SIGRID BÖGE

ORTHOGONALE GRUPPEN
UND DER SATZ VON MINKOWSKI-SIEGEL

$\tau(G)=2$

UNIVERSITÄTS-
BIBLIOTHEK
HEIDELBERG

ORTHOGONALE GRUPPEN UND DER SATZ VON MINKOWSKI-SIEGEL

Sigrid Böge

Orthogonale Gruppen und der Satz von Minkowski-Siegel

Vorlesung Wintersemester 2016/17

UNIVERSITÄTS-
BIBLIOTHEK
HEIDELBERG

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation
in der Deutschen Nationalbibliografie. Detaillierte bibliografische Daten
sind im Internet unter http://dnb.ddb.de abrufbar.

UNIVERSITÄTS-
BIBLIOTHEK
HEIDELBERG

Publiziert bei heiBOOKS,
Universitätsbibliothek Heidelberg 2018.

Die Online-Version dieser Publikation ist auf heiBOOKS, der E-Book-Plattform
der Universitätsbibliothek Heidelberg, http://books.ub.uni-heidelberg.de/heibooks,
dauerhaft frei verfügbar (Open Access).
urn: urn:nbn:de:bsz:16-heibooks-book-386-9
doi: https://doi.org/10.11588/heibooks.386.551

ISBN 978-3-946531-86-9 (Softcover)
ISBN 978-3-946531-87-6 (PDF)

Inhalt

Vorwort

Dieses Manuskript ist aus einer Vorlesung entstanden, die ich im Wintersemester 2016/17 in Heidelberg gehalten habe. Ziel war es, junge Studenten an ein Thema heranzuführen, das sie in einer Bachelor-Arbeit oder, wenn sie sich noch intensiver damit beschäftigen würden, in einer Master-Arbeit bearbeiten können. Der Reiz für mich bestand darin, wirklich im Einzelnen und mit allen Formeln in Evidenz zu setzen, daß die Minkowski-Siegel'sche Formel in der großen Arbeit von C. L. Siegel aus dem Jahre 1935 äquivalent ist zu der Aussage, daß die Tamagawa-Zahl der speziellen orthogonalen Gruppe in Dimension $m \geq 3$ (zunächst zu einer positiv definiten quadratischen Form) gleich 2 ist. Jeder weiß das, aber niemand hat das im Einzelnen vorgerechnet. Außerdem kann man die Formeln benutzen, um Darstellungen von Zahlen durch Formen (zum Beispiel Quadratsummen) zu betrachten. Den Ansatz dazu habe ich dem Buch von M. Kneser über quadratische Formen entnommen.

So ist das vorliegende Manuskript zwar einem speziellen Thema gewidmet. Es werden aber (grundlegende) Hilfsmittel aus verschiedenen Gebieten (Integration, Fourieranalysis, p-adische Zahlen, Funktionentheorie) benutzt. Da ich die Vorlesung für junge Studenten gedacht hatte, habe ich mir Mühe gegeben, Beweise wirklich auszuführen, zur Bequemlichkeit des Lesers. Vielleicht ist die Vorlesung auf diese Weise ein bißchen ein Zwitter, elementar und speziell zugleich: ich wollte mit wenigen Vorkenntnissen ein interessantes Ziel erreichen. Kundige Leser können ja die mehr elementaren Ausführungen überspringen.

Zum Ablauf der Vorlesung: Das Kapitel 18 habe ich an der Tafel nicht vorgerechnet, die Zeit reichte nicht, und es ist dafür auch nicht besonders geeignet. Es ist dem Seminar "Adeles and Algebraic Groups" von A. Weil entnommen. Dort sind gleichzeitig verschiedene Typen klassischer Matrizengruppen behandelt. Dadurch ist der Beweis sehr lang und mehrmals durch Fallunterscheidungen unterbrochen. Ich habe für den Zweck der Vorlesung den Fall der speziellen orthogonalen Gruppen (und dann auch noch zu positiv definiten Formen) herauspräpariert und so versucht, den Beweis möglichst durchsichtig (und wesentlich kürzer) aufzuschreiben. Das Kapitel 17 hat (zur Hälfte) ein Student in der parallel laufenden Übung vorgeführt. Die Minkowski'schen Ungleichungen (Kapitel 5 und 6) habe ich in dieser Form in der Literatur nicht bewiesen gefunden, sie sind aber natürlich nicht neu. In Kapitel 8 habe ich eine fast überall definierte invariante Differentialform höchsten Grades auf der speziellen orthogonalen Gruppe über $\mathbb{Q}$ beschrieben. Diese konnte ich nirgends in der Literatur finden und wäre für einen entsprechenden Hinweis sehr dankbar. Man kann mit ihr die Integrale im Reellen und über allen $\mathbb{Q}_p$ ausrechnen und so den Zusammenhang mit den Siegel'schen Darstellungszahlen herstellen.

Ich danke Kathrin Maurischat und Burak Cakir für die Hilfe beim Korrekturlesen.

1. Aufbau der orthogonalen Gruppe

K sei ein Körper der Charakteristik $\neq 2$ und V ein n-dimensionaler Vektorraum über K mit einer nicht ausgearteten symmetrischen Bilinearform $(\ ,\ )$. Ein Vektor $u \in V$ heißt isotrop, wenn $u \neq 0$ und $(u,u) = 0$. Ein Teilraum U von V heißt total isotrop, wenn $(x,y) = 0$ für alle $x, y \in U$.

Sei u isotrop. Da $(\ ,\ )$ nicht ausgeartet, gibt es $v_1 \in V$ mit $(u, v_1) = 1$. Für $v := v_1 - \frac{1}{2}(v_1, v_1)\, u$ gilt

$$(u,u) = (v,v) = 0, \quad (u,v) = 1$$

Man nennt u, v ein hyperbolisches Paar. Sei H die von u und v aufgespannte Ebene. Ist $x \in V$ beliebig, so ist

$$x - (x,u)v - (x,v)u \in H^\perp$$

Das zeigt

$$V = H \perp H^\perp$$

Auf $H^\perp$ ist $(\ ,\ )$ ebenfalls nicht ausgeartet. Sollte es in $H^\perp$ einen isotropen Vektor u_2 geben, so finden wir wie oben $v_2 \in H^\perp$, so daß u_2, v_2 ein hyperbolisches Paar bilden. Auf diese Weise finden wir paarweise senkrechte hyperbolische Ebenen H_i, so daß

$$V = H_1 \perp ..... \perp H_r \perp W,$$

und W enthält keinen isotropen Vektor mehr. Ein solches W nennt man anisotrop.

Analog zur bekannten Zerlegung einer reellen invertierbaren Matrix in "dreieckig mal orthogonal" wollen wir die spezielle orthogonale Gruppe

$$G = \{g \in GL(V) \mid (gx, gy) = (x,y) \text{ für alle } x, y \in V \text{ und } \det g = 1\}$$

zerlegen. Dazu sei

$$B = \{b \in G \mid bu_i \in \sum_{j \leq i} K\, u_j \text{ für } i = 1, ..., r\}$$

$$D = \{d \in G \mid du_i = \alpha_i u_i,\ dv_i = \frac{1}{\alpha_i} v_i,\ dw = w \text{ für alle } w \in W\} \quad (\alpha_i \in K^*)$$

Wir schreiben dafür auch $d = (\alpha_1, ..., \alpha_r)$.

Zerlegung von B: Besteht $d \in D$ aus den ersten r Diagonalelementen von b, so ist $d^{-1}bu_i \in u_i + \sum_{j<i} K u_j$. Insbesondere ist $d^{-1}bu_1 = u_1$. Aus Isometriegründen ist dann $d^{-1}bv_1 = v_1 + a_1 - \frac{1}{2}(a_1, a_1)u_1$ mit $a_1 \in H_1^\perp$

Definition: Ist u, v ein hyperbolisches Paar und $a \in H^\perp = u^\perp \cap v^\perp$, so heißt

$$\phi_{u,a} x = x + (x,u)a - (x,a)u - \frac{1}{2}(x,u)(a,a)u$$

eine Eichlertransformation.

Man rechnet nach, daß $\phi_{u,a}$ eine Isometrie mit Determinante 1 ist und daß $\phi_{u,a}\phi_{u,b} = \phi_{u,a+b}$. Vermöge $a \leftrightarrow \phi_{u,a}$ bilden die Eichlertransformationen $\phi_{u,a}$ mit festem u eine zur additiven Gruppe von $H^\perp$ isomorphe Untergruppe von G. (Bemerkung: Die

Eichlertransformationen hängen von v gar nicht ab, aber die Gruppe der $\phi_{u,a}$ ist wegen $\phi_{u,a} = \phi_{u,a+\lambda u}$ nur isomorph zu $u^\perp/Ku$, und das ist zu $H^\perp$ isomorph, wenn H irgendeine hyperbolische Ebene ist, die u enthält).

Sind nun d und b wie oben, so ist offenbar

$$d^{-1}bu_1 = u_1 = \phi_{u_1,a_1}u_1 \text{ und } d^{-1}bv_1 = \phi_{u_1,a_1}v_1$$

so daß also $\psi := \phi_{u_1,a_1}^{-1}d^{-1}b$ die Ebene H_1 elementweise fest läßt und als orthogonale Transformation von $H_1^\perp$ aufgefaßt werden kann. Für $i \geq 2$ findet man

$$\psi u_i = \phi_{u_1,a_1}^{-1}(u_i + \sum_{j<i}\lambda_{ji}u_j) = u_i + (u_i,a_1)u_1 + \sum_{j<i}\lambda_{ji}(u_j + (u_j,a_1)u_1) \in u_i + \sum_{j<i}Ku_j$$

insbesondere, da $\psi u_i \in H_1^\perp$, auch $\psi u_2 = u_2$. Daher kann man mit ψ in $H_1^\perp$ verfahren wie mit $d^{-1}b$ in V und findet schrittweise

$$b = d \cdot \phi_{u_1,a_1}.....\phi_{u_r,a_r} \cdot q$$

mit $a_i \in W^i := H_{i+1} \perp .... \perp H_r \perp W$ und einer orthogonalen Transformation q von W. Dabei gelten die Vertauschungsregeln

(1) $$d\phi_{u_i,a_i} = \phi_{u_i,\alpha_i da_i}\, d, \text{ wenn } d = (\alpha_1, ..., \alpha_r)$$

(2) $$\phi_{u_i,a_i}\phi_{u_j,a_j} = \phi_{u_j,\phi_{u_i,a_i}a_j}\phi_{u_i,a_i} \text{ für } j < i$$

weil $\phi_{u_i,a_i}u_j = u_j$ für $j < i$, und

(3) $$q \cdot \phi_{u_i,a_i} = \phi_{u_i,qa_i} \cdot q \text{ für } q \in G(W)$$

Die Gruppe B ist also ein semidirektes Produkt von K^{*r} mit Untergruppen, die zu den additiven Gruppen von $K^{n-2}, K^{n-4}, ..., K^{n-2r}$ isomorph sind, das Ganze mal der Gruppe $G(W)$.

Iwasawa-Zerlegung, reell: W ist anisotrop über $\mathbb{R}$ und daher positiv oder negativ definit. Nehmen wir an, W sei positiv definit. Wir setzen

$$e_i = \frac{u_i + v_i}{\sqrt{2}}, \quad f_i = \frac{u_i - v_i}{\sqrt{2}}, \quad u_i = \frac{e_i + f_i}{\sqrt{2}}, \quad v_i = \frac{e_i - f_i}{\sqrt{2}}$$

und

$$V^+ = (\sum_{i=1}^{r}\mathbb{R}e_i) \perp W, \quad V^- = \sum_{=1}^{r}\mathbb{R}f_i$$

V^+ ist positiv definit, V^- negativ definit, $V = V^+ \perp V^-$, und wenn $O(V)$ die volle orthogonale Gruppe von V bezeichnet, dann ist $K := G \cap (O(V^+)O(V^-))$ eine kompakte Untergruppe von G.

Lemma 1.

$$G = K \cdot B$$

Beweis: Für $r = 0$ und alle n ist $G = K$. Für $r = 1$ und $n = 2$ ist $G = B(= D)$. Für den Rest des Beweises sei $r \geq 1$ und $n \geq 3$. Sei $g \in G$ und $gu_1 = x + y$ mit $x \in V^+$ und $y \in V^-$. Dann ist $(x,x) + (y,y) = 0$ und $(x,x) > 0$. Mit $\rho := \sqrt{(x,x)} > 0$ ist $(x,x) = (\rho e_1, \rho e_1)$ und $(y,y) = (\rho f_1, \rho f_1)$. Es gibt $m^+ \in O(V^+)$ und $m^- \in O(V^-)$ mit $x = \rho m^+ e_1$ und $y = \rho m^- f_1$. Mit $m := m^+ m^-$ (das wir zur Not, weil V^+ oder V^- mindestens zweidimensional ist, so abändern können, daß $\det m = 1$), also $m \in K$, ist

$$gu_1 = x + y = \rho m(e_1 + f_1) = \rho m\sqrt{2}\, u_1$$

Wir definieren $d \in D$ durch $du_1 = \rho\sqrt{2}\, u_1$, $dv_1 = \frac{1}{\rho\sqrt{2}} v_1$ und $dx = x$ für $x \in H_1^\perp$ und haben $d^{-1}m^{-1}gu_1 = u_1$. Dann gibt es, wie schon gesehen, $a_1 \in W^1$ mit $\phi_{u_1,a_1}^{-1} d^{-1}m^{-1}g \in G(W^1)$. Sind K_1 und B_1 die analog zu K und B für W^1 definierten Untergruppen, so folgt nach Induktionsannahme

$$g \in md\phi_{u_1,a_1} K_1 B_1 \subset mK_1 d\phi_{u_1,W^1} B_1 = K \cdot B$$

Zusatz: Es war $B = \{d \cdot \phi_{u_1,a_1} .... \phi_{u_r,a_r} \cdot q \mid d \in D,\ a_i \in W^i,\ q \in G(W)\}$. Nun ist aber $G(W) \subset K$, und nach den Vertauschungsregeln kann man q an den ϕ_{u_i,a_i} vorbeiziehen und zu K schlagen. Setzen wir also

$$N = \{\phi_{u_1,a_1} .... \phi_{u_r,a_r} \mid a_i \in W^i\}$$

dann gilt sogar

$$G = K \cdot D \cdot N$$

Das ist die Iwasawa-Zerlegung der reellen orthogonalen Gruppe.

Iwasawa-Zerlegung, p-adisch : Sei jetzt $K = \mathbb{Q}_p$. Mit $\mathfrak{o}_p$ wird der Ring der ganzen p-adischen Zahlen bezeichnet, also

$$\mathfrak{o}_p = \{\lambda \in \mathbb{Q}_p \mid |\lambda|_p \leq 1\}$$

Wir benutzen die durch $|p|_p = \frac{1}{p}$ normierte p-adische Bewertung. Um eine kompakte Untergruppe von G zu definieren, benutzt man Gitter.

Wir benutzen je nach Zweck zwei Definitionen von Gitter:

Sei R ein Hauptidealring und K sein Quotientenkörper. Ferner sei V ein n-dimensionaler Vektorraum über K mit Basis $e_1, ..., e_n$.

Definition 1. Eine Teilmenge M von V heißt Gitter (genauer R-Gitter), wenn

1. M eine additive Untergruppe von V ist
2. $RM = M$
3. Es gibt $a, b \neq 0$ in R, so daß

$$a \cdot (Re_1 + ... + Re_n) \subset M \subset b^{-1}(Re_1 + ... + Re_n)$$

Definition 2. Eine Teilmenge M von V heißt Gitter, wenn V eine Basis $u_1, ..., u_n$ über K besitzt, so daß

$$M = Ru_1 + ... + Ru_n$$

Zusatz: Wenn V mit einer Form $(\ ,\ )$ ausgestattet ist, nimmt man $(e_i, e_j) \in R$ und verlangt $(M, M) \subset R$.

Wir beweisen die Äquivalenz der beiden Definitionen:

$1 \Rightarrow 2$: Nach Multiplikation mit b sei oE $M \subset Re_1 + ... + Re_n$. (An dieser Stelle wird Bedingung 3 benutzt). Dann besitzt jedes $x \in M$ eine Darstellung $x = \lambda_1 e_1 + ... + \lambda_n e_n$ mit $\lambda_i \in R$. Wenn x durch M läuft, dann läuft λ_1 durch ein Ideal in R. Da R ein Hauptidealring ist, besteht dieses aus den Vielfachen einer Zahl $\alpha_1 \neq 0$. Dieses α_1 ist selbst erster Koeffizient eines Vektors $u_1 \in M$:

$$u_1 = \alpha_1 e_1 + \text{ Linearkombination von } e_2, ..., e_n$$

Ist nun $x = \lambda_1 e_1 + ... + \lambda_n e_n$ beliebig in M, so ist λ_1 ein Vielfaches von α_1, etwa $\lambda_1 = \mu\alpha_1$. Dann ist

$$x - \mu u_1 \in M \cap (Re_2 + ... + Re_n)$$

Der letzte Modul erfüllt wieder die drei Bedingungen aus Definition 1 und besitzt nach Induktionsannahme eine Basis $u_2, ..., u_n$ über R.

$2 \Rightarrow 1$: Sei $u_1, ..., u_n$ eine Basis von V über K und $M = Ru_1 + ... + Ru_n$. Es gibt a_{ij} und b_{ij} in K mit

$$u_i = \sum_j a_{ji} e_j \quad \text{und } e_i = \sum_j b_{ji} u_j$$

Da K der Quotientenkörper von R ist, gibt es a und b in R, beide $\neq 0$, so daß alle $a \cdot a_{ij} \in R$ und alle $b \cdot b_{ij} \in R$. Dann ist $aM = Rau_1 + ... + Rau_n \subset Re_1 + ... + Re_n$ und genauso $b(Re_1 + ... + Re_n) \subset Ru_1 + ... + Ru_n = M$.

Wir wenden das an, wenn $K = \mathbb{Q}_p$ und $R = \mathfrak{o}_p$ ist. Zunächst folgt, daß die orthogonalen Transformationen, die ein Gitter in sich abbilden, durch Matrizen mit Einträgen in $\mathfrak{o}_p$ beschrieben werden können. Deshalb bilden sie eine kompakte Untergruppe von G

Lemma 2. *Wenn W anisotrop, dann bilden die $x \in W$ mit $|\frac{1}{2}(x, x)| \leq 1$ ein Gitter in W.*

Beweis: Wir verifizieren die Eigenschaften in Definition 1:
1. Sei $|\frac{1}{2}(x, x)| \leq 1$ und $|\frac{1}{2}(y, y)| \leq 1$. Zu zeigen ist $|\frac{1}{2}(x + y, x + y)| \leq 1$. Wäre dies nicht der Fall, so wäre nach der scharfen Dreiecksungleichung $|(x, y)| > 1$. Sei oE $0 < |(x, x)| \leq |(y, y)|$. Dann betrachten wir das Polynom

$$P(\lambda) = \frac{1}{(y,y)} \cdot (x + \lambda y, x + \lambda y) = \lambda^2 + 2\lambda \frac{(x,y)}{(y,y)} + \frac{(x,x)}{(y,y)}$$

$$= (\lambda + \frac{(x,y)}{(y,y)})^2 - (\frac{(x,y)}{(y,y)})^2 \cdot (1 - \frac{(x,x)(y,y)}{(x,y)^2})$$

Wegen der Voraussetzungen über x und y ist die letzte Klammer $\equiv 1 \bmod 4p$, und daher ein Quadrat. Somit hat das Polynom $P(\lambda)$ eine Nullstelle entgegen der Annahme, daß W anisotrop ist.

2. Das ist trivial.

3. Sei $e_1, ..., e_n$ eine Basis von W über $\mathbb{Q}_p$ und $M = \{x \in W \mid |\frac{1}{2}(x,x)| \leq 1\}$. Offenbar gibt es k mit $p^{2k} \cdot \frac{1}{2}(e_i, e_j) \in \mathfrak{o}_p$ für $i, j = 1, ..., n$, und für ein solches k ist

$$p^k(\mathfrak{o}_p e_1 + ... + \mathfrak{o}_p e_n) \subset M$$

Ist umgekehrt $x = \sum_{i=1}^n \xi_i e_i \in M$ (mit $\xi_i \in \mathbb{Q}_p$), so ist $(x, p^k e_i) \in \mathfrak{o}_p$ für alle i (denn nach 1. ist $(x,y) \in \mathfrak{o}_p$ für alle $x, y \in M$), das heißt

$$\sum_{i=1}^n \xi_i(e_i, e_j) \in p^{-k}\mathfrak{o}_p \text{ für } j = 1, ..., n$$

Ist D die Determinante der Matrix (e_i, e_j), so folgt $\xi_i \in \frac{1}{D}p^{-k}\mathfrak{o}_p$, also

$$M \subset \frac{1}{D}p^{-k}(\mathfrak{o}_p e_1 + ...\mathfrak{o}_p e_n)$$

Damit ist 3. bewiesen.

Definition: Sind $u_i, v_i,\ i = 1, ..., r$ paarweise senkrechte hyperbolische Paare und ist

$$V = \perp_{i=1}^r (\mathbb{Q}_p u_i + \mathbb{Q}_p v_i) \ \perp \ W$$

mit anisotropem W, so nennen wir

$$M := \perp_{i=1}^r (\mathfrak{o}_p u_i + \mathfrak{o}_p v_i) \ \perp \ \{x \in W \mid |\frac{1}{2}(x,x)| \leq 1\}$$

ein Standardgitter in V.

$G(M)$ bezeichnet die Gruppe aller $\phi \in G$ mit $\phi M = M$.

Lemma 3. *Sei $n \geq 3$ und M ein Standardgitter in V. Sind a und b primitiv und isotrop in M, dann gibt es $\phi \in G(M)$ mit $\phi a = b$.*

Beweis: Natürlich genügt es zu zeigen: es gibt $\phi \in G(M)$ mit $\phi a = u_1$. Sei $a = \sum_i \alpha_i u_i + \sum_i \beta_i v_i + w \in M$.
1. Fall: $|\beta_j| = 1$. Es gibt Spiegelungen mit

$$a \mapsto \begin{cases} u_1 & \text{wenn } j = 1 \\ u_j \mapsto v_j + v_1 \mapsto u_1 & \text{wenn } j > 1 \end{cases}$$

2. Fall: $|\alpha_j| = 1$. Es gibt Spiegelungen mit

$$a \mapsto v_j \mapsto \begin{cases} u_j & \text{falls } j = 1 \\ u_j + v_1 \mapsto u_1 & \text{falls } j > 1 \end{cases}$$

In jedem Falle gibt es in $M \cap u_1^\perp \supset M \cap \{\sum_{i=2}^r (\mathfrak{o}_p u_i + \mathfrak{o}_p v_i)\} \ \perp (M \cap W)$, weil $n \geq 3$, einen Spiegelungsvektor s (so daß die Spiegelung S längs s das Gitter M in sich abbildet). Sollte das in 1 und 2 angegebene Produkt aus ungerade vielen Spiegelungen bestehen, kann man noch S anfügen und erhält in jedem Falle ein $\phi \in G(M)$ mit $\phi a = u_1$.

3. Fall: Alle $|\alpha_j| < 1$ und alle $|\beta_j| < 1$. Dann ist $\frac{1}{2}(w,w) \equiv 0 \bmod p^2$ und $\frac{1}{p}a \in M$, also a nicht primitiv.

$G(M)$ ist eine kompakte Untergruppe von G. Wir bezeichnen sie mit K und nennen sie eine Standard-kompakte Untergruppe.

Zerlegung von G: Sei $g \in G$ und $\lambda \in \mathbb{Q}_p^*$ so. daß $\lambda g u_1$ ein primitiver Vektor in M ist. Nach dem Lemma gibt es $m \in K$ mit $mu_1 = \lambda g u_1$. Ist d definiert durch $du_1 = \lambda u_1$, $dv_1 = \frac{1}{\lambda}v_1$ und $dx = x$ für $x \in H_1^\perp$, so ist

$$m^{-1}gdu_1 = u_1,\ m^{-1}gdv_1 = v_1 + a_1 - \frac{1}{2}(a_1,a_1)u_1 = \phi_{u_1,a_1}v_1$$

mit $a_1 \in H_1^\perp$. Wir können also $\phi_{u_1,a_1}^{-1}m^{-1}gd$ als orthogonale Transformation von $H_1^\perp$ ansehen. Nach Induktionsannahme ist $\phi_{u_1,a_1}^{-1}m^{-1}gd = m_1b_1$ mit $m_1 \in K_1 := G(H_1^\perp \cap M)$ und $b_1u_i \in \sum_{j\le i}\mathbb{Q}_p u_j$. Dann wird (wegen $m_1u_1 = u_1$)

$$g = m\phi_{u_1,a_1}m_1b_1d^{-1} = mm_1\phi_{u_1,m_1^{-1}a_1}b_1d^{-1} \in K \cdot B$$

Auch hier haben wir wieder die Zusatzbemerkung: Wenn N wie oben im Falle $\mathbb{R}$ definiert ist, dann ist $B = DNG(W)$. Nach Definition des Gitters in W als $\{x \in W \mid |\frac{1}{2}(x,x)| \le 1\}$ ist dieses zwangsläufig invariant unter $G(W)$, also $G(W) \subset K$. Nach den Vertauschungsregeln ist nun sogar

$$G = K \cdot DN$$

Das ist die lokale Iwasawa-Zerlegung.

2. Adelisierung

1. Der Adelring von $\mathbb{Q}$.

Definition : Ein Adel ist ein Tupel $(x_\infty, ..., x_p, ...)$ mit

$$x_\infty \in \mathbb{R},\ x_p \in \mathbb{Q}_p \text{ für alle Primzahlen } p \text{ und } x_p \in \mathfrak{o}_p \text{ für fast alle } p$$

Die Adele bilden bei komponentenweiser Addition und Multiplikation einen Ring A, den sogenannten Adelring von $\mathbb{Q}$. Für jede endliche Menge S, welche ∞ enthält, bezeichne

$$A_S = \prod_{v \in S} \mathbb{Q}_v \ \times \prod_{p \notin S} \mathfrak{o}_p$$

Offenbar ist

$$A = \cup_{endliche\ S}\ A_S \tag{1}$$

A_S wird mit der Produkttopologie versehen ([Sch], Seite 31), und A wird so topologisiert, daß eine Teilmenge von A genau dann offen ist, wenn ihr Durchschnitt mit allen A_S offen in A_S ist. Konkret bedeutet das:
Die

$$W_{\epsilon,S} = \{x = (x_v)_v \mid |x_v|_v < \epsilon \text{ für } v \in S \text{ und } x_p \in \mathfrak{o}_p \text{ für } p \notin S\}$$

wo S alle endlichen Mengen von Bewertungen und ϵ alle reellen Zahlen > 0 durchläuft, bilden ein Fundamentalsystem von Nullumgebungen in A, und eine Teilmenge von A ist genau dann offen, wenn sie mit jedem a auch ein passendes $a + W_{\epsilon,S}$ enthält.
Nach dem Satz von Tychonoff ([Sch], Seite 67) sind alle A_S lokal kompakt, und damit ist auch A lokal kompakt. Dies ist ein Grund dafür, daß man nicht das volle direkte Produkt der $\mathbb{Q}_v$ betrachtet, sondern das "eingeschränkte direkte Produkt" (1).

Lemma 1. *Eine Teilmenge $C \subset A$ ist genau dann relativ kompakt (ihre abgeschlossene Hülle ist kompakt), wenn sie in einer Menge vom Typ*

$$\prod_{v \in S} C_v \ \times \prod_{p \notin S} \mathfrak{o}_p, \quad (S \textit{ endlich },\ C_v \textit{ kompakt in } \mathbb{Q}_v)$$

enthalten ist.

Beweis: Da $A = \cup_S A_S$ und alle A_S offen sind, gibt es ein endliches S mit $C \subset A_S$. Die Projektionen $\pi_v : A \to \mathbb{Q}_v$ sind stetig, daher sind alle $C_v := \pi_v C$ kompakt, und $C \subset \prod_v C_v \ \times \ \prod_{p \notin S} \mathfrak{o}_v$.

Ist ξ eine rationale Zahl, so ist ξ ganz für fast alle p, also ist $(\xi, ..., \xi, ...)$ ein Adel. Diese Adele heißen Hauptadele. Auf diese Weise fassen wir $\mathbb{Q}$ als Teilring von A auf. In Kapitel 1 hatten wir die p-adische Bewertung so normiert, daß $|p|_p = \frac{1}{p}$ Hier ist einer der Gründe dafür:

Beobachtung: Für alle $\xi \in \mathbb{Q},\ \xi \neq 0$, gilt die Produktformel $\prod_v |\xi|_v = 1$.
Beweis: Zerlege ξ in Primfaktoren: $\xi = \pm \prod_p p^{k_p}$, fast alle $k_p = 0$. Mit der Normierung ist $|\xi|_p = p^{-k_p}$ und $|\xi|_\infty = \prod_p p^{k_p}$.

Lemma 2. $\mathbb{Q}$ *ist diskret in* A .

Beweis: $(-1,1) \times \prod_p \mathfrak{o}_p$ ist offen in A und enthält wegen der Produkttformel keine rationale Zahl außer 0 .

Sei $x \in A$ beliebig. Für jede Primzahl p gibt es eine rationale Zahl y_p mit p-Potenznenner, so daß $x_p - y_p \in \mathfrak{o}_p$, und $y_p \neq 0$ nur für endlich viele p , etwa $p \in S$. Für die rationale Zahl $\xi := \sum_{p \in S} y_p$ ist dann $x - \xi \in \mathbb{R} \times \prod \mathfrak{o}_p$. Ist $n \in \mathbb{Z}$, so ist $x_p - \xi - n$ immer noch in $\mathfrak{o}_p$ für alle p , und man kann n so wählen, daß $x_\infty - n \in [0,1]$. Das beweist

Lemma 3. *Das Kompaktum* $[0,1] \times \prod_p \mathfrak{o}_p$ *enthält ein Vertretersystem für* A *modulo* $\mathbb{Q}$. *Mit anderen Worten:* $A/\mathbb{Q}$ *ist kompakt.*

2. Die Idelgruppe.

Definition: Die (im Ring A) invertierbaren Adele heißen Idele.

Ein Idel ist also ein Tupel

$$(x_\infty, ..., x_p, ...), \text{ für welches } x_v \neq 0 \text{ für alle } v \text{ und } |x_p|_p = 1 \text{ für fast alle } p$$

I wird so topologisiert, daß eine Teilmenge $U \subset I$ genau dann offen ist, wenn U und U^{-1} offen in A sind.

Sei $x \in I$. Für jedes p kann man schreiben

$$x_p = p^{\mu_p} \cdot u_p \text{ mit } \mu_p \in \mathbb{Z} \text{ und } |u_p|_p = 1$$

und dabei sind fast alle $\mu_p = 0$. Mit $\xi = \prod_p p^{\mu_p} \in \mathbb{Q}^*$ ist

$$x = \xi \cdot (y_\infty, ...y_p, ...), \text{ wobei } |y_p|_p = 1 \text{ für alle } p$$

Multipliziert man noch, wenn nötig, mit -1 , so erhält man

$$I = \mathbb{Q}^* \cdot (\mathbb{R}^*_{>0} \times \prod_p \mathfrak{o}_p^*) \tag{2}$$

(und diese Zerlegung ist direkt, denn die einzige positive rationale Zahl, die durch keine Primzahl teilbar ist, ist 1.)

Für jedes Idel x ist nach Definition von "Idel" $|x_p|_p = 1$ für fast alle p . Daher ist

$$|x| = \prod_v |x_v|_v$$

wohldefiniert. $|x|$ heißt der Idelbetrag von x . Die Produktformel sagt $|\xi| = 1$ für $\xi \in \mathbb{Q}^*$. Ist I^0 die Untergruppe aller $x \in I$ mit $|x| = 1$, so folgt aus (2), daß

$$I^0 = \mathbb{Q}^* \cdot (\{1\} \times \prod_p \mathfrak{o}_p^*)$$

und das zeigt

Lemma 4. *$I^0/\mathbb{Q}^*$ ist kompakt.*

3. Die orthogonale Gruppe.

V sei ein n-dimensionaler Vektorraum über $\mathbb{Q}$ mit einer nicht ausgearteten symmetrischen Bilinearform $(\ ,\ )$ und G seine spezielle orthogonale Gruppe. Für Oberkörper K von $\mathbb{Q}$ bezeichnen wir mit V_K bzw. G_K die Punkte von V bzw. G mit Koordinaten in K. Zum Beispiel für $K = \mathbb{Q}_p$ ist $V_{\mathbb{Q}_p}$ ein n-dimensionaler Vektorraum über $\mathbb{Q}_p$ und als solcher lokal kompakt. (Er ist die Vervollständigung von $V_{\mathbb{Q}}$ für die von der p-adischen Bewertung (komponentenweise) induzierte Topologie). Ebenso ist $G_{\mathbb{Q}_p}$ eine lokal kompakte Gruppe. Stellt man sich (nach Wahl einer Basis von V über $\mathbb{Q}$) die Elemente von G als Matrizen vor, so besteht $G_{\mathbb{Q}_p}$ aus Matrizen mit Einträgen in $\mathbb{Q}_p$. Da alle $X \in G$ Determinante 1 haben, bilden die $X \in G_{\mathbb{Q}_p}$ mit Einträgen in $\mathfrak{o}_p$ eine Untergruppe in $G_{\mathbb{Q}_p}$. Diese wird sinngemäß mit $G_{\mathfrak{o}_p}$ bezeichnet. Dann kann man G_A definieren als Menge aller Tupel $X = (X_\infty, ..., X_p, ...)$ mit $X_v \in G_{\mathbb{Q}_v}$ für alle v und $X_p \in G_{\mathfrak{o}_p}$ für fast alle p. Da $G_{\mathfrak{o}_p}$ eine abgeschlossene Teilmenge von $\mathfrak{o}_p^{n^2}$ ist, sind die $G_{\mathfrak{o}_p}$ kompakt. Für alle endlichen S ist

$$G_{A_S} := \prod_{v \in S} G_{\mathbb{Q}_v} \times \prod_{p \notin S} G_{\mathfrak{o}_p}$$

nach Tychonoff lokal kompakt. Wird G_A so topologisiert, daß eine Menge in G_A genau dann offen ist, wenn ihr Durchschnitt mit allen G_{A_S} offen ist (Topologie des induktiven Limes), dann ist auch G_A eine lokal kompakte Gruppe.

Eine basisunabhängige Beschreibung von G_A erhält man, wenn man dasselbe mit Gittern ausdrückt: Sei M ein $\mathbb{Z}$-Gitter in V und $M_p := M \otimes_{\mathbb{Z}} \mathfrak{o}_p$ seine Komplettierung an der Stelle p. Die Elemente von G sind jetzt Abbildungen von V auf sich, welche die Form $(\ ,\ )$ invariant lassen. Dann besteht G_A aus allen Tupeln

$$\Phi = (\Phi_\infty, ...\Phi_p, ...) \text{ mit } \Phi_v \in G_{\mathbb{Q}_v} \text{ für alle } v \text{ und } \Phi_p(M_p) = M_p \text{ für fast alle } p$$

Diese Definition ist unabhängig von dem benutzten Gitter M wegen

Lemma 5. *Sind L und M zwei Gitter in V, so ist $L_p = M_p$ für fast alle p.*

Beweis: Nach Definition 2 von Gitter ist $L = \sum_i \mathbb{Z}u_i$ und $M = \sum_i \mathbb{Z}v_i$. Die Basen u_i und v_i gehen durch Matrizen A und B auseinander hervor:

$$v_i = \sum_j a_{ji} u_j, \quad u_i = \sum_j b_{ji} v_j$$

In den Nennern aller a_{ji} und b_{ji} gehen nur endlich viele Primzahlen auf. Für alle anderen p ist $L_p = M_p$.

Um aus den lokalen Iwasawa-Zerlegungen eine Zerlegung von G_A zu gewinnen, möchten wir gerne Standardgitter benutzen. Dazu beweisen wir einen Satz über $\mathbb{Z}$-Gitter:

Satz 1.
(a) Für jedes Gitter M *ist* $M = \cap_p(V \cap M_p)$
(b) Sei M *ein festes Gitter. Zu jeder Kollektion* $\{L^p\}_p$ *von Gittern mit der Bedingung* $L^p = M_p$ *für fast alle* p *gibt es ein Gitter* L *mit* $L_p = L^p$ *für alle* p.

Beweis: (a): M besitzt eine Basis $u_1, ..., u_n$ über $\mathbb{Z}$. Damit ist $V \cap M_p = \sum_i \mathbb{Q}u_i \cap \sum_i \mathfrak{o}_p u_i = \sum_i (\mathbb{Q} \cap \mathfrak{o}_p)u_i$. Aus $\cap_p(\mathbb{Q} \cap \mathfrak{o}_p) = \mathbb{Z}$ folgt die Behauptung.
(b): Wir setzen $L = \cap_p(V \cap L^p)$ und behaupten zunächst, daß L ein Gitter ist. Daß L ein $\mathbb{Z}$-Modul ist, ist klar. Nach der ersten Definition von "Gitter" in Kapitel 1 muß noch gezeigt werden, daß es Zahlen $a, b \neq 0$ gibt mit

$$a \cdot M \subset L \subset b^{-1} \cdot M$$

Da L^p und M_p Gitter in V_p sind, gibt es natürliche Zahlen μ_p und ν_p mit

$$p^{\mu_p} M_p \subset L^p \subset p^{-\nu_p} M_p$$

Da nach Voraussetzung $L^p = M_p$ für fast alle p, kann man fast alle $\mu_p = \nu_p = 0$ nehmen. Dann sind $a = \prod_p p^{\mu_p}$ und $b = \prod_p p^{\nu_p}$ wohldefiniert, und es gilt

$$a\, M_p \subset L^p \subset b^{-1} M_p \quad \text{für alle } p$$

und daher nach Teil (a)

$$a\, M = a \cap_p (V \cap M_p) = \cap_p (V \cap aM_p) \subset \cap_p (V \cap L^p) = L, \text{ und genau so } bL \subset M$$

Also ist L ein $\mathbb{Z}$-Gitter und besitzt als solches eine Basis $x_1, ..., x_n$ über $\mathbb{Z}$. Jetzt wollen wir zeigen, daß die Komlettierungen von L die L^p sind: Jedenfalls ist $L \subset L^p$, und da L^p abgeschlossen ist, ist auch $L_p \subset L^p$. Wenn wir auch noch zeigen können, daß L dicht in L^p ist, dann ist $L_p = L^p$. Sei also $z \in L^p$ gegeben. Jedenfalls ist $z = \sum_i \xi_i x_i$ mit $\xi_i \in \mathbb{Q}_p$. Wir brechen die p-adische Entwicklung von ξ_i an der Stelle k ab (k wird später passend gewählt) :

$$\xi_i = \eta_i + \gamma_i \text{ mit } \gamma_i \in p^k \mathfrak{o}_p$$

η_i ist eine rationale Zahl mit p-Potenznenner, also ganz für alle $q \neq p$. Dann ist $y := \sum_i \eta_i x_i \in V \cap L_q \subset V \cap L^q$ für alle $q \neq p$ und $z - y = \sum_i \gamma_i x_i \in p^k L_p$, also $y \in L^p + p^k L_p$. Wenn k groß genug ist, folgt $y \in \cap_{alle\ q}(V \cap L^q) = L$, und nahe an z für p.

Zur Herstellung der Iwasawa-Zerlegung von G_A schreiben wir über $\mathbb{Q}$

$$V = H_1 \perp ..... \perp H_r \perp W$$

mit (über $\mathbb{Q}$) anisotopem W und hyperbolischen Ebenen $H_i = \mathbb{Q}u_i + \mathbb{Q}v_i$. Sei M irgendein Gitter in V. Für fast alle $p \neq 2$ enthält M_p die u_i und die v_i und ist unimodular. In diesem Falle hat man

$$M_p = (\mathfrak{o}_p u_1 + \mathfrak{o}_p v_1) \perp ..... \perp (\mathfrak{o}_p u_r + \mathfrak{o}_p v_r) \perp (W_p \cap M_p)$$

Wenn W_p isotrope Vektoren enthält, kann man (da M_p unimodular und $p \neq 2$ ist), weitere hyperbolische Teilgitter abspalten und erhält schließlich

$$M_p = (\mathfrak{o}_p u_1 + \mathfrak{o}_p v_1) \perp ..... \perp (\mathfrak{o}_p u_{r_p} + \mathfrak{o}_p v_{r_p}) \perp N_p$$

mit $r_p \geq r$ und einem anisotropen unimodularen Gitter N_p. Offenbar ist N_p enthalten in dem in Lemma 2 beschriebenen Gitter aller x mit $|\frac{1}{2}(x,x)| \leq 1$; da aber N_p als unimodulares Gitter maximal ist, ist N_p gleich diesem. Wir sehen: Für fast alle p ist M_p ein Standardgitter im Sinne der lokalen Betrachtung.
Sei S die Menge der endlich vielen übrigen p. Für $p \in S$ wählen wir irgendein Standardgitter L^p, in dessen Basis wir $u_1, ..., v_r$ aufnehmen. Nach Satz 1 gibt es ein Gitter L mit $L_p = L^p$ für $p \in S$ und $L_p = M_p$ für $p \notin S$. Dieses Gitter L benutzen wir in der Definition der Adelgruppe. Es hat den Vorzug, daß seine sämtlichen Komplettierungen Standardgitter sind, in deren Basis $u_1, ..., v_r$ vorkommen. Für die unendliche Stelle ergänzen wir $u_1, ...v_r$ irgendwie zu einem maximalen System $u_1, v_1, ..., u_{r_\infty}, v_{r_\infty}$ hyperbolischer Paare.

Die Gruppe

$$B = \{b \in G \mid bu_i \in \sum_{j \leq i} \mathbb{Q} u_j \text{ für } i = 1, ..., r\}$$

besitzt (wie G) Komplettierungen $B_{\mathbb{Q}_v}$ und eine Adelisierung B_A. Anderseits haben wir für jede Stelle v

$$B^v = \{b \in G_{\mathbb{Q}_v} \mid bu_i \in \sum_{j \leq i} \mathbb{Q}_v u_j \text{ für } i = 1, ..., r_v\}$$

und nach der lokalen Betrachtung war

$$G_{\mathbb{Q}_v} = K_v \cdot B^v$$

mit

$$K_v = \begin{cases} G_{\mathbb{R}} \cap (O(V^+)O(V^-)) & \text{wenn } v = \infty \\ G(L_p) & \text{wenn } v = p \text{ eine Primzahl ist} \end{cases}$$

Nun ist aber offenbar $B^v \subset B_{\mathbb{Q}_v}$, denn für die erste Gruppe werden mehr Bedingungen verlangt als für die zweite. Also gilt erst recht

$$G_{\mathbb{Q}_v} = K_v B_{\mathbb{Q}_v}$$

Das Produnkt $K = \prod_v K_v$ ist eine kompakte Untergruppe von G_A (deshalb mußten wir uns so viel Mühe geben bei der Definition der K_v). Jedes $g \in G_A$ zerlegen wir komponentenweise in $g_v = k_v b_v$. Nach Definition von G_A ist $g_p(L_p) = L_p$ für fast alle p. Für diese ist auch $b_p(L_p) = L_p$, das heißt $b = (b_v)_v$ ist ein Adel von B. Wir erhalten

$$G_A = K \cdot B_A$$

Das ist die Iwasawa-Zerlgung von G_A. Sie ist (im Gegensatz zur lokalen) nicht eindeutig; denn offenbar ist $K \cap B_A \neq 1$.

