L/K vom Grad $[L:K]=p$, welche durch Ziehen aller p-ten Wurzeln aus S-Einheiten $\alpha \in \mathfrak{o}_{K,S}^*$ entstehen $L=K(\alpha^{1/p})$. Jeder dieser Körper ist unverzweigt außerhalb von S und enthalten in $L_S = K(\mathfrak{o}_{K,S}^{1/p})$.*

Also

$$\sim \Big\backslash \left\{ \begin{matrix} \text{L/K mit Gal(L/K)}\cong \mathbb{F}_p \\ \text{unverzweigt für } w \notin S \end{matrix} \right\} \xrightarrow{\ \sim\ } \mathbb{P}^{\#S-1}(\mathbb{F}_p)\,.$$

Durch sukzessives Vergrößern von S folgt daraus

Korollar. *Die Klassen primzyklischer Körpererweiterungen L/K vom Primzahlgrad p entsprechen eineindeutig den Untergruppen von C_K vom Index p.*

Beweis von Lemma 2. Beachte $Kern\big(\mathfrak{o}_{K,S}^* \to K^*/(K^*)^p\big) = (\mathfrak{o}_{K,S}^*)^p$. Der Dirichletsche Einheitensatz liefert

$$\boxed{\tfrac{\mathfrak{o}_{K,S}^*}{(\mathfrak{o}_{K,S}^*)^p} \cong \mu_p(K) \times \mathbb{F}_p^{\#S-1} \cong \mathbb{F}_p^{\#S}}$$

wegen $\#\mu_p(K)=p$. Daraus folgt sofort Lemma 2 mittels Kummertheorie. □

Beweis von Lemma 1. $K^*(\prod_{w\in S} K_w^* \times \prod_{w\notin S}\mathfrak{o}_w^*)\Big/K^*N_S \hookrightarrow \mathbb{I}_K/K^*N_S$ hat zu p teilerfremden Index, und ist gleich

$$\frac{(\prod_{w\in S} K_w^* \times \prod_{w\notin S}\mathfrak{o}_w^*)\Big/N_S}{(\prod_{w\in S} K_w^* \times \prod_{w\notin S}\mathfrak{o}_w^*)\cap K^*\Big/(\prod_{w\in S}(K_w^*)^p \times \prod_{w\notin S}\mathfrak{o}_w^*)\cap K^*}$$

$$= \frac{\prod_{w\in S}\big(K_w^*/(K_w^*)^p\big)}{\mathfrak{o}_{K,S}^*/(N_S\cap K^*)} = \frac{\prod_{w\in S}\big(K_w^*/(K_w^*)^p\big)}{\mathfrak{o}_{K,S}^*/(\mathfrak{o}_{K,S}^*)^p}\,.$$

Entscheidend ist $N_S K^* = (\mathfrak{o}_{K,S}^*)^p$ (das nichttriviale Potenzkriterium 7.2).

Nun zur Struktur von $K_w^*/(K_w^*)^p$. Wir unterscheiden drei Fälle.

> *Fall 1.* $w \nmid p, \infty$. Dann hat $(K_w^*)/(K_w^*)^p \cong \pi_w^{\mathbb{Z}}/\pi_w^{p\mathbb{Z}} \times \left(\mathfrak{o}_w^*/(\mathfrak{o}_w^*)^p\right)$ die Kardinalität p^2. Wegen $\mu_p \subseteq K \subseteq K_w^*$ ist die p-Torsionsgruppe von ${\mathfrak{o}_w}^*$ nichttrivial (aus 4.6 folgt dann $\mathfrak{o}_w^*/(\mathfrak{o}_w^*)^p \cong \kappa_w^*/(\kappa_w^*)^p \cong \mathbb{F}_p$.
>
> *Fall 2.* $w|\infty$. Dann ist $(K_w^*)/(K_w^*)^p$=1 im Fall $p > 2$, da dann $K_w = \mathbb{C}$, beziehungsweise hat Kardinalität 2 für $p = 2$ und $K_w = \mathbb{R}$.
>
> *Fall 3.* $w|p$. Der Beitrag ist $\pi_w^{\mathbb{Z}}/\pi_w^{p\mathbb{Z}} \times \mathfrak{o}_w^*/(\mathfrak{o}_w^*)^p$. Beachte $\mu_p \backslash \mathfrak{o}_w^*/(1 + \pi_w^r \mathfrak{o}_w) \cong (\mathfrak{o}_w^*)^p/(1+p\pi_w^r \mathfrak{o}_w)$ für genügend großes r. Dies liefert $\mathfrak{o}_w^*/(\mathfrak{o}_w^*)^p \cong \mathbb{F}_p^{1+[K_w:\mathbb{Q}_p]}$ wegen $p^{[K_w:\mathbb{Q}_p]} = [(1 + \pi_w^r \mathfrak{o}_w) : (1 + \pi_w^r p\mathfrak{o}_w)] = \sum_{i=1}^{e_{w|p}} \kappa_w = p^{e_{w|p} f_{w|p}}$.

Die Beiträge aller $w|p$ liefern $\mathbb{F}_p^{2\#\{v|p\}}$ analog zu den Stellen $w \in S$, und noch einen zusätzlichen Beitrag $\mathbb{F}_p^{[K:\mathbb{Q}]}$ der $\mathbb{F}_p$-Dimension

$$\sum_{w|p} [K_w : \mathbb{Q}_p] = [K : \mathbb{Q}] = r_1 + 2r_2 = 2\#S_\infty - r_1 \ .$$

Die unendlichen Stellen liefern den Beitrag $\mathbb{F}_p^{r_1}$. Es folgt

$$\boxed{\prod_{w \in S} \frac{K_w^*}{(K_w^*)^p} \ \cong \ \mathbb{F}_p^{2\#S}} \ .$$

Es ist klar, daß die kanonische Projektion

$$\mathbb{I}_K \to \prod_{w \in S} K_w^* \to \prod_{w \in S} \frac{K_w^*}{(K_w^*)^p}$$

über den Quotienten $\mathbb{I}_K/(\mathbb{I}_K)^p$ faktorisiert. Da $\mathbb{I}_K/(K^* \cdot (\prod_{w \in S} K_w^* \times \prod_{w \notin S} \mathfrak{o}_w^*)) = Cl(K, S)$ teilerfremd zu p ist, wird $\mathbb{I}_K/K^*(\mathbb{I}_K)^p$ modulo $K^*(\mathbb{I}_K)^p N$ isomorph auf $\mathbb{F}_p^{2\#S}/\mathbb{F}_p^{\#S}$ abgebildet. □

Folgerung. $L_S = K(\mathfrak{o}_{K,S}^{1/p})$ *ist die maximale elementar-p-abelsche Erweiterung von* K*, welche unverzweigt außerhalb von* S *ist.*

Folgerung. *Die kanonische Abbildung* $\mathfrak{o}_{K,S}^*/(\mathfrak{o}_{K,S}^*)^p \to \prod_{w \in S} \frac{K_w^*}{(K_w^*)^p}$ *ist injektiv, und hat als Kokern*[1] *die Gruppe* $(C_K/N_S)[p]$.

[1] Nach Satz 7.5 folgt daraus das $N_S = N(C_{L_S}) \subseteq C_K$.

7.4 Zyklische Erweiterungen

Wir wenden erneut den Normenindexsatz (siehe Abschnitt 6.5)

$$[C_K : N(C_L)] = [L : K]$$

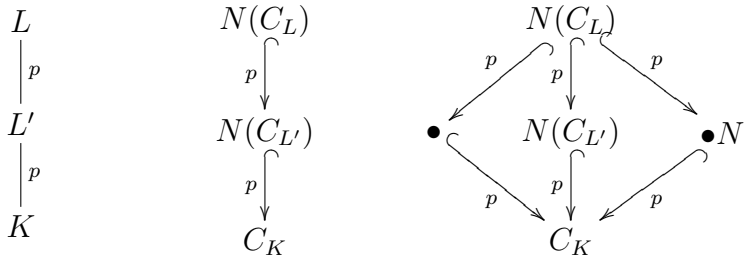
für zyklische Erweiterungen L/K von Zahlkörpern an, und erhalten zusammen mit dem Abzählargument das

Lemma. *Für zyklisches* L/K *gilt* $Gal(L/K) \cong C_K/N(C_L)$.

