Das Bild des Haar-Maßes von 2x2-Matrizen über lokalen Körpern unter der Spur-Norm-Abbildung

Diplomarbeit
zur Erlangung des akademischen Grades eines Diplom-Mathematikers
der Naturwissenschaftlich-Technischen Fakultät I
der Universität des Saarlandes

Bernd Mehnert

Saarbrücken, Oktober 2004

Betreuer: Prof. Dr. Ernst-Ulrich Gekeler

Ich erkläre hiermit an Eides statt, diese Arbeit selbständig geschrieben und keine Hilfsmittel außer den angegebenen verwendet zu haben.

Inhaltsverzeichnis

1 Einleitung

Es sei p eine Primzahl und es bezeichne $\mathbb{Z}_p$ den Ring der $p-$adischen ganzen Zahlen. Ferner sei η das normierte Haar-Maß auf $\mathbb{Z}_p^2$ und ξ das normierte Haar-Maß auf der Menge M der $2 \times 2-$Matrizen über $\mathbb{Z}_p$. Wir definieren die *Spur-Norm-Abbildung* auf M als die Abbildung

$$T : M \to \mathbb{Z}_p^2$$

gegeben durch

$$A \mapsto (\mathrm{Spur}(A), \mathrm{Det}(A)) \; .$$

Es ist leicht einzusehen, dass T stetig ist. Deshalb können wir das Bild $\nu = T(\xi)$ von ξ unter T betrachten. ν ist ein topologisches Maß auf $\mathbb{Z}_p^2$ und ist nach Definition für alle Borel-Mengen B aus $\mathbb{Z}_p^2$ gegeben durch

$$\nu(B) = \xi(T^{-1}(B)) \; .$$

Auf Grund der Normiertheit von ξ handelt es sich bei ν also um ein Wahrscheinlichkeitsmaß. $\nu(B)$ gibt die Wahrscheinlichkeit dafür an, dass eine Matrix A in M die Beziehung $T(A) \in B$ erfüllt.

Das Maß ν steht in engem Zusammenhang mit den Konstanten

$$\gamma_k(t,u) = \left\{ A \in \mathrm{Mat}(2, \mathbb{Z}/p^k\mathbb{Z}) : \mathrm{Spur}(A) = t \mod p^k, \mathrm{Det}(A) = u \mod p^k \right\} \; ,$$

wo t und u ganze Zahlen sind und k eine natürliche Zahl ist. Wir werden später (auch in einem allgemeineren Rahmen) sehen, dass die Beziehung

$$\gamma_k(t,u) = \nu((t,u) + p^k\mathbb{Z}_p^2) \cdot p^{4k}$$

gilt.

In einer Arbeit von Lang und Trotter (siehe [7], §7) wird gezeigt, dass ν eine stetige Dichte bezüglich η besitzt. D.h. es wird bewiesen, dass es eine stetige Funktion $f : \mathbb{Z}_p^2 \to \mathbb{R}$ mit

$$\nu(B) = \int_B f(x) d\eta(x)$$

für alle Borel-Mengen B in $\mathbb{Z}_p^2$ gibt. Neben anderen Eigenschaften von f sichern Lang und Trotter z.B. auch die Konstanz von f in einer Umgebung jedes Punktes $(t,u) \in \mathbb{Z}_p^2$, für den $D = t^2 - 4u \neq 0$ gilt.

Eine explizite Formel für f wird in der Arbeit von Gekeler (siehe [4], Remark 3.11) gegeben. Diese wird aus expliziten Formeln für die Konstanten $\gamma_k(t,u)$ gewonnen:

Für ein Paar $(t,u) \in \mathbb{Z}_p^2$ wird dort im Fall $D = t^2 - 4u \neq 0$ eine nicht negative ganze Zahl d bestimmt, die maximal ist mit

$$\begin{cases} p^{2d} | D & \text{falls } p > 2 \text{ gilt,} \\ p^{2d} | D \text{ und } D/p^{2d} \text{ ist ein Quadrat} \mod 4 & \text{falls } p = 2 \text{ gilt.} \end{cases}$$

Dann erhält Gekeler die folgende Formel:

$$f(t,u) = 1 + p^{-1} + \begin{cases} 0 & \text{falls } \left(\frac{D/p^{2d}}{p}\right) = 1 \text{ gilt,} \\ -(1+p)p^{-d-2} & \text{falls } \left(\frac{D/p^{2d}}{p}\right) = 0 \text{ gilt,} \\ -2 \cdot p^{-d-1} & \text{falls } \left(\frac{D/p^{2d}}{p}\right) = -1 \text{ gilt.} \end{cases}$$

Gilt $D = t^2 - 4u = 0$, so wird aus Gründen der Stetigkeit $f(t,u) = 1 + p^{-1}$ gesetzt. Dabei ist $\left(\frac{\cdot}{p}\right)$ für $p > 2$ das "Legendre-Symbol" und $\left(\frac{\cdot}{2}\right)$ das "Kronecker-Symbol", dessen Werte von Kongruenzen modulo 8 abhängen.

In der vorliegenden Arbeit betrachten wir die folgende, allgemeine Situation: Es sei K ein beliebiger lokaler Körper mit Ganzheitsring $\mathcal{O}_K$. Ferner vereinbaren wir

$$\begin{aligned} M &= \mathrm{Mat}(2, \mathcal{O}_K)\ , \\ \alpha &= \text{das Haar-Maß auf } K^2 \text{ mit } \alpha(\mathcal{O}_K^2) = 1\ , \\ \beta &= \text{das Haar-Maß auf } \mathrm{Mat}(2, K) \text{ mit } \beta(M) = 1\ . \end{aligned}$$

Weiter bezeichnen wir mit β_M die Einschränkung von β auf M, d.h. es gelte $\beta_M(B) = \beta(B \cap M)$ für alle Borel-Mengen B in $\mathrm{Mat}(2, K)$. Schließlich sei

$$T : \mathrm{Mat}(2, K) \to K^2\ ,\ A \mapsto (\mathrm{Spur}(A), \mathrm{Det}(A))$$

die Spur-Norm-Abbildung. Dann werden wir unter Anderem eine explizite Formel für eine stetige Dichte h des Maßes

$$\mu = T(\beta_M)$$

bezüglich α berechnen. Insbesondere werden wir also die Existenz einer solchen Dichte erhalten. Aus diesem "Hauptergebnis" werden schließlich einige Folgerungen gezogen. Ist speziell $K = \mathbb{Q}_p$ und $\mathcal{O}_K = \mathbb{Z}_p$, so ist die Einschränkung unseres Maßes μ auf $\mathbb{Z}_p^2$ gerade ν. Aus der expliziten Formel für h kann dann die oben angegebene Formel für f leicht erhalten werden. Aus der Kenntnis von h gewinnen wir z.B. auch die von Gekeler gefundene Formel für die Konstanten $\gamma_k(t,u)$ (siehe hierzu [4], Prop. 3.10) zurück.

Lang und Trotter gelangen im Wesentlichen auf maßtheoretischem Wege zur Existenz der Dichte f. Dabei sind ihre Methoden so konstruktiv, dass es nicht schwer ist, daraus die oben angegebene explizite Formel für f zu erhalten. Mehr noch, indem wir im Prinzip so vorgehen, wie Lang und Trotter, werden wir unsere explizite Formel für h gewinnen. Unter allen weiteren Methoden (darunter auch unsere ursprüngliche) zur Bestimmung von h, halten wir diesen maßtheoretischen Ansatz für den elegantesten.

Im Abschnitt 2 unserer Arbeit werden die Definition und die wichtigsten Eigenschaften lokaler Körper gegeben. Damit werden die Grundlagen für alles weitere gelegt.

In unserer Formel für h wird im Fall $\mathrm{Char}(K) \neq 2$ das "Hilbert-Symbol" eingehen. Ferner wird in Charakteristik 2 das "Artin-Schreier-Symbol" eine Rolle spielen. Die gesonderte Behandlung dieser beiden neuen Symbole erfolgt im Abschnitt 3.

Grundlegend für das Erreichen unseres Ergebnisses ist die Transformationsformel für lokale Körper. Eine Version dieser Formel wird in Abschnitt 4 gegeben. Ihr Beweis ist im Kern aus dem Buch von Igusa (siehe [5]) entnommen.

Schließlich erfolgt die Berechnung von h im Abschnitt 5. Wir bemerken noch, dass wir die Spur-Norm-Abbildung auf natürliche Weise verallgemeinern werden und vieles, was wir an Aussagen über h benötigen werden, in allgemeinerer Form abhandeln werden.

Ich möchte mich bei Herrn Prof. Gekeler für dieses interessante Thema bedanken. Insbesondere gilt ihm mein Dank auch für die gute Betreuung während der Bearbeitung und auch für das Durchlesen des Kerns der Arbeit. Außerdem möchte ich mich bei Frau Dipl. Math. Alice Keller bedanken, die mir oft mit guten Ratschlägen zur Seite stand.

2 Grundlagen

Wir gehen davon aus, dass der Leser dieser Arbeit mit den elementaren Begriffen und Aussagen aus der Topologie vertraut ist. D.h. Begriffe wie “topologischer Raum”, “Basis”, ”Umgebungsbasis”, “metrischer Raum”, “hausdorffsch”, “offen”, “abgeschlossen”, “kompakt”, etc. ... sollten bekannt sein.

Ferner verwenden wir in der Arbeit die Lebesgue-Integration von Maßen. Die wichtigsten Begriffe dieser Theorie werden jedoch, bevor sie eingesetzt werden, noch einmal kurz wiederholt.

Schließlich ist es hilfreich, wenn der Leser über elementare Kenntnisse aus der linearen Algebra, der Algebra und der elementaren Zahlentheorie verfügt. Begriffe wie “Gruppe”, ”Ring”, ”Körper”, ”Körper-Erweiterung”, ”Spur”, ”Norm”, “Elementarteilersatz”, etc... sollten geläufig sein.

In der ganzen Arbeit bezeichnen die Symbole $\mathbb{P}$, $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ die Menge der Primzahlen, der natürlichen Zahlen (d.h. der Zahlen {1,2,3,...}), der ganzen Zahlen, der rationalen Zahlen und der rellen Zahlen. Außerdem sei $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$. Und für ein $n \in \mathbb{N}$ setzen wir $\mathbb{N}_n := \{1, 2, 3, ..., n\}$. Ferner sei $\mathbb{F}_q$ mit $q = p^f$ und $p \in \mathbb{P}$ der endliche Körper mit q Elementen. Alle $\mathbb{F}_q$ gleicher Charakteristik seien in einen festen algebraischen Abschluss eingebettet. Außerdem sei $\widehat{\mathbb{R}} = \mathbb{R} \cup \{-\infty, +\infty\}$ die übliche Kompaktifizierung von $\mathbb{R}$. D.h. wir erweitern die Ordnung von $\mathbb{R}$, indem wir für alle $x \in \mathbb{R}$

$$-\infty < x < +\infty$$

setzen, und definieren Umgebungsbasen von $-\infty$ bzw. $+\infty$ durch die Mengen

$$[-\infty, a[:= \{x \in \widehat{\mathbb{R}} : -\infty \leq x < a\} \quad \text{bzw.} \quad]a, +\infty] := \{x \in \widehat{\mathbb{R}} : a < x \leq +\infty\}$$

mit $a \in \mathbb{R}$. Eine Umgebungsbasis eines Punkte $x \in \mathbb{R}$ ist nach wie vor durch die Mengen $]x - \epsilon, x + \epsilon[$ für $\epsilon > 0$ gegeben. Damit wird $\widehat{\mathbb{R}}$ zu einem kompakten topologischen Raum. Außerdem setzen wir dort, wo es möglich ist, die Addition und die Multiplikation von $\mathbb{R}$ so auf $\widehat{\mathbb{R}}$ fort, dass sie bezüglich unserer Topologie stetig wird. Wie üblich sind das z.B. für $a \in \mathbb{R}$ und $b \in \mathbb{R}$ mit $b > 0$ die Konventionen

$$a \pm \infty := \pm\infty \ , \ b \cdot \pm\infty := \pm\infty \ , \ \pm\infty + \pm\infty = \pm\infty \text{ , etc...}$$

Wir schreiben für $+\infty$ auch ∞.

Für einen kommutativen Ring R mit Eins bezeichne $\mathrm{Mat}(n, m, R)$ die $n \times m-$Matrizen über R. Dabei setzen wir speziell $\mathrm{Mat}(n, R) := \mathrm{Mat}(n, n, R)$. Außerdem sei $\mathrm{GL}(n, R)$ die Gruppe der invertierbaren Matrizen aus $\mathrm{Mat}(n, R)$. Ferner bezeichne I_n die Einheitsmatrix in $\mathrm{Mat}(n, R)$. Wir müssen I_n nicht zusätzlich mit R indizieren, denn es wird immer klar sein, in welchem Matrizen-Ring wir rechnen. Ferner schreiben wir Elemente a aus R^n stets als Zeilenvektoren $a = (a_1, a_2, ..., a_n)$ und meinen für eine Matrix $A \in \mathrm{Mat}(n, R)$ mit Aa die gewöhnliche Matrixmultiplikation von A

mit a transponiert. Den obigen Zeilenvektor a schreiben wir manchmal auch als $(a_i)_{i=1}^n$. Weiter bezeichnen wir mit $R[X_1, X_2, ..., X_m]$ den Polynomring in m Variablen $X_1, X_2, ..., X_m$ über R.

Es sei $L|K$ eine endliche Körpererweiterung. Wir bezeichnen für ein $a \in L$ die Norm von a bzw. die Spur von a bezüglich $L|K$ mit $\mathrm{N}_{L|K}(a)$ bzw. mit $\mathrm{Tr}_{L|K}(a)$. Und falls $L|K$ überdies galoissch ist, bezeichnen wir mit $\mathrm{Gal}(L|K)$ die Gruppe von $L|K$. Außerdem bezeichnen wir mit $\mathrm{Char}(K)$ die Charakteristik von K. Schließlich sei mit $\overline{K}$ ein fester algebraischer Abschluss von K gemeint.

2.1 Lokale Körper

Wir legen nun die nötigen Grundlagen für alles weitere in dieser Arbeit. Bei der Einführung des Begriffes des "lokalen Körpers" folgen wir dem Buch von Serre (siehe [11]).

2.1.1 Definition und Beispiele

Definition 2.1. Ein *diskret bewerteter* Körper ist ein Körper K, versehen mit einer *diskreten Bewertung* v_K (der Bewertung von K), d.h. einer Abbildung

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

mit den folgenden Eigenschaften:

(i) $v_K(a) = \infty$ gilt genau dann, falls $a = 0$ gilt.

(ii) $v_K : K^* \to \mathbb{Z}$ ist ein surjektiver Homomorphismus von der multiplikativen Gruppe K^* in die additive Gruppe $\mathbb{Z}$. Ferner gilt

(iii) $v_K(a + b) \geq \min\{v_K(a), v_K(b)\}$ für alle a, b in K.

Dafür haben wir den folgenden Satz:

Satz/Definition 2.2. *Es sei K ein diskret bewerteter Körper mit Bewertung v_K. Dann ist die Menge*
$$\mathcal{O}_K := \{x \in K : v_K(x) \geq 0\}$$
ein Hauptidealring mit der Einheitengruppe
$$\mathcal{O}_K^* := \{x \in K : v_K(x) = 0\}$$
und dem einzigen maximalen Ideal
$$\mathfrak{p}_K := \{x \in K : v_K(x) > 0\} \ .$$
$\mathcal{O}_K$ *heißt der* Ring der ganzen Zahlen *oder* Ganzheitsring von K, $\mathfrak{p}_K$ *das* Primideal von K *und der Körper* $F_K := \mathcal{O}_K/\mathfrak{p}_K$ *der* Restkörper von K. *Schließlich heißt ein Erzeuger von* $\mathfrak{p}_K$, *d.h. ein Element* $\pi \in \mathcal{O}_K$ *mit* $\mathfrak{p}_K = \pi\mathcal{O}_K$ *eine* Uniformisierende von K.

Beweis. Siehe das Buch von Neukirch ([8], Kapitel II, § 3, Satz 3.8, Satz 3.9). □

Proposition 2.3. *Es sei K ein diskret bewerteter Körper mit Bewertung v_K und π eine Uniformisierende von K, dann gilt für jedes x aus K^* die Beziehung*
$$x = \pi^{v_K(x)}\epsilon$$
mit einer Einheit ϵ aus $\mathcal{O}_K^*$.

Beweis. Nach Definition von $\pi \in \mathfrak{p}_K$ und der Surjektivität von v_K muss $v_K(\pi) = 1$ gelten. Daraus folgern wir für ein beliebiges k aus $\mathbb{Z}$ die Beziehung $v_K(\pi^k) = kv_K(\pi) = k$. Wegen
$$v_K\left(\frac{x}{\pi^{v_K(x)}}\right) = v_K(x) - v_K\left(\pi^{v_K(x)}\right) = v_K(x) - v_K(x) = 0$$
folgt schließlich, dass $x/\pi^{v_K(x)}$ in $\mathcal{O}_K^*$ liegt und das war zu zeigen. □

Nun kommen wir zur Topologie eines diskret bewerteten Körpers K:
Wir wählen uns irgendeine reelle Zahl δ mit $0 < \delta < 1$ und vereinbaren $\delta^\infty := 0$. Setzen wir für alle $x \in K$
$$\|x\| := \delta^{v_K(x)} \ ,$$
so erhalten wir eine nicht negative Abbildung $\|\cdot\| : K \to \mathbb{R}$, welche die folgenden Eigenschaften hat:

(i) $\|x\| = 0$ gilt genau dann, falls $x = 0$ gilt. Ferner gilt

(ii) $\|xy\| = \|x\| \|y\|$ für alle x, y in K. Außerdem gilt

(iii) $\|x + y\| \leq \max\{\|x\|, \|y\|\}$ für alle x, y aus K.

Dies folgt auf Grund der Eigenschaften von v_K. D.h. durch $\|\cdot\|$ ist ein *nichtarchimedischer Absolutbetrag* auf K gegeben. Insbesondere wird K vermöge der Distanzfunktion

$$d(\cdot,\cdot) : K \times K \to \mathbb{R}\ ,\ d(x,y) := \|x - y\|$$

zu einem metrischen Raum. Überdies sind, wie leicht nachgeprüft werden kann, die Addition und die Multiplikation von K bezüglich dieser Metrik stetig. D.h. K wird zu einem *topologischen Körper*.

Beispiel 2.4. Es sei K ein diskret bewerteter Körper mit Bewertung v_K und π eine Uniformisierende von K. Ferner seien δ und $\|\cdot\|$ wie oben gewählt. Für ein beliebiges $a \in K$ und ein $k \in \mathbb{Z}$ haben wir

$$\|x - a\| < \delta^k \Leftrightarrow \delta^{v_K(x-a)} < \delta^k \Leftrightarrow v_K(x - a) > k \Leftrightarrow x - a \in \pi^{k+1}\mathcal{O}_K\ .$$

D.h. bezüglich der von $\|\cdot\|$ erzeugten Topologie auf K ist eine Umgebungsbasis eines Elementes $a \in K$ durch die Mengen $a + \pi^k\mathcal{O}_K$ mit $k \in \mathbb{Z}$ gegeben.

Das obige Beispiel zeigt, dass die durch $\|\cdot\|$ induzierte Topologie auf einem diskret bewerteten Körper K unabhängig davon ist, welche Konstante δ wir wählen. Deswegen definieren wir:

Definition 2.5. Es sei K ein diskret bewerteter Körper. Wählen wir ein δ und $\|\cdot\|$ wie oben, so heißt die von $\|\cdot\|$ auf K induzierte Topologie die *Topologie von K*.

Nun können wir den Begriff des lokalen Körpers einführen:

Definition 2.6. Ein *lokaler Körper* ist ein diskret bewerteter Körper K mit Bewertung v_K, der einen endlichen Restkörper F_K besitzt und dessen Topologie vollständig ist. Ist q die Kardinalität von F_K, so setzen wir für alle $x \in K$

$$|x|_K := q^{-v_K(x)}$$

und nennen $|\cdot|_K$ *den Absolutbetrag von K* (d.h. wir wählen $|\cdot|_K := \|\cdot\|$ mit $\delta := q^{-1}$). Dieser (als einer von vielen Vertretern) definiert die Topologie von K.

Beispiel 2.7. Wir geben skizziert zwei wichtige Beispiele lokaler Körper an:

(i) Es sei $p \in \mathbb{P}$ eine Primzahl. Bekanntlich kann jede Zahl $a \in \mathbb{Q}^*$ in eindeutiger Weise als $a = p^{u(a)}\frac{x}{y}$ mit $u(a), x \in \mathbb{Z}$, $y \in \mathbb{N}$ und $p \nmid xy$ geschrieben werden. Setzen wir

$$|a|_p := \begin{cases} p^{-u(a)} & \text{falls } a \neq 0 \text{ gilt,} \\ 0 & \text{sonst,} \end{cases}$$

so überprüfen wir leicht, dass $|\cdot|_p$ ein nichtarchimedischer Absolutbetrag auf $\mathbb{Q}$ darstellt. Die bis auf Isomorphie eindeutige Vervollständigung von $\mathbb{Q}$ bezüglich $|\cdot|_p$, die wieder ein Körper ist, sei mit $\mathbb{Q}_p$ bezeichnet. $\mathbb{Q}_p$ heißt *Körper der $p-$adischen Zahlen*. Der Prozess der Vervollständigung liefert uns eine Einbettung $\mathbb{Q} \hookrightarrow \mathbb{Q}_p$ und eine Fortsetzung $|\cdot|_{\mathbb{Q}_p}$ unseres Betrages $|\cdot|_p$ auf $\mathbb{Q}_p$. Da $\mathbb{Q}$ in $\mathbb{Q}_p$ dicht liegt und da offenbar $|\mathbb{Q}^*|_p = p^{\mathbb{Z}}$ gilt, folgt zwingend $\left|\mathbb{Q}_p^*\right|_{\mathbb{Q}_p} = p^{\mathbb{Z}}$. Außerdem muss $|\cdot|_{\mathbb{Q}_p}$ wieder ein nichtarchimedischer Absolutbetrag sein. Definieren wir für ein a aus $\mathbb{Q}$

$$v_{\mathbb{Q}_p}(a) := \begin{cases} k & \text{falls } a \neq 0 \text{ und } |a|_{\mathbb{Q}_p} = p^{-k} \text{ gilt,} \\ \infty & \text{sonst,} \end{cases}$$

so erhalten wir offenbar eine diskrete Bewertung $v_{\mathbb{Q}_p}$ auf $\mathbb{Q}_p$. Wir sehen also, dass $\mathbb{Q}_p$ mit $v_{\mathbb{Q}_p}$ zu einem diskret bewerteten Körper wird. Der Ganzheitsring von $\mathbb{Q}_p$ wird mit $\mathbb{Z}_p$ bezeichnet und heißt Ring der *$p-$adischen ganzen Zahlen*. Ferner haben wir $\mathfrak{p}_{\mathbb{Q}_p} = p\mathbb{Z}_p$. Schließlich überlegen wir uns die Isomorphie

$$\mathbb{Z}/p\mathbb{Z} \cong \mathbb{Z}_p/p\mathbb{Z}_p$$

und sehen, dass der Restkörper $F_{\mathbb{Q}_p}$ von $\mathbb{Q}_p$ endlich und isomorph zu $\mathbb{Z}/p\mathbb{Z}$ ist. Damit ist also $\mathbb{Q}_p$ ein diskret bewerteter Körper, der bezüglich seiner Topologie vollständig ist und dessen Restkörper endlich ist, d.h. $\mathbb{Q}_p$ ist ein lokaler Körper. Dass es lokale Körper beliebiger positiver Charakteristik gibt, zeigt uns das nächste Beispiel.

(ii) Es sei k ein endlicher Körper der Charakteristik $p \in \mathbb{P}$ und t eine Unbestimmte über k. Für eine Folge $(a_i)_{i\in\mathbb{Z}}$ aus k, bei der höchstens endlich viele der a_i mit $i < 0$ von Null verschieden sind, schreiben wir

$$\sum_{n \gg -\infty} a_n t^n \text{ für die formale Reihe } \sum_{n\in\mathbb{Z}} a_n t^n \ .$$

($n \gg -\infty$ erinnert uns an die spezielle Bedingung, die wir an die Folge der a_i gestellt haben). Die Menge all dieser bezeichnen wir mit $k((t))$. Man überzeugt sich davon, dass $k((t))$ mit den wohldefinierten Verknüpfungen

$$\left(\sum_{n \gg -\infty} a_n t^n\right) + \left(\sum_{n \gg -\infty} b_n t^n\right) := \sum_{n \gg -\infty} (a_n + b_n) t^n$$

und

$$\left(\sum_{i\gg-\infty} a_i t^i\right)\cdot\left(\sum_{j\gg-\infty} b_j t^j\right) := \sum_{n\gg-\infty}\left(\sum_{i+j=n} a_i b_j\right) t^n$$

einen Körper der Charakteristik p mit der Eins $1 \in k$ und der Null $0 \in k$ bildet. $K := k((t))$ wird allgemein als *Körper der formalen Laurentreihen über* k bezeichnet. Jedes $f \neq 0$ aus K können wir offensichtlich in einer eindeutigen Form

$$f = t^{u(f)} \cdot \sum_{i=0}^{\infty} a_i t^i$$

mit $a_0 \neq 0$ und $u(f) \in \mathbb{Z}$ schreiben. Wir definieren die Abbildung

$$v_K : K \to \mathbb{Z} \cup \{\infty\}\ ,\ v_K(f) := \begin{cases} u(f) & \text{falls } f \neq 0 \text{ gilt,} \\ \infty & \text{sonst,} \end{cases}$$

dann ist offenbar K ein diskret bewerteter Körper mit Bewertung v_K und wir haben

$$\mathcal{O}_K = \left\{ f \in K : f = \sum_{i=0}^{\infty} a_i t^i \text{ mit } a_i \in k \right\} \text{ und } \mathfrak{p}_K = t\mathcal{O}_K\ .$$

Der Ring $\mathcal{O}_K$ wird gemeinhin mit $k\,[[t]]$ bezeichnet und heißt *Ring der formalen Potenzreihen über* k. Offensichtlich gilt

$$F_K = \mathcal{O}_K/\mathfrak{p}_K \cong k\ .$$

Also ist der Restkörper von K insbesondere endlich. Damit K ein lokaler Körper wird, muss K bezüglich seiner Topologie vollständig sein. Aber dies ist offensichtlich und sei als Übungsaufgabe empfohlen.

2.1.2 Aussagen über lokale Körper als vollständige topologische Körper

Es sei K ein lokaler Körper, $\mathcal{O}_K$ sein Ganzheitsring, $\mathfrak{p}_K$ sein Primideal mit einem Erzeuger π, F_K sein Restkörper der Ordnung q und $|\cdot|_K$ sein Betrag.

Satz 2.8. *Es sei $S \subset \mathcal{O}_K$ ein vollständiges Vertretersystem des Restkörpers $F_K = \mathcal{O}_K/\mathfrak{p}_K$ mit $0 \in S$. Dann besitzt jedes Element $x \in K$ mit $x \neq 0$ eine eindeutige Darstellung als konvergente Reihe*

$$x = \sum_{l=m}^{\infty} s_l \pi^l$$

mit $m \in \mathbb{Z}$, $s_l \in S$ für alle l und $s_m \neq 0$.

Beweis. Siehe Neukirch ([8], Kapitel II, § 4, Satz 4.4). □

Beispiel 2.9. Ist $K = \mathbb{Q}_p$, so wählen wir $S = \{0, 1, 2, ..., p-1\}$. S ist offenbar ein vollständiges Vertretersystem von $F_{\mathbb{Q}_p} \cong \mathbb{Z}/p\mathbb{Z}$. Wir erhalten also, dass sich jedes $x \in \mathbb{Q}_p$ als konvergente Reihe

$$x = \sum_{i=m}^{\infty} a_i p^i$$

mit ganzen Zahlen $a_i \in S$ schreiben lässt.

Proposition 2.10. *Notwendig und hinreichend dafür, dass die Topologie eines diskret bewerteten Körpers L lokal-kompakt ist, ist dass L bezüglich seiner Topologie vollständig ist und dass der Restkörper F_L endlich ist.*

Beweis. Siehe das Buch von Serre ([11], Chapitre II, § 1, Prop. 1). □

Korollar 2.11. *Die Topologie von K ist hausdorffsch, lokal-kompakt und besitzt eine abzählbare Basis von kompakt-offenen Mengen.*

Beweis. Die Topologie jedes metrischen Raumes ist hausdorffsch, also auch die Topologie von K. Ferner ist nach Proposition 2.10 die Topologie von K lokal-kompakt. Nun geben wir eine Basis der Topologie von K der versprochenen Art an:

Da K ein lokal-kompakter metrischer Raum ist, folgt wegen

$$\mathcal{O}_K = \{x \in K : |x|_K < q^1\} = \{x \in K : |x|_K \leq 1\} ,$$

dass $\mathcal{O}_K$ offen, abgeschlossen und beschränkt, also kompakt-offen ist. Damit sind offenbar auch alle Mengen $a + \pi^l \mathcal{O}_K$ mit $a \in K$ und $l \in \mathbb{Z}$ kompakt-offen. Es sei $S \subset \mathcal{O}_K$ ein vollständiges Vertretersystem von $F_K = \mathcal{O}_K/\mathfrak{p}_K$, welches die Null von K enthalte. Für jedes $i \in \mathbb{N}$ sei nun V_i die abzählbare Menge aller Summen

$$\sum_{l=-i}^{i} s_l \pi^l$$

mit $s_l \in S$ für alle l. Dann gibt es offenbar zu jedem $a \in K$ ein $l_0 \in \mathbb{N}$, so dass zu jedem $l \geq l_0$ ein $a' \in V_l$ mit $a' + \pi^l \mathcal{O}_K = a + \pi^l \mathcal{O}_K$ existiert. Offensichtlich bildet dann das folgende System von abzählbar vielen kompakt-offenen Mengen die gewünschte Basis der Topologie von K:

$$M = \{a_i + \pi^i \mathcal{O}_K : i \in \mathbb{N}, a_i \in V_i\} .$$

□

Schließlich zitieren wir noch die folgende Version des "Lemmas von Hensel":

Lemma 2.12. *(Lemma von Hensel) Es sei f aus $\mathcal{O}_K[X]$ und f' seine formale Ableitung. Gilt für a_0 aus $\mathcal{O}_K$ die Ungleichung*

$$|f(a_0)|_K < \left|f'(a_0)^2\right|_K ,$$

so gibt es ein $a \in \mathcal{O}_K$ mit $f(a) = 0$, so dass

$$|a - a_0|_K \leq \left| \frac{f(a_0)}{f'(a_0)^2} \right|_K < 1$$

gilt.

Beweis. Siehe das Buch von Lang ([6], Chapter XII, § 7, Prop. 21). $\square$

Beispiel 2.13. Es sei $f = X^2 + aX + b \in \mathcal{O}_K[X]$ ein Polynom mit ganzen Koeffizienten. Nehmen wir an, dass die Kongruenz

$$X^2 + aX + b \mod \mathfrak{p}_K$$

zwei $\mod \mathfrak{p}_K$ verschiedene Lösungen besitzt. Zwei Vertreter dieser beiden Klassen von Lösungen seien $a_0, a_1 \in \mathcal{O}_K$, dann gilt

$$f(a_0) - f(a_1) = (a_0 - a_1)(a_0 + a_1 + a) \equiv 0 \mod \mathfrak{p}_K$$

und wegen $a_0 \not\equiv a_1 \mod \mathfrak{p}_K$ folgt schließlich $a_0 + a_1 + a \equiv 0 \mod \mathfrak{p}_K$. Damit folgt

$$f'(a_0) = 2a_0 + a \equiv a_0 - a_1 \not\equiv 0 \mod \mathfrak{p}_K \ .$$

Also haben wir

$$|f(a_0)|_K \leq q^{-1} < 1 = \left|f'(a_0)^2\right|_K \ .$$

Damit besitzt f eine Nullstelle a in $\mathcal{O}_K$ mit $|a - a_0|_K < 1$, d.h. mit $a \equiv a_0 \mod \mathfrak{p}_K$. f zerfällt also über $\mathcal{O}_K$ in Linearfaktoren.

2.1.3 Erweiterungen und Klassifikation lokaler Körper

Satz 2.14. *Es sei K ein lokaler Körper und L ein Erweiterungskörper endlicher Dimesion $n = [L : K]$ über K, dann gelten die folgenden Aussagen:*

(i) L ist ebenfalls ein lokaler Körper und sein Ganzheitsring $\mathcal{O}_L$ ist ein freier $\mathcal{O}_K-$Modul vom Rang n.