3. Integration

f sei eine reellwertige stetige Funktion mit kompaktem Träger auf $\mathbb{Q}_p$, etwa $f = 0$ außerhalb $p^{-N}\mathfrak{o}_p$. Wir teilen $p^{-N}\mathfrak{o}_p$ ein in Restklassen mod p^k und wählen in jeder Restklasse einen Vertreter a. Dann bilden wir

$$I_k(f) = \sum_a f(a)p^{-k}$$

Natürlich hängt I_k außer von k auch noch von der Wahl der Vertreter a ab.
Behauptung: Zu $\epsilon > 0$ gibt es k so, daß

$$|I_k(f) - I_m(f)| < \epsilon \text{ für alle } m > k$$

$$\text{und alle Wahlen von Vertretern } \bmod p^k \text{ bzw. } \bmod p^m$$

Beweis: Als stetige Funktion auf einem Kompaktum ist f sogar gleichmäßig stetig: Zu $\epsilon > 0$ gibt es k so, daß $|f(x) - f(y)| < \epsilon$ falls $x \equiv y \bmod p^k$. Für $m > k$ besteht jede Restklasse mod p^k aus p^{m-k} Restklassen mod p^m. Daher ist

$$\sum_{a \bmod p^k} f(a)p^{-k} - \sum_{b \bmod p^m} f(b)p^{-m} =$$

$$\sum_{a \bmod p^k} \{\frac{1}{p^{m-k}} \sum_{b \equiv a \bmod p^k,\ b \bmod p^m} f(a)\} \cdot p^{-k} \quad - \sum_{b \bmod p^m} f(b)p^{-m} =$$

$$\sum_{a \bmod p^k} \sum_{b \equiv a \bmod p^k, b \bmod p^m} \{f(a) - f(b)\}p^{-m}$$

Diese Summe ist dem Betrage nach $< \epsilon p^N$ (die Anzahl der Summanden ist p^{N+m}).
Daher existiert der Limes I der $I_k(f)$ für $k \to \infty$ und alle Wahlen von Vertretern $a \bmod p^k$. Er ist ein lineares Funktional auf dem reellen Vektorraum der stetigen Funktionen mit kompaktem Träger auf $\mathbb{Q}_p$. Definiert man die verschobene Funktion f_c durch $f_c(x) = f(c + x)$, so gilt

$$I(f_c) = I(f)$$

Man nennt I ein Haarsches Maß auf $\mathbb{Q}_p$. (Für Einzelheiten siehe [L], Seite 107 ff). Das Haarsche Maß ist bis auf einen Faktor bestimmt. Wir schreiben

$$I(f) = \int f(x)\,dx$$

Mit der Definition von I ist das Maß so normiert, daß die offene kompakte Menge $\mathfrak{o}_p$ das Volumen 1 bekommt. Weil $\mathfrak{o}_p$ (für $n \geq 0$) die disjunkte Vereinigung von p^n Restklassen $c + p^n\mathfrak{o}_p$ ist, folgt aus der Translationsinvarianz, daß $p^n\mathfrak{o}_p$ das Volumen p^{-n} besitzt. Und das gilt auch für $n < 0$ (man schreibe $p^n\mathfrak{o}_p$ als Vereinigung von Restklassen mod $\mathfrak{o}_p$) Transformationsformel:

$$\int f(ax)\,dx = |a|_p^{-1} \int f(x)\,dx \tag{1}$$

Beweis: Nach Konstruktion des Integrals genügt es, die Behauptung für die Indikatorfunktion f einer Restklasse $c + p^k \mathfrak{o}_p$ zu beweisen. Ihr Integral ist p^{-k}. Sei $a = p^n u$ mit einer Einheit u und $g(x) = f(ax)$.

$$g(x) \neq 0 \Leftrightarrow f(ax) \neq 0 \Leftrightarrow ax \in c + p^k \mathfrak{o}_p \Leftrightarrow x \in \frac{c}{a} + p^{k-n} \mathfrak{o}_p$$

g ist also die Indikatorfunktion einer Restklasse $\bmod p^{k-n}$. Ihr Integral ist wie oben bemerkt $= p^{n-k}$. Nun ist

$$\int g(x)dx = p^{n-k} = p^n \int f(x)dx = |a|_p^{-1} \int f(x)dx$$

Auf $\mathbb{Q}_p^n$ nehmen wir das Produktmaß: Für stetige Funktionen f mit kompaktem Träger und $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Q}_p^n$ kann man es definieren als iteriertes Integral

$$\int f(x)dx = \int (\int .....(\int f(x_1, ..., x_n)dx_1).....dx_{n-1})dx_n$$

Der Satz von Fubini besagt, daß das Ergebnis unabhängig von der Reihenfolge der x_i ist. Ferner folgt aus der Translationsinvarianz der Integrale $\int ....dx_i$, daß das $\int f(x)dx$ sich nicht ändert bei elementaren Transformationen

$$\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \mapsto (1 + \lambda e_{ij}) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_i + \lambda x_j \\ \vdots \\ x_n \end{pmatrix}$$

Weil jede invertierbare Matrix Produkt von elementaren Matrizen $1 + \lambda e_{ij}$ und Diagonalmatrizen ist, folgt aus der Transformationsformel (1)

Satz 2. *Für jede invertierbare Matrix A gilt*

$$\int f(Ax)\, dx = |\det A|_p^{-1} \int f(x)\, dx$$

Adelisierung: Wir wollen auf dem Adelring A ein Haarsches Maß dx_A definieren mit in einem noch zu erklärenden Sinne $dx_A = \prod_v dx_v$: Jede Funktion auf A mit kompaktem Träger ist $= 0$ außerhalb eines passenden

$$A_S = \prod_{v \in S} \mathbb{Q}_v \times \prod_{p \notin S} \mathfrak{o}_p = \prod_{v \in S} \mathbb{Q}_v \times A^S$$

A^S ist eine kompakte Gruppe, und wir nehmen auf ihr das Haarsche Maß dx^S, für welches die ganze Gruppe das Volumen 1 bekommt. Sodann nehmen wir auf A_S das Produktmaß $dx_S = \prod_{v \in S} dx_v \cdot dx^S$. Das $\int_{A_S} f(x)dx_S$ ist unabhängig von der Wahl

der Menge S, für welche A_S den Träger von f enthält, nämlich: durch Vergleich von S,T mit $S \cup T$ genügt es, das einzusehen, wenn $S \subset T$. dx^S ist das Haarsche Maß auf $A^S = \prod_{p \notin S} \mathfrak{o}_p$, für welches A^S das Volumen 1 besitzt. Dieselbe Eigenschaft hat das Produktmaß $\prod_{p \in T \setminus S} dx_p \cdot dx^T$. Also ist dx_S die Einschränkung von dx_T auf A_S, und daraus folgt die Behauptung.

Beispiel: Wir sahen, daß

$$W = [0,1) \times \prod_p \mathfrak{o}_p$$

ein Vertetersystem für A modulo $\mathbb{Q}$ ist. Das Volumen von W ist

$$\int_W dx_A = \int_0^1 dx_\infty \cdot \prod_p \int_{\mathfrak{o}_p} dx_p = 1$$

Ist V ein n-dimensionaler Vektorraum über $\mathbb{Q}$, so wählen wir irgendeine Basis $v_1, .., v_n$ von V über $\mathbb{Q}$ und benutzen die Koeffizienten $x_1, ..., x_n$ in $x = \sum_i x_i v_i$ als Koordinaten. Bei Wahl einer anderen Basis gehen die neuen Koordinaten y_i durch eine lineare Transformation $y = Tx$ aus den alten hervor. Dabei multipliziert sich das Integral in $V_{\mathbb{Q}_p}$ nach Satz 2 mit dem p-Betrag der Determinante von T. Geht man zur Adelisierung V_A über, so multipliziert sich das Integral mit $\prod_v |\det T|_v$. Nun ist aber $\det T$ eine rationale Zahl , und nach der Produktformal ist $\prod_v |\det T|_v = 1$. Wir haben jetzt auf dem Adelraum V_A ein Maß definiert, welches von der Wahl der Basis von V über $\mathbb{Q}$ unabhängig ist !!

4. Der Kompaktheitssatz

Wir behalten die Bezeichnungen des vorigen Kapitels bei. Sei $0 \neq \rho \in \mathbb{Q}$ und

$$\Sigma = \{x \in V \mid (x,x) = \rho\}$$

die "Sphäre vom Radius ρ ". Sei $e \in \Sigma_{\mathbb{Q}}$ fest. Wir kürzen (x,x) mit $F(x)$ ab. Man definiert eine Abbildung π von G_A nach Σ_A durch

$$\pi(g) = g\,e \text{ für } g \in G_A$$

Lemma 1. *π ist stetig und offen.*

Beweis: "stetig" ist klar, weil π durch lineare Gleichungen in den Koeffizienten von g beschrieben werden kann. Für "offen" zeigen wir

1. Für alle v und alle offenen $U_v \subset G_{\mathbb{Q}_v}$ ist $\pi_v(U_v)$ offen in $\Sigma_{\mathbb{Q}_v}$; nämlich: Sei $a \in \pi_v(U_v)$, etwa $a = g_0 e$ mit $g_0 \in U_v$. Wenn $x \in \Sigma_{\mathbb{Q}_v}$ nahe an a ist, dann ist $a + x$ nicht isotrop (weil nahe an $2a$) und wenn S_a die Spiegelung längs a ist, dann ist $S_{a+x}S_a \in G_{\mathbb{Q}_v}$ nahe an 1, also $S_{a+x}S_a g_0$ nahe an g_0, mithin in U_v, und

$$x = S_{a+x}S_a a = S_{a+x}S_a g_0 e \in \pi_v(U_v)$$

Damit ist $\pi_v(U_v)$ offen.

2. Für fast alle p ist $\pi_p(G(M_p)) = M_p \cap \Sigma_{\mathbb{Q}_p}$. Nämlich: Sei M_p unimodular und $p \neq 2$ und $|\rho|_p = 1$. Wenn $x \in M_p \cap \Sigma_{\mathbb{Q}_p}$ und wenn $|(x+e, x+e)|_p = 1$, dann bilden S_e und S_{x+e} das Gitter M_p in sich ab und

$$S_{x+e}S_e e = x,$$

also $x \in \pi_p(G(M_p)$. Wenn $|(x+e,x+e)|_p < 1$, dann ist $|(x-e,x-e)|_p = 1$. Da M_p unimodular und $p \neq 2$, gibt es $u \in M_p$ mit $(u,e) = 0$ und $|(u,u)|_p = 1$. Dann ist $S_{x-e}S_u e = x$, also wieder $x \in \pi_p(G(M_p)$.

1 und 2 zusammen zeigen, daß π offene Mengen auf offene abbildet.

Lemma 2. *Sind X und Y lokal kompakte Räume und π eine Abbildung von X auf Y, die sowohl stetig als auch offen ist, dann besitzt jedes Kompaktum in Y ein partielles kompaktes Urbild in X.*

Beweis: Sei C kompakt in Y und $\tilde{C}$ das volle Urbild von C. Da π stetig ist, ist $\tilde{C}$ jedenfalls abgeschlossen. Für jedes $x \in \tilde{C}$ nehme man eine offene Umgebung U_x in X, deren abgeschlossene Hülle kompakt ist. Offenbar ist $\tilde{C} \subset \cup_{x \in \tilde{C}} U_x$ und damit $C = \pi(\tilde{C}) \subset \cup_{x \in \tilde{C}} \pi(U_x)$. Da π offen ist, sind alle $\pi(U_x)$ offen in Y. Da C kompakt ist, genügen endlich viele x; es ist $C \subset \cup_{i=1}^n \pi(U_{x_i}) = \pi(\cup_{i=1}^n U_{x_i})$ Die abgeschlossene Hülle C' von $\cup_{i=1}^n U_{x_i}$ ist kompakt, und damit ist auch ihr Durchschnitt mit der abgeschlossenen Menge $\tilde{C}$ kompakt. Dieser wird bei π genau auf C abgebildet.

Mit Hilfe dieser beiden Lemmata beweisen wir den Kompaktheitssatz:

Satz 3. *Wenn die quadratische Form über $\mathbb{Q}$ anisotrop ist, dann ist $G_A/G_{\mathbb{Q}}$ kompakt.*

Beweis: Für $n = 1$ ist der Satz trivialerweise richtig, weil dann G nur aus der Eins besteht. Sei $n > 1$ und der Satz bis $n-1$ bewiesen.
Man wählt ein Kompaktum $C \subset V_A$ mit $vol(C) > 1 (= vol(V_A/V_{\mathbb{Q}})$. Für $X \in G_A$ ist $vol(X^{-1}C) = vol(C) > 1$. Daher ist die Projektion $V_A \to V_A/V_{\mathbb{Q}}$ auf $X^{-1}C$ nicht injektiv. Das bedeutet: es gibt $x, y \in X^{-1}C$ mit $0 \neq x - y \in V_{\mathbb{Q}}$. Dann ist $\xi := x - y \in X^{-1}C'$, wobei $C' = C - C$ ebenfalls kompakt ist. Sei etwa $\xi = X^{-1}c$. Dann ist $F(\xi) = F(c) \in \mathbb{Q} \cap F(C')$. Da $\mathbb{Q}$ diskret in A und $F(C')$ kompakt ist, ist $\mathbb{Q} \cap F(C')$ endlich. Daher gehört $F(\xi)$ einem endlichen Vorrat (von 0 verschiedener, weil $V_{\mathbb{Q}}$ anisotrop) Zahlen $\{\zeta_1, ..., \zeta_h\}$ an. Die Betrachtung zeigt: Zu jedem $X \in G_A$ gibt es i mit $1 \leq i \leq h$ und $\xi \in V_{\mathbb{Q}}$ mit $X\xi \in C'$ und $F(\xi) = \zeta_i$
Die Sphäre $\Sigma_{i,A}$ vom Radius ζ_i ist abgeschlossen in V_A, also ist $E_i := \Sigma_{i,A} \cap C'$ kompakt in V_A. Sei e_i ein fester Vektor in $\Sigma_{i,\mathbb{Q}}$. Da $G_{\mathbb{Q}}$ transitiv auf $\Sigma_{i,\mathbb{Q}}$ ist, gibt es $\gamma \in G_{\mathbb{Q}}$ mit $\xi = \gamma e_i$. Die Projektion $G_A \to \Sigma_{i,A}$, gegeben durch $X \mapsto Xe_i$, ist nach Lemma 1 stetig und offen. Nach Lemma 2 gibt es ein partielles kompaktes Urbild K_i, so daß also $E_i = K_i(e_i)$. Nun ist

$$X\gamma e_i = X\xi \in E_i = K_i(e_i) \tag{1}$$

Sei g_i der Stabilisator von e_i. Nach (1) ist $X\gamma \in K_i g_{i,A}$. Damit ist gezeigt, daß

$$G_A = \cup_{i=1}^{h} K_i \cdot g_{i,A} \cdot G_{\mathbb{Q}} \tag{2}$$

Da $F(e_i) \neq 0$, ist der Stabilisator g_i die spezielle orthogonale Gruppe von $e_i^{\perp}$, also eines $(n-1)$-dimensionalen nicht ausgearteten Raumes. Nach Induktionsannahme gibt es Kompakta $B_i \subset g_{i,A}$ mit $g_{i,A} = B_i g_{i,\mathbb{Q}}$. Die Bilder der B_i bei der Einbettung von $g_{i,A}$ in G_A sind natürlich kompakt in G_A. Trägt man diese in (2) ein, so ist Satz 3 bewiesen.

Wenn $V_{\mathbb{Q}}$ die null darstellt, gilt der Satz offensichtlich nicht mehr; die orthogonale Gruppe enthält dann eine Gruppe von Diagonalmatrizen $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, $\lambda \neq 0$. Für diesen Fall wollen wir einen anderen Satz beweisen, wozu wir "Höhen" erklären müssen: In V_∞ wählen wir eine positiv definite quadratische Form $< , >$, welche unter der Gruppe $K_\infty = O(V^+)O(V^-) \cap G_\infty$ invariant ist, zum Beispiel $< x, x >= (x^+, x^+) - (x^-, x^-) = (x^+, x^+) + |(x^-, x^-)|$, wenn $x = x^+ + x^-$ in $V = V^+ \perp V^-$ ist. Dann setzen wir

$$||x||_\infty = \sqrt{< x, x >}$$

Sodann nehmen wir ein Gitter M in $V_{\mathbb{Q}}$ (vorzugsweise gleich eines, dessen sämtliche Komplettierungen M_p Standardgitter sind) und setzen für $x \in V_{\mathbb{Q}_p}$

$$||x||_p = p^n \text{ wenn } p^n x \text{ ein primitiver Vektor in } M_p \text{ ist}$$

(also $||x||_p \leq 1 \Leftrightarrow x \in M_p$). Dann sei

$$V_A^* = \{x \in V_A \mid x_p \text{ primitiv in } M_p \text{ für fast alle } p\}$$

Für $x \in V_A^*$ definieren wir die Höhe

$$||x|| = \prod_v ||x_v||_v$$

Lemma 3. *Zu $g \in G_A$ gibt es $c(g)$ mit*

$$||gx|| \leq c(g)\,||x|| \text{ für alle } x \in V_A^*$$

Beweis: Sei $g \in G_A$ und $x \in V_A^*$. Für fast alle p ist $g_p M_p = M_p$ und x_p primitiv in M_p, also $||g_p x_p||_p = 1$, und $\prod_v ||g_v x_v||_v$ ist wohldefiniert. Zu jedem v gibt es eine Schranke $c_v = c_v(g_v)$ mit $||g_v x_v||_v \leq c_v ||x_v||_v$ für alle x_v. Wenn $g_p M_p = M_p$, kann $c_p = 1$ genommen werden. Dann ist $c := \prod_v c_v$ wohldefiniert, und mit diesem c gilt die Behauptung.

Lemma 4. *Zu festem r gibt es nur endlich viele mod $\mathbb{Q}^*$ verschiedene $\xi \in V_\mathbb{Q}$ mit $||\xi|| \leq r$.*

Beweis: Aus der Definition folgt $||\gamma x|| = |\gamma| \cdot ||x||$ für jedes Idel γ und $x \in V_A^*$. Wegen der Produktformel ist $||\gamma x|| = ||x||$ wenn $\gamma \in \mathbb{Q}^*$. Ist nun $\xi \in V_\mathbb{Q}$, so gibt es $\gamma \in \mathbb{Q}^*$ so, daß $\eta := \gamma\xi$ ein primitiver Vektor in M ist. Für diesen ist $||\eta||_\infty = ||\eta|| = ||\xi|| \leq r$. In der Kugel vom Radius r in V_∞ gibt es aber nur endlich viele Gittervektoren.

Mit Hilfe der Höhe können wir formulieren und beweisen

Satz 4. *Wenn $V_\mathbb{Q}$ die Null darstellt, dann gibt es eine Konstante $c = c(V)$ mit der Eigenschaft: Zu jedem $g \in G_A$ gibt es einen isotropen Vektor $\xi \neq 0$ in $V_\mathbb{Q}$ mit $||g\xi|| \leq c$.*

Beweis: Ist $n = 2$, so wird V aufgespannt von einem hyperbolischen Paar u, v, und für $g \in G_A$ ist $gu = \lambda u$, $gv = \frac{1}{\lambda} v$, und man kann $c = max(||u||, ||v||)$ nehmen. Sei also $n \geq 3$.

M sei das Gitter in $V_\mathbb{Q}$, welches oben zur Definition der Höhe gedient hat. Damit das Argument durchsichtiger wird, benutzen wir ein Kompaktum $C = C_\infty \times \prod_p M_p$, wobei C_∞ die Kugel $< x, x > \leq R^2$ und R so groß ist, daß $vol(C) > vol(V_A/V_\mathbb{Q})$. Dann ist $C' := C - C = 2C_\infty \times \prod_p M_p$.

Wie im Beweis von Satz 3 gibt es eine endliche Menge $\{\zeta_0, \zeta_1, ..., \zeta_h\} \subset \mathbb{Q}$ und Vektoren $e_0, ..., e_h \in V_\mathbb{Q}$ mit $(e_i, e_i) = \zeta_i$ und der Eigenschaft: Zu $g \in G_A$ gibt es $\gamma \in G_\mathbb{Q}$ und ein i so, daß $g\gamma e_i \in C'$. Nur kann jetzt eines der ζ_i, etwa $\zeta_0 = 0$ sein. Jetzt gibt es für g drei Möglichkeiten:

1. $i = 0$. Wir nehmen $\xi = \gamma e_0$. Jeder Vektor $\neq 0$ in $V_\mathbb{Q}$ ist in fast allen M_p primitiv, und $g_p M_p = M_p$ für fast alle p. Daher ist $g\xi \in V_A^*$, und wegen $g\xi \in C'$ ist

$$||g\xi|| = ||g_\infty \xi||_\infty \cdot \prod_p ||g_p \xi||_p \leq 2R$$

2. $i \neq 0$ und $(e_i^\perp)_\mathbb{Q}$ enthält isotrope Vektoren. Bei der Abbildung $g \mapsto ge_i$ von G_A auf die Sphäre $\Sigma_{i,A}$ besitzt das Kompaktum $C' \cap \Sigma_{i,A}$ ein partielles kompaktes Urbild K_i. Es gibt $k \in K_i$ mit $g\gamma e_i = ke_i$. Nach Induktionsannahme gibt es c_i und zu $k^{-1}g\gamma \in Stab(e_i)_A$ ein isotropes $\eta \in (e_i^\perp)_\mathbb{Q}$ mit $||k^{-1}g\gamma\eta|| \leq c_i$. Die Konstanten $c(g)$ aus Lemma 1 sind auf dem Kompaktum K_i beschränkt, etwa $\leq d_i$, und mit $\xi = \gamma\eta$ ist

$$||g\xi|| \leq d_i c_i$$

3. $i \neq 0$ und $(e_i^\perp)_\mathbb{Q}$ ist anisotrop. Nach Satz 3 gibt es ein Kompaktum $D_i \subset g_{iA}$ mit $g_{iA} = D_i g_{i\mathbb{Q}}$. Wie unter 2. ist $k^{-1}g\gamma \in g_{iA}$, also nun etwa $k^{-1}g\gamma = d \cdot \delta$ mit $d \in D_i$

und $\delta \in g_{\mathbb{Q}}$. Nach Voraussetzung gibt es in $V_{\mathbb{Q}}$ einen istropen Vektor u_0. Man setzt $\xi = \gamma\delta^{-1}u_0$ und hat

$$||g\xi|| = ||kdu_0|| \leq const_i$$

weil u_0 fest und k und d in einem Kompaktum laufen. Damit ist Satz 4 bewiesen.

5. Siegelbereiche

Wir erinnern an die Iwasawa-Zerlegung

$$G_A = K \cdot B_A$$

aus Kapitel 2. Dabei war

$u_1, v_1; .....; u_r, v_r$ ein maximales System hyperbolischer Paare in $V_{\mathbb{Q}}$
H_i die von u_i und v_i aufgespannte hyperbolische Ebene
$W = \cap_{i=1}^{r} H_i^{\perp}$ und $w_{2r+1}, ..., w_n$ irgendeine Basis von W über $\mathbb{Q}$.

Bezüglich der Basis $u_1, ..., u_r, v_1, ..., v_r, w_{2r+1}, ..., w_n$ bestand B aus allen Matrizen

$$\begin{pmatrix} \begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ 0 & & \lambda_r \end{pmatrix} & & * & & * \\ & & & & \\ & 0 & & \begin{pmatrix} \frac{1}{\lambda_1} & & 0 \\ & \ddots & \\ * & & \frac{1}{\lambda_r} \end{pmatrix} & 0 & \\ & & & & \\ & 0 & & * & * \end{pmatrix}$$

$b \mapsto \lambda_i = \lambda_i(b)$ ist ein Homomorphismus von B in die multiplikative Gruppe, also von $B_{\mathbb{Q}}$ nach $\mathbb{Q}^*$, von $B_{\mathbb{Q}_v}$ nach $\mathbb{Q}_v^*$ und von B_A in die Idelgruppe I.

Lemma 1. *Wenn $b \in B_A \cap K$, dann ist $|\lambda_i| = 1$ für $i = 1, ..., r$.*

Beweis: B_A ist abgeschlossen in G_A (es ist durch Nullsetzen gewisser Matrixkoeffizienten in den ersten r Spalten definiert), und K ist kompakt. Daher ist $B_A \cap K$ kompakt. Und $|\lambda_i|$ ist stetig. Das Bild von $B_A \cap K$ ist daher eine kompakte Untergruppe von $\mathbb{R}^*_{>0}$. Die einzige solche ist $\{1\}$.
Folgerung: Für $g = k \cdot b \in K \cdot B_A$ ist

$$|\lambda_i(g)| := |\lambda_i(b)| \text{ wohldefiniert}$$

Ziel dieses Kapitels ist der Beweis der Minkowski'schen Ungleichungen für die λ_i. Das bereiten wir vor in der Gruppe $GL(n)$.

Bekanntlich ist jede reelle invertierbare Matrix = orthogonal mal dreieckig:

$$GL(n, \mathbb{R}) = SO(n, \mathbb{R}) \cdot B(n, \mathbb{R})$$

Für p gilt

Satz 5.

$$GL(n, \mathbb{Q}_p) = SL(n, \mathfrak{o}_p) \cdot B(n, \mathbb{Q}_p)$$

Beweis: Sei $X = (x_{ij})_{i,j} \in GL(n, \mathbb{Q}_p)$. Multiplikation mit einer Permutationsmatrix $\sum_i \pm e_{\pi(i),i} \in SL(n, \mathfrak{o}_p)$ von links bewirkt Vertauschung der Zeilen (bis aufs Vorzeichen).

Deshalb kann man annehmen, daß $|x_{11}| \geq |x_{i1}|$ für alle i. Dann ist $\lambda_i := \frac{x_{i1}}{x_{11}} \in \mathfrak{o}_p$ und $Y := 1 - \sum_{i=2}^{n} \lambda_i e_{i1} \in SL(n, \mathfrak{o}_p)$ und

$$Y\,X = \begin{pmatrix} x_{11} & \dots & x_{1n} \\ 0 & & \\ \vdots & * & \\ 0 & & \end{pmatrix}$$

Mit Induktion nach n folgt die Behauptung.

Hieraus haben wir die Iwasawa-Zerlegung von $GL(n)_A$: Mit der kompakten Gruppe $K = SO(n, \mathbb{R}) \times \prod_p SL(n, \mathfrak{o}_p)$ ist

$$GL(n)_A = K \cdot B_A$$

Lemma 2. *Sei dim $V = 2$. Es gibt eine Konstante e mit der Eigenschaft: Zu $g \in GL(V)_A$ mit $|\det g| = 1$ gibt es $\xi \in V_{\mathbb{Q}}$ mit $||g\xi|| \leq e$.*

Beweis: Man wählt ein Kompaktum $C \subset V_A$ mit $vol(C) > vol(V_A/V_{\mathbb{Q}})$, zum Beispiel $C_\infty \times \prod_p M_p$, wo M das Gitter ist, das zur Defintion der Höhe gedient hat ($||x||_p = p^k$, wenn $p^k x$ primitiv in M_p ist). Da $|\det g| = 1$, ist $vol(g^{-1}C) = vol(C)$. Daher wird $g^{-1}C$ modulo $V_{\mathbb{Q}}$ nicht injektiv projiziert: es gibt $x, y \in g^{-1}C$ mit $0 \neq x - y =: \xi \in V_{\mathbb{Q}}$. Dann ist $g\xi \in (C_\infty - C_\infty) \times \prod M_p =: C'$, außerdem in V_A^*. Auf $C' \cap V_A^*$ ist die Höhe beschränkt, etwa $\leq e$, und wir haben $||g\xi|| \leq e$.

Satz 6. *Sei dim $V = n$. Es gibt eine Konstante c mit folgender Eigenschaft: Zu $g \in GL(V)_A$ gibt es $\gamma \in GL(V)_{\mathbb{Q}}$ derart, daß in der Iwasawa-Zerlegung*

$$g\gamma = m \cdot p \text{ mit } m \in K \text{ und } p = \begin{pmatrix} t_1 & & * \\ & \ddots & \\ 0 & & t_n \end{pmatrix} \in B_A$$

für die Idele t_i die Ungleichungen $|t_i| \leq c|t_{i+1}|$ für $i = 1, ..., n-1$ gelten.

Beweis: Induktion nach n, Verankerung für $n = 2$: Wenn $|\det g| = 1$, dann liefert Lemma 2 einen Vektor $\xi \in V_{\mathbb{Q}}$, $\xi \neq 0$ mit $||g\xi|| \leq e$. Schreibe $\xi = \gamma e_1$ mit $\gamma \in GL(V)_{\mathbb{Q}}$ und zerlege $g\gamma = mp$ nach Iwasawa. Da die Höhe invariant unter K ist, folgt

$$e \geq ||g\xi|| = ||g\gamma e_1|| = ||mp\, e_1|| = ||p\, e_1|| = |t_1|$$

und

$$|\frac{t_1}{t_2}| = |t_1^2| \leq e^2$$

Im allgemeinen nehme man $\lambda \in \mathbb{R}^*$ mit $\lambda^2 |\det g| = 1$ und setze $h = (\lambda g_\infty, ..., g_p, ...)$. Dann ist $|\det h| = 1$, und wir haben γ, m und $p = \begin{pmatrix} t_1 & * \\ 0 & t_2 \end{pmatrix}$ mit $h\gamma = mp$ und $|\frac{t_1}{t_2}| \leq e^2$. Aber der Quotient $\frac{t_1}{t_2}$ ändert sich gar nicht beim Übergang von h zu g, daher ist die Behauptung auch für g richtig.

Induktionsschluß: Wir wählen γ zu g "schrittweise minimal" so: Nach Lemma 4, Kapitel 4, existieren alle folgenden Minima. Damit sei

$$r_1 = \min_{\xi \in V_{\mathbb{Q}}^*} ||g\xi||$$

Dann ist auch $r_1 = \min_{\gamma \in G_{\mathbb{Q}}} ||g\gamma e_1||$. Sei

$$R_1 = \{\gamma \in G_{\mathbb{Q}} \mid ||g\gamma e_1|| = r_1\}$$

In $R_1 e_2$ gibt es wieder einen Vektor ξ, für den $||g\xi||$ minimal ist, etwa $= r_2$. Sei

$$R_2 = \{\gamma \in R_1 \mid ||g\gamma e_2|| = r_2\}$$

Für $\gamma \in R_2$ ist

$$||g\gamma e_2|| \leq ||g\xi|| \text{ für alle } \xi \in R_1 e_2 \text{ und } ||g\gamma e_1|| \leq ||g\xi|| \text{ für alle } \xi \in V_{\mathbb{Q}}^*$$

So fortfahrend definiert man $R_1 \supset R_2 \supset ..... \supset R_n$, und für $\gamma \in R_n$ gilt schließlich

$$r_1 = ||g\gamma e_1|| \leq ||g\gamma' e_1|| \text{ für alle } \gamma' \in G_{\mathbb{Q}}$$

$$r_2 = ||g\gamma e_2|| \leq ||g\gamma' e_2|| \text{ für alle } \gamma' \text{ mit } ||g\gamma' e_1|| = r_1$$

$$\vdots$$

$$||g\gamma e_n|| \leq ||g\gamma' e_n|| \text{ für alle } \gamma' \text{ mit } ||g\gamma' e_i|| = r_i \text{ für } i = 1, ..., n-1$$

Die $\gamma \in R_n$ nennen wir minimal für g und behaupten, daß, wenn $\gamma \in R_n$ und $g\gamma = mp$ und $t_1, ..., t_n$ die Diagonalglieder von p sind, die Ungleichungen $|t_i| \leq c|t_{i+1}|$ für $i = 1, ..., n-1$ gelten. Nämlich: Angenommen nicht. Dann gibt es ein i mit $|t_j| \leq c|t_{j+1}|$ für $j < i$ und $|t_i| > c|t_{i+1}|$. Wir werden ein $\bar{\gamma}$ finden, welches γ echt unterbietet. Dazu schreiben wir

$$p = \begin{pmatrix} p'' & * & * \\ 0 & p' & * \\ 0 & 0 & p''' \end{pmatrix}$$

wo p' die aus der i-ten und $(i+1)$-ten Zeile und Spalte gebildete zweireihige Teilmatrix von p ist. Zu p' gibt es nach der Verankerung γ' mit $p'\gamma' = m'\bar{p}'$, so daß $\bar{p}' = \begin{pmatrix} \bar{t}_i & * \\ 0 & \bar{t}_{i+1} \end{pmatrix}$ und $|\bar{t}_i| \leq c|\bar{t}_{i+1}|$. Man setzt

$$\bar{\gamma} = \gamma \begin{pmatrix} 1 & 0 & 0 \\ 0 & \gamma' & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ und } \bar{m} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & m' & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Aus $g\gamma = mp$ erhalten wir

$$g\bar{\gamma} = m \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & m' & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} p'' & * & * \\ 0 & \bar{p}' & * \\ 0 & 0 & p''' \end{pmatrix}$$

Die letzte Matrix hat die Diagonalglieder $t_1, ..., t_{i-1}\bar{t}_i, \bar{t}_{i+1}, t_{i+2}, ...t_n$. Aus $p'\gamma' = m'\bar{p}'$ folgt durch Determinantenbildung $|t_i t_{i+1}| = |\bar{t}_i \bar{t}_{i+1}|$. Da $|t_i| > c|t_{i+1}|$ und $|\bar{t}_i| \leq c|\bar{t}_{i+1}|$, muß $|\bar{t}_i| < |t_i|$ sein, und das zeigt, daß γ von $\bar{\gamma}$ echt unterboten wird.

Mit Hilfe von Satz 6 beweisen wir für die orthogonale Gruppe

Satz 7. *Es gibt eine Konstante* $c = c(V)$ *mit der Eigenschaft: Zu* $g \in G_A$ *gibt es* $\gamma \in G_{\mathbb{Q}}$ *derart, daß für die zu Beginn dieses Kapitels erklärten* $|\lambda_i|$ *gilt*

$$|\lambda_i(g\gamma)| \leq c|\lambda_{i+1}(g\gamma)| \text{ für } 1 \leq i < r$$

Beweis: Wir schreiben die Elemente von G als Matrizen bezüglich der zu Beginn des Kapitels benutzten Basis $u_1, ..., u_r, v_1, ..., v_r, w_{2r+1}, ..., w_n$.

$$\iota(X) = \begin{pmatrix} X & 0 & 0 \\ 0 & X'^{-1} & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

ist eine Einbettung von $GL(r)$ in G . Ist nun $g \in G_A$ gegeben, so schreiben wir zunächst $g = k \cdot b$ mit $k \in K$ und $b \in B_A$. Nach Definition hat b die Gestalt

$$b = \begin{pmatrix} X & * & * \\ 0 & X'^{-1} & 0 \\ 0 & * & * \end{pmatrix}$$

Nach Satz 6 gibt es zu X ein $\gamma \in GL(r)_{\mathbb{Q}}$ so, daß in der Zerlegung $X\gamma = mp$ mit $p = \begin{pmatrix} t_1 & * & * \\ 0 & \ddots & * \\ 0 & 0 & t_r \end{pmatrix}$ gilt

$$|t_i| \leq c|t_{i+1}| \text{ für } i = 1, ..., r-1 \tag{1}$$

Dann ist

$$g = k \cdot \begin{pmatrix} X & * & * \\ 0 & X'^{-1} & 0 \\ 0 & * & * \end{pmatrix} = k \cdot \begin{pmatrix} X\gamma & * & * \\ 0 & (X\gamma)'^{-1} & 0 \\ 0 & * & * \end{pmatrix} \begin{pmatrix} \gamma^{-1} & 0 & 0 \\ 0 & \gamma' & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= k \cdot \begin{pmatrix} mp & * & * \\ 0 & m'^{-1}p'^{-1} & 0 \\ 0 & * & * \end{pmatrix} \begin{pmatrix} \gamma^{-1} & 0 & 0 \\ 0 & \gamma' & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$= k \cdot \iota(m) \cdot \begin{pmatrix} p & * & * \\ 0 & p'^{-1} & 0 \\ 0 & * & * \end{pmatrix} \cdot \iota(\gamma^{-1})$$

Nun ist $\iota(m) \in K$; denn
1. für $m_\infty \in SO(r, \mathbb{R})$ ist $m_\infty = m_\infty'^{-1}$, und daraus folgt $i(m)_\infty(u_i + v_i) \in V^+$, genauso $i(m)_\infty(u_i - v_i) \in V^-$, und
2. Wenn $m_p \in GL(r, \mathfrak{o}_p)$, dann gilt dasselbe für $m_p'^{-1}$.
Natürlich ist $\iota(\gamma) \in G_{\mathbb{Q}}$. und

$$g\iota(\gamma) \in K \cdot \begin{pmatrix} p & * & * \\ 0 & p'^{-1} & 0 \\ 0 & * & * \end{pmatrix}$$

Die $|\lambda_i(g\iota(\gamma)|$ sind die $|t_i|$ aus (1); das beweist den Satz.

Zusatz: Wenn $n > 2r$, dann gilt mit denselben Bezeichungen

$$|\lambda_r(g\gamma)| \leq c_0$$

mit einer gewissen Konstanten c_0.
Beweis: Mit offensichtlicher Abkürzung schreiben wir

$$p = (\lambda_1, ..., \lambda_r)\phi_{u_1a_1}.....\phi_{u_ra_r}q$$

mit $q \in G(W)_A$ und Eichlertransformationen $\phi_{u_ia_i}$. Wir setzen $\tilde{p} = (1, ..., 1, \lambda_r)\phi_{u_ra_r}q$. Das ist ein Automorphismus von $H_r \perp W$. Nach Satz 4 gibt es einen isotropen Vektor $\xi \in (H_r \perp W)_{\mathbb{Q}}$ mit $||\tilde{p}\xi|| \leq c_0$, wo c_0 eine nur von V abhängige Schranke ist. Da $n > 2r$, ist $H_r \perp W$ mindestens dreidimensional, daher gibt es $\tilde{\gamma} \in G(H_r \perp W)_{\mathbb{Q}}$ mit $\tilde{\gamma}u_r = \xi$. In $H_r \perp W$ schreiben wir $\tilde{p}\tilde{\gamma} = m^*p^*$. Nun ist

$$\begin{aligned} g\gamma\tilde{\gamma} = mp\tilde{\gamma} &= m(\lambda_1, ..., \lambda_{r-1}, 1)(1, ..., 1, \lambda_r)\phi_{u_1a_1}....\phi_{u_ra_r}q\tilde{\gamma} \\ &= m(\lambda_1, ..., \lambda_{r-1}, 1)\phi_{u_1b_1}.....\phi_{u_{r-1}b_{r-1}}\tilde{p}\tilde{\gamma} \\ &= m(\lambda_1, ..., \lambda_{r-1}, 1)\phi_{u_1b_1}....\phi_{u_{r-1}b_{r-1}}m^*p^* \\ &= mm^*(\lambda_1, ..., \lambda_{r-1}, 1)\phi_{u_1c_1}....\phi_{u_{r-1}c_{r-1}}p^* \end{aligned}$$

mit $b_i = (1, ..., 1, \lambda_r)a_i$ und $c_i = m^{*-1}b_i$. Weil p^* die Vektoren $u_1, ..., u_{r-1}$ fest läßt, ist

$$|\lambda_j(g\gamma\tilde{\gamma})| = |\lambda_j| = |\lambda_j(g\gamma)| \text{ für } j = 1, ..., r-1$$

$|\lambda_r(g\gamma\tilde{\gamma})|$ ist nach Definition der Betrag des Koeffizienten von u_r in

$$(\lambda_1, ..., \lambda_{r-1}, 1)\phi_{u_1c_1}....\phi_{u_{r-1}c_{r-1}}p^*u_r$$

Weil $p^* \in G(H_r \perp W)_A \cap B_A$, ist $p^*u_r = \mu u_r$ mit einem Idel μ, und

$$(\lambda_1, ..., \lambda_{r-1}, 1)\phi_{u_1c_1}.....\phi_{u_{r-1}c_{r-1}}p^*u_r \in \mu u_r + \sum_{j<r} Au_j$$

Also ist

$$|\lambda_r(g\gamma\tilde{\gamma})| = |\mu|$$

Anderseits ist

$$|\mu| = ||\mu u_r|| = ||p^*u_r|| = ||m^*p^*u_r|| = ||\tilde{p}\tilde{\gamma}u_r|| = ||\tilde{p}\xi|| \leq c_0$$

Damit ist der Zusatz bewiesen.

Für reelles $c > 0$ sei im Falle $n > 2r$

$$B_c = \{b \in B_A \mid |\lambda_i(b)| \leq c|\lambda_{i+1}(b)| \text{ für } i = 1, ..., r-1 \text{ und } |\lambda_r(b)| \leq c\}$$

und

$$S_c = KB_c$$

S_c heißt ein Siegelbereich. Das Ergebnis dieses Kapitels ist: Wenn $n > 2r$, dann gibt es ein c so, daß

$$G_A = S_cG_{\mathbb{Q}}$$

Der Fall $n = 2r$ ist etwas komplizierter und bekommt ein eigenes Kapitel.

6. Minkowski'sche Ungleichungen, der Fall $n = 2r$

Wir behandeln zuerst den Fall $n = 2r = 4$ und führen den Fall $n = 2r > 4$ auf diesen zurück.

Den vierdimensionalen Vektorraum V mit zwei zueinander senkrechten hyperbolischen Ebenen kann man realisieren als Vektorraum der zweireihigen Matrizen mit der quadratischen Form

$$(x, x) = 2 \det x$$

(auf diese Idee hat Herr Freitag mich gebracht). Die zugehörige symmetrische Bilinearform ist

$$(x, y) = \det(x + y) - \det x - \det y = x_{11}y_{22} + x_{22}y_{11} - x_{12}y_{21} - x_{21}y_{12}$$

Die Matrizen

$$u_1 := e_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \ , \ v_1 := e_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

bilden ein hyperbolisches Paar, und

$$u_2 := e_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \ , \ v_2 := -e_{21} = \begin{pmatrix} 0 & 0 \\ -1 & 0 \end{pmatrix}$$

das dazu senkrechte.

Lemma 1. *Jede orthogonale Transformation T von V mit Determinante 1 hat die Gestalt*

$$T(X) = AXB$$

mit invertierbaren Matrizen A und B mit $\det A \cdot \det B = 1$.

Beweis: $T(e_{11})$ ist $\neq 0$, aber $\det T(e_{11}) = 0$. Daher ist $T(e_{11})$ eine Matrix vom Rang 1, also von der Gestalt ab' für zwei Spalten $a, b \neq 0$. Analog ist $T(e_{22}) = cd'$. Die Isometriebedingung lautet

$$1 = (e_{11}, e_{22}) = (ab', cd') = (a_1c_2 - a_2c_1)(b_1d_2 - -b_2d_1)$$

Das zeigt, daß $a = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$ und $c = \begin{pmatrix} c_1 \\ c_2 \end{pmatrix}$ nicht proportional sind, ebenso nicht b und d . Die Matrizen

$$A = \begin{pmatrix} a_1 & c_1 \\ a_2 & c_2 \end{pmatrix} \text{ und } B = \begin{pmatrix} b_1 & b_2 \\ d_1 & d_2 \end{pmatrix}$$

sind daher invertierbar, und man findet nach kurzer Rechnung

$$Ae_{11}B = T(e_{11}), \quad Ae_{22}B = T(e_{22})$$

Damit T eine orthogonale Transformation ist, muß $\det A \cdot \det B = 1$ sein. Setzt man

$$S(X) = A^{-1}T(X)B^{-1}$$

so ist S eine orthogonale Transformation mit $S(e_{11}) = e_{11}$ und $S(e_{22}) = e_{22}$.

Die Links- ebenso wie die Rechtsmultiplikation mit einer Matrix A, betrachtet als lineare Transformation des Vektorraumes der n-reihigen Matrizen, hat bekanntlich die Determinante $(\det A)^n$. Folglich hat $X \mapsto AXB$ die Determinante $(\det A \cdot \det B)^2$. Wegen $\det A \cdot \det B = 1$ ist das $= 1$. Die Transformation S bewirkt nun eine orthogonale Transformation mit Determinante 1 in der von e_{12} und e_{21} aufgespannten hyperbolischen Ebene. Alle solchen sind von der Gestalt

$$e_{12} \mapsto \lambda e_{12}, \quad e_{21} \mapsto \frac{1}{\lambda} e_{21}$$

Dies wird bewirkt durch die Transformation $X \mapsto CXC^{-1}$ mit $C = \begin{pmatrix} \lambda & 0 \\ 0 & 1 \end{pmatrix}$ (welche e_{11} und e_{22} fest läßt). Also gilt $T(X) = AC\,XC^{-1}B$ für alle X, und Lemma 1 ist bewiesen.

Damit die Abbildung $(A, B) \mapsto T_{A,B}$ ein Homomorphismus wird, definieren wir

$$T_{A,B}(X) = AXB'$$

Nach Satz 6 des vorigen Kapitels kann man A schreiben als $A = PD\Gamma$ mit P in der kompakten Untergruppe, einer Dreiecksmatrix $\begin{pmatrix} d_1 & * \\ 0 & d_2 \end{pmatrix}$ mit

$$|d_1| \leq c|d_2| \tag{1}$$

und $\Gamma \in GL(2, \mathbb{Q})$. Die Matrix $\begin{pmatrix} \frac{1}{\det \Gamma} & 0 \\ 0 & 1 \end{pmatrix} \cdot \Gamma$ liegt immer noch in $GL(2, \mathbb{Q})$ und hat aber Determinante 1. Den Faktor $\begin{pmatrix} \frac{1}{\det \Gamma} & 0 \\ 0 & 1 \end{pmatrix}^{-1}$ schlagen wir zu D (dabei ändern sich die $|d_i|$ nicht wegen der Produktformel) und erhalten eine neue Darstellung $A = PD\Gamma$ mit denselben $|d_i|$ und $\det \Gamma = 1$. Dasselbe machen wir mit der Matrix B und haben $B = QE\Delta$ mit $E = \begin{pmatrix} e_1 & * \\ 0 & e_2 \end{pmatrix}$ und

$$|e_1| \leq c|e_2| \tag{2}$$

Und dann ist

$$T_{A,B} = T_{P,Q} T_{D,E} T_{\Gamma,\Delta} \tag{3}$$

Um die $|\lambda_i|$ ins Spiel zu bringen, kehren wir zur Basis u_1, u_2, v_1, v_2 zurück. Bezüglich dieser Basis ist die Linksmultiplikation L_A mit A beschrieben durch

$$L_A = \begin{pmatrix} a_{11} & 0 & 0 & -a_{12} \\ 0 & a_{11} & a_{12} & 0 \\ 0 & a_{21} & a_{22} & 0 \\ -a_{21} & 0 & 0 & a_{22} \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12}W \\ -a_{21}W & a_{22} \end{pmatrix}$$

mit $W = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Für die Rechtsmultiplikation mit B' erhält man

$$R_{B'} = \begin{pmatrix} B & 0 \\ 0 & \tilde{B}' \end{pmatrix}, \quad \tilde{B} = \text{ Adjunkte von } B$$

1. Behauptung: Wenn $P \in SO(2,\mathbb{R})$, dann bilden L_P und $R_{P'}$ die Räume V^+ und V^- auf sich ab.
Beweis: V^+ war aufgespannt von $u_1 + v_1$ und $u_2 + v_2$. Nach der Identifikation von V mit dem Matrizenring sind dies die Matrizen $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Sie spannen den Raum aller $\begin{pmatrix} \lambda & -\mu \\ \mu & \lambda \end{pmatrix}$ auf, und dieser wird bei Links- und Rechtmultiplikation mit Drehmatrizen $\begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ auf sich abgebildet. Das Gleiche gilt für den Raum V^-, der aus allen $\begin{pmatrix} \lambda & \mu \\ \mu & -\lambda \end{pmatrix}$ besteht.

2. Behauptung: Wenn $P \in GL(2,\mathfrak{o}_p)$, dann bilden die Links- und Rechtsmultiplikationen mit P das Standardgitter $\mathfrak{o}_p u_1 + \mathfrak{o}_p v_1 + \mathfrak{o}_p u_2 + \mathfrak{o}_p v_2$ auf sich ab.
Beweis: Offensichtlich haben in diesem Falle die Matrizen L_P und R_P ganze Einträge und sind auch ganz invertierbar (weil $\det P$ Einheit in $\mathfrak{o}_p$ ist).

Folgerung: In der Zerlegung (1) ist $T_{P,Q} \in K$, also $T_{A,B} \in K \cdot T_{D,E} G_{\mathbb{Q}}$

Es bleibt also $T_{D,E}$ zu betrachten. Es ist

$$T_{D,E} = L_D R_{E'} = \begin{pmatrix} d_1 & * \\ 0 & d_2 \end{pmatrix} \begin{pmatrix} E & 0 \\ 0 & \tilde{E}' \end{pmatrix} = \begin{pmatrix} d_1 E & * \\ 0 & d_2 \tilde{E}' \end{pmatrix}$$

Die ersten beiden Diagonalglieder dieser Matrix sind $\lambda_1 = d_1 e_1$ und $\lambda_2 = d_1 e_2$. Da $T_{D,E}$ eine orthogonale Ttransformation ist, ist $\det D \cdot \det E = 1$, also $d_1 d_2 e_1 e_2 = 1$. Nun folgt

$$|\frac{\lambda_1}{\lambda_2}| = |\frac{e_1}{e_2}| \leq c \text{ nach (2)}$$

und

$$|\lambda_1 \lambda_2| = |d_1^2 e_1 e_2| = |\frac{d_1}{d_2}| \leq c \text{ nach (1)}$$

Das sind die Minkowski'schen Ungleichungen im Falle $n = 2r = 4$.