Beweis. Nach dem Normenindexsatz haben $G = Gal(L/K)$ und $G' = C_K/N(C_L)$ dieselbe Kardinalität. Es genügt Erweiterungen von Primpotenzordnung zu betrachten. Also $G = \mathbb{Z}/p^r\mathbb{Z}$ und $G/pG = \mathbb{F}_p$. Wäre G' nicht zyklisch, wäre $G'/pG' = (\mathbb{F}_p)^k$ für ein $k \geq 2$. Wegen Proposition 5.2 und Lemma7.1

$$N(C_L) \subseteq N(C_{L'}) \subseteq C_K \quad \Longleftrightarrow \quad K \subseteq L' \subseteq L$$

gäbe es daher eine Untergruppe N mit $N(C_L) \subseteq N \subseteq C_K$ vom Index p in C_K, welche nicht die Normengruppe einer Erweiterung L' vom Grad p ist (diese müsste nämlich zwischen L und K liegen, und da gibt es nur eine). Dies ist ein Widerspruch zu Korollar 7.3, zumindestens wenn p-te Einheitswurzeln $\zeta_p \neq 1$ in K liegen. Im Bild der Fall $Gal(L/K) = \mathbb{Z}/p^2\mathbb{Z}$



$\zeta_p \in K$ können wir aber obdA annehmen! Ersetze einfach K durch $K' = K(\zeta_p)$. Dies ist eine Erweiterung vom Grad d mit $dd' = p - 1$. Multiplikation mit d ist ein Isomorphismus auf C_K/p, da d teilerfremd zu p ist. Für die natürliche Abbildung $i : C_K/p \to C_{K'}/p$ gilt $N \circ i = d \cdot id$. C_K/p ist also ein direkter Summand von $C_{K'}/p = C_K/p \oplus Kern(N)$. Da die Zwischenköper von L/K den Zwischenkörpern von LK'/K' entsprechen (durch Körper-Kompositum), und sich die p-Potenzquotienten von C_K (mittels der Norm) treu nach K' vererben, genügt der obige Schluß angewendet auf K' anstelle von K. □

7.5 Das Hauptresultat

Im letzten Abschnitt wurde bereits der nachfolgende Satz für zyklische Erweiterungen L/K von Zahlkörpern bewiesen. Aus dem zyklischen Fall leitet man aber sofort - wie wir sehen werden - alle weiteren Aussagen dieses Satzes für abelsche Erweiterungen L/K von Zahlkörpern ab.

Satz. *Für abelsche Erweiterung L/K mit Galoisgruppe $G = Gal(L/K)$ gilt*

1. *$\Sigma_{L/K} \subseteq \mathcal{N}_{L/K}$ stimmen bis auf eine Menge der K-Dichte Null überein.*
2. *Zwischenkörper $K \subseteq K' \subseteq L$ entsprechen eineindeutig den Untergruppen $N(C_{K'})/N(C_K)$ der Gruppe $C_K/N(C_L)$.*
3. *Zwischenkörper $K \subseteq K' \subseteq L$ entsprechen eineindeutig den Quotientengruppen $C_K/N(C_{K'})$ der Gruppe $C_K/N(C_L)$.*
4. *G und $C_K/N(C_L)$ sind isomorph*

$$\boxed{G \cong C_K/N(C_L)}\,.$$

Insbesondere gilt $[C_K : N(C_L)] = [L : K]$.

Beweis. Offensichtlich sind *2.*) und *3.*) sind äquivalent.

Wir benutzen. Eine endliche abelsche Gruppe G ist festgelegt durch die Familie (!) $\mathcal{Q}(G)$ ihrer zyklischen Quotientengruppen: a) $\mathcal{Q}(G) \subseteq \mathcal{Q}(G') \Longrightarrow \#G \leq \#G'$. b) $\mathcal{Q}(G) \subseteq \mathcal{Q}(G')$ und $\#G = \#G' \Longrightarrow G \cong G'$. [Der Hauptsatz für endliche abelsche Gruppen]. Wir wenden dies an für $G' = C_K/N(C_L)$.

Für zyklische Erweiterungen gelten diese Aussagen. Jeder zyklischen Erweiterung K'/K in L ist die Zwischengruppe $N(C_L) \subseteq N(C_{K'}) \subseteq C_K$ zugeordnet. Die zyklische Erweiterung K'/K in L ist außerdem durch $N(C_{K'}) \subseteq C_K$ eindeutig bestimmt! Oder alternativ durch den Quotienten $C_K \twoheadrightarrow C_K/N(C_{K'})$. (Siehe 7.4). Zyklische Erweiterungen entsprechen aber zyklischen Quotienten $G \twoheadrightarrow Gal(K'/K)$ der Galoisgruppe G. Dies definiert eine Injektion

$$\mathcal{Q}(G) \subseteq \mathcal{Q}(C_K/N(L))\,.$$

Es folgt $\mathcal{Q}(G) \subseteq \mathcal{Q}(G')$, und damit $\#G \leq \#G'$. Wegen $\#G' \leq [L:K] = \#G$ (Satz 5.4) folgt $\#G = \#G'$. Aus $\mathcal{Q}(G) \subseteq \mathcal{Q}(G')$ folgt daher sogar $G \cong G'$. Dies zeigt *2.),3.),4.)*, insbesondere daher $m = [L:K] = [C_K/N(C_L)]$. Letzteres impliziert Aussage *1* dann nach Zusatz 5.4 für beliebige abelsche Erweiterungen L/K.). □

Zur Erinnerung. Für eine Stelle w von K gilt

(i) w zerfällt in $L/K \implies Bild(K_w^* \to C_K) \subseteq N(C_L)$

(ii) w ist unverzweigt in $L/K \implies Bild(\mathfrak{o}_w^* \to C_K) \subseteq N(C_L)$.

Hierbei folgt (i) aus 5.3 und (ii) aus 4.7.

Ein Ausblick. Man kann zeigen, daß für beide Implikationen (i) und (ii) auch die Umkehrung gilt! Man reduziert dies auf zyklische Erweiterung L/K. In diesem Fall hat man wegen dem Hasseschen Normensatz eine exakte Sequenz

$$0 \to K^*/N(L^*) \to \mathbb{I}_K/N(\mathbb{I}_L) \to C_K/N(C_L) \to 0\ .$$

Zum Beweis der eben erwähnten Umkehrungen braucht man eine genaue Beschreibung der im Moment noch mysteriösen zusammengesetzten Abbildung

$$K_w^* \ \to\ \mathbb{I}_K/N(C_L) \ \to\ C_K/N(C_L) \ \cong\ Gal(L/K)\ .$$

Entscheidend wird es dabei sein diese Abbildung richtig zu deuten (das Bild von K_w^* ist die Zerlegungsgruppe $G_w \subseteq G = Gal(L/K)$, wie sich in Kapitel **??** herausstellen wird). Entscheidend wird dabei sein das

Artinsche Reziprozitätsgesetz. *Für alle unverzweigten Stellen w von K wird dieser Homomorphismus gegeben durch*

$$\pi_w \cdot \mathfrak{o}_w^* \ \mapsto\ F_w \in Gal(L/K)\ .$$

Das heißt ein PRIMELEMENT π_w in K_w^* wird auf den FROBENIUS F_w in $Gal(L/K)$ abgebildet. Beachte - da w unverzweigt angenommen wurde - ist das Bild von $\mathfrak{o}_w^*$ unter dieser Abbildung notwendigerweise trivial (siehe oben).