(ii) Wir haben eine endeutige Konstante $e = e(L|K) \in \mathbb{N}$ mit $v_L(x) = e \cdot v_K(x)$ für alle $x \in K$. Sind π_K und π_L Uniformisierenden von K bzw. L, so gilt insbesondere

$$\pi_K \mathcal{O}_L = \pi_L^e \mathcal{O}_L \ .$$

(iii) Wir haben eine natürliche Injektion $F_K \hookrightarrow F_L$ und die Erweiterung $F_L|F_K$ ist von endlicher Dimension $f = f(L|K) = [F_L : F_K]$.

(iv) Es gilt $n = ef$.

Beweis. Siehe das Buch von Serre ([11], Chapitre II, § 2, Prop. 3, Cor. 1-4). $\square$

Bemerkung 2.15.

(i) Für $x \in L$ gilt die Formel

$$v_L(x) = \frac{1}{f} v_K(\mathrm{N}_{L|K}(x)) \ .$$

Um den Blick für das in dieser Arbeit Notwendige nicht zu trüben, haben wir sie nicht in obigem Satz aufgeführt.

(ii) Satz 2.14 lehrt uns also insbesondere, dass endliche Erweiterungen von Körpern $\mathbb{Q}_p$ und $k((t))$ lokale Körper sind. Die Frage ist nun, ob es noch mehr lokale Körper gibt. Die Antwort darauf gibt der folgende Satz:

Satz 2.16. *Es sei K ein lokaler Körper.*

(i) Gilt Char$(K) = 0$, so ist K isomorph zu einer endlichen Erweiterung eines Körpers $\mathbb{Q}_p$ mit p aus $\mathbb{P}$.

(ii) Gilt Char$(K) = p$ mit $p \in \mathbb{P}$, so ist K isomorph zu dem Laurentreihenkörper $F_K((T))$, wobei F_K der Restkörper von K ist und T eine Unbestimmte über F_K.

Beweis. Siehe das Buch von Neukirch ([8], Kapitel II, § 5, Satz 5.2). □

2.1.4 Die Einheitengruppe eines lokalen Körpers

Es sei K ein lokaler Körper, $\mathcal{O}_K$ sein Ganzheitsring, $\mathfrak{p}_K$ sein Primideal mit einem Erzeuger π, $|\cdot|_K$ sein Betrag und F_K sein Restkörper der Ordnung q. Ferner vereinbaren wir für $m \in \mathbb{N}$ die Notation

$$\begin{aligned} E_m(K) &= \text{die von den } m\text{−ten Einheitswurzeln in } K \text{ gebildete Gruppe.} \\ C_m &= \text{die zyklische Gruppe der Ordnung } m. \end{aligned}$$

Wir interessieren uns im Folgenden für die multiplikative Gruppe K^* von K. Dazu definieren wir:

Satz/Definition 2.17. *Für jedes $n \in \mathbb{N}$ ist die Menge*

$$U_K^{(n)} := 1 + \mathfrak{p}_K^n$$

*eine Untergruppe von $\mathcal{O}_K^*$. Sie heißt die n−*te Einseineitengruppe von K*. Die Gruppe $U_K^{(1)}$ heißt auch einfach* Einseinheitengruppe von K.

Beweis. Der einfache Beweis sei dem Leser überlassen. □

Wir haben nun den folgenden Satz:

Satz 2.18. *Wir haben die Isomorphie*

$$K^* \cong \langle \pi \rangle \times C_{q-1} \times U_K^{(1)} \ .$$

Beweis. Siehe Neukrich ([8], Kapitel II, § 5, Satz 5.3) . □

Nun reicht es also, sich auf die Gruppe $U_K^{(1)}$ zu konzentrieren.

Lemma 2.19. *Es sei Char*$(F_K) = p$. *Für jedes* $x \in U_K^{(1)} = 1 + \mathfrak{p}_K$ *besitzt der Gruppenhomomorphismus* $\mathbb{Z} \to U_K^{(1)}$, $a \mapsto x^a$ *eine eindeutige, stetige Fortsetzung*

$$\mathbb{Z}_p \to U_K^{(1)} \ ,$$

dessen Anwendung auf ein $a \in \mathbb{Z}_p$ *wieder mit* x^a *bezeichnet wird. Dieser macht* $U_K^{(1)}$ *zu einem multiplikativ geschriebenen* $\mathbb{Z}_p-$*Modul.*

Beweis. Siehe hierzu das Buch von A.Weil ([14], Chapter II, § 6, Seite 32 (Mitte)) . □

Beispiel 2.20. Es sei $K = \mathbb{Q}_2$, dann gilt $U_{\mathbb{Q}_2}^{(1)} = 1 + 2\mathbb{Z}_2$. Wegen $-1 = 1 - 2 \in U_{\mathbb{Q}_2}^{(1)}$ haben wir die nach dem vorangehenden Lemma stetige Abbildung

$$\mathbb{Z}_2 \to U_{\mathbb{Q}_2}^{(1)} \ , \ a \mapsto (-1)^a$$

zur Verfügung. Aus der Stetigkeit folgt für $a \in \mathbb{Z}_2$

$$(-1)^a = \begin{cases} 1 & \text{falls } 2|a \text{ gilt,} \\ -1 & \text{sonst,} \end{cases}$$

denn da $\mathbb{Z}$ in $\mathbb{Z}_2$ dicht liegt, finden wir für jedes $a \in \mathbb{Z}_2$ eine Folge $(a_n)_{n\in\mathbb{N}}$ aus $\mathbb{Z}$ mit $a_n \to a$ für $n \to \infty$. Insbesondere gilt $|a - a_n|_{\mathbb{Q}_2} < 1$, d.h. $a \equiv a_n \mod 2$ für alle bis auf endlich viele n. Also ist für alle bis auf endlich viele n die Zahl $(-1)^{a_n}$ gleich 1 oder -1 je nachdem, ob $2|a$ oder $2 \nmid a$ gilt. Wegen $(-1)^a = \lim_{n\to\infty}(-1)^{a_n}$ folgt dann die Behauptung.

Nun können wir eine Beschreibung von $U_K^{(1)}$ angeben:

Satz 2.21. *Gilt Char*$(F_K) = p$, *so gelten die folgenden Aussagen:*

(i) Im Falle Char$(K) = 0$ *ist* K *eine endliche Erweiterung von* $\mathbb{Q}_p$ *mit* $d := [K : \mathbb{Q}_p] < \infty$ *und wir haben die folgende Isomorphie von* $\mathbb{Z}_p-$*Moduln:*

$$U_K^{(1)} \cong \mathbb{Z}_p/p^m\mathbb{Z}_p \times \mathcal{O}_K \cong \mathbb{Z}_p/p^m\mathbb{Z}_p \times \mathbb{Z}_p^d \ .$$

Dabei ist $m \in \mathbb{N}_0$ *maximal mit der Eigenschaft gewählt, dass* K *eine primitive* p^m-*te Einheitswurzel enthält.*

(ii) Im Falle Char$(K) = p$ haben wir die folgende Isomorphie von $\mathbb{Z}_p$–Moduln:

$$U_K^{(1)} \cong \mathbb{Z}_p^{\mathbb{N}} \ .$$

Beweis. Siehe das Buch von A.Weil ([14], Chapter II, § 6, Proposition 9 und 10). □

Aus diesem Resultat folgt schließlich (unter gewissen Einschränkungen) eine Formel für den Index der Gruppen

$$K^{*n} := \{x^n : x \in K^*\} \ \text{ bzw. } \ \mathcal{O}_K^{*n} := \{u^n : u \in \mathcal{O}_K^*\}$$

in K^* bzw. $\mathcal{O}_K^*$:

Korollar 2.22. *Es sei $n \in \mathbb{N}$ und es gelte im Falle Char$(K) = p > 0$ die Beziehung ggT$(n,p) = 1$, dann gilt*

$$(K^* : K^{*n}) = n(\mathcal{O}_K^* : \mathcal{O}_K^{*n}) = \frac{n}{|n|_K} E_n(K) \ .$$

Beweis. Siehe das Buch von Neukirch ([8], Kapitel II, § 6, Kor. 5.8) oder das Buch von A.Weil ([14], Chapter II, § 3, Prop. 8 und das Korollar zu Prop. 9). □

3 Lokale Symbole und quadratische Kongruenzen

Es sei K ein lokaler Körper mit den Daten $\mathcal{O}_K, \mathfrak{p}_K$ und F_K ($\#F_K = q$). Außerdem wählen wir eine Uniformisierende π von K. Schließlich wollen wir für ein a aus $\mathcal{O}_K$ mit $\overline{a}$ die Restklasse von a in $F_K = \mathcal{O}_K/\mathfrak{p}_K$ bezeichnen.

Es seien a und b aus $\mathcal{O}_K$. Wir bezeichnen mit $N(a,b)$ die Anzahl der $\mod \mathfrak{p}_K$ verschiedenen Lösungen der quadratischen Kongruenz

$$X^2 + aX + b \equiv 0 \mod \mathfrak{p}_K \ .$$

Bekanntlich gilt $N(a,b) \in \{0,1,2\}$ (denn wir rechnen in dem Körper F_K). Ziel dieses Abschnittes ist die Berechnung der Abbildung

$$\left(\frac{\cdot,\cdot}{K}\right) : \mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z} \quad , \quad \left(\frac{a,b}{K}\right) := \begin{cases} 1 & \text{falls } N(a,b) = 2 \ , \\ 0 & \text{falls } N(a,b) = 1 \ , \\ -1 & \text{falls } N(a,b) = 0 \ , \end{cases}$$

mit Hilfe bekannter Symbole der algebraischen Zahlentheorie. Bevor wir weitergehen, erwähnen wir noch die offensichtliche Regel

$$\left(\frac{a,b}{K}\right) = \left(\frac{-a,b}{K}\right) \ .$$

Wir können den Fall $\left(\frac{a,b}{K}\right) = 0$ sofort behandeln:

Proposition 3.1. *Es gilt*

$$\left(\frac{a,b}{K}\right) = 0 \Leftrightarrow \begin{cases} D = a^2 - 4b \in \mathfrak{p}_K & \textit{falls } Char(K) \neq 2 \textit{ gilt,} \\ a \in \mathfrak{p}_K & \textit{falls } Char(K) = 2 \textit{ gilt.} \end{cases}$$

Beweis. "$\Leftarrow$": Es sei die rechte Seite der obigen Äquivalenz erfüllt.

Gilt $\pi | 2$, d.h. gilt $\mathrm{Char}(F_K) = 2$, so folgt offenbar in jedem Fall $a \equiv 0 \mod \mathfrak{p}_K$. Da in F_K die Gleichung $X^2 = \overline{b}$ genau eine Lösung hat (die Abbildung $x \mapsto x^2$ ist bekanntlich bijektiv in endlichen Körpern der Charakteristik 2), folgt die linke Seite der zu beweisenden Äquivalenz.

Gilt $\pi \nmid 2$, so gilt $2 \in \mathcal{O}_K^*$. Deswegen ist

$$(*) \qquad X^2 + aX + b \equiv 0 \mod \mathfrak{p}_K \text{ äquivalent zu } (2X - a)^2 \equiv D \mod \mathfrak{p}_K \ .$$

Auf Grund der Voraussetzung $D \equiv 0 \mod \mathfrak{p}_K$ folgt damit die Beziehung $\left(\frac{a,b}{K}\right) = 0$. Also ist auch hier die linke Seite der zu beweisenden Äquivalenz erfüllt.

"$\Rightarrow$": Es gelte $\left(\frac{a,b}{K}\right) = 0$. Wir folgern die rechte Seite der zu beweisenden Äquivalenz:

Gilt $\pi | 2$, so gilt $\mathrm{Char}(F_K) = 2$. Wäre $\overline{a} \neq 0 \in F_K$ und besäße die Gleichung

$$X^2 + \overline{a}X + \overline{b} = 0$$

in F_K eine Lösung γ, so wäre offenbar auch $\gamma + \overline{a} \neq \gamma$ eine Lösung der obigen Gleichung. Dies stünde aber im Widerspruch zur Voraussetzung $\left(\frac{a,b}{K}\right) = 0$, also folgt $a \equiv 0 \mod \mathfrak{p}_K$. Damit erhalten wir offenbar die rechte Seite der zu beweisenden Äquivalenz.

Gilt $\pi \nmid 2$, so folgt $D \equiv 0 \mod \mathfrak{p}_K$ sofort aus der Beziehung $(*)$, denn wegen $1 \neq -1$ in F_K besitzt die Gleichung $Y^2 = \overline{D}$ in F_K genau zwei Lösungen oder keine Lösung, falls $\overline{D} \neq 0 \in F_K$ gilt. □

Wir haben also nur noch zu untersuchen, in welchen Fällen das Symbol $\left(\frac{\cdot,\cdot}{K}\right)$ zu 1 oder -1 auswertet.

3.1 Quadratische Kongruenzen im Fall Char$(K) \neq 2$

Im ganzen Unterabschnitt gelte $\mathrm{Char}(K) \neq 2$.

3.1.1 Der Zusammenhang mit dem Hilbert-Symbol

Das Hilbert-Symbol ist wie folgt gegeben:

Definition 3.2. Für $a, b \in K^*$ definieren wir die Abbildung

$$(\cdot,\cdot)_K : K^* \times K^* \to \{\pm 1\} \subset K^*$$

durch

$$(a,b)_K := \begin{cases} 1 & \text{falls } ax^2 + by^2 = z^2 \text{ für ein } (x,y,z) \text{ aus } K^3 - \{(0,0,0)\} \text{ gilt,} \\ -1 & \text{sonst.} \end{cases}$$

Die Abbildung $(\cdot,\cdot)_K$ wird das *Hilbert-Symbol* von K genannt.

Wir können direkt die Verbindung unseres Symbols $\left(\frac{\cdot,\cdot}{K}\right)$ zum Hilbert-Symbol herstellen:

Satz 3.3. *Es seien a, b aus $\mathcal{O}_K$. Wir setzen $D := a^2 - 4b$, dann gilt:*

$$\left(\frac{a,b}{K}\right) = \begin{cases} 1 & \text{falls } D \in \mathcal{O}_K^* \text{ und } (D,\pi)_K = 1 \text{ gilt,} \\ 0 & \text{falls } D \in \mathfrak{p}_K \text{ gilt,} \\ -1 & \text{falls } D \in \mathcal{O}_K^* \text{ und } (D,\pi)_K = -1 \text{ gilt.} \end{cases}$$

Beweis. Auf Grund der Proposition 3.1 reicht es aus, $D \in \mathcal{O}_K^*$ anzunehmen und die Beziehung

$$\left(\frac{a,b}{K}\right) = 1 \Leftrightarrow (D,\pi)_K = 1$$

zu bestätigen.

"$\Rightarrow$": Nach dem Lemma von Hensel (siehe hierzu auch das Beispiel 2.13) existiert ein $x \in \mathcal{O}_K$ mit $x^2 + ax + b = 0$, d.h. mit $(a-2x)^2 = D$. Also folgt wegen

$$D \cdot 1^2 + \pi \cdot 0^2 = (a-2x)^2$$

die Beziehung $(D,\pi)_K = 1$.

"$\Leftarrow$": Es sei $(x,y,z) \neq (0,0,0)$ aus K^3 eine Lösung von

$$Dx^2 + \pi y^2 = z^2 \ .$$

Wir können o.B.d.A. annehmen, dass x, y und z ganz sind und dass $\mathrm{ggT}(x,y,z) = x\mathcal{O}_K + y\mathcal{O}_K + z\mathcal{O}_K = (1) = \mathcal{O}_K$ gilt, denn wir können die obige Gleichung mit einer entsprechenden Potenz π^{2l} mit $l \in \mathbb{Z}$ durchmultiplizieren. x kann kein Vielfaches von π sein, denn sonst wäre z auch ein Vielfaches von π und damit würde $\mathrm{ggT}(x,y,z) \subset \pi\mathcal{O}_K \neq \mathcal{O}_K$ gelten. Deswegen sind $r := z/x$ und $s := y/x$ ganz. Wir haben also

$$D = r^2 - \pi s^2 \ .$$

Im Fall, dass π nicht 2 teilt, haben wir für ein u aus $\mathcal{O}_K$

$$u^2 + au + b \equiv 0 \mod \mathfrak{p}_K \text{ genau dann, wenn } (2u-a)^2 = D \mod \mathfrak{p}_K$$

gilt. Dies ist aber genau dann der Fall, wenn D ein Quadrat modulo $\mathfrak{p}_K$ ist. Also folgt $\left(\frac{a,b}{K}\right) = 1$.

Von nun an sei π ein Teiler von 2, d.h. es gelte $(\pi^e) = (2)$ für ein e in $\mathbb{N}$. Es ist $r^2 - a^2 - \pi s^2$ durch 4 teilbar, also gilt $\pi \mid r^2 - a^2$. Wegen $(a+r) + (a-r) = 2a$ ist jede π-Potenz kleiner oder gleich e, die $a+r$ teilt auch ein Teiler von $a-r$. Ist also $a^2 - r^2$ höchstens durch π^k teilbar mit $k < 2e$, so muss k gerade sein und in diesem Fall gilt $|r^2 - a^2|_K \neq |\pi s^2|_K$. D.h. es ergäbe sich ein Widerspruch, da $r^2 - a^2 - \pi s^2$ niemals ein Vielfaches von 4 sein könnte. Also ist $r^2 - a^2$ durch 4 teilbar. Somit ist s^2 durch π^{2e-1} und damit auch durch 4 teilbar. Also haben wir $a + r = 2u$ mit einem u aus $\mathcal{O}_K$ und es gilt $D = (2u-a)^2 - 4\pi v$ mit einem v aus $\mathcal{O}_K$. Daraus folgt $\left(\frac{a,b}{K}\right) = 1$, denn es ist

$$u^2 + au + b \equiv 0 \mod \mathfrak{p}_K \text{ äquivalent zu } (2u-a)^2 = D \mod 4\mathfrak{p}_K \ .$$

Damit ist der Satz bewiesen. $\square$

3.1.2 Eigenschaften des Hilbert-Symbols

Wir wollen nun einige Aussagen über das Hilbert-Symbol zusammentragen, um später einfacher Beispiele angeben zu können. Einige Eigenschaften können wir sofort aus unserer Definition ablesen:

Proposition 3.4. *Es gelten die folgenden Aussagen:*

(i) *Für alle a, b, c, d in K^* gilt $(ab^2, cd^2)_K = (a, c)_K$, d.h. die Abbildung $(\cdot, \cdot)_K$ induziert eine Abbildung*

$$K/K^{*2} \times K/K^{*2} \to \{\pm 1\} ,$$

vermöge $(aK^{*2}, bK^{*2}) \mapsto (a, b)_K$.

(ii) *Es gilt $(a, -a)_K = 1$ und $(a, 1-a)_K = 1$ für alle $a \in K^*$.*

(iii) *Es gilt $(a, b)_K = (b, a)_K$ für alle a, b aus K^*.*

(iv) *Es gilt $(a, b)_K = 1$ genau dann, falls a eine Norm in der Erweiterung $K(\sqrt{b})|K$ ist (dabei bezeichnet $\sqrt{b}$ eine Nullstelle von $X^2 - b \in K[X]$).*

Beweis. *Zu (i)*: Wir haben auf Grund von $a, b \neq 0$

$$\begin{aligned} (ab^2, cd^2)_K = 1 \quad &\Leftrightarrow \quad \text{Es gilt } ab^2x^2 + cd^2y^2 = z^2 \text{ für ein } (x, y, z) \in K^3 - \{(0,0,0)\}. \\ &\Leftrightarrow \quad \text{Es gilt } a(bx)^2 + c(dy)^2 = z^2 \text{ für ein } (x, y, z) \in K^3 - \{(0,0,0)\}. \\ &\Leftrightarrow \quad \text{Es gilt } ax'^2 + cy'^2 = z^2 \text{ für ein } (x', y', z) \in K^3 - \{(0,0,0)\}. \\ &\Leftrightarrow \quad (a, c)_K = 1 . \end{aligned}$$

Zu (ii): Es gilt

$$a \cdot 1^2 - a \cdot 1^2 = 0^2 \;\text{ und }\; a \cdot 1^2 + (1-a) \cdot 1^2 = 1^2 ,$$

woraus mit der Definition von $(\cdot, \cdot)_K$ die Aussage (ii) folgt.

Zu (iii): Dies ist nach Definition unseres Symbols offensichtlich.

Zu (iv): " $\Rightarrow$": Es gelte $(a, b)_K = 1$. Wir finden also ein $(x, y, z) \neq (0,0,0)$ in K^3 mit

$$ax^2 + by^2 = z^2 .$$

Gilt $K(\sqrt{b}) = K$, d.h. gilt $b \in K^{*2}$, so gilt $\mathrm{N}_{K(\sqrt{b}):K} = id_K$ und $a \in K^*$ ist dann trivialerweise eine Norm von $K(\sqrt{b})|K$. Gilt $K(\sqrt{b}) \neq K$, d.h. ist $K(\sqrt{b})$ eine (galoissche) Erweiterung vom Grad 2 über K und insbesondere b kein Quadrat in K^*, so kann x nicht 0 sein, denn sonst stünde der Widerspruch $by^2 = z^2$ mit $(y, z) \neq (0,0)$ da. D.h. wenn wir $y' := y/x$ und $z' := z/x$ setzen, erhalten wir

$$a = z'^2 - by'^2 = (z' - \sqrt{b}y')(z' + \sqrt{b}y') = \mathrm{N}_{K(\sqrt{b}):K}(z' + \sqrt{b}y') .$$

Also ist die Richtung "$\Rightarrow$" gezeigt.

"$\Leftarrow$": Diese Richtung erhält man ebenso einfach wie die Richtung " $\Rightarrow$", sie sei dem Leser als Übung überlassen. □

Wir notieren noch einige weitere nicht so offensichtliche Eigenschaften von $(\cdot,\cdot)_K$:

Satz 3.5. *Es gilt*

(i) $(a,b)_K(a',b)_K = (aa',b)_K$ *für alle* a, a', b *in* K^*,

(ii) $(a,b)_K(a,b')_K = (a,bb')_K$ *für alle* a, b, b' *in* K^*; *außerdem gilt:*

(iii) $(a,b)_K = 1$ *für alle* $a \in K^*$ *impliziert* $b \in K^{*2}$.

Beweis. Siehe z.B. das Buch von Serre ([11], Kaptiel XIV, § 2, Prop. 7) oder das Buch von Neukirch ([8], Kapitel V, § 3, Satz 3.2). □

Bemerkung 3.6.

(i) Der vorangehende Satz besagt gerade, dass die durch unser Symbol $(\cdot,\cdot)_K$ induzierte Abbildung
$$K/K^{*2} \times K/K^{*2} \to \{\pm 1\}$$
bilinear und nicht ausgeartet ist, d.h. wir können erwarten, dass explizite Formeln für $(\cdot,\cdot)_K$ umso komplizierter werden, je größer die Ordnung der Gruppe K/K^{*2} ist. Und dies ist auf Grund der Formel
$$(K^* : K^{*2}) = \frac{2}{|2|_K}\#E_2(K) = \frac{4}{|2|_K}$$
(siehe Korollar 2.22) sicherlich dann der Fall, falls $(\pi^e) = (2)$ für ein möglichst großes e aus $\mathbb{N}$ gilt.

(ii) Schreiben wir zwei Elemente $a, b \in K^*$ als $a = \pi^k\epsilon$ und $b = \pi^l\epsilon'$ mit $\epsilon, \epsilon' \in \mathcal{O}_K^*$ und $k, l \in \mathbb{Z}$, so erhalten wir auf Grund der Bilinearität von und der Symmetrie von $(\cdot,\cdot)_K$:
$$(a,b)_K = (\pi,b)_K^k(\epsilon,b)_K = (\pi,\pi)_K^{lk}(\epsilon',\pi)_K^k(\epsilon,\pi)_K^l(\epsilon,\epsilon')_K\ .$$
D.h. um $(\cdot,\cdot)_K$ anzugeben, reicht es aus, $(\pi,\pi)_K$ zu bestimmen und Formeln für $(\epsilon,\epsilon')_K$ und $(\epsilon,\pi)_K$ mit $\epsilon, \epsilon' \in \mathcal{O}_K^*$ anzugeben.

3.1.3 Beispiele und Bemerkungen zu höheren Hilbert-Symbolen

Wir geben nun einige wohlbekannte Beispiele für explizite Formeln des Hilbert-Symbols an. Dabei interessieren uns natürlich besonders Formeln für $(\epsilon,\pi)_K$ mit $\epsilon \in \mathcal{O}_K^*$.

Definition 3.7. Wir definieren die Abbildung $\left(\frac{\cdot}{K}\right) : \mathcal{O}_K^* \to \{\pm 1\} \subset K^*$ durch
$$\left(\frac{a}{K}\right) = \begin{cases} 1 & \text{, falls } a \equiv b^2 \mod \mathfrak{p}_K \text{ für ein } b \in \mathcal{O}_K^* \text{ gilt ,} \\ -1 & \text{sonst .} \end{cases}$$

$\left(\frac{\cdot}{K}\right)$ heißt das *Legendre-Symbol* von K. Offensichtlich wertet es immer zu 1 aus, falls $\mathrm{Char}(F_K) = 2$ gilt, d.h. falls K eine endliche Erweiterung von $\mathbb{Q}_2$ ist.

Proposition 3.8. *Es sei K eine endliche Erweiterung von $\mathbb{Q}_p$ mit $p > 2$. Dann gilt $(a, \pi)_K = \left(\frac{a}{K}\right)$ für alle $a \in \mathcal{O}_K^*$ und es gilt das* "Euler-Kriterium"*: Für jedes $a \in \mathcal{O}_K^*$ gilt*

$$\left(\frac{a}{K}\right) \equiv a^{(q-1)/2} \mod \mathfrak{p}_K \ .$$

Dabei wird das Zeichen von $\left(\frac{\cdot}{K}\right)$ durch obige Kongruenz eindeutig festgelegt.

Beweis. Ähnliche Überlegungen wie im Beweis von Satz 3.3 liefern uns für ein $a \in \mathcal{O}_K^*$ die Beziehung

$$(a, \pi)_{\mathbb{Q}_p} = 1 \Leftrightarrow a \text{ ist ein Quadrat} \mod \mathfrak{p}_K \ .$$

Daraus erhalten wir die erste zu beweisende Aussage. Nun beweisen wir noch die fehlende Aussage:

F_K ist ein endlicher Körper und daher ist seine multiplikative Gruppe zyklisch. Es sei α ein Erzeuger von F_K und es gelte $\alpha^r = \overline{a} \in F_K^*$. Wegen $\# F_K^* = q - 1$ haben wir $\left(\overline{a}^{\frac{q-1}{2}}\right)^2 = \overline{a}^{q-1} = 1$, d.h. wir haben $\overline{a} \in \{-1, 1\} \subset F_K$. Dann gilt :

$$1 \equiv a^{(q-1)/2} \mod \mathfrak{p}_K \Leftrightarrow \overline{a}^{\frac{q-1}{2}} = 1 \Leftrightarrow \alpha^{r\frac{q-1}{2}} = 1 \Leftrightarrow q-1 | r\frac{q-1}{2} \Leftrightarrow r|2 \Leftrightarrow \left(\frac{a}{K}\right) = 1 \ .$$

Damit ist auch das Euler-Kriterium bewiesen. $\square$

Proposition 3.9. *Es sei $p \in \mathbb{P}$ ungerade. Für $a = p^k\epsilon$ und $b = p^l\epsilon'$ aus $\mathbb{Q}_p^*$ mit $\epsilon, \epsilon' \in \mathbb{Z}_p^*$ und $k, l \in \mathbb{Z}$ gilt:*

$$(a,b)_{\mathbb{Q}_p} = (-1)^{\frac{p-1}{2}kl} \left(\frac{\epsilon}{\mathbb{Q}_p}\right)^k \left(\frac{\epsilon'}{\mathbb{Q}_p}\right)^l .$$

Beweis. Auf Grund des vorangehenden Lemmas, der Bilinearität und der Symmetrie des Hilbertsymbols haben wir

$$\begin{aligned}(a,b)_{\mathbb{Q}_p} &= (p,p)_{\mathbb{Q}_p}^{kl}(\epsilon,p)_{\mathbb{Q}_p}^{k}(\epsilon',p)_{\mathbb{Q}_p}^{l}(\epsilon,\epsilon')_{\mathbb{Q}_p} \\ &= (p,p)_{\mathbb{Q}_p}^{kl}(\epsilon,p)_{\mathbb{Q}_p}^{k-1}(\epsilon',p)_{\mathbb{Q}_p}^{l}(\epsilon,p\epsilon')_{\mathbb{Q}_p} \\ &= (p,p)_{\mathbb{Q}_p}^{kl} \left(\frac{\epsilon}{\mathbb{Q}_p}\right)^k \left(\frac{\epsilon'}{\mathbb{Q}_p}\right)^l .\end{aligned}$$

Zu untersuchen bleibt also noch $(p,p)_{\mathbb{Q}_p}$:

Ist $p \equiv 1 \mod 4$, so gibt es nach dem "Zwei-Quadrate-Satz" von Fermat zwei natürliche Zahlen a und b mit $p = a^2 + b^2$. Dies bedeutet aber wegen $pa^2 + pb^2 = p^2$, dass wir $(p,p)_{\mathbb{Q}_p} = 1$ haben.

Ist $p \equiv 3 \mod 4$ und nehmen wir an, es gelte $(p,p)_{\mathbb{Q}_p} = 1$, so finden wir nach Definition des Hilbert-Symbols Elemente x, y, z aus K^* (nicht alle Null) mit

$$px^2 + py^2 = z^2 .$$

Nachdem wir die Gleichung mit einer entsprechenden Potenz p^{2l} mit $l \in \mathbb{Z}$ durchmultipliziert haben, können wir annehmen, dass $x, y, z \in \mathbb{Z}_p$ und dass $\mathrm{ggT}(x,y,z) = x\mathbb{Z}_p + y\mathbb{Z}_p + z\mathbb{Z}_p = \mathbb{Z}_p$ gilt. Aus der obigen Gleichung gewinnen wir dann sofort die Beziehung $p|z$ und damit $p|(x^2+y^2)$. Es ist eine bekannte Tatsache aus der elementaren Zahlentheorie, dass dies nur sein kann, falls $p|x$ und $p|y$ gilt. Dies ist aber ein Widerspruch zu $\mathrm{ggT}(x,y,z) = \mathbb{Z}_p$. Damit muss $(p,p)_{\mathbb{Q}_p} = -1$ gelten.

Wir können die obigen Erörterungen offenbar so zusammenfassen:

$$(p,p)_{\mathbb{Q}_p} = (-1)^{\frac{p-1}{2}} .$$

Damit folgt offenbar die Behauptung unserer Proposition. □

Nun geben wir noch eine wohlbekannte Formel für $(\cdot,\cdot)_{\mathbb{Q}_2}$ an. Wir haben $\mathbb{Z}_2^* = U_{\mathbb{Q}_2}^{(1)} = 1 + 2\mathbb{Z}_2$. Für $\epsilon \in \mathbb{Z}_2^*$ setzen wir

$$u(\epsilon) := \frac{\epsilon - 1}{2} \quad \text{und} \quad v(\epsilon) := \frac{\epsilon^2 - 1}{8} .$$

Dann gilt offenbar $u(\mathbb{Z}_2^*) \subset \mathbb{Z}_2$ und $v(\mathbb{Z}_2^*) \subset \mathbb{Z}_2$. Außerdem erwähnen wir noch einmal, dass wir wegen $-1 = 1 - 2 \in U_{\mathbb{Q}_2}^{(1)}$ den wohlbestimmten stetigen Homomorphismus

$\mathbb{Z}_2 \to U^{(1)}_{\mathbb{Q}_2}$, $a \mapsto (-1)^a$ zur Verfügung haben (siehe Lemma 2.19). Dieser hatte nach Beispiel 2.20 die Eigenschaft

$$(-1)^a = \begin{cases} 1 & \text{falls } 2|a \text{ gilt,} \\ -1 & \text{sonst.} \end{cases}$$

Es gilt der folgende Satz:

Satz 3.10. *Es gelte $a = 2^k\epsilon, b = 2^l\epsilon' \in \mathbb{Q}_2$ mit $\epsilon, \epsilon' \in \mathbb{Z}_2^*$ und $k, l \in \mathbb{Z}$, dann folgt*

$$(a, b)_{\mathbb{Q}_2} = (-1)^{u(\epsilon)u(\epsilon')+kv(\epsilon)+lv(\epsilon')} .$$

Insbesondere haben wir also für jede Einheit $\epsilon \in \mathbb{Z}_2^*$ die Formel $(\epsilon, 2)_{\mathbb{Q}_2} = (-1)^{\frac{\epsilon^2-1}{8}}$.