Satz 8. *Sei $n = 2r \geq 4$. Es gibt eine Konstante $c = c(V)$ mit der Eigenschaft: Zu $g \in G_A$ gibt es $\gamma \in G_{\mathbb{Q}}$ derart daß*

(4) $\qquad |\lambda_i(g\gamma)| \leq c|\lambda_{i+1}(g\gamma)$ *für* $i = 1, ..., r-1$ *und* $|\lambda_{r-1}(g\gamma)\lambda_r(g\gamma)| \leq c$

(4) sind die Minkowski'schen Ungleichungen, wenn $n = 2r$.
Beweis: Die ersten $r-1$ Ungleichungen folgen wie in Satz 7, Kapitel 5, wenn γ wie dort minimal gewählt wird. Wir behalten die Bezeichnungen aus Satz 7 bei. Nur der Raum W ist jetzt nicht mehr vorhanden. Wir schreiben

$$g\gamma = mp \text{ mit } p = (\lambda_1, ..., \lambda_r)\phi_{u_1 a_1} ....\phi_{u_{r-1} a_{r-1}}$$

$$= (\lambda_1, ..., \lambda_{r-2}, 1, 1)\phi_{u_1 b_1} .....\phi_{u_{r-2} b_{r-2}} \cdot (1, ..., 1, \lambda_{r-1}, \lambda_r)\phi_{u_{r-1} a_{r-1}}$$

mit $b_i = (1, ..., 1, \lambda_{r-1}, \lambda_r)\, a_i$. Wir setzen

$$(1, ..., 1, \lambda_{r-1}, \lambda_r)\phi_{u_{r-1} a_{r-1}} = \tilde{p}$$

Bei der natürlichen Einbettung von $G(H_{r-1} \perp H_r)$ in G wird die Standard- kompakte Untergruppe der ersteren in K abgebildet. Nach dem schon bewiesenen Fall $n = 4$ gibt es $\tilde{\gamma} \in G_{\mathbb{Q}}(H_{r-1} \perp H_r)$, welches wir uns durch Identität in $H_1 \perp .... \perp H_{r-2}$ auf V fortgesetzt denken, und $\tilde{m} \in G_A(H_{r-1} \perp H_r) \cap K$ mit

$$\tilde{p}\tilde{\gamma} = \tilde{m}(1, ..., 1, \mu_{r-1}, \mu_r)\phi_{u_{r-1} e}$$

mit einem gewissen Vektor $e \in (H_r)_A$, so daß

$$|\mu_{r-1}| \leq c|\mu_r| \text{ und } |\mu_{r-1}\mu_r| \leq c \tag{5}$$

Dann wird mit gewissen durch die Vertauschungsregeln entstehenden d_i

$$g\gamma\tilde{\gamma} = mp\tilde{\gamma} = m(\lambda_1, ..., \lambda_{r-2}, 1, 1)\phi_{u_1 b_1} ....\phi_{u_{r-2} b_{r-2}}\tilde{p}\tilde{\gamma}$$

$$= m(\lambda_1, ..., \lambda_{r-2}, 1, 1)\phi_{u_1 b_1} .....\phi_{u_{r-2} b_{r-2}}\tilde{m}(1, ..., 1, \mu_{r-1}, \mu_r)\phi_{u_{r-1} e}$$

$$= m\tilde{m}(\lambda_1, ..., \lambda_{r-2}, \mu_{r-1}, \mu_r)\phi_{u_1 d_1} .....\phi_{u_{r-2} d_{r-2}}\phi_{u_{r-1} e}$$

Daraus folgt

$$|\lambda_j(g\gamma\tilde{\gamma})| = |\lambda_j| \text{ für } j = 1, ..., r-2$$

$$|\lambda_j(g\gamma\tilde{\gamma})| = |\mu_j| \text{ für } j = r-1, r$$

Wegen der Minimalwahl von γ ist $|\lambda_{r-1}| \leq |\mu_{r-1}|$, also erst recht $|\lambda_{r-2}| \leq c|\lambda_{r-1}| \leq c|\mu_{r-1}|$. Zusammen mit (5) bedeutet das, daß mit $\gamma\tilde{\gamma}$ statt γ die sämtlichen Ungleichungen (4) bewiesen sind.

Mit Hilfe von Satz 7 und 8 wollen wir einen Bereich S in G_A konstruieren, der jedenfalls ein Vertretersystem für G_A nach $G_{\mathbb{Q}}$ enthält und von dem wir im nächsten Kapitel beweisen wollen, daß er endliches Volumen hat (für ein Haarsches Maß auf G_A). Man setzt zunächst

$$T_{A,c} = \{(\lambda_1, ..., \lambda_r) \mid |\lambda_i| \leq c|\lambda_{i+1}| \text{ für } i = 1, ..., r-1 \text{ und} \tag{6}$$

$$\begin{cases} |\lambda_r| \leq c & \text{wenn } n > 2r \\ |\lambda_{r-1}\lambda_r| \leq c & \text{wenn } n = 2r \end{cases}$$

und

$$N_A = \{\phi_{u_1 x_1} .....\phi_{u_r x_r} \mid x_i \in W_A^i\}$$

Dann besagen Satz 7 und 8: es gibt c so, daß

$$G_A = K \cdot T_{A,c} N_A G(W)_A \cdot G_{\mathbb{Q}} \tag{7}$$

Zuerst zerlegen wir $T_{A,c}$: Wir schreiben die Idele λ_i in der Form

$$\lambda_i = a_i \cdot (1, ..., \omega_{ip}, ...) \cdot (t_i, 1, ...) =: a_i \cdot \omega_i \cdot (t_i, 1, ...)$$

mit reellem $t_i > 0$ und Einheiten ω_{ip} in $\mathfrak{o}_p$ und einem Hauptidel $a_i \in \mathbb{Q}^*$. Das Tupel $\omega := (\omega_1, ..., \omega_r)$ ist in K, und $a := (a_1, ..., a_r) \in G_{\mathbb{Q}}$ Wir identifizieren die reelle Zahl t_i mit dem Idel $(t_i, 1, ...)$ und bezeichnen mit T_c die Menge aller Tupel $(t_1, ..., t_r)$, die den Minkowski'schen Ungleichungen (6) (im Folgenden mit (MU) abgekürzt) genügen. Der Torus T_A normalisiert die Gruppe N_A und ist elementweise mit $G(W)_A$ vertauschbar, und deshalb folgt aus (7), daß

$$G_A = K \cdot T_c \cdot N_A \cdot G(W)_A G_{\mathbb{Q}}$$

Nach dem Kompaktheitssatz gibt es ein Kompaktum $E \subset G(W)_A$ mit $G(W)_A = E \cdot G(W)_{\mathbb{Q}}$. Daraus haben wir

$$G_A = K \cdot T_c \cdot N_A \cdot E \cdot G_{\mathbb{Q}}$$

Mit Hilfe der Operation von $G_{\mathbb{Q}}$ von rechts wollen wir N_A noch verkleinern. (Die Idee dahinter ist: N ist aufgebaut aus additiven Gruppen, und $A = F + \mathbb{Q}$ mit einem relativ kompakten Fundamentalbereich F)

Zunächst stört E zwischen N_A und $G_{\mathbb{Q}}$. Wir schreiben also

$$\phi_{u_1 y_1} .... \phi_{u_r y_r} e = e \phi_{u_1 z_1} .... \phi_{u_r z_r}$$

mit $z_i = e^{-1} y_i$. Zur Abkürzung setzen wir $\phi_{u_2 z_2} .... \phi_{u_r z_r} = \Phi$. Wir haben

$$\Phi u_i = u_i + \sum_{j<i} \eta_{ji} u_j$$

mit gewissen durch $z_2, ..., z_r$ bestimmten η_{ji}.

$$\Phi v_i = v_i + \sum_{j>i} \eta^*_{ji} v_j + \sum_j \zeta_{ji} u_j + w_i$$

und für $w \in W_A$ ist mit gewissen Linearformen f_i

$$\Phi w = w - \sum_{i=2}^{r} f_i(w) u_i$$

Für einen Vektor

$$a_1 = \sum_{i=2}^{r} \lambda_i u_i + \sum_{i=2}^{r} \mu_i v_i + w$$

ist dann

$$\Phi a_1 = \sum_{j=2}^{r} [\lambda_j + \sum_{i>j} \lambda_i \eta_{ji} + \sum_i \mu_i \zeta_{ji} - f_j(w)] \; u_j + \sum_{j=2}^{r} [\mu_j + \sum_{i<j} \mu_i \eta^*_{ji}] \; v_j + \sum_{i=2}^{r} \mu_i w_i + w$$

und

$$\phi_{u_1 z_1}.....\phi_{u_r z_r}\phi_{u_1 a_1} = \phi_{u_1, z_1+\Phi a_1}\phi_{u_2 z_2}.....\phi_{u_r z_r}$$

Sei F ein Fundamentalbereich für A modulo $\mathbb{Q}$, zum Beispiel $[0,1) \times \prod_p \mathfrak{o}_p$. Zu gegebenen $z_1, ..., z_r$ wählt man jetzt zuerst $\mu_2 \in \mathbb{Q}$ so, daß die v_2-Komponente von $z_1 + \Phi a_1$ in F liegt. Danach wählt man μ_3 für die v_3-Komponente, usw. bis μ_r. Als nächstes wählt man $w \in W_{\mathbb{Q}}$ so, daß die W-Komponente von $z_1 + \Phi a_1$ in einem Fundamentalbereich F_W für W_A modulo $W_{\mathbb{Q}}$ liegt, zum Beispiel $F_W = \sum_i F b_i$, wenn $\{b_i\}$ eine Basis von $W_{\mathbb{Q}}$ über $\mathbb{Q}$ ist. Zuletzt wählt man die λ_j in der Reihenfolge $\lambda_r, ...\lambda_3, \lambda_2$. Das Ergebnis ist:

Zu $z_1, ..., z_r$ gibt es $a_1 \in W^1_{\mathbb{Q}}$ so, daß $z_1 + \Phi a_1 \in F_1 := \sum_{i\geq 2} F u_i + \sum_{i\geq 2} F v_i + F_W$. Das bedeutet

$$\phi_{u_1 z_1}.....\phi_{u_r z_r} \cdot \phi_{u_1 a_1} = \phi_{u_1 f_1}\phi_{u_2 z_2}....\phi_{u_r z_r} \text{ mit } f_1 \in F_1$$

Genauso können wir $a_2 \in W_{\mathbb{Q}}$ suchen, so daß

$$\phi_{u_2 z_2}.....\phi_{u_r z_r}\phi_{u_2 a_2} = \phi_{u_2 f_2}\phi_{u_3 z_3}.....\phi_{u_r z_r}$$

Schließlich haben wir $a_1, ..., a_r$ mit $a_i \in W^i_{\mathbb{Q}}$, so daß

$$\phi_{u_1 z_1}.....\phi_{u_r z_r} \cdot \phi_{u_1 a_1}.....\phi_{u_r a_r} = \phi_{u_1 f_1}.....\phi_{u_r f_r} \text{ mit } f_i \in F_1$$

Damit ist oben

$$\phi_{u_1 y_1}.....\phi_{u_r y_r} e = e\phi_{u_1 f_1}.....\phi_{u_r f_r}(\phi_{u_1 a_1}.....\phi_{u_r a_r})^{-1}$$

$$\in e\phi_{u_1 f_1}....\phi_{u_r f_r} \cdot G_{\mathbb{Q}} = \phi_{u_1, ef_1}.....\phi_{u_r, ef_r} \cdot eG_{\mathbb{Q}}$$

Wenn e durch das Kompaktum E läuft, dann bleiben die $\phi_{u_1, ef_1}.....\phi_{u_r, ef_r}$ in einem Kompaktum $N_F \subset N_A$, und wir haben

$$G_A = K \cdot \{(t_1, ..., t_r)\} \cdot N_F \cdot E \cdot G_{\mathbb{Q}}$$

wobei die reellen positiven Zahlen $t_1, ..., t_r$ den MU genügen. Bezeichnen wir die Menge dieser r-Tupel mit T_c, so folgt, daß $K \cdot T_c \cdot N_F \cdot E$ einen Fundamentalbereich für G_A nach $G_{\mathbb{Q}}$ enthält.

7. Integration auf homogenen Räumen

Dieses Kapitel dient dazu, das Volumen eines Fundamentalbereichs für G_A nach $G_{\mathbb{Q}}$ nach oben abzuschätzen.

Nach Kapitel 6 enthält die Menge $KT_cN_FE \subset G_A$ ein Vertretersystem für G_A modulo $G_{\mathbb{Q}}$. Wir wollen zeigen, daß sie endliches Volumen hat für das Haarsche Maß auf G_A. Zu Existenz und Eigenschaften des Haarschen Maßes siehe zum Beispiel [W1]. Die wichtigste Eigenschaft ist die Invarianz unter Translation in der Gruppe: Ist f_a die um a verschobene Funktion, also $f_a(x) = f(ax)$, so ist

$$\int f_a(x)\, dx = \int f(x)\, dx \quad (\text{ Linksinvarianz })$$

Ein wichtiger Satz ist, daß das Haarsche Maß bis auf einen (positiven reellen) Faktor eindeutig bestimmt ist.

Definition: Eine Gruppe heißt unimodular, wenn das linksinvariante Maß auch rechtsinvariant ist.

Ist G kompakt, so ist die konstante Funktion Eins integrierbar. Sie ist gleich allen ihren Translaten: Jede kompakte Gruppe ist unimodular.

Satz 9. *Die Gruppen $G_{\mathbb{Q}_v}$ sind unimodular.*

Beweis: Sei G eine der Gruppen $G_{\mathbb{R}}$, $G_{\mathbb{Q}_p}$. Sei $\int f(x)dx$ linksinvariant. Für festes $a \in G$ ist $f \mapsto \int f(xa)dx$ linksinvariant. Wegen der Eindeutigkeit des Haarschen Maßes ist es proportional zu $\int f(x)dx$, der Proportionalitätsfaktor hängt natürlich von a ab:

$$\int f(xa)dx = \chi(a) \int f(x)dx \text{ für alle } f$$

χ ist ein Homomorphismus von G in die multiplikative Gruppe der positiven reellen Zahlen. Auf der Kommutatorgruppe von G muß er gleich 1 sein. Nun beobachten wir:

1. Die spezielle orthogonale Gruppe eines Vektorraumes V über einem beliebigen Körper K der Charakterisik $\neq 2$ wird von Umlegungen erzeugt. (Eine orthogonale Transformation ϕ heißt Umlegung, wenn V eine Zerlegung $V = A \perp B$ besitzt, so daß $\phi = 1$ auf A und $\phi = -1$ auf B und $\dim B = 2$.)
Nämlich: Eine Umlegung ist ein Produkt von zwei Spiegelungen mit zueinander senkrechten Spiegelungsvektoren. Bekanntlich wird die volle orthogonale Gruppe von Spiegelungen erzeugt, die spezielle also von den ST, wenn S und T Spiegelungen sind. Wenn $s^\perp \cap t^\perp$ einen nicht isotropen Vektor r enthält, dann ist $ST = SR \cdot RT$ Produkt von zwei Umlegungen. Ist das nicht der Fall, so ist $s^\perp \cap t^\perp$ total isotrop, also $\subset Ks + Kt$. Das geht nur, wenn $n - 2 \leq 2$, also $n \leq 4$ ist. Aber $n = 4$ scheidet aus, weil dann $s^\perp \cap t^\perp = Ks + Kt$ total isotrop wäre, was nicht geht, weil s nicht isotrop ist. Also ist $n = 3$. Dann sind $-S$ und $-T$ Umlegungen, und $ST = (-S)(-T)$.

2. Ist G eine Gruppe mit lauter involutorischen Erzeugenden, so liegen alle Quadrate in der Kommutatorgruppe G' von G; nämlich:

$$(a_1....a_k)^2 = a_1a_2....a_k. \cdot a_1^{-1}....a_k^{-1} \equiv (a_2....a_k)^2 \bmod G'$$

Nach 1 und 2 liegen alle Quadrate im Kern von χ:

$$1 = \chi(a^2) = \chi(a)^2 \text{ für alle } a \in G$$

Da die Werte von χ positive reelle Zahlen sind, folgt $\chi = 1$.

Als nächstes wollen wir invariante Maße auf gewissen homogenen Räumen konstruieren.

Definition: Ist G eine lokal kompakte Gruppe und K eine abgeschlossene Untergruppe, so heißt

$$\{Kg \mid g \in G\} =: K\backslash G$$

ein homogener Raum von G.

$$\pi : g \mapsto Kg$$

ist eine Abbildung von G auf $K\backslash G$. Auf $K\backslash G$ operiert G transitiv von rechts vermöge $(Kg)g_0 = K(gg_0)$. Der Raum $K\backslash G$ wird topologisiert, indem die offenen Mengen von $K\backslash G$ genau die Bilder $\pi(U)$ der offenen Mengen U von G sind. Damit ist π stetig und offen.

Satz 10. *G sei unimodular und K eine kompakte Untergruppe von G und dx bzw. dk Haarsche Maße auf G bzw. K. Dann gibt es ein unter der Operation von G invariantes Integral dP auf dem homogenen Raum $K\backslash G$ mit*

$$\int_G f(x)dx = \int_{K\backslash G} \{\int_K f(kx)dk\}dP \quad (P = \pi(x))$$

Bis auf einen konstanten Faktor ist dP das einzige rechtsinvariante Integral auf $K\backslash G$.

Beweis: Sei F eine stetige Funktion mit kompaktem Träger C auf $K\backslash G$. Nach Lemma 2, Kapitel 4 gibt es zu C ein partielles kompaktes Urbild $C' \subset G$. Es gibt eine stetige Funktion Φ mit kompaktem Träger auf G mit Werten zwischen 0 und 1, die auf C' immer gleich 1 ist (Urysohn). Dann setzt man

$$f(x) = \begin{cases} \frac{F(Kx)\Phi(x)}{\int_K \Phi(kx)dk} & \text{wenn } \int_K \Phi(kx)dk \neq 0 \\ 0 & \text{sonst} \end{cases}$$

Diese Funktion ist stetig mit kompaktem Träger auf G und so konstruiert, daß

$$\int_K f(kx)dk = F(Kx) \text{ für alle } x \in G \tag{1}$$

(Dabei wird die Rechtsinvarianz von dk ausgenutzt). Wir können f über G integrieren. Wir behaupten, daß das $\int_G f(x)dx$ von der Wahl der Funktion Φ unabhängig ist; nämlich: Wir zeigen, daß alle f, die (1) erfüllen, dasselbe $\int_G f(x)dx$ besitzen. Oder, durch Differenzbildung:

$$\text{wenn } \int_K f(kx)dk = 0 \text{ für alle } x \in G, \text{ dann ist } \int_G f(x)dx = 0$$

Um das zu zeigen, sei h eine beliebige stetige Funktion mit kompaktem Träger auf G Wenn $\int_K f(kx)dk = 0$ für alle $x \in G$, dann ist

$$0 = \int_G h(x^{-1}) \cdot \{\int_K f(kx)dk\}\ dx = \int_G \int_K h(x^{-1}) f(kx)dk\, dx$$

$$= \int_K \int_G h(x^{-1}) f(kx)dx\, dk \text{ nach Fubini}$$

$$= \int_K \int_G h(x^{-1}k) f(x)dx\, dk \text{ weil } dx \text{ auch linksinvariant}$$

$$= \int_G f(x)\ \{\int_K h(x^{-1}k)dk\}\ dx \text{ wieder nach Fubini} \tag{2}$$

Sei C der Träger von f. Dann ist $C^{-1}K$ eine kompakte Teilmenge von G. Es gibt eine stetige Funktion h mit kompaktem Träger, welche auf $C^{-1}K$ überall gleich 1 ist (Urisohn's Lemma) . Für diese gilt

$$f(x) \neq 0 \Rightarrow x \in C \Rightarrow h(x^{-1}k) = 1 \text{ für alle } k \in K \Rightarrow \int_K h(x^{-1}k)dk = \int_K dk = const \neq 0$$

Aus (2) folgt $\int_G f(x)dx = 0$.

Jetzt ist

$$J(F) := \int_G f(x)dx$$

wohldefiniert. Statt $J(F)$ schreibt man auch $\int_{K\backslash G} F(P)dP$. Dann hat man die Formel

$$\int_G f(x)dx = \int_{K\backslash G} \{\int_K f(kx)dk\}\ dP \tag{3}$$

worin gemeint ist, daß $P = Kx$. Offensichtlich ist dP rechtsinvariant unter G. Ist umgekehrt $d\mu(P)$ irgendein rechtsinvariantes Integral auf $K\backslash G$, so definiert die rechte Seite von (3) mit $d\mu(P)$ statt dP ein rechtsinvariantes Integral auf G. Dieses ist bis auf einen Faktor bestimmt. Also ist

$$\int_{K\backslash G} \{\int_K f(kx)dk\}\ d\mu(P) = \rho \int_{K\backslash G} \{\int_K f(kx)dk\}\ dP$$

Da wie gesehen jede stetige Funktion mit kompaktem Träger auf $K\backslash G$ sich als ein Integral über K darstellen läßt, folgt die Eindeutigkeit von dP bis auf einen Faktor.

Zusatz: Daß G unimodular ist, wurde in der letzten Zeile vor (2) ausgenutzt. Genau besehen wurde aber nur benutzt, daß dx invariant unter Linksmultiplikation mit Elementen aus K ist ($d(k^{-1}x) = dx$). Im allgemeinen ist $d(ax) = \Delta(a) \cdot dx$, wo Δ ein stetiger Homomorphismus von G in die positive reelle Achse ist. Und für den Schluß hat es genügt, daß $\Delta(k) = 1$ ist für alle $k \in K$. Das ist aber sicher der Fall, wenn K kompakt ist. Auf die Voraussetzung " G unimodular" kann also bei kompaktem K verzichtet werden. (vgl. [W1], Seite 45).

Zuletzt benötigen wir noch einen Isomorphiesatz, der für abstrakte Gruppen wohlbekannt und sehr leicht zu beweisen ist. Aber es ist nicht ganz trivial zu zeigen, daß er auch topologisch gilt:

Sei G eine lokal kompakte Gruppe, K eine kompakte und B eine abgeschlossene Untergruppe und $G = KB$. Die Abbildung $\bar{f}(b) = Kb$ von B nach $K\backslash G$ ist wegen $G = KB$ surjektiv, und

$$\bar{f}(b_1) = \bar{f}(b_2) \Leftrightarrow b_1 \in (K \cap B)b_2$$

Sie definiert also eine Bijektion

$$f \ : \ (K \cap B)\backslash B \to K\backslash G$$

Satz 11. *f ist stetig und offen.*

Beweis: Wir zeigen, daß eine Folge $(K\cap B)b_n$ in $(K\cap B)\backslash B$ genau dann gegen $(K\cap B)b$ konvergiert, wenn die Bildfolge Kb_n in $K\backslash G$ gegen Kb konvergiert. Indem man um b^{-1} verschiebt, sieht man, daß es genügt, $b = 1$ zu nehmen. Dann bedeutet ersteres:
Zu jeder offenen Einsumgebung U in B gibt es n_0 so, daß

$$(K \cap B)b_n \subset (K \cap B)U, \text{ das heißt } b_n \in (K \cap B)U \text{ für } n > n_0$$

Das zweite bedeutet: Zu jeder offenen Einsumgebung W in G gibt es n_0 , so daß

$$Kb_n \subset KW, \text{ das heißt } b_n \in KW \text{ für } n > n_0$$

Die offenen Mengen von B sind die Durchschnitte der offenen Mengen von G mit B. Die beiden Aussagen sind daher äquivalent, wenn gilt
1. Zu jedem offenen $W \ni 1$ in G gibt es offenes $U \ni 1$ in G so, daß

$$(K \cap B)(U \cap B) \subset KW$$

und
2. Zu jedem offenen $U \ni 1$ in G gibt es offenes $W \ni 1$ in G so, daß

$$KW \cap B \subset (K \cap B)(U \cap B)$$

Das erste ist trivial (mit $U = W$) . Die zweite Formel ist äquivalent mit

$$KW \cap B \subset (K \cap B)U$$

Ist nun offenes $U \ni 1$ in G gegeben, so wählt man zuerst eine offene Einsumgebung V mit $V^2 \subset U$ und betrachtet dann

$$K' := \{k \in K \mid k \notin (K \cap B)V\}$$

K' ist abgeschlossen in K, also auch kompakt. B ist abgeschlossen in G, sein Komplement also offen in G. Daher gibt es zu $g \notin B$ eine offene Einsumgebung Y mit

$$gY \cap B = \emptyset$$

oE $Y = Y^{-1}$. Dann ist $g \notin BY$. Es gibt eine offene Einsumgebung Y_1 mit $Y_1^2 \subset Y$. Damit ist $g \notin BY_1 \cdot Y_1$ und daher $g \notin \overline{BY_1}$. Das zeigt: Zu $g \notin B$ gibt es eine offene Einsumgebung W so, daß $g \notin \overline{BW}$. Nun sind aber alle $k' \in K'$ nicht in B, und es folgt

$$K' \cap \bigcap_{W\ offen \ni 1} \overline{BW} = \emptyset.$$

Da K' kompakt, ist bereits ein endlicher Durchschnitt leer:

$$K' \cap \bigcap_{i=1}^{N} \overline{BW_i} = \emptyset \quad \text{erst recht } K' \cap \bigcap_{i=1}^{N} BW_i = \emptyset$$

Nach Definition von K' heißt das

$$K \cap \bigcap_{i=1}^{N} BW_i \subset (K \cap B)V$$

Setzt man $W_0 = V \cap \bigcap_{i=1}^{N} W_i$ und $W = W_0 \cap W_0^{-1}$, so ist W eine offene Einsumgebung, und aus $K \cap BW \subset (K \cap B)V$ folgt

$$KW \cap B \subset (K \cap BW)W \subset (K \cap B)VW \subset (K \cap B)V^2 \subset (K \cap B)U$$

Damit ist Satz 11 bewiesen.

Die Sätze 10 und 11 wollen wir benutzen, wenn $G = G_A$ die Adelgruppe der speziellen orthogonalen Gruppe und K die in Kapitel 2 beschriebene kompakte Untergruppe von G_A ist. Die Gleichung $G_A = KB_A$ bleibt erhalten, wenn wir B_A durch $B_A^+ = \{b \in B_A \mid \lambda_{i,\infty}(b_\infty) > 0\})$ ersetzen. In Kapitel 6 sahen wir, daß für genügend großes c die Menge $S_c = KT_cN_FE$ die Eigenschaft $G_A = S_c \cdot G_{\mathbb{Q}}$ besitzt. Wir wollen das Volumen von S_c (für das Haarsche Maß von G_A) nach oben abschätzen. Sei f die Indikatorfunktion von S_c. Im Sinne von Satz 10 ist

$$\int_{G_A} f(g)\, dg = \int_{K\backslash G_A} (\int_K f(kg)dk\ )d\dot{g}$$

Das innere Integral ist $= \int_K dk$, wenn $g \in S_c$ und $= 0$ sonst. Nun ist $K\backslash G_A = K\backslash KB_A^+ \simeq (K \cap B_A^+)\backslash B_A^+$, und nach Satz 11 ist dieser Isomorphismus stetig und offen. Außerdem ist er mit Multiplikationen von rechts mit Elementen aus B_A^+ vertauschbar. deshalb tranportiert er das rechtsinvariante Maß $d\dot{g}$ von $K\backslash G_A$ in ein rechtsinvariantes Maß auf $(K \cap B_A^+)\backslash B_A^+$. Bis auf einen Faktor gibt es aber nur ein solches, nämlich das von B_A^+ geerbte $d\dot{b}$ (letzte Aussage in Satz 10). Der Integrationsbereich $K\backslash S_c$ geht dabei über in $(K \cap B_A^+)\backslash (K \cap B_A^+)T_cN_FE$. Wendet man wieder Satz 10 an, so erhält man schließlich

$$\int_{G_A} f(g)\, dg = \frac{\int_K dk}{\int_{K \cap B_A^+} dk'} \cdot \int_{B_A^+} \tilde{f}(b)\, db$$

Dabei ist $\tilde{f}$ die Indikatorfunktion von $S_c \cap B_A^+ = (K \cap B_A^+)T_cN_FE$. Wir beschreiben $K \cap B_A^+$ komponentenweise:

1. $K_\infty \cap B_\infty^+ = \{b = (t_1, ..., t_r)\phi_{u_1 a_1} ... \phi_{u_r a_r} q \in K_\infty\}$. Die t_i sind reell > 0 und homomorphe Bilder von $b \in B_\infty$. Wenn b in einer kompakten Untergruppe läuft, sind sie gleich 1. Die a_i laufen in reellen Vektorräumen. Aus den Vertauschungsregeln für die Eichlertransformationen sieht man, daß $b \mapsto a_r$ ein Homomorphismus in die additive Gruppe W_∞^r ist. Auf einer kompakten Untergruppe ist er gleich 0. Danach sieht man dasselbe für a_{r-1} usw. Zum Schluß folgt

$$K_\infty \cap B_\infty^+ = K_\infty \cap G(W)_\infty$$

2. $K_p \cap B_p = G(M_p) \cap B_p \subset G(M_p)$ für alle p.

Die Vertretersysteme F_i für W_A^i nach $W_{\mathbb{Q}}^i$ kann man in der Form $F_{i\infty} \times \prod_p (W_{\mathbb{Q}_p}^i \cap M_p)$ wählen. Dadurch sind die Elemente von $(N_F)_\infty$ Produkte von Eichlertransformationen $\phi_{u_i a_i}$ bei denen die a_i in einem (beschränkten) Quader in W_∞^i liegen, und die $(N_F)_p$ liegen in $G(M_p)$. Wir erhalten

$$(K_\infty \cap B_\infty^+) T_c N_{F,\infty} E_\infty \subset (K_\infty \cap G(W)_\infty) T_c N_{F,\infty} E_\infty \subset T_c N_{F^*,\infty} E_\infty^*$$

F^* besteht aus Transformierten von F unter $K_\infty \cap G(W)_\infty$ und ist deshalb in einem beschränkten Quader enthalten. E_∞^* ist als Produkt zweier kompakter Mengen ebenfalls kompakt.

$$(K_p \cap B_p^+) N_{F,p} E_p \subset G(M_p) E_p =: E_p^*$$

Da E kompakt, ist E_p kompakt für alle p und $\subset G(W \cap M_p) \subset G(M_p)$ für fast alle p, und daher ist $\prod_p E_p^*$ kompakt.

Wir zerlegen

$$B_A^+ = B_\infty^+ \times B^{+f}$$

Darin ist

$$(K \cap B_A^+) T_c N_F E \subset [T_c N_{F^*,\infty} E_\infty^*] \times \prod_p E_p^*$$

B^{+f} ist eine lokal kompakte Gruppe mit einem Haarschen Maß, und $\prod E_p^*$ ist ein Kompaktum darin. Die Menge $(K \cap B_A^+) T_c N_F E$ hat in B_A^+ endliches Volumen genau dann, wenn $T_c N_{F^*,\infty} E_\infty^*$ endliches Volumen in B_∞^+ hat. Dieses ist leicht abzuschätzen, wenn man einmal ein Haarsches Maß auf B_∞^+ gefunden hat: In $b = (t_1, ..., t_r)\phi_{u_1 x_1} .... \phi_{u_r x_r} q$ sind die t_i, die x_i sowie q durch b bestimmt. Wir benutzen die Lebesgue-Maße dt_i auf der positiven reellen Achse und die in Kapitel 3 beschriebenen Maße dx_i auf den W_A^i und irgendein Haarsches Maß dq auf $G(W)_A$. Dann bestimmen wir die Funktion h so, daß $h \cdot dt_1 .... dt_r dx_1 .... dx_r dq$ rechtsinvariant ist. Dazu benutzen wir die im vorigen Kapitel hergeleitete Formel für die Rechtsverschiebung:

$$\phi_{u_1 x_1} ..... \phi_{u_r x_r} \cdot \phi_{u_1 a_1} .... \phi_{u_r a_r} = \phi_{u_1 y_1} .... \phi_{u_r y_r}$$

wo $y_i = x_i + f_i$ und die f_i nur von $x_{i+1}, ... x_r$ und den a_i abhängen. Wenn $\alpha = (\alpha_1, ..., \alpha_r) \in T$, dann ist

$$\phi_{u_1 x_1} ..... \phi_{u_r x_r} \cdot \alpha = \alpha \cdot \phi_{u_1, \alpha_1^{-1} \alpha^{-1} x_1} ..... \phi_{u_r, \alpha_r^{-1} \alpha^{-1} x_r}$$

Wenn also

$$(t_1, ..., t_r)\phi_{u_1 x_1} ..... \phi_{u_r x_r} \cdot (\alpha_1, ..., \alpha_r)\phi_{u_1 a_1} .... \phi_{u_r a_r} = (t_1^*, ..., t_r^*)\phi_{u_1 x_1^*} ..... \phi_{u_r x_r^*}$$

dann ist

$$t_i^* = \alpha_i t_i \quad \text{und } x_i^* = \alpha_i^{-1}\alpha^{-1}x_i + \{ \text{ Vektoren, die nur von } x_{i+1}, ..., x_r \text{ abhängen } \}$$

Die Funktionaldeterminante ist

$$\frac{\partial(t_1^*, ..., t_r^*, x_1^*, ..., x_r^*)}{\partial(t_1, , , , .t_r, x_1, ...x_r)} = \prod_{i=1}^{r} \alpha_i^{1-\dim W^i} = \prod_{i=1}^{r} \alpha_i^{1-(n-2i)}$$

Folgerung:

$$db = \prod_{i=1}^{r} t_i^{n-2i-1} dt_1....dt_r dx_1....dx_r dq$$

ist rechtsinvariant auf B_∞^+ .

Nun ist das Volumen von $T_c N_{F^*,\infty} E_\infty^*$ gleich

$$\int_{T_c} \prod_{i=1}^{r} t_i^{n-2i-1} dt_1....dt_r \cdot \int_{N_{F^*,\infty}} dx_1.....dx_r \cdot \int_{E_\infty^*} dq$$

Der zweite und dritte Faktor sind endlich. Um den ersten Faktor auszurechnen, unterscheiden wir zwei Fälle:

$n > 2r$: Zu integrieren ist über den Bereich $0 < t_i \leq ct_{i+1}$ für $i = 1, ..., r-1$ und $0 < t_r \leq c$. Wir substituieren

$$s_i = \frac{t_i}{t_{i+1}} \text{ für } i < r \text{ und } s_r = t_r$$

mit der Umkehrung

$$t_r = s_r, \quad t_{r-1} = s_{r-1}s_r, ..., t_1 = s_1.....s_r$$

Der t-Bereich geht dabei über in den Quader Q: $0 < s_i \leq c$ für $i = 1, ..., r$. Die Funktionaldeterminante ist

$$\frac{\partial(t_1, ..., t_r)}{\partial(s_1, ..., s_r)} = \begin{vmatrix} s_2....s_r & * & ..... & * \\ 0 & s_3....s_r & ..... & * \\ \vdots & \ddots & & * \\ 0 & ..... & & 1 \end{vmatrix} = s_2 s_3^2 .....s_r^{r-1}$$

Man erhält das

$$\int_Q \prod_{i=1}^{r} (s_i....s_r)^{n-2i-1} \cdot \prod_{i=1}^{r} s_i^{i-1} \; ds_1.....ds_r$$

Nach Zusammenfassem der s_i-Potenzen ist das

$$\int_Q \prod_{j=1}^{r} s_j^{j(n-j-1)-1} ds_1....ds_r$$

Da $1 \le j \le r$ und $n \ge 2r+1$, sind die Exponenten $\ge 1 \cdot (2r+1-r-1)-1 = r-1 \ge 0$. Daher ist das Integral $< \infty$.

$n = 2r(\ge 4)$: Die MU sind jetzt $0 < t_i \le c t_{i+1}$ für $i = 1, ..., r-1$ und $0 < t_{r-1} t_r \le c$. Wir benutzen dieselbe Substitution wie oben und erhalten denselben Integranden, aber einen anderen Integrationsbereich, nämlich

$$0 < s_i \le c \text{ für } i < r \text{ und } 0 < s_{r-1} s_r^2 \le c$$

Die Integrale über die s_i mit $i < r-1$ sind dieselben wie oben. Aber für die letzten beiden Koordinaten erhalten wir jetzt

$$\int_{0<s_{r-1}\le c,\ 0<s_{r-1}s_r^2\le c} s_{r-1}^{(r-1)r-1} s_r^{r(r-1)-1} ds_{r-1} ds_r = \int_0^c \int_0^{\sqrt{\frac{c}{x}}} (xy)^{r(r-1)-1}\, dx\, dy$$

Eine kurze Rechnung ergibt den Wert $\frac{2c^{r(r-1)}}{[r(r-1)]^2}$. Damit ist bewiesen

Satz 12. *Für alle $c > 0$ hat der Bereich*

$$S_c = K \cdot T_c N_F E \subset G_A$$

endliches Volumen, und für genügend große c ist

$$G_A = S_c \cdot G_{\mathbb{Q}}$$

8. Die orthogonale Gruppe als reelle Mannigfaltigkeit

Das Haarsche Maß auf einer lokal kompakten Gruppe ist nur bis auf einen Faktor bestimmt. Ist jedoch G die spezielle orthogonale Gruppe einer über $\mathbb{Q}$ definierten quadratischen Form, so besitzt ihre Adelgruppe G_A ein ausgezeichnetes invariantes Integral , das sogenannte Tamagawa -Maß. Dieses soll in den nächsten Kapiteln beschrieben werden. Dazu benötigt man eine bereits über $\mathbb{Q}$ definierte Differentialform, mit der man dann in allen $\mathbb{Q}_v$ rechnen kann.

A sei eine symmetrische Matrix mit rationalen Einträgen, und nicht singulär. Die zugehörige reelle spezielle orthogonale Gruppe ist

$$G = \{P \in M_n(\mathbb{R}) \mid P'AP = A,\ \det P = 1\}$$

Sie ist in der offenen Teilmenge $\det P > 0$ des n^2-dimensionalen Raumes $M_n(\mathbb{R})$ das Nullstellengebilde von $F(P) = P'AP - A$. Als solches ist G eine reelle Mannigfaltigkeit der Dimension $\frac{n(n-1)}{2}$, nämlich:

Nach Definition beschreibt $F : \mathbb{R}^m \to \mathbb{R}^k$ durch $F(P) = 0$ eine Mannigfaltigkeit G der Dimension $m - k$, wenn F in jedem Punkt P_0 von G differenzierbar ist und die Funktionalmatrix (Jacobi-Matrix) $D_{P_0}F$ den Rang k hat. Diese Funktionalmatrix ist in unserem Falle eine Matrix mit $\frac{n(n+1)}{2}$ Zeilen und n^2 Spalten, die man sich lieber nicht (in irgendeiner Anordnung der Zeilen und Spalten) hingeschrieben vorstellen möchte. Stattdessen gehen wir auf die Definition der Differenzierbarkeit von Abbildungen von $\mathbb{R}^{n^2}$ nach $\mathbb{R}^{\frac{n(n+1)}{2}}$ zurück: F ist differenzierbar im Punkte P_0, wenn es eine lineare Abbildung $L = L_{P_0}$ vom $\mathbb{R}^{n^2}$ in den $\mathbb{R}^{\frac{n(n+1)}{2}}$ gibt , derart daß

$$F(P) - F(P_0) = L(P - P_0) + \ Rest(P; P_0) \quad \text{mit } \frac{|Rest|}{|P - P_0|} \to 0 \text{ für } P \to P_0$$

L ist dann die Jacobi-Abbildung. Hier haben wir

$$F(P) - F(P_0) = P'AP - P_0'AP_0 = (P' - P_0')AP_0 + P_0'A(P - P_0) + (P' - P_0')A(P - P_0)$$

Der letzte Term ist quadratisch in $P - P_0$, also können wir L_{P_0} ablesen:

$$L_{P_0}(X) = X'AP_0 + P_0'AX$$

Alle Matrizen $L_{P_0}(X)$ sind symmetrisch. Umgekehrt: Wenn $S = S'$, so muß man nur $X = \frac{1}{2}A^{-1}P_0'^{-1}S$ setzen (beachte, daß die $P_0 \in G$ invertierbar sind), um $L_{P_0}(X) = S$ zu erhalten. Also besteht das Bild von L_{P_0} aus allen symmetrischen Matrizen. Nach Definition ist G eine Mannigfaltigkeit der Dimension $n^2 - \frac{n(n+1)}{2} = \frac{n(n-1)}{2}$.

Der Tangentialraum am Einselement besteht nach Definition aus allen X mit $L_1(X) = 0$. Hier ist also

$$T_1(G) = \{X \in M_n(\mathbb{R}) \mid AX + X'A = 0\}$$

Es gibt nun für die orthogonale Gruppe eine Besonderheit: Man kann die (0 enthaltende) offene Teilmenge $\det(1+X) \neq 0$ des Tangentialraumes *rational* auf die offene (Eins enthaltende) Teilmenge $\det(1+P) \neq 0$ in G abbilden und dadurch eine Parameterdarstellung erhalten. Dies ermöglicht es, dieselben Rechnungen in anderen Erweiterungskörpern von $\mathbb{Q}$ außer $\mathbb{R}$ anzustellen, zum Beispiel in den $\mathbb{Q}_p$. Doch bleiben wir zunächst in $\mathbb{R}$.

Wenn A positiv definit ist, dann ist die Parameterdarstellung sogar überall definiert:

Lemma 1. *Wenn $A = A'$ positiv definit und AX schief und $\epsilon = \pm 1$, dann ist $1+\epsilon X$ invertierbar.*

Beweis: Wenn $v \in \mathbb{R}^n$ und $(1+\epsilon X)v = 0$, dann ist

$$v'Av = -v'A\epsilon Xv = \epsilon v'(AX)'v = \epsilon v'X'Av = -\epsilon^2 v'Av = -v'Av$$

Daraus folgt $v = 0$.

Im allgemeinen beschränken wir uns auf den offenen Teil $\det(1+X) \neq 0$ von $T_1(G)$. Dort ist

$$f(X) = (1+X)^{-1}(1-X)$$

wohldefiniert.

Satz 13. *(Cayley) Die Abbildung f ist eine Bijektion von $\{X \in T_1(G) \mid \det(1+X) \neq 0\}$ auf $\{Y \in G \mid \det(1+Y) \neq 0\}$.*

Beweis: 1. Wenn $X \in T_1(G)$ und $\det(1+X) \neq 0$, dann ist $f(X) \in G$, nämlich:

$$f(X)'Af(X) = (1-X')(1+X')^{-1}A(1+X)^{-1}(1-X) =$$

$$(1+AXA^{-1})(1-AXA^{-1})^{-1}A(1+X)^{-1}(1-X) = A$$

und

$$\det(1-X) = \det(1-X') = \det(1-A^{-1}X'A) = \det(1+X), \text{ also } \det[(1+X)^{-1}(1-X)] = 1$$

Also ist $f(X) \in G$. und

$$\det(1+f(X)) = \det(1+(1+X)^{-1}(1-X)) = \det\{(1+X)^{-1}\cdot 2\} \neq 0$$

2. Sei $P \in G$ und $\det(1+P) \neq 0$. Man setzt $X = (1+P)^{-1}(1-P)$. Dann ist

$$AX + X'A = A(1+P)^{-1}(1-P) + (1-P')(1+P')^{-1}A =$$

$$A(1+P)^{-1}(1-P) + (1-AP^{-1}A^{-1})(1+AP^{-1}A^{-1})^{-1}A$$
$$= A(1+P)^{-1}(1-P) + A(1-P^{-1})(1+P^{-1})^{-1} = 0$$

und

$$\det(1+X) = \det(1+(1+P)^{-1}(1-P)) = \det(1+P)^{-1}\det(1+P+1-P) \neq 0$$

Also liegt tatsächlich X im Teil $\det(1+X) \neq 0$ von $T_1(G)$, und man rechnet leicht nach, daß $f(X) = P$ (die Matrix $\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$ ist bis auf einen Faktor ihre eigene Inverse). Damit sieht man auch, daß f bijektiv ist.

Jetzt wollen wir feststellen, wie die Gruppenmultiplikation im Tangentialraum aussieht. Das heißt, zu gegebenem X, Y in $T_1(G)$ suchen wir $Z \in T_1(G)$ mit $f(Z) = f(X)\cdot f(Y)$.

$$f(Z) = f(X)\cdot f(Y) \Leftrightarrow Z = (1-f(X)\cdot f(Y))(1+f(X)\cdot f(Y))^{-1} \Leftrightarrow$$

$$Z = [1-(1+X)^{-1}(1-X)(1+Y)^{-1}(1-Y)]\cdot[1+(1+X)^{-1}(1-X)(1+Y)^{-1}(1-Y)]^{-1}$$
$$= (1+X)^{-1}[(1+X)(1+Y)-(1-X)(1-Y)](1+Y)^{-1}\cdot$$
$$\{(1+X)^{-1}[(1+X)(1+Y)+(1-X)(1-Y)](1+Y)^{-1}\}^{-1}$$
$$= (1+X)^{-1}(X+Y)(1+XY)^{-1}(1+X)$$

Setzt man also

$$\lambda_X(Y) = (1+X)^{-1}(X+Y)(1+XY)^{-1}(1+X) \tag{1}$$

so gilt

1. $\lambda_X(Y)$ ist definiert für alle $X, Y \in T_1(G)$ mit $\det(1+X)\cdot\det(1+Y)\cdot\det(1+XY) \neq 0$
2. Für alle $X, Y \in T_1(G)$ mit $\det(1+X)\det(1+Y)\det(1+XY) \neq 0$ ist das Diagramm

$$\begin{array}{ccc} G^* & \overset{f(X)\bullet}{\to} & G \\ f\uparrow & & \uparrow f \\ T_1(G)^* & \overset{\lambda_X}{\to} & T_1(G)^* \end{array}$$

kommutativ

wobei der Exponent $*$ bedeutet, daß nur die X, Y eingesetzt werden sollen, die den angegebenen Bedingungen genügen.