7.6 Appendix

Satz. *Sei L/K eine primzyklische Erweiterung vom Grad p und seien die p-ten Einheitswurzeln in K. Sei $x \in K^*$ und sei $x \in N(L_w^*)$ für alle Stellen $w \neq w_0$ von K. Dann gilt $x \in N(L^*)$.*

Nach dem Hasseschen Normensatz genügt dazu $x \in N(L_{w_0})$.

Beweis. Im Fall $K_{w_0}/N(L_{w_0}^*) = 0$ ist die Aussage trivial. Im anderen Fall betrachte

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K^*/N(L^*) & \longrightarrow & \mathbb{I}_K/N(\mathbb{I}_L) & \longrightarrow & \mathbb{F}_p = C_K/N(C_L) & \longrightarrow & 0 \\ & & & & \uparrow & & \| & & \\ & & & & K_{w_0}/N(L_{w_0}^*) & \longrightarrow & \mathbb{F}_p & & \end{array}$$

Wäre $pr_{w_0}(x) \neq 0$ in $K_{w_0}/N(L_{w_0}^*)$, dann erzeugt es $K_{w_0}/N(L_{w_0}^*)$, da nach lokaler Klassenkörpertheorie gilt $K_{w_0}/N(L_{w_0}^*) \cong \mathbb{F}_p$ und die untere Abbildung wäre Null. Also genügt es zu zeigen, daß die untere Abbildung surjektiv ist.

Wäre dies nicht der Fall, wäre $K_{w_0}^*$ von x und $N(L_{w_0}^*)$ erzeugt. Also $K_{w_0}^* = N(L_{w_0}^*) \cdot \langle pr_{w_0}(x) \rangle \subseteq N(L_{w_0}^*) \cdot \langle x \rangle \cdot N(\mathbb{I}_L)$, da nach Annahme $x \cdot pr_{w_0}(x)^{-1} \in N(\mathbb{I}_L)$. Also $K_{w_0}^* \subseteq K^* \cdot N(\mathbb{I}_L)$. Nach dem Zerlegungskriterium zerfällt w_0 in der Erweiterung L/K. Es folgt $pr_{w_0}(x) \in N(L_{w_0}^*) = K_{w_0}^*$. Ein Widerspruch. □

Zerlegungssatz. *Sei L/K eine primzyklische Erweiterung vom Grad p und seien die p-ten Einheitswurzeln in K. Sei $K_w \subseteq K^* \cdot N(\mathbb{I}_L)$, dann zerfällt L/K bei w.*

Beweis. Siehe Lang p.215-217.

Kapitel 8

Artinsche L-Reihen

8.1 Definition von $Z(\rho, s)$

Sei $K/\mathbb{Q}$ eine galoissche Körpererweiterung von Zahlkörpern mit Gruppe G. Für einen endlich dimensionalen $\mathbb{C}$-Vektorraum V sei

$$\rho : Gal(K/\mathbb{Q}) \to Gl(V)$$

ein Gruppenhomomorphismus (eine sogenannte komplexe Darstellung von G). Nach dem Vorbild der RIEMANNSCHEN ZETAFUNKTION konstruieren wir ein Produkt, welches als Funktion der komplexen Variable s absolut konvergiert für $Re(s) > 1$. Das Produkt läuft über alle Stellen v von K

$$Z(\rho, s) \;=\; \prod_v Z_v(\rho, s) \; .$$

Der einfachste Fall. Für $Z(s) = Z(\mathbb{Q}, 1, s)$ und die triviale Darstellung $\rho(g) = 1$ und $dim(V) = 1$ sind die lokalen Faktoren $Z_p(s) = (1 - p^{-s})^{-1}$ für die endlichen Primstellen und $Z_\infty(s) = \pi^{-s/2}\Gamma(s/2)$ gerade die Faktoren der Riemannschen Zetafunktion.

Zerlegungsgruppen. Für jede (!) Stelle v von $\mathbb{Q}$ sei nun $G_v \subseteq G$ der Stabilisator von v in G (Zerlegungsgruppe). Sei $I_v \subseteq G_v$ die Trägheitsgruppe. Hier sei I_∞ per Definition trivial. $I_v \neq 0$ nur für Primzahlen $v = p$, welche in $K/\mathbb{Q}$ verzweigen. Ist $I_p \neq 0$, dann ist I_p ein Normalteiler in G_p. Daher operiert G_v (und damit G_v/I_v) auf dem Fixraum

$$V^{I_v} = \{v \in V \mid \rho(\sigma)v = v \; \forall \sigma \in I_v\} \; .$$

[Beachte $\rho(h)v = v$ für $h \in I_v$ impliziert $\rho(h)\rho(g)v = \rho(g)(\rho(g^{-1}hg)v) = \rho(g)v$, also $\rho(g)v \in V^{I_v}$.] Die Quotientengruppe $G_v/I_v =< F_v >$ ist zyklisch. Dies gilt für alle Stellen. Für archimedische Stellen hat G_v/I_v die Ordnung $f_v = 2$ oder $f_v = 1$, je nach dem ob $L_v/K_w = \mathbb{C}/\mathbb{R}$ ist oder nicht). Der Erzeuger F_∞ ist hierbei im letzten Fall die komplexe Konjugation. Für nicht archimedische Stellen erzeugt der geometrische Frobenius F_v die Gruppe G_v/I_v der Ordnung f_v. Wir wollen nun für jede Stelle v von $\mathbb{Q}$ einen lokalen Faktor $Z_v(\rho, s)$ definieren, welcher bezüglich ρ nur abhängt von der Operation

$$\rho(F_v) \in Gl(V^{I_v}) \; .$$

Ansatz. Wir zerlegen dazu V^{I_v} in die F_v-Eigenräume

$$V^{I_v} = \bigoplus_\mu V_\mu \quad , \quad v \in V_\mu \iff \rho(F_v)(v) = \lambda_\mu \cdot v \; .$$

Die Eigenwerte sind offensichtlich gewisse f_v-te Einheitswurzeln $\lambda_\mu = \exp(\frac{2\pi i \cdot \mu}{f_v})$. Wir setzen

$$Z_v(\rho, s) = \prod_{\mu=0}^{f_v-1} Z_v\Big(s + \frac{\log(\lambda_\mu)}{\log(p_v)}\Big)^{dim(V_\mu)}$$

für die durch die Riemannsche Zetafunktion definierten Faktoren $Z_v(s)$. Hierbei sei formal außerdem $\log(p_\infty) := \pi i$ für $v = \infty$.

Absolute Konvergenz. (Per Definition) konvergiert ein Produkt komplexer Zahlen absolut, wenn die Reihe der Logarithmen absolut konvergiert. Dabei kann man obdA endliche viele Faktoren ignorieren. Sei daher $v = p$ unverzweigt. Dann ist $Z_p(\rho, s)$ ein Produkt von $dim(V)$ Faktoren der Gestalt $(1 - \lambda_\mu p^{-s})^{-1}$. Wegen $|\lambda_\mu|_{\mathbb{C}} = 1$ besitzt $\log(1 - \lambda_\mu p^{-s})$ die Majorante $\sum_m p^{-ms}/m = \log(1 - p^{-s})$. Also ist $dim(V)\log(\zeta(s))$ eine für $Re(s) > 1$ absolut konvergente Majorante von $\log(\rho, s)$. Somit konvergiert $Z(\rho, s)$ absolut für $Re(s) > 1$, und ist insbesondere nicht Null in diesem Bereich.