Beweis. Nach Bemerkung 3.6 reicht es aus, für Elemente $\epsilon, \epsilon' \in \mathbb{Z}_2^*$ die Formeln

$$(\epsilon, \epsilon')_{\mathbb{Q}_2} = (-1)^{\frac{\epsilon-1}{2}\frac{\epsilon'-1}{2}} , \ (\epsilon, 2)_{\mathbb{Q}_2} = (-1)^{\frac{\epsilon^2-1}{8}} \ \text{ und } \ (2, 2)_{\mathbb{Q}_2} = 1$$

nachzuprüfen. Die letzte Formel ist wegen $2 \cdot 1^2 + 2 \cdot 1^2 = 2^2$ richtig. Nun zu den ersten beiden Formeln: Wir setzen abkürzend $U^{(n)} := U^{(n)}_{\mathbb{Q}_2} = 1 + 2^n\mathbb{Z}_2$.

Für x und y aus $\mathbb{Z}_2^* = 1 + 2\mathbb{Z}_2$ gelten wegen $x^2 \equiv y^2 \equiv 1 \mod 8$ die Beziehungen

$$\begin{aligned} (xy - 1) - (x - 1) - (y - 1) &= (x - 1)(y - 1) \in 4\mathbb{Z}_2 \ \text{ und} \\ ((xy)^2 - 1) - (x^2 - 1) - (y^2 - 1) &= (x^2 - 1)(y^2 - 1) \in 64\mathbb{Z}_2 . \end{aligned}$$

Also haben wir

$$u(xy) \equiv u(x) + u(y) \mod 2 \ \text{ und } \ v(xy) \equiv v(x) + v(y) \mod 2 .$$

D.h. die rechte Seite der ersten, noch zu beweisenden Formel ist bilinear in ϵ und ϵ' und die der zweiten ist linear in ϵ. Auf Grund der Bilinearität von $(\cdot,\cdot)_{\mathbb{Q}_2}$ reicht es also aus, die Formeln auf einer Erzeuger-Menge $E \subset \mathbb{Z}_2^*$ der Gruppe $\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}$ zu beweisen.

(i) Wir zeigen: Ein Erzeugendensystem $E \subset \mathbb{Z}_2^*$ von $\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}$ ist gegeben durch $E = \{-1, 5\}$. Nach unserem Satz über die Struktur der Einheitengruppe eines lokalen Körpers ist $\mathbb{Z}_2^* = U^{(1)}$ als $\mathbb{Z}_2-$Modul isomorph zu dem additiv geschriebenen $\mathbb{Z}_2-$Modul $\mathbb{Z}_2/2^a\mathbb{Z}_2 \times \mathbb{Z}_2$, wobei $a \in \mathbb{N}_0$ maximal ist mit der Eigenschaft, dass $\mathbb{Q}_2$ eine primitive 2^a-te Einheitswurzel enthält. Wegen $-1 \in \mathbb{Q}_2$ und $1 \neq -1$ gilt $a \geq 1$. Damit haben wir

$$\mathbb{Z}_2^*/\mathbb{Z}_2^{*2} \cong (\mathbb{Z}_2/2^a\mathbb{Z}_2)/(2\mathbb{Z}_2/2^a\mathbb{Z}_2) \times \mathbb{Z}_2/2\mathbb{Z}_2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} .$$

D.h. unsere Gruppe $\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}$ ist vom Typ $(2, 2)$. Damit ist ein Erzeugendensystem von $\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}$ durch zwei Nichtquadrate gegeben, deren Produkt ebenfalls ein Nichtquadrat ist. Da wegen $(1 + 2c)^2 = 1 + 4c(c + 1) \equiv 1 \mod 8$ für jedes $c \in \mathbb{Z}_2$ offenbar $\mathbb{Z}_2^{*2} \subset U^{(3)} = 1 + 8\mathbb{Z}_2$ gilt, liegen $-1 = 1 - 2$ und $5 = 1 + 4$ und auch $(-1) \cdot 5 = 1 - 2 - 4$ nicht in $\mathbb{Z}_2^{*2}$. Und damit ist $E = \{-1, 5\}$ ein Erzeugendensystem von $\mathbb{Z}_2^*/\mathbb{Z}_2^{*2}$.

(ii) Wir beweisen die zweite Formel. Dabei erinnern wir uns an die Eigenschaften des Hilbert-Symbols. Wir haben $1 = (1-2,2)_{\mathbb{Q}_2} = (-1,2)_{\mathbb{Q}_2}$. Würde auch $(5,2)_{\mathbb{Q}_2} = 1$ gelten, so würde $(\epsilon,2)_{\mathbb{Q}_2} = 1$ für alle $\epsilon \in \mathbb{Z}_2^*$ folgen. Damit würde wegen $(2,2)_{\mathbb{Q}_2} = 1$ auch $(a,2)_{\mathbb{Q}_2} = 1$ für alle $a \in \mathbb{Q}_2^*$ richtig sein, d.h. es würde $2 \in \mathbb{Q}_2^{*2}$ folgen, was offensichtlich nicht der Fall ist. Damit gilt $(5,2)_{\mathbb{Q}_2} = -1$. Wegen $(-1)^{\frac{(-1)^2-1}{8}} = 1$ und $(-1)^{\frac{5^2-1}{8}} = -1$ folgt daher die zweite Formel.

(iii) Wir verifizieren die erste Formel: Wegen $5 \cdot 1^2 + (-1) \cdot 1^2 = 2^2$ haben wir $(5,-1)_{\mathbb{Q}_2} = (-1,5)_{\mathbb{Q}_2} = 1$. Ferner haben wir wegen $5 \cdot 1^2 + 5 \cdot 2^2 = 5^2$ die Beziehung $(5,5)_{\mathbb{Q}_2} = 1$. Wäre $(-1,-1)_{\mathbb{Q}_2} = 1$, so folgte wegen $(-1,2)_{\mathbb{Q}_2} = (5,-1)_{\mathbb{Q}_2} = (-1,5)_{\mathbb{Q}_2} = 1$ die Beziehung $(-1,a)_{\mathbb{Q}_2} = 1$ für alle $a \in \mathbb{Q}_2^*$. Damit würde $-1 \in \mathbb{Q}_2^{*2}$ gelten. Dies ist aber nicht möglich, denn es gilt $-1 \notin U^{(3)} \subset 1 + 8\mathbb{Z}_2$. Damit folgt $(-1,-1)_{\mathbb{Q}_2} = -1$. Außerdem haben wir $(-1)^{\frac{-1-1}{2}\frac{-1-1}{2}} = -1, (-1)^{\frac{5-1}{2}\frac{5-1}{2}} = 1$ und $(-1)^{\frac{5-1}{2}\frac{-1-1}{2}} = 1$, d.h. auch die erste Formel gilt.

Damit ist der Beweis abgeschlossen.

□

Bemerkung 3.11. Das von uns eingeführte Hilbert-Symbol $(\cdot,\cdot)_K$ ist nur ein Spezialfall eines allgemeineren Hilbertsymbols, das wie folgt konstruiert werden kann:

Wir wählen uns eine natürliche Zahl n und setzen voraus, dass im Falle $\mathrm{Char}(K) = p > 0$ die Beziehung $\mathrm{ggT}(p,n) = 1$ gilt. Außerdem enthalte K die zyklische Gruppe E_n der $n-$ten Einheitswurzeln. Es sei ferner $\overline{K}$ ein festgewählter algebraischer Abschluss von K. Wir definieren

$$L := K\left(\sqrt[n]{K^*}\right) := K(\{\gamma \in \overline{K} : \gamma^n \in K^*\}) \; .$$

Dann ist $L \subset \overline{K}$ die per Inclusion maximale abelsche Erweiterung von K vom Exponenten n (die *Kummertheorie* liefert bekanntlich eine Bijektion $B \mapsto K\left(\sqrt[n]{B}\right)$ zwischen den Untergruppen $B \subset K^*$ mit $K^{*n} \subset B$ und den abelschen Erweiterungen $L' \subset \overline{K}$ von K vom Exponenten n). Dann kann gezeigt werden:

(i) Die Kummertheorie liefert einen Gruppenisomorphismus

$$K^*/K^{*n} \cong \mathrm{Hom}(\mathrm{Gal}(L|K), E_n) \; .$$

(ii) Auf Grund der *der lokalen Klassenkörpertheorie* erhalten wir die folgenden Beziehungen:

$$K^*/K^{*n} = K^*/\mathrm{N}_{L|K}(L^*) \cong \mathrm{Gal}(L|K) \; .$$

Insbesondere erhalten wir also einen Gruppenisomorphismus $K^*/K^{*n} \cong \mathrm{Gal}(L|K)$.

(iii) Wir haben die nicht ausgeartete bilineare Paarung

$$\mathrm{Hom}(\mathrm{Gal}(L|K), E_n) \times \mathrm{Gal}(L|K) \to E_n \; , \; (\chi, \sigma) \mapsto \chi(\sigma) \; .$$

Alle drei Punkte zusammen liefern uns eine nicht ausgeartete bilineare Paarung

$$(\cdot,\cdot)_{n,K} : K^*/K^{*n} \times K^*/K^{*n} \to E_n ,$$

von der man sich davon überzeugt, dass sie im Falle $n = 2$ mit unserem Hilbert-Symbol übereinstimmt. Näheres über diesen Ansatz kann im Buch von Neukirch ([8], Kapitel V, S.349 f.f.) nachgelesen werden.

Im Fall, dass $\mathrm{Char}(F_K)$ die Zahl n nicht teilt, kann eine einfache, geschlossene Formel für $(\cdot,\cdot)_{n,K}$ angegeben werden. Diese kann wiederum im Buch von Neukirch nachgelesen werden. Ist aber K eine endliche Erweiterung von $\mathbb{Q}_p$ mit $p \in \mathbb{P}$, so wurden im Falle $n = p^l$ mit l aus $\mathbb{N}$ erst sehr spät explizite Formeln für $(\cdot,\cdot)_{n,K}$ gefunden. Wir verweisen hierzu auf die Arbeiten von Helmut Brückner (vgl. [2]), S.V. Vostokov (vgl. [13]) und Shankar Sen (vgl. [9]) .

3.2 Quadratische Kongruenzen im Fall $\mathrm{Char}(K) = 2$

Es sei im ganzen Unterabschnitt K von der Charakteristik 2. Dann besitzt K einen zu F_K isomorphen Teilkörper k, so dass für jede Uniformisierende t aus K die Beziehung $K = k((t))$ gilt. Die Elemente von K sind also formale Potenzreihen

$$\sum_{i \gg -\infty} s_i t^i$$

mit Koeffizienten s_i aus k.

3.2.1 Quadratische Gleichungen in Körpern $\mathbb{F}_{2^n}$

Es sei $n \in \mathbb{N}$. Ferner wählen wir zwei Elemente a und b aus $\mathbb{F}_{2^n}$. Wir wollen die Anzahl der Lösungen der quadratischen Gleichung

$$X^2 + aX + b = 0$$

über $\mathbb{F}_{2^n}$ ermitteln. Bekanntlich ist die Erweiterung $\mathbb{F}_{2^n}|\mathbb{F}_2$ zyklisch (insbesondere also galoissch) vom Grade n. Ein Erzeuger von $G := \mathrm{Gal}(\mathbb{F}_{2^n}|\mathbb{F}_2)$ ist der auf $\mathbb{F}_{2^n}$ eingeschränkte Frobenius-Automorphismus

$$F : \overline{\mathbb{F}_2} \to \overline{\mathbb{F}_2}\ ,\ x \mapsto x^2\ .$$

In dieser speziellen Situation haben wir für jedes a aus $\mathbb{F}_{2^m}$ die Relation

$$\mathrm{Tr}_{\mathbb{F}_{2^n}|\mathbb{F}_2}(a) = \sum_{\sigma \in G} \sigma(a) = \sum_{i=0}^{n-1} a^{2^i}\ .$$

Der Schlüssel für die wohlbekannte Lösung unseres Problems ist die folgende "additive Version" des "Satzes 90" von Hilbert:

Satz 3.12. *(Hilbert 90) Es sei $M|L$ eine endliche galoissche Erweiterung mit zyklischer Galois-Gruppe $G = Gal(M|L)$. Ferner sei $\beta \in M$ und σ ein Erzeuger von G, dann gilt*

$$\beta = a - \sigma(a) \text{ für ein } a \in M \text{ genau dann, falls } Tr_{M|L}(\beta) = 0 \text{ gilt.}$$

Beweis. Siehe z.B. Lang ([6], Kapitel VIII, §6, Seite 215). □

Korollar 3.13. *Die Gleichung* $X^2 + aX + b = 0$ *mit* $a, b \in \mathbb{F}_{2^n}$ *besitzt in* $\mathbb{F}_{2^n}$

- *keine Lösung im Falle* $a \neq 0$ *und* $Tr_{\mathbb{F}_{2^n}:\mathbb{F}_2}(\frac{b}{a^2}) = 1$,
- *eine Lösung im Falle* $a = 0$ *und*
- *zwei Lösungen im Falle* $a \neq 0$ *und* $Tr_{\mathbb{F}_{2^n}:\mathbb{F}_2}(\frac{b}{a^2}) = 0$.

Beweis. Es sei $a = 0$. Da der auf $\mathbb{F}_{2^n}$ eingeschränkte Frobenius-Automorphismus bijektiv ist, gibt es genau ein $x \in \mathbb{F}_{2^n}$ mit $F(x) = x^2 = b$.

Es sei $a \neq 0$. Ist α eine Lösung der Gleichung in der Behauptung unseres Korollars, so offenbar auch $\alpha + a \neq \alpha$. D.h. es sind nur noch zwei oder keine Lösungen möglich. Beachten wir, dass wir in Charakteristik 2 rechnen, so folgt für ein $x \in \mathbb{F}_{2^n}$

$$\begin{aligned} x^2 + ax + b = 0 \quad &\Leftrightarrow \quad \left(\frac{x}{a}\right)^2 + \frac{x}{a} = \frac{b}{a^2} \\ &\Leftrightarrow \quad \frac{x}{a} - F\left(\frac{x}{a}\right) = \frac{b}{a^2} \ . \end{aligned}$$

Nun ist wie schon eingangs bemerkt die endliche Erweiterung $\mathbb{F}_{2^n}|\mathbb{F}_2$ zyklisch und $F|_{\mathbb{F}_{2^n}}$ ein Erzeuger von $\mathrm{Gal}(\mathbb{F}_{2^n}|\mathbb{F}_2)$. Deswegen folgt mit der additiven Version des Satzes 90 von Hilbert

$$\frac{x}{a} - F\left(\frac{x}{a}\right) = \frac{b}{a^2} \Leftrightarrow \mathrm{Tr}_{\mathbb{F}_{2^n}:\mathbb{F}_2}(\frac{b}{a^2}) = 0 \ .$$

Da die Abbildung $\mathrm{Tr}_{\mathbb{F}_{2^n}:\mathbb{F}_2}$ nur Werte in $\mathbb{F}_2 = \{0, 1\}$ annimmt, folgt daraus die Behauptung. □

Beispiel 3.14. Das Polynom $f = X^3 + X + 1 \in \mathbb{F}_2[X]$ ist irreduzibel, denn wenn es reduzibel wäre, hätte es einen linearen Faktor, was nicht der Fall ist. Wählen wir ein $\alpha \in \overline{\mathbb{F}_2}$ mit $f(\alpha) = 0$, so gilt

$$\mathbb{F}_{2^3} = \mathbb{F}_2[\alpha] \cong \mathbb{F}_2[X]/(f) \ .$$

Eine $\mathbb{F}_2-$Basis von $\mathbb{F}_{2^3}$ ist gegeben durch $\{1, \alpha, \alpha^2\}$. Wegen der $\mathbb{F}_2-$Linearität der Spur-Abbildung $\mathrm{Tr} := \mathrm{Tr}_{\mathbb{F}_{2^3}:\mathbb{F}_2}$ gilt für jedes

$$a := a_1 + a_2\alpha + a_3\alpha^2 \in \mathbb{F}_{2^3}$$

mit $a_1, a_2, a_3 \in \mathbb{F}_2$ die Beziehung

$$\mathrm{Tr}(a) = a_1\mathrm{Tr}(1) + a_2\mathrm{Tr}(\alpha) + a_3\mathrm{Tr}(\alpha^2) \ .$$

Nun gilt mit Hilfe der Relation $\alpha^3 = \alpha + 1$

$$\mathrm{Tr}(1) = 1^1 + 1^2 + 1^4 = 1 \ , \ \mathrm{Tr}(\alpha) = \alpha + \alpha^2 + \alpha^4 = 0 \ \text{ und}$$
$$\mathrm{Tr}(\alpha^2) = \alpha^2 + \alpha^4 + \alpha^8 = \alpha^2(1 + \alpha^2 + \alpha^6) = 0 \ .$$

Damit folgt $\mathrm{Tr}(a) = a_1$. Nach unserem Korollar besitzt die Gleichung

$$x^2 + x = a$$

in $\mathbb{F}_{2^3}$ genau 2 Lösungen, falls $a_1 = 0$ gilt und im Fall $a_1 = 1$ keine Lösung.

3.2.2 Differentiale und Residuen

Es sei t eine Uniformisierende von K, dann gilt $K = k((t))$. Für ein Element $f = \sum_{i \gg -\infty} a_i t^i$ mit Koeffizienten a_i in k ist die formale Ableitung nach t definiert durch

$$\frac{\partial f}{\partial t} := \sum_{i \gg -\infty} i a_i t^{i-1} \, .$$

Hierführ haben wir das folgende Lemma:

Lemma 3.15. *Es sei t eine Uniformisierende von K . Dann gilt:*

(i) Für f, g aus K gilt die Produktregel

$$\frac{\partial (fg)}{\partial t} = f \frac{\partial g}{\partial t} + g \frac{\partial f}{\partial t} \, .$$

(ii) Ist t' eine weitere Uniformisierende von K, so gilt für jedes f aus K

$$\frac{\partial f}{\partial t'} \frac{\partial t'}{\partial t} = \frac{\partial f}{\partial t} \, .$$

Beweis. Siehe z.B. das Buch von Artin ([1], Kapitel 10., Abschnitt 3., S. 200). □

Definition 3.16. Es sei M ein $K-$Vektorraum. Wir nennen eine Abbildung $\delta : K \to M$ *eine stetige $k-$Derivation von K nach M*, falls für alle $f \in K$ und alle Uniformisierenden t von K die Beziehung

$$\delta(f) = \frac{\partial f}{\partial t}\delta(t) \tag{3.1}$$

gilt. Insbesondere ist, da die formale Ableitung $k-$linear ist und die Produktregel gilt, jede stetige $k-$Derivation von K nach M auch eine $k-$Derivation von K nach M, d.h. es gilt

$$\delta(fg) = f\delta(g) + g\delta(f) \text{ und } \delta(af + bg) = a\delta(f) + b\delta(g)$$

für alle $a, b \in k$ und $f, g \in K$.

D.h. die Funktionen $\frac{\partial \cdot}{\partial t}$ sind stetige $k-$Derivationen von K nach K.

Bemerkung 3.17.

(i) Es reicht aus die Bedingung 3.1 für eine feste Uniformisierende t zu bestätigen, denn ist t' eine weitere Uniformisierende von K, so folgt

$$\frac{\partial f}{\partial t'}\delta(t') = \frac{\partial f}{\partial t'}\frac{\partial t'}{\partial t}\delta(t) = \frac{\partial f}{\partial t}\delta(t) \ .$$

(ii) Das Bild einer stetigen $k-$Derivation $\delta : K \to M$ ist offenbar eine Teilmenge des eindimensionalen Vektorraums $V := \delta(t)K \subset M$ für eine Uniformisierende t. Dieser erbt auf natürliche Weise die Topologie von K. Und bezüglich dieser Topologie wird δ stetig, da die formalen Ableitungen $\frac{\partial \cdot}{\partial t}$ stetig sind.

Definition 3.18. Es sei
N das $K-$freie Erzeugnis der Menge (von Symbolen) $\{d_f : f \in K\}$ und
N' der $K-$Untervektorraum von N, der durch Vektoren der Form

$$d_f - \frac{\partial f}{\partial t}d_t$$

mit Uniformisierenden t von K und beliebigen Elementen f aus K erzeugt sei. Dann nennen wir den $K-$Vektorraum

$$\Omega'_{K|k} := N/N'$$

den *$K-$Vektorraum der Differentiale von K* und die stetige $k-$Derivation

$$d : K \to \Omega'_{K|k} \ , \ d(f) := d_f \mod N'$$

heißt die *universelle stetige Derivation* von $K|k$. Wir schreiben, falls keine Widersprüche zu erwarten sind, auch df statt $d(f)$.

Proposition 3.19. *$\Omega'_{K|k}$ ist ein eindimensionaler $K-$Vektorraum, der für jede Uniformisierende t von K die Basis $\{dt\}$ hat.*

Beweis. Es sei t eine Uniformisierende von K. Offenbar ist $\{dt\}$ ein Erzeugendensystem von $\Omega'_{K|k}$. Zu zeigen ist noch $dt \neq 0$. Nehmen wir an, es würde $d_t \in N'$ gelten. Da N' offenbar schon von den Elementen $d_f - \frac{\partial f}{\partial t} d_t$ mit $f \in K$ erzeugt wird, können wir d_t als Linear-Kombination linear unabhängiger solcher Erzeuger schreiben:

$$d_t = \sum_{i=1}^{r} \alpha_i \left(d_{f_i} - \frac{\partial f_i}{\partial t} d_t \right) = \sum_{i=1}^{r} \alpha_i d_{f_i} - \left(\sum_{i=1}^{r} \alpha_i \frac{\partial f_i}{\partial t} \right) d_t \ .$$

Da die Vektoren $d_{f_1}, d_{f_2}, ..., d_{f_r}$ und d_t nach Konstruktion alle paarweise verschieden und damit linear unabhängig sind, folgt aus der obigen Identität $\alpha_i = 0$ für $i = 1, ..., r$. Damit wäre aber $d_t = 0 \in N$, was nicht sein kann. Also war die Annahme $d_t \in N'$ falsch und es gilt $dt \neq 0$. Das war zu zeigen. □

Bemerkung 3.20. Bezeichnet $\Omega_{K|k}$ den $K-$Vektorraum der Kähler-Differentiale von $K|k$ und $\delta : K \to \Omega_{K|k}$ die universelle Derivation von $K|k$, so gilt

$$\Omega'_{K|k} \simeq \Omega_{K|k}/U$$

mit dem $K-$Untervektorraum $U = \cap_{i=1}^{\infty} \mathfrak{p}_K^i \delta(\mathcal{O}_K)$ von $\Omega_{K|k}$ (siehe dazu z.B. das Buch von Serre ([10] , Kapitel II, 7., Lemma 2)).

Definition 3.21. Es sei t eine Uniformisierende von K. Jedes ω aus $\Omega'_{K|k}$ besitzt eine eindeutige Darstellung $\omega = f dt$ mit $f = \sum_{i \gg -\infty} a_i t^i \in K = k((t))$. Wir setzen $\mathrm{Res}_t(\omega) := a_{-1}$ und erhalten so eine wohlbestimmte $k-$lineare Abbildung

$$\mathrm{Res}_t : \Omega'_{K|k} \to k \ .$$

Dazu haben wir den folgenden Satz:

Satz/Definition 3.22. *Für zwei beliebige Uniformisierende t und t' von K gilt $Res_t = Res_{t'}$. Deswegen setzen wir $Res := Res_t$ und erhalten eine wohlbestimmte $k-$lineare Abbildung*

$$Res : \Omega'_{K|k} \to k \ .$$

Für ein $\omega \in \Omega'_{K|k}$ heißt $Res(\omega)$ das Residuum *von ω.*

Beweis. Siehe das Buch von Serre ([10], Kapitel II, 7., Prop. 5') . □

3.2.3 Das Artin-Schreier-Symbol und quadratische Kongruenzen

Definition 3.23. Wir definieren die Abbildung

$$[\cdot,\cdot)_K : K \times K^* \to \mathbb{F}_2 \subset K$$

durch

$$[f,g)_K := \mathrm{Tr}_{k|\mathbb{F}_2}\left(\mathrm{Res}\left(f\frac{dg}{g}\right)\right) .$$

$[\cdot,\cdot)_K$ heißt das *Artin-Schreier-Symbol* von K.

Wir wollen gleich die Bedeutung dieses Symbols für unser Ausgangsproblem hervorheben:

Satz 3.24. *Es gelte $a, b \in \mathcal{O}_K$, dann gilt:*

$$\left(\frac{a,b}{K}\right) = \begin{cases} 1 & \textit{falls } a \in \mathcal{O}_K^* \textit{ und } \left[\frac{b}{a^2},\pi\right)_K = 0 \textit{ gilt,} \\ 0 & \textit{falls } a \in \mathfrak{p}_K \textit{ gilt,} \\ -1 & \textit{falls } a \in \mathcal{O}_K^* \textit{ und } \left[\frac{b}{a^2},\pi\right)_K = 1 \textit{ gilt.} \end{cases}$$

Beweis. Auf Grund der Bemerkung 3.1 reicht es wieder aus, $a \in \mathcal{O}_K^*$ anzunehmen und die Beziehung

$$\left(\frac{a,b}{K}\right) = 1 \Leftrightarrow \left[\frac{b}{a^2},\pi\right)_K = 0$$

zu bestätigen. Es gilt $K = k((\pi))$. Wir schreiben

$$a = \sum_{i=0}^{\infty} a_i\pi^i \quad \text{und} \quad b = \sum_{i=0}^{\infty} b_i\pi^i$$

mit $a_i, b_i \in k$ für alle i und $a_0 \neq 0$. Mit Hilfe von Korollar 3.13 haben wir

$$\begin{aligned} \left(\frac{a,b}{K}\right) = 1 \quad &\Leftrightarrow \quad x^2 + ax + b \equiv 0 \mod \mathfrak{p}_K \text{ für ein } x \in \mathcal{O}_K. \\ &\Leftrightarrow \quad x^2 + a_0x + b_0 = 0 \text{ für ein } x \in k. \\ &\Leftrightarrow \quad \mathrm{Tr}_{k|\mathbb{F}_2}\left(\frac{b_0}{a_0^2}\right) = 0 \, . \end{aligned}$$

Auf Grund der Definition des Artin-Schreier-Symbols bleibt nur noch aus, die Beziehung

$$\mathrm{Res}\left(\frac{b}{a^2}\frac{d\pi}{\pi}\right) = \frac{b_0}{a_0^2}$$

zu bestätigen. Offenbar gilt

$$\frac{b}{a^2} \equiv \frac{b_0}{a_0^2} \mod \mathfrak{p}_K \text{ ; d.h. es gilt } \frac{b}{a^2\pi} - \frac{b_0}{a_0^2\pi} \in \mathcal{O}_K \, .$$

Also haben wir

$$\mathrm{Res}\left(\frac{b}{a^2}\frac{d\pi}{\pi}\right) = \mathrm{Res}\left(\frac{b_0}{a_0^2}\frac{d\pi}{\pi}\right) = \frac{b_0}{a_0^2} \, .$$

Damit ist der Beweis des Satzes abgeschlossen. □

3.2.4 Eigenschaften des Artin-Schreier-Symbols

Definition 3.25. Für einen beliebigen Körper F der Charakteristik 2 definieren wir den Operator

$$\wp : F \to F \ , \ x \mapsto x^2 - x \ .$$

Dieser ist offenbar ein Endomorphismus der additiven Gruppe von F.

Nun folgen einige wohlbekannte Eigenschaften des Artin-Schreier-Symbols, die wir direkt an der Definition ablesen können:

Satz 3.26. *Es gelten:*

(i) $[a+a', b)_K = [a, b)_K + [a', b)_K$ *für* $a, a' \in K$ *und* $b \in K^*$.

(ii) $[a, bb')_K = [a, b)_K + [a, b')_K$ *für* $a \in K$ *und* $b, b' \in K^*$.

(iii) Es gilt $[\wp(a), b)_K = 0$ *und* $[a, b^2)_K = 0$ *für alle* $a \in K$ *und* $b \in K^*$ *und daher induziert* $[\cdot,\cdot)_K$ *eine bilineare Abbildung*

$$K/\wp(K) \times K^*/K^{*2} \to \mathbb{F}_2 \ .$$

Beweis. Zu (i) und (ii): Beide Aussagen folgen auf Grund der Additivität von $\mathrm{Tr}_{k|\mathbb{F}_2}$ und Res, sowie der Identitäten

$$(a+a')\frac{db}{b} = a\frac{db}{b} + a'\frac{db}{b} \quad \text{und} \quad a\frac{d(bb')}{bb'} = a\frac{db}{b} + a\frac{db'}{b'}$$

in $\Omega'_{K|k}$ für $a, a' \in K$ und $b, b' \in K^*$.

Zu (iii): Es seien $a \in K$ und $b \in K^*$ vorgegeben.

Wir zeigen $[\wp(a), b)_K = 0$. Wir können $b \in K^*$ als $b = \pi^l \epsilon = \pi^{l-1}\pi'$ mit l aus $\mathbb{Z}$, ϵ aus $\mathcal{O}_K^*$ und Uniformisierenden π und π' schreiben. Deswegen reicht es auf Grund der Linearität von $[\cdot,\cdot)_K$ im zweiten Argument aus, die Behauptung $[\wp(a), t)_K = 0$ für eine feste Uniformisierende t von K zu beweisen. Schreiben wir a als

$$a = \sum_{i \gg -\infty} a_i t^i$$

mit a_i in k für alle i und setzen wir

$$a' := \sum_{i<0} a_i t^i \quad \text{und} \quad a'' := \sum_{i>0} a_i t^i \ ,$$

so folgt auf Grund der Additivität von Res und $\wp$ die Beziehung

$$\begin{aligned} \mathrm{Res}\left(\wp(a)\frac{dt}{t}\right) &= \mathrm{Res}\left(\wp\left(a'\right)\frac{dt}{t}\right) + \mathrm{Res}\left(\wp(a_0)\frac{dt}{t}\right) + \mathrm{Res}\left(\wp\left(a''\right)\frac{dt}{t}\right) \\ &= 0 + \mathrm{Res}\left(\wp(a_0)\frac{dt}{t}\right) + 0 \\ &= \mathrm{Res}\left(\wp(a_0)\frac{dt}{t}\right) = \wp(a_0) \ . \end{aligned}$$

Ist f die Dimension von k über $\mathbb{F}_2$, so gilt

$$\operatorname{Tr}_{k|\mathbb{F}_2}(\wp(a_0)) = \operatorname{Tr}_{k|\mathbb{F}_2}(a_0^2 - a_0) = \sum_{i=0}^{f-1} \left(a_0^{2^{i+1}} - a_0^{2^i} \right) = 0 \; .$$

Damit folgt schließlich $[\wp(a), t)_K = 0$ und das war zu zeigen.

Jetzt zeigen wir $[a, b^2)_K = 0$. Wegen $a\frac{d(b^2)}{b^2} = 2 \cdot ba\frac{db}{b^2} = 0 \in \Omega'_{K|k}$ folgt offenbar

$$\left[a, b^2\right)_K = \operatorname{Tr}_{k|\mathbb{F}_2}\left(\operatorname{Res}\left(a\frac{d(b^2)}{b^2} \right) \right) = \operatorname{Tr}_{k|\mathbb{F}_2}\left(\operatorname{Res}(0)\right) = 0 \; .$$

$\square$

4 Die Transformationsformel für lokale Körper

Im ganzen Abschnitt sei K ein lokaler Körper mit Ganzheitsring $\mathcal{O}_K$, Primideal $\mathfrak{p}_K$ und Betrag $|\cdot|_K$. Ferner sei π eine Uniformisierende von K.