Jetzt ist es nicht so schwierig, die Jacobi-Abbildung von λ_X (als Funktion von Y) zu berechnen:

$$\lambda_X(Y) - \lambda_X(Y_0) = (1+X)^{-1}\{(X+Y)(1+XY)^{-1} - (X+Y_0)(1+XY_0)^{-1}\}(1+X)$$

Die geschweifte Klammer ist

$$= (Y-Y_0)(1+XY)^{-1} + (X+Y_0)[(1+XY)^{-1} - (1+XY_0)^{-1}]$$

Die eckige Klammer ist

$$= (1+XY)^{-1}[X(Y_0-Y)](1+XY_0)^{-1}$$

Die Summe ist

$$= (Y-Y_0)(1+XY_0)^{-1} - (X+Y_0)((1+XY_0)^{-1}X(Y-Y_0)(1+XY_0)^{-1} + ...$$
$$= [1-(X+Y_0)(1+XY_0)^{-1}X](Y-Y_0)(1+XY_0)^{-1} + ...$$

wobei ..... Terme bedeutet, die mindestens quadratisch in $Y-Y_0$ sind.
Es ist $(1+XY_0)^{-1}X = X(1+Y_0X)^{-1}$. Dies eingesetzt, erhält man nach kurzer Rechnung

$$\lambda_X(Y) - \lambda_X(Y_0) = (1-X)(1+Y_0X)^{-1}(Y-Y_0)(1+XY_0)^{-1}(1+X) + ...$$

Hieraus kann man die Jacobi-Abbildung ablesen:

$$Jac_{Y_0}(\lambda_X)(T) = (1-X)(1+Y_0X)^{-1}\cdot T\cdot(1+XY_0)^{-1}(1+X) \text{ für alle } T \in T_1(G)$$

$Jac_{Y_0}(\lambda_X)$ ist eine lineare Abbildung von $T_1(G)$ auf sich. Ihre Determinante ist von der (zur Berechnung benutzten) Basis von $T_1(G)$ unabhängig. $T_1(G) = \{T \mid AT = -(AT)'\}$ besitzt als Basis die $\frac{n(n-1}{2}$ Matrizen $A^{-1}(e_{rs} - e_{sr})$, $r > s$, und für diese ist

$$Jac_{Y_0}(\lambda_X)(A^{-1}(e_{rs} - e_{sr}) = (1 - X)(1 + Y_0X)^{-1}A^{-1}(e_{rs} - e_{sr})(1 + XY_0)^{-1}(1 + X)$$

$$= A^{-1}(1 + X')(1 + Y_0'X')^{-1}(e_{rs} - e_{sr})(1 + XY_0)^{-1}(1 + X) = A^{-1}C'(e_{rs} - e_{sr})C$$

mit $C = (1 + XY_0)^{-1}(1 + X)$. Das zeigt: Die Determinante von $Jac_{Y_0}(\lambda_X)$ ist dieselbe wie die Determinante der Abbildung $S \mapsto C'SC$ im Raum der schiefsymmetrischen Matrizen. Diese Determinante ist eine multiplikative Funktion von C und deshalb $= 1$, wenn C eine elementare Matrix $1 + \lambda e_{ik}$ ist (weil jede elementare Matrix ein Kommutator von zwei Matrizen ist). Also brauchen wir die Determinante nur auszurechnen, wenn $C = \begin{pmatrix} \lambda_1 & & \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ eine Diagonalmatrix ist. In diesem Falle ist sie $= \prod_{i>j} \lambda_i\lambda_j = \prod_{i=1}^n \lambda_i^{n-1} = \det C^{n-1}$. Das ergibt

$$\det\, Jac_{Y_0}(\lambda_X) = [\frac{\det(1 + X)}{\det(1 + XY_0)}]^{n-1}$$

Die $Y \in T_1(G)$ drücken wir durch die eben benutzte Basis aus: $Y = \sum_{r>s} y_{rs}A^{-1}(e_{rs} - e_{sr})$ und setzen $dY = \wedge_{r>s} dy_{rs}$. Das ist eine Differentialform höchsten Grades auf $T_1(G)$. Für $Z = \lambda_X(Y)$ ist

$$dZ = \det\, Jac_Y(\lambda_X)\, dY$$

Satz 14.

$$\frac{dZ}{\det(1 + Z)^{n-1}} = \frac{dY}{\det(1 + Y)^{n-1}}$$

Beweis: Wir setzen den gefundenen Ausdruck für die Jacobi-Determinante ein:

$$\frac{dZ}{\det(1 + Z)^{n-1}} = \frac{\det(1 + X)^{n-1}}{\det(1 + XY)^{n-1} \cdot \det(1 + \lambda_X(Y))^{n-1}}\, dY$$

Setzt man den Ausdruck (1) für $\lambda_X(Y)$ ein, so erhält man nach kurzer Rechnung die Behauptung.

Satz 14 kann man auch so ausdrücken: Die Differentialform

$$\frac{dY}{\det(1 + Y)^{n-1}}$$

ist invariant gegen λ_X. (Das gilt für alle X, Y, für die $\det(1 + X)\det(1 + Y)\det(1 + XY) \neq 0$)

Mit Hilfe der Cayley-Transformation wird daraus eine in einer Zariski-offenen Einsumgebung in G definierte Differentialform ω höchsten, das heißt $\frac{n(n-1)}{2}$-ten Grades: Sei

$$U = \{P \in G \mid \det(1 + P) \neq 0\}$$

Offenbar ist $U = U^{-1}$. Für $P \in U$ setzen wir

$$\omega(P) = \frac{dX}{\det(1+X)^{n-1}}, \text{ wenn } P = f(X) = (1+X)^{-1}(1-X)$$

Ist $P_0 \in G$ beliebig, so ist P_0U eine offene Umgebung von P_0. Die $P \in P_0U$ sind durch die Parameterdarstellung $P = P_0 f(X)$ mit $X \in T_1(G)$ und $\det(1+X) \neq 0$ gegeben. Wir setzen

$$\omega_{P_0}(P) = \frac{dX}{\det(1+X)^{n-1}} \tag{2}$$

Satz 15. *Wenn $P \in P_0U \cap P_1U$, dann ist*

$$\omega_{P_0}(P) = \omega_{P_1}(P)$$

Beweis: Wenn $P = P_0 f(Y) = P_1 f(Z)$, dann ist $f(Z) = P_1^{-1}P_0 f(Y) =: Q \cdot f(Y)$. Wenn $Q = f(X)$, dann ist $f(Z) = f(X) \cdot f(Y)$, also $Z = \lambda_X(Y)$ und nach Satz 14

$$\frac{dZ}{\det(1+Z)^{n-1}} = \frac{dY}{\det(1+Y)^{n-1}}, \text{ also } \omega_{P_0}(P) = \omega_{P_1}(P)$$

Ist hingegen $P_1^{-1}P_0 \notin U$, so nehmen wir einen Punkt $R \in U \cap PU \cap P_0U \cap P_1U$ (dieser Durchschnitt ist nicht leer, weil U Zariski-offen und G (als algebraische Menge) irreduzibel ist). Dann haben wir (unter Benutzung von $U = U^{-1}$)

$$P \in P_0U \cap RU \text{ und } R^{-1}P \in U \text{ also } \omega_{P_0}(P) = \omega_R(P) \text{ nach Schritt 1}$$

und dasselbe mit P_1 statt P_0, also zusammen $\omega_{P_0}(P) = \omega_R(P) = \omega_{P_1}(P)$.

Folgerung: Durch (2) wird eine Differentialform ω auf G wohldefiniert. Nach Konstruktion ist sie linksinvariant.

Diese Differentialform liefert ein Integral auf $G_{\mathbb{R}}$, das zugehörige (nicht orientierte) Volumenelement bezeichnen wir mit ω_∞ und das Lebesguemaß im $\mathbb{R}^{\frac{n(n-1)}{2}}$ mit dX_∞. Nach der Integraltransformationsformel aus Analysis III ist ω_∞ nur von ω, aber nicht von der Parameterwahl abhängig. Insbesondere ist ω_∞ auch linksinvariant. Für alle Funktionen g mit Träger in U ist

$$\int_G g(P)\omega_\infty(P) = \int_{T_1(G)} g(f(X)) \frac{dX_\infty}{|\det(1+X)^{n-1}|_\infty}$$

$|\ |_\infty$ ist der Absolutbetrag.

9. Das Maß im Reellen

In diesem Kapitel berechnen wir mit Benutzung des im vorigen Kapitel erklärten Maßes das Volumen der speziellen orthogonalen Gruppe im Falle $A = 1$. Wir haben also auszuwerten

$$\int_{Y'=-Y} \frac{dY}{\det(1+Y)^{n-1}}\,, \quad \text{wobei } dY = dy_{21}.....dy_{n,n-1}$$

Beachte, daß $\det(1+Y)$ stets >0. Das sieht man an den folgenden Formeln, aber es folgt natürlich auch daraus, daß $\det(1+Y)$ stets $\neq 0$ und der Raum der schiefsymmetrischen Matrizen zusammenhängend ist. Für $n>2$ entwickeln wir die Determinante nach der ersten Zeile und Spalte: Wir kürzen $\det X$ ab durch $|X|$.

$$\begin{vmatrix} 1 & -y_2 & \dots & -y_n \\ y_2 & & & \\ \vdots & & 1+Z & \\ y_n & & & \end{vmatrix} = |1+Z| + \sum_{i,j=2}^{n} y_i(1\tilde{+}Z)_{ij}y_j$$

$$= |1+Z|\{1+y'(1+Z)^{-1}y\}$$

Dabei ist $(1\tilde{+}Z)$ die Adjunkte von $1+Z$.
Setzt man $(1+Z)^{-1}y = z$, so ist ($dy_2....dy_n$ abgekürzt $= dy$)

$$dy = |1+Z|\,dz$$

und

$$y'(1+Z)^{-1}y = z'(1-Z)z = z'z$$

weil $z'Zz = 0$. Für $L_n := \int_{Y'=-Y} \frac{dY}{|1+Y|^{n-1}}$ erhalten wir die Rekursionsformel

$$L_n = L_{n-1} \cdot \int_{\mathbb{R}^{n-1}} \frac{dx}{(1+x_2^2+.....+x_n^2)^{n-1}}$$

Lemma 1. *Sei $f(x)$ eine stetige Funktion ≥ 0 auf $\mathbb{R}^n$, die nur von r abhängt ($r^2 = x_1^2+.....+x_n^2$), also $f(x) = g(r)$, und g sei monoton. Dann ist*

$$\int_{\mathbb{R}^n} f(x)\,dx = nV_n(1)\int_0^\infty g(r)r^{n-1}dr$$

wobei $V_n(r)$ das Volumen der Kugel vom Radius r im $\mathbb{R}^n$ ist.

Beweis: Für $R>0$ und $0 = r_0 < r_1 < ..... < r_N = R$ ist

$$\int_{\sum x_i^2 \leq R^2} f(x)\,dx = \sum_{i=0}^{N-1} \int_{r_i^2 \leq \sum x_j^2 \leq r_{i+1}^2} f(x)\,dx$$

Nach dem Zwischenwertsatz, angewandt auf g, ist dies mit $\xi_i \in [r_i, r_{i+1}]$

$$= \sum_{i=0}^{N-1} g(\xi_i)(V(r_{i+1}) - V(r_i)) = \sum_{i=0}^{N-1} g(\xi_i)(r_{i+1}^n - r_i^n)\,V(1) =$$

$$\sum_{i=0}^{N-1} g(\xi_i) n \eta_i^{n-1} V(1)(r_{i+1} - r_i)$$

mit $\eta_i \in [r_i, r_{i+1}]$.. Nach Definition des Riemann-Integrals strebt diese Summe mit wachsender Verfeinerung gegen $nV(1)\int_0^R g(r) r^{n-1} dr$.

Folgerung:

$$L_n = L_{n-1} \cdot (n-1) V_{n-1}(1) \int_0^\infty \frac{r^{n-2} dr}{(1+r^2)^{n-1}}$$

Mit der Substitution $r = \tan x$ wird das Integral zu

$$\int_0^{\frac{\pi}{2}} (\sin x \cos x)^{n-2} dx = \frac{1}{2^{n-1}} \int_0^\pi (\sin x)^{n-2} dx$$

Für das Integral

$$I_k := \int_0^\pi \sin^k x dx$$

findet man schrittweise durch partielle Integration

$$I_k = \begin{cases} \frac{(k-1)(k-3).....\cdot 2}{k(k-2).....\cdot 3} \cdot 2 & \text{wenn } k \text{ ungerade} \\ \frac{(k-1)(k-3).....\cdot 3 \cdot 1}{k(k-2).....\cdot 4 \cdot 2} \cdot \pi & \text{wenn } k \text{ gerade} \end{cases}$$

Für ungerades k erweitern wir den Bruch mit seinem Zähler, für gerades k mit seinem Nenner. Dann erhalten wir

$$I_k = \begin{cases} \frac{2^k (\frac{k-1}{2}!)^2}{k!} & \text{wenn } k \text{ ungerade} \\ \frac{k!}{2^k (\frac{k}{2}!)^2} \pi & \text{wenn } k \text{ gerade} \end{cases}$$

Für die Gammafunktion $\Gamma(z) = (z-1)!$ gilt nach Legendre

$$\Gamma(z) = \frac{2^{z-1}}{\sqrt{\pi}} \Gamma(\frac{z}{2}) \Gamma(\frac{z+1}{2})$$

([FB], Seite 201). Daher wird für ungerades k

$$I_k = \frac{2^k \Gamma(\frac{k+1}{2})^2}{\Gamma(k+1)} = \frac{\Gamma(\frac{k+1}{2})}{\Gamma(\frac{k}{2}+1)} \sqrt{\pi}$$

Für gerades k hat man den Zähler $k! = \Gamma(k+1)$ nach Legendre zu ersetzen und erhält ebenfalls $\frac{\Gamma(\frac{k+1}{2})}{\Gamma(\frac{k}{2}+1} \sqrt{\pi}$.

Jetzt müssen wir das alles zusammensetzen:

$$\frac{L_n}{L_{n-1}} = \int_{\mathbb{R}^{n-1}} \frac{dz}{(1 + z_2^2 + ... + z_n^2)^{n-1}}$$

$$= (n-1) \frac{\pi^{\frac{n-1}{2}}}{\frac{n-1}{2}!} \int_0^\infty \frac{r^{n-2}}{(1+r^2)^{n-1}} dr$$

$$= (n-1)\frac{\pi^{\frac{n-1}{2}}}{\Gamma(\frac{n+1}{2})} \cdot \frac{1}{2^{n-1}} I_{n-2}$$

$$= \frac{1}{2^{n-2}} \cdot \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})}$$

(unter Ausnutzung von $\Gamma(x+1) = x\Gamma(x)$).
Multipliziert man das alles zusammen und beachtet $L_2 = \pi$, so erhält man

$$\int_{G_{\mathbb{R}}} \omega_\infty = L_n = (\frac{1}{2})^{\frac{(n-1)(n-2)}{2}} \frac{\pi^{\frac{n(n+1)}{4}}}{\prod_{j=1}^{n} \Gamma(\frac{j}{2})}$$

wenn $A = 1$.

Ist A positiv definit, so gibt es T mit $A = T'T$. Der Tangentialraum $T_1(G)$ bestand aus allen Y , für die AY schief ist. Setzt man $Z = TYT^{-1}$, so ist Z schief. Man hat

$$Z = \sum_{r>s} z_{rs}(e_{rs} - e_{sr}) = TYT^{-1} = T\sum_{r>s} y_{rs}A^{-1}(e_{rs} - e_{sr})T^{-1} =$$

$$\sum_{r>s} y_{rs}T'^{-1}(e_{rs} - e_{sr})T^{-1}$$

Die Abbildung $X \mapsto T'^{-1}XT^{-1}$ ist eine lineare Transformation Q des Raumes aller schiefsymmetrischen Matrizen auf sich. Ihre Determinante ist eine multiplikative Funktion von T , welche man findet, indem man für T eine Diagonalmatrix einsetzt: $\det Q = (\det T)^{-(n-1)}$. Nach Definition von dY und dZ folgt nun

$$dZ = (\det T)^{-(n-1)} dY = (\det A)^{-\frac{n-1}{2}} dY$$

Jetzt erhalten wir

$$\int_{Y \in T_1(G)_{\mathbb{R}}} \frac{dY_\infty}{|1+Y|_\infty^{n-1}} = |A|^{\frac{n-1}{2}} \int_{Z=-Z'} \frac{dZ_\infty}{|1+Z|_\infty^{n-1}} = |A|^{\frac{n-1}{2}} L_n$$

mit dem oben angegebenen Wert von L_n .

10. Abzählungen mod p

Um später die p-adischen Integrale auszurechnen, zählen wir Vektoren mod p auf Sphären und orthogonale Transformationen mod p. In diesem Kapitel sei $p \neq 2$ und zuerst

$\rho \neq 0$

Ein zweidimensionaler Vektorraum E über $\mathbb{F}_p$ ist entweder eine hyperbolische Ebene oder (als Vektorraum) isomorph zur quadratischen Erweiterung $\mathbb{F}_p(\sqrt{d})$ über $\mathbb{F}_p$ mit der Normform $x^2 - dy^2$. Dabei ist d ein Nichtquadrat in $\mathbb{F}_p$. Für die Anzahl $A(E,\rho)$ der Vektoren $x \in E$ mit $(x,x) = \rho$ findet man

$$A(E,\rho) = \begin{cases} p-1 & \text{wenn } E \text{ hyperbolisch} \\ p+1 & \text{wenn } E \text{ anisotrop} \end{cases} \tag{1}$$

denn die hyperbolische Form kann auf $(x,x) = x_1x_2$ transformiert werden, und die Norm ist ein Homomorphismus von $\mathbb{F}_{p^2}^*$ auf $\mathbb{F}_p^*$, ihr Kern hat also $p+1$ Elemente. Für die Darstellung der 0 findet man

$$A(E,0) = \begin{cases} 2p-1 & \text{wenn } E \text{ hyperbolisch} \\ 1 & \text{wenn } E \text{ anisotrop} \end{cases}$$

Jeder mindestens dreidimensionale Raum über $\mathbb{F}_p$ stellt 0 dar, von ihm kann man also eine hyperbolische Ebene abspalten. Ist nun $V = U \perp H$ und H hyperbolisch, so ist

$$A(V,\rho) = \sum_{\mu} A(U,\mu)A(H,\rho-\mu)$$

$$= (2p-1)A(U,\rho) + \sum_{\mu\neq\rho}(p-1)A(U,\mu) = p\cdot A(U,\rho) + (p-1)p^{n-2}$$

Um eine Rekursion zu haben, schreiben wir vorübergehend $A(n,\rho)$ statt $A(V,\rho)$. Dann haben wir

$$A(n,\rho) = p\cdot A(n-2,\rho) + (p-1)p^{n-2}$$

Dasselbe gilt für $n-2i$ anstelle von n, solange $n-2i \geq 3$:

$$A(n-2i,\rho) = p\cdot A(n-2i-2,\rho) + (p-1)p^{n-2i-2}$$

Diese Gleichung multiplizieren wir mit p^i und summieren über $i = 0, ..., k$:

$$A(n,\rho) = p^{k+1}A(n-2k-2,\rho) + p^{n-1} - p^{n-k-2} \tag{2}$$

Dies funktioniert, solange $n-2k-2 \geq 1$, also $2k \leq n-3$.

1. Fall: n gerade: Man schreibt

$$V = H \perp ..... \perp H \perp E \quad (H \text{ hyperbolisch, dim } E = 2)$$

Man nimmt $k = \frac{n}{2} - 2$ und erhält

$$A(n,\rho) = p^{\frac{n}{2}-1}A(2,\rho) + p^{n-1} - p^{\frac{n}{2}} \tag{3}$$

Mit $A(2,\rho)$ ist natürlich $A(E,\rho)$ gemeint, nach (1) also $p-1$ oder $p+1$, je nachdem ob E hyperbolisch oder anisotrop ist. Nun ist

$$E \text{ hyperbolisch } \Leftrightarrow -\det E \text{ Quadrat } \Leftrightarrow (-1)^{\frac{n}{2}} \det V \text{ Quadrat}$$

Wir können einheitlich schreiben

$$A(E,\rho) = p - \epsilon \text{ mit } \epsilon = (\frac{(-1)^{\frac{n}{2}} \det V}{p})$$

Setzt man dies in (3) ein, so erhält man

$$A(V,\rho) = p^{n-1} - \epsilon p^{\frac{n}{2}-1} \tag{4}$$

2. Fall: n ungerade. Jetzt schreibt man

$$V = H \perp ..... \perp H \perp \mathbb{F}_p e$$

und nimmt $k = \frac{n-3}{2}$. Dann erhält man

$$A(V,\rho) = p^{\frac{n-1}{2}} A(\mathbb{F}_p e,\rho) + p^{n-1} - p^{\frac{n-1}{2}}$$

Offensichtlich ist

$$A(\mathbb{F}_p e,\rho) = \begin{cases} 2 & \text{wenn } \rho(e,e) \text{ Quadrat} \\ 0 & \text{sonst} \end{cases}$$

Bis auf ein Quadrat ist (e,e) gleich $(-1)^{\frac{n-1}{2}} \det V$. Setzen wir

$$\epsilon' = (\frac{(-1)^{\frac{n-1}{2}} \rho \det V}{p})$$

so erhalten wir

$$A(V,\rho) = p^{n-1} + \epsilon' p^{\frac{n-1}{2}} \tag{5}$$

Jetzt wollen wir auch noch die isotropen Vektoren zählen (also die $x \neq 0$ mit $(x,x) = 0$). Die Formel (2) gilt kraft ihrer Herleitung auch für $\rho = 0$. Bei geradem n benutzen wir sie für $k = \frac{n}{2} - 2$. Die Anzahl *aller* $x \in V$ mit $(x,x) = 0$ ist

$$A(V,0) = p^{\frac{n}{2}-1} A(E,0) + p^{n-1} - p^{\frac{n}{2}}$$

und

$$A(E,0) = \begin{cases} 1 & \text{wenn } E \text{ anisotrop , das heiß } \epsilon = -1 \\ 2p-1 & \text{wenn } E \text{ hyperbolisch, das heißt } \epsilon = 1 \end{cases}$$

Das ergibt

$$A(V,0) = \begin{cases} p^{\frac{n}{2}-1} + p^{n-1} - p^{\frac{n}{2}} & \text{wenn } E \text{ anisotrop} \\ p^{\frac{n}{2}} - p^{\frac{n}{2}-1} + p^{n-1} & \text{wenn } E \text{ hyperbolisch} \end{cases}$$

Die Zahl $A^*(V,0)$ der isotropen Vektoren ist 1 weniger. Unter Benutzung von ϵ kann man sie einheitlich schreiben:

$$A^*(V,0) = (p^{\frac{n}{2}} - \epsilon)(p^{\frac{n}{2}-1} + \epsilon)$$

Für ungerades n folgt aus $A(1,0) = 1$, daß $A(n,0) = p^{n-1}$. also

$$A^*(V,0) = p^{n-1} - 1$$

Mit Hilfe dieser Formeln können wir zählen, wie viele orthogonale Transformationen V gestattet. Dazu nehmen wir eine Orthogonalbasis $e_1, ..., e_n$ von V über $\mathbb{F}_p$, mit $(e_i, e_i) =: \alpha_i$. Für jede orthogonale Transformation T ist $(Te_1, Te_1) = \alpha_1$. Umgekehrt: Wenn $(x,x) = \alpha_1$, dann gibt es eine orthogonale Transformation T mit $x = Te_1$, und solange $\dim V \geq 2$, kann $\det T = 1$ genommen werden. Daraus folgt: Wenn $G(V)$ die spezielle orthogonale Gruppe ist, dann gilt

$$|G(V)| = A(V, \alpha_1) \cdot |G(\mathbb{F}_p e_2 \perp ..... \perp \mathbb{F}_p e_n)|$$

Setzt man $V_i = \mathbb{F}_p e_{i+1} \perp ..... \perp \mathbb{F}_p e_n$, so folgt rekursiv

$$|G(V)| = A(V_0, \alpha_1)A(V_1, \alpha_2).....A(V_{n-2}, \alpha_{n-1})|G(\mathbb{F}_p e_n)|$$

und der letzte Faktor ist 1. Aus den Formeln 4 und 5 erhalten wir

$$A(V_{n-2}, \alpha_{n-1}) = p - (\frac{-\alpha_{n-1}\alpha_n}{p})$$

$$A(V_{n-3}, \alpha_{n-2}) = p^2 + (\frac{-\alpha_{n-1}\alpha_n}{p})p$$

$$A(V_{n-4}, \alpha_{n-3}) = p^3 - (\frac{\alpha_{n-3}\alpha_{n-2}\alpha_{n-1}\alpha_n}{p})p$$

$$A(V_{n-5}, \alpha_{n-4}) = p^4 + (\frac{\alpha_{n-3}\alpha_{n-2}\alpha_{n-1}\alpha_n}{p})p^2$$

Wenn n ungerade ≥ 3 ist, hat man am Ende

$$A(V_1, \alpha_2) = p^{n-2} - (\frac{(-1)^{\frac{n-1}{2}}\alpha_2.....\alpha_n}{p})p^{\frac{n-1}{2}-1}$$

$$A(V_0, \alpha_1) = p^{n-1} + (\frac{(-1)^{\frac{n-1}{2}}\alpha_2.....\alpha_n}{p})p^{\frac{n-1}{2}}$$

Hier kann man die Faktoren paarweise zusammenfassen und erhält

$$|G(V)| = p^{1+2+....+(n-1)}(1-p^{-2})(1-p^{-4}).....(1-p^{-(n-1)}) \tag{6}$$

Wenn n gerade ist, dann bleibt V_0 übrig, und man erhält

$$|G(V)| = p^{1+2+....+(n-1)}(1-p^{-2})(1-p^{-4}).....(1-p^{-(n-2)})(1-(\frac{(-1)^{\frac{n}{2}}\det V}{p})p^{-\frac{n}{2}}) \tag{7}$$

11. Berechnung der p-adischen Integrale für fast alle p

Der Tangentialraum $T_1(G)$ (vgl. Kapitel 8) bestand aus allen Matrizen Y, für die AY schiefsymmetrisch ist. Dabei war A die für die ganze Vorlesung gegebene symmetrische invertierbare Matrix mit Koeffizienten in $\mathbb{Z}$. Wir benutzen weiter die Basis $\{A^{-1}(e_{rs} - e_{sr})\}_{r>s}$ von $T_1(G)$. Seien y_{rs} die Koordinaten bezüglich dieser Basis:
$Y = \sum_{r>s} y_{rs} A^{-1}(e_{rs} - e_{sr})$. Dann sei $dY_p = dy_{21,p}....dy_{n,n-1,p}$ das in Kapitel 3 beschriebene Volumenelement über $\mathbb{Q}_p$. Nach den Formeln des Kapitels 8 (die über $\mathbb{Q}$ definiert waren und in allen $\mathbb{Q}_p$ ihren Sinn behalten) ist

$$\frac{dY_p}{|\det(1+Y)|_p^{n-1}}$$

vermöge der Cayley-Transformation auf $G_{\mathbb{Q}_p}$ aufgefaßt invariant gegen Translationen in der Gruppe, also ein Haarsches Maß. Dieses bezeichnen wir kurz mit ω_p.

Es war

$$G_{\mathbb{Q}_p} = \{X \in M_n(\mathbb{Q}_p) \mid X'AX = A \text{ und } \det X = 1\}$$

Die X mit Einträgen in $\mathfrak{o}_p$ bilden (wegen $\det X = 1$) eine Untergruppe $G_{\mathfrak{o}_p}$, und $G_{\mathfrak{o}_p}$ ist kompakt, hat also für das Haarsche Maß endliches Volumen. Dieses wollen wir berechnen, zunächst unter der Voraussetzung, daß $p \nmid 2 \det A$:

1. Schritt: Wir teilen $G_{\mathfrak{o}_p}$ in Kongruenzklassen mod p: $P_1 \equiv P_2 \bmod p$, wenn P_1 und P_2 koeffizientenweise kongruent sind mod p, also $P_1 = P_2 + pQ$ mit ganzem Q. Da P_2^{-1} ganz ist, gilt $P_1 = P_2(1 + pP_2^{-1}Q)$, und die Klammer ist $\equiv 1 \bmod p$. Ist also

$$U = \{X \in G_{\mathfrak{o}_p} \mid X \equiv 1 \bmod p\}$$

so ist

$$P_1 \equiv P_2 \bmod p \Leftrightarrow P_1 \in P_2 \cdot U$$

Es gibt nur endlich viele Kongruenzklassen (sicher weniger als p^{n^2}), etwa k. Wegen der Invarianz von ω_p haben sie alle das gleiche Volumen. Daher ist

$$\int_{G_{\mathfrak{o}_p}} \omega_p = k \cdot \int_U \omega_p$$

2. Schritt: Ist $X \leftrightarrow Y$ bei der Cayley-Transformation, so gilt

$$X \in U \Leftrightarrow Y \equiv 0 \bmod p$$

Beweis: Ist $Y \equiv 0 \bmod p$, so ist offensichtlich

$$X = (1+Y)^{-1}(1-Y) \equiv 1 \bmod p, \text{ also } X \in U$$

Ist umgekehrt $X = 1 + pT$ mit ganzem T, so ist $Y = (1-X)(1+X)^{-1} = -pT(2 + pT)^{-1} \equiv 0 \bmod p$, weil $p \neq 2$.

Nach Definition von ω_p ist nun

$$\int_U \omega_p = \int_{Y \equiv 0 \bmod p} \frac{dY_p}{|\det(1+Y)|_p^{n-1}} = \int_{Y \equiv 0 \bmod p} dY_p = p^{-\frac{n(n-1)}{2}}$$

Nach Schritt 1 und 2 bleibt nun k auszurechnen. Dazu lesen wir alles modulo p und erhalten statt V einen Vektorraum $\bar{V}$ über $\mathbb{F}_p$. Wegen $p \nmid \det A$ trägt $\bar{V}$ ein nicht ausgeartetes Skalarprodukt, und $p \neq 2$. Jede Kongruenzklasse mod p liefert durch Redukion mod p eine spezielle orthogonale Transformation von $\bar{V}$. Aber auch umgekehrt: Jede spezielle orthogonale Transformation ϕ von $\bar{V}$ ist Reduktion mod p eines $P \in G_{\mathfrak{o}_p}$.
Beweis: Zu ϕ nehme man irgendein Urbild $P_0 \in M_n(\mathfrak{o}_p)$. Das muß natürlich nicht schon in $G_{\mathfrak{o}_p}$ liegen, aber weil ϕ orthogonal ist, ist

$$P_0' A P_0 \equiv A \bmod p$$

Jetzt kommt Hensel: Angenommen, man hat schon $P_0, P_1, ..., P_m$ mit

$$P_k \equiv P_{k-1} \bmod p^k \text{ für } k = 1, ..., m$$

$$P_k' A P_k \equiv A \bmod p^{k+1} \text{ für } k = 0, ..., m \tag{1}$$

Dann setzt man $P_{m+1} = P_m + p^{m+1}T$, wobei man T so bestimmt, daß (1) auch für $k = m+1$ gilt. Nämlich: Aus

$$P_m' A P_m = A + p^{m+1} X \text{ mit ganzem } X$$

folgt

$$P_{m+1}' A P_{m+1} = A + p^{m+1}X + p^{m+1}(P_m' A T + T' A P_m) + p^{2m+2} T' A T$$

$$\equiv A + p^{m+1}(X + P_m' A T + T' A P_m) \bmod p^{m+2} \text{ weil } 2m+2 \geq m+2$$

Da $p \neq 2$ und P_m^{-1} und nach Voraussetzung auch A^{-1} ganz für p ist, kann man $T = -\frac{1}{2} A^{-1} {P_m'}^{-1} X$ setzen und erhält

$$P_{m+1}' A P_{m+1} \equiv A \bmod p^{m+2}$$

Nach Konstruktion der Folge existiert $P := \lim P_m$. Er erfüllt $P' A P = A$. Aus $\det P_0 \equiv 1 \bmod p$ folgt $\det P \equiv 1 \bmod p$, und aus $P' A P = A$ folgt $(\det P)^2 = 1$. Da $p \neq 2$, folgt $\det P = 1$.

Die gesuchte Zahl k ist also gleich der Zahl der speziellen orthogonalen Transformationen des durch Reduktion modulo p entstandenen Vektorraumes $\bar{V}$ über $\mathbb{F}_p$. Diese haben wir in Kapitel 10 bestimmt. Danach erhalten wir

Für $p \nmid 2 \det A$ ist

$$\int_{G_{\mathfrak{o}_p}} \omega_p =$$

$$\begin{cases} (1-p^{-2})(1-p^{-4}).....(1-p^{-(n-1)}) & \text{wenn } n \text{ ungerade} \\ (1-p^{-2})(1-p^{-4}).....(1-p^{-(n-2)})(1-(\frac{(-1)^{\frac{n}{2}} \det A}{p})p^{-\frac{n}{2}}) & \text{wenn } n \text{ gerade} \end{cases} \tag{2}$$

Dieses Ergebnis setzt uns in den Stand, das Tamagawa-Maß auf G_A zu definieren: Sei $Y \mapsto X = X(Y)$ die Cayley-Transformation $T_1(G) \to G$. Für alle v ($= \infty$ oder eine Primzahl) ist durch

$$\int_{G_{\mathbb{Q}_v}} f(X)\omega_v = \int_{T_1(G)_v} f(X(Y)) \frac{dY_v}{|\det(1+Y)|_v^{n-1}}$$

(falls der Träger von f in $\{\det(1+Y) \neq 0\}$ enthalten ist) ein invariantes Integral auf $G_{\mathbb{Q}_v}$ definiert. Für die Primzahlen p ist $G_{\mathfrak{o}_p}$ eine kompakte Untergruppe, und man setzt

$$\lambda_p = \int_{G_{\mathfrak{o}_p}} \omega_p$$

Aus den Formeln (2) folgt, daß das $\prod_p \lambda_p$ absolut konvergiert, wenn $n \geq 3$ (auf die endlich vielen $p \,|\, 2 \det A$ kommt es für die Konvergenz ja nicht an). Dies ist der entscheidende Punkt: Es gibt Gruppen, für die das entsprechende Produkt nicht konvergiert.

Die Adelgruppe von G ist

$$G_A = \cup_S \, (G_S \times G^S)$$

wobei S durch alle endlichen Mengen von Bewertungen läuft und

$$G_S = \prod_{v \in S} G_{\mathbb{Q}_v} \quad \text{und } G^S = \prod_{p \notin S} G_{\mathfrak{o}_p}$$

Wir nehmen auf dem endlichen Produkt G_S das Produktmaß $\omega_S = \prod_{v \in S} \omega_v$ und auf der kompakten Gruppe G^S dasjenige Haarsche Maß ω^S, für welches G^S das Volumen $\prod_{p \notin S} \lambda_p$ bekommt. Dann nehmen wir auf $G_S \times G^S$ das Produktmaß $\omega_S \omega^S$.

Wenn $S \subset T$, dann ist $G_S \times G^S \subset G_T \times G^T$. Die Einschränkung von $\omega_T \omega^T$ auf $G_S \times G^S$ ist ein Haarsches Maß auf $G_S \times G^S$ ebenso wie $\omega_S \times \omega^S$. Die beiden sind also proportional. Für jede Funktion der Gestalt $f(x) = \prod_{v \in S} f_v(x_v) \cdot \prod_{p \notin S} \mathbf{1}_{G_{\mathfrak{o}_p}}$ liefern sie denselben Wert ($\mathbf{1} =$ Indikatorfunktion). Daher sind sie gleich.

Ist nun f eine stetige Funktion mit kompaktem Träger auf G_A, so ist dieser Träger in einem passenden $G_S \times G^S$ enthalten. Wie gerade gesehen, ist das $\int_{G_S \times G^S} f \, \omega_S \omega^S$ von S unabhängig, und dieser Wert wird als das Tamagawa-Maß $\int_{G_A} f \, \omega_A$ auf G_A definiert. Es ist wie die ω_v linksinvariant. Aus seiner Konstruktion und aus Satz 9, Kapitel 7 folgt, daß auch G_A unimodular ist

12. Betrachtung der p-adischen Integrale ohne die Voraussetzung $p \dagger 2 \det A$

Um eine quantitative Beziehung zwischen dem Siegel'schen Satz und seiner Weil'schen Umformulierung herzustellen, müssen wir die Integrale $\int_{G_{\mathfrak{o}_p}} \omega_p$ für alle p berechnen. Das soll in diesem Kapitel geschehen.

Wir teilen $G_{\mathfrak{o}_p}$ in Restklassen mod p^k:

$$\int_{G_{\mathfrak{o}_p}} \omega_p = \sum_{C \bmod p^k} \int_{X \equiv C \bmod p^k} \omega_p = \sum_{C} \int_{X \equiv 1 \bmod p^k} \omega_p$$

wegen der Invarianz von ω_p. Ist N^+ die Anzahl der Restklassen $C \bmod p^k$ mit $C \in G_{\mathfrak{o}_p}$, so gilt also

$$\int_{G_{\mathfrak{o}_p}} \omega_p = N^+ \cdot \int_{X \equiv 1 \bmod p^k} \omega_p$$

Siegel verwendet anstelle von G die volle orthogonale Gruppe. Dazu:

Lemma 1. *Jedes Gitter M_p gestattet eine Spiegelung.*

Beweis: Man nimmt $s \in M_p$, für welches $|(s,s)|_p$ maximal ist. Dann ist

$$|2(x,s)|_p = |(x+s, x+s) - (x,x) - (s,s)|_p \leq |(s,s)|_p$$

und die Spiegelung $x \mapsto x - 2\frac{(x,s)}{(s,s)} s$ bildet M_p in sich ab.

Folgerung: Ist N die Anzahl aller $C \bmod p^k$ mit $C'AC = A$, so ist $N^+ = \frac{1}{2}N$.

Wir berechnen das $\int_{G_{\mathfrak{o}_p}} \omega_p$, indem wir zuerst N und dann das Integral über die Untergruppe $X \equiv 1 \bmod p^k$ in $G_{\mathfrak{o}_p}$ berechnen.

1. Umformung von N: Sei $\delta = v_p(2 \det A)$. Wenn $X'AX = A$, dann ist offenbar erst recht $X'AX \equiv A \bmod p^{k+\delta}$. Umgekehrt:

Lemma 2. *Sei $C'AC \equiv A \bmod p^{k+\delta}$ und $k > \delta$. Dann gibt es $X \equiv C \bmod p^k$ mit $X'AX = A$.*

Beweis mit Hensel: Man setzt $X_0 = C$ und nimmt an, man habe $X_0, \ldots .. X_m$ mit

$$X_i' A X_i \equiv A \bmod p^{k+\delta+i} \text{ für } 0 \leq i \leq m \text{ und } X_i \equiv X_{i-1} \bmod p^{k+i-1} \text{ für } 0 < i \leq m$$

Für $m = 0$ stimmt das. Ansatz:

$$X_{m+1} = X_m + p^{k+m} T \text{ mit ganzem } T$$

Nach Induktionsannahme und wegen $2(k+m) > k+m+\delta$ ist mit ganzem B

$$X_{m+1}' A X_{m+1} = X_m' A X_m + p^{k+m}(T'AX_m + X_m'AT) + p^{2(k+m)} T'AT$$

$$\equiv A + p^{k+m}(p^\delta B + T'AX_m + X_m'AT) \bmod p^{k+\delta+m+1}$$

Wegen $X'_m A X_m \equiv A \bmod p^{k+\delta+m}$ ist $\det X_m$ eine Einheit, also X_m ganz invertierbar, und die Adjunkte von A ist ebenfalls ganz. Nach Definition von δ ist nun

$$T := -\frac{p^\delta}{2 \det A} \tilde{A} {X'_m}^{-1} B$$

ganz, und für dieses T ist

$$p^\delta B + T' A X_m + X'_m A T \equiv 0 \bmod p^{\delta+1}$$

und das bdeutet

$$X'_{m+1} A X_{m+1} \equiv A \bmod p^{k+\delta+m+1}$$

Die Folge X_m konvergiert gegen eine Matrix $X \equiv C \bmod p^k$ mit $X' A X = A$.

Das Lemma 2 bedeutet, daß jede Restklasse $\bmod p^k$ von Matrizen X mit $X' A X \equiv A \bmod p^{k+\delta}$ durch eine Matrix C mit $C' A C = A$ vertreten werden kann. Die Anzahl N der modulo p^k verschiedenen ganzen C mit $C' A C = A$ ist daher dieselbe wie die Anzahl der modulo p^k verschiedenen ganzen C mit $C' A C \equiv A \bmod p^{k+\delta}$. Es sei $C_1, ..., C_N$ ein Vertretersystem für diese Klassen.

Für jedes C_r bestimmen wir die Anzahl

$$N_r = |\{X \bmod p^{k+\delta} \mid X \equiv C_r \bmod p^k \text{ und } X' A X \equiv A \bmod p^{k+\delta}\}|$$

$$= |\{T \bmod p^\delta \mid (C_r + p^k T)' A (C_r + p^k T) \equiv A \bmod p^{k+\delta}\}|$$

$$= |\{T \bmod p^\delta \mid T' A C_r + C'_r A T \equiv 0 \bmod p^\delta\}|$$

weil $C'_r A C_r = A$ und $2k > k + \delta$.

Nach dem Elementarteilersatz gibt es unimodulare U, V so, daß $A = UDV$ mit einer Diagonalmatrix $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$ und $d_1 | .... | d_n$. Hier ist zudem $UDV = A = A' = V' D U'$, und man erhält

$$N_r = |\{T \bmod p^\delta \mid T' V' D U' C_r + C'_r U D V T \equiv 0 \bmod p^\delta\}|$$

Mit T durchläuft auch $Z := V T C_r^{-1} U'^{-1}$ die ganzen Matrizen $\bmod p^k$. und

$$N_r = |\{Z \bmod p^\delta \mid Z' D + D Z \equiv 0 \bmod p^\delta\}|$$

Die Bedingungen lauten ausgeschrieben

$$z_{ji} d_j + d_i z_{ij} \equiv 0 \bmod p^\delta$$

Für $i < j$ ist $d_i \mid d_j$, und die Bedingungen sind

$$2 d_i z_{ii} \equiv 0 \bmod p^\delta \text{ für } i = 1, ..., n$$

und, wenn man $v_p(d_i) = \delta_i$ setzt,

$$z_{ij} + \frac{d_j}{d_i} z_{ji} \equiv 0 \bmod p^{\delta - \delta_i} \text{ für } i < j$$

Die Anzahl der $z_{ii} \bmod p^\delta$ ist $p^{\delta_i + v_p(2)} =: p^{\delta_i + \nu}$. Für $i < j$ kann man $z_{ji} \bmod p^\delta$ beliebig wählen. Danach muß $z_{ij} \equiv -\frac{d_j}{d_i} z_{ji} \bmod p^{\delta - \delta_i}$ sein. Dafür gibt es p^{δ_i} Möglichkeiten. Die Anzahl der $Z \bmod p^\delta$ ist nun $N_i = p^e$ mit

$$e = \sum_{i=1}^{n} (\delta_i + \nu) + \sum_{i<j} (\delta + \delta_i) = n\nu + \delta \frac{n(n-1)}{2} + \sum_{i=1}^{n} (n + 1 - i)\delta_i$$

Dieses Ergebnis hängt offenbar von C_r nicht ab. Durch Summation über die r erhalten wir die Anzahl $A_{k+\delta}$ der $\bmod p^{k+\delta}$ verschiedenen X mit $X'AX \equiv A \bmod p^{k+\delta}$ als

$$A_{k+\delta} = N \cdot p^e \text{ mit } e = n\nu + \delta \frac{n(n-1)}{2} + \sum_{i=1}^{n} (n + 1 - i)\delta_i \tag{1}$$

2. Umformung von $\int_{X \in G_{\circ_p}, X \equiv 1 \bmod p^k} \omega_p$:

Nach Definition von ω_p müssen wir die Y finden mit

$$AY + Y'A = 0 \text{ und } (1+Y)^{-1}(1-Y) \equiv 1 \bmod p^k$$

Lemma 3. *Wenn $k > \nu (= v_p(2))$, dann ist*

$$(1+Y)^{-1}(1-Y) \equiv 1 \bmod p^k \Leftrightarrow Y \equiv 0 \bmod p^{k-\nu}$$

Beweis: Ist $(1+Y)^{-1}(1-Y) = 1 + p^k T$, so ist $p^k T + 2Y + p^k YT = 0$, also $2Y \equiv 0 \bmod p^k$. Ist umgekehrt $Y \equiv 0 \bmod \frac{1}{2} p^k$ und $k > v_p(2)$, dann ist $1 + Y$ ganz invertierbar und $(1+Y)^{-1}(1-Y) - 1 = -2(1+Y)^{-1}Y \equiv 0 \bmod p^k$.

Wir setzen $k - \nu = k'$ und erhalten

$$\int_{X \in G_{\circ_p}, X \equiv 1 \bmod p^k} \omega_p = \int_{Y \in T_1(G)_p, Y \equiv 0 \bmod p^{k'}} \frac{dY_p}{|\det(1+Y)|_p^{n-1}} = \tag{2}$$

$$\int_{Y \in T_1(G)_p, Y \equiv 0 \bmod p^{k'}} dY_p$$

Um die $Y \equiv 0 \bmod p^{k'}$ zu finden, für die AY schief ist, schreiben wir wieder $A = UDV$ mit $D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_n \end{pmatrix}$ und $d_1 | .... | d_n$. Wegen $UDV = A = A' = V'DU'$ ist dann

$$AY + Y'A = 0 \Leftrightarrow UDVY + Y'V'DU' = 0 \Leftrightarrow DVYU'^{-1} + U^{-1}Y'V'D = 0$$

Wir setzen $VYU'^{-1} = Z$. Wenn Y durch $T_1(G)$ läuft, dann läuft Z durch alle Matrizen mit $DZ + Z'D = 0$, das heißt

$$2d_i z_{ii} = 0 \text{ und } d_i z_{ij} + z_{ji} d_j = 0$$

In diesem Bereich können die z_{ij} mit $i > j$ als Parameter dienen und wegen $z_{ji} = -\frac{d_i}{d_j} z_{ij}$ und $d_j | d_i$ für $i > j$ hat Z genau dann lauter ganze Einträge, wenn die z_{ij} mit $i > j$ ganz sind. Wir müssen $dY = \wedge_{r>s} dy_{rs}$ durch $dZ := \wedge_{i>j} dz_{ij}$ ausdrücken.
Nach Definition ist $Z = VYU'^{-1}$, also $D \cdot Z = DVYU'^{-1} = U^{-1}AYU'^{-1}$. Die Koeffizienten von $D \cdot Z$ gehen also aus denen von AY (das sind die y_{rs}) durch eine unimodulare Transformation hervor, und dann gehen die $d_i z_{ij}$ mit $i > j$ jedenfalls durch eine ganzzahlige Transformation aus den $y_{rs}, r > s$ hervor. Da nun aber umgekehrt auch $AY = U\, D \cdot Z\, U'$, arbeitet dasselbe Argument in der umgekehrten Richtung. Das zeigt: Der Übergang von $y_{21}, ..., y_{n,n-1}$ zu $d_2 z_{21}, ..., d_n z_{n,n-1}$ ist unimodular. Es folgt

$$dY_p = |\prod_{i>j} d_i|_p dZ_p$$

Nach der Integraltransformationsformel ist nun das Integral (2) gleich

$$|\prod_{i=1}^{n} d_i^{i-1}|_p \int_{Z \equiv 0 \bmod p^{k'}} dZ = |\prod_{i=1}^{n} d_i^{i-1}|_p \cdot p^{-k' \frac{n(n-1)}{2}}$$

Das können wir mit dem Wert für N aus (1) zusammemsetzen und erhalten

$$\int_{G_{\mathfrak{o}_p}} \omega_p = N^+ \cdot \int_{X \equiv 1 \bmod p^k} \omega_p$$

$$= \frac{1}{2} N \cdot \int_{X \equiv 1 \bmod p^k} \omega_p$$

$$= \frac{1}{2} A_{k+\delta} p^{-e} \cdot |\prod_{i=1}^{n} d_i^{i-1}|_p \cdot p^{-k' \frac{n(n-1)}{2}}$$

also

$$\int_{G_{\mathfrak{o}_p}} \omega_p = \frac{1}{2} A_{k+\delta}\; p^{-(k+\delta)\frac{n(n-1)}{2}} \cdot p^{\nu \frac{n(n-3)}{2}} \cdot |\det A|_p^n \tag{3}$$

Die Zahlen $\frac{1}{2} A_m p^{-m\frac{n(n-1)}{2}}$ sind die von Siegel definierten α_p ([S], Formel (38), Seite 552). Sie sind, wie die Formel (3) zeigt, von m unabhängig, sobald $m \geq 2\delta + 1$.