□

Isomorphieinvarianz. Zwei Darstellungen (ρ_1, V_1) und (ρ_2, V_2) einer Gruppe G heißen isomorph, wenn es eine $\mathbb{C}$-linearen Isomorphismus $T : V_1 \cong V_2$ gibt mit $T\rho_1(\sigma) = \rho_2(\sigma)T$ für alle σ. Die Dimensionen der Frobenius-Eigenräumen sind für isomorphe Darstellungen dieselben. Also hängt $Z(\rho, s)$ nur von der Isomorphieklasse von ρ ab.

Summen. Für die direkte Summe der Homomorphismen $\rho = \rho_1 \oplus \rho_2$ gilt $V_\mu = (V_1)_\mu \oplus (V_2)_\mu$. Daher offensichtlich $Z(\rho, s) = Z(\rho_1, s)Z(\rho_2, s)$.

8.2 Verallgemeinerung

Sei allgemeiner L/K eine galoissche Körpererweiterung von Zahlkörpern. Für einen endlich dimensionalen $\mathbb{C}$-Vektorraum V sei

$$\rho : Gal(L/K) \to Gl(V)$$

ein Gruppenhomomorphismus (eine sogenannte Darstellung von G). Wir wollen nun als Produkt über alle Stellen v von K eine Funktion definieren

$$Z(K, \rho, s) \;=\; \prod_v Z_v(L/K, \rho, s)\ .$$

Bemerkung. Jede Surjektion $Gal(\tilde{L}/K) \twoheadrightarrow Gal(L/K)$ definiert durch Komposition einen Homomorphismus $\tilde{\rho} : Gal(\tilde{L}/K) \to Gl(V)$. Die Definition wird so sein, daß gilt $Z(\tilde{L}/K, \tilde{\rho}, s) = Z(L/K, \rho, s)$. Wir schreiben aus diesem Grund einfach nur $Z(L/K, \rho, s) = Z(K, \rho, s)$. Dies erlaubt es obdA $L/\mathbb{Q}$ galoissch anzunehmen. Dann ist $H = Gal(L/K)$ eine Untergruppe von $G = Gal(L/\mathbb{Q})$, und man definiert nun

$$Z(K, \rho, s) := Z(Ind(\rho), s)$$

durch die von ρ induzierten Darstellung $Ind(\rho)$ von G.

Induktion. Sei H Untergruppe einer G vom Index n und $\rho : H \to Gl(V)$ eine Darstellung von H. Wähle Repräsentanten σ_i der Nebenklassen $G = \coprod_{i=1}^{n} \sigma_i H$. Durch ρ wird V zu einem H-Modul. Wir definieren nun

$$W = \bigoplus_{i=1}^{n} \sigma_i V$$

als $\mathbb{C}$-Vektorraum isomorph zu V^n. Um die induzierte Darstellung $Ind(\rho)$ auf W zu definieren, muss man erklären wie $\sigma \in G$ auf W operiert: Für jedes $\sigma \in G$ und jeden Repräsentant σ_i gibt es ein eindeutig bestimmtes $j = j(i, \sigma)$ mit $\sigma\sigma_i H = \sigma_j H$ (Operation von G auf den Nebenklassen G/H). Also $\sigma\sigma_i = \sigma_j \tau$. Dies definiert $\tau = \sigma_j^{-1}\sigma\sigma_i \in H$. Per Definition

$$Ind(\rho)(\sigma)\Big(\sum_{i=1}^{n} \sigma_i \cdot v_i\Big) := \sum_{i=1}^{n} \sigma_j \cdot \rho(\sigma_j^{-1}\sigma\sigma_i)v_i$$

für die Komponenten $v_i \in V$ des Vektors $\sum \sigma_i \cdot v_i \in W$. Man sieht leicht, daß $Ind(\rho(.)$ einen Gruppenhomomorphismus von G nach $Gl(W)$ definiert. Man zeigt auch leicht $Ind(\rho_1 \oplus \rho_2) = Ind(\rho_1) \oplus Ind(\rho_2)$ und $Ind(Ind(\rho)) = Ind(\rho)$ (Induktion in Schritten für eine Kette $H_1 \subseteq H_2 \subseteq G$ von Untergruppen). Es folgt

Induktion. Ist jetzt $H = Gal(\tilde{L}/L)$ Untergruppe von $G = Gal(\tilde{L}/K)$ für Körper $K \subseteq L \subseteq \tilde{L}$, dann folgt für $\rho : H \to Gl(W)$ durch Induktion in Schritten daher sofort

$$\boxed{Z(L, \rho, s) = Z(K, Ind(\rho), s)}\,.$$

Summen. Für die direkte Summe von Homomorphismen $\rho = \rho_1 \oplus \rho_2$ wollen wir

$$\boxed{Z(K, \rho, s) = Z(K, \rho_1, s)Z(K, \rho_2, s)}\,.$$

Isomorphieinvarianz. Die Zetafunktion $Z(K,\rho,s)$ hängt nur von der Isomorphieklasse der Darstellung ρ ab. [Ein Isomorphismus $T : (\rho_1, V_1) \cong (\rho_2, V_2)$ setzt sich fort zu einem Isomorphismus $\tilde{T} : Ind(\rho_1) \to Ind(\rho_2)$ definiert durch $\tilde{T}(\sigma_i v_i) := \sigma_i T(v_i)$. Dimensionen von Frobenius-Eigenräumen bleiben unter $\tilde{T}$ daher erhalten.] Wir fassen zusammen

Lemma. *Die so definierten Funktionen $Z(K,\rho,s)$ sind kompatibel mit Isomorphie, Summen und Induktion, und konvergieren als Produkte absolut im Bereich für $Re(s) > 1$ der komplexen Ebene.*

Lokale Pole. Für die lokalen Faktoren gilt

$$ord_{s=0}\Big(Z_v(K,\rho,s)\Big) = dim_{\mathbb{C}}(V^{G_v}) \ ,$$

und $Z_v(K,\rho,s)$ ist holomorph für $Re(s) > 0$.

Globale Pole. $Z(K,\rho,s)$ ist holomorph für $Re(s) > 1$. Dies folgt unmittelbar aus der Konvergenz des Produktes und der Gestalt der Majorante (lokal gleichmässige Konvergenz in s). Für die Darstellung $\rho : G \to Gl(V)$ gilt

$$ord_{s=1}\Big(Z(K,\rho,s)\Big) = dim_{\mathbb{C}}(V^{G}) \ .$$

Diese Aussage ist alles andere als trivial, und wird erst später gezeigt werden können!

Artin Vermutung. *Die Funktionen $Z(K,\rho,s)$ besitzen meromorphe Fortsetzungen auf ganz $\mathbb{C}$ und erfüllen eine Funktionalgleichung*[1] *der Gestalt*

$$\boxed{Z(K,\rho,s) = W(\rho,s)Z(K,\overline{\rho},1-s)}$$

für die konjugiert komplexe Darstellung $\overline{\rho}$ von ρ. Hierbei ist $W(\rho,s)$ ein Faktor der Gestalt $W(\rho,s) = C(\rho)D(\rho)^s$ für Konstanten $C(\rho)$ und $D(\rho)$. Die Funktion $Z(K,\rho,s)$ ist holomorph in $\mathbb{C} \setminus \{0,1\}$.

Bemerkung. Die verallgemeinerte Riemannsche Vermutung besagt außerdem, daß alle Nullstellen der Funktionen $Z(K,\rho,s)$ auf der Gerade $Re(s) = \frac{1}{2}$ liegen.

Bemerkung. Die Artin Vermutung über die Lage der Pole in der komplexen Ebene ist bis heute unbewiesen. Die anderen Aussagen können aber bewiesen werden. Dies zu zeigen bedarf noch etlicher Anstrengungen.

[1] Die Funktionalgleichung ist genau genommen selbst nicht Teil der Artin Vermutung.