Ein wichtiges Hilfsmittel für die Bestimmung der in der Einleitung erwähnten Dichte h ist die Transformationsformel für lokale Körper. Sie ist das Analogon der wohlbekannten Transformationsformel im $\mathbb{R}^n$ und hat die Form

$$\int_{\phi(U)} f(x)d\mu(x) = \int_U f \circ \phi(x) \, |J\phi(x)|_K \, d\mu(x) \; .$$

Dabei ist nun U eine offene Teilmenge des K^n (anstatt des $\mathbb{R}^n$), ϕ eine injektive "$K-$analytische" Funktion deren Jacobische nirgends verschwindet (anstatt einer injektiven C^1-Funktion, deren Jacobische nicht verschwindet), μ ein Haar-Maß auf K^n (anstatt des auf die Borel-Mengen des $\mathbb{R}^n$ eingeschränkten Lebesgue-Maßes) und schließlich f eine beliebige $\mu-$integrierbare Funktion des K^n (anstatt des $\mathbb{R}^n$). Wir geben im Wesentlichen den Beweis im Buch von Igusa (vgl. [5]) wieder.

4.1 Maßtheoretische Hilfssätze und Konventionen

Es sei $\widehat{\mathbb{R}} = \mathbb{R} \cup \{-\infty, \infty\}$ die eingangs dieser Arbeit definierte Kompaktifizierung von $\mathbb{R}$. Wir setzen wie in der Maßtheorie üblich zusätzlich

$$\infty - \infty := -\infty + \infty := 0 \cdot \infty := 0 \; .$$

Dies ist keineswegs topologisch motiviert. Es hat jedoch den Vorteil, dass wir später integrierbare Funktionen, die ja höchstens auf messbaren Mengen vom Maß Null den Wert ∞ oder $-\infty$ annehmen können, addieren können. Insbesondere wird das Integral dann $\mathbb{R}-$linear werden. Wir wiederholen im "Schnelldurchlauf" einige Definitionen und Aussagen aus der Maßtheorie, die wir benötigen werden. Als Grundlage dient uns dabei das Buch von Elstrodt (siehe [3]).

Definition 4.1. (Maße) Es sei X eine Menge und $\mathcal{P}(X) := \{M : M \subset X\}$ ihre Potenzmenge.

(i) Eine *$\sigma-$Algebra* Σ auf X ist eine Teilmenge von $\mathcal{P}(X)$, die die Mengen $\emptyset$, X und jede abzählbare Vereinigung sowie Komplemente von Mengen aus Σ enthält.

(ii) Es sei $S \subset \mathcal{P}(X)$, dann ist die *von S erzeugte* $\sigma-$Algebra auf X der Durchschnitt aller $\sigma-$Algebren auf X, die S enthalten. Dieser Durchschnitt ist bekanntlich nicht leer und wieder eine $\sigma-$Algebra.

(iii) Es sei Σ eine $\sigma-$Algebra auf X. Ein *Maß μ auf X* ist eine Abbildung

$$\mu : \Sigma \to [0, \infty] \, ,$$

die für jede Folge $(A_i)_{i\in\mathbb{N}}$ paarweise disjunkter Elemente $A_i \in \Sigma$ die Eigenschaften

$$\mu(\emptyset) = 0 \ \text{ und } \ \mu\left(\cup_{i=1}^{\infty} A_i\right) = \sum_{i=1}^{\infty} \mu(A_i)$$

erfüllt. Σ heißt die *zu μ gehörige $\sigma-$Algebra* oder einfach die *$\sigma-$Algebra von μ* und die Elemente von Σ heißen *$\mu-$messbar* oder einfach *messbar,* wenn klar ist, um welches Maß μ es sich handelt.

Definition 4.2. (Messbare Funktionen) Es sei X eine Menge und μ ein Maß auf X mit der $\sigma-$Algebra Σ.

(i) Für eine Teilmenge $M \subset X$ definieren wir die *charakteristische Funktion von M* als die Funktion $\chi_M : X \to \mathbb{R}$ gegeben durch

$$\chi_M(x) := \begin{cases} 1 & \text{falls } x \in M \text{ gilt,} \\ 0 & \text{sonst.} \end{cases}$$

(ii) Eine *$\mu-$Treppenfunktion* auf X ist eine Funktion $s = \sum_{i=1}^{r} a_i \chi_{M_i}$ mit Konstanten $a_i \in \mathbb{R}$ und $\mu-$messbaren Mengen $M_i \subset X$.

(iii) Eine *$\mu-$messbare Funktion* ist eine Funktion $f : X \to \widehat{\mathbb{R}}$, bei der für jedes $a \in \mathbb{R}$ das Urbild von $]a, \infty]$ eine $\mu-$messbare Menge ist. Die Menge der $\mu-$messbaren Funktionen bezeichnen wir mit $\mathcal{M}(\mu, X)$. Offenbar ist jede $\mu-$Treppenfunktion messbar.

Wir kommen jetzt zur Integral-Definition. Dazu schreiben wir für zwei Funktionen $f, g : X \to \widehat{\mathbb{R}}$

$$f \leq g \text{ genau dann, falls für alle } x \in X \text{ die Beziehung } f(x) \leq g(x) \text{ gilt .}$$

Satz/Definition 4.3. *(Lebesgue-Integration) Es sei μ ein Maß auf einer Menge X.*

(i) Wir definieren für eine nicht negative $\mu-$Treppenfunktion $s = \sum_{i=1}^r a_i \chi_{M_i}$ das Integral von s *als*

$$\int_X s(x)d\mu(x) := \sum_{i=1}^{r} a_i \mu(M_i) \; .$$

Dies ist wohldefiniert, also unabhängig von der Wahl der Darstellung von s als Linearkombination charakterisitscher Funktionen.

(ii) Für eine nicht negative Funktion $f \in \mathcal{M}(\mu, X)$ definieren wir das Integral von f *als*

$$\int_X f(x)d\mu(x) := \sup \left\{ \int_X s(x)d\mu(x) : 0 \leq s \leq f, s \text{ Treppenfkt.} \right\} \; .$$

*Dies ist offenbar wohldefiniert. f heißt $\mu-$*integrierbar*, falls sein Integral einen Wert kleiner als ∞ hat.*

(iii) Es sei $I \in \mathcal{M}(\mu, X)$ beliebig. Dann lässt sich I in eindeutiger Weise als $I = f_1 - f_2$ mit nicht negativen $\mu-$messbaren Funktionen f_1 und $f_2$schreiben. Sind f_1 und f_2 beide $\mu-$integrierbar so heißt I $\mu-$integrierbar und wir definieren das Integral von I *als*

$$\int_X I(x)d\mu(x) := \int_X f_1(x)d\mu(x) - \int_X f_2(x)d\mu(x) \; .$$

Die Menge der $\mu-$integrierbaren Funktionen werde mit $\mathcal{L}(\mu, X)$ bezeichnet. Das Integral gibt uns eine $\mathbb{R}-$lineare Abbildung

$$\mathcal{L}(\mu, X) \to \mathbb{R} \; .$$

Beweis. Offensichtlich ist nur (i) und (iii) zu beweisen. Siehe hierzu das Buch von Elstrodt ([3], Kapitel III, Kor. 4.10, Kapitel IV, Lem. 1.1.). □

Satz 4.4. *Es sei μ ein Maß auf einer Menge X.*

(i) Eine Funktion $f : X \to [0, \infty]$ ist genau dann $\mu-$messbar, falls es eine monoton steigende Folge $(t_i)_{i \in \mathbb{N}}$ nicht negativer $\mu-$Treppenfunktionen gibt, die punktweise gegen f konvergiert.

(ii) (Satz von B.Levi) Es sei $(f_i)_{i \in \mathbb{N}}$ eine monotone Folge nicht negativer $\mu-$messbarer Funktionen auf X, die punktweise gegen eine Funktion $f : X \to \widehat{\mathbb{R}}$ konvergiere, dann ist f ebenfalls nicht negativ und $\mu-$messbar und es gilt

$$\lim_{i \to \infty} \int_X f_i(x) d\mu(x) = \int_X f(x) d\mu(x) \ .$$

Beweis. Vergleiche das Buch von Elstrodt ([3], Kapitel III, Satz 4.13, Kapitel IV, Satz 2.7). □

Definition 4.5. (Topologische Maße) Es sei X ein Hausdorff-Raum und $\tau \subset \mathcal{P}(X)$ die Menge der offenen Mengen in X. Wir bezeichnen ferner mit $C_c(X)$ die Menge der stetigen Funktionen $f : X \to \mathbb{R}$ mit kompaktem Träger.

(i) Die $\sigma-$Algebra auf X, die durch τ erzeugt wird, werde mit $\mathcal{B}(X)$ bezeichnet und heißt die Menge der *Borel-Mengen* von X.

(ii) Jedes Maß μ auf X, welches als $\sigma-$Algebra $\mathcal{B}(X)$ hat, heißt *topologisches Maß* auf X. Offensichtlich sind dann die Funktionen aus $C_c(X)$ alle $\mu-$messbar.

(iii) Ein *Radon-Maß* auf X ist ein topologisches Maß auf X, bezüglich dessen jede Funktion $f \in C_c(X)$ integrierbar ist.

(iv) Ist $G := X$ zusätzlich eine (additiv geschriebene) topologische Gruppe, so heißt jedes Radon-Maß μ auf G, welches nicht identisch Null ist und für das

$$\mu(a + B) = \mu(B)$$

für alle $a \in G$ und $B \in \mathcal{B}(G)$ gilt, ein (linkes) *Haar-Maß* auf G.

Die Existenz von Haar-Maßen auf lokal-kompakten Hausdorff-Räumen ist gesichert. Es gilt nämlich der folgende Satz:

Satz 4.6. *Es sei G eine lokal-kompakte hausdorffsche topologische Gruppe. Dann existiert auf G ein Haar-Maß μ und jedes weitere Haar-Maß μ' auf G erfüllt $\mu' = c\mu$ für eine Konstante $c \in \mathbb{R}$ mit $c > 0$.*

Beweis. Siehe das Buch von Elstrodt ([3], Kapitel VIII, Satz 3.12). □

Nun führen wir den für unsere Zwecke wichten Begriff des Bild-Maßes ein:

Satz/Definition 4.7. *Es seien X und Y Hausdorff-Räume. Dann gilt:*

(i) Ist $f : X \to Y$ eine stetige Funktion, dann gilt für jedes $B \in \mathcal{B}(Y)$ die Beziehung $f^{-1}(B) \in \mathcal{B}(X)$, d.h. das Urbild jeder Borel-Menge in Y unter f ist eine Borel-Menge in X.

(ii) (Bild-Maß) Ist μ ein topologisches Maß auf X und $f : X \to Y$ stetig, so heißt das topologische Maß $f(\mu)$ auf Y gegeben durch

$$f(\mu)(B) := \mu(f^{-1}(B))$$

für alle $B \in \mathcal{B}(Y)$ das Bild-Maß *oder einfach das* Bild *von μ unter f.*

Beweis. Es ist nur (i) zu beweisen. Siehe hierzu Elstrodt ([3], Kapitel III, Kor. 1.4). □

Schließlich geben wir noch einige Eigenschaften von Radon-Maßen auf lokal-kompakten Hausdorff-Räumen mit abzählbarer Basis an. Beispiele für solche Räume sind K^m oder $\mathrm{Mat}(m, K)$ mit $m \in \mathbb{N}$.

Satz 4.8. *Es sei X ein lokal-kompakter Hausdorff-Raum mit abzählbarer Basis, dann gilt:*

(i) Ein topologisches Maß μ auf X ist genau dann ein Radon-Maß, falls $\mu(C) < \infty$ für alle kompakten Mengen $C \subset X$ gilt.

(ii) (Regularität) Ein Radon-Maß μ auf X ist regulär, *d.h. es gilt für jede Borelmenge $B \in \mathcal{B}(X)$:*

$$\sup\{\mu(C) : C \subset B, C \text{ kompakt}\} = \mu(B) = \inf\{\mu(U) : U \supset B, U \text{ offen}\} .$$

(iii) (Produktmaße) Es seien μ ein Radon-Maß auf X und ν ein Radon-Maß auf einem weiteren lokal-kompakten Hausdorff-Raum mit abzählbarer Basis Y, dann gilt:

1. *Die von $\mathcal{B}(X) \times \mathcal{B}(Y)$ erzeugte $\sigma-$Algebra über dem Produkt-Raum $X \times Y$ ist gleich $\mathcal{B}(X \times Y)$.*
2. *Es gibt genau ein Radon-Maß $\mu \times \nu$ auf $X \times Y$ mit*

$$\mu \times \nu(B \times B') = \mu(B)\nu(B')$$

für alle $B \in \mathcal{B}(X)$ und $B' \in \mathcal{B}(Y)$. $\mu \times \nu$ heißt das Produkt-Maß von μ und ν.

Beweis. Siehe Elstrodt ([3], Kapitel VIII, Kor. 1.12, Kapitel V, Bsp. 1.7 b.)). □

4.2 $K-$analytische Funktionen

Wir führen nun den Begriff der $K-$analytischen Funktion ein. Das Ziel dieses Abschnittes ist der Nachweis, dass eine beliebige $K-$analytische Funktion, deren Jacobische in einem Punkt nicht verschwindet, sich dort als Komposition gewisser einfacher bijektiver, in beiden Richtungen $K-$analytischer Funktionen schreiben lässt. Dieses Ergebnis bildet einen wichtigen Teil von Igusas Beweis der Transformationsformel.

Es sei für den ganzen Unterabschnitt $m \in \mathbb{N}$ fest gewählt. Es sei weiter $X := (X_1, X_2, ..., X_m)$ ein $m-$Tupel von Variablen über K. Wir bezeichnen mit $K[[X]]$ die Menge der formalen Potenzreihen

$$\sum_{i \in \mathbb{N}_0^m} c_i X^i := \sum_{(i_1, i_2, ..., i_m) \in \mathbb{N}_0^m} c_{i_1, i_2, ..., i_m} X_1^{i_1} X_2^{i_2} \cdots X_m^{i_m}$$

mit Koeffizienten c_i in K. Diese bildet bekanntlich mit den beiden wohldefinierten Verknüpfungen

$$\left(\sum_{i \in \mathbb{N}_0^m} c_i X^i \right) + \left(\sum_{j \in \mathbb{N}_0^m} d_j X^j \right) := \sum_{k \in \mathbb{N}_0^m} (c_k + d_k) X^k$$

und

$$\left(\sum_{i \in \mathbb{N}_0^m} c_i X^i \right) \cdot \left(\sum_{j \in \mathbb{N}_0^m} d_j X^j \right) := \sum_{k \in \mathbb{N}_0^m} \left(\sum_{i+j=k} c_i d_j \right) X^k$$

einen kommutativen Ring (mit der Eins $1 \in K$). $K[[X]]$ besitzt ein einziges maximales Ideal

$$\mathfrak{m} = \langle X_1, X_2, ..., X_m \rangle \ ,$$

ist also ein *lokaler Ring.*

$K[[X]]$ ist ferner ein topologischer Ring bezüglich der $\mathfrak{m}-$*adischen Topologie*, d.h der Topologie, bei der eine Umgebungsbasis jedes Punktes $f \in K[[X]]$ durch die Mengen $f + \mathfrak{m}^k$ mit $k \in \mathbb{N}_0$ gegeben ist. Auf Grund der Tatsache $\cap_{k=0}^{\infty} \mathfrak{m}^k = (0)$ ist $K[[X]]$ ein Hausdorff-Raum. Man überlegt sich, dass $K[[X]]$ bezüglich der $\mathfrak{m}-$adischen Topologie vollständig ist.

Ferner stellt man sicher, dass für eine Folge $(f_k)_{k \in \mathbb{N}}$ aus $K[[X]]$ die Summe

$$\sum_{i=1}^{\infty} f_i$$

genau dann konvergent ist, falls für jedes $N \in \mathbb{N}$ nur endlich viele der f_i nicht in $\mathfrak{m}^N$ liegen. Gilt insbesondere $f_1, f_2, ..., f_m \in \mathfrak{m}$ und $g \in K[[X]]$ so ist

$$g(f_1(X), f_2(X), ..., f_m(X))$$

wieder eine formale Potenzreihe (das ist die Einsetzungsregel für formale Potenzreihen). Über lokale Ringe kann man sich näher etwa in dem Buch von Serre (vgl. [12]) informieren.

Bevor wir zum Begriff der konvergenten formalen Potenzreihe kommen, wollen wir einige einfache Aussagen über die Konvergenz von Reihen in K festhalten.

Lemma 4.9. *Es sei $(a_i)_{i\in\mathbb{N}}$ eine Folge in K.*

(i) Für die Konvergenz der Reihe

$$\sum_{i=1}^{\infty} a_i$$

ist notwendig und hinreichend, dass $(a_i)_{i\in\mathbb{N}}$ eine Nullfolge in K ist.

(ii) Ist $\phi : \mathbb{N} \to \mathbb{N}$ eine Bijektion, dann ist mit jeder Nullfoge $(a_i)_{i\in\mathbb{N}}$ in K auch $(a_{\phi(i)})_{i\in\mathbb{N}}$ eine Nullfolge und es gilt die folgende Gleichheit konvergenter Reihen:

$$\sum_{i=1}^{\infty} a_i = \sum_{i=1}^{\infty} a_{\phi(i)} \ .$$

Beweis. Beide Aussagen sind eine Konsequenz der Tatsache, dass für $|\cdot|_K$ die starke Dreiecksungleichung gilt. Der einfache Beweis sei als Übung empfohlen. $\square$

Definition 4.10. Es sei I eine abzählbare Indexmenge. Wir nennen eine Familie $(a_i)_{i\in I}$ von Elementen a_i aus K *stark summierbar*, falls I endlich ist, oder falls im Falle $\#I = \infty$ für eine (und damit nach Lemma 4.9 (ii) für jede) Bijektion $\phi : \mathbb{N} \to I$ die Reihe

$$\sum_{n=1}^{\infty} a_{\phi(n)}$$

konvergiert. Dies ist nach Lemma 4.9 (i) genau dann der Fall, falls $(a_{\phi(n)})_{n\in\mathbb{N}}$ eine Nullfolge ist. Wir setzen dann

$$\sum_{i\in I} a_i := \begin{cases} \sum_{n=1}^{\infty} a_{\phi(i)} & \text{falls } \#I = \infty \text{ gilt,} \\ \sum_{i\in I} a_i & \text{sonst.} \end{cases}$$

Das ist wieder nach Lemma 4.9 (ii) wohldefiniert, also unabhängig von der eventuellen Wahl von ϕ. Schließlich nennen wir dann $\sum_{i\in I} a_i$ eine *stark konvergente Reihe.*

Offenbar ist eine Familie $(a_i)_{i\in I}$ von Elementen a_i aus K genau dann stark summierbar, falls für jedes $\epsilon > 0$ alle bis auf endlich viele a_i die Bedingung $|a_i|_K < \epsilon$ erfüllen. Wir werden im Folgenden oft für ein $m \in \mathbb{N}$ die Indexmenge $I := \mathbb{N}_0^m$ wählen. Setzen wir für ein Tupel $i = (i_1, i_2, ..., i_m)$ aus $\mathbb{N}_0^m$

$$|i| := i_1 + i_2 + ... + i_m \ ,$$

so können wir die starke Summierbarkeit von $(a_i)_{i\in\mathbb{N}_0^m}$ auch dadurch beschreiben, dass es zu jedem $\epsilon > 0$ ein $N \in \mathbb{N}$ mit

$$|a_i|_K < \epsilon$$

für $|i| \geq N$ gibt. Wir schreiben dann "$a_i \to 0$ für $|i| \to \infty$".

Lemma 4.11. *Es sei I eine abzählbare Indexmenge. Für jede stark summierbare Familie $(a_i)_{i\in I}$ gilt die Abschätzung*

$$\left|\sum_{i\in I} a_i\right|_K \leq \sup\{|a_i|_K : i \in I\} < \infty \ .$$

Beweis. Dies sei wiederum eine Übung für den Leser. □

Für stark summierbare Familien gilt der "große Umordnungssatz":

Satz 4.12. *Es seien M und I abzählbare Indexmengen . Weiter sei*

$$M = \bigcup_{\alpha\in I} M_\alpha$$

eine disjunkte Zerlegung von M in nichtleere Teilmengen M_α. Ist nun $(a_i)_{i\in M}$ stark summierbar, so gilt dies auch für jede Teilfamilie $(a_i)_{i\in M_\alpha}$. Setzen wir $s_\alpha := \sum_{i\in M_\alpha} a_i$

für $\alpha \in I$, so ist auch $(s_\alpha)_{\alpha\in I}$ summierbar und wir erhalten die folgende Identität konvergenter Reihen:

$$\sum_{i\in M} a_i = \sum_{\alpha\in I} s_\alpha \ .$$

Beweis. Wir zeigen: $(a_i)_{i\in M_\alpha}$ ist für jedes $\alpha \in I$ wieder stark summierbar. Nach Voraussetzung ist $(a_i)_{i\in M}$ stark summierbar und das heißt, dass für jedes $\epsilon > 0$ nur endlich viele Indizes i in M liegen, für die $|a_i|_K \geq \epsilon$ gilt, damit gilt dies sicher auch für die Indizes in $M_\alpha \subset M$. Also ist auch hier $(a_i)_{i\in M_\alpha}$ stark summierbar.

Wir zeigen nun, dass auch $(s_\alpha)_{\alpha\in I}$ stark summierbar ist. Für jedes $\alpha \in I$ haben nach Lemma 4.11 die Abschätzung

$$|s_\alpha|_K \leq \sup\{|a_i|_K : i \in M_\alpha\} \ .$$

Da $(a_i)_{i\in M}$ stark summierbar ist, kann es zu jedem $\epsilon > 0$ nur endlich viele Indizes $\alpha \in I$ geben, so dass es ein $a_i \in M_\alpha$ mit $|a_i|_K \geq \epsilon$ gibt. D.h. zu vorgegebenem $\epsilon > 0$ gilt für alle bis auf endlich viele Indizes α

$$|s_\alpha|_K \leq \epsilon \ .$$

Damit ist auch $(s_\alpha)_{\alpha\in I}$ stark summierbar.

Nun zur behaupteten Gleicheit: Wir setzen $s := \sum_{i\in M} a_i$ und zeigen: Für jedes $\epsilon > 0$ gilt

$$\left| s - \sum_{\alpha\in I} s_\alpha \right|_K \leq \epsilon \ ,$$

dann muss die behauptete Gleichheit gelten. Es sei $\epsilon > 0$ vorgegeben. Da $(a_i)_{i\in M}$ stark summierbar ist, gibt es eine endliche Teilmenge E von M mit $|a_i|_K < \epsilon/2$ für $i \in M - E$. Also gilt wieder mit Hilfe von Lemma 4.11

$$\left| s - \sum_{i\in E} a_i \right|_K \leq \epsilon/2 \ \text{ und } \ \left| s_\alpha - \sum_{i\in E\cap M_\alpha} a_i \right|_K \leq \epsilon/2$$

für alle $\alpha \in I$. Also folgt

$$\begin{aligned}
\left| s - \sum_{\alpha\in I} s_\alpha \right|_K &\leq \left| s - \sum_{i\in E} a_i \right|_K + \left| \sum_{i\in E} a_i - \sum_{\alpha\in I} s_\alpha \right|_K \\
&\leq \left| s - \sum_{i\in E} a_i \right|_K + \left| \sum_{\alpha\in I} \left(\sum_{i\in E\cap M_\alpha} a_i - s_\alpha \right) \right|_K \\
&\leq \epsilon/2 + \epsilon/2 = \epsilon \ .
\end{aligned}$$

Das war zu zeigen. $\square$

Definition 4.13. Es sei $(c_i)_{i\in\mathbb{N}_0^m}$ eine Familie von Elementen aus K. Die formale Potenzreihe

$$f = \sum_{i\in\mathbb{N}_0^m} c_i X^i$$

aus $K[[X]] = K[[X_1, X_2, ..., X_m]]$ heiße *konvergent,* falls es eine offene Umgebung V von $0 \in K^m$ gibt, so dass die Familie $(c_i x^i)_{i\in\mathbb{N}_0^m}$ für alle x in V stark summierbar ist. Für ein x aus V heißt dann die stark konvergente Reihe

$$f(x) = \sum_{i\in\mathbb{N}_0^m} c_i x^i$$

die *Auswertung von f an der Stelle x.*

Wir wollen nun einige einfache Eigenschaften konvergenter Potenzreihen zitieren.

Proposition 4.14. *Es sei $f = \sum_{i\in\mathbb{N}_0^m} c_i X^i \in K[[X]] = K[[X_1, X_2, ..., X_m]]$ eine konvergente Potenzreihe und V wie in der vorangehenden Definition.*

(i) Es gilt der Indentitätssatz*: Gilt $f(x) = 0$ für alle $x \in V$, so gilt $f = 0 \in K[[X]]$, d.h. es gilt $c_i = 0$ für alle i.*

(ii) Für jedes $a \in K^m$ ist durch

$$g : a + V \to K \ , \ x \mapsto f(x-a) = \sum_{i\in\mathbb{N}_0^m} c_i (x-a)^i$$

eine stetige Funktion gegeben.

(iii) Die formale Ableitung $\frac{\partial f}{\partial X_j} \in K[[X]]$ nach jeder Variable X_j ist wieder eine konvergente Potenzreihe und konvergiert dort stark, wo f stark konvergiert. Ferner ist die Funktion g in (ii) in jedem Punkt $u \in a + V$ partiell differenzierbar. D.h. bezeichnen wir für ein beliebiges $j \in \mathbb{N}_m$ mit E_j den Vektor aus K^m, der in der $j-$ten Komponente eine Eins hat und sonst nur Nullen hat, so existiert der Grenzwert

$$\frac{\partial g}{\partial x_j}(u) := \lim_{h\to 0} \frac{g(u + hE_j) - g(u)}{h} \ .$$

Überdies gilt $\frac{\partial g}{\partial x_j}(u) = \frac{\partial f}{\partial X_j}(u-a)$ für alle $u \in a + V$.

(iv) Es seien $f_1, f_2, ..., f_m, g$ aus $K[[X]] = K[[X_1, X_2, ..., X_m]]$ konvergente Potenzreihen. Wir bilden $f := (f_1, f_2, ..., f_m)$. Besitzen alle f_i keine konstanten Terme (d.h. gilt $f(0) = 0 \in K^m$), so ist $g(f_1(X), f_2(X), ..., f_m(X))$ ebenfalls eine konvergente Potenzreihe.

Beweis. Die Aussage (iv) ist offensichtlich. Für die Aussagen (i)-(iii) vergleiche man das Buch von Igusa ([5], Lemma 2.1.3). □

Definition 4.15. Es sei $U \subset K^m$ offen. Eine Funktion $f : U \to K$ heißt $K-$*analytisch*, falls für jeden Punkt $a = (a_1, a_2, ..., a_m)$ aus U eine offene Umgebung $V \subset U$ von a und eine Familie $(c_i)_{i \in \mathbb{N}_0^m}$ von Elementen aus K existiert, so dass f sich für alle $x \in V$ als stark konvergente Reihe

$$f(x) = \sum_{i \in \mathbb{N}_0^m} c_i (x - a)^i$$

darstellen lässt. Ferner nennen wir für ein $r \in \mathbb{N}$ eine Funktion $g : U \to K^r$ eine $K-$*analytische* Funktion, falls die Komponentenfunktionen $g_i : U \to K$ von $g = (g_1, g_2, ..., g_r)$ alle $K-$analytisch sind.

Beispiel 4.16.

(i) Es sei $U \subset K^m$ offen und r aus $\mathbb{N}$. Wir nennen eine Funktion $f : U \to K^r$ eine *Polynomfunktion*, falls es Polynome $f_1, f_2, ..., f_r \in K[X_1, X_2, ..., X_m]$ mit

$$f(x) = (f_1(x), f_2(x), ..., f_r(x))$$

für alle $x \in U$ gibt. Offenbar ist jede Polynomfunktion eine $K-$analytische Funktion.

(ii) Wir wählen eine Familie $(c_i)_{i \in \mathbb{N}_0^m}$ von Elementen aus $\mathcal{O}_K$ mit den Eigenschaften

$$c_0 = 0 \quad \text{und} \quad c_i \equiv 0 \mod \mathfrak{p}_K^{|i|-1}$$

für alle i aus $\mathbb{N}_0^m$ mit $|i| \geq 1$. Für $x = (x_1, x_2, ..., x_m)$ aus $\mathcal{O}_K^m$ gilt

$$\left|c_i x^i\right|_K = \left|c_i \prod_{k=1}^{m} x_k^{i_k}\right|_K \leq |c_i|_K \leq q^{-(i_1+i_2+...+i_m-1)} .$$

D.h. es folgt $c_i x^i \to 0$ für $|i| \to \infty$. Deswegen erhalten wir die Funktion $f : \mathcal{O}_K^m \to \mathcal{O}_K$, die durch die stark konvergente Reihe

$$f(x) = \sum_{i \in \mathbb{N}_0^m} c_i x^i$$

für alle x aus $\mathcal{O}_K^m$ gegeben ist. Wir zeigen nun, dass f eine $K-$analytische Funktion ist. Dazu müssen wir zeigen, dass sich f um jedem Punkt $a \in \mathcal{O}_K^m$ in eine stark konvergente Reihe entwickeln lässt. Wir schreiben für jedes i aus $\mathbb{N}_0^m$

$$x^i = (x - a + a)^i = \sum_{j \in \mathbb{N}_0^m} d_{i,j} (x - a)^j$$

mit Konstanten $d_{i,j}$ aus $\mathcal{O}_K$ (von denen alle bis auf endlich viele Null sind). Für ein x aus $V := a + \pi \mathcal{O}_K^m$ finden wir:

$$\left|c_i d_{i,j} (x - a)^j\right|_K \leq \left|c_i (x - a)^j\right|_K \leq q^{-(i_1+i_2+...+i_m-1)} q^{-(j_1+j_2+...+j_m)} .$$

Also folgt $c_i d_{i,j}(x-a)^j \to 0$ für $|(i,j)| \to \infty$. Wenden wir den starken Umordnungssatz an, so erhalten wir für alle $x \in V \subset \mathcal{O}_K^m$ eine Darstellung von f als stark konvergente Reihe

$$f(x) = \sum_{i \in \mathbb{N}_0^m} c_i x^i = \sum_{i \in \mathbb{N}_0^m} \sum_{j \in \mathbb{N}_0^m} c_i d_{i,j}(x-a)^j = \sum_{j \in \mathbb{N}_0^m} \left(\sum_{i \in \mathbb{N}_0^m} c_i d_{i,j} \right) (x-a)^j \ .$$

Die folgenden beiden Aussagen sind eine direkte Konsequenz der Definition der $K-$analytischen Funktionen und des Lemmas 4.14:

Proposition 4.17. *Es sei $U \subset K^m$ offen. Dann ist jede $K-$analytische Funktion $f : U \to K$ ist stetig. Ferner existieren überall die partiellen Ableitungen und bilden ebenfalls $K-$analytische Funktionen, d.h. die Abbildungen $\frac{\partial f}{\partial x_j} : U \to K$ sind wieder $K-$analytisch.*

Proposition 4.18. *Es seien $U \subset K^m$ und $V \subset K^n$ offene Mengen. Ferner seien $f : U \to V$ und $g : V \to K^r$ beide $K-$analytisch, dann ist auch die Komposition $g \circ f : U \to K^r$ eine $K-$analytische Funktion.*

Wie in der "gewöhnlichen" Analysis definieren wir nun:

Definition 4.19. Es sei $U \subset K^m$ offen. Für eine $K-$analytische Funktion $f = (f_1, f_2, ..., f_n) : U \to K^n$ und einen Punkt $a \in U$ definieren wir die $n \times m-$Matrix

$$Df(a) := \left(\frac{\partial f_i}{\partial x_j}(a) \right)_{1 \le i \le n, 1 \le j \le m}$$

mit Koeffizienten in K. $Df(a)$ heißt *Jacobi-Matrix von f im Punkt a*. In dem Fall, dass $m = n$ gilt, setzen wir

$$Jf(a) := \mathrm{Det}(Df(a))$$

und nennen $Jf(a) \in K$ die *Jacobische von f im Punkt a*.

Daraus ergibt sie analog zur Situation über $\mathbb{R}$ die folgende, wohlbekannte Aussage:

Proposition 4.20. *Es seien $V \subset K^m$ und $W \subset K^n$ offene Mengen. Ferner seien $f : V \to W$ und $g : W \to K^r$ beide $K-$analytische Funktionen, dann ist $g \circ f : V \to K^r$ nach Proposition 4.18 wieder $K-$analytisch und es gilt*

$$D(g \circ f)(a) = Dg(f(a))Df(a) \ .$$

Definition 4.21.

(i) Wir nennen eine formale Potenzreihe

$$f = \sum_{i \in \mathbb{N}_0^m} c_i X^i$$

aus $K[[X]] = K[[X_1, X_2, ..., X_m]]$ nach Igusa eine *SRP* ("special restricted power series"), falls für alle $i \in \mathbb{N}_0^m$ die Beziehungen $c_i \in \mathcal{O}_K$, $c_0 = 0$ und $c_i \equiv 0 \mod \mathfrak{p}_K^{|i|-1}$ für $|i| \geq 1$ gelten.