(3) stellt den Zusammenhang her zwischen den Siegel'schen Zahlen und den p-adischen Integralen.

13. Die Minkowski-Siegel'sche Formel

In diesem Kapitel sei der Vektorraum V mit seiner quadratischen Form positiv definit (das heißt $(x,x) > 0$ für alle $x \in V_\infty$). Wie vorher bezeichne G die spezielle orthogonale Gruppe von V. Ihre Adelgruppe G_A operiert auf der Menge der Gitter in V, nämlich: Ist M ein Gitter in V und $\Phi = (\Phi_v)_v \in G_A$, so ist nach Definition der Adelgruppe $\Phi_p M_p = M_p$ für fast alle p. Nach Kapitel 2, Satz 1 gibt es genau ein Gitter L mit $L_p = \Phi_p M_p$ für alle p. Dieses Gitter L wird mit ΦM bezeichnet.

Definition 1. Zwei Gitter M und N gehören zum selben engeren Geschlecht, wenn es $\Phi \in G_A$ gibt mit $N = \Phi M$.

Definition 2. Zwei Gitter gehören zur selben engeren Klasse, wenn es $\sigma \in G_{\mathbb{Q}}$ gibt mit $N = \sigma M$.

Definition 3. Zwei Gitter gehören zur selben Klasse, wenn es eine orthogonale Transformation σ gibt (also nicht notwendig $\det \sigma = 1$) mit $N = \sigma M$.

Bemerkung: Bei Siegel gehören zwei symmetrische Matrizen A und B mit ganzzahligen Einträgen und Determinante $\neq 0$ zum selben Geschlecht, wenn es zu jedem p und m eine ganzzahlige Matrix T gibt mit $T'AT \equiv B \bmod p^m$. Nach Hensel (vgl. Kapitel 11) gibt es dann zu jedem p eine Matrix $T \in GL(n, \mathfrak{o}_p)$ mit $T'AT = B$. Sind nun M und N zwei Gitter mit Basen $u_1, ..., u_n$ bzw. $v_1, ..., v_n$ über $\mathbb{Z}$ und A und B deren Gram-Matrizen $(a_{ij} = (u_i, u_j))$ und ist Φ_p eine Isometrie von M_p auf N_p, so bilden die $\Phi_p u_i$ eine Basis von N_p, gehen also aus $v_1, ..., v_n$ durch eine p-ganze und p-ganz invertierbare Matrix T auseinander hervor, und es ist

$$B = \text{ Gram } (v_1, ..., v_n) = T' \text{ Gram } (\Phi_p u_1, ..., \Phi_p u_n) T = T' Gram(u_1, ..., u_n) T = T'AT$$

Umgekehrt liefert jedes solche T ein Isometrie von M_p auf N_p.
Wir sahen in Kapitel 11, daß jedes lokale Gitter M_p eine Spiegelung gestattet. Wenn es also eine Isometrie von M_p auf N_p gibt, dann auch eine mit Determinante 1, das heißt ein Element aus $G_{\mathbb{Q}_p}$: Geschlecht und engeres Geschlecht fallen zusammen. In Definition 1 können wir "engeren" streichen. Nicht jedoch in Definition 2; zum Beispiel im Gitter $\mathbb{Z}e_1 + \mathbb{Z}e_2$ mit der Gram-Matrix $\begin{pmatrix} 3 & 1 \\ 1 & 5 \end{pmatrix}$ sind $\pm e_1$ die einzigen Vektoren x mit $(x,x) = 3$, jede Isometrie muß also e_1 in e_1 oder in $-e_1$ überführen. Die einzige Spiegelung, die e_1 in $-e_1$ überführt, ist die längs e_1, und die einzige, die e_1 fest läßt, ist die längs $e_1^\perp$. Keine von beiden führt das Gitter in sich über.

Für ein Gitter M bezeichne $G_A(M)$ die Untergruppe aller $\Phi \in G_A$ mit $\phi M = M$.
Behauptung: Die engeren Klassen im Geschlecht des Gitters M entspechen umkehrbar eindeutig den Doppelnebenklassen $G_{\mathbb{Q}} \backslash G_A / G_A(M)$ in G_A.
Beweis: Das Geschlecht von M besteht aus allen ΦM mit $\Phi \in G_A$. Zwei solche, etwa ΦM und ΨM gehören zur selben engeren Klasse, wenn es $\sigma \in G_{\mathbb{Q}}$ gibt mit $\Psi M = \sigma \Phi M$. Dies bedeutet, $\Psi^{-1} \sigma \Phi \in G_A(M)$. Also ist $\Phi \in G_{\mathbb{Q}} \Psi G_A(M)$, und Φ und Ψ bestimmen dieselbe Doppelnebenklasse.

Da V positiv definit ist, ist nach Kapitel 4 der homogene Raum $G_{\mathbb{Q}} \backslash G_A$ kompakt. Da $G_A(M)$ offen in G_A ist, gibt es nur endlich viele Doppelnebenklassen $G_{\mathbb{Q}} \backslash G_A / G_A(M)$, also nur endlich viele engere Klassen und erst recht nur endlich viele Klassen. Sei h

die Anzahl der Klassen und h^+ die Anzahl der engeren Klassen im Geschlecht von M. Durch die (disjunkte) Zerlegung

$$G_A = \cup_{i=1}^{h^+} G_{\mathbb{Q}} \Phi_i G_A(M)$$

erhält man

$$\int_{G_{\mathbb{Q}} \backslash G_A} \omega_A = \sum_{i=1}^{h^+} \int_{G_{\mathbb{Q}} \backslash G_{\mathbb{Q}} \Phi_i G_A(M)} \omega_A$$

$$= \sum_{i=1}^{h^+} \int_{G_{\mathbb{Q}} \backslash G_{\mathbb{Q}} \Phi_i G_A(M) \Phi_i^{-1}} \omega_A \text{ wegen der Rechtsinvarianz von } \omega_A$$

$$= \sum_{i=1}^{h^+} \int_{G_{\mathbb{Q}} \backslash G_{\mathbb{Q}} G_A(M_i)} \omega_A \quad \text{mit } M_i = \Phi_i M$$

$$= \sum_{i=1}^{h^+} \int_{G_{\mathbb{Q}} \cap G_A(M_i) \backslash G_A(M_i)} \omega_A \quad (\text{ vgl Kapitel 7 })$$

$G_A(M_i)$ ist eine kompakte Gruppe (weil G_∞ kompakt ist), ihr Durchschnitt mit der diskreten Gruppe $G_{\mathbb{Q}}$ ist endlich. Er besteht aus denjenigen speziellen orthogonalen Transformationen von $V_{\mathbb{Q}}$, die das Gitter M_i in sich transformieren, den sogenannten Einheiten von M_i mit Determinante 1. Ihre Anzahl wird mit $E^+(M_i)$ bezeichnet. Der letzte Ausdruck wird damit

$$= \sum_{1=1}^{h^+} \frac{1}{E^+(M_i)} \int_{G_A(M_i)} \omega_A = \sum_{i=1}^{h^+} \frac{1}{E^+(M_i)} \int_{G_A(M)} \omega_A$$

(letzteres wegen der Rechts- und Linksinvarianz von ω).

Sei $E(M_i)$ die Anzahl aller Einheiten von M_i. Bei Siegel kommt die $\sum_{i=1}^{h} \frac{1}{E(M_i)}$ vor. Zusammenhang mit unserer Summe:

Für die Summanden unterscheiden wir zwei Fälle:

1. M_i gestattet keine orthogonale Transformation mit Determinante -1. Dann zerfällt die Klasse vom M_i in zwei engere Klassen, etwa vertreten durch M_i und M_i', und für beide ist $E = E^+$.
2. M_i gestattet eine orthogonale Transformation mit Determinante -1. Dann ist die Klasse von M_i zugleich die engere Klasse, und $E = 2E^+$.

Das ergibt

$$\sum_{i=1}^{h^+} \frac{1}{E^+(M_i)} = \sum_{ersterFall} \left(\frac{1}{E^+(M_i)} + \frac{1}{E^+(M_i')}\right) + \sum_{zweiterFall} \frac{1}{E^+(M_i)} = \sum_{i=1}^{h} \frac{2}{E(M_i)}$$

Nun haben wir

$$\int_{G_{\mathbb{Q}} \backslash G_A} \omega_A = \sum_{i=1}^{h} \frac{2}{E(M_i)} \int_{G_A(M)} \omega_A \tag{1}$$

Das letzte Integral ist

$$\int_{G_A(M)} \omega_A = \int_{G_\infty} \omega_\infty \cdot \prod_p \int_{G(M_p)} \omega_p$$

Wir setzen die in Kapitel 9 und 12 gefundenen Werte für die lokalen Integrale ein:

$$\int_{G_\infty} \omega_\infty = (\frac{1}{2})^{\frac{(n-1)(n-2)}{2}} \cdot (\det A)^{\frac{n-1}{2}} \cdot \frac{\pi^{\frac{n(n+1)}{4}}}{\prod_{j=1}^{n} \Gamma(\frac{j}{2})}$$

$$\int_{G(M_p)} = \frac{1}{2} A_m p^{-m\frac{n(n-1)}{2}} \cdot p^{\nu\frac{n(n-3)}{2}} \cdot |\det A|_p^n \text{ für } m \geq 2\delta + 1$$

Die (für $m \geq 2\delta+1$) von m unabhängigen Zahlen $\frac{1}{2} A_m p^{-m\frac{n(n-1)}{2}}$ sind die Siegel'schen α_p .
Man erhält

$$\int_{G_A(M)} \omega_A = \frac{1}{2} (\det A)^{-\frac{n+1}{2}} \cdot \frac{\pi^{\frac{n(n+1)}{4}}}{\prod_{j=1}^{n} \Gamma(\frac{j}{2})} \cdot \prod_p \alpha_p$$

Zusammen mit (1) haben wir nun

Satz 16.

$$\sum_{i=1}^{h} \frac{1}{E(M_i)} = \frac{\Gamma(\frac{1}{2})\Gamma(\frac{3}{2}).....\Gamma(\frac{n}{2}) \cdot (\det A)^{\frac{n+1}{2}}}{\pi^{\frac{n(n+1)}{4}} \cdot \prod_p \alpha_p} \cdot \int_{G_{\mathbb{Q}} \backslash G_A} \omega_A \tag{2}$$

Die Minkowski-Siegel'sche Formel besagt, daß an Stelle des letzten Integrals der Faktor 2 stehen sollte ([S],Formel (72) auf Seite 568). Die Formel (2) zeigt, daß der Minkowski-Siegel'sche Satz äquivalent ist zur Aussage, daß das Volumen eines Fundamentalbereichs für die Adele nach den Hauptadelen der speziellen orthogonalen Gruppe G gleich 2 ist. Dieses Volumen heißt die Tamagawa-Zahl von G , kurz $\tau(G)$.

Im nächsten Kapitel wollen wir zur Minkowski-Siegel'schen Formel einige Beispiele rechnen. Danach wollen wir $\tau(G) = 2$ beweisen nach [W2], Seite 76-116. Dort werden fünf Typen von klassischen Gruppen gleichzeitig behandelt, wodurch der Beweis natürlich sehr lang und durch Fallunterscheidungen unterbrochen wird. Diese Vorlesung versucht, den Spezialfall der orthogonalen Gruppen möglichst durchsichtig darzustellen. Ganz zum Schluß werden wir uns sogar wieder auf den positiv definiten Fall zurückziehen, obwohl wir die Existenz des Tamagawa-Maßes für Formen von beliebigem Index (und Dimension ≥ 3) eingesehen haben und auch klar sein wird, welche Zusatzbetrachtungen man im allgemeinen Fall anstellen müßte.

14. Beispiele

Als erstes Beispiel behandeln wir die Gitter $\mathbb{Z}^n$ für $n \leq 8$, also $M = \sum_{i=1}^n \mathbb{Z}e_i$ mit $(e_i, e_j) = \delta_{ij}$. Wir müssen die α_p bestimmen. Nach Definition war

$$\alpha_p = \frac{1}{2} p^{-m\frac{n(n-1)}{2}} A_m \text{ für } m >> 0$$

mit

$$A_m = |\{X \bmod p^m \mid X'AX \equiv A \bmod p^m\}|$$

Für $A =$ Einheitsmatrix zeigt das Hensel'sche Lemma, daß $m = 1$ genügt, wenn $p \neq 2$, und $m = 3$ für $p = 2$. Wir entledigen uns zuerst des schwierigeren Falles $p = 2$. Zur Vereinfachung schreiben wir in diesem Teil M statt M_2.

Lemma 1. *Die Automorphismengruppe von M ist transitiv auf $\{x \in M \mid (x,x) = 1\}$.*

Beweis: Der Fall $n = 1$ ist trivial. Sei also $2 \leq n \leq 8$ und $x = \sum_{i=1}^n x_i e_i \in M$ mit $(x,x) = 1$. Sei t die Anzahl der ungeraden x_i (gemeint sind die x_i mit $|x_i|_2 = 1$): Dann ist $1 = (x,x) = \sum_{i=1}^n x_i^2 \equiv t \bmod 4$, wegen $n \leq 8$ also $t = 1$ oder $t = 5$. Daher gibt es ein gerades x_j (wenn $t = 1$ weil $n > 1$ und wenn $t = 5$ wegen $5 \not\equiv 1 \bmod 8$). Man setzt $s = x - e_j$. Dann ist $(s,s) \equiv 2 \bmod 4$ und die Spiegelung längs s führt M in sich und x in e_j über. Da die Permutationen der e_i ebenfalls Automorphismen von M sind, kann man jedes x mit $(x,x) = 1$ in e_1 überführen.

Folgerung: Wenn $x \in M$ und $(x,x) \equiv 1 \bmod 8$, dann gibt es einen Automorphismus τ von M mit $\mathfrak{o}_2 \tau x = \mathfrak{o}_2 e_1$.
Beweis: Jede Zahl $\equiv 1 \bmod 8$ ist Quadrat in $\mathfrak{o}_2$. Also gibt es eine Einheit ρ mit $(x,x) = \rho^2$. Auf $\frac{1}{\rho}x$ kann man das Lemma anwenden.

Bemerkung: Für $n = 9$ ist das Lemma nicht richtig: Sei $x = \frac{1}{3}\sum_{i=1}^9 e_i$. Dann ist $(x,x) = 1$. Die Vektoren im Orthokomplement von x sind die y mit $\sum_{i=1}^9 y_i = 0$. Für diese ist $(y,y) = \sum_{i=1}^9 y_i^2 \equiv 0 \bmod 2$. Also enthält $M \cap x^\perp$ keine Einheitsvektoren, wohl aber $e_1^\perp$. Also kann man sicherlich nicht x in e_1 durch einen Automorphismus von M überführen.

Jetzt sei $A_8(n,1)$ die Anzahl der $x \bmod 8$ in M mit $(x,x) \equiv 1 \bmod 8$.

$n = 1$:

$$A_8(1,1) = 4$$

$n = 2$: Ist $x_1^2 + x_2^2 \equiv 1 \bmod 8$, so ist genau eines der x_i ungerade und dann das andere $\equiv 0$ oder $4 \bmod 8$. Dafür gibt es $2 \cdot 4 \cdot 2$ Möglichkeiten.

$$A_8(2,1) = 16$$

$n = 3$: Sei $x_1^2 + x_2^2 + x_3^2 \equiv 1 \bmod 8$. Ist t die Anzahl der ungeraden x_i, so ist $t \equiv 1 \bmod 4$, also $t = 1$. Ist etwa x_1 ungerade, so ist $x_2^2 + x_3^2 \equiv 0 \bmod 8$. Also sind x_2^2 und x_3^2 entweder beide 0 oder beide $4 \bmod 8$. Das heißt x_2 und x_3 sind beide $\equiv 2, 6 \bmod 8$ oder beide $\equiv 0, 4 \bmod 8$. Dafür gibt es $2 \cdot 4 = 8$ Möglichkeiten.

Das ungerade x_1 kann 4 Werte annehmen, und statt x_1 könnte auch x_2 oder x_3 ungerade sein. Zusammen sind das $3 \cdot 4 \cdot 8$ Möglichkeiten.

$$A_8(3,1) = 3 \cdot 2^5$$

$n = 4$: Wieder ist $t = 1$. Die Anzahl s der $x_i \equiv 2$ oder $6 \bmod 8$ ist gerade.
$s = 0$: $x_2, x_3, x_4 \equiv 0$ oder$4 \bmod 8$. das sind 2^3 Möglichkeiten.
$s = 2$: Ein x_i ist 0 oder 4, die beiden anderen 2 oder $6 \bmod 8$. Zusammen sind das $4 \cdot 4 \cdot (2^3 + 3 \cdot 2^3)$ Möglichkeiten.

$$A_8(4,1) = 2^9$$

$n = 5$: Wegen $t \neq n$ (sonst wäre $1 \equiv (x,x) \equiv n \bmod 8$) fällt $t = 5$ immer noch aus, es ist $t = 1$. Und wieder ist s gerade. Wir zählen die x mit festem ungeraden x_1.
$s = 0$: $x_2, ..., x_5 \equiv 0, 4 \bmod 8$. Das sind 2^4 Vektoren.
$s = 2$: Ein Paar ist $2, 6$, das andere $0, 4 \bmod 8$. Das ergibt $\binom{4}{2} \cdot 2^4$ Vektoren.
$s = 4$: Alle $x_i \equiv 2, 6 \bmod 8$. Das sind 2^4 Vektoren.
Zusammen sind das $5 \cdot 4 \cdot (2^4 + 6 \cdot 2^4 + 2^4)$ Vektoren.

$$A_8(5,1) = 5 \cdot 2^9$$

$n = 6$: Jetzt kann in der Tat $t = 1$ oder $t = 5$ sein. Für $t = 5$ sind etwa $x_1, ..., x_5$ ungerade und x_6 gerade. Dann ist $(x,x) \equiv 5 + x_6^2 \bmod 8$, und daraus folgt $x_6 \equiv 2, 6 \bmod 8$. Also haben wir $6 \cdot 4^5 \cdot 2 = 3 \cdot 2^{12}$ Vektoren mit $t = 5$.
Für $t = 1$ haben wir
$s = 0$ mit 2^5 Fällen
$s = 2$ mit $\binom{5}{2} \cdot 2^5$ Fällen
$s = 4$ mit $5 \cdot 2^5$ Fällen.
Das sind $6 \cdot 4 \cdot 2^5 \cdot (1 + 10 + 5) = 3 \cdot 2^{12}$ Fälle mit $t = 1$. Zusammen

$$A_8(6,1) = 3 \cdot 2^{13}$$

$n = 7$: Für $t = 5$, etwa $x_1, ..., x_5$ ungerade, muß $5 + x_6^2 + x_7^2 \equiv 1 \bmod 8$ sein, also $x_6^2 + x_7^2 \equiv 4 \bmod 8$. Dazu muß $x_6 \equiv 2, 6 \bmod 8$ und $x_7 \equiv 0, 4 \bmod 8$ sein oder umgekehrt. Dafür gibt es $2 \cdot 2 \cdot 2$ Möglichkeiten. Das ergibt $\binom{7}{2} \cdot 4^5 \cdot 2^3$ Fälle mit $t = 5$.
Mit $t = 1$ haben wir zunächst bei festem ungeraden x_1
$s = 0$ mit 2^6 Fällen
$s = 2$ mit $\binom{6}{2} \cdot 2^6$ Fällen
$s = 4$ mit $\binom{6}{2} \cdot 2^6$ Fällen
$s = 6$ mit 2^6 Fällen.
Das sind $7 \cdot 4 \cdot 2^6(1 + 15 + 15 + 1)$ Vektoren mit $t = 1$. Adiert man dazu die für $t = 5$ erhaltenen, so erhält man

$$A(7,1) = 7 \cdot 2^{15}$$

$n = 8$: Ist $t = 5$ und etwa $x_1, ..., x_5$ ungerade, so muß $x_6^2 + x_7^2 + x_8^2 \equiv 4 \bmod 8$ sein. Dazu muß genau eines der drei $\equiv 2, 6 \bmod 8$ sein oder alle drei. Das ergibt $3 \cdot 2^3 + 2^3 = 2^5$ Vektoren, also von $t = 5$ einen Beitrag $\binom{8}{5} \cdot 4^5 \cdot 2^5 = 7 \cdot 2^{18}$.

Für $t = 1$ haben wir (bei festem ungeraden x_1)
$s = 0$ mit 2^7
$s = 2$ mit $\binom{7}{2} \cdot 2^7 = 7 \cdot 3 \cdot 2^7$
$s = 4$ mit $\binom{7}{4} \cdot 2^7 = 7 \cdot 5 \cdot 2^7$
$s = 6$ mit $7 \cdot 2^7$ Vektoren. Der Beitrag von $t = 1$ ist also $8 \cdot 4 \cdot 2^7 \cdot (1+21+35+7) = 2^{18}$.

$$A_8(8, 1) = 2^{21}$$

Nun zählen wir die ganzen Matrizen modulo 8 mit $X'X \equiv 1 \bmod 8$. Ist a die erste Spalte von X, so gilt für die übrigen Spalten b, daß $b'a \equiv 0 \bmod 8$. Da $a'a \equiv 1 \bmod 8$, gibt es nach der Folgerung zu Lemma 1 einen Gitterautomorphismus τ mit $\mathfrak{o}_2 \tau a = \mathfrak{o}_2 e_1$. Daher ist die Anzahl der möglichen Spalten $b \bmod 8$ mit $b'a \equiv 0 \bmod 8$ und $b'b \equiv 1 \bmod 8$ genau so groß wie die Anzahl der Spalten $b \bmod 8$ in $e_1^\perp = \sum_{i=2}^n \mathfrak{o}_2 e_i$ mit $b'b \equiv 1 \bmod 8$. Daraus folgt die Rekursion: ist

$$A_8(n) = |\{X \in M_n(\mathfrak{o}_2) \bmod 8 \mid X'X \equiv 1 \bmod 8\}|$$

so ist

$$A_8(n) = A_8(n, 1) \cdot A_8(n-1, 1) \ldots\ldots A_8(2, 1) \cdot A_8(1, 1)$$

Daraus finden wir

$$A_8(1) = 4 \qquad A_8(2) = 2^6 \qquad A_8(3) = 3 \cdot 2^{11}$$
$$A_8(4) = 3 \cdot 2^{20} \qquad A_8(5) = 3 \cdot 5 \cdot 2^{29} \qquad A_8(6) = 3^2 \cdot 5 \cdot 2^{42}$$
$$A_8(7) = 3^2 \cdot 5 \cdot 7 \cdot 2^{57} \qquad A_8(8) = 3^2 \cdot 5 \cdot 7 \cdot 2^{78}$$

Für die Siegel'schen Zahlen $\alpha_p = \frac{1}{2} p^{-3\frac{n(n-1)}{2}} A_p$ ergibt sich daraus

n	2	3	4	5	6	7	8
α_2	4	6	6	$\frac{15}{4}$	$\frac{45}{16}$	$\frac{315}{128}$	$\frac{315}{128}$

Für $p \neq 2$ ist $\alpha_p = \frac{1}{2} p^{-\frac{n(n-1)}{2}} A_1$, und $\frac{1}{2} A_1$ ist die Ordnung der speziellen orthogonalen Gruppe G über dem Körper $\mathbb{F}_p$. Diese haben wir am Ende von Kapitel 10 bestimmt. Speziell für die Form $\sum x_i^2$ ($\det V = 1$) übernehmen wir

$$\alpha_p(3) = 1 - p^{-2}$$

$$\alpha_p(4) = (1 - p^{-2})^2$$

$$\alpha_p(5) = (1 - p^{-2})(1 - p^{-4})$$

$$\alpha_p(6) = (1 - p^{-2})(1 - p^{-4})(1 - (\frac{-1}{p}) p^{-3})$$

$$\alpha_p(7) = (1 - p^{-2})(1 - p^{-4})(1 - p^{-6})$$

$$\alpha_p(8) = (1 - p^{-2})(1 - p^{-4})^2(1 - p^{-6})$$

Für $n \geq 3$ ist das Produkt der α_p absolut konvergent. Zum Beispiel erhält man für $n = 8$

$$\prod_p \alpha_p = \alpha_2 \prod_{p \neq 2} \alpha_p = \frac{315}{128} \cdot \prod_{p \neq 2} (1 - p^{-2})(1 - p^{-4})^2 (1 - p^{-6})$$

$$= \frac{315}{128} \cdot \frac{4 \cdot 16^2 \cdot 64}{3 \cdot 15^2 \cdot 63} \cdot \frac{1}{\zeta(2)\zeta(4)^2\zeta(6)} = \frac{2^{12} \cdot 3^5 \cdot 5^2 \cdot 7}{\pi^{16}}$$

Dies eingesetzt in die Maßformel ergibt auf der rechten Seite

$$\frac{2\Gamma(\frac{1}{2}).....\Gamma(\frac{7}{2})\Gamma(4) \cdot \pi^{16}}{\pi^{18} \cdot 2^{12} \cdot 3^5 \cdot 5^2 \cdot 7} = \frac{1}{2^{15} \cdot 3^2 \cdot 5 \cdot 7}$$

Die Automorphismengruppe des Gitters $\mathbb{Z}^n$ besteht offenbar aus allen Permutationsmatrizen mit Einträgen ± 1 und hat die Ordnung $2^8 \cdot 8! = 2^{15} \cdot 3^2 \cdot 5 \cdot 7$. Die Maßformel zeigt jetzt: Im Geschlecht der 8-reihigen Einheitsform liegt nur eine Klasse.

Zur Kontrolle vergleichen wir auch noch mit dem Siegel'schen Beispiel $n = 5$:

$$\prod \alpha_p = \alpha_2 \prod_{p \neq 2} \alpha_p = \frac{15}{4} \prod_{p \neq 2} (1 - p^{-2})(1 - p^{-4}) = \frac{15}{4} \cdot \frac{4}{3} \cdot \frac{16}{15} \cdot \frac{1}{\zeta(2)\zeta(4)} = \frac{2^6 \cdot 3^2 \cdot 5}{\pi^6}$$

Dies eingesetzt in die Maßformel ergibt auf der rechten Seite

$$\frac{2\Gamma(\frac{1}{2})\Gamma(\frac{3}{2})\Gamma(\frac{5}{2}) \cdot \pi^6}{\sqrt{\pi}^{15} \cdot 2^6 \cdot 3^2 \cdot 5} = \frac{1}{2^8 \cdot 3 \cdot 5}$$

Die Ordnung der Automorphismengruppe ist $2^5 \cdot 5! = 2^8 \cdot 3 \cdot 5$: Also folgt wieder, daß im Geschlecht der 5-reihigen Einheitsform nur eine Klasse liegt.

Auf dieselbe Weise kann man für alle $n \neq 6$ mit $3 \leq n \leq 8$ einsehen, daß im Geschlecht von $\mathbb{Z}^n$ nur eine Klasse liegt. Für $n = 6$ liefert die Minkowski-Siegel'sche Formel

$$\sum_{i=1}^{h} \frac{1}{E(M_i)} = \frac{1}{2^5 \cdot 3^2 \cdot 5} \cdot \frac{L(3, \chi)}{2\pi^3} = \frac{1}{6! \cdot 2^6} \cdot \frac{2^5 \cdot L(3, \chi)}{\pi^3}$$

wobei

$$L(s, \chi) = \prod_{p \neq 2} (1 - \chi(p)p^{-s})^{-1} = \sum_{k=0}^{\infty} \frac{\chi(1 + 2k)}{(1 + 2k)^s}$$

die L-Reihe zum Charakter $\chi(x) = (-1)^{\frac{x-1}{2}}$ ist. Wenn man nun aus irgendeiner anderen Quelle weiß (zum Beispiel [Bö], Kapitel 12), daß im Geschlecht von $\mathbb{Z}^6$ nur eine Klasse liegt, dann muß

$$L(3, \chi) = \frac{\pi^3}{2^5}$$

sein.

Als zweites Beispiel betrachten wir das Gitter E_8. Es ist gerade, unimodular und vom Rang 8, und positiv definit. Seine Determinante ist $= 1$. Wir wollen zeigen, daß es bis auf Isomorphie das einzige Gitter mit diesen Eigenschaften ist.

Jedes unimodulare Gitter über $\mathfrak{o}_p$ für eine Primzahl $p \neq 2$ besitzt eine Orthogonalbasis $e_1, ..., e_n$ mit $(e_i, e_i) = 1$ für $i < n$. Ist seine Determinante gleich 1, so ist (e_n, e_n) Quadrat, also oE auch $= 1$. Für $p \neq 2$ haben wir also dieselben Anzahlen $A_p(n)$ wie beim Gitter $\mathbb{Z}^n$. Aber für $p = 2$ müssen wir neue Betrachtungen anstellen. Wir sagen, ein Gitter ist vom Typ $A = (a_{ij})_{i,j}$, wenn es eine Basis $u_1, ..., u_n$ besitzt mit $(u_i, u_j) = a_{ij}$.

Lemma 2. *Jedes gerade unimodulare anisotrope Gitter L vom Rang 2 über $\mathfrak{o}_2$ ist vom Typ* $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

Beweis: Sei $x \in L$ mit maximalem $|(x,x)|$ (gemeint ist der 2-Betrag). Dann ist x primitiv, und, weil L unimodular, gibt es $y \in L$ mit $(x,y) = 1$. Die zugehörige Gram-Matrix ist $\begin{pmatrix} \alpha & 1 \\ 1 & \beta \end{pmatrix}$. Da L anisotrop, ist $-\det L = 1 - \alpha\beta$ nicht Quadrat, also ist $\alpha\beta \not\equiv 0 \bmod 8$. Anderseits sind α und β gerade. Es folgt $\alpha = 2a$, $\beta = 2b$ mit Einheiten a, b. Für $\lambda = 1$ und $\mu = 1 - a - b (\equiv 1 \bmod 2$, also $\mu^2 \equiv 1 \bmod 8)$ ist

$$a\lambda^2 + \lambda\mu + b\mu^2 \equiv a + (1 - a - b) + b \equiv 1 \bmod 8$$

Nach Hensel ist $a\lambda^2 + \lambda\mu + b\mu^2 = 1$ in $\mathfrak{o}_2$ lösbar, und für $u := \lambda x + \mu y$ gilt $(u,u) = 2$. Also hätten wir gleich mit einem Vektor $x \in L$ mit $(x,x) = 2$ beginnen können. L ist dann vom Typ $\begin{pmatrix} 2 & 1 \\ 1 & 2b \end{pmatrix}$ mit einer Einheit b. Dann ist $4b - 1 \equiv 3 \bmod 8,$, also $4b - 1 = 3\gamma^2$ mit einer Einheit γ in $\mathfrak{o}_2$. Nun ist $y' := \frac{1+\gamma}{2\gamma}x - \frac{1}{\gamma}y \in L$, und $(y', x) = 1$ und $(y', y') = 2$.

1. Bemerkung: Insbesondere ist $\begin{pmatrix} 2 & 1 \\ 1 & 2\epsilon \end{pmatrix} \simeq \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ für jede Einheit ϵ.

2. Bemerkung: Ein gerades unimodulares Gitter, welches 0 darstellt, ist offensichtlich hyperbolisch.

Lemma 3. *Sei L gerade unimodular vom Rang $2m$ und $\det L = (-1)^m$. Dann ist L direkte Summe von m hyperbolischen Gittern.*

Beweis: Solange $\dim L \geq 5$, stellt L die 0 dar, und man kann ein hyperbolisches Gitter abspalten. Also ist

$$L \quad = \quad \underbrace{H \perp ..... \perp H}_{r - \text{ mal}} \quad \perp \quad M$$

mit einem Gitter M vom Rang $2s = 0$ oder 2 oder 4, welches anisotrop und unimodular ist. Wenn es nicht 0 ist, kann man darin x, y finden mit $(x,y) = 1$. Diese spannen ein unimodulares anisotropes Gitter vom Rang 2 auf, welches man als orthogonalen direkten Summanden abspalten kann, m.a. W. $M = 0$ oder E oder $E \perp E$ mit $E = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ nach Lemma 1.

$M = E$ fällt aus, weil sonst $(-1)^m = \det L = (-1)^{m-1} \cdot 3$ und -3 nicht Quadrat.

$M = E \perp E$ fällt aus, weil sonst $M = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \begin{pmatrix} 2 & 1 \\ 1 & -2 \end{pmatrix}$ (nach Bemerkung 2 zu Lemma 1) isotrop wäre.

Also bleibt nur $M = 0$, und das ist die Behauptung.

Sei $L_n = \perp^n H$ direkte Summe von n hyperbolischen Gittern (vom Rang 2) und

$$A(n,t) = |\{u \in L_n, u \bmod 8 \mid (u,u) \equiv t \bmod 8\}|$$

Offenbar

$$A(n,t) = \sum_{s \bmod 8} A(1,s)A(n-1,t-s) \tag{1}$$

$A(1,t)$ ist die Anzahl aller Paare $(\lambda,\mu) \bmod 8$ mit $2\lambda\mu \equiv t \bmod 8$. Die folgende Tabelle zeigt die Anzahl der $\lambda \bmod 8$ mit $2\lambda\mu \equiv t \bmod 8$ bei gegebenem μ :

μ	0	1	2	3	4	5	6	7	$A(1,t) = \sum$
$t=0$	8	2	4	2	8	2	4	2	32
$t=2$	0	2	0	2	0	2	0	2	8
$t=4$	0	2	4	2	0	2	4	2	16

Die Zeile mit $t = 6$ ist dieselbe wie die mit $t = 2$. Aus (1) folgt

$$A(n,t) = 32A(n-1,t) + 8A(n-1,t-2) + 16A(n-1,t-4) + 8A(n-1,t-6)$$

$$= 8[A(n-1,t)+A(n-1,t-2)+A(n-1,t-4)+A(n-1,t-6)]+24A(n-1,t)+8A(n-1,t-4)$$

Die eckige Klammer ist die Anzahl aller $u \bmod 8$ in L_{n-1}, also $= 8^{2(n-1)}$. Hieraus können wir schrittweise alle $A(n,t)$ berechnen, wobei für unser Ziel $t = 0$ und 4 genügt:

$$A(n,t) = 8 \cdot 2^{6(n-1)} + 24A(n-1,t) + 8A(n-1,t-4)$$

$$\begin{array}{cc} A(1,0) = 32 & A(1,4) = 16 \\ A(2,0) = 2^7 \cdot 11 & A(2,4) = 2^7 \cdot 9 \\ A(3,0) = 2^{11} \cdot 37 & A(3,4) = 2^{11} \cdot 35 \\ A(4,0) = 2^{15} \cdot 137 & A(4,4) = 2^{15} \cdot 135 \end{array}$$

Hiervon müssen wir die Anzahl der nicht primitiven $u \bmod 8$ mit $(u,u) \equiv 0 \bmod 8$ abziehen. Das ist einfach die Anzahl aller $2u \bmod 8$ in L_n, also 4^{2n}.

Ergebnis: Die Anzahl $A^*(4,0)$ der primitiven $u \bmod 8$ mit $(u,u) \equiv 0 \bmod 8$ in jedem unimodularen Gitter vom Rang 8 mit Determinante 1 ist

$$A^*(4,0) = 2^{15} \cdot 137 - 2^{16} = 2^{15} \cdot 3^3 \cdot 5$$

Auf dieselbe Weise erhält man

$$A^*(3,0) = 2^{11} \cdot 5 \cdot 7$$

$$A^*(2,0) = 2^7 \cdot 9$$

$$A^*(1,0) = 2^4$$

Jetzt zählen wir die hyperbolischen Paare: Zu jedem primitiven u gibt es v mit $(u,v) = 1$. Man erhält alle solchen $v \bmod 8$, indem man zu einem festen v einen Vektor z mit $(z,u) \equiv 0 \bmod 8$ addiert. Also gibt es zu jedem primitiven u modulo 8 genau 8^{2n-1} Vektoren v mit $(u,v) \equiv 1 \bmod 8$. Diese v teilen wir ein in Gruppen zu je 8, nämlich $v, v-u, v-2u, ..., v-7u$. Unter diesen 8 gibt es genau zwei mit $(v-\lambda u, v-\lambda u) \equiv 0 \bmod 8$, nämlich für $2\lambda \equiv (v,v) \bmod 8$. Ein Viertel aller Vektoren v mit $(u,v) \equiv 1 \bmod 8$ erfüllt also zusätzlich $(v,v) \equiv 0 \bmod 8$. Zu jedem u gibt es also $\frac{1}{4} \cdot 8^{2n-1} = 2^{6n-5}$ Vektoren v.

Ergebnis: In L_n gibt es $B^*(n) := A^*(n) \cdot 2^{6n-5}$ Paare $u, v \bmod 8$ mit $(u,u) \equiv (v,v) \equiv 0 \bmod 8$ und $(u,v) \equiv 1 \bmod 8$. Die Werte sind

$$B^*(1) = 2^5$$

$$B^*(2) = 2^{14} \cdot 3^2$$

$$B^*(3) = 2^{24} \cdot 5 \cdot 7$$

$$B^*(4) = 2^{34} \cdot 3^3 \cdot 5$$

Jedes solche Paar spannt ein hyperbolisches Gitter auf; denn seine Gram-Determinante ist (-1) mal ein Quadrat.

Jetzt sei X eine lineare Abbildung von

$$L_n = H \perp ..... \perp H$$

auf sich mit

$$(Xx, Xy) \equiv (x,y) \bmod 8 \text{ für alle } x, y \in L_n$$

XH wird von einem modulo 8 hyperbolischen Paar u, v aufgespannt, ist also ein hyperbolisches Teilgitter und kann direkt abgespalten werden:

$$L_n = XH \perp M$$

Es ist (sinngemäß alles bis auf Quadrate)

$$(-1)^n = \det L_n = \det(XH) \det M = (-1) \cdot \det M$$

Damit erfüllt M die Voraussetzung von Lemma 2: M ist gerade, unimodular vom Rang $2(n-1)$, und $\det M = (-1)^{n-1}$. Nach Lemma 2 ist M direkte Summe von $n-1$ hyperbolischen Gittern.
Die beiden ersten Spalten von X sind u, v. Die dritte und vierte Spalte sind modulo 8 auf u und v senkrecht. Dann können wir sie modulo 8 so abändern, daß sie in M liegen. Daraus sehen wir:

Die Anzahl der $X \bmod 8$ mit $(Xx, Xy) \equiv (x,y) \bmod 8$ für alle $x, y \in L_n$ ist gleich

$$B^*(n)B^*(n-1).....B^*(1)$$

Mit den oben gefundenen Werten von B^* ist das gleich

$$2^{77} \cdot 3^5 \cdot 5^2 \cdot 7$$

Nach der Siegel'schen Definition war α_2 das $\frac{1}{2} \cdot 2^{-3 \cdot 28}$-fache davon, also

$$\alpha_2 = 2^{-8} \cdot 3^5 \cdot 5^2 \cdot 7$$

Wie schon bemerkt, sind die α_p für $p \neq 2$ dieselben wie für das Gitter $\mathbb{Z}^n$, also

$$\alpha_p = (1 - p^{-2})(1 - p^{-4})^2(1 - p^{-6})$$

Dadurch wird

$$\prod_p \alpha_p = \{2^{-8} \cdot 3^5 \cdot 5^2 \cdot 7\} \cdot \frac{4 \cdot 16^2 \cdot 64}{3 \cdot 15^2 \cdot 63} \cdot \frac{1}{\zeta(2)\zeta(4)^2\zeta(6)} = \frac{2^{11} \cdot 3^8 \cdot 5^3 \cdot 7}{\pi^{16}}$$

Setzt man dies in die Maßformel ein, so erhält man

$$\sum_{i=1}^{h} \frac{1}{E(M_i)} = \frac{1}{2^{14} \cdot 3^5 \cdot 5^2 \cdot 7}$$

Der Nenner ist gerade die Ordnung der Automorphismengruppe des aus der Theorie der Liealgebren bekannten Gitters E_8 (für einen Beweis siehe zum Beispiel [Bö], Kapitel 12). Es folgt, daß im Geschlecht von E_8 nur eine Klasse liegt. Vergleichsweise einfach ist zu sehen, daß alle geraden positiv definiten Gitter mit Determinante 1 ein Geschlecht bilden (und nur in durch 8 teilbarer Dimension existieren). Damit folgt:

Bis auf Isomorphie gibt es nur ein positiv definites unimodulares gerades Gitter vom Rang 8 über $\mathbb{Z}$

15. Charaktere

Der Weil'sche Beweis für $\tau(G) = 2$ benötigt Fouriertransformation auf der additiven Gruppe V_A. Zur Vorbereitung davon dienen die Kapitel 15 und 16.

Definition : Ein Charakter einer abelschen topologischen Gruppe G ist eine stetiger Homomorphismus von G in die Gruppe der komplexen Zahlen vom Betrag 1.

In diesem Kapitel wollen wir die Charaktere von $\mathbb{Q}_p$, A und V_A bestimmen.

$\mathbb{Q}_p$ Sei χ ein stetiger Homomorphismus von $\mathbb{Q}_p$ nach $\{|z| = 1\}$. Zu $\epsilon > 0$ existiert m mit $|\chi(x) - 1| < \epsilon$ für $x \equiv 0 \bmod p^m$. Das Bild $\chi(p^m \mathfrak{o}_p)$ ist eine Untergruppe in $\{|z| = 1\}$. Wählt man ϵ so klein, daß $\{|z - 1| < \epsilon\}$ keine Untergruppe $\neq 1$ von $\{|z| = 1\}$ enthält, so muß $\chi(p^m \mathfrak{o}_p) = 1$ sein.
Wir bestimmen zuerst alle Charaktere mit $\chi(\mathfrak{o}_p) = 1$: Sei χ ein solcher. Dann ist $\chi(\frac{1}{p^n})$ eine p^n-te Einheitswurzel, etwa

$$\chi(\frac{1}{p^n}) = e^{\frac{2\pi i}{p^n} \cdot a_n} \text{ mit } 0 \leq a_n < p^n$$

Aus

$$e^{\frac{2\pi i}{p^{n-1}} a_{n-1}} = \chi(\frac{1}{p^{n-1}}) = \chi(p \cdot \frac{1}{p^n}) = \chi(\frac{1}{p^n})^p = e^{\frac{2\pi i}{p^n} a_n p}$$

folgt

$$a_n \equiv a_{n-1} \bmod p^{n-1}$$

Daraus und aus $0 \leq a_n < p^n$ folgt, daß die Ziffern $\in \{0, 1, ..., p-1\}$ in der p-adischen Entwicklung von a_n und a_{n-1} bis zur Stelle $n-2$ übereinstimmen. Es gibt also eine ganze p-adische Zahl $c = \sum_{i=0}^{\infty} c_i p^i$ mit

$$a_n \equiv c \bmod p^n \text{ für alle } n$$

Ist $x \in \mathbb{Q}_p$ beliebig, etwa

$$x = \frac{x_{-m}}{p^m} + ... + \frac{x_{-1}}{p} + x^0 \text{ mit } x^0 \in \mathfrak{o}_p \text{ und } 0 \leq x_i < p$$

so ist, weil $\chi(\mathfrak{o}_p) = 1$,

$$\chi(x) = \chi(\sum_{j=1}^{m} \frac{x_{-j}}{p^j}) = \prod_{j=1}^{m} \chi(\frac{1}{p^j})^{x_{-j}} = \prod_{j=1}^{m} e^{\frac{2\pi i}{p^j} a_j x_{-j}} =$$

$$e^{2\pi i \sum_{j=1}^{m} \sum_{k=0}^{j-1} c_k p^k x_{-j} p^{-j}}$$

Die Summe im Exponenten läuft über alle Paare (k, j) mit $k - j < 0$. Sie ist der sogenannte p-adische Hauptteil $h_p(cx)$ von cx. Dieser ist für $y \in \mathbb{Q}_p$ nach Definition modulo $\mathbb{Z}$ gekennzeichnet durch

1. $h_p(y)$ ist eine rationale Zahl mit p-Potenznenner
2. $y - h_p(y) \in \mathfrak{o}_p$.

Wir sehen: Zu jedem Charakter χ von $\mathbb{Q}_p$ mit $\chi(\mathfrak{o}_p) = 1$ gibt es eine Zahl $c \in \mathfrak{o}_p$ mit

$$\chi(x) = e^{2\pi i h_p(cx)} \text{ für alle } x \in \mathbb{Q}_p$$

Für einen beliebigen Charakter χ von $\mathbb{Q}_p$ gibt es m mit $\chi(p^m \mathfrak{o}_p) = 1$. Der Charakter $\psi(x) := \chi(p^m x)$ ist gleich 1 auf $\mathfrak{o}_p$, also von der Gestalt $e^{2\pi i h_p(cx)}$, und damit ist $\chi(x) = e^{2\pi i h_p(p^{-m} cx)}$.