8.3 Einige Formeln

Lemma. *Für* $\rho : Gal(L/K) \to Gl(V)$ *gilt*

$$Z(K,\rho,s) = \prod_{v|\infty} Z_v(\rho,s) \prod_{P \in Div_K,\, prim} det\Big(1 - \rho(F_P)N(P)^{-s}, V^{I_P}\Big)^{-1} .$$

Beweis. ObdA ist L galoisch über $\mathbb{Q}$. Der Einfachheit halber sei p unverzweigt in $L/\mathbb{Q}$. Im zyklischen Körperturm $\mathbb{Q}_p \subseteq K_v \subseteq L_w$ erzeugt dann der Frobenius $\sigma = F_p$ die Gruppe $Gal(L_w/\mathbb{Q}_p)$, und $n := f_{p|v}$ erzeugt $F_v = F^n$ die Untergruppe $Gal(L_w/K_v)$. Wir berechnen die Eigenräume $W_\lambda \subseteq W = Ind(V)$ von σ. Aus $Ind(\rho)(\sigma)w = \lambda w$ folgt $Ind(\rho)(\sigma^n)w = \lambda^n w$.

Induktion. Sei V ein Modul einer Untergruppe $H = \langle\sigma^n\rangle$ vom Index n in der zyklischen Gruppe $\langle\sigma\rangle$. Die σ^i für $i = 0, .., n-1$ sind Repräsentanten der Nebenklassen der Untergruppe $\langle\sigma^n\rangle$. Auf $W = Ind(\rho) = V^n$ operiert σ dann via

$$\sigma(v_1, ..., v_n) = (\sigma^n v_n, v_1, .., v_{n-1}) .$$

Das heißt insbesondere $\sigma^n(v_1, ..., v_n) = (\sigma^n v_1, ..., \sigma^n v_n)$.

Eigenwerte. Aus $Ind(\rho)(\sigma)w = \lambda w$ folgt $\rho(\sigma^n)v_i = \lambda^n v_i$ für alle Komponenten $v_i \in V$ von $w = \sum_{i=0}^{n-1} v_i \in V^n = W$. Also genügt es den λ Eigenraum von $(V_{\lambda^n})^n \subseteq W$ zu berechnen (für $V_{\lambda^n} = \{v \in V \mid \rho(\sigma^n)v = \lambda^n v\}$). Dazu sei obdA $V = V_{\lambda^n}$ eindimensional! Die Matrix $\rho(\sigma)$ hat dann die Gestalt

$$\begin{pmatrix} 0 & 0...0 & 0 & \lambda^n \\ 1 & 0...0 & 0 & 0 \\ 0 & 1...0 & 0 & 0 \\ . & ..... & . & 0 \\ 0 & 0...0 & 1 & 0 \end{pmatrix}$$

und das charakteristische Polynom $\chi(X) = X^n - \lambda^n = \prod_{i=0}^{n-1}(X - \zeta_n^i\lambda)$. Mit paarweise verschiedenen Eigenwerten.

Zusammenfassung. Die Eigenwerte λ_W von σ auf der induzierten Darstellung W (mit Vielfachheiten) sind daher genau die Lösungen der Gleichung $\lambda_W^n = \lambda_V$, wobei λ_V die Eigenwerte von σ^n auf V durchläuft (mit Vielfachheiten). Es folgt

$Z_p(Ind(\rho), s) = \prod_{\lambda_V} \prod_{i=0}^{n-1} (1 - \zeta_n^i (\lambda_V)^{1/n} p^{-s})^{-1} = \prod_{\lambda_V} (1 - \lambda_V p^{-ns})^{-1}$ oder wegen $N(P_w) = \#\kappa_w = p^n$ (siehe obige Definition von n) und $F_p^n = F_w$

$$Z_p(Ind(\rho), s) = det(1 - \rho(F_w) N(P_w)^{-s})^{-1} .$$

□

Sei G zyklisch oder abelsch. Dann zeigt eine analoge Rechnung: Die von der eindimensonalen trivialen Darstellung der trivialen Untergruppe induzierte Darstellung $Ind(1)$ ist isomorph zur direkten Summe $\sum_\chi (\chi, \mathbb{C})$ aller Charaktere $\chi : G \to S^1 \subseteq Gl(1, \mathbb{C}^*)$. Für abelsche Erweiterungen L/K daher

$$\boxed{Z(L, s) = \prod_{\chi : G \to S^1} L(K, \chi, s)} .$$

Spezialfall. Ist ρ die triviale eindimensionale Darstellung, dann ergibt sich für $Z(K, \rho, s) = Z(K, s)$ die Formel

$$Z(K, s) = \prod_{v|\infty} Z_v(K, s) \prod_{P \in Div_K \ prim} (1 - N(P)^{-s})^{-1}$$

in vollkommener Analogie zur Definition der Riemannschen Zetafunktion! Da $(1 - N(P)^{-s})^{-1} = \sum_{n=0}^{\infty} N(P)^{ns}$ für $s > 1$ nur positive Glieder besitzt, folgt aus der absoluten Konvergenz durch Umordnung (dann sogar für $Re(s) > 1$)

$$\boxed{Z(K, s) = Z_\infty(s)^{r_1 + r_2} Z_\infty(s + 1)^{r_2} \sum_{I \text{ Ideal}} N(I)^{-s}} .$$

Kapitel 9

Appendix

9.1 Appendix I (Fourierreihen)

Sei X eine kompakte topologische Gruppe, zum Beispiel eine endliche Gruppe oder die Gruppe $S^1 = \mathbb{R}/\mathbb{Z}$, oder eine der verwandten Gruppen $K\backslash\mathbb{A}_K$ oder $X_K = K^* Z_K \backslash \mathbb{I}_K$. Wir fixieren auf X ein Haarmaß dx mit $vol(X, dx) = 1$. Dies definiert den Hilbertraum $L^2(X, dx)$ aller messbaren quadratintegierbaren Funktionen auf X.

Unitäre Darstellung von X. Auf diesem Hilbertraum operiert X durch Translation $f(y) \mapsto R_x(\varphi)(y) = \varphi(yx)$. Man zeigt leicht $R_{x_1 x_2} = R_{x_1} \circ R_{x_2}$, und R_x ist ein unitärer Operator auf $L^2(X, dx)$

$$X \to U\Big(L^2(X, dx)\Big) .$$

R_x besitzt daher im allgemeinen keine Spur (außer wenn X endlich ist).

Faltung. Man betrachtet daher besser eine genügend glatte Funktionen f auf X und die verschmierte Operation $R_f(\varphi) = \int_X f(x) R_x(\varphi) dx$. Man zeigt dann leicht für stetiges f, daß $R_f(\varphi)$ wieder in $L^2(X, dx)$ liegt. Wegen $R_f(\varphi)(y) = \int_X f(x)\varphi(yx)dx = \int_X f(y^{-1}x)\varphi(x)dx$ ist $Rf(\varphi)$ dann sogar glatt (nach dem Satz von der dominierten Konvergenz). R_f ist also ein Glättungsoperator mit Integralkern $K(y, x) = f(y^{-1}x)$.

Eine Variante von Glattheit. Sei U eine abgeschlossene Untergruppe von X und es gelte $f(yu) = f(y)$ für alle $u \in U$ (Periodizität bezüglich U). Dann gilt auch $R_f(\varphi)(yu) = R_f(\varphi)(y)$ für alle $u \in U$ wegen der Translationsinvarianz des Haarmaßes. Insbesondere erhält R_f dann den Hilbertraum $L^2(X/U, dx/du)$ der U-invarianten Funktionen, und wir können im Prinzip zur Quotientengruppe X/U anstatt X übergehen.