(ii) Eine SRP wie in (i) ist nach Beispiel 4.16 (ii) auf ganz $\mathcal{O}_K^m$ stark konvergent und induziert eine $K-$analytische Funktion $f : \mathcal{O}_K^m \to \mathcal{O}_K$. Diese bezeichnen wir ebenfalls als SRP (es wird aus dem Zusammenhang immer klar sein, ob wir die formale Potenzreihe oder die Funktion meinen).

(iii) Ferner wollen wir eine Funktion $g = (g_1, g_2, ..., g_m) : \mathcal{O}_K^m \to \mathcal{O}_K^m$, bei der jede Komponente eine SRP ist, eine *SAF* ("Spezielle $K-$analytische Funktion") nennen.

Bemerkung 4.22. Ist $f : \mathcal{O}_K^m \to \mathcal{O}_K$ die SRP, die von der SRP

$$\sum_{i \in \mathbb{N}_0^m} c_i X^i$$

aus $\mathcal{O}_K[[X]] = \mathcal{O}_K[[X_1, X_2, ..., X_m]]$ induziert wird, so haben wir für jedes x aus $\mathcal{O}_K^m$ offenbar

$$f(x) = \sum_{i \in \mathbb{N}_0^m} c_i x^i \equiv \sum_{|i|=1} c_i x^i \mod \mathfrak{p}_K \ .$$

Daraus folgt sofort

$$\frac{\partial f}{\partial x_j}(a) \equiv \frac{\partial f}{\partial x_j}(0) \mod \mathfrak{p}_K$$

für alle a aus $\mathcal{O}_K^m$ und $j = 1, 2, 3, ..., m$. Insbesondere folgt also für jede SAF

$$g : \mathcal{O}_K^m \to \mathcal{O}_K^m$$

die Beziehung $Jg(x) \equiv Jg(0) \mod \mathfrak{p}_K$ für alle x aus $\mathcal{O}_K^m$.

Entscheidend für den am Ende dieses Unterabschnittes aufgeführten "Struktursatz" über $K-$analytische Funktionen ist der folgende Satz:

Satz 4.23. *Es sei $g = (g_1, g_2, ..., g_m) : \mathcal{O}_K^m \to \mathcal{O}_K^m$ eine SAF. Gilt*

$$Jg(0) \not\equiv 0 \mod \mathfrak{p}_K \ ,$$

so ist g bijektiv und besitzt als Inverse ebenfalls eine SAF $f : \mathcal{O}_K^m \to \mathcal{O}_K^m$ mit

$$Jf(0) \not\equiv 0 \mod \mathfrak{p}_K \ .$$

Beweis. Im Korollar 2.2.1 (ii) des Buches [5] von Igusa wird gezeigt:

Es seien $s_1, s_2, ..., s_m$ allesamt SRP's aus $\mathcal{O}_K[[X]]$ mit $X = (X_1, X_2, ..., X_m)$. Wir bilden $s = (s_1, s_2, ..., s_m)$. Gilt

$$Js(0) := \operatorname{Det}\left(\left(\frac{\partial s_i}{\partial X_j}(0)\right)_{i,j}\right) \not\equiv 0 \mod \mathfrak{p}_K \ ,$$

so gibt es genau ein $m-$Tupel $r = (r_1, r_2, ..., r_m)$ von SRPs aus $\mathcal{O}_K[[X]]$ mit $Jr(0) \not\equiv 0$ mod $\mathfrak{p}_K$ und

$$s(r(X)) = X \ .$$

Sind s' und r' die von s und r induzierten SAF's $\mathcal{O}_K^m \to \mathcal{O}_K^m$, so sind diese auf Grund des obigen Korollars von Igusa notwendig bijektiv und invers zueinander. Denn auf Grund von $s'(r'(x)) = x$ für alle x aus $\mathcal{O}_K^m$ folgt notwendig, dass s' surjektiv und r' injektiv ist. Da aber r ebenfalls die Voraussetzungen des Korollars von Igusa erfüllt, ist r' auch surjektiv, ist also bijektiv. Damit ist auch s' bijektiv und besitzt als Inverses r'.

Da unsere vorgegebene SAF offenbar von einem Tupel s wie oben induziert wird, folgt die Behauptung des Satzes. □

Korollar 4.24. *Ist $f = (f_1, f_2, ..., f_m) : \mathcal{O}_K^m \to \mathcal{O}_K^m$ eine SAF und gilt*

$$Jf(0) \not\equiv 0 \mod \mathfrak{p}_K \ ,$$

so ist das Bild der offenen Menge $U := a + \pi^l \mathcal{O}_K^m$ unter f gegeben durch $f(a) + \pi^l \mathcal{O}_K^m$.

Beweis. (Dieses Ergebnis findet sich mit einem ähnlichen Beweis im Buch von Igusa wieder (siehe [5], Beweis zu Lemma 7.4.3 (ii)) Wir brauchen nur

$$f(a + \pi^l \mathcal{O}_K^m) \subset f(a) + \pi^l \mathcal{O}_K^m$$

zu zeigen, denn die nach Satz 4.23 existierende zu f inverse Funktion g ist ebenfalls eine SAF mit den im Satz gewünschten Eigenschaften und es folgt

$$g(f(a) + \pi^l \mathcal{O}_K^m) \subset a + \pi^l \mathcal{O}_K^m \qquad \text{was zu} \qquad f(a) + \pi^l \mathcal{O}_K^m \subset f(a + \pi^l \mathcal{O}_K^m)$$

äquivalent ist.

Sei nun $a + \pi^l b = (a_1 + \pi^l b_1, ..., a_m + \pi^l b_m) \in a + \pi^l \mathcal{O}_K^m$ gegeben. Wir zeigen $f(a+\pi^l b) \in f(a) + \pi^l \mathcal{O}_K^m$. Nach Voraussetzung besitzt f für alle x aus $\mathcal{O}_K^m$ und alle $j = 1, 2, 3, ..., m$ eine Darstellung

$$f_j(x) = \sum_{i \in \mathbb{N}_0^m} c_{i,j} x^i$$

mit $c_{i,j} \in \mathcal{O}_K$. Für jedes $i \in \mathbb{N}_0^m$ folgt damit

$$c_{i,j}(a+\pi^l b)^i = c_{i,j} \prod_{l=1}^{m} (a_l + \pi^l b_l)^{i_l} \equiv c_{i,j} \prod_{l=1}^{m} a_l^{i_l} = c_{i,j} a^i \mod \mathfrak{p}_K^l .$$

D.h. es gilt

$$\left| f_j(a+\pi^l b) - f_j(a) \right|_K \leq \sup\{ \left| c_{i,j}(a+\pi^l b)^i - c_{i,j} a^i \right|_K : i \in \mathbb{N}_0^m \} \leq q^{-l}$$

für alle $j = 1, 2, 3, ..., m$ und das war zu zeigen. □

Korollar 4.25. *Es sei μ ein Haar-Maß auf K^m, dann ist jede SAF $\phi : \mathcal{O}_K^m \to \mathcal{O}_K^m$ mit $J\phi(0) \not\equiv 0 \mod \mathfrak{p}_K$ maßerhaltend, d.h. für jede Borel-Menge $B \subset \mathcal{O}_K^m$ gilt $\mu(B) = \mu(\phi(B))$.*

Beweis. Wegen Korollar 4.24 und der Translationsinvarianz von μ gilt für eine Menge $A = a + \pi^l \mathcal{O}_K^m \in \mathcal{O}_K^m$

$$\mu(A) = \mu(a + \pi^l \mathcal{O}_K) = \mu(\pi^l \mathcal{O}_K) = \mu(\phi(a) + \pi^l \mathcal{O}_K^m) = \mu(\phi(A)) .$$

Da offenbar jede kompakt-offene Menge $C \in \mathcal{T}(K^m)$ eine endliche disjunkte Vereinigung solcher Mengen A ist, folgt daher für alle Elemente $C \in \mathcal{T}(K^m)$ mit $C \subset \mathcal{O}_K^m$ die Gleichheit $\mu(C) = \mu(\phi(C))$.

Es sei nun $C \subset K^m$ kompakt, also nicht notwendig kompakt-offen. Auf Grund der Regularität von μ (Satz 4.8 (ii)) finden wir eine Folge $(U_i)_{i \in \mathbb{N}}$ von offenen Obermengen von C mit $\lim_{i\to\infty} \mu(U_i) = \mu(C)$. Da C kompakt ist, können wir es mit endlich vielen kompakt-offenen Mengen innerhalb jeder Menge U_i überdecken. Wir können also für jedes U_i ein C_i aus $\mathcal{T}(K^m)$ mit $C \subset C_i \subset U_i$ wählen. Also folgt

$$\mu(C) = \lim_{i\to\infty} \mu(C_i) = \lim_{i\to\infty} \mu(\phi(C_i)) \geq \mu(\phi(C)) .$$

Indem wir C durch $\phi(C)$ ersetzen und ϕ durch die SAF ϕ^{-1} (ϕ^{-1} erfüllt ebenfalls die Voraussetzung des Satzes), erhalten wir die fehlende Ungleichung zur Gleicheit. Wir haben also für kompakte Mengen $C \subset \mathcal{O}_K^m$ die Gleicheit $\mu(C) = \mu(\phi(C))$.

Es sei schließlich $B \in \mathcal{B}(K^m)$ beliebig. Wegen der Regularität von μ gibt es eine Folge $(C_i)_{i \in \mathbb{N}}$ kompakter Teilmengen von B mit $\lim_{i\to\infty} \mu(C_i) = \mu(B)$. Es folgt

$$\mu(B) = \lim_{i\to\infty} \mu(C_i) = \lim_{i\to\infty} \mu(\phi(C_i)) \leq \mu(\phi(B)) .$$

Tauschen wir B durch $\phi(B)$ aus und verwenden wieder die SAF ϕ^{-1} anstatt ϕ so erhalten wir die umgekehrte Ungleichung. Damit ist das Korollar bewiesen. □

Nun folgt das Hauptergebnis dieses Abschnittes:

Satz 4.26. *Es sei $U \subset K^m$ offen und $f = (f_1, f_2, ..., f_m) : U \to K^m$ eine $K-$analytische Funktion, für die in einem Punkt $a \in U$ die Beziehungen*

$$f(a) = 0 \quad \text{und} \quad Jf(a) \neq 0$$

erfüllt seien. Wir setzen $A := Df(a)^{-1}$. Dann gibt es ein $l \in \mathbb{N}$ mit $a + \pi^l A\mathcal{O}_K^m \subset U$ und eine SAF $g : \mathcal{O}_K^m \to \mathcal{O}_K^m$ mit $Jg(0) \not\equiv 0 \mod \mathfrak{p}_K$, so dass wir das folgende kommutative Diagramm $K-$analytischer Funktionen erhalten:

$$\begin{array}{ccc} a + \pi^l A\mathcal{O}_K^m & \xrightarrow{f} & \pi^l \mathcal{O}_K^m \\ {\scriptstyle a+\pi^l A\cdot}\uparrow & & \uparrow{\scriptstyle \cdot\pi^l} \\ \mathcal{O}_K^m & \xrightarrow[g]{} & \mathcal{O}_K^m \end{array}$$

Beweis. (Der folgende Beweis ist im Wesentlichen in dem Beweis von Satz 7.4.1 im Buch [5] von Igusa zu finden) Nach Voraussetzung existiert eine offene Umgebung $V \subset U$ von a, so dass sich jede Komponente f_j von f für alle $x \in V$ als stark konvergente Reihe

$$f_j(x) = \sum_{i \in \mathbb{N}_0^m} c_{i,j}(x-a)^i$$

mit Konstanten $c_{i,j}$ aus K und $c_{0,j} = 0$ darstellen lässt. Es gilt offenbar

$$f(x) = Df(a)(x-a) + \left(\sum_{|i| \geq 2} c_{i,j}(x-a)^i \right)_{j=1}^m .$$

Es sei $A := Df(a)^{-1}$. Dann haben wir für alle x aus K^m mit $Ax + a \in V$

$$\begin{aligned} f(Ax+a) &= x + \left(\sum_{|i| \geq 2} c_{i,j}(Ax)^i \right)_{j=1}^m \\ &= x + \left(\sum_{|i| \geq 2} c'_{i,j} x^i \right)_{j=1}^m \end{aligned}$$

mit Konstanten $c'_{i,j} \in K$. Für alle $j = 1, 2, ..., m$ und jedes $x \in K^m$ mit $Ax + a \in V$ gilt $c'_{i,j} x^i \to 0$ für $|i| \to \infty$. Also gibt es ein $l_0 \in \mathbb{N}$ mit $c'_{i,j}\pi^{l_0|i|} \to 0$ für $|i| \to \infty$. Demnach kann es nur endlich viele Paare (i, j) mit $\left|c'_{i,j}\pi^{l_0|i|}\right|_K > 1$ geben. D.h. es gibt ein $l_1 \in \mathbb{N}$, so dass für alle i, j die Konstante

$$c''_{i,j} := \pi^{l_1} c'_{i,j} \pi^{l_0|i|}$$

einen Betrag kleiner oder gleich eins hat und damit $c''_{i,j} \in \mathcal{O}_K$ gilt. Wir wählen ein $l \in \mathbb{N}$ mit $l \geq 2l_0 + l_1 + 1$ und so dass für alle $x \in \mathcal{O}_K$ die Beziehung $A\pi^l x + a \in V$ gilt. Ferner setzen wir für alle $x \in \mathcal{O}_K^m$ und $j = 1, 2, 3, ..., m$

$$g_j(x) := \pi^{-l} f_j(A\pi^l x + a) = x_j + \sum_{|i| \geq 2} c'''_{i,j} x^i$$

mit

$$c'''_{i,j} = \pi^{l(|i|-1)} c'_{i,j} = \pi^{(l-1)(|i|-1)-l_1-l_0|i|} \cdot (\pi^{|i|-1} c''_{i,j}) \ .$$

Es gilt

$$\begin{array}{rcl} (l-1)(|i|-1) - l_1 - l_0|i| & \geq & (2l_0 + l_1)(|i|-1) - l_1 - l_0|i| \\ & = & l_0|i| - 2l_0 + l_1|i| - 2l_1 \geq 0 \end{array}$$

für $|i| \geq 2$. Demnach gilt $c'''_{i,j} \in \mathcal{O}_K$ und $\pi^{|i|-1} | c'''_{i,j}$ für alle i aus $\mathbb{N}_0^m$ mit $|i| \geq 2$ und $j = 1, 2, 3, ..., m$. Insgesamt also ist $g = (g_1, g_2, ..., g_m)$ eine SAF mit $Jg(0) \equiv 1 \not\equiv 0 \mod \mathfrak{p}_K$. Mit der Matrix A, dem konstruierten g und der Konstanten l ist offensichtlich die Aussage des Satzes erfüllt. $\square$

4.3 Der Beweis der Transformationsformel

Mit Hilfe unserer Vorbereitungen in den beiden letzten Unterabschnitten werden wir nun die Transformationsformel für lokale Körper zügig erhalten. Es sei noch einmal erwähnt, dass wir mit $\mathcal{T}(X)$ die lokal-kompakten Mengen und mit $\mathcal{B}(X)$ die Borel-Mengen eines topologischen Raumes X bezeichnen. Schließlich bezeichen wir für ein Maß μ auf einer Menge X mit $\mathcal{M}(\mu, X)$ die $\mu-$messbaren Funktionen auf X.

Lemma 4.27. *Es sei m aus $\mathbb{N}$ und μ ein Haar-Maß auf K^m mit $\mu(\mathcal{O}_K^m) = 1$, dann gilt für beliebige Konstanten $a_1, a_2, .., a_m \in K$ und $k_1, k_2, ..., k_m \in \mathbb{N}_0$ die Beziehung*

$$\mu\left(\prod_{i=1}^{m}(a_i + \pi^{k_i}\mathcal{O}_K^m)\right) = \prod_{i=1}^{m} q^{-k_i} \ .$$

Beweis. Wegen der Translationsinvarianz von μ gilt

$$\begin{aligned} \mu\left(\prod_{i=1}^{m}(a_i + \pi^{k_i}\mathcal{O}_K)\right) &= \mu\left((a_1, a_2, ..., a_m) + \prod_{i=1}^{m}(\pi^{k_i}\mathcal{O}_K)\right) \\ &= \mu\left(\prod_{i=1}^{m}(\pi^{k_i}\mathcal{O}_K)\right) \ . \end{aligned}$$

Für $i = 1, 2, .., m$ sei $R_i \subset \mathcal{O}_K$ ein vollständiges Vertretersystem der Gruppe $\mathcal{O}_K/\pi^{k_i}\mathcal{O}_K$. Offenbar hat R_i genau q^{k_i} Elemente. Wir haben die disjunkte Zerlegung

$$\mathcal{O}_K^m = \bigcup_{(\alpha_1,\alpha_2,..,\alpha_m)\in\prod_{i=1}^{m} R_i} \left((\alpha_1, \alpha_2, .., \alpha_m) + \prod_{i=1}^{m}(\pi^{k_i}\mathcal{O}_K)\right) \ .$$

Daraus erhalten wir

$$1 = \mu\left(\mathcal{O}_K^m\right) = \left(\prod_{i=1}^{m}\#R_i\right)\mu\left(\prod_{i=1}^{m}(\pi^{k_i}\mathcal{O}_K)\right) = \left(\prod_{i=1}^{m}q^{k_i}\right)\mu\left(\prod_{i=1}^{m}(\pi^{k_i}\mathcal{O}_K)\right) \ .$$

Daraus folgt die Behauptung. □

Lemma 4.28. *Es sei μ ein Haar-Maß auf K^m und es sei $\phi : K^m \to K^m$ ein Homöomorphismus und gleichzeitig ein Gruppenhomomorphismus der additiven Gruppe von K^m. Dann ist für jede Borel-Menge $B \subset K^m$ auch $\phi(B)$ eine Borel-Menge von K^m und die Zuordnung*

$$B \mapsto \mu(\phi(B))$$

für $B \in \mathcal{B}(K^m)$ definiert ein Haar-Maß auf K^m.

Beweis. Dies ist offensichtlich. □

Beachten wir, dass für jede Matrix $A \in \mathrm{GL}(m, K)$ durch

$$A : K^m \to K^m \ , \ x \mapsto Ax$$

sowohl ein Homöomorphismus als auch ein Gruppenisomorphismus der additiven Gruppe von K gegeben ist, so erhalten wir:

Lemma 4.29. *Es sei $m \in \mathbb{N}$ und $A \in GL(m, K)$. Ferner wählen wir ein Haar-Maß μ auf K^m. Dann ist nach dem vorhergehenden Lemma $\mu \circ A$ wieder ein Haar-Maß auf K^m. Ist $X \in \mathcal{B}(K^m)$, so haben wir*

$$\mu(AX) = |Det(A)|_K \, \mu(X) \ .$$

Beweis. Es sei $c := |\mathrm{Det}(A)|_K > 0$. Wir haben die folgende Identität von Haar-Maßen zu beweisen:

$$\mu \circ A = c\mu \ .$$

Da sich zwei Haar-Maße nur um einen positiven Faktor unterscheiden, haben wir die zu beweisende Identität nur für die kompakt-offene Menge $X := \mathcal{O}_K^m$ nachzuprüfen, denn für diese hat jedes Haar-Maß positives und endliches Maß. Ferner können wir O.B.d.A. $\mu(\mathcal{O}_K^m) = 1$ annehmen, denn gilt die zu beweisende Relation für irgendein festes Haar-Maß μ, so auch für alle $c\mu$ mit $c > 0$ und damit für alle Haar-Maße.

Fall 1. Es sei $A \in \mathrm{GL}(m, \mathcal{O}_K)$ eine unimodulare Matrix. Dann gilt wegen $A\mathcal{O}_K^m = \mathcal{O}_K^m$

$$\mu(AX) = \mu(A\mathcal{O}_K^m) = \mu(\mathcal{O}_K^m) = \mu(X) = |\mathrm{Det}(A)|_K \, \mu(X) \ ,$$

denn in unserem Fall gilt $|\mathrm{Det}(A)|_K = 1$. Also ist die Behauptung des Lemmas für unimodulare Matrizen A richtig.

Fall 2. Es sei nun $A \in \mathrm{Mat}(m, \mathcal{O}_K)$. $\mathcal{O}_K$ ist ein Hauptidealring, also ist der Elementarteilersatz anwendbar. Wir finden also Matrizen $\sigma, \tau \in \mathrm{GL}(m, \mathcal{O}_K)$ und eine Diagonalmatrix $D \in \mathrm{Mat}(m, \mathcal{O}_K)$ mit

$$A = \sigma D \tau \ .$$

Daher erhalten wir mit Hilfe von Fall 1

$$\mu(AX) = \mu(\sigma^{-1}AX) = \mu(D\tau\mathcal{O}_K^m) = \mu(D\mathcal{O}_K^m) \ .$$

Gilt

$$D = \mathrm{Diag}(\delta_1, .., \delta_m)$$

und schreiben wir $\delta_i = \pi^{k_i}\epsilon_i$ mit $k_i \in \mathbb{N}_0$ und $\epsilon_i \in \mathcal{O}_K^*$ für alle i, so folgt

$$\begin{aligned} D\mathcal{O}_K^m &= \delta_1\mathcal{O}_K \times ... \times \delta_m\mathcal{O}_K \\ &= \pi^{k_1}\mathcal{O}_K \times ... \times \pi^{k_m}\mathcal{O}_K \ . \end{aligned}$$

D.h. wir haben mit Hilfe von Lemma 4.27

$$\mu(D\mathcal{O}_K^m) = \mu\left(\prod_{i=1}^{m}(\pi^{k_i}\mathcal{O}_K)\right) = \prod_{i=1}^{m} q^{-k_i} = \prod_{i=1}^{m} |\delta_i|_K = |\mathrm{Det}(A)|_K \, \mu(X) \; .$$

Fall 3. Es sei nun A aus $\mathrm{GL}(m, K)$ beliebig gewählt. Zu A finden wir ein l aus $\mathbb{N}$ mit $\pi^l A \in \mathrm{Mat}(m, \mathcal{O}_K^m)$. Damit gilt mit Hilfe von Fall 2 :

$$\begin{aligned}
\mu(AX) &= \mu((\pi^l A)(\pi^{-l}X)) \\
&= \left|\mathrm{Det}(\pi^l A)\right|_K \mu(\pi^{-l}X) \\
&= |\mathrm{Det}(A)|_K \left|\mathrm{Det}(\pi^l I_m)\right|_K \mu(\pi^{-l}X) \\
&= |\mathrm{Det}(A)|_K \, \mu((\pi^l I_m)\pi^{-l}X) = |\mathrm{Det}(A)|_K \, \mu(X) \; .
\end{aligned}$$

Damit ist das Lemma bewiesen. □

Lemma 4.30. *Es sei μ ein Haar-Maß auf K^m. Ferner sei $U \subset K^m$ offen und $\phi : U \to K^m$ eine $K-$analytische Funktion, für die $J\phi(x) \neq 0$ für alle $x \in U$ gelte. Dann besitzt jeder Punkt $a \in U$ eine Umgebung $U_a \subset U$, so dass $|J\phi(x)|_K = |J\phi(a)|_K$ für alle x aus U_a gilt und so dass für jedes B aus $\mathcal{B}(K^m)$ mit $B \subset U_a$ die Beziehung*

$$\mu(\phi(B)) = |J\phi(a)|_K \, \mu(B) = \int_B |J\phi(x)|_K \, d\mu(x)$$

gilt.

Beweis. Es sei $a \in U$. Wir setzen $f := \phi - \phi(a)$. Wegen $f(a) = 0$ und $Jf(a) = J\phi(a) \neq 0$ ist für f die Voraussetzung des Satzes 4.26 erfüllt. Setzen wir $D := Df(a)$, so liefert uns der Satz eine offene Umgebung $U_a := a + \pi^l D^{-1}\mathcal{O}_K^m \subset U$ von a und eine SAF $g : \mathcal{O}_K^m \to \mathcal{O}_K^m$ mit $Jg(x) \not\equiv 0 \mod \mathfrak{p}_K$, d.h. mit $|Jg(x)|_K = 1$ für alle $x \in \mathcal{O}_K^m$, so dass für jedes $x \in U_a$

$$f(x) = \pi^l g(\pi^{-l}(Dx - a))$$

gilt. Daraus folgt offenbar sofort die Aussage über die Konstanz von $|J\phi|_K$ eingeschränkt auf U_a (man wende auf die obige Zerlegung von f einfach für die Produktformel für die Jacobi-Matrix an (Proposition 4.20)). Es sei $B \in \mathcal{B}(K^m)$ mit $B \subset U_a$ gewählt. Beachten wir, dass μ translationsinvariant ist, dass g maßerhaltend ist und verwenden wir Lemma 4.29, so folgt die Behauptung:

$$\begin{aligned}
\mu(\phi(B)) = \mu(f(B)) &= q^{-ml}\mu(g(\pi^{-l}(DB - a))) \\
&= q^{-ml}\mu(\pi^{-l}(DB - a)) \\
&= \mu(DB - a) = |J\phi(a)|_K \, \mu(B) \; .
\end{aligned}$$

□

Satz 4.31. *(Transformationsformel für lokale Körper) Es seien μ,ϕ und U wie in Lemma 4.30. ϕ sei zusätzlich injektiv. Eine $\mu-$messbare Funktion f auf K^m ist genau dann integrierbar, falls $f \circ \phi \cdot |J\phi|_K$ integrierbar ist und in diesem Fall gilt*

$$\int_{\phi(U)} f(x) d\mu(x) = \int_U f \circ \phi(x) \, |J\phi(x)|_K \, d\mu(x) \, .$$

Beweis. Der Beweis verläuft in mehreren Schritten:

Schritt 1: Wir zeigen, dass für alle $B \in \mathcal{B}(K^m)$ mit $B \subset U$ die Formel

$$\mu(\phi(B)) = \int_B |J\phi(x)|_K \, d\mu(x)$$

gilt. Dazu geben wir uns zunächst ein $C \in \mathcal{T}(K^m)$ mit $C \subset U$ vor und beweisen die Formel für alle Borel-Mengen B mit $B \subset C$. D.h. wir zeigen die Formel zuerst für alle beschränkten Borel-Mengen $B \subset U$.

Wegen Lemma 4.30 gibt es zu jedem $a \in C$ eine Umgebung $U_a \subset C$, so dass die Formel für alle Borel-Mengen $B \subset U_a$ gilt. Da C insbesondere kompakt ist, gibt es endlich viele Mengen $U_1, U_2, ..., U_r$ unter den Mengen U_a, die C überdecken.

Wir wählen nun eine beliebige Borel-Menge $B \subset C$ und setzen $B_i := \cup_{l=1}^{i} (U_l \cap B)$ für $i = 1, 2, ..., r$. Dann gilt $B_r = B$. Wir zeigen per Induktion über i, dass die Formel für alle B_i gilt :

Fall $i = 1$. Hier gilt die Formel nach Voraussetzung (Lemma 4.30).

Fall $i > 1$. Die Formel gelte für B_{i-1}. Nach Voraussetzung gilt sie ebenfalls für $G := U_i \cap B$. Es folgt:

$$\begin{aligned} \mu(\phi(B_i)) &= \mu(\phi(B_{i-1})) + \mu(\phi(G)) - \mu(\phi(B_{i-1} \cap G)) \\ &= \int_{B_{i-1} \cup G - (B_{i-1} \cap G)} |J\phi(x)|_K \, d\mu(x) = \int_{B_i} |J\phi(x)|_K \, d\mu(x) \, . \end{aligned}$$

Sei nun $B \subset U$ eine beliebige Borel-Menge. Für jedes $i \in \mathbb{N}$ setzen wir $B_i := B \cap \pi^{-i} \mathcal{O}_K^m$, dann haben wir eine aufsteigende Folge beschränkter Borel-Mengen $(B_i)_{i \in \mathbb{N}}$ mit $\cup_{i=1}^{\infty} B_i = B$ und es folgt die Behauptung z.B. mit dem Satz von B.Levi:

$$\mu(\phi(B)) = \lim_{i \to \infty} \mu(\phi(B_i)) = \lim_{i \to \infty} \int_{B_i} |J\phi(x)|_K \, d\mu(x) = \int_B |J\phi(x)|_K \, d\mu(x) \, .$$

Schritt 2. Die in Schritt 1 gewonnene Formel lässt sich für jede Borel-Menge $B \subset U$ auch schreiben als

$$\int_{\phi(U)} \chi_{\phi(B)}(x) d\mu(x) = \int_U \chi_{\phi(B)} \circ \phi(x) \, |J\phi(x)|_K \, d\mu(x) \, . \tag{4.2}$$

Durch Linearkombination erhalten wir damit die Behauptung unseres Satzes für Treppenfunktionen

$$f = \sum_{i=1}^{r} a_i \chi_{B_i}$$

mit reellen Zahlen $a_1, a_2, ..., a_r \geq 0$ und $B_i \in \mathcal{B}(K^m)$ für alle i.

Sei nun $f \in \mathcal{M}(\mu, K^m)$ eine messbare Funktion mit $f \geq 0$. Zu f finden wir eine monoton wachsende Folge $(f_n)_{n\in\mathbb{N}}$ von nicht negativen Treppenfunktionen, die punktweise gegen f konvergieren (siehe Satz 4.4 (i)). Dann ist offenbar $(f_n \circ \phi \cdot |J\phi|_K)_{n\in\mathbb{N}}$ eine monotone Folge nicht negativer Funktionen aus $\mathcal{M}(\mu, K^m)$, die punktweise gegen $f \circ \phi \cdot |J\phi|_K$ konvergiert und es gilt mit Hilfe des Satzes von B.Levi :

$$\begin{aligned}
\int_{\phi(U)} f(x)d\mu(x) &= \lim_{i\to\infty} \int_{\phi(U)} f_n(x)d\mu(x) \\
&= \lim_{i\to\infty} \int_U f_n \circ \phi(x) \left|J\phi(x)\right|_K d\mu(x) \\
&= \int_U f \circ \phi(x) \left|J\phi(x)\right|_K d\mu(x) \ .
\end{aligned}$$

Auf Grund der Definition des Lebesgue-Integrals und der $\mu-$Integrierbarkeit folgt offenbar hieraus schon die Aussage des Satzes für beliebige Funktionen f aus $\mathcal{M}(\mu, K^m)$. Damit ist der Beweis abgeschlossen. $\square$

5 Das Maß $T(\beta_M)$ und seine Dichte h bezüglich α

Es sei K ein lokaler Körper mit seinen Daten $\mathcal{O}_K, \mathfrak{p}_K,\ F_K = \mathcal{O}_K/\mathfrak{p}_K$ und $|\cdot|_K$. Ferner sei π eine Uniformisierende von K und es gelte $\#F_K = q$.

Für Matrizen $A, B \in \mathrm{Mat}(m, n, \mathcal{O}_K)$ und eine Konstante $a \in \mathcal{O}_K$ vereinbaren wir weiter

$$A \equiv B \mod a$$

genau dann, falls $A - B \in a \cdot \mathrm{Mat}(m, n, \mathcal{O}_K)$ gilt. Außerdem sei $A \mod a$ die Restklasse von A in $\mathrm{Mat}(m, n, \mathcal{O}_K/a\mathcal{O}_K)$. Speziell setzen wir $\overline{A} := A \mod \pi$. Zudem vereinbaren wir für ein beliebiges n aus $\mathbb{N}$ die folgende Notation:

$$\begin{array}{lcl} M_n & = & \mathrm{Mat}(n, \mathcal{O}_K)\ , \\ \alpha^n & = & \text{das Haar-Maß auf } K^n \text{ mit } \alpha^n(\mathcal{O}_K^n) = 1\ , \\ \beta^n & = & \text{das Haar-Maß auf } \mathrm{Mat}(n, K) \text{ mit } \beta^n(M_n) = 1\ , \\ \beta_U^n & = & \text{die Einschränkung von } \beta^n \text{ auf eine messbare} \\ & & \text{Teilmenge } U \subset \mathrm{Mat}(n, K)\ , \\ f(\lambda) & = & \text{Das Bild des Maßes } \lambda \text{ unter der Abbildung } f\ . \end{array}$$

Da uns der Fall $n = 2$ besonders interessiert, setzen wir zur Vereinfachung der Notation

$$M = M_2\ ,\ \alpha = \alpha^2\ ,\ \beta = \beta^2 \text{ und } \beta_U = \beta_U^2\ .$$

Schließlich definieren wir die *Spur-Norm-Abbildung* als die Abbildung

$$T : \mathrm{Mat}(2, K) \to K^2\ ,\ A \mapsto (\mathrm{Spur}(A), \mathrm{Det}(A))\ ,$$

Ziel des Abschnittes und auch dieser Arbeit ist es, eine stetige Funktion $h : K^2 \to \mathbb{R}$ mit

$$T(\beta_M) = h\alpha\ , \tag{5.3}$$

d.h. mit

$$T(\beta_M)(B) = \beta(T^{-1}(B) \cap M) = \int_B h(x) d\alpha(x)$$

für alle $B \in \mathcal{B}(K^2)$ explizit zu bestimmen, insbesondere also die Existenz einer solchen zu beweisen und danach einige Konsequenzen aus dem Ergebnis zu ziehen.