Die Abbildung $c \mapsto \chi_c$ mit $\chi_c(x) = e^{2\pi i h_p(cx)}$ von $\mathbb{Q}_p$ in seine Charaktergruppe $\hat{\mathbb{Q}}_p$ ist also surjektiv. Sie ist offensichtlich ein Homomorphismus, und injektiv ($h_p(cx) \in \mathbb{Z}$ für alle x ist nur möglich für $c = 0$). Sie ist zudem stetig und offen: Die Charaktergruppe wird nach Definition dadurch toplogisiert, daß die Mengen

$$W_{C,\epsilon} := \{\chi \mid \chi(C) \subset U_\epsilon(1)\}$$

wobei C die Kompakta $\ni 0$ und ϵ die positiven reellen Zahlen durchläuft und $U_\epsilon(1) = \{z \mid |z-1| < \epsilon\}$, ein Fundamentalsystem von offenen Einsumgebungen bilden. Nun:

$$\chi_c \; m\text{- nahe 1 in } \hat{\mathbb{Q}}_p \Leftrightarrow \chi(cp^{-m}\mathfrak{o}_p) \text{ nahe 1} \Leftrightarrow h_p(cp^{-m}\mathfrak{o}_p) \subset \mathbb{Z} \Leftrightarrow c \equiv 0 \bmod p^m$$

Ergebnis:

Satz 17. $\hat{\mathbb{Q}}_p \simeq \mathbb{Q}_p$ *als topologische Gruppe.*

$\mathbb{R}$ Dies entnehmen wir aus der Analysis: $c \mapsto \chi_c(x) := e^{-2\pi i c x}$ identifiziert $\mathbb{R}$ (algebraisch und topologisch) mit seiner Charaktergruppe.

A Sei $\chi \in \hat{A}$. Die Kompakta in A sind enthalten in Mengen der Gestalt

$$C = C_\infty \times \prod_p p^{-m_p}\mathfrak{o}_p, \text{ fast alle } m_p = 0$$

Mit demselben Schluß wie oben ($\{|z| = 1\}$ enthält keine kleinen Untergruppen) sehen wir: es gibt eine endliche Menge S und m_p für $p \in S$, so daß

$$\chi(\{0\} \times \prod_{p \in S} p^{-m_p}\mathfrak{o}_p \times \prod_{p \notin S} \mathfrak{o}_p) = 1$$

Für jede Stelle v sei i_v die Einbettung $x \mapsto (0, , ..., 0, x, 0, ...)$ von $\mathbb{Q}_v$ in A. Dann ist $\chi_v := \chi \circ i_v$ ein Charakter von $\mathbb{Q}_v$. Dazu gibt es c_∞ mit $\chi_\infty(x) = e^{-2\pi i c_\infty x}$ und c_p mit $\chi_p(x) = e^{2\pi i h_p(c_p x)}$.
Für $x \in A$ ist $x_p \in \mathfrak{o}_p$ für fast alle p, etwa für $p \notin T$. Wir schreiben

$$x = (x_\infty, ..., x_p, 0, ...) + (0, ..., 0, x_q, ...) = \sum_{v \in S \cup T} i_v(x_v) + (0, ..., 0, x_q, ...)$$

Nach Bestimmung von S ist

$$\chi(x) = \prod_{v \in S \cup T} \chi_v(x_v)$$

Da $\chi_p(x_p) = 1$ für $p \notin S \cup T$, kann man die $\chi_p(x_p)$ formal dem Produkt hinzufügen und schreiben

$$\chi(x) = \prod_v \chi_v(x_v) = e^{-2\pi i c_\infty x_\infty + 2\pi i \sum_p h_p(c_p x_p)} \tag{1}$$

Aus $\chi_p(\mathfrak{o}_p) = 1$ für $p \notin S$ folgt $c_p \in \mathfrak{o}_p$ für $p \notin S$. Also ist $c := (c_\infty, ..., c_p, ...)$ ein Adel. Die Abbildung $c \mapsto \chi_c$ von A nach $\hat{A}$, wo χ_c durch die rechte Seite von (1) definiert ist, ist bijektiv. Sie ist auch stetig und offen:

$$\chi_c \text{ nahe 1 in } \hat{A} \Longleftrightarrow$$

mit großem C_0 und großem S und großen m_p ist

$$e^{-2\pi i c_\infty x_\infty + 2\pi i \sum_p c_p x_p} \text{ nahe 1 in } \mathbb{C} \text{ für } x \in C_\infty \times \prod_{p \in S} p^{-m_p}\mathfrak{o}_p \times \prod_{p \notin S} \mathfrak{o}_p$$

$$\Longleftrightarrow c_\infty \text{ nahe } 0, c_p \equiv 0 \bmod p^{m_p} \text{ für } p \in S, c_p \in \mathfrak{o}_p \text{ für } p \notin S$$

$$\Longleftrightarrow c \text{ nahe 0 in } A$$

Ergebnis:

Satz 18. *$\hat{A} \simeq A$ algebraisch und topologisch .*

Ab jetzt bezeichnen wir $\chi_c(x) =< x, c >$.

Lemma 1. *Für $\xi \in \mathbb{Q}$ ist $\xi \equiv \sum_p h_p(\xi) \bmod \mathbb{Z}$.*

Beweis: $\xi - \sum_p h_p(\xi) = [\xi - h_q(\xi)] - \sum_{p \neq q} h_p(\xi)$ ist ganz für q. Dies gilt für jedes q. Also ist $\xi - \sum_p h_p(\xi) \in \mathbb{Z}$.

Für eine Untergruppe $B \subset A$ bezeichne

$$B^\perp = \{x \in A \mid < x, b >= 1 \text{ für alle } b \in B\}$$

Aus Lemma 1 folgt $\mathbb{Q} \subset \mathbb{Q}^\perp$
Mit $C = [0,1] \times \prod_p \mathfrak{o}_p$ war $A = C + \mathbb{Q}$.

$$W_{C,\epsilon} = \{\chi \in \hat{A} \mid \chi(C) \subset U_\epsilon(1)\}$$

ist offen in $\hat{A}$, und

$$\chi \in W_{C,\epsilon} \cap \mathbb{Q}^\perp \Rightarrow \chi(A) = \chi(C) \subset U_\epsilon(1), \text{ also } = 1 \quad (\epsilon \text{ klein})$$

weil $\chi(A)$ eine Untergruppe von $\{|z| = 1\}$ ist. Das zeigt: $\mathbb{Q}^\perp$ ist diskret in A. Dann ist auch $\mathbb{Q}^\perp/\mathbb{Q}$ diskret in $A/\mathbb{Q}$. Da $A/\mathbb{Q}$ kompakt, ist $\mathbb{Q}^\perp/\mathbb{Q}$ endlich. Anderseits ist $\mathbb{Q}^\perp$ offenbar ein $\mathbb{Q}$-Vektorraum. Dies zusammen ist nur möglich, wenn

$$\mathbb{Q} = \mathbb{Q}^\perp$$

V_A Man nimmt eine über $\mathbb{Q}$ definierte nicht ausgeartete symmetrische Bilinearform $(\ ,\ )$ und identifiziert V_A mit seiner Charaktergruppe vermöge $y \mapsto \chi_y$ mit

$$\chi_y(x) = \chi((x,y))$$

wobei

$$\chi(a) = e^{-2\pi i a_\infty + 2\pi i \sum_p h_p(a_p)}$$

der oben betrachtete Charakter von A ist. Dabei ist wieder

$$V_{\mathbb{Q}}^{\perp} = V_{\mathbb{Q}}$$

denn

$$\chi_y(V_{\mathbb{Q}}) = 1 \Leftrightarrow \chi((y,V_{\mathbb{Q}})) = 1 \Leftrightarrow \chi(\mathbb{Q}\cdot(y,V_{\mathbb{Q}})) = 1 \Leftrightarrow (y,V_{\mathbb{Q}}) \subset \mathbb{Q} \Leftrightarrow y \in V_{\mathbb{Q}}$$

Spezialfall: $V = D$ eine Quaternionenalgebra. Hier nimmt man die symmetrische Bilinearform $(x,y) = sp\,(xy)$, wobei sp die reduzierte Spur von D ist. Wenn $e_0, ..., e_3$ eine Basis von D ist mit $e_0 = 1, e_1^2 = a,\ e_2^2 = b$ und $e_1 e_2 = -e_2 e_1$, $a, b \in \mathbb{Q}^*$, und $x = x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3$, dann ist $sp\,(x) = 2x_0$. Ist D der zweireihige Matrizenring, dann ist sp die Matrizenspur.

16. Fouriertransformation

Allgemein: Ist G eine lokal kompakte abelsche Gruppe und $\hat{G}$ ihre Charaktergruppe, so definiert man für jede absolut integrierbare Funktion auf G die Fouriertransformierte $\hat{f}$ durch

$$\hat{f}(\chi) = \int_G f(x)\chi(x)dx$$

$\hat{f}$ ist eine stetige Funktion auf $\hat{G}$. Wir betrachten die für uns wichtigen Beispiele:

1. V_p Sei M_p ein Gitter in V_p und f eine lokal konstante Funktion mit kompaktem Träger auf V_p. Zu einer solchen f gibt es m mit $f(x) = 0$ außerhalb $p^{-m}M_p$. Für jedes $a \in p^{-m}M_p$ gibt es $k = k(a)$ mit $f(x) = f(a)$ falls $x \equiv a \bmod p^{k(a)}$. Aus der Überdeckung

$$p^{-m}M_p = \bigcup_{a \in p^{-m}M_p} (a + p^{k(a)}M_p)$$

kann man eine endliche auswählen:

$$p^{-m}M_p = \cup_{i=1}^{N}(a_i + p^{k(a_i)}M_p)$$

Die Zahl $k = max\ _i k_i$ hat die Eigenschaft

$$x, y \in p^{-m}M_p,\ x \equiv y \bmod p^k M_p \Longrightarrow f(x) = f(y)$$

f ist also auf den Restklassen $a + p^k M_p$ konstant,

$$f = \sum_a f(a)\mathbf{1}_{a+p^k M_p}$$

ist eine endliche Linearkombination von Indikatorfunktionen $\mathbf{1}_{a+p^k M_p}$. Berechnen wir von solchen f die Fouriertransformierte:

$$\hat{f}(y) = \int_{a+p^k M_p} < x, y > dx = \int_{p^k M_p} < a + x, y > dx =$$

$$< a, y > \cdot \begin{cases} vol(p^k M_p) & \text{wenn } y \in (p^k M_p)^\perp \\ 0 & \text{sonst} \end{cases}$$

$$=< a, y > vol(p^k M_p)\mathbf{1}_{(p^k M_p)^\perp}$$

Da $< a, y >$ bei festem a eine lokal konstante Funktion von y ist, zeigt dies: Die Fouriertransformierte ist wieder lokal konstant. Ihre Fouriertransformierte ist

$$\hat{\hat{f}}(z) = \int_{y \in (p^k M_p)^\perp} < a, y > vol(p^k M_p) < y, z > dy = vol(M_p)vol(M_p^\perp)\mathbf{1}_{p^k M_p}(a + z)$$

weil $M_p^{\perp\perp} = M_p$ und $(p^k M_p)^\perp = p^{-k}M_p^\perp$. Dies zeigt:
Für jede lokal konstante Funktion f mit kompaktem Träger ist

$$\hat{\hat{f}}(x) = \gamma_p f(-x)$$

Dabei ist $\gamma_p = vol(M_p) \cdot vol(M_p^\perp)$ eine nur von p (und der Identifizierung von V_p mit seiner Charaktergruppe, aber nicht von M_p) abhängige Konstante.

2. $V_\mathbb{R}$. Wir betrachten Funktionen des Typs *Polynom mal* $e^{-pos\,def\,quadratische\,Form}$. Ist $A = A'$ positiv definit, so ist

$$\int e^{-\pi x' Ax + 2\pi i x' y} dx = const \cdot e^{-\pi\, y' A^{-1} y}$$

und mit A ist auch A^{-1} positiv definit. Hieraus und (zum Beispiel) aus den Formeln in [E], Seite 86 sieht man: Mit f ist auch die Fouriertransformierte $\hat{f}$ vom beschriebenen Typ.

3. V_A.

Definition: Eine Funktion Φ auf V_A heißt Standardfunktion, wenn

1. $\Phi(x) = \prod_v \Phi_v(x_v)$ $\qquad\qquad$ $(\ x = (x_\infty, ..., x_p, ...)\ )$

2. Φ_∞ ist vom Typ Polynom mal $e^{-pos\,def\,quadratische\,Form}$ und alle ϕ_p sind lokal konstant mit kompaktem Träger

3. Für fast alle p ist Φ_p die Indikatorfunktion von M_p, wobei M ein fest vorgegebenes $\mathbb{Z}$-Gitter in $V_\mathbb{Q}$ ist.

Für eine Standardfunktion Φ ist

$$\hat{\Phi}(y) = \int_{V_A} \Phi(x) < x, y > dx =$$

$$\lim_S \prod_{v \in S} \int_{V_v} \Phi_v(x_v) < x_v, y_v > \ dx_v \cdot \prod_{p \notin S} \int_{V_p} \Phi_p(x_p) < x_p, y_p > dx_p$$

Für fast alle p ist Φ_p die Indikatorfunktion von M_p und $M_p = M_p^\perp$ und $vol(M_p) = 1$. Für alle S^*, die die Ausnahmestellen enthalten, ist

$$\hat{\Phi}(y) = \prod_{v \in S^*} \hat{\Phi}_v(y_v) \cdot \prod_{p \notin S^*} \mathbf{1}_{M_p}(y_p)$$

Das zeigt, daß $\hat{\Phi}$ wieder eine Standardfunktion ist.

Satz 19. *Für jede Standardfunktion Φ ist $\sum_{\xi \in V_\mathbb{Q}} \Phi(x + \xi)$ absolut konvergent, und zwar gleichmäßig in x auf jedem Kompaktum $C \subset V_A$.*

Beweis: Sei $C = C_\infty \times \prod_{p \in T} C_p \times \prod_{p \notin T} M_p$ und $x \in C$.

$$\Phi(x + \xi) \neq 0 \Rightarrow \Phi_p(x_p + \xi) \neq 0 \text{ für alle } p \Rightarrow \xi \in -C_p + Tr(\phi_p) \text{ für alle } p$$

$D_p := -C_p + Tr(\Phi_p)$ ist kompakt für alle p und $= M_p$ für fast alle p. Daher liegen die $\xi \in V_\mathbb{Q}$ mit $\Phi(\xi) \neq 0$ in einem Gitter $L \subset V_\mathbb{Q}$. Alle Φ_p sind beschränkt und fast alle gleich 1 auf M_p. Daher ist

$$\sum_{\xi \in V_\mathbb{Q}} |\Phi(x + \xi)| \leq const \cdot \sum_{\xi \in L} |\Phi_\infty(\xi)|$$

wobei die Konstante (außer von Φ) nur von dem Kompaktum C abhängt. Nach Definition von Standardfunktion ist die letzte Reihe konvergent.

$F(x) := \sum_{\xi \in V_{\mathbb{Q}}} \Phi(x+\xi)$ ist wegen der gleichmäßigen Konvergenz eine stetige Funktion auf $V_A/V_{\mathbb{Q}}$. Die Charaktergruppe von $V_A/V_{\mathbb{Q}}$ ist $\mathbb{Q}^{\perp} \subset V_A$. Die Fourierkoeffizienten von F sind

$$c(\eta) = \int_{V_A/V_{\mathbb{Q}}} F(x) < x, \eta > dx = \int_{V_A/V_{\mathbb{Q}}} \sum_{\xi \in V_{\mathbb{Q}}} \Phi(x+\xi) < x, \eta > dx =$$

$$\int_{V_A/V_{\mathbb{Q}}} \sum_{\xi \in V_{\mathbb{Q}}} \Phi(x+\xi) < x+\xi, \eta > \text{ weil } < \xi, \eta >= 1$$

$$= \int_{V_A} \Phi(x) < x, \eta > dx = \hat{\Phi}(\eta)$$

(vergleiche das Kapitel über Integration auf homogenen Räumen). $\hat{\Phi}$ ist wie gesehen wieder eine Standardfunktion, daher ist $\sum_{\eta \in V_{\mathbb{Q}}} |c(\eta)|$ konvergent, und damit ist die $\sum_{\eta \in V_{\mathbb{Q}}} c(\eta) < x, \eta >$ absolut konvergent. Nun besagt ein allgemeiner Satz aus der Theorie der Fouriertransformation: Wenn f und $\hat{f}$ beide absolut integrierbar sind und f stetig, dann gilt bei geeigneter Normierung der Haarschen Maße die Umkehrformel. Wenn zum Beispiel die Gruppe G kompakt ist, dann ist ihre Charaktergruppe $\hat{G}$ diskret, und die Maße sind richtig normiert, wenn die ganze Gruppe G das Volumen 1 bekommt und in $\hat{G}$ jeder Punkt die Masse 1. Hier ist $G = V_A/V_{\mathbb{Q}}$ mit dem Volumen 1, und das Integral über $\hat{G} \simeq V_{\mathbb{Q}}$ ist die $\sum_{\eta \in V_{\mathbb{Q}}}$. Das bedeutet jetzt: Die Funktion F auf $V_A/V_{\mathbb{Q}}$ wird durch ihre Fourierreihe dargestellt:

$$\sum_{\xi \in V_{\mathbb{Q}}} \Phi(x+\xi) = \sum_{\eta \in V_{\mathbb{Q}}} \hat{\Phi}(\eta) < x, \eta >$$

An der Stelle $x = 0$ ist das die Poisson'sche Summenformel.

17. Quaternionenalgebren

D sei eine Quaternionenalgebra über $\mathbb{Q}$, das ist ein vierdimensionaler $\mathbb{Q}$-Vektorraum mit Basis e_0, e_1, e_2, e_3 mit $e_0 = 1, e_1^2 = a, e_2^2 = b, e_1 e_2 = -e_2 e_1$, $a, b \in \mathbb{Q}^*$. Für $x = x_0 + x_1 e_1 + x_2 e_2 + x_3 e_3$ wird die reduzierte Norm definiert durch

$$N(x) = x_0^2 - a x_1^2 - b x_2^2 + ab x_3^2$$

In diesem Kapitel wird vorausgesetzt, daß die Norm über $\mathbb{Q}$ die 0 nicht darstellt, das bedeutet, daß die Algebra $D_{\mathbb{Q}}$ nullteilerfrei ist.

$$\frac{dx}{(Nx)^2} = \frac{dx_0 \wedge .... \wedge dx_3}{(Nx)^2}$$

ist eine invariante Differentialform auf der multiplikativen Gruppe D^*. Leider existiert das analog zu Kapitel 11 gebildete Maß auf der Adelgruppe D_A^* nicht, nämlich: Für fast alle p ist D_p der zweireihige Matrizenring über $\mathbb{Q}_p$, also $D_p^* \simeq GL_2(\mathbb{Q}_p)$ und

$$\int_{GL_2(\mathfrak{o}_p)} \frac{dx_p}{|N(x)|_p^2} = p^{-4} |GL_2(\mathbb{F}_p)| = p^{-4}(p^2-1)(p^2-p)$$

$$= (1-p^{-1})(1-p^{-2})$$

und das Produkt über p hiervon ist nicht konvergent. Aber die Formel zeigt: Setzt man $\lambda_p = (1 - \frac{1}{p})^{-1}$, so konvergiert das Produkt

$$\prod_p \lambda_p \int_{GL_2(\mathfrak{o}_p)} \frac{dx_p}{|N(x)^2|_p}$$

und liefert auf dieselbe Weise wie in Kapitel 11 ein Maß auf D_A^*. Dieses bezeichnen wir mit $d_A^* x$, und die $\frac{dx_p}{|N(x)^2|}$ kurz mit $d^* x_p$.

In Kapitel 16 wurde "Standardfunktion" definiert. Für eine Standardfunktion Φ und eine komplexe Variable s wollen wir die Existenz des folgenden Integrals untersuchen:

$$\int_{D_A^*} |N(x)|^s \Phi(x) d_A^* x$$

Nach Definition ist es gleich

$$\lim_S \prod_{v \in S} \int_{D_v^*} |N(x_v)|_v^s \Phi_v(x_v) \lambda_v dx_v^* \cdot \prod_{p \notin S} \int_{D^*(\mathfrak{o}_p)} |N(x_p)|_p^s \Phi_p(x_p) \lambda_p d^* x_p$$

(dabei wurde formal $\lambda_\infty = 1$ gesetzt).

Für die Existenz muß gezeigt werden:

1. $\int_{D_v^*}$ existiert für jedes v
2. $\prod_{p \notin S} \int_{D^*(\mathfrak{o}_p)}$ konvergiert für jedes endliche S.
3. $\lim_S$ existiert.

Zu 1. Weil $\Phi_\infty = Polynom \cdot e^{-pos\ def}$, konvergiert das $\int_{D_\infty^*} |N(x)|_\infty^{s-2}\Phi_\infty(x)\ dx$ für $Re\ s > 2$. Für $p \neq \infty$ haben wir, falls $Re\ s > 2$, eine stetige Funktion über ein Kompaktum zu integrieren, also existiert auch hier das Integral für $Re\ s > 2$.

Zu 2. Bekanntlich ist $D_p \simeq M_2(\mathbb{Q}_p)$ für fast alle p. Sei S so groß, daß für alle $p \notin S$

$D_p \simeq M_2(\mathbb{Q}_p)$

Die Übergangsformeln von den x_ν in $x = x_0 + x_1 i + x_2 j + x_3 ij$ zu den Matrixkoeffizienten x_{rs} unimodular sind

Φ_p die Indikatorfunktion von $M_2(\mathfrak{o}_p)$ ist.

Dann wird

$$\int_{D_p^*} |N(x)|_p^s \Phi_p(x)\, \lambda_p d^* x_p = \int_{GL_2(\mathbb{Q}_p)\cap M_2(\mathfrak{o}_p)} |\det x|_p^s \cdot \lambda_p \frac{dx_p}{|\det x|_p^2}$$

Aus der Zerlegung

$$GL_2(\mathbb{Q}_p) \cap M_2(\mathfrak{o}_p) = \cup_{k,l\geq 0, b \bmod p^k} \begin{pmatrix} p^k & b \\ 0 & p^l \end{pmatrix} GL_2(\mathfrak{o}_p)$$

erhalten wir für dieses Integral

$$\sum_{k,l\geq 0, b \bmod p^k} p^{-(k+l)s} \lambda_p \int_{\begin{pmatrix} p^k & b \\ 0 & p^l \end{pmatrix} GL_2(\mathfrak{o}_p)} \frac{dx_p}{|\det x|_p^2}$$

$$= \sum_{k,l\geq 0, b \bmod p^k} p^{-(k+l)s} \lambda_p \int_{GL_2(\mathfrak{o}_p)} \frac{dx_p}{|\det x|_p^2}$$

wegen der Links-Invarianz des Integrals

$$= \sum_{k,l\geq 0, b \bmod p^k} p^{-(k+l)s} \lambda_p (p^2-1)(p^2-p)p^{-4}$$

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

Das beweist gleichzeitig 2. und 3. und rechtfertigt die Definition

$$Z(s,\Phi) := \int_{D_A^*} |N(x)|^s \Phi(x) d_A^* x \tag{1}$$

und wir haben den

Satz 20. *$Z(s,\Phi)$ ist für Re $s>2$ durch (1) definiert und stellt dort eine differenzierbare Funktion von s dar.*

(Die letzte Behauptung kann man durch Abschätzung des Differenzenquotienten nachrechnen).

Berechnung des Residuums an der Stelle $s=2$:

Sei S so groß, daß die eben durchgeführte Rechnung für $p\notin S$ gilt. Dann ist

$$Z(s,\Phi)=\frac{\prod_{v\in S}\int_{D_v^*}|Nx|_v^s\Phi_v(x)\lambda_v d^*x_v}{\prod_{p\in S}(1-p^{-2})(1-p^{1-s})^{-1}(1-p^{-s})^{-1}}\cdot\frac{\zeta(s-1)\zeta(s)}{\zeta(2)}$$

Der linke Bruch (bestehend aus endlich vielen Faktoren in Zähler und Nenner) strebt für $s\to 2$ gegen

$$\frac{\prod_{v\in S}\int_{D_v^*}\Phi_v(x)\lambda_v dx_v}{\prod_{p\in S}(1-p^{-1})^{-1}}=\prod_{v\in S}\int_{D_v^*}\Phi_v(x)dx_v=\prod_{v\in S}\int_{D_v}\Phi_v(x)dx_v$$

(Rechtfertigung des letzten Schritts: Auf $N(x)=x_0^2-ax_1^2-bx_2^2+abx_3^2=0$ ist $dx_0\wedge dx_1\wedge dx_2\wedge dx_3=0$). Da die Riemannsche Zetafunktion an der Stelle 1 das Residuum 1 hat, folgt

$$\lim_{s\to 2}(s-2)Z(s,\Phi)=\prod_{v\in S}\int_{D_v}\Phi_v(x)dx_v=\int_{D_A}\Phi(x)dx_A=\hat{\Phi}(0) \tag{2}$$

denn $\int_{D_p}\Phi_p(x)dx_p=1$ für $p\notin S$.

Die "additive Rechnung": Hier wird vorausgesetzt, daß $D_{\mathbb{Q}}$ **nullteilerfrei** ist: Zuerst zerlegen wir $Z(s,\Phi)$ in einen holomorphen Summanden und den Rest: Wir setzen für $x\in D_A^*$

$$\lambda_+(x)=\begin{cases}1 & \text{wenn } |Nx|>1\\ \frac{1}{2} & \text{wenn } |Nx|=1\\ 0 & \text{sonst}\end{cases}$$

und $\lambda_-(x)=\lambda_+(\frac{1}{x})$. Dann ist $\lambda_+(x)+\lambda_-(x)=1$ für alle x, und mit

$$Z_\pm(s,\Phi)=\int_{D_A^*}\lambda_\pm(x)\Phi(x)|Nx|^s d_A^*x$$

ist

$$Z(s.\Phi)=Z_+(s,\Phi)+Z_-(s,\Phi)$$

Beide Integrale Z_+ und Z_- sind konvergent für Re $s>2$. Das für Z_+ konvergiert aber umso besser, je kleiner der Realteil von s ist. Daher ist Z_+ in der ganzen s-Ebene konvergent. Man zeigt unmittelbar (durch Betrachtung des Differenzenquotienten), daß $Z_+(s,\Phi)$ eine differenzierbare Funktion von s ist. Also ist $Z_+(s,\Phi)$ eine ganze Funktion von s.

Die (im allgemeinen vorhandene) Singularität von $Z(s,\Phi)$ steckt also in Z_-:

Sei D_A^1 die Untergruppe aller $x \in D_A^*$ mit $|Nx| = 1$ (Idelbetrag). Vermöge

$$(t, y) \to (\sqrt{t}y_\infty, ..., y_p, ...)$$

identifizieren wir $\mathbb{R}_{>0}^* \times D_A^1$ mit D_A^* . und normieren das Haarsche Maß auf D_A^1 so, daß

$$\int_{D_A^*} f(x) d_A^* x = \int_0^\infty (\int_{D_A^1} f(ty) d_A^1 y) \, \frac{dt}{t}$$

Damit wird

$$Z_-(s, \Phi) = \int_0^\infty (\int_{D_A^1} \lambda_-(ty)|N(ty)|^s \Phi(ty) d_A^1 y) \, \frac{dt}{t}$$

$$= \int_0^\infty \lambda_-(t) t^s \int_{D_A^1} \Phi(ty) d_A^1 y \, \frac{dt}{t}$$

$$= \int_0^1 t^s \int_{D_{\mathbb{Q}}^* \backslash D_A^1} (\sum_{\xi \in D_{\mathbb{Q}}^*} \Phi(t\xi y) d_A^1 \dot{y}) \, \frac{dt}{t}$$

(vgl Kapitel 7). Mit dem am Ende von Kapitel 15 beschriebenen Charakter von D_A und der Identifizierung von D_A mit seiner Charaktergruppe ist die Fouriertransformierte von $\Psi(z) := \Phi(tzy)$ (vgl. Kapitel 16)

$$\hat{\Psi}(w) = \int_{D_A} \Phi(tzy) \chi(sp(zw)) dz = \int_{D_A} t^{-2} \Phi(z) \chi(sp(t^{-1} z y^{-1} w)) dz$$

$$= \int_{D_A} t^{-2} \Phi(z) \chi(sp(z y^{-1} w t^{-1}) dz = t^{-2} \hat{\Phi}(y^{-1} w t^{-1})$$

Nach der Poisson'schen Summenformel (Kapitel 16) folgt

$$\sum_{\xi \in D_{\mathbb{Q}}^*} \Phi(t\xi y) = -\Phi(0) + \sum_{\xi \in D_{\mathbb{Q}}} \Phi(t\xi y) \text{ weil } D_{\mathbb{Q}} \text{ nullteilerfrei}$$

$$= -\Phi(0) + \sum_{\xi \in D_{\mathbb{Q}}} t^{-2} \hat{\Phi}(y^{-1} \xi t^{-1})$$

Setzt man dies ein, so erhält man

$$Z_-(s, \Phi) = \int_0^1 t^s \{ \int_{D_{\mathbb{Q}}^* \backslash D_A^1} [-\Phi(0) + t^{-2} \hat{\Phi}(0) + \sum_{\xi \in D_{\mathbb{Q}}^*} t^{-2} \hat{\Phi}((\xi^{-1} y)^{-1} t^{-1}] \, d_A^1 \dot{y} \} \, \frac{dt}{t}$$

Wir benutzen ein zweites Mal, daß $D_{\mathbb{Q}}$ nullteilerfrei ist, also N über $\mathbb{Q}$ nicht die 0 darstellt. In Kapitel 4 haben wir gesehen, daß für die spezielle orthogonale Gruppe G eines anisotropen Raumes der homogene Raum $G_A/G_{\mathbb{Q}}$ kompakt ist. Mit einem ganz ähnlichen Schluß sieht man hier, daß $D_{\mathbb{Q}}^* \backslash D_A^1$ kompakt ist. Zur Bequemlichkeit des Lesers sei diese Modifikation hier kurz ausgeführt (für die Kompaktheit ist es natürlich unerheblich, ob die diskrete Untergruppe links oder rechts ausdividiert wird):

Satz 21. *Wenn $D_{\mathbb{Q}}$ nullteilerfrei ist, dann ist der homogene Raum $D_{\mathbb{Q}}^*\backslash D_A^1$ kompakt.*

Beweis: Man nimmt ein Kompaktum C in der additiven Gruppe D_A, dessen Volumen echt größer ist als das Volumen von $D_{\mathbb{Q}}\backslash D_A$ (also >1 nach der Normierung des Maßes auf D_A). Ist nun $a \in D_A^1$, so ist nach der Integraltransformationsformel $vol\,(aC) = vol\,(Ca^{-1}) = vol\,(C) > 1$. Folglich sind die Translate $\xi + aC$, $\xi \in D_{\mathbb{Q}}$ nicht disjunkt: es gibt $\xi \neq \eta$ in $D_{\mathbb{Q}}$ und $c_1, c_2 \in C$ mit $\xi + ac_1 = \eta + ac_2$, d.h. $0 \neq \xi - \eta = a(c_2 - c_1)$, das heißt wir haben (Bezeichnungswechsel) ein Element ξ mit

$$0 \neq \xi \in D_{\mathbb{Q}} \cap aC' \quad \text{und genauso } 0 \neq \eta \in D_{\mathbb{Q}} \cap C'a^{-1}$$

und dabei ist $C' := C - C$ kompakt. Da $D_{\mathbb{Q}}$ nullteilerfrei ist, folgt

$$0 \neq \eta\xi \in C' \cdot C' \cap D_{\mathbb{Q}}$$

und $C'C'$ ist ebenfalls kompakt in D_A. Daher ist $C'C' \cap D_{\mathbb{Q}}$ endlich, und $\eta\xi$ gehört einem endlichen Wertevorrat an: $\eta\xi \in \{\zeta_1, ..., \zeta_h\}$, alle $\zeta_i \neq 0$. Ist $\eta\xi = \zeta_i$, so haben wir

$$\eta a \in C' \text{ und } (\eta a)^{-1} = a^{-1}\eta^{-1} = a^{-1}\xi\zeta_i^{-1} \in C'\zeta_i^{-1}$$

Setzt man $\cup_{i=1}^h C'\zeta_i^{-1} = E$, so ist E kompakt, und wir haben gezeigt: Zu $a \in D_A^1$ gibt es $\eta \in D_{\mathbb{Q}}^*$ so, daß

$$(\eta a, (\eta a)^{-1}) \in C' \times E$$

Die Menge

$$F = \{b \in D_A^* \mid (b, b^{-1}) \in C' \times E\}$$

ist kompakt in der multiplikativen Gruppe D_A^*, und $D_A^1 \subset D_{\mathbb{Q}}^* \cdot F$.

Wir fahren fort in der Behandlung von Z_-: Der homogene Raum $D_{\mathbb{Q}}^*\backslash D_A^1$ hat nun sicher endliches Volumen, etwa $= \mu$, und damit wird

$$(3) \qquad Z_-(s, \Phi) = [\frac{-\Phi(0)}{s} + \frac{\hat{\Phi}(0)}{s-2}] \cdot \mu + \int_0^1 t^{s-2} \int_{D_{\mathbb{Q}}^*\backslash D_A^1} \sum_{\xi \in D_{\mathbb{Q}}^*} \hat{\Phi}((\xi^{-1}y)^{-1}t^{-1}) d^1\dot{y}\, \frac{dt}{t}$$

Nach Kapitel 7 ist

$$\int_{D_A^1} \hat{\Phi}(y^{-1}t^{-1}) d_A^1 y = \int_{D_{\mathbb{Q}}^*\backslash D_A^1} \sum_{\xi \in D_{\mathbb{Q}}^*} \hat{\Phi}((\xi y)^{-1}t^{-1}) d^1\dot{y}$$

Daher ist das Integral in (3) (es ist egal, ob man über ξ^{-1} oder ξ summiert) gleich

$$\int_0^1 t^{s-2} \int_{D_A^1} \hat{\Phi}(y^{-1}t^{-1}) d_A^1 y\, \frac{dt}{t}$$

Weil $d_A^1 y$ und $\frac{dt}{t}$ invers-invariant sind, ist dies gleich

$$\int_1^\infty t^{2-s} \int_{D_A^1} \hat{\Phi}(yt) d_A^1 y\, \frac{dt}{t}$$

und, weil $yt = ty$, gleich

$$\int_0^\infty \lambda_+(x)|Nx|^{2-s} \hat{\Phi}(x) d_A^* x = Z_+(2-s, \hat{\Phi})$$

Damit haben wir bewiesen

Satz 22.

$$Z(s,\Phi) = [-\frac{\Phi(0)}{s} + \frac{\hat{\Phi}(0)}{s-2}] \cdot \mu + Z_+(s,\Phi) + Z_+(2-s,\hat{\Phi}))$$

und $Z_+(s,\Phi)$ *ist eine ganze Funktion von* s .

Man kann aus diesem Satz das Residuum von $Z(s,\Phi)$ an der Stelle $s = 2$ ablesen, nämlich

$$\lim_{s\to 2}(s-2)Z(s,\phi) = \hat{\Phi}(0) \cdot \mu$$

Vergleich mit dem Ergebnis (1) der "multiplikativen Rechnung" zeigt $\mu = 1$, oder noch einmal ausführlich formuliert

Satz 23. *Für das oben definierte Maß auf* D_A^1 *hat der homogene Raum* $D_{\mathbb{Q}}^* \backslash D_A^1$ *das Volumen 1.*

Wir wollen Satz 23 benutzen, um die Verankerung bei $n = 3$ für die Berechnung der Tamagawa-Zahl der orthogonalen Gruppen zu machen. Das genügt für die orthogonalen Gruppen in Dimension ≥ 3 , wenn man sich auf Formen beschränkt, die anisotrop über $\mathbb{Q}$ sind. Wenn man beliebige Formen betrachtet, muß man in zwei aufeinander folgenden Dimensionen verankern, also etwa 3 und 4. Warum, werden wir in Kapitel 18 genauer sehen.

Sei Z das Zentrum der Quaternionenalgebra D , bestehend aus den Vielfachen von e_0 . Dann ist $G := D^*/Z^*$ die spezielle orthogonale Gruppe des dreidimensionalen Raumes $V =< -a, -b, ab >$. Die Projektion

$$\pi : D^* \to G, \quad \text{gegeben durch } \pi(x)\, v = xvx^{-1}$$

mit Kern Z^* besitzt lokale Schnitte, so daß sie auch für die Adelgruppen surjektiv ist : $G_A \simeq D_A^*/Z_A^*$. Die Gruppe Z_A^* ist die Idelgruppe I von $\mathbb{Q}$.

Wir wissen (Kapitel 8), daß es auf G eine invariante Differentialform $\omega \neq 0$ höchsten (also dritten) Grades gibt. Dann ist $\psi(x) = \omega(\pi x)$ eine invariante Form dritten Grades auf D^* . Die Form ersten Grades $\frac{1}{2}\frac{d(Nx)}{Nx}$ ist invariant auf D^* . Dann ist auch $\frac{1}{2}\frac{d(Nx)}{Nx} \wedge \psi(x)$ invariant auf D^* (und $\neq 0$). Weil es bis auf rationale Vielfache nur eine über $\mathbb{Q}$ definierte invariante Form höchsten Grades gibt, ist

$$\frac{1}{2}\frac{d(Nx)}{Nx} \wedge \omega(\pi x) = \gamma \cdot \frac{dx_0 \wedge ..... \wedge dx_3}{(Nx)^2}$$

mit einer rationalen Konstanten γ . Für die lokalen aus diesen Differentialformen abgeleiteten Maße bedeutet das

$$|\gamma|_p \int_{D_p^*} f(x) \frac{(dx_0....dx_3)_p}{|Nx|_p^2} = \int_{D_p^*} f(x) \cdot \frac{(d(Nx))_p}{|2Nx|_p}\ \psi(x)_p$$

Nach Kapitel 7 ist dies gleich

$$\int_{G_p} (\int_{Z_p^*} f(zx) \cdot \frac{dN(zx)_p}{|2N(zx)|_p})\ \omega_p(\pi x)$$

Bei festem x gilt

$$\frac{dN(zx)}{N(zx)} = \frac{d(z^2Nx)}{z^2Nx} = 2\frac{dz}{z}$$

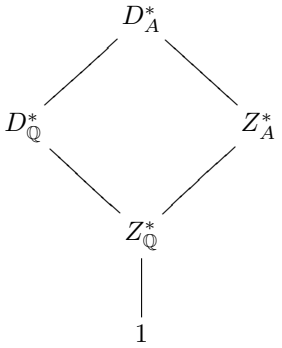
Es folgt

$$|\gamma|_p \int_{D_p^*} f(x) \frac{(dx_0....dx_3)_p}{|Nx|_p^2} = \int_{G_p} (\int_{Z_p^*} f(zx) \frac{dz_p}{|z|_p}) \, \omega_p(\pi x) \tag{4}$$

In jedem der drei Integrale geht das Volumenelement aus einer über $\mathbb{Q}$ definierten Differentialform hervor. Bei dem Integral über G_p handelt es sich also um die p-Komponente des Tamagawa-Maßes (siehe Kapitel 11). Für die beiden anderen konvergiert leider das Produkt der Integrale über $Z_{\mathfrak{o}_p}^* = \mathfrak{o}_p^*$ bzw. über $D_{\mathfrak{o}_p}^*$ nicht, nämlich:

Für fast alle p ist $D_{\mathfrak{o}_p} \simeq M_2(\mathfrak{o}_p)$ und das Integral hat den Wert $(p^2-1)(p^2-p)\cdot p^{-4} = (1-p^{-2})(1-p^{-1})$, und das Integral über $\mathfrak{o}_p^*$ ist $= 1-p^{-1}$. Wir multiplizieren beide Seiten von (4) mit $\lambda_p := (1-\frac{1}{p})^{-1}$ und benutzen die mit den Konvergenzfaktoren λ_p versehenen Maße d_A^*x auf D_A^* bzw. d_I^*z auf $Z_A^* = I$. Bei der Produktbildung heben sich die Faktoren $|\gamma|_p$ weg wegen der Produkformel (es war $\gamma \in \mathbb{Q}$)

In dem Diagramm



integrieren wir zunächst links herum:

$$\int_{D_A^*} f(x) d_A^* x = \int_{D_{\mathbb{Q}}^* \backslash D_A^*} \sum_{\xi \in D_{\mathbb{Q}}^*} f(\xi x) \; d_A^* \dot{x}$$

und dann rechts

$$\int_{D_A^*} f(x) d_A^* x = \int_{D_A^*/Z_A^*} (\int_{Z_A^*} f(xz) d_I^* z) \omega_A(\pi x)$$

$$= \int_{G_A} (\int_I f(xz) d_I^* z) \omega_A(\pi x)$$

Also haben wir

$$\int_{D_{\mathbb{Q}}^* \backslash D_A^*} \sum_{\xi \in D_{\mathbb{Q}}^*} f(\xi x) d_A^* \dot{x} = \int_{G_A} (\int_I f(xz) \; d_I^* z) \; \omega_A(\pi x)$$

Die obigen Vorbetrachtungen dienten dazu, einzusehen, daß diese Formel nicht nur wie in Kapitel 7 mit irgendwelchen geeignet normierten Maßen gilt, sondern mit dem Tamagawa-Maß von G und den modifizierten Tamagawa-Maßen von D^* und Z.

Das Integral über G_A behandeln wir weiter, indem wir zuerst über die Untergruppe $G_{\mathbb{Q}}$ summieren. Der Integrand ist $\int_I f(xz)d_I^*z =: F(\pi x)$. Wir erhalten

$$\int_{G_A/G_{\mathbb{Q}}} \sum_{\gamma\in G_{\mathbb{Q}}} F(\pi x\cdot\gamma)\omega_A$$

Die Summanden sind alle von der Form $F(\pi x\cdot\gamma) = F(\pi(x\xi))$, denn jedes γ ist ein $\pi(\xi)$. Um jeden Summanden genau einmal zu erhalten, muß man ξ modulo $Z_{\mathbb{Q}}^* = \mathbb{Q}^*$ laufen lassen. Dadurch erhält man

$$\int_{G_A/G_{\mathbb{Q}}} \sum_{\xi\in D_{\mathbb{Q}}^*/\mathbb{Q}^*} \int_I f(x\xi z)d_I^*z\ \omega_A(\pi x)$$

Im Integral über I summieren wir wieder zuerst über $\zeta\in\mathbb{Q}^*$ und erhalten

$$\int_{G_A/G_{\mathbb{Q}}} \sum_{\xi\in D_{\mathbb{Q}}^*/\mathbb{Q}^*} \int_{I/\mathbb{Q}^*} \sum_{\zeta\in\mathbb{Q}^*} f(x\xi z\zeta)d_I^*\dot z\ \omega_A(\pi x) \tag{5}$$

Wir möchten $\sum$ und $\int$ vertauschen. Dazu betrachten wir die Funktion $H(x,\xi,z) := \sum_{\zeta\in\mathbb{Q}^*} f(x\xi\zeta z)$. Die Funktion f habe kompakten Träger $C\subset D_A^*$, und $\dot z$ laufe in einem Kompaktun $E_0\subset I/\mathbb{Q}^*$, also, wenn $E\subset I$ ein partielles kompaktes Urbild (siehe Kapitel 4) von E_0 ist, $z\in E\mathbb{Q}^*$. Dann

$$H(x,\xi,z)\neq 0 \Rightarrow \text{es gibt } \zeta\in\mathbb{Q}^* \text{ mit } f(x\xi\zeta z)\neq 0 \Rightarrow \text{ es gibt } \zeta\in\mathbb{Q}^* \text{ mit } x\xi z\zeta\in C$$

$$\Rightarrow x\xi z\in C\mathbb{Q}^* \Rightarrow \xi\in x^{-1}CE^{-1}\mathbb{Q}^* \Rightarrow \gamma=\pi\xi\in\pi(x^{-1}CE^{-1})$$

Da die letzte Menge kompakt und $\gamma=\pi(\xi)$ in der diskreten Untergruppe $G_{\mathbb{Q}}$ liegt, ist $\sum_{\xi \bmod \mathbb{Q}^*} H(x,\xi,z)$ in jedem $\dot z$-Kompaktum eine endliche Summe, und wir können sie gliedweise integrieren. Dies rückwärts gelesen und in (5) eingesetzt ergibt für das gesamte Integral den Wert

$$\int_{G_A/G_{\mathbb{Q}}}\int_{I/\mathbb{Q}^*} \sum_{\gamma\in G_{\mathbb{Q}}}\sum_{\zeta\in\mathbb{Q}^*} f(x\xi\zeta z)d_I^*\dot z\ \ \omega_A(\pi x)\quad(\gamma=\pi\xi)$$

$$=\int_{G_A/G_{\mathbb{Q}}}\int_{I/\mathbb{Q}^*} \sum_{\xi\in D_{\mathbb{Q}}^*} f(x\xi z)d_I^*\dot z\ \ \omega_A(\pi x)$$

Integrieren wir in dem Diagramm links herum, so erhalten wir ein Integral über den homogenen Raum $D_A^*/D_{\mathbb{Q}}^*$, und das ergibt die Gleichung

$$\int_{D_A^*/D_{\mathbb{Q}}^*}\sum_{\xi\in D_{\mathbb{Q}}^*} f(x\xi)d_A^*(\dot x) = \int_{G_A/G_{\mathbb{Q}}}\int_{I/\mathbb{Q}^*}\sum_{\xi\in D_{\mathbb{Q}^*}} f(x\xi z)d_I^*(\dot z)\omega_A(\pi\dot x)$$

Wie in Kapitel 7 gesehen, läßt sich jede stetige Funktion mit kompaktem Träger auf $D_A^*/D_{\mathbb{Q}}^*$ als eine Summe $\sum_{\xi\in D_{\mathbb{Q}}^*} f(x\xi)$ schreiben, wobei f kompakten Träger in D_A^* hat. Daher gilt

$$\int_{D_A^*/D_{\mathbb{Q}}^*} f(x)d_A^*(\dot{x}) = \int_{G_A/G_{\mathbb{Q}}}\int_{I/\mathbb{Q}^*} f(xz)d_I^*(\dot{z})\omega_A(\pi x)$$

für jede stetige Fumktion mit kompaktem Träger in $D_A^*/D_{\mathbb{Q}}^*$. Hat die Funktion F einer positiven reellen Variablen kompakten Träger $\subset(0,\infty)$, so folgt aus Satz 21, daß $f(\dot{x}) := F(|Nx|)$ kompakten Träger in $D_A^*/D_{\mathbb{Q}}^*$ hat. Für jede solche Funktion F gilt also

$$\int_{D_A^*/D_{\mathbb{Q}}^*} F(|Nx|)d_A^*(\dot{x}) = \int_{G_A/G_{\mathbb{Q}}}\int_{I/\mathbb{Q}^*} F(|z|^2|Nx|)d_I^*z\ \omega_A$$

Wir werten beide Seiten aus:

Linke Seite: Wir benutzen wieder die Isomorphie

$$D_A^* \simeq \mathbb{R}_{>0}^* \times D_A^1 \ \text{ mit } d_A^*x = \frac{dt}{t}\times d_A^1x$$

Sie liefert für die linke Seite

$$\int_0^\infty \int_{D_A^1/D_{\mathbb{Q}}^*} F(t)d_A^1\dot{x}\ \frac{dt}{t} = vol(D_A^1/D_{\mathbb{Q}}^*)\cdot\int_0^\infty F(t)\ \frac{dt}{t}$$

Nach Satz 23 ist dies gleich

$$\int_0^\infty F(t)\frac{dt}{t}$$

Rechte Seite: $(0,\infty)\times\prod\mathfrak{o}_p^*$ ist ein Fundamentalbereich für I modulo $\mathbb{Q}^*$. Daher ist, weil $\prod_p\lambda_p\int_{\mathfrak{o}_p^*}\frac{dx}{|x|_p}=1$,

$$\int_{I/\mathbb{Q}^*} F(|z|^2|Nx|)d_I^*z = \int_0^\infty F(t^2|Nx|)\frac{dt}{t}$$

$$= \frac{1}{2}\int_0^\infty F(t\,|Nx|)\frac{dt}{t} \quad \text{weil } \frac{dt^2}{t^2}=2\frac{dt}{t}$$

$$= \frac{1}{2}\int_0^\infty F(t)\,\frac{dt}{t} \quad \text{weil } \frac{dt}{t} \text{ invariant}$$

Vergleicht man rechte und linke Seite, so sieht man

Satz 24.

$$\int_{G_A/G_{\mathbb{Q}}}\omega_A = 2$$

Bemerkung: Wir haben $\int_{G_A/G_{\mathbb{Q}}}\omega_A = 2$ bewiesen für anisotrope Formen vom Typ $<-a,-b,ab>$. Aber jede Form ist Vielfaches einer solchen:
$<a_1,a_2,a_3>=\frac{a_1a_2}{a_3}\ \cdot\ <\frac{a_3}{a_2},\frac{a_3}{a_1},\frac{a_3^2}{a_1a_2}>$.