Abelsches X. Sei von nun an X abelsch. Dann bilden die Charaktere eine Basis des Hilbertraumes. [Offensichtlich sind sie orthogonal bezüglich des Skalarproduktes $\langle\varphi, \psi\rangle = \int_X \varphi(x)\overline{\psi}(x)dx$ und liegen dicht in $L^2(X, dx)$. Dazu genügt, daß Dichtigkeit in $C(X)$. Letzteres folgt aus dem Satz von Stone-Weierstraß, da nach einem allgemeinen Satz die Algebra aufgespannt von den Charakteren von X Punkte trennt. Für uns genügt der Fall $X = (S^1)^n \times E$ für endliches E, wo dies trivial ist.] Es folgt $L^2(X, dx) = \hat{\bigoplus}_{\chi \in X^D} \mathbb{C}\chi$ (siehe Skript Analysis III für den entscheidenden Fall $X = S^1$). Bezüglich dieser Basis ist $R_x(\chi) = \chi(x)\chi$

diagonal, ebenso wie daher die Mittelung

$$R_f(\chi)(y) = \chi(f) \cdot \chi(y)$$

für die komplexe Konstante $\chi(f) = \int_X f(x)\chi(x)dx$.

Beispiel. $X = K\backslash\mathbb{A}_K$ und $U = \prod_{v\nmid\infty} Q_v$ mit $Q_v = \pi_v^{n_v}\mathfrak{o}_v$ wie in 2.6 mit $X/U = (\mathbb{A}_{K,\infty}/\mathfrak{o}_K) \times \prod_{v\nmid\infty} \mathfrak{o}_v/U_v \cong (S^1)^n \times E$ für endliches $E = \prod_{v\nmid\infty} \mathfrak{o}_v/U_v$, oder $X_K = K^*Z_K\backslash\mathbb{I}_K$ und $U = \prod_{v\nmid\infty} U_v$ mit $U_v = 1 + \pi_v^{n_v}$ mit $X/U \cong (S^1)^{n-1} \times E$ für endliches E (siehe 2.10). Alle Funktionen, die wir in diesen beiden Situationen betrachten, haben eine solche Periodengruppe U. Das heißt für unsere Zwecke ist nun obdA

$$X = (S^1)^n \times E$$

ein Produkt einer endlichen Gruppe E und endlich vielen Kreisringen S^1, insbesondere also abelsch.

Lemma. *Sei E endlich abelsch und $X = E \times (S^1)^n$ und $f \in C^\infty(X)$, dann ist der Kern $K_f(x,y) = f(y^{-1}x)$ des Faltungsoperator $R_f(y) = \int_X K(y,x)\varphi(x)dx$ gleich der auf $X \times X$ absolut und gleichmäßig konvergenten Reihe*

$$K_f(x,y) = \sum_{\chi\in X^D} \chi(f)\chi(y)\overline{\chi}(x) \; .$$

Somit konvergiert die folgende Summe (genannt Spur von R_f) absolut

$$\sum_{\chi\in X^D} \chi(f) = \int_X K_f(x,x)dx \; .$$

Beweis. Beachte $X^D = E^D \times (S^1)^D \times \cdot\ldots\cdot (S^1)^D = E^D \times \mathbb{Z}^n$, denn $(S^1)^D = \{\chi_m(x) = exp(2\pi imx) \mid m \in \mathbb{Z}^n\}$ wie man sofort sieht. Man reduziert die Aussage daher leicht auf den Fall $X = E$ (siehe 1.3) und $X = (S^1)^n$. Im letzteres Fall genügt es wegen $|\chi_m(y)\overline{\chi}_m(x)| = 1$ die absolute Konvergenz der Reihe $\sum_{m\in\mathbb{Z}^n} a_m(f)$ der Fourierkoeffizienten

$$a_m(f) = \int_0^1 f(x)exp(2\pi imx)dx = \chi_m(f)$$

zu zeigen. Aus der L^2-Theorie folgt für $f \in C(X) \subseteq L^2(X)$ die Konvergenz von $\sum_m a_m(f)\chi_m(x) \to f(x)$ im L^2-Sinn, daher die absolute Konvergenz der Reihe

$\langle f, f\rangle = \sum_m |a_m|^2$. Somit $|a_m| \leq const$. Für $\Delta f = \sum_{i=1}^n \frac{\partial^2 f}{\partial x_i^2} \in C^\infty(X)$ anstatt f (etc. höhere Potenzen von Δ) gilt $a_{\Delta^k f} = (-4\pi^2\|m\|^2)^k a_f$. Daher liefert die L^2-Konvergenz sogar $|a_m| \leq const' \cdot m^{-n-1}$ für alle $m \neq 0$ (wähle $2k \geq n+1$) und damit die absolute Konvergenz wegen $\sum_{0\neq m\in\mathbb{Z}^n} \|m\|^{-n-1} < \infty$. $\square$.

Variante 1. Für einen Automorphismus $\theta : X \to X$ endlicher Ordnung setzt man $R_\theta(\varphi)(y) = \varphi(\theta^{-1}(y))$, und man kann analog wie oben $R_x R_\theta$ oder $R_f R_\theta$ betrachten. Mit demselben Argument gilt dann $R_f R_\theta(\chi)(y) = (\chi\theta)(f) \cdot \chi^\theta(y)$ für die komplexe Konstante $(\chi\theta)(f) = \int_X f(\theta(x))\chi(x)dx$, sowie für den Kern $K(y,x) = f(y^{-1}\theta(x)) = \sum_{\chi\in X^D} \chi\theta(f)\chi^\theta(y)\overline{\chi}(x)$ und für die Spur

$$\sum_{\chi=\chi^\theta} (\chi\theta)(f) = \int_X K(x,x)dx\ .$$

Variante 2. In vielen Fällen ist $X = \Gamma\backslash Y$ ein Quotient eines einfacheren aber nicht kompakten Raumes Y nach einer diskreten Gruppe Γ (z.B. $S^1 = \mathbb{Z}\backslash\mathbb{R}$ oder $\mathbb{A}_K = K\backslash\mathbb{A}_K$ für $Y = \mathbb{R}$ oder $Y = \mathbb{A}_K$ etc.). In diesen Fällen ist es oft besser eine glatte Funktion $h : Y \to \mathbb{C}$ mit kompaktem Träger $h \in C_c^\infty(Y)$ zu betrachten, sowie $f(x) = \sum_{\gamma\in\Gamma} h(\gamma + y)$ für $Y \ni y \mapsto \pi(x) = x \in X$. In diesem Fall ist $\int_X f(x)\chi(x)dx = \int_Y h(y)\chi(\pi(y))dy = \chi(h)$, wenn dx das Quotientenmaß eines Haarmaßes von Y nach dem diskreten Zählmaß auf Γ ist. Formuliert für h anstatt f erhält obiges Lemma dann die Form einer Spurformel

$$\sum_{\chi\in X^D} \chi(h) = \sum_{\gamma\in\Gamma} \int_X K(x,\gamma x)dx$$

wie in Kapitel 3.4 und 6.2.

9.2 Appendix II (Kummertheorie)

G-Moduln. Sei G eine Gruppe. Ein G-Modul ist eine abelsche Gruppe $(M,+)$ mit einem Homomorphismus $G \to Aut(M,+)$. d.h. einer Operation von G auf M, für die gilt $g(m_1+m_2) = gm_1 + gm_2$. Eine Abbildung $T : M \to N$ zwischen G-Moduln heißt G-linear, falls $gT(m) = T(gm)$ gilt für alle $g \in G, m \in M$.

Invarianten. Für einen G-Modul M sei $M^G = \{m \in M \mid gm = m \; \forall g \in G\}$ der maximale triviale G-Untermodul von M. Eine G-lineare Abbildung $T : A \to B$ induziert einen Homomorphismus $T : A^G \to B^G$ abelscher Gruppen.