5.1 Die Verallgemeinerung der Situation

Ein Großteil der Betrachtungen, die wir anstellen können, um ein h wie in Gleichung 5.3 zu bestimmen, sind auch unabhängig vom speziellen Fall $n = 2$ durchführbar, wenn wir die folgende Verallgemeinerung der Spur-Norm-Abbildung hinzunehmen:

Wir wählen eine Unbestimmte X über K und definieren die Abbildung

$$T_n : \mathrm{Mat}(n, K) \to K^n\ ,\ A \mapsto (a_1, a_2, ..., a_n)\ ,$$

wobei

$$(-X)^n + a_1(-X)^{n-1} + ... + a_{n-2}(-X)^2 + a_{n-1}(-X) + a_n = \mathrm{Det}(A - I_nX)$$

das charakteristische Polynom von A ist. Auf Grund der Identität

$$\mathrm{Det}\,(A - XI_2) \quad = \quad (-X)^2 + \mathrm{Spur}(A)(-X) + \mathrm{Det}(A)$$

für beliebige Matrizen $A \in \mathrm{Mat}(2, K)$ gilt also insbesondere $T = T_2$.

5.1.1 Die Maße $\mu_U^n = T_n(\beta_U^n)$ und ihre Dichten $h_{n,U}$ bezüglich α^n

Die verallgemeinerte Spur-Norm-Abbildung T_n gibt uns die Möglichkeit, eine Verallgemeinerung des Maßes μ und der Dichte h anzugeben. Bevor wir dazu kommen, brauchen wir das folgende Lemma:

Lemma 5.1. *Ein Maß $\eta : \mathcal{B}(K^n) \to [0, \infty]$ werde durch zwei stetige Dichten $f_1, f_2 : K^n \to \mathbb{R}$ bezüglich α^n dargestellt, d.h. es gelte $\eta = f_1\alpha^n = f_2\alpha^n$, dann gilt $f_1 = f_2$.*

Beweis. Nehmen wir an, wir hätten $\eta = f_i\alpha^n$ für zwei stetige Funktionen $f_1, f_2 : K^n \to \mathbb{R}$ mit $f_1 \neq f_2$. Daraus wollen wir einen Widerspruch ableiten, so dass die Aussage des Lemmas folgt. O.B.d.A gelte $f_1(x_0) > f_2(x_0)$ für ein $x_0 \in K^n$ (ist dies nicht der Fall, so muss die umgekehrte Ungleichung erfüllbar sein und wir tauschen die Namen der Funktionen). Auf Grund der Tatsache, dass f_1 und f_2 stetig sind, existiert eine offene Menge $V \subset K^n$ und ein $\epsilon > 0$, so dass $f_1(x) - f_2(x) \geq \epsilon$ gilt. Daraus erhalten wir unseren gewünschten Widerspruch:

$$0 = \eta(V) - \eta(V) = \int_V (f_1(x) - f_2(x))d\alpha^n(x) \geq \epsilon\alpha^n(V) > 0\ .$$

□

Definition 5.2. Wir setzen für jede kompakt-offene Menge $U \subset M_n$

$$\mu_U^n := T_n(\beta_U^n)\ ,$$

und, falls existent, sei $h_{n,U}$ die nach Lemma 5.1 eindeutig bestimmte stetige Dichte von μ_U^n bezüglich α^n, d.h. die reellwertige stetige Funktion $h_{n,U}$ mit

$$\mu_U^n(B) = \beta^n(T_n^{-1}(B) \cap U) = \int_B h_{n,U}(x)d\alpha^n(x)$$

für alle $B \in \mathcal{B}(K^n)$. Zur Vereinfachung der Notation setzen wir noch

$$\mu^n := \mu_{M_n}^n \text{ und } h_n := h_{n,M_n}\ .$$

Unabhängig von allen weitern Betrachtungen wollen wir gleich eine Interpretation des Maßes μ^n geben. Dazu definieren wir:

Definition 5.3. Es seien a aus $\mathcal{O}_K^n$ und k aus $\mathbb{N}_0$ gewählt. Dann setzen wir

$$\gamma_{n,k}(a) := \#\left\{A \mod \pi^k : A \in M_n, T_n(A) \equiv a \mod \pi^k\right\} .$$

Wir setzen schließlich noch $\gamma_k := \gamma_{2,k}$.

Für $a = (a_1, a_2, ..., a_n) \in \mathcal{O}_K^2$ gibt die Konstante $\gamma_{n,k}(a)$ also an, wieviele Matrizen in $\mathrm{Mat}\left(n, \mathcal{O}_K/\mathfrak{p}_K^k\right)$ ein charakteristisches Polynom

$$f = (-X)^n + b_1(-X)^{n-1} + ... + b_{n-1}(-X) + b_n \in \mathcal{O}_K/\mathfrak{p}_K^k[X]$$

mit $b_i = a_i \mod \mathfrak{p}_K^k$ für alle $i = 1, 2, 3, ..., n$ haben. Es gibt nun einen einfachen und engen Zusammenhang zwischen den Konstanten $\gamma_{n,k}(a)$ und dem Maß μ_n:

Proposition 5.4. *Für jedes Tupel $a := (a_1, a_2, ..., a_n) \in \mathcal{O}_K^n$ und jedes k aus $\mathbb{N}_0$ gilt*

$$\gamma_{n,k}(a) = \mu^n(a + \pi^k\mathcal{O}_K^n) \cdot q^{n^2k} .$$

Beweis. Nach Definition gilt

$$\mu^n(a + \pi^k\mathcal{O}_K^n) = \beta^n(T_n^{-1}(a + \pi^k\mathcal{O}_K^n) \cap M_n) .$$

Offenbar liegt $A \in \mathrm{Mat}(n, K)$ genau dann in $T_n^{-1}(a + \pi^k\mathcal{O}_K^n) \cap M_n$ falls

$$A \in M_n \text{ und } T_n(A) \in a + \pi^k\mathcal{O}_K^n$$

gilt, d.h. falls

$$A \in M_n \text{ und } T_n(A) \equiv a \mod \pi^k$$

gilt. Ist also $S \subset M_n$ ein vollständiges Vertretersystem der $\mod \pi^k$ verschiedenen Lösungen der Kongruenz

$$T_n((X_{i,j})) \equiv a \mod \pi^k$$

in den Unbestimmten $X_{i,j}$ $(i, j = 1, 2, 3, ..., n)$, so erhalten wir die disjunkte Vereinigung

$$T_n^{-1}(a + \pi^k\mathcal{O}_K^n) \cap M_n = \bigcup_{A \in S} A + \pi^k M_n .$$

Da β^n ein Haar-Maß ist, folgt daraus

$$\mu^n(a + (\pi^k\mathcal{O}_K)^n) = \#S/q^{n^2k} .$$

Wegen $\#S = \gamma_{n,k}(a)$ folgt schließlich die Behauptung. $\square$

5.1.2 Die Eigenschaften der Dichten $h_{n,U}$

In den folgenden Untersuchungen wird es uns in einigen Fällen gelingen, die Dichten $h_{n,U}$ explizit auszurechnen. Uns interessiert auch, wie sich $h_{n,U}$ verändert, wenn wir U linear transformieren. Bei allem, was wir erreichen werden, wird sich die Transformationsformel für lokale Körper als entscheidendes Hilfsmittel herausstellen.

Um die Transformationsformel auch bei der Integration von Funktionen auf offenen Teilmengen von $\mathrm{Mat}(n, K)$ anwenden zu können, um insbesondere den Begriff der Jacobi-Matrix zur Hand zu haben, haben wir die Reihenfolge der Komponenten einer Matrix festzulegen. Es sei dazu $n \in \mathbb{N}$ gewählt. Mit Hilfe der Bijektion

$$\sigma_n : \mathbb{N}_n \times \mathbb{N}_n \to \mathbb{N}_{n^2},\ (i,j) \mapsto i + n(j-1)$$

definieren die Abbildung

$$\tau_n : \mathrm{Mat}(n, K) \to K^{n^2}\ ,\ (a_{i,j}) \mapsto (b_1, b_2, ..., b_{n^2}) \text{ mit } a_{i,j} = b_{\sigma_n(i,j)} \text{ für } i,j \in \mathbb{N}_n\ .$$

D.h. für $n = 2$ haben wir

$$\tau_2 \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) = (a, c, b, d)\ .$$

Gemäß τ_n übertragen wir nun Begriffe wie "$K-$analytisch", "Jacobi-Matrix", "Jacobische", etc. auch auf Funktionen $f : U \to \mathrm{Mat}(n, K)$, wobei $U \subset \mathrm{Mat}(n, K)$ offen ist. Beispielsweise ist die Funktion $f : M \to M$ definiert durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a^2 & bc \\ 1 & 3b \end{pmatrix}$$

nun $K-$analytisch und besitzt im Punkt $x = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \in M$ die gleiche Jacobi-Matrix wie die auf K^4 definierte Funktion

$$(a, c, b, d) \mapsto (a^2, 1, bc, 3b)$$

im Punkt (a_0, c_0, b_0, d_0), nämlich

$$Df(x) = \begin{pmatrix} 2a_0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & b_0 & c_0 & 0 \\ 0 & 0 & 3 & 0 \end{pmatrix}\ .$$

Zunächst wollen wir einige einfache, aber nützliche Eigenschaften unserer Funktion T_n festhalten:

Proposition 5.5. *Für die Abbildung T_n gelten die folgenden Aussagen:*

(i) Für jedes τ aus $GL(n,K)$ und jede nichtleere Teilmenge $S \subset K^n$ gilt

$$\tau^{-1}T_n^{-1}(S)\tau = T_n^{-1}(S) \ .$$

(ii) Sei k aus $\mathbb{N}$ und $S := \prod_{i=1}^n \pi^{ik} S_i \subset K^n$, dann gilt

$$\pi^{-k} \cdot T_n^{-1}(S) = T_n^{-1}\left(\prod_{i=1}^n S_i\right) \ .$$

Beweis. Zu (i): Es gilt

$$A \in \tau^{-1}T_n^{-1}(S)\tau \Leftrightarrow T_n(\tau A \tau^{-1}) \in S \Leftrightarrow T_n(A) \in S \Leftrightarrow A \in T_n^{-1}(S) \ .$$

Zu (ii) : Es gelte $A \in \mathrm{Mat}(n,K)$ und sei X eine Unbestimmte über K. Auf Grund der Relation

$$\mathrm{Det}(\pi^k A - XI_n) = \mathrm{Det}\left(\pi^k\left(A - \frac{X}{\pi^k}I_n\right)\right) = \pi^{nk}\mathrm{Det}\left(A - \frac{X}{\pi^k}I_n\right)$$

ist

$$(-X)^n + a_1(-X)^{n-1} + ... + a_{n-2}(-X)^2 + a_{n-1}(-X) + a_n$$

genau dann das charakteristische Polynom von A, falls

$$(-X)^n + a_1\pi^k(-X)^{n-1} + ... + a_{n-2}\pi^{(n-2)k}(-X)^2 + a_{n-1}\pi^{(n-1)k}(-X) + a_n\pi^{nk}$$

das Charakteristische Polynom von $\pi^k A$ ist. D.h. es gilt

$$T_n(\pi^k A) = (a_1\pi^k, a_2\pi^{2k}, ..., a_n\pi^{nk})$$

genau dann, falls

$$T_n(A) = (a_1, a_2, ..., a_n)$$

gilt.

Sei nun B aus $T_n^{-1}(S)$, d.h. es sei $T_n(B) = (b_1\pi^k, b_2\pi^{2k}, ..., b_n\pi^{nk})$ aus S; dann ist das genau dann der Fall, falls $T_n(B/\pi^k) = (b_1, b_2, ..., b_n) \in \prod_{i=1}^n S_i$ gilt, d.h. falls $B/\pi^k \in T_n^{-1}(\prod_{i=1}^n S_i)$ gilt. Daraus folgt (ii). □

Unser erstes Ziel besteht darin, für Mengen der Form $U = A + \pi^l M_n$ mit bestimmten Matrizen $A \in M_n$ die Funktion $h_{n,U}$ direkt zu bestimmen. Wir werden dazu zunächst einsehen, dass die Abbildungen $h_{n,U}$ invariant bleiben, falls wir U durch ein Konjugat ersetzen.

Lemma 5.6. *Es sei $U \subset M_n$ offen. Ferner wählen wir ein τ aus $GL(n,\mathcal{O}_K)$. Dann existiert $h_{n,U}$ genau dann, falls $h_{n,\tau U\tau^{-1}}$ existiert, und im Falle der Existenz gilt $h_{n,U} = h_{n,\tau U \tau^{-1}}$.*

Beweis. Wir zeigen $\mu_U^n = \mu_{\tau U \tau^{-1}}^n$, dann folgt auf Grund der Eindeutigkeit der Dichten $h_{n,U}$ (siehe Lemma 5.1) die Behauptung.

Es sei $B \in \mathcal{B}(K^n)$ beliebig . Wir bilden die offensichtlich injektive $K-$analytische Funktion

$$\phi : \mathrm{Mat}(n,K) \to \mathrm{Mat}(n,K) \ , \ A \mapsto \tau A \tau^{-1} \ .$$

ϕ erfüllt offenbar für alle $A \in \mathrm{Mat}(n,K)$ die Beziehung

$$|J\phi(A)|_K = 1 \ .$$

Beachten wir, dass nach Proposition 5.5 (i) $\tau T_n^{-1}(B)\tau^{-1} = T_n^{-1}(B)$ gilt, so folgt mit Hilfe der Transformationsformel:

$$\begin{aligned} \mu_{\tau U \tau^{-1}}^n(B) &= \beta^n(T_n^{-1}(B) \cap \tau U \tau^{-1}) \\ &= \beta^n(\phi(T_n^{-1}(B) \cap U)) \\ &= 1 \cdot \beta^n(T_n^{-1}(B) \cap U) \\ &= \mu_U^n(B) \ . \end{aligned}$$

Damit ist das Lemma bewiesen. □

Definition 5.7. Eine Matrix $A \in M_n$ heiße *gutartig*, falls ihre Reduktion $\bar{A} \in \mathrm{Mat}(n, F_K)$ ein Minimalpolynom vom Grad n aus $F_K[X]$ besitzt.

Dazu haben wir das folgende Lemma:

Lemma 5.8. *Es sei σ aus M_n gutartig. Dann finden wir ein τ aus $GL(n, \mathcal{O}_K)$ und Konstanten $b_1, b_2, ..., b_n$ aus $\mathcal{O}_K$, so dass für $\sigma' := \tau\sigma\tau^{-1}$ die Beziehung*

$$\sigma' \equiv \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & b_1 \\ 1 & 0 & 0 & \cdots & 0 & b_2 \\ 0 & 1 & 0 & \cdots & 0 & b_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & b_{n-1} \\ 0 & 0 & 0 & \cdots & 1 & b_n \end{pmatrix} \mod \pi$$

gilt.

Beweis. $\overline{\sigma}$ ist ein F_K-Endomorphismus über F_K^n und macht F_K^n vermöge

$$f \cdot v := f(\overline{\sigma})v$$

zu einem endlich erzeugten $F_K[X]-$Torsions-Modul. D.h. auf Grund der Theorie endlich erzeugter $R-$Moduln über Hauptidealringen haben wir die folgende Isomorphie von $F_K[X]-$Moduln:

$$F_K^n \backsimeq F_K[X]/(q_1) \oplus F_K[X]/(q_2) \oplus ... \oplus F_K[X]/(q_r) \ .$$

Dabei gilt unter Anderem $q_1|q_2|q_3|\dots|q_r$, wobei q_r das Minmalpolynom von $\overline{\sigma}$ ist. Da die obige Isomorphie wegen $F_K \hookrightarrow F_K[x]$ insbesondere auch im Sinne von F_K-Vektorräumen gilt, muss wegen

$$\dim_{F_K} F_K[x]/q_i = \mathrm{Grad}(q_i) \text{ für alle } i, \, \mathrm{Grad}(q_r) = n$$

und

$$n = \sum_{i=1}^{r} \mathrm{Grad}(q_i)$$

die Beziehung $r = 1$ gelten. Demnach ist F_K^n isomorph zu dem zyklischen $F_K[x]-$Modul $F_K[x]/(q_r)$. D.h. es existiert ein $v \in F_K^n$ mit $F_K[X] \cdot v = F_K[\overline{\sigma}]v = F_K^n$. Damit bilden die Elemente

$$v, \overline{\sigma}v, \overline{\sigma}^2 v, ..., \overline{\sigma}^{n-1} v$$

eine Basis des F_K-Vektorraums F_K^n und $\overline{\sigma}$ hat bezüglich dieser Basis gerade die Form wie $\overline{\sigma'}$ in der Behauptung des Lemmas. Sei $\tau \in M_n$ so gewählt, dass $\overline{\tau}$ den Basiswechsel vollzieht, dann ist wegen $\mathrm{Det}(\overline{\tau}) \neq 0 \in F_K$, also wegen $\pi \nmid \mathrm{Det}(\tau)$ die Matrix τ in $\mathrm{GL}(n, \mathcal{O}_K)$ und wir haben $\overline{\tau}^{-1} = \overline{\tau^{-1}}$. Damit gilt für $\sigma' := \tau\sigma\tau^{-1}$ die Behauptung. $\square$

Satz 5.9. *Es sei $A := (a_{i,j}) \in M_n$ gutartig. Ferner setzen wir $U := A + \pi^l M_n$ für ein l aus $\mathbb{N}$. Dann existiert $h_{n,U}$. Genauer haben wir $T_n(U) = T_n(A) + \pi^l \mathcal{O}_K^2$ und es gilt für jedes $x \in K^n$ die Formel*

$$h_{n,U}(x) = \begin{cases} 1/q^{ln(n-1)} & \text{falls } x \in T_n(U) \text{ gilt,} \\ 0 & \text{sonst.} \end{cases}$$

Beweis. Auf Grund des vorangehenden Lemmas und Lemma 5.6, welches besagt, dass $h_{n,U}$ gleich bleibt, falls wir U durch eine Konjugierte von U ersetzen, können wir o.B.d.A. annehmen, dass

$$A \equiv \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & b_1 \\ 1 & 0 & 0 & \cdots & 0 & b_2 \\ 0 & 1 & 0 & \cdots & 0 & b_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & b_{n-1} \\ 0 & 0 & 0 & \cdots & 1 & b_n \end{pmatrix} \mod \pi \tag{5.4}$$

gilt. Es gelte $T_n(A) = (\delta_1, \delta_2, ..., \delta_n) \in \mathcal{O}_K^n$. Wir bilden die Funktionen

$$f : M_n \to U \quad , \quad f((x_{i,j})) := A + \pi^l (x_{i,j})$$

und

$$g : \mathcal{O}_K^n \to T_n(A) + \pi^l \mathcal{O}_K^n \quad , \quad g(y_1, y_2, .., y_n) := (\delta_1 + \pi^l y_1, \delta_2 + \pi^l y_2, ..., \delta_n + \pi^l y_n) \quad .$$

Außerdem definieren wir die Abbildung

$$T'_n : M_n \to \mathcal{O}_K^n \quad , \quad (x_{i,j}) \mapsto \frac{1}{\pi^l}\left(T_n(A+\pi^l(x_{i,j})) - T_n(A)\right) \ .$$

Dass diese wirklich nach $\mathcal{O}_K^n$ abbildet, folgt aus $T_n(A+\pi^l(x_{i,j})) \equiv T_n(A) \mod \pi^l$. T'_n macht nach Konstruktion das folgende Diagramm kommutativ :

$$\begin{array}{ccc} U & \xrightarrow{T_n} & T_n(U) \subset T_n(A) + \pi^l\mathcal{O}_K^n \\ f\Big\uparrow & & \Big\uparrow g \\ M_n & \xrightarrow[T'_n]{} & \mathcal{O}_K^n \end{array}$$

Wir setzen nun $T'_n := (T'_{1,n}, T'_{2,n}, .., T'_{n,n})$ mit den Komponentenfunktionen $T'_{i,n} : M_n \to \mathcal{O}_K$ für $i = 1, 2, .., n$. Nehmen wir an, wir hätten gezeigt, dass durch

$$\Phi : M_n \to M_n \ ,$$

$$(x_{i,j}) \mapsto \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n-1} & T'_{1,n}((x_{i,j})) \\ x_{2,1} & x_{2,2} & \cdots & x_{2,n-1} & T'_{2,n}((x_{i,j})) \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_{n,1} & x_{n,2} & \cdots & x_{n,n-1} & T'_{n,n}((x_{i,j})) \end{pmatrix}$$

eine bijektive $K-$analytische Funktion mit $J\Phi((x_{i,j})) \not\equiv 0 \mod \pi$ für alle $(x_{i,j}) \in M_n$ gegeben ist. Dann sehen wir einerseits wegen $T_n^{'}(M_n) = \mathcal{O}_K^n$ und dem obigen Diagramm, dass $T_n(U) = T_n(A) + \pi^l\mathcal{O}_K^n$ gilt. Andererseits erhalten wir, dass Φ maßerhaltend ist und können die angegebene Formel für $h_{n,U}$ wie folgt bestätigen:

Offenbar sind f und g injektive $K-$analytische Funktionen, deren Jacobische

$$|Jf((x_{i,j}))|_K = 1/q^{ln^2} \quad \text{und} \quad |Jg(x)|_K = 1/q^{ln}$$

für alle $(x_{i,j})$ aus M_n und x aus $\mathcal{O}_K^n$ erfüllen. Es sei $B \in \mathcal{B}(K^m)$ beliebig. Setzen wir $B' := B \cap T_n(U)$, dann gilt auf Grund des obigen Diagramms

$$\begin{aligned} T_n^{-1}(B) \cap U &= \left(gT'_nf^{-1}\right)^{-1}(B') \\ &= f\left(T'^{-1}_n\left(g^{-1}(B')\right)\right) \ . \end{aligned}$$

Deswegen folgt mit Hilfe der Transformationsformel:

$$\begin{aligned} \mu_U^n(B) &= \beta^n\left(f\left(T'^{-1}_n\left(g^{-1}(B')\right)\right)\right) \\ &= q^{-ln^2}\beta^n\left(T'^{-1}_n(g^{-1}(B'))\right) \ . \end{aligned}$$

Wir setzen nun $M' := \mathrm{Mat}(n, n-1, \mathcal{O}_K)$. Ferner sei ν das Haar-Maß auf $\mathrm{Mat}(n, n-1, K)$ mit $\nu(M') = 1$; dann gilt $\beta^n = \nu \times \alpha^n$. Wegen der Identität

$$T'^{-1}_n(g^{-1}(B')) = \Phi^{-1}\left(M' \times g^{-1}(B')\right)$$

und der Tatsache, dass Φ und damit auch Φ^{-1} maßerhaltend sind, erhalten wir mit der Transformationsformel

$$\begin{aligned} \mu_U^n(B) &= q^{-ln^2} \cdot \beta^n\left(M' \times g^{-1}(B')\right) \\ &= q^{-ln^2} \cdot \nu(M') \cdot \alpha^n\left(g^{-1}(B')\right) \\ &= q^{-ln^2} \cdot 1 \cdot q^{ln} \cdot \alpha^n\left(B'\right) \\ &= \int_{B \cap T_n(U)} q^{-(ln(n-1))} d\alpha^n(x) \, . \end{aligned}$$

Dies war zu zeigen.

Uns fehlt noch der Nachweis der Behauptung über Φ, d.h. der Nachweis der Bijektivität von Φ und der Eigenschaft $J\Phi((x_{i,j})) \not\equiv 0 \mod \pi$ für alle $(x_{i,j}) \in M_n$.

Wir untersuchen dazu zuerst die Funktionen $T'_{k,n}$ etwas genauer. Es sei dazu $(x_{i,j}) \in M_n$ und X eine Unbestimmte über K. Ferner sei mit b die Basis $\{(-X)^i : i \in \mathbb{N}_0\}$ von $K[X]$ gemeint. Erinnern wir uns an die Definition von T_n und bilden wir das Polynom

$$P = \frac{1}{\pi^l}\left(\mathrm{Det}(A + \pi^l(x_{i,j}) - XI_n) - \mathrm{Det}(A - XI_n)\right) \ ,$$

so ist $T'_{k,n}((x_{i,j}))$ gerade der Koeffizient von $(-X)^{k-1}$ in der Darstellung von P bezüglich b. Wir setzen

$$\delta_{i,j} := \begin{cases} 1 & \text{falls } i = j \ , \\ 0 & \text{sonst} \ . \end{cases}$$

Dann erhalten wir mit Hilfe der Leibniz-Formel für die Determinante die Beziehung

$$\begin{aligned} P &= \frac{1}{\pi^l} \sum_{\sigma \in S_n} \mathrm{Sign}(\sigma) \left(\prod_{i=1}^n (a_{i,\sigma(i)} + \pi^l x_{i,\sigma(i)} - X\delta_{i,\sigma(i)}) - \prod_{i=1}^n (a_{i,\sigma(i)} - X\delta_{i,\sigma(i)}) \right) \\ (*) \qquad &= \sum_{\sigma \in S_n} \mathrm{Sign}(\sigma) \left(\sum_{i=1}^n x_{i,\sigma(i)} \prod_{j=1, j\neq i}^n (a_{j,\sigma(j)} - X\delta_{j,\sigma(j)}) \right) + \pi^l Q \end{aligned}$$

mit einem Polynom Q aus $\mathcal{O}_K[X]$. Wählen wir uns eine Permutation σ aus S_n mit $\sigma(i) = n$ für ein i aus $\mathbb{N}_n$, so dass der Koeffizient von $(-X)^{k-1}$ in der Darstellung von

$$\prod_{j=1, j\neq i}^n (a_{j,\sigma(j)} - X\delta_{j,\sigma(j)})$$

bezüglich b bei Reduktion $\mod \pi$ nicht verschwindet, so sehen wir :

- Wegen $a_{l,l} \equiv 0 \mod \pi$ für $l = 1, 2, 3, ..., n-1$ muss σ genau $k-1$ Fixpunkte verschieden von i besitzen.

- Ist l aus $\mathbb{N}_n - \{i\}$ kein Fixpunkt von σ, so muss auf Grund der speziellen Struktur von $A = (a_{i,j})$ die Beziehung $\sigma(l) = l - 1$ gelten.

Aus diesen beiden Punkten folgt, dass eine Zahl l aus $\mathbb{N}_n$ mit $l < i$ ein Fixpunkt von σ sein muss, sonst wäre σ keine Abbildung mehr. D.h. wir haben zwingend $i = k$. Außerdem folgt $\sigma(l) = l - 1$ für $l = k+1, ..., n$. Also ist σ die Permutation

$$\sigma_k := (k, n, n-1, n-2, ..., k+1)$$

und der betreffende Koeffizient von $(-X)^{k-1}$ in obigem Produkt ist kongruent zu 1 modulo π. Setzen wir $\epsilon_k := \mathrm{Sign}(\sigma_k) \in \{\pm 1\}$, so erhalten wir also aus (*)

$$T'_{k,n}((x_{i,j})) \equiv \epsilon_k x_{k,n} + \sum_{(i,j) \in \mathbb{N}_n \times \mathbb{N}_{n-1}} c_{i,j} x_{i,j} \mod \pi \tag{5.5}$$

mit Konstanten $c_{i,j}$ aus $\mathcal{O}_K$. Jetzt können wir die Behauptungen über Φ beweisen:

Zur Bijektivität von Φ: Dazu zeigen wir : Zu jeder Matrix $N \in M_n$ gibt es genau eine Matrix $M \in M_n$ mit $\Phi(M) = N$:

Es sei dazu $(y_{i,j}) \in M_n$ vorgegeben. Dann bilden wir für Unbestimmte $X_{i,n}$ mit $i \in \mathbb{N}_n$ die Matrix

$$Y := \begin{pmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,n-1} & X_{1,n} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,n-1} & X_{2,n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ y_{n,1} & y_{n,2} & \cdots & y_{n,n-1} & X_{n,n} \end{pmatrix} .$$

Nach Konstruktion der Funktionen $T'_{k,n}$ ist das folgende Gleichungssystem über $\mathcal{O}_K$ in den Unbestimmten $X_{1,n} X_{2,n}, ..., X_{n,n}$

$$\begin{array}{rcl} T'_{1,n}(Y) & = & y_{1,n} \\ T'_{2,n}(Y) & = & y_{2,n} \\ \vdots & \vdots & \vdots \\ T'_{n,n}(Y) & = & y_{n,n} \end{array}$$

linear. Bringen wir die konstanten Terme auf der linken Seite auf die rechte Seite und schreiben wir das Gleichungssystem in der Form

$$W(X_{1,n}, X_{2,n}, ..., X_{n,n}) = y'$$

mit $W \in M_n$ und $y' \in \mathcal{O}_K^n$, so erhalten wir auf Grund der Kongruenz 5.5

$$W \equiv \mathrm{Diag}(\epsilon_1, \epsilon_2, ..., \epsilon_n) \mod \pi .$$

D.h. W ist unimodular und damit das obige Gleichungssystem eindeutig lösbar. Die Lösung sei $(x_{1,n}, x_{2,n}, ..., x_{n,n}) \in \mathcal{O}_K^n$. Setzen wir noch $x_{i,j} := y_{i,j}$ für alle $(i,j) \in \mathbb{N}_n \times \mathbb{N}_{n-1}$, so ist offenbar $(x_{i,j})$ eine Lösung von $\Phi((x_{i,j})) = (y_{i,j})$ und gleichzeitig die Einzige. Das war die Bijektivität von Φ.

Zur Aussage über die Jacobische von Φ: Aus unserer Relation 5.5 schließen wir für i, k aus $\mathbb{N}_n$ und $(x_{r,s})$ und M_n:

$$\frac{\partial T'_{k,n}}{\partial x_{i,n}}((x_{r,s})) \equiv \begin{cases} \epsilon_k \mod \pi & \text{falls } i = k \text{ gilt} , \\ 0 \mod \pi & \text{falls } i \neq k \text{ gilt} . \end{cases}$$

Die Jacobi-Matrix von Φ in einem Punkt $(x_{i,j})$ aus M_n erfüllt damit die folgende Kongruenz:

$$D\Phi((x_{i,j})) \equiv \begin{pmatrix} I_{n(n-1)} & & & & & \\ * & \epsilon_1 & & & & \\ * & & \epsilon_2 & & & \\ \vdots & & & \ddots & & \\ * & & & & \epsilon_{n-1} & \\ * & & & & & \epsilon_n \end{pmatrix} \mod \pi .$$

D.h. es gilt $J\Phi((x_{i,j})) \not\equiv 0 \mod \pi$, was zu zeigen war. Damit ist der Satz bewiesen. $\square$

Definition 5.10. Wir setzen

$$\Omega_n := \{A \in M_n : A \text{ ist gutartig}\} .$$

Außerdem vereinbaren wir für $x \in K^n$:

$$\kappa_n(x) := \begin{cases} \begin{array}{c} \text{Die Anzahl der } \mod \pi \text{ verschiedenen} \\ \text{Matrizen } A \in \Omega_n \text{ mit } x \in T_n(A + \pi M_n) \end{array} & \text{falls } x \in \mathcal{O}_K^n , \\ 0 & \text{sonst} . \end{cases}$$

κ_n ist also eine Funktion $K^n \to \mathbb{N}_0$.