18. Die Zetafunktion einer quadratischen Form

Die in diesem Kapitel ausgeführte Berechnung der Tamagawazahl der speziellen orthogonalen Gruppe ist den Abschnitten 4.4 und 4.5 von [W2] entnommen.
Wir denken uns die quadratische Form F auf Diagonalgestalt gebracht:

$$F(x) = \sum_{i=1}^{n} a_i x_i^2, \quad a_i \in \mathbb{Q},\ a_i \neq 0$$

Dann sei

$$V^* = \{x \in V \mid F(x) \neq 0\}, \quad \text{also}$$
$$V_A^* = \{x \in V_A \mid F(x) \in I\}$$
$$V_{\mathfrak{o}_p}^* = \{x \in V_{\mathfrak{o}_p} \mid |F(x)|_p = 1\}$$

$dx_1 \wedge ..... \wedge dx_n$ ist eine Differentialform höchsten Grades und $\neq 0$ auf V^*. Um daraus ein Tamagawa-Maß auf V_A^* abzuleiten, müssen wir zuerst berechnen

$$\int_{V_{\mathfrak{o}_p}^*} dx_1....dx_n = 1 - \int_{|F(x)|<1} dx_1.....dx_n$$

Die Anzahl der isotropen Vektoren mod p ist nach Kapitel 10, wenn alle $|a_i| = 1$ sind,

$$(1) \qquad = \begin{cases} p^{n-1} - 1 & \text{wenn } n \text{ ungerade} \\ (p^{\frac{n}{2}-1} + \eta)(p^{\frac{n}{2}} - \eta) & \text{wenn } n \text{ gerade} \end{cases}$$

wobei $p \neq 2$ und

$$\eta = (\frac{(-1)^{\frac{n}{2}} \det V}{p})$$

Beachte, daß in dem Integral über $\{|F(x)| < 1\}$ alle Vektoren x mit $F(x) \equiv 0 \bmod p$ mitzuzählen sind, also auch $x \equiv 0$, der bei den isotropen Vektoren nicht mitgezählt war. Dann folgt aus (1)

$$(2) \qquad \int_{V_{\mathfrak{o}_p}^*} dx_1....dx_n = \begin{cases} 1 - p^{-1} & \text{wenn } n \text{ ungerade} \\ (1 - p^{-1})(1 - \eta p^{-\frac{n}{2}}) & \text{wenn } n \text{ gerade} \end{cases}$$

Dies zeigt: $\lambda_p := (1 - p^{-1})^{-1}$ ist ein System von Konvergenzfaktoren. Wir bezeichnen $d'x$ das von der Differentialform $dx_1 \wedge ..... \wedge dx_n$ und den Konvergenzfaktoren λ_p abgeleitete Tamagawa-Maß.

Satz 25. *Für jede Standardfunktion Φ auf V_A und $n \geq 3$, Re $s > 0$ existiert das Integral*

$$\int_{V_A^*} |F(x)|^s \Phi(x)\ d'x$$

(Nach Definition von V_A^* ist $F(x)$ ein Idel , $|F(x)|^s$ ist also wohldefiniert)

Beweis: Nach Definition ist das Integral gleich

$$\lim_S \prod_{v \in S} \int_{V_v^*} |F(x)|_v^s \Phi_v(x) d'x_v \ \cdot \ \prod_{p \notin S} \int_{V_{\mathfrak{o}_p}^*} |F(x)|_p^s \Phi_p(x)\ d'x_p$$

Zu zeigen ist

1. Alle Integrale existieren
2. Das $\prod_{p\notin S}$ konvergiert
3. Der $\lim_S$ existiert

1. ist klar
2. Nach Definition ist $|F(x)|_p = 1$ auf $V^*_{\mathfrak{o}_p}$, und für genügend große S ist Φ_p die Indikatorfunktion von $V_{\mathfrak{o}_p}$. Daher sind im $\prod_{p\notin S}$ alle Integranden gleich 1, wenn S groß genug ist. Nach (2) konvergiert das Produkt absolut, wenn $n \geq 3$.
3. S_0 enthalte alle Primteiler von $2 \det F$ sowie ∞ und alle p, für die Φ_p nicht die Indikatorfunktion von $M_p := V_{\mathfrak{o}_p}$ ist. Für alle $p \notin S_0$ ist

$$\int_{V_p^*} |F(x)|^s \Phi_p(x) d'x_p = \int_{M_p} |F(x)|^s d'x_p$$

Wir setzen $x = p^\mu z$ mit primitivem $z \in M_p$. Die Menge der primitiven Vektoren von M_p sei M_p^*. Dann ist

$$\int_{M_p} |F(x)|^s d'x_p = \sum_{\mu=0}^{\infty} p^{-2\mu s} \int_{z\in M_p^*} |F(z)|^s p^{-\mu n} d'z_p$$

$$= \sum_{\mu=0}^{\infty} p^{-\mu(2s+n)} \int_{M_p^*} |F(z)|_p^s d'z_p$$

Das letzte Integral ist

$$\int_{M_p^*} |F(z)|^s d'z_p = \sum_{\nu=0}^{\infty} p^{-\nu s} \int_{|F(z)|=p^{-\nu}} d'z_p = \sum_{\nu=0}^{\infty} p^{-\nu s} [\int_{|F(z)|\leq p^{-\nu}} - \int_{|F(z)|\leq p^{-\nu-1}}]$$

Sei N_ν die Anzahl der mod p^ν verschiedenen $z \in M_p^*$ mit $F(z) \equiv 0 \bmod p^\nu$.

Behauptung: Für $\nu \geq 1$ ist $N_{\nu+1} = p^{n-1} N_\nu$.

Beweis: Sei $\nu \geq 1$ und $F(z) \equiv 0 \bmod p^\nu$. Dann ist $F(z + p^\nu u) \equiv F(z) + 2p^\nu (z,u) \bmod p^{\nu+1}$. Da z primitiv, gibt es zu jedem $\beta \in \mathfrak{o}_p$ genau p^{n-1} mod p verschiedene u mit $(z,u) \equiv \beta \bmod p$. Da $p \neq 2$, gibt es also zu $z \in M_p^*$ mit $F(z) \equiv 0 \bmod p^\nu$ genau p^{n-1} mod $p^{\nu+1}$ verschiedene $z + p^\nu u$ mit $F(z + p^\nu u) \equiv 0 \bmod p^{\nu+1}$. Daher

$$N_{\nu+1} = p^{n-1} N_\nu \text{ und schrittweise } N_\nu = p^{(n-1)(\nu-1)} N_1$$

Bei den Summanden mit $\nu \geq 1$ erhält man

$$p^{-\nu s}[N_\nu p^{-\nu n} - N_{\nu+1} p^{-(\nu+1)n}] = p^{-\nu s}[p^{(n-1)(\nu-1)-\nu n} - p^{(n-1)\nu-(\nu+1)n}] N_1$$

$$= (p-1) p^{-\nu(s+1)} \cdot p^{-n} N_1$$

Für $\nu = 0$ ist

$$\int_{M_p^*} dz_p - \int_{z\in M_p^*, |F(z)|<1} dz_p = 1 - p^{-n} - N_1 p^{-n}$$

Summiert man über ν, so erhält man

$$1 - p^{-n} - N_1 p^{-n} + N_1 p^{-n}(p-1)\frac{p^{-s-1}}{1-p^{-s-1}} = 1 - p^{-n} + N_1 p^{-n}\frac{p^{-s}-1}{1-p^{-s-1}}$$

N_1 ist die Anzahl der isotropen Vektoren mod p. Setzt man die dafür in (1) angegebenen Werte ein, berücksichtigt die Konvergenzfaktoren λ_p und multipliziert noch mit der Summe

$$\sum_{\mu \geq 0} p^{-\mu(2s+n)} = \frac{1}{1-p^{-2s-n}}$$

so erhält man: Für fast alle p ist

$$\int_{V_p^*} |F(x)|^s \Phi_p(x) d'x_p = \begin{cases} \frac{1-p^{-n-s}}{(1-p^{-s-1})(1-p^{-2s-n})} & \text{wenn } n \text{ ungerade} \\ \frac{1-\eta p^{-\frac{n}{2}}}{(1-p^{-s-1})(1-\eta p^{-s-\frac{n}{2}})} & \text{wenn } n \text{ gerade} \end{cases}$$

Das beweist Satz 25, denn das Produkt $\prod_p$ dieser Faktoren konvergiert absolut für $Re\ s > 0$ und $n \geq 3$.

Definition:

$$Z(s, \Phi) = \int_{V_A^*} |F(x)|^s \Phi(x) d'x$$

Die Formeln aus dem Beweis von Satz 25 erlauben es, das Residuum von $Z(s, \Phi)$ an der Stelle $s = 0$ auszurechnen: Ist S so groß, daß $p \dagger 2 \det F$ und Φ_p die Indikatorfunktion von M_p ist für $p \notin S$, dann ist für ungerades n

$$Z(s, \Phi) = \prod_{v \in S} \int_{V_v^*} |F(x)|_v^s \Phi_v(x) d'x_v \ \cdot \ \prod_{p \notin S} \frac{1-p^{-s-n}}{(1-p^{-s-1})(1-p^{-2s-n})} =$$

$$Z_\infty \cdot \prod_{p \in S} \frac{\int_{V_p^*} |F(x)|_p^s \Phi_p(x) d'x_p}{(1-p^{-s-n})(1-p^{-s-1})^{-1}(1-p^{-2s-n})^{-1}} \ \cdot \ \frac{\zeta(s+1)\zeta(2s+n)}{\zeta(s+n)}$$

mit $Z_\infty = \int_{V_\infty} |F(x)|_\infty^s \Phi_\infty(x) d'x_\infty$ Das erste Produkt hat nur endlich viele Fakoren und ist damit eine stetige Funktion von s in $Re\, s \geq 0$. Sein Grenzwert für $s \to 0$ ist eingedenk von $d'x_p = (1-p^{-1})^{-1} dx_p$ gleich $\prod_{p \in S} \int_{V_p} \Phi_p(x) dx_p$ (die Menge $V_p \setminus V_p^*$ trägt zum Integral nichts bei). Dadurch wird, weil die Riemannsche Zetafunktion an der Stelle 1 das Residuum 1 hat,

$$\lim_{s \to 0} sZ(s, \Phi) = \prod_{v \in S} \int_{V_v} \Phi_v(x) dx_v$$

Für $p \notin S$ ist nun aber $\Phi_p = \mathbf{1}_{M_p}$ und damit $\int_{V_p} \Phi_p(x) dx_p = 1$. Diese Faktoren können wir also dem Produkt einfach hinzufügen und erhalten

$$\lim_{s \to 0} sZ(s, \Phi) = \int_{V_A} \Phi(x) dx_A = \hat{\Phi}(0) \tag{3}$$

Für gerades n stellen wir dieselbe Überlegung an und erhalten in dem Produkt $\prod_{p\notin S}$ die Eulerfaktoren von $\frac{\zeta(s+1)L(s+\frac{n}{2},\eta)}{L(\frac{n}{2},\eta)}$, wobei $L(s,\eta)$ die L-Reihe zum Dirichletcharakter $\eta = (\frac{(-1)^{\frac{n}{2}}\det F}{p})$ ist. Man findet wieder die Formel (3) für das Residuum.

Verfeinerung dieser Zetafunktion: Sei S eine endliche Menge von Primstellen, welche 2 und ∞ enthält. Man setzt

$$H_S = I^2 \cdot \prod_{p\notin S} \mathfrak{o}_p^* = \{x \in I \mid x_v \in \mathbb{Q}_v^{*2} \text{ für } v \in S \text{ und } v_p(x_p) \text{ gerade für } p \notin S\}$$

H_S ist eine Untergruppe von I.

Lemma 1. $(I : H_S\mathbb{Q}^*) = 2^{|S|}$

Beweis: Wir erinnern daran, daß I eine direkte Zerlegung besitzt:

$$I = \mathbb{Q}^* \cdot (\mathbb{R}^*_{>0} \times \prod_{p\in S(p\neq\infty)} \mathfrak{o}_p^* \times \prod_{p\notin S} \mathfrak{o}_p^*)$$

($\mathbb{Q}^*$ und die Klammer treffen sich nur in 1). Und darin ist

$$H_S\mathbb{Q}^* = \mathbb{Q}^* \cdot (\mathbb{R}^{*2} \times \prod_{p\in S(p\neq\infty)} \mathfrak{o}_p^{*2} \times \prod_{p\notin S} \mathfrak{o}_p^*)$$

Das zeigt

$$I/H_S\mathbb{Q}^* \simeq \prod_{p\in S(p\neq\infty)} \mathfrak{o}_p^*/\mathfrak{o}_p^{*2}$$

Da die Quadrate in der Einheitengruppe eine Untergruppe vom Index 2 bilden, falls $p \neq 2$, und vom Index 4, wenn $p = 2$, und da $2 \in S$ und $\infty \in S$, hat diese Gruppe gerade die Ordnung $2^{|S|}$.

Lemma 2. *Sei λ ein Charakter von I, der auf $H_S\mathbb{Q}^*$ gleich 1 ist. Dann gehört zu λ ein Dirichlet Charakter χ auf $\mathbb{Z}$. Wenn $\lambda \neq 1$, dann ist auch $\chi \neq 1$.*

Beweis: Sei ι_v die Einbettung

$$x \mapsto (1, ..., 1, x, 1, ...)$$

von $\mathbb{Q}_v^*$ in I und $\lambda_v = \lambda \circ \iota_v$. Für ein festes Idel $x = (x_v)_v$ ist dann $\lambda_p(x_p) = 1$ für fast alle p und $\lambda(x) = \prod_v \lambda_v(x_v)$.
Für $p \notin S$ ist $\lambda_p(\mathfrak{o}_p^*) = 1$, das heißt, für $x \in \mathbb{Q}_p^*$ hängt $\lambda_p(x)$ nur von $|x|_p$ ab:

$$\lambda_p(x) = |x|_p^{it_p}$$

Nebenbei bemerkt sind alle diese Werte gleich ± 1, weil $\lambda(I^2) = 1$. Wir setzen $p^{it_p} = \epsilon_p$. Wenn $\lambda_\infty = 1$, dann setzen wir

$$m = m_0 = \begin{cases} \prod_{p\in S} p & \text{wenn } \lambda_2(\mathfrak{o}_2^*) = 1 \\ 4\prod_{p\in S} p & \text{wenn } \lambda_2(\mathfrak{o}_2^*) \neq 1 \end{cases}$$

Wenn $\lambda_\infty \neq 1$, dann setzen wir

$$m = \infty \cdot m_0$$

Nach Konvention bedeutet dann für $a, b \in \mathbb{Z}$

$$ggT(a, m) = 1, \text{ daß } ggT(a, m_0) = 1 \text{ und } a > 0 \text{ wenn } m = \infty \cdot m_0$$

und

$$a \equiv b \bmod m, \text{ daß } a \equiv b \bmod m_0 \text{ und } ab > 0 \text{ wenn } m = \infty \cdot m_0$$

Man definiert den Charakter χ für zu m teilerfremde $a \in \mathbb{Z}$ durch

$$\chi(a) = \prod_{v \in S} \lambda_v(a)$$

Dann gilt

1. Für Primzahlen $p \notin S$ (das heißt $p \dagger m$)

$$\chi(p) = \prod_{v \in S} \lambda_v(p) = \lambda(p) \cdot \lambda_p(p)^{-1} = \epsilon_p$$

weil $\lambda(\mathbb{Q}^*) = 1$ und $\lambda_q(p) = 1$ für $q \notin S,\ q \neq p$.

2. $\chi(ab) = \chi(a)\chi(b)$, weil dasselbe für λ und alle λ_v gilt.

3. Seien a, b teilerfremd zu m und $a \equiv b \bmod m$. Wenn $\infty | m$, dann bedeutet das $ab > 0$, also $\lambda_\infty(a) = \lambda_\infty(b)$. Sei r eine Primzahl in S. Aus $a \equiv b \bmod r$ (bzw. mod $4r$, wenn $r = 2$) folgt, daß a und b zur selben Quadratklasse in $\mathfrak{o}_r^*$ gehören. Dann ist $\lambda_r(a) = \lambda_r(b)$. Das zeigt

$$a \equiv b \bmod m \Rightarrow \chi(a) = \chi(b)$$

Damit ist bewiesen, daß χ ein Dirichlet Charakter mod m ist. (m ist nicht notwendig der kleinste Erklärungsmodul, aber das schadet nicht.)

Nun betrachten wir zu jedem Charakter λ von I mit $\lambda(H_S\mathbb{Q}^*) = 1$

$$Z(s, \Phi, \lambda) := \int_{V_A^*} |F(x)|^s \lambda(x) \Phi(x) d'x$$

(Das Integral existiert (für $Re\, s > 0$); man hat ja nur die integrierbare Funktion $|F(x)|^s \Phi(x)$ mit einer stetigen Funktion vom Betrag 1 multipliziert). Die lokalen Faktoren für $p \notin S$ sind

$$Z_p(s, \Phi, \lambda) = \int_{V_p^*} |F(x)|_p^s \lambda_p(F(x)) \Phi_p(x) d'x_p = \int_{V_p^*} |F(x)|^{s+it_p} \Phi_p(x) d'x_p$$

Wir brauchen in den alten Formeln für die lokalen Integrale nur s durch $s + it_p$ zu ersetzen und erhalten für $p \notin S$ und ungerade n

$$Z_p(s, \Phi, \lambda) = \frac{1 - p^{-n-s-it_p}}{(1 - p^{-s-it_p-1})(1 - p^{-2(s+it_p)-n})} = \frac{1 - \epsilon_p p^{-n-s}}{(1 - \epsilon_p p^{-s-1})(1 - p^{-2s-n})}$$

Dies sind die Eulerfaktoren zu

$$\frac{L(s+1,\chi)\zeta(2s+n)}{L(s+n,\chi)}$$

Für gerades n erhält man unter Benutzung der alten Formeln

$$Z_p(s,\Phi,\lambda) = \frac{1-\eta p^{-\frac{n}{2}}}{(1-\epsilon_p p^{-s-1})(1-\epsilon_p p^{-s-\frac{n}{2}})}$$

Das sind die Eulerfaktoren von

$$\frac{L(s+1,\chi)L(s+\frac{n}{2},\chi)}{L(\frac{n}{2},\eta)}$$

Da die L-Funktionen zu Charakteren $\neq 1$ an der Stelle 1 holomorph sind, liefern die $Z(s,\Phi,\lambda)$ mit $\lambda \neq 1$ keinen Beitrag zum Residuum an der Stelle 0, und daher ist, wenn man über alle Charaktere λ summiert, die auf $H_S\mathbb{Q}^*$ gleich 1 sind,

$$res_{s=0} \sum_\lambda Z(s,\Phi,\lambda) = \hat{\Phi}(0)$$

Nach den bekannten Charakterrelationen und der Berechnung des Index $(I : H_S\mathbb{Q}^*)$ in Lemma 1 ist

$$\sum_\lambda \lambda(x) = \begin{cases} 2^{|S|} & \text{wenn } x \in H_S\mathbb{Q}^* \\ 0 & \text{sonst} \end{cases}$$

Also ist

$$\sum_\lambda Z(s,\Phi,\lambda) = 2^{|S|} \int_{F(x)\in H_S\mathbb{Q}^*} |F(x)|^s \Phi(x) d'x$$

$H_S\mathbb{Q}^*$ ist die Vereinigung aller $H_S\rho$ mit $\rho \in \mathbb{Q}^*$, und weil $H_S \cap \mathbb{Q}^* = \mathbb{Q}^{*2}$, erhält man eine disjunkte Vereinigung, wenn man $\rho \bmod \mathbb{Q}^{*2}$ laufen läßt, und

$$\int_{F(x)\in H_S\mathbb{Q}^*} = \sum_{\rho\in\mathbb{Q}^*/\mathbb{Q}^{*2}} \int_{F(x)\in H_S\rho}$$

.

Das Ergebnis ist

Satz 26. *Die Funktion*

$$Z_S(s) = \sum_{\rho\in\mathbb{Q}^*/\mathbb{Q}^{*2}} \int_{F(x)\in H_S\rho} |F(x)|^s \Phi(x) d'x$$

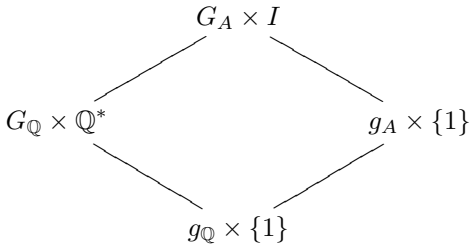
ist holomorph für $Re\, s > 0$ *und hat an der Stelle* $s = 0$ *das Residuum* $2^{-|S|}\hat{\Phi}(0)$.

Jetzt wird die Gruppe G_A ins Spiel gebracht: Die Gruppe $G \times GL(1)$ operiert auf V vermöge $x \mapsto Xxt$, $(X \in G, t \in GL(1))$. Wir sahen bereits, daß $\{1\}$ Konvergenzfaktoren für G_A sind, und $\{\lambda_\infty = 1,\ \lambda_p = (1-\frac{1}{p})^{-1}\}$ für die Idelgruppe I. Wir

bezeichnen mit ω_A das Tamagawa-Maß von G_A und setzen $\prod_v \lambda_v(\frac{dt}{t})_v = d^*t$. Dann ist $\omega_A d^*t$ ein rechts- und linksinvariantes Maß auf $G_A \times I$. Sei $e \in V_{\mathbb{Q}}$ fest und $F(e) = \rho \neq 0$. Der Stabilisator g von e in G ist die spezielle orthogonale Gruppe von $e^{\perp}$, sein Tamagawa-Maß $\bar{\omega}_A$ ist ebenfalls rechts und links invariant. Deshalb können wir wie in Kapitel 7 auf dem homogenen Raum G_A/g_A integrieren. Dieser ist vermöge $x \leftrightarrow Xe$ die Sphäre $\Sigma_A = \{x \in V_A \mid F(x) = \rho\}$ (siehe Kapitel 4). Auf der Sphäre Σ ist nach Lemma 1, Seite 121 für alle i, j

$$(-1)^i \frac{dx_1 \wedge .... \not{i} ... \wedge dx_n}{a_i x_i} = (-1)^j \frac{dx_1 \wedge .... \not{j} .... \wedge dx_n}{a_j x_j} =: \psi$$

eine G-invariante Differentialform, und die Sphäre hat Konvergenzfaktoren $\{1\}$. Sei ψ_A das davon abgeleitete Maß auf Σ_A. Die Differentialform ψ ist bis auf einen rationalen Faktor bestimmt, und daher ist wegen der Produktformel $\omega_A = \bar{\omega}_A \psi_A$. In dem Diagramm



integrieren wir einmal links herum und einmal rechts herum.

Rechts:

$$\int_{G_A \times I/g_{\mathbb{Q}} \times \{1\}} |t|^{2s+n} \Phi(Xet) \omega_A(X) d^*t = \int_{\Sigma_A \times I} |t|^{2s+n} \int_{g_A/g_{\mathbb{Q}}} \Phi(XYet) \bar{\omega}_A(Y) \psi_A(Xe) d^*t$$

$\Phi(XYet) = \Phi(Xet)$ hängt von $Y \in g_A$ gar nicht ab, und nach Induktionsannahme (die wir ab Dimension 3 benutzen können, wir müssen also in unserer Rechnung $n \geq 4$ annehmen) ist $\int_{g_A/g_{\mathbb{Q}}} \bar{\omega}_A = 2$. Also erhält man

$$2 \cdot \int_{\Sigma_A \times I} |t|^{2s+n} \Phi(xt) \psi_A(x) d^*t$$

Links:
Das gesamte Integral ist

$$\int_{G_A/G_{\mathbb{Q}} \times I/\mathbb{Q}^*} \sum_{\sigma \in G_{\mathbb{Q}}, \sigma \bmod g_{\mathbb{Q}}, \tau \in \mathbb{Q}^*} |t\tau|^{2s+n} \Phi(X\sigma et\tau) \omega_A(X) d^*t$$

Wegen der Produktformel ist $|\tau| = 1$. Läuft nun σ durch $G_{\mathbb{Q}}$ modulo $g_{\mathbb{Q}}$ und τ durch $\mathbb{Q}^*$, so läuft $\sigma e \tau$ zweimal durch die Vektoren $\xi \in V_{\mathbb{Q}}$ mit $F(\xi) \in \mathbb{Q}^{*2}\rho$ (für jedes ξ mit $F(\xi) \neq 0$ gibt es $\sigma \in G_{\mathbb{Q}}$ mit $\sigma\xi = -\xi \in \mathbb{Q}^*\xi$) . Daher ist die innere Summe

$$= 2 \sum_{\xi \in V_{\mathbb{Q}}, F(\xi) \in \mathbb{Q}^{*2}\rho} \Phi(X\xi t)$$

Durch Vergleich der beiden Integrationswege erhalten wir

$$(4)\quad \int_{G_A/G_{\mathbb{Q}}\times I/\mathbb{Q}^*} |t|^{2s+n} \sum_{\xi\in V_{\mathbb{Q}}, F(\xi)\in\mathbb{Q}^{*2}\rho} \Phi(X\xi t)\omega_A(X)d^*t = \int_{\Sigma_A\times I} |t|^{2s+n}\Phi(xt)\psi_A(x)d^*t$$

Im nächsten Abschnitt berechnen wir die lokalen Faktoren des rechten Integrals, was gleichzeitig die Existenz der obigen Integrale beweist.

Die lokalen Faktoren sind die Integrale

$$\int_{\Sigma_p\times\mathbb{Q}_p^*} |t|_p^{2s+n}\Phi_p(tx)\psi_p(x)d^*t_p$$

Wir rechnen sie aus für die p, die nicht in $2\det F$ aufgehen und für die Φ_p die Indikatorfunktion von M_p ist:

$(x,t)\mapsto(tx,t)$ ist eine Bijektion von $\Sigma_p\times\mathbb{Q}_p^* = \{(x,t)\mid F(x)=\rho,\ t\in\mathbb{Q}_p^*\}$ auf $\{(y,t)\mid F(y)=t^2\rho,\ t\in\mathbb{Q}_p^*\}$. Dabei ist $\psi_p(y)d^*t_p = |t|_p^{n-2}\psi_p(x)d^*t_p$. Also ist das Integral $=: I_p =$

$$\int_{y\in M_p, t\in\mathbb{Q}_p^*, F(y)=\rho t^2} |t|_p^{2s+2}\psi_p(y)d^*t_p$$

Wir setzen $y=p^\lambda z$ mit primitivem z in M_p und $t=p^\mu r$ mit $|r|=1$. Dann ist $d^*t_p = d^*r_p$. Sei $\rho=p^\alpha u$ mit $|u|=1$.

$$F(y)=\rho t^2 \Longleftrightarrow F(z)=p^{-2\lambda}p^\alpha u p^{2\mu}r^2$$

Wegen $F(z)\in\mathfrak{o}_p$ ist $\alpha+2\mu-2\lambda\geq 0$, und es ist $\psi_p(y)=p^{-\lambda(n-2)}\psi_p(z)$. Damit spaltet sich des Integral I_p auf in die Summe

$$I_p = \sum_{0\leq 2\lambda\leq\alpha+2\mu} p^{-\mu(2s+2)}p^{-\lambda(n-2)}\int_{z\in M_p^*, F(z)=p^{\alpha+2\mu-2\lambda}ur^2}\psi_p(z)d^*r_p$$

In dem Integral über z und r kann man z durch $\frac{1}{r}z$ ersetzen, ohne daß sich $\psi_p(z)$ ändert. Danach hängt das Integral über z gar nicht mehr von r ab, und das Integral über r ist gleich 1. So wird schließlich

$$I_p = \sum_{0\leq 2\lambda\leq\alpha+2\mu} p^{-\mu(2s+2)}p^{-\lambda(n-2)}\int_{z\in M_p^*, F(z)=p^{\alpha+2\mu-2\lambda}u}\psi_p(z)$$

Das Integral ist $= p^{-(n-1)}$ mal Anzahl N der mod p verschiedenen $z\in M_p^*$ mit $F(z)\equiv p^{\alpha+2\mu-2\lambda}u \bmod p$, nämlich:

Für $c\in\mathfrak{o}_p$ gilt

$$\int_{z\in M_p^*, F(z)=c}\psi_p(z) = \sum_{b\in M_p^*,\ F(b)=c,\ b \bmod p}\ \int_{z\equiv b \bmod p, F(z)=c}\psi_p(z)$$

Für $b \in M_p^*$ ist mindestens eine Koordinate Einheit, etwa b_1. Für $z \equiv b \bmod p$ ist dann auch $|z_1|_p = 1$ und $\psi_p(z) = (dz_2....dz_n)_p$. Schreibt man $z = b + py$ mit $y \in M_p$, so ist

$$F(z) = c \Leftrightarrow 2p(b,y) + p^2 F(y) = 0 \Leftrightarrow 2a_1 b_1 y_1 + p a_1 y_1^2 = -2\sum_{i=2}^{n} a_i b_i y_i - p\sum_{i=2}^{n} a_i y_i^2 =: a_1 d$$

Diese Gleichung hat zu vorgegebenen $y_2, ..., y_n \in \mathfrak{o}_p$ genau eine Lösung $y_1 \in \mathfrak{o}_p$; denn für

$$f(y_1) := 2b_1 y_1 + p y_1^2 - d$$

gilt

$$f(\frac{d}{2b_1}) \equiv 0 \bmod p$$

und

$$f'(\frac{d}{2b_1}) \not\equiv 0 \bmod p$$

Nach Hensel gibt es eine Lösung $y_1 \equiv \frac{d}{2b_1}$, also in $\mathfrak{o}_p$. Die Summe der beiden Nullstellen von f ist $= -\frac{2b_1}{p} \notin \mathfrak{o}_p$, also ist die andere Nullstelle nicht in $\mathfrak{o}_p$. Daher kann man auf $\{z \equiv b \bmod p, F(z) = c\}$ die Koordinaten $y_2, ..., y_n$ als Parameter benutzen. Außerdem kann man jede Restklasse $b \bmod p$ mit $b \in M_p^*$ und $F(b) \equiv c \bmod p$ durch einen Vektor b mit $F(b) = c$ vertreten. Mit $(dz_2.....dz_n)_p = p^{-(n-1)}(dy_2.....dy_n)_p$ wird

$$\int_{z \in M_p^*, F(z) = p^{\alpha+2\mu-2\lambda}u} \psi_p(z) = \sum_{b \in M_p^*,\, b \bmod p,\, F(b) \equiv p^{\alpha+2\mu-2\lambda}u} p^{-(n-1)} = N \cdot p^{-(n-1)}$$

wie behauptet. Für diese Anzahl N müssen wir vier Fälle unterscheiden. Die angegebenen Werte stammen aus Kapitel 10, Seite 60.

1. $\alpha + 2\mu - 2\lambda = 0$ und n gerade.

$$N = p^{n-1} - \epsilon p^{\frac{n}{2}-1} \text{ mit } \epsilon = (\frac{(-1)^{\frac{n}{2}} \det F}{p})$$

2. $\alpha + 2\mu - 2\lambda = 0$ und n ungerade.

$$N = p^{n-1} + \epsilon' p^{\frac{n-1}{2}} \text{ mit } \epsilon' = (\frac{(-1)^{\frac{n-1}{2}} u \det F}{p})$$

3. $\alpha + 2\mu - 2\lambda > 0$ und n gerade

$$N_0 = (p^{\frac{n}{2}} - \epsilon)(p^{\frac{n}{2}-1} + \epsilon)$$

4. $\alpha + 2\mu - 2\lambda > 0$ und n ungerade

$$N_0 = p^{n-1} - 1$$

Wenn α ungerade ist, dann kommen in der Summe nur Summanden vom Typ 3 oder 4 vor. Die Summe ist dann

$$= \sum_{0 \le \lambda \le \frac{\alpha-1}{2}+\mu} p^{-\mu(2s+2)} p^{-\lambda(n-2)} = \frac{p^{(\alpha-1)(s+1)}}{(1-p^{-2s-2})(1-p^{-n-2s})}$$

Wir erhalten

$$(1-p^{-2s-2})(1-p^{-2s-n}) \cdot I_p = p^{(\alpha-1)(s+1)} \cdot (1-p^{-(n-1)}) \tag{5}$$

wenn α ungerade und n ungerade

$$(1-p^{-2s-2})(1-p^{-2s-n}) \cdot I_p = p^{(\alpha-1)(s+1)} \cdot (1-\epsilon p^{-\frac{n}{2}})(1+\epsilon p^{-(\frac{n}{2}-1)}) \tag{6}$$

wenn α ungerade und n gerade. Ist hingegen α gerade, so gibt es in der Summe den Anfangsterm mit $2\lambda = \alpha + 2\mu$. Die zugehörige Teilsumme ist

$$\sum_{0 \le 2\lambda = a+2\mu} p^{-\mu(2s+2)} p^{-\lambda(n-2)} = \frac{p^{\alpha(s+1)}}{1-p^{-2s-n}}$$

Die restliche Teilsumme ist

$$\sum_{0 \le 2\lambda < \alpha+2\mu} p^{-\mu(2s+2)} p^{-\lambda(n-2)} = \frac{p^{(\alpha-2)(s+1)}}{(1-p^{-2s-2})(1-p^{-2s-n})}$$

Multipliziert man die erste Summe mit N und die zweite mit N_0 und faßt alles zusammen, so erhält man

$$(1-p^{-2s-2})(1-p^{-2s-n}) \cdot I_p = p^{\alpha(s+1)}(1+\epsilon' p^{-\frac{n-1}{2}})(1-\epsilon' p^{-\frac{n-1}{2}-2s-2}) \tag{7}$$

wenn α gerade und n ungerade Wenn n gerade ist, macht man dasselbe und erhält

$$(1-p^{-2s-2})(1-p^{-2s-n}) \cdot I_p = p^{\alpha(s+1)}(1-\epsilon p^{-\frac{n}{2}})(1+\epsilon p^{-\frac{n}{2}-2s-1}) \tag{8}$$

wenn α gerade und n gerade

Diese Formeln zeigen zunächst, daß das Produkt über alle p für $Re\ s > 0$ konvergiert (wir haben $n \ge 4$). Damit existiert das rechte Integral in (4). Wir würden nun in Anbetracht von (4) gerne das Ganze noch über $\rho \in \mathbb{Q}^*/\mathbb{Q}^{*2}$ summieren. Um die Konvergenz dieser Summe zu beweisen, vergleichen wir sie gliedweise mit der als konvergent erkannten Summe in Satz 26. Diese war

$$\sum_{\rho \in \mathbb{Q}^*/\mathbb{Q}^{*2}} \int_{F(x) \in H_S \rho} |F(x)|^s \Phi(x) d'x \tag{A}$$

Und nun wollen wir die Konvergenz von

$$\sum_{\rho \in \mathbb{Q}^*/\mathbb{Q}^{*2}} \int_{\Sigma(\rho)_A \times I} |t|^{2s+n} \Phi(tx) \psi_A(x) d^*t \tag{B}$$

einsehen. Dabei ist $\Sigma(\rho)$ die Sphäre $F(x) = \rho$.

In den Integralen (B) rechnen wir die Differentialform um: Mit $y = tx$ ist

$$dy_1 \wedge .... \wedge dy_n = (x_1 dt + t dx_1) \wedge ..... \wedge (x_n dt + t dx_n) = t^{n-1} \sum_{i=1}^{n} x_i dx_1 \wedge ... \wedge dt ..... \wedge dx_n$$

(weil $dx_1 \wedge ..... \wedge dx_n = 0$ wegen $\sum a_i x_i^2 = const$)

$$= t^{n-1} dt \wedge \sum_{i=1}^{n} (-1)^{i-1} a_i x_i^2 \frac{dx_1 \wedge .... \not{i} ... \wedge dx_n}{a_i x_i} = \rho t^{n-1} dt \wedge \psi$$

Sodann schreiben wir die Integrale in (A) und (B) als unendliche Produkte (für genügend große S) hin:

$$(A) \qquad \prod_{v \in S} \int_{F(x) \in \rho \mathbb{Q}_v^{*2}} |F(x)|_v^s \Phi_v(x) d'x_v \cdot \prod_{p \notin S} \int_{x \in M_p, F(x) \in \rho \mathbb{Q}_p^{*2} \mathfrak{o}_p^*} |F(x)|_p^s d'x_p$$

Läßt man in den Integralen (B) das Paar (x, t) durch $\Sigma(\rho)_v \times \mathbb{Q}_v^*$ laufen, so läuft $y = tx$ genau zweimal durch die Menge $F(y) \in \rho \mathbb{Q}_v^{*2}$. Daher erhalten wir in (B), indem wir $\psi_A(x) d^*t$ durch $|\rho^{-1} t^{-n}| d'y$ ersetzen

$$(B) \ \prod_{v \in S} 2 \cdot \int_{F(y) \in \rho \mathbb{Q}_v^{*2}} |\rho|_v^{-s-1} |F(y)|_v^s \Phi_v(y) d'y_v \cdot \prod_{p \notin S} 2 \cdot \int_{y \in M_p, F(y) \in \rho \mathbb{Q}_p^{*2}} |\rho|_p^{-s-1} |F(y)|_p^s d'y_p$$

Die Faktoren $|\rho|_v$ in (B) lassen wir weg, weil ihr Produkt über alle v gleich 1 ist ($\rho \in \mathbb{Q}^*$). Danach unterscheiden sich die Faktoren für $v \in S$ in (A) und (B) um den Fakor 2. Teilt man (A) durch (B), so erhält man also $2^{-|S|}$ mal den Quotienten für $p \notin S$. Diese Quotienten sind

$$\{ \int_{x \in M_p, F(x) \in \rho \mathbb{Q}_p^{*2} \mathfrak{o}_p^*} |F(x)|_p^s d'x_p \} \cdot \{ 2 \int_{x \in M_p, F(x) \in \rho \mathbb{Q}_p^{*2}} |F(x)|_p^s d'x_p \}^{-1}$$

Für $p \notin S$ ist $\mathfrak{o}_p^*$ Vereinigung von zwei Quadratklassen (weil $2 \in S$). Ist δ eine Einheit in $\mathfrak{o}_p$, die nicht Quadrat ist, so ist der Zähler in diesem Ausdruck gleich der Summe der über $F(x) \in \rho \mathbb{Q}_p^{*2}$ und $F(x) \in \rho \delta \mathbb{Q}_p^{*2}$ erstreckten Integrale. Ist n gerade, so sind nach den Formeln (5) bis (8) diese beiden Integrale gleich, und der Beitrag der Stelle p zum Quotienten $\frac{A}{B}$ ist gleich 1. Ist jedoch n ungerade (und $\alpha = 0$, was für fast alle p der Fall ist), dann liefert p nach den Formeln (5) bis (8) zum Quotienten $\frac{A}{B}$ den Beitrag

$$\frac{(1 - \epsilon' p^{-\frac{n-1}{2}})(1 + \epsilon' p^{-\frac{n-1}{2} - 2s - 2}) + (1 + \epsilon' p^{-\frac{n-1}{2}})(1 - \epsilon' p^{-\frac{n-1}{2} - 2s - 2})}{2(1 + \epsilon' p^{-\frac{n-1}{2}})(1 - \epsilon' p^{-\frac{n-1}{2} - 2s - 2})}$$

$$= \frac{1 - p^{-n-1-2s}}{(1 + \epsilon' p^{-\frac{n-1}{2}})(1 - \epsilon' p^{-\frac{n-1}{2} - 2s - 2})} =: \Theta(p)^{-1}$$

mit $\epsilon' = \pm 1$. Für reelle $a > b > 0$ gilt $1 - p^{-b} < 1 - p^{-a} < 1 + p^{-a} < 1 + p^{-b}$, und indem man $\epsilon' = 1$ und $\epsilon' = -1$ getrennt diskutiert, findet man, daß für reelle $s > 0$ in beiden Fällen

$$1 - p^{-\frac{n-1}{2}} < \Theta(p) < 1 + p^{-\frac{n-1}{2}}$$

Man setzt $\lambda(S) = \prod_{p \notin S}(1-p^{-\frac{n-1}{2}})$ und $\mu(S) = \prod_{p \notin S}(1+p^{-\frac{n-1}{2}})$. Da $n \geq 4$ und hier aber ungerade, ist $\frac{n-1}{2} \geq 2$, und diese Produkte konvergieren. Aus $\frac{B}{A} = 2^{|S|}\prod_p \Theta(p)$ erhält man

$$0 < 2^{|S|}\lambda(S) \leq \frac{B}{A} \leq 2^{|S|}\mu(S)$$

Rufen wir die Abhängigkeit von ρ in Erinnerung: $A = A(\rho)$, $B = B(\rho)$. Für reelle $s > 0$ und alle $\rho \in \mathbb{Q}^*$ haben wir

$$0 < \lambda(S)2^{|S|}A(\rho) \leq B(\rho) \leq \mu(S)2^{|S|}A(\rho)$$

Aus der absoluten Konvergenz von $\sum_\rho A(\rho)$ folgt hiermit die absolute Konvergenz von $\sum_\rho B(\rho)$ für reelle $s > 0$ und damit in der Halbebene $Re\ s > 0$. Damit ist auch $\sum_\rho B(\rho)$ eine dort holomorphe Funktion. Da $\sum_\rho A(\rho)$ an der Stelle $s = 0$ das Residuum $2^{-|S|}\hat{\Phi}(0)$ hat, liegt das Residuum von $\sum_\rho B(\rho)$ zwischen $\lambda(S)\hat{\Phi}(0)$ und $\mu(S)\hat{\Phi}(0)$. Wenn man S groß genug nimmt, dann liegen $\lambda(S)$ und $\mu(S)$ beliebig nahe an 1. Es folgt

Satz 27.

$$\sum_{\rho \in \mathbb{Q}^*/\mathbb{Q}^{*2}} \int_{\Sigma(\rho)_A \times I} |t|^{2s+n}\Phi(xt)\psi_A(x)d^*t$$

und damit nach (4) die Summe

$$\sum_{\rho \in \mathbb{Q}^*/\mathbb{Q}^{*2}} \int_{G_A/G_\mathbb{Q} \times I/\mathbb{Q}^*} |t|^{2s+n} \sum_{F(\xi) \in \rho\mathbb{Q}^{*2}} \Phi(X\xi t)\omega_A(X)d^*t$$

ist eine holomorphe Funktion von s in $Re\ s > 0$, und ihr Residuum an der Stelle $s = 0$ ist $\hat{\Phi}(0)$.

In Satz 27 wollen wir Summe und Integral vertauschen: Durch Zerlegung in Positiv- und Negativteil können wir annehmen, daß $\Phi \geq 0$. Nach den obigen Betrachtungen existieren

$$H_\rho(X,t) = \sum_{\xi \in V_\mathbb{Q}, F(\xi) \in \rho\mathbb{Q}^{*2}} |t|^{2s+n}\Phi(X\xi t)$$

$$\int_{G_A/G_\mathbb{Q} \times I/\mathbb{Q}^*} H_\rho(X,t)\omega_A(X)d^*t =: J_\rho$$

und

$$\sum_{\rho \in \mathbb{Q}^*/\mathbb{Q}^{*2}} J_\rho$$

Aus den definierenden Eigenschaften der Standardfunktion Φ folgt, daß

$$K(X,t) := \sum_{\rho \in \mathbb{Q}^*/\mathbb{Q}^{*2}} H_\rho(X,t)$$

auf jedem Kompaktum $C \subset G_A/G_\mathbb{Q} \times I/\mathbb{Q}^*$ absolut und gleichmäßig konvergiert. Also ist

$$\int_C K(X,t)\omega_A(X)d^*t = \sum_\rho \int_C H_\rho(X,t) \leq \sum_\rho \int H_\rho = \sum_\rho J_\rho < \infty$$

Also existiert das Supremum über C der linken Seite, und dieses ist nach Definition das $\int K(X,t)$.

Nun vertauschen wir in Satz 27 Summe und Integral. Dann entsteht unter dem Integral die Summe

$$\sum_{\xi\in V_{\mathbb{Q}},\xi\neq 0}\Phi(X\xi t),\ \text{und wir erhalten}$$

Satz 28 .

$$\tilde{Z}(s,\Phi):=\int_{G_A/G_{\mathbb{Q}}\times I/\mathbb{Q}^*}|t|^{2s+n}\sum_{\xi\in V_{\mathbb{Q}},F(\xi)\neq 0}\Phi(X\xi t)\omega_A(X)d^*t$$

ist eine holomorphe Funktion von s *in* $Re\ s>0$, *und ihr Residuum an der Stelle* $s=0$ *ist* $\hat{\Phi}(0)$.