Die Gruppe $H^1(G,A)$. Für eine kurze exakte Sequenz von G-Moduln erhält man eine exakte Sequenz $0 \to A^G \to B^G \to C^G$. [Beachte $A \cap B^G = A^G$. Für $b \in B^G$ mit verschwindendem Bild in C^G liegt $b \in B^G \cap A = A^G$. Also ist diese Sequenz exakt bei B^G]. Im allgemeinen ist $B^G \to C^G$ aber nicht mehr surjektiv. Für $c \in C^G \subseteq C$ gibt es ein Urbild $b \in B$, aber nicht notwendig in B^G. Das Hindernis $a(g) = gb - b$ ist im allgemeinen nicht Null. Wegen $g_1g_2b - b = (g_1b - b) + g_1(g_2b - b)$ ist die Funktion $a : g \mapsto a(g) \in A$ ein KOZYKEL, d.h. es gilt für alle $g_1, g_2 \in G$

$$\boxed{a(g_1g_2) = a(g_1) + g_1a(g_2)}\,.$$

Sei $Z^1(G)$ die Gruppe aller Kozykel $a : G \to A$. Offensichtlich bilden die KORÄNDER $g \mapsto ga - a$ (für $a \in A$) eine Untergruppe $B^1(G,A)$ von $Z^1(G,A)$. Die Kohomologiegruppe $H^1(G,A) = Z^1(G,A)/B^1(G,A)$ ist die Quotientengruppe, und der Kern des Hoimomorphismus

$$\delta : C^G \to H^1(G,A)\,,$$

welcher $c \in C^G$ auf die Klasse von $a(g)$ schickt, ist das Bild von B^G in C^G. [Liegt c im Kern von δ, gilt $a(g) = ga - a$ für ein $a \in A$. Ersetzt man b (welches $a(g) = gb - b$ definiert) durch $b - a$, gilt $c = Bild(b-a)$ und $g(b-a) = (b-a)$ für alle $g \in G$. Also hat $(b-a) \in B^G$ das Bild c.] Man erhält daher eine exakte Sequenz

$$0 \to A^G \to B^G \to C^G \to H^1(G,A)$$

Ist $H^1(G,B) = 0$, dann ist die rechte Abbildung außerdem surjektiv, denn jeder Kozykel $a(g)$ mit Werten in A hat dann die Gestalt $a(g) = gb - b$ für ein $b \in B$. Offensichtlich ist dann das Bild c von b invariant unter G. Es folgt $[a(g)] = \delta(c)$.

Hilbert Theorem 90. *Ist L/K galoissch mit Galoisgruppe G, dann gilt*

$$\boxed{H^1(G, L^*) = 0}\,.$$

Beweis. Für $a(g) \in Z^1(G, L^*)$ wähle $x \in L$ mit $y = \sum_{h\in G} a(h)h(x) \neq 0$ (lineare Unabhängigkeit der $g \in G$). Dann gilt $g(y) = \sum_h \frac{a(gh)}{a(g)} gh(x) = y/a(g)$ oder $a(g) = g(y^{-1})/(y^{-1}) \in B^1(G, L^*)$. Also ist die Klasse $[a(g)]$ gleich Null. □

Sei $\overline{K}$ der algebraische Abschluß von K (Charakteristik Null). Potenzieren mit einer Zahl $q \in \mathbb{N}$ liefert eine exakte Sequenz, deren Kern die Gruppe μ_q der q-ten Einheitswurzeln in $\overline{K}$ ist

$$0 \to \mu_q \to \overline{K}^* \to \overline{K}^* \to 0\,.$$

Dies ist eine Sequenz von $G = G_K$-Moduln für die absolute Galoisgruppe G_K von K (Appendix III). Aus $(\overline{K}^*)^G = K^*$ und Hilbert Satz 90 folgt

$$0 \to (\mu_q)^G \to K^* \to K^* \to H^1(G, \mu_q) \to 0\,.$$

Also $\delta : K^*/(K^*)^q \cong H^1(G, \mu_q)$. Liegt μ_q in K^*, operiert G trivial auf μ_q. Aus der Definition von Kozykeln folgt dann sofort

Satz. *Sei K ein Körper (der Charakteristik Null), der die q-ten Einheitswurzeln enthält, dann gilt*

$$\delta : K^*/(K^*)^q \;\cong\; Hom(G_K, \mu_q)\,.$$

Bemerkung. Die rechte Seite beschreibt die abelschen Galoiserweiterungen von K, deren Galoisgruppe von q annuliert wird.

Äquivarianz. Für eine exakte Sequenz $0 \to A \to B \to C \to 0$ von G-Moduln, auf der eine Gruppe Δ äquivariant operiert, ist der Verbindungshomomorphismus $\delta : C^G \to H^1(G, A)$ definiert durch $\delta(c) = a(g) = (g-1)b$ für $b \in B$ mit Bild c. Für $\theta \in \Delta$ gilt daher $\theta(\delta(c)(\theta^{-1}g)) = \theta((\theta^{-1}g - 1)c) = (g-1)\theta(c) = \delta(\theta c)$. Also ist der Verbindungshomomorphismus Δ-äquivariant.

Anwendung. Für die Kummertheorie hat dies folgende Anwendung. Sei K ein Körper (der Charakteristik $\neq p$), der eine primitive q-te Einheitswurzel enthält. Für die absolute Galoisgruppe G_K von K gilt dann (funktoriell !)

$$\delta :\; K^*/(K^*)^q \cong Hom(G_K, \mu_q)\,,$$

wobei der Nebenklasse $x(K^*)^p$ der Charakter $\rho(\sigma) = \sigma(x^{1/q})/x^{1/q}$ zugeordnet wird. Dieser Isomorphismus ist $Aut(K)$-äquivariant. Die Gruppe $Aut(K) = Gal(K/\mathbb{Q})$ operiert dabei auf μ_q mit dem zyklotomischen Charakter.

9.3 Appendix III (Projektive Limiten)

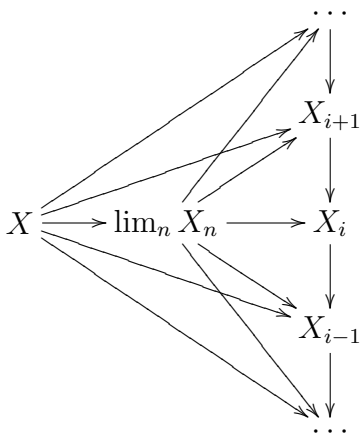
Seien X_i für $i = 0, 1, 2, ..$ Ringe und $p_i : X_i \to X_{i-1}$ Ringhomomorphismen. Dann erklärt man den projektiven Limes

$$\lim_n X_n = \lim_n (X_i, p_i)$$

als den Unterring des kartesischen Produktes

$$\lim_n X_n \subseteq \prod_{n=1}^{\infty} X_n$$

aller Elemente $(\cdots, x_i, x_{i-1}, \cdots) \in \prod_{i=1}^{\infty} X_n$ mit der Eigenschaft $p_i(x_i) = x_{i-1}$. Offensichtlich hat man natürliche Ringhomomorphismen $\psi_n : \lim_n X_n \to X_n$ definiert durch $\psi_n(\cdots, x_i, x_{i-1}, \cdots) = x_n$. Diese machen das Diagram



kommutativ. Sind $\varphi_n : X \to X_n$ Ringhomomorphismen $\varphi_n : X \to X_n$ mit $p_n \circ \varphi_n = \varphi_{n-1}$ für alle n, dann existiert ein eindeutig bestimmter Ringhomomorphismus $\varphi : X \to \lim_n X_n$, so daß gilt $\varphi_n = \psi_n \circ \varphi$ für alle n. Diese universelle Eigenschaft des projektiven Limes, bestimmt $\lim_n X_n$ zusammen mit allen ψ_n eindeutig bis auf Isomorphie.