Wählen wir ein vollständiges Vertretersystem $V \subset \Omega_n$ von $\mod \pi$ verschiedenen Matrizen, so erhalten wir die endliche disjunkte Zerlegung

$$\Omega_n = \bigcup_{A \in V} A + \pi M_n .$$

Insbesondere ist also Ω_n kompakt-offen. Es ergeben sich offenbar

$$\mu^n_{\Omega_n} = \sum_{A \in V} \mu^n_{A+\pi M_n} \quad \text{und} \quad h_{n,\Omega_n} = \sum_{A \in V} h_{n,A+\pi M_n} .$$

Deswegen erhalten wir aus Satz 5.9 das folgende Korollar:

Korollar 5.11. *Die Dichte h_{n,Ω_n} existiert. Genauer gilt für alle $x \in K^n$ die Beziehung*

$$h_{n,\Omega_n}(x) = \kappa_n(x) q^{-n(n-1)}.$$

Beispiel 5.12. Wir bestimmen κ_2 :

Es ist offenbar Ω_2 die Menge der $\mod \pi$ nichtskalaren Matrizen aus M_2, d.h. die Menge der Matrizen $A \in M_2$, für die es kein $a \in \mathcal{O}_K$ mit $A \equiv aI_2 \mod \pi$ gibt.

Sei nun $(t,u) \in \mathcal{O}_K^2$ vorgegeben. Beachten wir, dass $T_2 = T$ die Spur-Norm-Abbildung ist, so gilt

$$\begin{aligned}
\kappa_2(t,u) &= \#\{\bar{A} : A \in \Omega_2 \text{ und } (t,u) \in T_2(A + \pi M_2) = T_2(A) + \pi \mathcal{O}_K^2\} \\
&= \#\{\bar{A} : A \in \Omega_2 \text{ mit } T_2(A) \equiv (t,u) \mod \pi\} \\
&= \#\left\{ \bar{A} = \overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} : \begin{array}{r} (a+d, ad-bc) \equiv (t,u) \mod \pi, \\ A \in \Omega_2 \end{array} \right\} \\
&= \#\left\{ \overline{(a,b,c)} : \begin{array}{c} -bc \equiv a^2 - ta + u \mod \pi, \\ \begin{pmatrix} a & b \\ c & t-a \end{pmatrix} \in \Omega_2 \end{array} \right\} .
\end{aligned}$$

Die Anzahl N der $\mod \pi$ verschiedenen Lösungen (a,b,c) der Kongruenz

$$-bc \equiv a^2 - ta + u \mod \pi$$

zerfällt in die Anzahl N_1 der $\mod \pi$ verschiedenen Lösungen mit $\pi \nmid b$ und der Anzahl N_2 der $\mod \pi$ verschiedenen Lösungen mit $\pi \mid b$.

Offensichtlich gilt $N_1 = (q-1)q$, denn $\overline{c}$ ist für jedes fest gewählte $\overline{b}$ festgelegt und $\overline{a}$ ist beliebig wählbar. Um N_2 zu bestimmen, erinnern wir nochmal an das Symbol $\left(\frac{\cdot,\cdot}{K}\right)$ (mit Werten in $\mathbb{Z}$). Dabei wertet $\left(\frac{-t,u}{K}\right) = \left(\frac{t,u}{K}\right)$ zu $1, 0$ oder -1 aus, je nachdem ob das Polynom $\chi_{t,u} := X^2 - \overline{t}X + \overline{u} \in F_K[X]$ eine, zwei oder keine Nullstelle in F_K besitzt.

Offenbar gilt $N_2 = q\left(1 + \left(\frac{t,u}{K}\right)\right)$, denn es gilt $b \equiv 0 \mod \pi$ und $\overline{c}$ ist für jede Nullstelle von $\chi_{t,n}$ frei wählbar. Wir erhalten somit die schöne Formel

$$N = N_1 + N_2 = q^2 + \left(\frac{t,u}{K}\right) q \ .$$

Um $\kappa_2(t,n)$ zu bestimmen, müssen wir unter den N Lösungen die Lösungen $\overline{(a,b,c)}$ ausschließen, bei denen $\begin{pmatrix} a & b \\ c & t-a \end{pmatrix}$ nicht in Ω_2 liegt, dies ist genau dann der Fall, falls gleichzeitig $t \equiv 2a \mod \pi$ und $b \equiv c \equiv 0 \mod \pi$ gilt. Und das ist offenbar nur möglich, falls $\left(\frac{t,u}{K}\right) = 0$ gilt. Umgekehrt überzeugt man sich davon, dass man, welche Charakteristik F_K auch hat, in diesem Fall genau eine Lösung "streichen" muss. Es folgt

$$\kappa_2(t,u) = \begin{cases} q^2 + q & \text{falls } \left(\frac{t,u}{K}\right) = 1 \text{ gilt} , \\ q^2 - 1 & \text{falls } \left(\frac{t,u}{K}\right) = 0 \text{ gilt} , \\ q^2 - q & \text{falls } \left(\frac{t,u}{K}\right) = -1 \text{ gilt} . \end{cases}$$

Damit ist κ_2 berechnet.

Nun wollen wir uns anschauen, was passiert, wenn wir bei $h_{n,U}$ die Menge U durch ein Translat ersetzt. Wir wählen eine Unbestimmte X über K und definieren für ein $a \in \mathcal{O}_K$ die Abbildung

$$\omega_{n,a} : K^n \to K^n \ , \ (a_1, a_2, ..., a_n) \mapsto (a_1', a_2', ..., a_n') \ ,$$

wobei die a_i' durch die Identität

$$\begin{gathered}(-X)^n + a_1'(-X)^{n-1} + ... + a_{n-2}'(-X)^2 + a_{n-1}'(-X)^1 + a_n' \\ = \\ (-(X-a))^n + a_1(-(X-a))^{n-1} + ... + a_{n-2}(-(X-a))^2 + a_{n-1}(-(X-a))^1 + a_n\end{gathered}$$

definiert seien (die a_i' sind eindeutig bestimmt: ein Polynom wird in zwei verschiedenen Basen von $K[X]$ dargestellt). Offensichtlich ist $\omega_{n,a}$ eine $K-$analytische Funktion, denn die Komponentenfunktionen von $\omega_{n,a}$ sind Polynomfunktionen. Ferner ist offensichtlich, dass die Jacobi-Matrix von $\omega_{n,a}$ in jedem Punkt $x \in K^n$ eine untere Dreiecks-Matrix mit lauter Einsen auf der Diagonalen ist. Wegen der Identität

$$\mathrm{Det}((aI_n + A) - XI_n) = \mathrm{Det}(A - (X-a)I_n)$$

für eine Matrix A aus $\mathrm{Mat}(n, K)$ und der Definition der Abbildung T_n beschreibt also $\omega_{n,a}$, wie sich $T_n(aI_n + A)$ aus $T_n(A)$ berechnen lässt, nämlich durch $\omega_{n,a}(T_n(A))$. Insbesondere ist $\omega_{n,a}$ eine Bijektion mit der Inversen $\omega_{n,-a}$, was aus

$$\omega_{n,-a}(\omega_{n,a}(T_n(A))) = \omega_{n,a}(\omega_{n,-a}(T_n(A))) = T_n(A)$$

und der Surjektivität von T_n folgt. Wir erhalten schließlich für jede offene Menge $U \subset M_n$ das folgende kommutative Diagramm:

$$\begin{tikzcd} aI_n + U \arrow[r, "T_n"] & T_n(aI_n + U) \\ U \arrow[u, "+aI_n"] \arrow[r, "T_n"'] & T_n(U) \arrow[u, "\omega_{n,a}"'] \end{tikzcd}$$

Als Konsequenz aus den obigen Überlegungen erhalten wir die folgende Proposition:

Proposition 5.13. *Für jede offene Menge $U \subset M_n$ und jedes a aus $\mathcal{O}_K$ gilt: Existiert $h_{n,U}$, so exstiert auch h_{n,aI_n+U} und es gilt $h_{n,aI_n+U} = h_{n,U} \circ \omega_{n,-a}$.*

Beweis. Wir wählen eine Borel-Menge $B \in \mathcal{B}(K^n)$, dann gilt mit Hilfe der Transformationsformel:

$$\mu_U^n(\omega_{n,-a}(B)) = \int_{\omega_{n,-a}(B)} h_{n,U}(x) d\alpha^n(x) = \int_B h_{n,U}(\omega_{n,-a}(x)) \cdot 1 \cdot d\alpha^n(x) \ .$$

Andererseits gilt auf Grund des Diagramms für die Funktion $\omega_{n,a}$ die Beziehung

$$T_n^{-1}(\omega_{n,-a}(B)) \cap U + aI_n = T_n^{-1}(B) \cap (aI_n + U)$$

und es folgt mit der Translationsinvarianz von β^n:

$$\begin{aligned} \mu_U^n(\omega_{n,-a}(B)) &= \beta^n(T_n^{-1}(\omega_{n,-a}(B)) \cap U) \\ &= \beta^n(T_n^{-1}(B) \cap (aI_n + U)) = \mu_{aI_n+U}^n(B) \ . \end{aligned}$$

Aus der Tatsache, dass $h_{n,U} \circ \omega_{n,-a}$ stetig ist und der Eindeutigkeit von h_{n,aI_n+U} (Lemma 5.1) folgt die Behauptung. $\square$

Beispiel 5.14. Es sei $(t,u) \in K^2$, $a \in \mathcal{O}_K$ und es sei X eine Unbestimmte über K. Es gilt

$$(-(X+a))^2 + t(-(X+a)) + u = (-X)^2 + (t-2a)(-X) + (a^2 - ta + u) \ .$$

Also folgt $\omega_{2,-a}(t,u) = (t-2a, a^2 - ta + u)$. Haben wir also für eine offene Menge $U \subset M_2$ die Funktion $h_{2,U}$ bestimmt, so folgt für alle $(t,u) \in K^2$

$$h_{2,aI_2+U}(t,u) = h_{2,U}(t-2a, a^2 - ta + u) \ .$$

Das nächste Ergebnis zeigt uns, wie wir aus $h_{n,U}$ die Funktion $h_{n,\pi^k U}$ erhalten können.

Proposition 5.15. *Sei $U \subset M_n$ offen und $k \in \mathbb{N}$ fest gewählt. Existiert $h_{n,U}$, dann existiert auch $h_{n,\pi^k U}$ und es gilt*

$$h_{n,\pi^k U}((a_i)_{i=1}^n) = \frac{1}{q^{mk}} h_{n,U}\left(\left(\frac{a_i}{\pi^{ik}}\right)_{i=1}^n\right) \ .$$

Dabei ist $m := n^2 - n(n+1)/2$.

Beweis. Wir definieren die Abbildung

$$\phi : K^n \to K^n \ , \ (a_i)_{i=1}^n \mapsto \left(\frac{a_i}{\pi^{ik}}\right)_{i=1}^n$$

und zeigen für jedes $B \in \mathcal{B}(K^m)$ die Identität

$$\mu_{\pi^k U}^n(B) = \frac{1}{q^{mk}} \int_B h_{n,U}\left(\phi(x)\right) d\alpha^n\left(x\right) \ .$$

Dann ist der Satz bewiesen. Wir führen zusätzlich die Abbildung

$$\psi : U \to \pi^k U \ , \ A \mapsto \pi^k A$$

ein und erhalten das folgende kommutative Diagramm:

$$\begin{tikzcd} U \arrow[r, "\psi"] \arrow[d, "T_n"'] & \pi^k U \arrow[d, "T_n"] \\ \mathcal{O}_K^n & \prod_{i=1}^n \pi^{ik}\mathcal{O}_K \arrow[l, "\phi"] \end{tikzcd}$$

ϕ und ψ sind offenbar beide $K-$analytisch und injektiv. Ferner gilt für alle $A \in U$ und $a \in K^n$

$$\left|J\psi(A)\right|_K = (1/q^k)^{n^2} = 1/q^{kn^2} \text{ und } \left|J\phi(a)\right|_K = q^{k(1+2+3+\ldots+n)} = q^{kn(n+1)/2} \ .$$

Wir wählen ein beliebiges $B \in \mathcal{B}(K^n)$. Auf Grund von Proposition 5.5 (ii) haben wir

$$\pi^{-k} \cdot T_n^{-1}(B) = T_n^{-1}(\phi(B)) \ .$$

Daraus folgern wir mit Hilfe der Transformationsformel :

$$\begin{aligned} \mu_{\pi^k U}^n(B) &= \beta^n(\pi^k U \cap T_n^{-1}(B)) \\ &= \beta^n(\psi^{-1}(U \cap \pi^{-k} \cdot T_n^{-1}(B))) \\ &= \frac{1}{q^{kn^2}} \beta^n(U \cap T_n^{-1}(\phi(B))) \\ &= \frac{1}{q^{kn^2}} \mu_U^n(\phi(B)) \ . \end{aligned}$$

Verwenden wir nun, dass nach Voraussetzung $h_{n,U}$ existiert und verwenden abermals die Transformationsformel, so erhalten wir

$$\begin{aligned} \frac{1}{q^{kn^2}} \mu_U^n \left(\phi(B)\right) &= \frac{1}{q^{kn^2}} \int_{\phi(B)} h_{n,U}\left(x\right) d\alpha^n \left(x\right) \\ &= \frac{q^{kn(n+1)/2}}{q^{kn^2}} \int_B h_{n,U}\left(\phi(x)\right) d\alpha^n \left(x\right) \ . \end{aligned}$$

Setzen wir unsere Rechnungen zusammen, so erhalten wir die zu beweisende Identität. Damit ist die Proposition bewiesen. □

Bemerkung 5.16. Die Einführung der Dichten $h_{n,U}$ sowie die Aussagen, die wir darüber in diesem Unterabschnitt erhalten haben, gehen im Fall $K = \mathbb{Q}_p$ mit $p \in \mathbb{P}$ und $n = 2$ auf Lang und Trotter zurück. Wir haben die Aussagen unter Anderem deswegen so allgemein formuliert, da wir neben der Bestimmung von h auch an der Bestimmung der Dichten h_n interessiert waren.

5.2 Eine Formel für die Dichte h

Es sei $S_0 := \Omega_2 \subset M$ die Menge der $\mod \pi$ nichtskalaren 2×2-Matrizen aus $M = M_2$. Ferner setzen wir für eine offene Menge $U \subset M$

$$\mu_U := \mu_U^2 \ , \ \mu := \mu_M \ \text{ und falls existent } \ h_U := h_{2,U} \text{ und } h := h_2 \ .$$

Wir werden nun im Verlaufe dieses Unterabschnittes h bestimmen.

Mit Hilfe von Beispiel 5.12 und Korollar 5.11 erhalten wir

$$h_{S_0}(t,u) = \kappa_2(t,u) q^{-2(2-1)} = \begin{cases} 1 + q^{-1} & \text{falls } \left(\frac{t,u}{K}\right) = 1 \text{ gilt} , \\ 1 - q^{-2} & \text{falls } \left(\frac{t,u}{K}\right) = 0 \text{ gilt} , \\ 1 - q^{-1} & \text{falls } \left(\frac{t,u}{K}\right) = -1 \text{ gilt} \end{cases} \tag{5.6}$$

für alle $(t,u) \in \mathcal{O}_K^2$ und $h_{S_0}(t,u) = 0$ für $(t,u) \in K^2 - \mathcal{O}_K^2$. Dabei ist $\left(\frac{t,u}{K}\right)$ gleich $1, 0$ oder -1 je nachdem, ob das Polynom $X^2 - \overline{t}X + \overline{u}$ aus $F_K[X]$ zwei, eine oder keine Nullstelle in F_K besitzt.

Existiert für eine offene Menge $V \subset M$ die Abbildung h_V, so existieren nach dem, was wir schon wissen, auch h_{aI+V} und $h_{\pi^k V}$ und es gilt für alle $(t,u) \in K^2$

$$h_{aI+V}(t,u) = h_V(t - 2a, a^2 - ta + u)$$

und

$$h_{\pi^k V}(t,u) = q^{-k} h_V \left(\frac{t}{\pi^k}, \frac{u}{\pi^{2k}} \right) \ .$$

D.h., da wir h_{S_0} bestimmt haben, erhalten wir nun die Existenz von h_U für Mengen $U := aI + \pi^k S_0$ mit $a \in \mathcal{O}_K$ und $k \in \mathbb{N}_0$. Setzen wir

$$\delta_{a,k}(t,u) := \left(\frac{t - 2a}{\pi^k}, \frac{a^2 - ta + u}{\pi^{2k}} \right) \ ,$$

so erhalten wir

$$h_U(t,u) = q^{-k} h_{S_0} \left(\delta_{a,k}(t,u) \right) \ . \tag{5.7}$$

Die oben eingeführten Größen $\delta_{a,k}(t,u)$ haben die folgenden Eigenschaften:

Lemma 5.17. *Es sei $(t,u) \in K^2$ und $k \in \mathbb{N}_0$. Dann gelten die folgenden Aussagen:*

(i) Gilt $\delta_{a,k}(t,u) \in \mathcal{O}_K^2$ für ein a aus $\mathcal{O}_K$, dann gilt $(t,u) \in \mathcal{O}_K^2$ und es gilt $\delta_{a,k'}(t,u) \in \pi^{k-k'}\mathcal{O}_K^2$ für alle ganzen Zahlen k' mit $0 \leq k' \leq k$.

(ii) Es gelte $\delta_{a,k}(t,n), \delta_{a',k}(t,u) \in \mathcal{O}_K^2$ für $a, a' \in \mathcal{O}_K$, dann gilt $a \equiv a' \mod \pi^k$.

(iii) Es gelte $\delta_{a,k}(t,u) \in \mathcal{O}_K^2$ und $a \equiv a' \mod \pi^k$ für $a, a' \in \mathcal{O}_K$, dann folgt $\delta_{a',k}(t,u) \in \mathcal{O}_K^2$.

Beweis. Zu (i) : Dies ist nach Definition der $\delta_{a,k}(t,u)$ offensichtlich.

Zu (ii) : Für $a, a' \in \mathcal{O}_K$ gelte $\delta_{a,k}(t,u), \delta_{a',k}(t,u) \in \mathcal{O}_K^2$. Wir zeigen, dass daraus $a \equiv a' \mod \pi^k$ folgt. Nach Voraussetzung erfüllen a und a' die beiden Kongruenzen

$$t - 2x \equiv 0 \mod \pi^k \text{ und } x^2 - tx + u \equiv 0 \mod \pi^{2k} .$$

Hieraus erhalten wir auf Grund der Identitäten

$$\begin{aligned} a^2 - ta + u - (a'^2 - ta' + u) &= (a-a')(a+a'-t) \text{ und} \\ (a-a') - (t-2a') &= a + a' - t \end{aligned}$$

die Kongruenzen

$$(a-a')(a+a'-t) \equiv 0 \mod \pi^{2k} \text{ und } a - a' \equiv a + a' - t \mod \pi^k .$$

Beide sind offenbar nur dann erfüllbar, falls $a - a' \equiv 0 \mod \pi^k$ gilt.

Zu (iii) : Dies erhält man mit ähnlich einfachen Argumenten wie im Beweis zu (ii) Deswegen überlassen wir den Beweis dem Leser als Übung . □

Wir haben gesehen, dass wir h_U für Mengen $U = aI + \pi^k S_0$ berechnen können. Wie wir nun sehen werden, genügt dies, um die Existenz von h sicher zu stellen.

Wir können die Menge M wie folgt zerlegen: Es sei für jedes $i \in \mathbb{N}$ die Menge $V_i \subset \mathcal{O}_K$ ein vollständiges Vertretersystem von $\mathcal{O}_K/\mathfrak{p}_K^i$ (V_i hat offenbar q^i Elemente). Dann bilden wir die disjunkte Vereinigung

$$S_i := \bigcup_{a \in V_i} aI + \pi^i S_0 .$$

S_i ist kompakt-offen (denn S_0 ist kompakt-offen und V_i endlich) und besteht offenbar aus den Matrizen $A \in M$, die $\mod \pi^i$ skalar sind, aber nicht $\mod \pi^{i+1}$. Führen wir zusätzlich noch die Skalar-Matrizen

$$S_\infty := \{A \in M : A - aI = 0 \in M \text{ für ein } a \in \mathcal{O}_K\}$$

ein, so erhalten wir offenbar die disjunkte Zerlegung

$$M = \bigcup_{i \in \mathbb{N}_0 \cup \{\infty\}} S_i . \tag{5.8}$$

Für jede Borelmenge $B \in \mathcal{B}(K^2)$ gilt wegen $S_\infty \subset W := \begin{pmatrix} \mathcal{O}_K & 0 \\ 0 & \mathcal{O}_K \end{pmatrix}$

$$0 \leq \mu_{S_\infty}(B) = \beta(T^{-1}(B) \cap S_\infty) \leq \beta(S_\infty) \leq \beta(W) = 0 \ .$$

D.h. μ_{S_∞} ist also das Null-Maß und liefert damit keinen Beitrag zu μ. Mit Hilfe der Zerlegung von M in Zeile 5.8 erhalten wir schließlich

$$\mu = \sum_{i=0}^{\infty} \mu_{S_i} \ .$$

Nun können wir die Existenz von h nachweisen:

Satz 5.18. *Das Maß $\mu = T(\beta_M)$ besitzt eine stetige Dichte h bezüglich α. Und zwar erhält man h als die auf ganz K^2 gleichmäßig konvergierende Funktionen-Reihe stetiger Funktionen*

$$h = \sum_{k=0}^{\infty} h_{S_k} \ .$$

Beweis. Zunächst wollen wir einsehen, dass die Summe

$$H := \sum_{k=0}^{\infty} h_{S_k}$$

gleichmäßig auf K^2 konvergiert. Wir haben offenbar für jedes $k \in \mathbb{N}_0$

$$h_{S_k} = \sum_{a \in V_k} h_{a+\pi^i S_0} \ .$$

Benutzen wir Gleichung 5.7, so erhalten wir für ein Paar $(t,u) \in K^2$

$$h_{S_k}(t,u) = \sum_{a \in V_k} h_{aI+\pi^k S_0}(t,u) = \sum_{a \in V_k} q^{-k} h_{S_0}(\delta_{a,k}(t,u)) \ .$$

Nun liefert aber wie wir wissen $h_{S_0}(\delta_{a,k}(t,u))$ höchstens dann einen Beitrag zur obigen Summe, falls $\delta_{a,k}(t,u) \in \mathcal{O}_K^2$ gilt (siehe Gleichung 5.6). Da $V_k \subset \mathcal{O}_K$ ein vollständiges Vertretersystem der Reste $\mod \pi^k$ ist, kann dies höchstens für genau ein $a \in V_k$ geschehen (siehe Lemma 5.17 (ii)). Da die Funktion h_{S_0} offenbar nach oben durch 2 beschränkt ist, folgt schließlich für alle $(t,u) \in K^2$

$$h_{S_k}(t,u) \leq 2q^{-k} \ .$$

D.h. H besitzt eine konvergente Majorante und ist deshalb gleichmäßig konvergent.

Als gleichmäßiger Limes von stetigen Funktionen ist H überdies stetig. Es bleibt noch nachzurechnen, dass H eine Dichte von μ bezüglich α ist. Dies ergibt sich sofort auf Grund des Satzes von B.Levi (siehe Satz 4.4 (ii)): Es sei $B \in \mathcal{B}(K^2)$ beliebig. Dann folgt:

$$\mu(B) = \sum_{k=0}^{\infty} \mu_{S_k}(B) = \sum_{k=0}^{\infty} \int_B h_{S_k}(x) d\alpha(x) = \int_B H(x) d\alpha(x) \ .$$

Das war zu zeigen. $\square$

Bemerkung 5.19. Um die Darstellung von h als gleichmäßig konvergente Funktionen-Reihe zu erhalten, sind wir analog vorgegangen, wie Lang und Trotter bei der Untersuchung der in der Einleitung erwähnten Dichte f (siehe [7], §7).

Nun wollen wir expliziter werden. Wir definieren dazu die Abbildung

$$r : \mathcal{O}_K^2 \to \widehat{\mathbb{R}} \ ,$$

die für jedes Paar $(t,u) \in \mathcal{O}_K^2$ gegeben sei durch

$$r(t,u) := \sup\{k \in \mathbb{N}_0 : \delta_{a,k}(t,n) \in \mathcal{O}_K^2 \text{ für ein } a \in \mathcal{O}_K\} \ .$$

Ziel wird es sein, für ein Paar $(t,u) \in \mathcal{O}_K^2$ den Wert $h(t,u)$ explizit aus der Größe $r(t,u)$ zu berechnen. Wie wir später sehen, ist $r(t,u)$ umso einfacher zu bestimmen, je kleiner die maximale $\pi-$Potenz ist, die in der 2 aufgeht. Es folgen zunächst einige Eigenschaften von r.

Offensichtlich gilt $r(\mathcal{O}_K^2) \subset \mathbb{N}_0 \cup \{\infty\}$ und wir werden nun insbesondere sehen, dass r stetig ist:

Proposition 5.20. *Die Funktion $r : \mathcal{O}_K^2 \to \widehat{\mathbb{R}}$ ist stetig und in einer Umgebung jedes Punktes $(t,u) \in \mathcal{O}_K^2$ mit $r(t,u) < \infty$ konstant. Genauer gilt für $(t,u) \in \mathcal{O}_K^2$ mit $r(t,u) = d \in \mathbb{N}_0$ die Beziehung*

$$r\left((t,u) + \pi^{2(d+1)}\mathcal{O}_K^2\right) = \{d\} \ .$$

Beweis. Die Stetigkeit in Punkten $(t,u) \in \mathcal{O}_K^2$ mit $r(t,u) < \infty$ ist offenbar gezeigt, wenn wir die Konstanz von r in einer Umgebung solcher Punkte gezeigt haben. Es sei $r(t,u) = d \in \mathbb{N}_0$ und es sei $(x,y) \in \mathcal{O}_K^2$ beliebig. Wir setzen $t' := t + \pi^{2(d+1)}x$ und $u' := u + \pi^{2(d+1)}y$ und zeigen

$$r(t,u) = r\left(t',u'\right) \ ;$$

dann haben wir die Zusatz-Behauptung des Lemmas gleich mitbewiesen. Nach Definition haben wir $\delta_{a,i}(t,u) \in \mathcal{O}_K^2$ genau dann,

$$\text{falls } t - 2a \equiv 0 \mod \pi^i \ \text{ und } \ a^2 - ta + u \equiv 0 \mod \pi^{2i} \text{ gilt} \ .$$

Da nach Voraussetzung $\delta_{a,d}(t,n) \in \mathcal{O}_K^2$ gilt, folgt offenbar auch $\delta_{a,d}\left(t',u'\right) \in \mathcal{O}_K$. Ferner würde offenbar $\delta_{a',d+1}\left(t',u'\right) \in \mathcal{O}_K$ für ein $a' \in \mathcal{O}_K$ auch $\delta_{a',d+1}(t,u) \in \mathcal{O}_K^2$ implizieren, was nicht erfüllbar ist. Also gilt die behauptete Gleichheit.

Es sei nun ein Punkt $(t,u) \in \mathcal{O}_K^2$ mit $r(t,u) = \infty$ gewählt. Wir zeigen, dass r in (t,u) stetig ist. Dazu sei $V :=]N, \infty]$ eine Umgebung von ∞. Wir müssen zeigen, dass es eine Umgebung $U \subset \mathcal{O}_K^2$ von (t,u) gibt, mit $r(U) \subset V$. Es sei $k \in V \cap \mathbb{N}$ gewählt. Nach Voraussetzung gibt es ein $a \in \mathcal{O}_K$ mit $\delta_{a,k}(t,u) \in \mathcal{O}_K^2$. Damit folgt offenbar für $U := (t,u) + \pi^{2k}\mathcal{O}_K^2$ die Beziehung $\delta_{a,k}(U) \subset \mathcal{O}_K^2$. Dies bedeutet aber $r(U) \subset V$, was zu zeigen war. $\square$

Jetzt überlegen wir uns, in welchen Punkten $(t,u) \in \mathcal{O}_K^2$ die Beziehung $r(t,u) = \infty$ gilt:

Proposition 5.21. *Es gilt die folgende Äquivalenz:*

$$r(t,u) = \infty \Leftrightarrow \begin{cases} D = t^2 - 4u = 0 & \textit{falls } Char(K) \neq 2 \textit{ gilt,} \\ t = 0 \textit{ und } n = a^2 \textit{ für ein } a \in \mathcal{O}_K & \textit{falls } Char(K) = 2 \textit{ gilt.} \end{cases}$$

Beweis. "$\Rightarrow$": Wegen $r(t,u) = \infty$ finden wir eine Folge $(a_i)_{i\in\mathbb{N}}$ in $\mathcal{O}_K$ mit $\delta_{a_i,i}(t,u) \in \mathcal{O}_K^2$ für $i \in \mathbb{N}$. Die Folge $(a_i)_{i\in\mathbb{N}}$ ist eine Cauchy-Folge, denn für natürliche Zahlen $N,k,l \in \mathbb{N}$ mit $k,l \geq N$ gilt $\delta_{a_k,N}(t,u), \delta_{a_l,N}(t,u) \in \mathcal{O}_K^2$ (siehe Lemma 5.17 (i)), und daraus folgt mit Lemma 5.17 (ii)

$$a_k \equiv a_l \mod \pi^N \text{, was äquivalent ist zu } |a_k - a_l|_K \leq q^{-N} \ .$$

Also ist $(a_i)_{i\in\mathbb{N}}$ konvergent gegen ein $a \in \mathcal{O}_K$. Es folgt einerseits

$$t - a_i \to t - 2a \ \text{ und } \ a_i^2 - ta_i + u \to a^2 - ta + u$$

für $i \to \infty$. Andererseits folgen wegen

$$\delta_{a_i,i}(t,u) \in \mathcal{O}_K^2, \text{ d.h. wegen } |t-2a_i|_K \leq q^{-i} \text{ und } \left|a_i^2 - ta_i + u\right|_K \leq q^{-2i}$$

für $i \in \mathbb{N}$ die Beziehungen

$$t - a_i \to 0 \text{ und } a_i^2 - ta_i + u \to 0$$

für $i \to \infty$. Also folgt $t = 2a$ und $a^2 - ta + u = 0$, woraus wir offenbar den Rest dieser Richtung erhalten.

"$\Leftarrow$": Im Falle $\mathrm{Char}(K) \neq 2$ wählen wir $a := t/2$. Dann folgt offenbar $a \in \mathcal{O}_K$, denn es gilt $\left(\frac{t}{2}\right)^2 = u \in \mathcal{O}_K$. Außerdem gilt $\delta_{a,i}(t,u) = (0,0) \in \mathcal{O}_K^2$ für alle $i \in \mathbb{N}$. D.h. es gilt $r(t,u) = \infty$. Gilt $\mathrm{Char}(K) = 2$, so folgt mit dem in der Behauptung der Aufgabe angegebenen $a \in \mathcal{O}_K$ ebenfalls $\delta_{a,i}(t,u) = (0,0) \in \mathcal{O}_K^2$ für alle $i \in \mathbb{N}$ und damit $r(t,u) = \infty$. □

Bemerkung 5.22. Im Falle $\mathrm{Char}(K) = 2$ ist das Element $a \in \mathcal{O}_K$ mit $a^2 = u$ aus der vorangehenden Proposition eindeutig bestimmt. Denn ganz allgemein ist in jedem Körper der Charakteristik 2 die Abbildung $x \mapsto x^2$ eine Injektion .

Wir werden nun sehen, dass wir die Konstante $r(t,u)$ im Falle $\mathrm{Char}(K) \neq 2$ anhand der Diskriminante $D = t^2 - 4u$ berechnen können. Dabei können wir auf Grund dessen, was wir schon über $r(t,u)$ wissen, den Fall $r(t,u) = \infty$ ausschließen .

Proposition 5.23. *Es gelte $\mathrm{Char}(K) \neq 2$. Haben wir für ein Paar $(t,u) \in \mathcal{O}_K^2$ die Beziehung $r(t,u) < \infty$ und setzen wir $D := t^2 - 4u$, so folgt*

$$r(t,u) = \begin{cases} \sup\{d \in \mathbb{N}_0 : \pi^{2k} | D\} & \textit{falls } \pi \nmid 2 \textit{ gilt,} \\ \sup\left\{k \in \mathbb{N}_0 : \begin{array}{c} \pi^{2k}|D \textit{ und} \\ D/\pi^{2k} \textit{ ist ein Quadrat} \mod 4 \end{array}\right\} & \textit{falls } \pi | 2 \textit{ gilt.} \end{cases}$$

Beweis. Wir gehen die einzelnen Fälle durch:

Der Fall $\mathrm{Char}(F_K) \neq 2$: Es sei k aus $\mathbb{N}_0$ beliebig. Da $2 \in \mathcal{O}_K^*$ gilt, haben wir die folgende Kette von Äquivalenzen:

$$\begin{array}{ll} & \text{Es gilt } \delta_{a,k}(t,n) \in \mathcal{O}_K^2 \text{ für ein } a \text{ aus } \mathcal{O}_K. \\ \Leftrightarrow & \text{Es gilt } t - 2a \equiv 0 \mod \pi^k \text{ und } a^2 - ta + u \equiv 0 \mod \pi^{2k} \text{ für ein } a \text{ aus } \mathcal{O}_K. \\ \Leftrightarrow & \text{Es gilt } t - 2a \equiv 0 \mod \pi^k \text{ und } (t-2a)^2 \equiv D \mod \pi^{2k} \text{ für ein } a \text{ aus } \mathcal{O}_K. \\ \Leftrightarrow & \text{Es gilt } D \equiv 0 \mod \pi^{2k} . \end{array}$$

Für die Rückrichtung der letzten Äquvivalenz wähle man einfach ein a aus $\mathcal{O}_K$ mit $t \equiv 2a \mod \pi^k$. Dies ist möglich, da $2 \in \mathcal{O}_K^*$ gilt. Also folgt die Aussage für diesen Fall.