Beispiele. 1) Für $X_n = X$ mit $p_n = id_X$ ist $\lim_n X_n = X$. 2) Für $X = \mathbb{Z}/p^n\mathbb{Z}$ und die kanonischen Projektionen $p_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^{n-1}\mathbb{Z}$ ist $\lim_n X_n = \mathbb{Z}_p$ der Ring der p-adisch ganzen Zahlen. 3) Für einen Ring R und ein Ideal $I \subseteq R$ sei $X_n = R/I^n$ und $p_n(x \mod I^n) = x \mod I^{n-1}$. Den projektiven Limes dieses

Systems nennt man die I-adische Komplettierung von R. Ist der natürliche Ringhomomorphismus von R in diese Komplettierung ein Isomorphismus, nennt man R vollständig (bezüglich I). In diesem Sinn ist für Zahlringe $R = \mathfrak{o}_K$ und ein Primideal $I = P$ eines Zahlkörpers der lokale Ring $\mathfrak{o}_P$ die P-adische Komplettierung. Siehe 2.5.

Varianten. Seien $p_i : M_i \to M_{i-1}$ Homomorphismen von R_n-Moduln mit der Eigenschaft $p_i(rm) = p_i(r)p_i(m)$ für $r \in R_i$ und $m \in M_i$ (für alle i) und ein projektives System $p_i : R_i \to R_{i-1}$ von Ringen. Für ein solches 'projektives System' (M_i, p_i) erklärt man analog wie oben den projektiven Limes $\lim_n M_n \subseteq \prod_n M_n$. Für den Limesring $R = \lim_n R_n$ wird M zu einem R-Modul.

Gruppen. An Stelle der Indexmenge $\mathbb{Z}$ kann auch eine andere gerichtete Menge treten, etwa die Menge aller endlich separablen Körpererweiterungen L/K eines Körpers. Setzt man $X_{L/K} = Gal(L/K)$, dann hat man natürliche Gruppenhomomorphismen $X_{L/K} \to X_{K'K}$ im Fall $K \subseteq K' \subseteq L$. Man kann ähnlich wie oben wieder den projektiven Limes definieren $G_K = \lim_{L/K} X_{L/K}$, die sogenannte absolute Galoisgruppe G_K des Körpers K. Versehen mit die endlichen Faktoren $Gal(L/K)$ mit der diskreten Topologie, und G_K mit der vom Produkt $\prod_{L/K} Gal(L/K)$ induzierten Einschränkungstopologie ist G_K nach dem Satz von Tychonoff in natürlicher Weise eine kompakte topologische Gruppe.

Exakte Sequenzen. Seien alle waagrechten Zeilen des folgenden Diagramms kurz exakt, und $(A_n), (B_n), (C_n)$ seien projektive Systeme abelscher Gruppen, und das Diagramm sei kommutativ

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A_n & \longrightarrow & B_n & \longrightarrow & C_n & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & A_{n-1} & \longrightarrow & B_{n-1} & \longrightarrow & C_{n-1} & \longrightarrow & 0 \end{array}$$

Dann ist die Sequenz der Limiten exakt

$$0 \to \lim_n A_n \to \lim_n B_n \to \lim_n C_n \to 0 \ ,$$

falls die Übergangsabbildungen $p_n : A_n \to A_{n-1}$ surjektiv sind fast alle n (dies ist eine leichte Übungsaufgabe).

9.4 Appendix IV ($H^1(G, C_L) = 0$)

Kozykelrelationen. Sei $a(g)$ ein Kozykel von G. Gilt $a(h) = 0$ für alle $h \in H$ in einer Untergruppe $H \subseteq G$, dann implizieren die Kozykel Relationen $a(gh) = a(g) + ga(h) = a(g)$ und $a(hg) = ha(g) + a(h) = ha(g)$ für $h \in H$ und $g \in G$. Aus den Relationen folgt im übrigen $a(1) = a(1 \cdot 1) = a(1)a(1)$, also $a(1) = 0$.

Normalteiler. Ist H ein Normalteiler, gilt sogar $ha(g) = a(hg) = a(g(g^{-1}hg)) = a(g)$. Also $a(g) \in M^H$ und damit

$$a(g) \in Z^1(G/H, M^H) \; .$$

Zyklisches G. Ist $G = \langle \sigma \rangle$ zyklisch von der Ordnung n, setze $a = a(\sigma)$. Aus den Kozykelrelationen folgt $N(a) = a\sigma(a) \cdots \sigma^{n-1}(a) = a(\sigma^n) = a(1) = 0$. Gilt $a \in (\sigma - 1)M$, folgt sofort $a(g) \in B^1(G, M)$. [Beachte, $a(g)$ ist durch den Wert $a = a(\sigma)$ eindeutig festgelegt].

Lemma. *Für beliebige galoissche Erweiterungen L/K von Zahlkörpern mit Galoisgruppe G gilt*

$$\boxed{H^1(G, C_L) = 0} \; .$$

Beweis. L/K zyklisch. Für $x \in \mathbb{I}_L$ werde die Restklasse in C_L von der Norm N annuliert, d.h. $N(x) \in L^*$ oder $N(x) \in L^* \cap N(I_L) = K^* \cap N(\mathbb{I}_L)$. Wegen dem Normensatz von Hasse 6.5 gilt dann $N(x) = N(\delta)$ für ein $\delta \in L^*$. Also $N(x/\delta) = 1$ und damit $x/\delta \in (\sigma - 1)\mathbb{I}_L$ wegen $H^1(G, \mathbb{I}_L) = 0$ (siehe 1.2). Somit ist die Klasse von x in C_L bereits in der Untergruppe $(\sigma - 1)C_L$. Es folgt $H^1(G, C_L) = 0$ für zyklische Erweiterung L/K mit Galoisgruppe G.

L/K auflösbar. Für auflösbares G (etwa eine p-Sylowgruppe) ist $H^1(G, C_L) = 0$. [G besitzt einen zyklischen Normalteiler $H \neq 0$. Für zyklisches $H = Gal(L/L^H)$ gilt $H^1(H, C_L) = 0$. Für $a(g) \in Z^1(G, C_L)$ gilt daher obdA $a(h) = 0$ für $h \in H$ durch Abändern mit einem Korand. Nach den Vorbemerkungen ist dann a ein Kozykel der Faktorgruppe $G/H = Gal(L^H/K)$ mit Werten in $C_{L^H} = (C_L)^H$ ($H^1(H, L^*) = 0$ liefert $(C_L)^H = \mathbb{I}_{L^H}/(L^H)^* = C_{L^H}$). Man schließt dann per Induktion nach $\#G$.]

Allgemeiner Fall. Wäre $H^1(G, M) \neq 1$ für $M = C_L$, so existiert eine Klasse $[a(g)] \neq 0$ in $H^1(G, M)$ mit Primzahlordnung p. Sei H eine p-Sylowgruppe von G. Da H auflösbar ist, liegt wie bereits gezeigt $a(h) \in B^1(H, M)$. Durch Abändern mit einem Korand gilt obdA $a(h) = 0$ für alle $h \in H$.

Nach obigen Vorbemerkungen ist dann folgendes Element $m \in M$ wohldefiniert

$$m = \sum_{\tilde{g} \in G/H} a(\tilde{g}H) \; .$$

$gm = \sum_{\tilde{g} \in G/H} ga(\tilde{g}H) = \sum_{\tilde{g} \in G/H} \big(a(g\tilde{g}H) - a(g)\big) = m - [G : H]a(g)$ liefert $[G : H]a(g) = m - gm \in B^1(G, M)$. Also $[G : H][a(g)] = 0$. Da p und $[G : H]$ teilerfremd sind, folgt $[a(g)] = 0$. Ein Widerspruch! $\square$