Der Fall $\mathrm{Char}(F_K) = 2$: Es sei wieder k aus $\mathbb{N}_0$ beliebig. Jetzt müssen wir beachten, dass $\pi|2$ gilt. Wir erhalten:

$$\begin{array}{rl} & \text{Es gilt } \delta_{a,k}(t,u) \in \mathcal{O}_K^2 \text{ für ein } a \text{ aus } \mathcal{O}_K. \\ \Leftrightarrow & \text{Es gilt } t - 2a \equiv 0 \mod \pi^k \text{ und } a^2 - ta + u \equiv 0 \mod \pi^{2k} \text{ für ein } a \text{ aus } \mathcal{O}_K. \\ \Leftrightarrow & \text{Es gilt } t - 2a \equiv 0 \mod \pi^k \text{ und } (t-2a)^2 \equiv D \mod 4\pi^{2k} \text{ für ein } a \text{ aus } \mathcal{O}_K. \\ \Leftrightarrow & \text{Es gilt } D \equiv 0 \mod \pi^{2k} \text{ und } D/\pi^{2k} \text{ ist ein Quadrat } \mod 4\,. \end{array}$$

Zur Rückrichtung der letzten Äquivalenz beachte man: Es existieren s und v aus $\mathcal{O}_K$ mit $D/\pi^{2k} = s^2 + 4v$, d.h. mit $t^2 - 4u = (\pi^k s)^2 + 4\pi^{2k} v$. Wir haben also

$$t^2 - (\pi^k s)^2 = (t - \pi^k s)(t + \pi^k s) \equiv 0 \mod 4\,.$$

Wegen $(t-\pi^k s)+(t+\pi^k s) = 2t \equiv 0 \mod 2$ schließen wir daraus $t \equiv \pi^k s \mod 2$. D.h. wir finden ein $a \in \mathcal{O}_K$ mit $t - \pi^k s = 2a$. Dieses a erfüllt offensichtlich die vorletzte Zeile unserer Äquivalenzkette. Damit ist die Aussage der Proposition bewiesen. □

Bevor wir nun zum Hauptergebnis dieser Arbeit gelangen, brauchen wir noch ein Lemma. Es sei noch einmal daran erinnert, dass wir das Hilbert-Symbol von K mit $(\cdot,\cdot)_K$ und das Artin-Schreier-Symbol von K mit $[\cdot,\cdot)_K$ bezeichnet hatten. Die beiden Symbole gaben uns die Möglichkeit, das Symbol $\left(\frac{\cdot,\cdot}{K}\right)$ zu berechnen (siehe die Sätze 3.3 und 3.24).

Lemma 5.24. *Es seien $k \in \mathbb{N}_0$, $a \in \mathcal{O}_K$ und $(t,u) \in \mathcal{O}_K^2$ so gewählt, dass $\delta_{a,k}(t,u) \in \mathcal{O}_K^2$ gilt.*

(i) Gilt $\mathrm{Char}(K) \neq 2$ und setzen wir $D := t^2 - 4u$, so folgt

$$\left(\frac{\delta_{a,k}(t,u)}{K}\right) = \begin{cases} 1 & \text{falls } u \in \mathcal{O}_K^* \text{ und } \left(\frac{D}{\pi^{2k}}, \pi\right)_K = 1 \text{ gilt,} \\ 0 & \text{falls } \frac{D}{\pi^{2k}} \in \mathfrak{p}_K \text{ gilt,} \\ -1 & \text{falls } u \in \mathcal{O}_K^* \text{ und } \left(\frac{D}{\pi^{2k}}, \pi\right)_K = -1 \text{ gilt.} \end{cases}$$

(ii) Im Fall $\mathrm{Char}(K) = 2$ haben wir

$$\left(\frac{\delta_{a,k}(t,u)}{K}\right) = \begin{cases} 1 & \text{falls } \frac{t}{\pi^k} \in \mathcal{O}_K^* \text{ und } \left[\frac{n}{t^2}, \pi\right)_K = 0 \text{ gilt,} \\ 0 & \text{falls } \frac{t}{\pi^k} \in \mathfrak{p}_K \text{ gilt,} \\ -1 & \text{falls } \frac{t}{\pi^k} \in \mathcal{O}_K^* \text{ und } \left[\frac{n}{t^2}, \pi\right)_K = 1 \text{ gilt.} \end{cases}$$

Beweis. Zu (i) : Wir setzen $(t', u') := \delta_{a,k}(t,u)$ und $D' := t'^2 - 4u'$. Mit Hilfe von Satz 3.3 und der Identität

$$\begin{aligned} D' &= \left(\frac{t-2a}{\pi^k}\right)^2 - 4\left(\frac{a^2 - ta + u}{\pi^{2k}}\right) \\ &= \frac{(t-2a)^2 - 4\,(a^2 - ta + u)}{\pi^{2k}} = \frac{D}{\pi^{2k}} \end{aligned}$$

erhalten wir offensichtlich Aussage (i).

Zu (ii) : Wir setzen wie oben $(t', u') := \delta_{a,k}(t, u)$ und verwenden Satz 3.24. Gilt $t' = \frac{t-2a}{\pi^k} = \frac{t}{\pi^k} \in \mathfrak{p}_K$, so ist offenbar nichts zu zeigen. Im Falle $t' \in \mathcal{O}_K^*$ haben wir, wenn wir uns die Aussage unseres Satzes 3.24 anschauen, noch die Gleichheit $\left[\frac{u'}{t'^2}, \pi\right)_K = \left[\frac{u}{t^2}, \pi\right)_K$ zu überprüfen. Erinnern wir uns daran, dass das Artin-Schreier-Symbol eigentlich eine Abbildung

$$K/\wp(K) \times K^*/K^{*2} \to \mathbb{F}_2$$

mit $\wp(x) := x^2 - x$ ist (siehe Satz 3.26 (iii)), so folgt

$$\begin{aligned}
\left[\frac{u'}{t'^2}, \pi\right)_K &= \left[\frac{(a^2 - ta + u)/\pi^{2k}}{(t/\pi^k)^2}, \pi\right)_K \\
&= \left[\frac{a^2 - ta + u}{t^2}, \pi\right)_K \\
&= \left[\wp\left(\frac{a}{t}\right) + \frac{u}{t^2}, \pi\right)_K \\
&= \left[\frac{u}{t^2}, \pi\right)_K .
\end{aligned}$$

Damit ist das Lemma bewiesen. $\square$

Nun können wir eine Formel für h angeben, so dass sich $h(t, u)$ nur anhand von $r(t, u)$ berechnen lässt. Dabei müssen wir nur h eingeschränkt auf M beschreiben, da h außerhalb von M identisch Null ist.

Satz 5.25. *(Hauptergebnis) Es sei* $(t,u) \in \mathcal{O}_K^2$.

Es gelte $Char(K) \neq 2$ *und* $d := r(t,u) < \infty$. *Setzen wir* $D := D(t,u) = t^2 - 4u$, *so erhalten wir*

$$h(t,u) = 1 + q^{-1} + \begin{cases} 0 & \textit{falls } \frac{D}{\pi^{2d}} \in \mathcal{O}_K^* \textit{ und } \left(\frac{D}{\pi^{2d}}, \pi\right)_K = 1 \textit{ gilt,} \\ -(1+q)q^{-d-2} & \textit{falls } \frac{D}{\pi^{2d}} \in \mathfrak{p}_K \textit{ gilt,} \\ -2q^{-d-1} & \textit{falls } \frac{D}{\pi^{2d}} \in \mathcal{O}_K^* \textit{ und } \left(\frac{D}{\pi^{2d}}, \pi\right)_K = -1 \textit{ gilt.} \end{cases}$$

Ist $Char(K) = 2$ *und gilt* $d := r(t,u) < \infty$, *so erhalten wir die Beziehung*

$$h(t,u) = 1 + q^{-1} + \begin{cases} 0 & \textit{falls } \frac{t}{\pi^{d}} \in \mathcal{O}_K^* \textit{ und } \left[\frac{u}{t^2}, \pi\right)_K = 0 \textit{ gilt,} \\ -(1+q)q^{-d-2} & \textit{falls } \frac{t}{\pi^{d}} \in \mathfrak{p}_K \textit{ gilt,} \\ -2q^{-d-1} & \textit{falls } \frac{t}{\pi^{d}} \in \mathcal{O}_K^* \textit{ und } \left[\frac{u}{t^2}, \pi\right)_K = 1 \textit{ gilt.} \end{cases}$$

Gilt $r(t,u) = \infty$, *so folgt in jeder Charakteristik* $h(t,u) = 1 + q^{-1}$.

Beweis. Es sei $d := r(t,u) < \infty$. Nach Voraussetzung gibt es ein $a \in \mathcal{O}_K$ mit $\delta_{a,d}(t,u) \in \mathcal{O}_K^2$ und d ist maximal mit dieser Eigenschaft. Auf Grund von Lemma 5.17 (i) haben wir dann $\delta_{a,i}(t,u) \in \mathcal{O}_K^2$ für alle $i \in \mathbb{N}_0$ mit $0 \leq i \leq d$. Es seien die Mengen $V_i \subset \mathcal{O}_K$ und $S_i \subset M$ für $i \in \mathbb{N}_0$ wie in der Vorbereitung zu Satz 5.18 gewählt. O.B.d.A. gelte $a \in V_i$ für $0 \leq i \leq d$, dann gilt für alle $i \in \mathbb{N}_0$

$$h_{S_i}(t,u) = \sum_{a' \in V_i} q^{-i} h_{S_0}(\delta_{a',i}(t,u)) = \begin{cases} q^{-i} h_{S_0}(\delta_{a,i}(t,u)) & \text{falls } i \leq d \text{ gilt,} \\ 0 & \text{sonst.} \end{cases}$$

Beachten wir nun, dass im Falle $0 \leq i < d$ die Beziehung

$$\delta_{a,i}(t,u) \in \pi\mathcal{O}_K^2 \text{ gilt und damit } \left(\frac{\delta_{a,i}(t,u)}{K}\right) = 0 \text{ folgt,}$$

so erhalten wir mit Hilfe der expliziten Formel 5.6 für h_{S_0} :

$$\begin{aligned} h(t,u) &= \sum_{i=0}^{\infty} h_{S_i}(t,u) \\ &= \sum_{i=0}^{d} q^{-i} h_{S_0}(\delta_{a,i}(t,u)) \\ &= \sum_{i=0}^{d-1} q^{-i}(1-q^{-1}) + q^{-d} h_{S_0}(\delta_{a,d}(t,u)) \ . \end{aligned}$$

Verwenden wir die Beziehung

$$\sum_{i=0}^{d-1} q^{-i}\left(1-q^{-2}\right) = \frac{1-q^{-d}}{1-q^{-1}}\left(1-q^{-2}\right) = 1 + q^{-1} - q^{-d-1} - q^{-d}$$

und abermals die Formel 5.6 und fassen zusammen, so erhalten wir:

$$h(t,u) = 1 + q^{-1} + \begin{cases} 0 & \text{falls } \left(\frac{\delta_{a,d}(t,u)}{K}\right) = 1 \text{ gilt} , \\ -(1+q)q^{-d-2} & \text{falls } \left(\frac{\delta_{a,d}(t,u)}{K}\right) = 0 \text{ gilt} , \\ -2q^{-d-1} & \text{falls } \left(\frac{\delta_{a,d}(t,u)}{K}\right) = -1 \text{ gilt} . \end{cases}$$

Daraus ergibt sich mit Hilfe von Lemma 5.24 die Behauptung für den Fall $r(t,u) < \infty$.

Es gelte nun für ein Paar $(t,u) \in \mathcal{O}_K^2$ die Beziehung $r(t,u) = \infty$. Wir geben zwei Beweise von $h(t,u) = 1 + q^{-1}$.

Erster Beweis. Auf Grund von $r(t,u) = \infty$ gibt es ein $a \in \mathcal{O}_K^2$ mit $\delta_{a,i}(t,u) = (0,0) \in \mathcal{O}_K^2$ für alle $i \in \mathbb{N}_0$ (siehe hierzu noch einmal den Beweis zur Proposition 5.21). Wir verwenden wieder die Konstruktion mit den Mengen S_i und V_i und setzen voraus, dass $a \in V_i$ für alle $i \in \mathbb{N}_0$ gilt. Auf Grund der Tatsache

$$\left(\frac{\delta_{a,i}(t,u)}{K}\right) = 0$$

für alle $i \in \mathbb{N}_0$ erhalten wir dann mit Hilfe der Formel 5.6

$$\begin{aligned} h(t,u) &= \sum_{i=0}^{\infty} h_{S_i}(t,u) \\ &= \sum_{i=0}^{\infty} q^{-i} h_{S_0}(\delta_{a,i}(t,u)) \\ &= \sum_{i=0}^{\infty} q^{-i}(1-q^{-1}) \\ &= 1 + q^{-1} . \end{aligned}$$

Zweiter Beweis. Da die Menge

$$W := \{(x,y) \in \mathcal{O}_K^2 : r(x,y) = \infty\}$$

offenbar abgeschlossen ist und kein Inneres besitzt (siehe Lemma 5.21), finden wir eine Folge $(a_n)_{n\in\mathbb{N}}$ in $\mathcal{O}_K^2 - W$ mit $a_n \to (t,u)$ für $n \to \infty$. Dann folgt $r(a_n) \to \infty$ für $n \to \infty$, da r stetig ist. Wegen $r(a_n) < \infty$ für alle $n \in \mathbb{N}$ folgt daher mit dem schon bewiesenen Teil des Satzes $h(a_n) \to 1 + q^{-1}$ für $n \to \infty$.

□

Korollar 5.26. *Die Dichte h von μ bezüglich α ist in einer Umgebung jedes Punktes $(t,u) \in \mathcal{O}_K^2$ mit $d := r(t,u) < \infty$ konstant. Genauer gilt*

$$h\left((t,u) + \pi^{2(d+1)}\mathcal{O}_K^2\right) = \{h(t,u)\} .$$

Beweis. Proposition 5.20 liefert uns

$$r\left((t,u)+\pi^{2(d+1)}\mathcal{O}_K^2\right)=\{d\}\ .$$

Auf Grund unseres Haupsatzes und des Lemmas 5.24 reicht es nun aus, für ein $a\in\mathcal{O}_K$ mit $\delta_{a,d}(t,u)\in\mathcal{O}_K^2$ und beliebige $(t',u')\in(t,u)+\pi^{2(d+1)}\mathcal{O}_K^2$ die Beziehungen $\delta_{a,d}(t',u')\in\mathcal{O}_K^2$ und

$$\left(\frac{\delta_{a,d}(t',u')}{K}\right)=\left(\frac{\delta_{a,d}(t,u)}{K}\right)$$

zu bestätigen. Dies ist aber Auf Grund der offensichtlichen Beziehung

$$\delta_{a,d}(t,u)-\delta_{a,d}(t',u')\in\pi\mathcal{O}_K^2$$

für alle zu betrachtenden Paare (t',u') klar. □

Nun erinnern wir uns noch einmal daran, dass wir für ein Paar $(t,u)\in\mathcal{O}_K^2$ und eine natürliche Zahl $k\in\mathbb{N}_0$

$$\gamma_k(t,u)=\#\left\{A\in\mathrm{Mat}(2,\mathcal{O}_K/\mathfrak{p}_K^k):\mathrm{Spur}(A)=t\mod\mathfrak{p}_K^k,\mathrm{Det}(A)=u\mod\mathfrak{p}_K^k\right\}$$

vereinbart hatten. Dann erhalten wir aus unserem Hauptergebnis die folgende Aussage:

Korollar 5.27. *Es sei* $(t,u) \in \mathcal{O}_K^2$ *mit* $d := r(t,u) < \infty$ *gewählt. Ferner erfülle* k *aus* $\mathbb{N}$ *die Beziehung* $k \geq 2 \cdot (d+1)$.

Ist $Char(K) \neq 2$ *und setzen wir* $D := D(t,u) = t^2 - 4u$, *so haben wir*

$$\gamma_k(t,u) = q^{2k} + q^{2k-1} + \begin{cases} 0 & \textit{falls } \frac{D}{\pi^{2d}} \in \mathcal{O}_K^* \textit{ und } \left(\frac{D}{\pi^{2d}}, \pi\right)_K = 1 \textit{ gilt,} \\ -(1+q)q^{2k-d-2} & \textit{falls } \frac{D}{\pi^{2d}} \in \mathfrak{p}_K \textit{ gilt,} \\ -2q^{2k-d-1} & \textit{falls } \frac{D}{\pi^{2d}} \in \mathcal{O}_K^* \textit{ und } \left(\frac{D}{\pi^{2d}}, \pi\right)_K = -1 \textit{ gilt.} \end{cases}$$

Gilt $Char(K) = 2$, *so erhalten wir*

$$\gamma_k(t,u) = q^{2k} + q^{2k-1} + \begin{cases} 0 & \textit{falls } \frac{t}{\pi^{d}} \in \mathcal{O}_K^* \textit{ und } \left[\frac{u}{t^2}, \pi\right)_K = 0 \textit{ gilt,} \\ -(1+q)q^{2k-d-2} & \textit{falls } \frac{t}{\pi^{d}} \in \mathfrak{p}_K \textit{ gilt,} \\ -2q^{2k-d-1} & \textit{falls } \frac{t}{\pi^{d}} \in \mathcal{O}_K^* \textit{ und } \left[\frac{u}{t^2}, \pi\right)_K = 1 \textit{ gilt.} \end{cases}$$

Beweis. Einerseits liefert uns Proposition 5.4 die Beziehung

$$\gamma_k(t,u) = \mu\left((t,u) + \pi^k \mathcal{O}_K^2\right) \cdot q^{4k} \ .$$

Andererseits ist die Dichte h von μ bezüglich α nach dem vorangehenden Korollar auf $(t,u) + \pi^k \mathcal{O}_K^2$ konstant gleich $h(t,u)$, d.h. es gilt

$$\begin{aligned} \mu\left((t,u) + \pi^k \mathcal{O}_K^2\right) &= \int_{(t,u)+\pi^k \mathcal{O}_K^2} h(x) d\alpha(x) \\ &= h(t,u) \cdot \alpha\left((t,u) + \pi^k \mathcal{O}_K^2\right) \\ &= h(t,u) q^{-2k} \ . \end{aligned}$$

Setzen wir die beiden gewonnenen Formeln zusammen, so folgt die Behauptung auf Grund unseres Hauptergebnisses. □

Bemerkung 5.28. Ganz allgemein haben wir für ein beliebiges $k \in \mathbb{N}_0$ die Beziehung

$$\gamma_k(t,u) = \mu\left((t,u) + \pi^k \mathcal{O}_K^2\right) \cdot q^{4k} = \int_{(t,u)+\pi^k \mathcal{O}_K^2} q^{4k} h(x) d\alpha(x) \ ,$$

wobei für kleine k der Integrand des Integrals auf der rechten Seite nicht konstant sein muss.

5.3 Beispiele und Bemerkungen

In den folgenden beiden Beispielen werden die im letzen Unterabschnitt gewonnenen Erkenntnisse speziell im Fall $K = \mathbb{Q}_p$ mit $p \in \mathbb{P}$ noch einmal veranschaulicht.

Beispiel 5.29. Es $K = \mathbb{Q}_2$, dann ist $\mathcal{O}_K = \mathbb{Z}_2$, $\mathfrak{p}_K = 2\mathbb{Z}_2$, $F_K = \mathbb{Z}_2/2\mathbb{Z}_2$ und $\#F_K = 2$.

Es gelte $t, u \in \mathbb{Z}_2$. Wir bilden $D = t^2 - 4u$. Beachten wir, dass $0 \mod 4$ und $1 \mod 4$ die einzigen Quadrate in $\mathbb{Z}_2/4\mathbb{Z}_2$ sind, so haben wir mit Hilfe der Propositionen 5.21 und 5.23

$$r(t,u) = \begin{cases} \sup\{k : 2^{2k}|D, D/2^{2k} \equiv 0,1 \mod 4\} & \text{falls } D \neq 0 \text{ gilt },\\ \infty & \text{sonst }. \end{cases}$$

Ferner erinnern wir uns an den Abschnitt über das Hilbert-Symbol $(\cdot,\cdot)_K$ und insbesondere daran, dass wir für $a \in \mathbb{Z}_2^* = 1 + 2\mathbb{Z}_2$ die schöne Beziehung

$$(a,2)_{\mathbb{Q}_2} = (-1)^{\frac{a^2-1}{8}}$$

gefunden hatten. Insbesondere gilt also $(a,2)_{\mathbb{Q}_2} = 1$, falls $a \equiv 1 \mod 8$ gilt und $(a,2)_{\mathbb{Q}_2} = -1$ in den Fällen $a \equiv 3 \mod 8$ und $a \equiv 5 \mod 8$. Wir definieren nun für ein beliebiges $a \in \mathbb{Z}_2$

$$\left(\frac{a}{2}\right) := \begin{cases} 1 & \text{falls } a \equiv 1 \mod 8 ,\\ 0 & \text{falls } 2|a \text{ gilt },\\ -1 & \text{sonst }. \end{cases}$$

Das Symbol $\left(\frac{\cdot}{2}\right)$ heißt *Kronecker-Symbol*. Jetzt gelte für ein Paar $(t,u) \in \mathbb{Z}_2^2$ die Beziehung $d := r(t,u) < \infty$. Wählen wir ein k aus $\mathbb{N}$ mit $k \geq 2d+2$, so erhalten wir mit Hilfe von Korollar 5.27 die Formel

$$\gamma_k(t,u) = 2^{2k} + 2^{2k-1} + \begin{cases} 0 & \text{falls } \left(\frac{D/2^{2d}}{2}\right) = 1\text{gilt},\\ -(1+2)2^{2k-d-2} & \text{falls } \left(\frac{D/2^{2d}}{2}\right) = 0 \text{ gilt},\\ -2\cdot 2^{2k-d-1} & \text{falls } \left(\frac{D/2^{2d}}{2}\right) = -1 \text{ gilt}. \end{cases}$$

Nun können wir z.B. die folgende Frage beantworten: Wie lautet die Anzahl N an Matrizen A in $\mathrm{Mat}(2, \mathbb{Z}/2^{17}\mathbb{Z})$, die $\mathrm{Spur}(A) = 5 \mod 2^{17}$ und $\mathrm{Det}(A) = 3 \mod 2^{17}$ erfüllen?

Antwort: Offensichtlich ist die gesuchte Anzahl gleich der Anzahl der Matrizen A aus $\mathrm{Mat}(2, \mathbb{Z}_2/2^{17}\mathbb{Z}_2)$ mit $\mathrm{Spur}(A) = 5 \mod 2^{17}$ und $\mathrm{Det}(A) = 3 \mod 2^{17}$. Deswegen können wir schauen, ob wir $\gamma_{17}(5,3)$ bestimmen können. Es gilt $D = 25 - 4\cdot 3 = 13 \equiv 1 \mod 4$. Also haben wir $d := r(5,3) = 0$. Wegen $17 \geq 2\cdot 0 + 2$ können wir somit die obige Formel anwenden. Wegen $D \equiv 13 \equiv 5 \mod 8$ haben wir $\left(\frac{D/2^{2d}}{2}\right) = -1$ und damit ergibt sich für unsere Zahl N:

$$N = \gamma_{17}(5,3) = 2^{2\cdot 17} + 2^{2\cdot 17-1} - 2\cdot 2^{2\cdot 17-0-1} = 17179869184 .$$

Beispiel 5.30. Nun sei $K = \mathbb{Q}_p$ mit $p > 2$ aus $\mathbb{P}$. Wir haben $\mathcal{O}_K = \mathbb{Z}_p$, $\mathfrak{p}_K = p\mathbb{Z}_p$, $F_K = \mathbb{Z}_p/p\mathbb{Z}_p$ und $\#F_K = p$.

Es seien t, u aus $\mathbb{Z}_p$. Wir bilden $D = t^2 - 4u$, dann haben wir mit Hilfe der Propositionen 5.21 und 5.23

$$r(t,u) = \begin{cases} \sup\{k : 2^{2k} | D\} & \text{falls } D \neq 0 \text{ gilt },\\ \infty & \text{sonst }. \end{cases}$$

Im Abschnitt über das Hilbert-Symbol haben wir gesehen, dass für alle $a \in \mathbb{Z}_p^*$

$$(a,p)_{\mathbb{Q}_p} = \left(\frac{a}{\mathbb{Q}_p}\right)$$

gilt (dabei ist $\left(\frac{\cdot}{K}\right)$ das Legendre-Symbol). Wir erweitern das Legendre-Symbol, wie das allgemein in der elementaren Zahlentheorie getan wird: Für $a \in \mathbb{Z}_p$ setzen wir

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{falls } p \nmid a \text{ gilt und } a \text{ ein Quadrat } \mod p \text{ ist },\\ 0 & \text{falls } p|a \text{ gilt },\\ -1 & \text{sonst }. \end{cases}$$

Es sei ein Paar $(t,u) \in \mathbb{Z}_p^2$ mit $d := r(t,u) < \infty$ gegeben. Wir bilden $D = t^2 - 4u$, dann haben wir auf Grund des Korollars 5.27 für jedes $k \in \mathbb{N}$ mit $k \geq 2d + 2$

$$\gamma_k(t,u) = p^{2k} + p^{2k-1} + \begin{cases} 0 & \text{falls } \left(\frac{D/p^{2d}}{p}\right) = 1 \text{gilt},\\ -(1+p)p^{2k-d-2} & \text{falls } \left(\frac{D/p^{2d}}{p}\right) = 0 \text{ gilt},\\ -2 \cdot p^{2k-d-1} & \text{falls } \left(\frac{D/p^{2d}}{p}\right) = -1 \text{ gilt}. \end{cases}$$

Bemerkung 5.31.

(i) Die in den beiden vorangehenden Beispielen angegebenen Formeln für $\gamma_k(t,u)$ über den Körpern $K = \mathbb{Q}_p$ sind exakt die, die bei Gekeler bewiesen werden. Siehe hierzu Gekeler ([4], Prop. 3.10).

(ii) Es bleibt nun das Problem, Formeln für die Dichten h_n zu finden. Diese sind schon auf Grund der Proposition 5.4 von Interesse.

6 Symbolverzeichnis

Im der ganzen Arbeit bezeichne

$\mathbb{N}$	die Menge der natürlichen Zahlen, d.h. die Menge $\{1,2,3,4,...\}$, 8
$\mathbb{N}_0$	die Menge $\mathbb{N}\cup\{0\}$, 8
$\mathbb{N}_n$	für $n\in\mathbb{N}$ die Menge $\{1,2,3,...,n\}$, 8
$\mathbb{P}$	die Menge der Primzahlen, 8
$\mathbb{Z}$	die ganzen Zahlen, 8
$\mathbb{Q}$	die rationalen Zahlen, 8
$\mathbb{F}_q$	der endliche Körper mit $q=p^f$ Elementen, 8
$\widehat{\mathbb{R}}$	die Menge $\mathbb{R}\cup\{-\infty,+\infty\}$, also die Kompaktifizierung von $\mathbb{R}$, 8
$\mathrm{Mat}(n,m,R)$	die $n\times m-$Matrizen über dem Ring R, 8
$\mathrm{Mat}(n,R)$	die Menge $\mathrm{Mat}(n,n,R)$, 8
$\mathrm{GL}(n,R)$	die invertierbaren Matrizen aus $\mathrm{Mat}(n,R)$, 8
$R[X_1,...,X_m]$	der Polynomring in den Variablen $X_1,X_2,...,X_m$ über R, 9
$\mathrm{N}_{L\|K},\mathrm{Tr}_{L\|K}$	Norm und Spur der Erweiterung $L\|K$, 9
$\overline{K}$	ein fester algebraischer Abschluss von K, 9
$\mathcal{O}_K,v_K,\mathfrak{p}_K,F_K$	der Ganzheitsring, die Bewertung, das Primideal, der Restkörper des lokalen Körpers K, 10
$\|\cdot\|_K$	der Betrag des lokalen Körpers K, 11
$\mathbb{Q}_p$	für $p\in\mathbb{P}$ der Körper der $p-$adischen Zahlen, 12
$\mathbb{Z}_p$	die $p-$adischen ganzen Zahlen, 12
$k((t))$	der Laurentreihenkörper über dem Körper k, 12
$\sum_{i\gg-\infty}s_it^i$	ein Element von $k((t))$, 12
$E_m(K)$	die Gruppe der $m-$ten Einheitswurzeln in K, 16
$U_K^{(n)}$	die Gruppe der $n-$ten Eins-Einheiten von K, 16
$\left(\frac{\cdot,\cdot}{K}\right)$	ein Symbol, 19

$(\cdot,\cdot)_K$	das Hilbert-Symbol, 20
$\left(\frac{\cdot}{K}\right)$	das Legendre Symbol, 23
$[\cdot,\cdot)_K$	das Artin-Schreier-Symbol, 34
$\wp$	der Operator $x \to x^2 - x$ über Körpern der Charakteristik 2, 35
$\mathcal{M}(\mu, X)$	die für ein Maß μ auf dem Raum X messbaren Funktionen $f : X \to \widehat{\mathbb{R}}$, 38
$\mathcal{B}(X)$	die Borel-Mengen eines topologischen Raumes X, 40
$f(\mu)$	das Bild des Maßes μ unter der Abbildung f, 41
$\mu \times \nu$	das Produkt-Maß von μ und ν, 41
$Df(a), Jf(a)$	die Jacobi-Matrix bzw. die Jacobische von f im Punkt a, 48
$\mathcal{T}(X)$	die kompakt-offenen Mengen eines topologischen Raumes X. 51

Literatur

[1] Emil Artin. *Algebraic numbers and algebraic functions.* Gordon and Breach Science Publishers, New York, 1967.

[2] Helmut Brückner. Eine explizite Formel zum Reziprozitätsgesetz für Primzahlexponenten p. In *Algebraische Zahlentheorie (Ber. Tagung Math. Forschungsinst. Oberwolfach, 1964)*, pages 31–39. Bibliographisches Institut, Mannheim, 1967.

[3] Jürgen Elstrodt. *Maß- und Integrationstheorie*, volume 2. Springer, Berlin, 1999.

[4] Ernst-Ulrich Gekeler. Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.*, (37):1999–2018, 2003.

[5] Jun-ichi Igusa. *An introduction to the theory of local zeta functions*, volume 14 of *AMS/IP Studies in Advanced Mathematics.* American Mathematical Society, Providence, RI, 2000.

[6] Serge Lang. *Algebra.* Addison-Wesley Publishing Co., Inc., Reading, Mass., 1965.

[7] Serge Lang and Hale Trotter. *Frobenius distributions in* GL_2*-extensions.* Springer-Verlag, Berlin, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers, Lecture Notes in Mathematics, Vol. 504.

[8] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer-Verlag, Berlin Heidelberg, 1992.

[9] Shankar Sen. On explicit reciprocity laws. II. *J. Reine Angew. Math.*, 323:68–87, 1981.

[10] Jean-Pierre Serre. *Groupes algébriques et corps de classes.* Publications de l'institut de mathématique de l'université de Nancago, VII. Hermann, Paris, 1959.

[11] Jean-Pierre Serre. *Corps locaux.* Hermann, Paris, 1968. Deuxième édition, Publications de l'Université de Nancago, No. VIII.

[12] Jean-Pierre Serre. *Local algebra.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2000. Translated from the French by CheeWhye Chin and revised by the author.

[13] S. V. Vostokov. An explicit form of the reciprocity law. *Izv. Akad. Nauk SSSR Ser. Mat.*, 42(6):1288–1321, 1439, 1978.

[14] André Weil. *Basic number theory.* Die Grundlehren der mathematischen Wissenschaften, Band 144. Springer-Verlag New York, Inc., New York, 1967.