Analytische Fortsetzung: Für $t\in(0,\infty)$ setzt man

$$f^+(t)=\begin{cases}1 & \text{wenn } t>1\\ 0 & \text{wenn } t<1\\ \frac{1}{2} & \text{wenn } t=1\end{cases}$$

und $f^-(t)=f(\frac{1}{t})=1-f^+(t)$. Dann zerlegt man $\tilde{Z}(s,\Phi)=Z^+(s,\Phi)+Z^-(s,\Phi)$ mit

$$Z^+(s,\Phi)=\int_{G_A/G_{\mathbb{Q}}\times I/\mathbb{Q}^*}f^+(|t|)|t|^{2s+n}\sum_{F(\xi)\neq 0}\Phi(X\xi t)\ \omega_A(X)d^*t$$

und Z^- entsprechend mit f^- statt f^+. Das ursprüngliche Integral $\tilde{Z}$ war konvergent für $Re\ s>0$, also ist auch Z^+ für $Re\ s>0$ konvergent. Nun konvergiert aber das Integral Z^+ umso besser. je kleiner $Re\,s$ ist. Es liefert die holomorphe Fortsetzung von Z^+ auf die ganze s-Ebene.

Das Integral $Z^-(s,\Phi)$ formen wir um : Wir benutzen jetzt, daß F anisotrop ist. Dann ist

$$\sum_{F(\xi)\neq 0}\Phi(X\xi t)=-\Phi(0)+\sum_{\xi\in V_{\mathbb{Q}}}\Phi(X\xi t)$$

Auf die Summe wenden wir die Poisson'sche Summenformel an. Zur Identifizierung von V_A mit seiner Charaktergruppe benutzen wir die gegebene quadratische Form auf V, für $x,y\in V_A$ ist also

$$<x,y>=\chi((x,y))=\chi(x'Cy)$$

wenn C die Gram-Matrix der quadratischen Form F ist ($F(x)=x'Cx$). Für $X\in G$ ist dann
$<Xx,y>=<x,X^{-1}y>$, und die Fouriertransformierte von $\Psi(x):=\Phi(Xxt)$ ist

$$\hat{\Psi}(y)=\int_{V_A}\Phi(Xxt)<x,y>dx=|t|^{-n}\int_{V_A}\Phi(z)<X^{-1}zt^{-1},y>dz(\ \text{weil}\ \det X=1)$$

$$=|t|^{-n}\int_{V_A}\Phi(z)<z,Xyt^{-1}>dz=|t|^{-n}\hat{\Phi}(Xyt^{-1})$$

Dies setzen wir in Z^- ein:

$$Z^-(s,\Phi) =$$

$$\int_{G_A/G_{\mathbb{Q}}\times I/\mathbb{Q}^*} f^-(|t|)|t|^{2s+n}\{-\Phi(0)+|t|^{-n}\hat{\Phi}(0)+|t|^{-n}\sum_{\eta\neq 0}\hat{\Phi}(X\eta t^{-1})\}\,\omega_A(X)d^*t$$

Für den ersten Summanden finden wir

$$-\Phi(0)\int_{G_A/G_{\mathbb{Q}}}\omega_A\cdot\int_{I/\mathbb{Q}^*} f^-(|t|)|t|^{2s+n}d^*t$$

Nun ist $I/\mathbb{Q}^* \simeq (0,\infty)\times\prod_p \mathfrak{o}_p^*$, und $\int_{\mathfrak{o}_p^*} d^*t_p = 1$. Dadurch wird

$$\int_{I/\mathbb{Q}^*} f^-(|t|)|t|^{2s+n}d^*t = \int_0^1 t^{2s+n}\frac{dt}{t} = \frac{1}{2s+n}$$

analog für den zweiten Summanden mit $2s$ statt $2s+n$.

$\int_{G_A/G_{\mathbb{Q}}}\omega_A$ ist die Tamagawa-Zahl $\tau(G)$. So wird

$$Z^-(s,\Phi) = \tau(G)\{-\frac{\Phi(0)}{2s+n}+\frac{\hat{\Phi}(0)}{2s}\}+\int_{G_A/G_{\mathbb{Q}}\times I/\mathbb{Q}^*} f^-(|t|)|t|^{2s}\sum_{\eta\neq 0}\hat{\Phi}(X\eta t^{-1})\omega_A(X)d^*t$$

Das Integral wird durch die Substitution $t\mapsto\frac{1}{t}$, bei der d^*t invariant bleibt, zu

$$\int_{G_A/G_{\mathbb{Q}}\times I/\mathbb{Q}^*} f^+(|t|)|t|^{-2s}\sum_{\eta\neq 0}\hat{\Phi}(X\eta t)\omega_A(X)d^*t$$

Der letzte Summand ist der Plusteil der Zetafunktion Z zur Standardfunktion $\hat{\Phi}$ an der Stelle $-s-\frac{n}{2}$. Wie gesehen, ist dies eine in der ganzen s-Ebene holomorphe Funktion von s. Ergebnis:

$$\tilde{Z}(s,\Phi) = Z^+(s,\Phi)+Z^+(-s-\frac{n}{2},\hat{\Phi})+\tau(G)[-\frac{\Phi(0)}{2s+n}+\frac{\hat{\Phi}(0)}{2s}]$$

Mit Hilfe von Satz 28 lesen wir hieraus ab

Satz 29. *Die Tamagawa-Zahl der speziellen orthogonalen Gruppe einer quadratischen Form in $n\geq 3$ Variablen über $\mathbb{Q}$ ist gleich 2.*

Wir haben den Satz nur für anisotrope Formen bewiesen. Will man ihn allgemein beweisen, so muß man außerdem die Sphäre vom Radius 0 berücksichtigen. Im Diagramm (D) muß man dafür statt e auch isotrope Vektoren zulassen. Deren Stabilisator ist aber nicht eine orthogonale Gruppe in einer Dimension weniger, sondern das semidirekte Produkt aus einem $(n-2)$-dimensionalen Vektorraum und einer orthogonalen Gruppe in zwei Dimensionen weniger. Deshalb braucht man für den Induktionsschluß die Verankerung in Dimension 3 und 4 (und zusätzliche Betrachtungen für das semidirekte Produkt)

19. Darstellung von Zahlen durch Formen

In Siegels Arbeit aus dem Jahre 1935 werden Darstellungen von Formen durch Formen betrachtet, das heißt es werden die $X = X_{n,m} \bmod p^k$ gezählt, für die $X'SX \equiv T \bmod p^k$ mit gegebenen $S = S_{n,n}$ und $T = T_{m,m}$. Bei der Herstellung des Zusammenhanges mit Tamagawa-Zahlen beschränken wir uns auf den Fall $m = 1$, das heißt die Darstellung von Zahlen durch Formen, das ist interessant und schwierig genug. Und wir betrachten (wie Siegel in der ersten Arbeit) positiv definite Formen.

Sei V ein n-dimensionaler Vektorraum über $\mathbb{Q}$ mit einer positiv definiten quadratischen Form $(\ ,\ )$, $n \geq 4$ und $t > 0$ eine ganze Zahl. M sei ein Gitter in V, und es wird wie immer angenommen, daß die Form auf M nur ganzzahlige Werte annimmt. Wir betrachten Paare (x, M) wo $x \in M$ und $(x, x) = t$ ist. Wir übernehmen die Bezeichnungen der früheren Kapitel: $G, G_{\mathbb{Q}}, G_A, G_A(M)$ usw.

Definition: $(x, M) \sim (y, N)$ wenn es $\Phi \in G_A$ gibt mit $\Phi x = y$ und $\Phi M = N$. Für festes (a, M) heißt $\{(x, N) \sim (a, M)\}$ das Geschlecht von (a, M).

Definition: $(x, M) \approx (y, N)$ wenn es $\sigma \in G_{\mathbb{Q}}$ gibt mit $\sigma x = y$ und $\sigma M = N$. Für festes (a, M) heißt $\{(x, N) \approx (a, M)\}$ die Klasse von (a, M).

Unserem früheren Sprachgebrauch entsprechend müßten wir eigentlich von "engerer Klasse" reden, aber wir betrachten im Folgenden immer nur die Gruppe G und schenken uns in diesem Kapitel das "enger".

Wenn $a, x \in V_{\mathbb{Q}}$ und $\Phi \in G_A$ und $\Phi a = x$, dann gibt es, da $n \geq 3$, ein $\sigma \in G_{\mathbb{Q}}$ mit $x = \sigma a$, und $\sigma^{-1}\Phi$ liegt im Stabilisator $Stab(a)_A$. Die $(x, N) \sim (a, M)$ werden also gegeben in der Form $(\Phi a, \Phi M)$ mit $\Phi \in G_{\mathbb{Q}} Stab(a)_A$.

Lemma 1. *Die Klassen im Geschlecht von (a, M) entsprechen umkehrbar eindeutig den Doppelnebenklassen*

$$Stab(a)_{\mathbb{Q}}\, \phi\, [Stab(a)_A \cap G_A(M)] \subset Stab(a)_A$$

Beweis: Alle $(x, N) \sim (a, M)$ sind von der Gestalt $(\sigma\phi a, \sigma\phi M) = (\sigma a, \sigma\phi M)$ mit $\sigma \in G_{\mathbb{Q}}$ und $\phi \in Stab(a)_A$, und die Klasse von $(\sigma a, \sigma\phi M)$ ist dieselbe wie die von $(a, \phi M)$, also durch ϕ bestimmt. Dabei ist

$$(a, \phi M) \approx (a, \psi M) \Leftrightarrow \text{ es gibt } \sigma \in G_{\mathbb{Q}} \text{ mit } a = \sigma a,\ \psi M = \sigma\phi M \Leftrightarrow$$

$$\phi \in Stab(a)_{\mathbb{Q}} \psi G_A(M) \Leftrightarrow \phi \in Stab(a)_{\mathbb{Q}}\, \psi\, [G_A(M) \cap Stab(a)_A]$$

Lemma 2. *Sei (a, M) fest und ebenso M^*. Die Anzahl der Paare $(x, M^*) \approx (a, M)$ ist*

$$= \begin{cases} 0 & \text{wenn } M^* \not\simeq M \\ (G(M) : [G(M) \cap Stab(a)]) & \text{wenn } M^* \simeq M \end{cases}$$

Beweis: Die erste Zeile ist klar. Zur zweiten: Wenn $M^* = \sigma_0 M$, dann sind die $(x, M^*) \approx (a, M)$ genau alle $(\sigma_0\rho a, \sigma_0\rho M)$ mit $\rho \in G(M)$, und $(\sigma_0\rho_1 a, \sigma_0\rho_1 M) = (\sigma_0\rho_2 a, \sigma_0\rho_2 M) \Leftrightarrow \rho_1^{-1}\rho_2 \in G(M) \cap Stab(a)$. Das beweist die zweite Zeile.

Da $Stab(a)_{\mathbb{Q}} \backslash Stab(a)_A$ kompakt ist (Satz 3, Kapitel 4) und $G_A(M)$ offen (in G_A) ist, gibt es in Lemma 1 nur endlich viele Doppelnebenklassen. Sie mögen vertreten sein durch $\psi_1, ..., \psi_N$. Es sei $A(a, M, M^*)$ die Anzahl der $(x, M^*) \sim (a, M)$. Aus Lemma 1 und 2 folgt

$$A(a, M, M^*) = \sum_{j=1}^{N} \{Anzahl\ der\ (x, M^*) \approx (a, \psi_j M)\}$$

$$= \sum_{j=1,\ \psi_j M \simeq M^*}^{N} (G(\psi_j M) : [Stab(a) \cap G(\psi_j M)])$$

Es kann natürlich nur dann $(x, M^*) \sim (a, M)$ geben, wenn M^* im Geschlecht von M liegt. Wenn $M_1, ..., M_h$ Vertreter für die Klassen im Geschlecht von M sind (hier ist h das h^+ aus Kapitel 13), dann muß also M^* zu einem der M_i isomorph sein, damit überhaupt $A(a, M, M^*) \neq 0$ ist. Wir benutzen die Formel für M_k statt M^*:

$$A(a, M, M_k) = \sum_{j=1,\ \psi_j M \simeq M_k}^{N} (G(\psi_j M) : [Stab(a) \cap G(\psi_j M)])$$

$$= \sum_{j=1, \psi_j M \simeq M_k}^{N} \frac{|G(M_k)|}{|Stab(a) \cap G(\psi_j M)|}$$

Summieren wir dies über k, so erhalten wir

$$\sum_{k=1}^{h} \frac{A(a, M, M_k)}{|G(M_k)|} = \sum_{j=1}^{N} \frac{1}{|Stab(a) \cap G(\psi_j M)|} \tag{1}$$

denn jedes $\psi_j M$ ist zu genau einem M_k isomorph.

Aus der Doppelnebenklassenzerlegung

$$Stab(a)_A = \cup_{j=1}^{N} Stab(a)_{\mathbb{Q}}\ \psi_j\ [Stab(a)_A \cap G_A(M)]$$

folgt

$$vol(Stab(a)_{\mathbb{Q}} \backslash Stab(a)_A) = \sum_{j=1}^{N} vol(Stab(a)_{\mathbb{Q}} \backslash Stab(a)_{\mathbb{Q}} \psi_j [Stab(a)_A \cap G_A(M)])$$

$$= \sum_{j=1}^{N} vol(Stab(a)_{\mathbb{Q}} \backslash Stab(a)_{\mathbb{Q}} [Stab(a)_A \cap G_A(\psi_j M)])$$

weil vol rechtsinvariant und $\psi_j a = a$

$$= \sum_{j=1}^{N} vol([Stab(a)_{\mathbb{Q}} \cap G(\psi_j M)] \backslash [Stab(a)_A \cap G_A(\psi_j M)]$$

(vergleiche den Homeomorphiesatz in Kapitel 7)

$$= \sum_{j=1}^{N} \frac{1}{|Stab(a)_{\mathbb{Q}} \cap G(\psi_j M)|} \; vol(Stab(a)_A \cap G_A(\psi_j M))$$

$$= vol(Stab(a)_A \cap G_A(M)) \sum_{j=1}^{N} \frac{1}{|Stab(a)_{\mathbb{Q}} \cap G(\psi_j M)|}$$

weil $G_A(\psi_j M) \cap Stab(a)_A$ innerhalb $Stab(a)_A$ zu $G_A(M) \cap Stab(a)_A$ konjugiert ist.

Am Anfang der Rechnung steht auf der linken Seite die Tamagawa-Zahl $(= 2)$ von $Stab(a)$, denn dieser ist die spezielle orthogonale Gruppe des $(n-1 \geq 3)$-dimensionalen Raumes $a^{\perp}$ $(\; n \geq 4)$. Setzen wir das ein, so erhalten wir

$$\frac{2}{vol(Stab(a)_A \cap G_A(M))} = \sum_{j=1}^{N} \frac{1}{|Stab(a)_{\mathbb{Q}} \cap G(\psi_j M)|}$$

Vergleichen wir dies mit (1), so kommt

$$\sum_{k=1}^{h} \frac{A(a, M, M_k)}{|G(M_k)|} = \frac{2}{vol(G_A(M) \cap Stab(a)_A)} \tag{2}$$

Sei Σ die Sphäre $(x,x) = t$. Auf $\Sigma_A \cap M_A$ operiert die Gruppe $G_A(M)$. Wir teilen $\Sigma_A \cap M_A$ in Bahnen:

$$\Sigma_A \cap M_A = \cup_{i=1}^{r} G_A(M) z_i$$

Weil die Bahnen $G_A(M)z$ offen sind und $\Sigma_A \cap M_A$ kompakt, sind es tatsächlich endlich viele.

Lemma 3. *Jede Bahn kann vertreten werden durch ein* $\Phi_{k_i}^{-1} x_i$, *wo* $\Phi_{k_i} M = M_{k_i}$ *eines der Gitter* $M_1, ..., M_h$ *und* $x_i \in M_{k_i}$ *ist.*

Beweis: Sei $z \in \Sigma_A \cap M_A$ gegeben. Da $n \geq 4$, stellt die quadratische Form jede positive Zahl rational dar. Also gibt es $x \in V_{\mathbb{Q}}$ mit $(x,x) = t$. Dem Beweis von Lemma 1 in Kapitel 4 entnimmt man, daß G_A transitiv auf Σ_A operiert. Daher gibt es $\Phi \in G_A$ mit $x = \Phi z$. Das Gitter ΦM liegt im Geschlecht von M, ist also $= \tau M_k$ für ein $\tau \in G_{\mathbb{Q}}$ und einen Klassenvertreter M_k. Schreibt man $M_k = \Phi_k M$, so ist $\Phi_k^{-1} \tau^{-1} \Phi \in G_A(M)$. Wegen $x \in \Phi M = \tau M_k$ ist $y := \tau^{-1} x \in M_k$ und

$$G_A(M)z = G_A(M)\Phi_k^{-1}\tau^{-1}\Phi z = G_A(M)\Phi_k^{-1}\tau^{-1}x = G_A(M)\Phi_k^{-1} y$$

mit $y \in M_k$. Damit haben wir einen Vertreter der gewünschten Art gefunden.

Wir haben nun eine disjunkte Zerlegung

$$\Sigma_A \cap M_A = \cup_{i=1}^{r} G_A(M)\Phi_{k_i}^{-1} x_i$$

mit gewissen k_i und $x_i \in M_{k_i}$.

Sei nun M_k irgendeiner der Klassenrepräsentanten und $x \in M_k$ mit $(x,x) = t$. Dann ist $\Phi_k^{-1} x \in \Sigma_A \cap M_A$, liegt also in einer der Bahnen $G_A(M)\Phi_{k_i}^{-1} x_i$, ist also ein $\Phi\Phi_{k_i}^{-1} x_i$ mit $\Phi \in G_A(M)$. Die Gleichungen

$$x = \Phi_k \Phi \Phi_{k_i}^{-1} x_i \text{ und } M_k = \Phi_k M = \Phi_k \Phi M = \Phi_k \Phi \Phi_{k_i}^{-1} M_{k_i}$$

setzen in Evidenz, daß

$$(x, M_k) \sim (x_i, M_{k_i})$$

(und diese Äquivalenz hat statt für genau ein i). Bezeichnet $A(t, M_k)$ die Anzahl aller $x \in M_k$ mit $(x,x) = t$, so folgt

$$A(t, M_k) = \sum_{i=1}^{r} A(x_i, M_{k_i}, M_k) \tag{3}$$

Volumenberechnung: Die Sphäre Σ ist ein homogener Raum der speziellen orthogonalen Gruppe G, der Stabilisator des Vektors $a \in \Sigma$ ist die spezielle orthogonale Gruppe des $(n-1)$-dimensionalen Raumes $a^{\perp}$. Wie in Kapitel 4 gesehen, ist auch die Abbildung $\pi : G_A \to \Sigma_A$ surjektiv. Sei $\bar{\omega}_A$ das Tamagawa-Maß von $Stab(a)$ und wie früher ω_A das von G. Sei ψ_A das durch

$$\int_{G_A} f(X)\omega_A(X) = \int_{\Sigma_A} (\int_{Stab(a)_A} f(Xu)\bar{\omega}_A(u))\ \psi_A(Xa)$$

bestimmte Maß auf Σ_A (vgl Kapitel 7). Wir benutzen diese Formel, wenn f die Indikatorfunktion der kompakten Untergruppe $G_A(M)$ ist. Dann steht auf der linken Seite das Volumen von $G_A(M)$, und auf der rechten Seite ist das innere Integral über $Stab(a)_A$ gleich 0, wenn es gar kein $u \in Stab(a)_A$ gibt mit $Xu \in G_A(M)$. Gibt es hingegen ein solches, etwa $Xu_0 = \Phi \in G_A(M)$, so gilt

$$Xu \in G_A(M) \Leftrightarrow u_0^{-1} u \in G_A(M) \cap Stab(a)_A$$

und das innere Integral ist

$$\int_{Stab(a)_A} f(Xu)\bar{\omega}_A(u) = \int_{u \in u_0(Stab(a)_A \cap G_A(M))} \bar{\omega}_A(u) = vol(Stab(a)_A \cap G_A(M))$$

Daher ist

$$vol(G_A(M)) = vol(Stab(a)_A \cap G_A(M)) \cdot \int_{z \in G_A(M)a} \psi_A(z)$$

Dies benutzen wir für die Paare x_i, M_{k_i} anstelle von a, M. Weil $G_A(M_{k_i})$ in G_A zu $G_A(M)$ konjugiert ist (also beide dasselbe Volumen haben), erhalten wir

$$\frac{vol(G_A(M))}{vol(Stab(x_i)_A \cap G_A(M_{k_i}))} = \int_{z \in G_A(M_{k_i})x_i} \psi_A(z)$$

Der Integrationsbereich $G_A(M_{k_i})x_i$ ist $= \Phi_{k_i} G_A(M) \phi_{k_i}^{-1} x_i$, und weil ψ invariant unter G ist (Beweis in Kapitel 20, Lemma 1), ist das Integral auf der rechten Seite $= \int_{z \in G_A(M)\Phi_{k_i}^{-1} x_i} \psi_A(z)$. Die linke Seite ersetzen wir nach Gleichung (2) und erhalten

$$\frac{1}{2} vol(G_A(M)) \cdot \sum_{k=1}^{h} \frac{A(x_i, M_{k_i}, M_k)}{|G(M_k)|} = \int_{z \in G_A(M)\Phi_{k_i}^{-1} x_i} \psi_A(z)$$

Summieren wir dies über i, so erhalten wir auf der rechten Seite das Integral über $\Sigma_A \cap M_A$, und auf der linken Seite taucht nach (3) die Darstellungszahl $A(t, M_k)$ auf. Das ergibt

$$\sum_{k=1}^{h} \frac{A(t, M_k)}{|G(M_k)|} = \frac{2}{vol(G_A(M))} \cdot \int_{\Sigma_A \cap M_A} \psi_A(z)$$

Die linke Seite ist das Ziel unserer Mühe, auf der rechten Seite wollen wir einen anderen Ausdruck für das Integral finden.

20. Berechnung des Integrals über die Sphäre

Mit Hilfe einer $\mathbb{Z}$-Basis $v_1, ..., v_n$ von M identifizieren wir M mit $\mathbb{Z}^n$ und M_p mit $\mathfrak{o}_p^n$. Ist A die Matrix der $a_{ij} := (v_i, v_j)$, so ist die quadratische Form gegeben durch $x'Ax$.

Lemma 1. *1) Auf* $\{x'Ax = t,\ (Ax)_i(Ax)_j \neq 0\}$ *gilt*

$$(-1)^i \frac{dx_1 \wedge ... \not{i} ... \wedge dx_n}{(Ax)_i} = (-1)^j \frac{dx_1 \wedge .... \not{j} .... \wedge dx_n}{(Ax)_j}$$

2) Für $T \in G$ *und* $\psi(x) := \frac{dx_2 \wedge ..... \wedge dx_n}{(Ax)_1}$ *gilt*

$$\psi(Tx) = \psi(x)$$

Beweis: Auf $x'Ax = t$ ist $\sum_{\mu,\nu} a_{\mu\nu} x_\mu dx_\nu = 0$. Durch Multiplikation mit

$$dx_1 \wedge .... \not{i} .... \not{j} ..... \wedge dx_n$$

folgt hieraus 1). Weiter: Entsteht T_{ij} aus T durch Streichen der i-ten Zeile und j-ten Spalte und ist $\tilde{T}$ die Adjunkte von T, so ist

$$d(Tx)_2 \wedge ..... \wedge d(Tx)_n = \sum_{j=1}^{n} \det T_{1j} dx_1 \wedge .... \not{j} .... \wedge dx_n = \sum_{j=1}^{n} (-1)^{j+1} \tilde{t}_{j1} dx_1 \wedge .... \not{j} .... \wedge dx_n$$

$$= \sum_{j=1}^{n} \tilde{t}_{j1} (Ax)_j \psi(x) = (\tilde{T}' Ax)_1 \psi(x) = (ATx)_1 \psi(x)$$

Das ist 2).

Sei $\bar{\omega}$ eine invariante Differentialform höchsten Grades auf $Stab(v)$ und ω eine ebensolche auf G. $\bar{\omega}$ läßt sich zu einer invarianten Differentialform $\tilde{\omega}$ auf G fortsetzen. Sei $(v, v) = t$ und π die durch $\pi(X) = Xv$ definierte Abbildung von G auf die Sphäre Σ. Dann ist $\tilde{\omega} \wedge (\psi \circ \pi)$ eine invariante Differentialform höchsten Grades auf G. Bis auf einen rationalen Faktor $\gamma \neq 0$ ist sie $= \omega$:

$$\omega = \gamma \bar{\omega} \wedge (\psi \circ \pi)$$

Bildet man zu den drei Differentialformen $\bar{\omega}, \omega$ und ψ die Tamagawa-Maße (wir wissen schon, daß alle drei konvergent sind), so fällt wegen der Produktformel γ wieder heraus. Damit ist gerechtfertigt: Das im vorigen Kapitel benutzte ψ_A ist das Tamagawa-Maß zu der Differentialform aus Lemma 1.

Berechnung von $\int_{M_p \cap \Sigma_p} \psi_p$:

Wir zerlegen den Integrationsbereich in Restklassen mod p^k:

$$\int_{M_p \cap \Sigma_p} \psi_p(x) = \sum_{c \in M_p,\, c'Ac = t,\, c \bmod p^k} \int_{x'Ax = t,\, x \equiv c \bmod p^k} \psi_p(x)$$

Sei $c \in M_p$ fest mit $c'Ac = t$. Für $x = c + p^k z$ ist $x'Ax = t$ gleichbedeutend mit

$$z'Ac + \frac{1}{2} p^k z'Az = 0$$

Man nehme $b \in M_p$ so, daß $|b'Ac|_p$ maximal ist, das heißt $|b'Ac|_p \geq |z'Ac|_p$ für alle $z \in M_p$. Dieses Maximum ist auf jeden Fall $\geq |c'Ac|_p = |t|_p$. Ein solches b ist primitiv, daher gibt es ein Gitter N vom Rang $n-1$ mit $M_p = \mathfrak{o}_p b \oplus N$. Man schreibt $z = \lambda b + u$ mit $u \in N$.

Lemma 2. *Wenn* $k > v_p(2t^2)$ *, dann gibt es zu jedem* $u \in N$ *genau ein* $\lambda \in \mathfrak{o}_p$ *mit*

$$f(\lambda) := (\lambda b + u)' Ac + \frac{1}{2} p^k (\lambda b + u)' A(\lambda b + u) = 0$$

Beweis: Geordnet nach Potenzen von λ ist

$$f(\lambda) = u' Ac + \frac{1}{2} p^k u' Au + [b' Ac + p^k b' Au] \cdot \lambda + \frac{1}{2} p^k b' Ab \cdot \lambda^2$$

Sei $\rho = v_p(b' Ac)$ Aus $k \geq 2\rho + 1$ folgt $k > \rho$, woraus $|b' Ac + p^k b' Au|_p = |b' Ac|_p$. Nach Definition von b ist $|u' Ac|_p \leq |b' Ac|_p$. Schließlich ist nach Voraussetzung $k - v_p(2) \geq \rho$. Aus diesen drei Tatsachen folgt, daß

$$\lambda_0 := -\frac{u' Ac + \frac{1}{2} p^k u' Au}{b' Ac + p^k b' Au}$$

ganz, das heißt in $\mathfrak{o}_p$ ist. Offenbar gilt

$$f(\lambda_0) = \frac{1}{2} p^k b' Ab \cdot \lambda_0^2 \equiv 0 \bmod p^{k - v_p(2)} \tag{1}$$

$$v_p(f'(\lambda_0)) = v_p(p^k b' Ab \cdot \lambda_0 + [b' Ac + p^k b' Au]) = \rho \tag{2}$$

Wenn $k - v_p(2) \geq 2\rho + 1$ (was nach Voraussetzung im Lemma der Fall ist), dann sagt das Hensel'sche Lemma, daß f eine Nullstelle $\lambda \equiv \lambda_0 \bmod p^{k - v_p(2) - \rho}$, also in $\mathfrak{o}_p$ besitzt. Für die andere Nullstelle λ' von f gilt nach Vieta

$$\lambda + \lambda' = -\frac{2(b' Ac + p^k b' Au)}{p^k b' Ab} \notin \mathfrak{o}_p, \quad \text{also } \lambda' \notin \mathfrak{o}_p$$

Das Lemma zeigt: Die $z \in M_p$ mit $z' Ac + \frac{1}{2} p^k z' Az = 0$ entsprechen umkehrbar eindeutig den $u \in N$ vermöge $z = \lambda b + u$, wobei λ die in $\mathfrak{o}_p$ gelegene Nullstelle von f ist. Auf der Menge $\{x' Ax = t,\ x \equiv c \bmod p^k\}$ können wir also u als Parameter benutzen.

Umrechnung der Differentialform: Sei $b_2, ..., b_n$ eine Basis von N und $b_1 = b$. Dann ist $b_1, ..., b_n$ eine Basis von M_p. Die aus den b_i gebildete Matrix B ist also unimodular und hat oE die Determinante 1.

Sind $e_1, ..., e_n$ die Standard- Basisvektoren, so ist $(Ac)_i = e_i' Ac$, nach Definition von b also $|(Ac)_i|_p \leq |b' Ac|_p$ für alle i und $=$ für mindestens ein i. Ist etwa $i = 1$, so benutzen wir die Form

$$\psi = \frac{dx_2 \wedge .... \wedge dx_n}{(Ax)_1}$$

aus Lemma 1. Ist $x \equiv c \bmod p^k$, so ist $(Ax)_1 \equiv (Ac)_1 \bmod p^k$, also $|(Ax)_1|_p = |(Ac)_1|_p = |b' Ac|_p \geq |t|_p$, wenn $k > v_p(t)$. Dann wird

$$\int_{x' Ax = t,\ x \equiv c \bmod p^k} \psi_p(x) = \frac{1}{|b' Ac|_p} \int_{x' Ax = t,\ x \equiv c \bmod p^k} dx_2 .... dx_n$$

$$= \frac{1}{|b'Ac|_p} p^{-k(n-1)} \int_{z'Ac+\frac{1}{2}p^k z'Az=0,\, z\in \mathfrak{o}_p^n} dz_2....dz_n$$

b war irgendein Vektor in M_p, für den $|b'Ac|_p$ maximal war. Das ist jetzt der Fall für e_1 statt b, also können wir $b = e_1$ setzen. Drücken wir $u \in N$ durch die Basis $b_2, ..., b_n$ aus, so haben wir

$$z = \lambda b + u = \lambda b + \sum_{i=2}^{n} \lambda_i b_i = \begin{pmatrix} \lambda & + & \lambda_2 b_{12} & + & \dots & + & \lambda_n b_{1n} \\ & & \lambda_2 b_{22} & + & & + & \lambda_n b_{2n} \\ & & \vdots & & & & \vdots \\ & & \lambda_2 b_{n2} & + & \dots & + & \lambda_n b_{nn} \end{pmatrix}$$

Daraus folgt

$$dz_2 \wedge .... \wedge dz_n = \det \begin{pmatrix} b_{22} & \dots & b_{2n} \\ \vdots & & \vdots \\ b_{n2} & \dots & b_{nn} \end{pmatrix} d\lambda_2 \wedge .... \wedge d\lambda_n$$

Weil $\det B = 1$, ist auch die Determinante dieser Teilmatrix $= 1$. Wir erhalten

$$\int_{x'Ax=t,\, x\equiv c \bmod p^k} \psi_p(x) = \frac{p^{-k(n-1)}}{|b'Ac|_p}$$

Dabei hängt b (und damit natürlich auch $|b'Ac|_p$) von c ab.

Dies wollen wir in Zusammenhang bringen mit den Siegel'schen Darstellungszahlen

$$A_{p^m}(t, A) = \text{ Anzahl der } x \bmod p^m \text{ mit } x'Ax \equiv t \bmod p^m$$

Sei c fest mit $c'Ac \equiv t \bmod p^m$ und $m > k$. Wir zählen die $x \bmod p^m$ mit $x'Ax \equiv t \bmod p^m$, welche $\equiv c \bmod p^k$ sind. Diese setzen wir an in der Form $x = c + p^k y$ und zählen die ganzen $y \bmod p^{m-k}$ mit

$$c'Ac + 2p^k c'Ay + p^{2k} y'Ay \equiv t \bmod p^m$$

also

$$2c'Ay + p^k y'Ay \equiv 0 \bmod p^{m-k}$$

Wählt man zu c wieder b und N wie oben und schreibt $y = \lambda b + u$, so muß

$$2c'Au + p^k u'Au + 2[b'Ac + p^k b'Au] \cdot \lambda + p^k b'Ab \cdot \lambda^2 \equiv 0 \bmod p^{m-k}$$

sein. Nach Lemma 2 gibt es, wenn $k > 2\rho + v_p(2)$, zu jedem $u \in N$ genau eine Nullstelle $\lambda_0 \in \mathfrak{o}_p$ des Polynoms auf der linken Seite. Und λ ist Nullstelle mod p^{m-k} genau dann wenn

$$2(\lambda - \lambda_0)c'Ab \equiv 0 \bmod p^{m-k}$$

also

$$\lambda \equiv \lambda_0 \bmod p^{m-k-\rho-v_p(2)}$$

Wir haben $p^{(n-1)(m-k)}$ modulo p^{m-k} verschiedene Möglichkeiten für u und für jedes u nochmal $p^{\rho+v_p(2)}$ Möglichkeiten, bei festem c. Das ergibt

$$A_{p^m}(t,A) = \sum_{c \bmod p^k,\, c'Ac \equiv t \bmod p^m} p^{(n-1)(m-k)+\rho_c+v_p(2)} \tag{1}$$

wobei wir ρ_c geschrieben haben, weil ja ρ von c abhängig ist. Vorher hatten wir

$$\int_{M_p \cap \Sigma_p} \psi_p(x) = \sum_{c \bmod p^k,\, c'Ac = t} p^{-k(n-1)+\rho_c} \tag{2}$$

Nun folgt wieder aus dem Hensel'schen Lemma, daß man (wenn m groß genug ist) jede Restklasse $c \bmod p^k$ mit $c'Ac \equiv t \bmod p^m$ durch ein c mit $c'Ac = t$ vertreten kann. Dann liefert Vergleich von (1) und (2)

$$p^{-m(n-1)} A_{p^m}(t,A) = p^{v_p(2)} \int_{M_p \cap \Sigma_p} \psi_p(x)$$

Diese Gleichung zeigt, daß $p^{-m(n-1)} A_{p^m}(t,A)$ für große m von m unabhängig ist. Nach Siegel (Formel (38), Seite 558) setzt man

$$\alpha_p = p^{-m(n-1)} A_{p^m}(t,A) \text{ für } m >> 0$$

Das Ergebnis ist

$$\int_{M_p \cap \Sigma_p} \psi_p(x) = \begin{cases} \alpha_p & \text{wenn } p \neq 2 \\ \frac{1}{2}\alpha_p & \text{wenn } p = 2 \end{cases}$$

Jetzt bleibt nur noch das Integral an der unendlichen Stelle für dieselbe Differentialform auszurechnen, also das

$$\int_{x'Ax=t} \frac{dx_2 .... dx_n}{|(Ax)_1|}$$

und hierin ist jetzt $|\,|$ der gewöhnliche Absolutbetrag.

Da wir angenommen haben, daß die Form positiv definit ist, gibt es T mit $A = T'T$. Setzt man $Tx = y$, so ist $y'y = t$ und

$$dy_2 \wedge ..... \wedge dy_n = \sum_{i=1}^{n} \det(T_{1i}) dx_1 \wedge ... \not{dx_1} .... \wedge dx_n$$

$$= \sum_{i=1}^{n} (-1)^{i+1} \tilde{t}_{i1} dx_1 \wedge ... \not{dx_1} ... \wedge dx_n$$

$$= \sum_{i=1}^{n} \tilde{t}_{i1} \frac{(Ax)_i}{(Ax)_1} dx_2 \wedge ..... \wedge dx_n$$

nach Lemma 1. Wegen $\tilde{T} = (\det T) \cdot T^{-1}$ und $T'T = A$ ist

$$\tilde{T} = \sqrt{\det A} \cdot A^{-1} T'$$

und

$$\sum_{i=1}^{n} \tilde{t}_{i1}(Ax)_i = (\tilde{T}'Ax)_1 = (\tilde{T}'T'Tx)_1 = (\det T)\cdot(Tx)_1 = \sqrt{\det A}\cdot y_1$$

und

$$dy_2 \wedge .... \wedge dy_n = \sqrt{\det A}\frac{y_1}{(Ax)_1} dx_2 \wedge ..... \wedge dx_n$$

Es folgt

$$\int_{x'Ax=t} \psi_\infty(x) = (\det A)^{-\frac{1}{2}} \int_{y'y=t} \frac{dy_2....dy_n}{|y_1|}$$

Wir setzen noch $y = \sqrt{t}\, z$ und erhalten

$$\int_{x'Ax=t} \psi_\infty(x) = (\det A)^{-\frac{1}{2}} \cdot t^{\frac{n}{2}-1} \cdot \int_{z'z=1} \frac{dz_2....dz_n}{|z_1|}$$

Etwas aufpassen beim Integrieren: Zu jedem $(n-1)$-Tupel $z_2, ..., z_n$ mit $\sum_{i=2}^{n} z_i^2 < 1$ gehören zwei Punkte im Integrationsbereich ! Dessen eingedenk erkennt man, daß das letzte Integral gleich der Oberfläche der Einheitskugel im $\mathbb{R}^n$ ist, also

$$= 2\frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})}$$

Zusammen wird

$$\int_{x'Ax=t} \psi_\infty(x) = 2(\det A)^{-\frac{1}{2}} t^{\frac{n}{2}-1} \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})}$$

Multipliziert man die für die Primzahlen p und für ∞ erhaltenen Ergebnisse, so erhält man (der Faktor 2 bei ∞ und $\frac{1}{2}$ bei $p=2$ heben sich gerade weg)

$$\int_{z\in M_A \cap \Sigma_A} \psi_A(z) = (\det A)^{-\frac{1}{2}} t^{\frac{n}{2}-1} \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})} \cdot \prod_p \alpha_p$$

Wir erinnern an die Gleichung

$$\sum_{k=1}^{h} \frac{A(t.M_k)}{|G(M_k)|} = \frac{2}{vol\, G_A(M)} \int_{z\in M_A \cap \Sigma_A} \psi_A(z)$$

Hierin ersetzen wir das Integral durch den soeben dafür gefundenen Wert und entnehmen $\frac{2}{vol\, G_A(M)}$ aus Kapitel 13:

$$2 = \tau(G) = vol(G_{\mathbb{Q}} \backslash G_A) = \sum_{k=1}^{h} \frac{1}{|G(M_k)|} \cdot vol(G_A(M))$$

Dann erhalten wir die Siegel'sche Formel

$$\frac{\sum_{k=1}^{h} \frac{A(t.M_k)}{|G(M_k)|}}{\sum_{k=1}^{h} \frac{1}{|G(M_k)|}} = (\det A)^{-\frac{1}{2}} t^{\frac{n}{2}-1} \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})} \cdot \prod_p \alpha_p \tag{3}$$

Bemerkung: Nach Herleitung wird über die engeren Klassen im Geschlecht von M summiert, und $|G(M_k)|$ ist die Anzahl der Automorphismen von M_k mit Determinante $+1$. Sei $O(M_k)$ die Gruppe aller Automorphismen von M_k. Wir stellen dieselbe Betrachtung an wie in Kapitel 13:

1. Fall: M_k gestattet einen Automorphismus mit Determinante -1. Dann ist $|O(M_k)| = 2|G(M_k)|$ und die Klasse von M_k ist gleichzeitig die engere Klasse.

2. Fall: M_k gestattet keinen solchen. Dann ist $O(M_k) = G(M_k)$, und wenn σ eine beliebige orthogonale Transformation mit Determinante -1 von $V_{\mathbb{Q}}$ ist, dann liegen M_k und σM_k in verschiedenen engeren Klassen. Sie stellen aber beide die Zahl t gleich oft dar und haben gleich viele Automorphismen. Daher

$$\sum_{k=1}^{h} \frac{A(t,M_k)}{|G(M_k)|} = \sum_{1.Fall} \frac{A(t,M_k)}{\frac{1}{2}|O(M_k)|} + \sum_{2.Fall} [\frac{A(t,M_k)}{|O(M_k)|} + \frac{A(t,\sigma M_k)}{|O(\sigma M_k)|}] = 2 \sum_{Klassen} \frac{A(t,M_k)}{|O(M_k)|}$$

wobei zuletzt tatsächlich über die Klassen und nicht über die engeren Klassen summiert wird. Das Gleiche passiert im Nenner der Formel (3). Das heißt, in der Siegel'schen Formel ändert sich gar nichts, wenn man gleichzeitig die Gruppen $G(M_k)$ durch die Gruppen $O(M_k)$ ersetzt und über die Klassen statt engeren Klassen summiert. Und so ist die Formel auch in der Siegel'schen Atbeit gemeint.

21. Beispiele

1. Quadratsummen: Für $n \leq 8$ ist nach Kapitel 14 das Geschlecht von $\mathbb{Z}^n$ einklassig. Die Siegel'sche Formel liefert in diesem Falle Darstellungszahlen für das Gitter $\mathbb{Z}^n$ und nicht nur die über die Klassen im Geschlecht gemittelten Darstellungszahlen. Wir berechnen die $\alpha_p = p^{-m(n-1)} A_{p^m}(\mathbb{Z}^n, t)$. Der Einfachheit halber nehmen wir zunächst t quadratfrei und $\equiv 1 \bmod 8$.

$p = 2$: Mit Hensel genügt $m = 3$. Wegen $t \equiv 1 \bmod 8$ können wir die $A_8(n,t) := A_8(\mathbb{Z}^n, t)$ aus Kapitel 14 übernehmen.

n	2	3	4	5	6	7	8
$A_8(n,t)$	16	$3 \cdot 2^5$	2^9	$5 \cdot 2^9$	$3 \cdot 2^{13}$	$7 \cdot 2^{15}$	2^{21}
$\alpha_2 = 2^{-3(n-1)} A_8(n,t)$	2	$\frac{3}{2}$	1	$\frac{5}{8}$	$\frac{3}{4}$	$\frac{7}{8}$	1

$p \dagger 2t$: Diese $A_p(n,t)$ haben wir in Kapitel 10 berechnet:

$$A_p(n,t) = \begin{cases} p^{n-1} - (\frac{-1}{p})^{\frac{n}{2}} p^{\frac{n}{2}-1} & \text{wenn } n \text{ gerade} \\ p^{n-1} + (\frac{(-1)^{\frac{n-1}{2}} t}{p}) p^{\frac{n-1}{2}} & \text{wenn } n \text{ ungerade} \end{cases}$$

Die α_p sind die $p^{-(n-1)}$-fachen davon.

$p|t$: Sei $m \geq 1$ und $(c,c) = \sum c_i^2 \equiv t \bmod p^m$, etwa $= t + p^m \gamma$ mit $\gamma \in \mathfrak{o}_p$. Dann ist

$$\sum (c_i + p^m y_i)^2 \equiv t + p^m \gamma + 2p^m \sum c_i y_i \bmod p^{m+1}$$

Ist c primitiv (i.e. nicht alle c_i durch p teilbar), so gibt es genau p^{n-1} modulo p verschiedene Lösungen y von $2\sum c_i y_i + \gamma \equiv 0 \bmod p$. Zu jedem primitiven c mit $(c,c) \equiv t \bmod p^m$ gehören daher genau p^{n-1} Lösungen $c^* = c + p^m y$ mit $(c^*, c^*) \equiv t \bmod p^{m+1}$. Ist nun $m \geq 2$, so folgt aus $(c,c) \equiv t \bmod p^m$ und $p^2 \dagger t$ automatisch, daß c primitiv ist. Daher

$$(a) \qquad A_{p^{m+1}}(n,t) = p^{n-1} A_{p^m}(n,t) \text{ wenn } m \geq 2$$

Für $m = 1$ hat man sich auf die primitiven c zu beschränken, das heißt

$$(b) \quad A_{p^2}(n,t) = p^{n-1} \cdot \text{ Anzahl } A_p^* \text{ der } c \bmod p \text{ mit } c \not\equiv 0 \bmod p \text{ und } \sum c_i^2 \equiv t \bmod p$$

Wegen $p|t$ ist die letzte Anzahl die Zahl der isotropen Vektoren mod p. Diese entnehmen wir aus Kapitel 10 und erhalten aus (a) und (b)

$$\alpha_p = p^{-m(n-1)} A_{p^m}(n,t) = p^{-(n-1)} A_p^* =$$

$$p^{-(n-1)} \cdot \begin{cases} (p^{\frac{n}{2}} - (\frac{-1}{p})^{\frac{n}{2}})(p^{\frac{n}{2}-1} + (\frac{-1}{p})^{\frac{n}{2}}) & \text{wenn } n \text{ gerade} \\ p^{n-1} - 1 & \text{wenn } n \text{ ungerade} \end{cases}$$

Für gerades n setzen wir $\chi(p) = (\frac{-1}{p})$ und

$$\chi_n(p) = \chi(p)^{\frac{n}{2}} = \begin{cases} 1 & \text{wenn } n \equiv 0 \bmod 4 \\ (\frac{-1}{p}) & \text{wenn } n \equiv 2 \bmod 4 \end{cases}$$

Für ungerades n setzen wir

$$\psi_n(p) = (\frac{(-1)^{\frac{n-1}{2}}t}{p}) = \begin{cases} (\frac{-t}{p}) & \text{wenn } n \equiv 3 \bmod 4 \\ (\frac{t}{p}) & \text{wenn } n \equiv 1 \bmod 4 \end{cases}$$

Für gerades n erhalten wir dann

$$\prod_{p\neq 2} \alpha_p = \prod_{p\dagger 2t}(1-\chi_n(p)p^{-\frac{n}{2}}) \cdot \prod_{p|t}(1-\chi_n(p)p^{-\frac{n}{2}})(1+\chi_n(p)p^{1-\frac{n}{2}})$$

$$= \prod_{p\neq 2}(1-\chi_n(p)p^{-\frac{n}{2}}) \cdot \prod_{p|t}(1+\chi_n(p)p^{1-\frac{n}{2}})$$

$$= \begin{cases} \frac{1}{1-2^{-\frac{n}{2}}} \cdot \zeta(\frac{n}{2})^{-1} \cdot \prod_{p|t}(1+p^{1-\frac{n}{2}}) & \text{wenn } n \equiv 0 \bmod 4 \\ L(\frac{n}{2},\chi)^{-1} \cdot \prod_{p|t}(1+\chi(p)p^{1-\frac{n}{2}}) & \text{wenn } n \equiv 2 \bmod 4 \end{cases}$$

Für ungerades n wird

$$\prod_{p\neq 2} \alpha_p = \prod_{p\dagger 2t}(1+\psi_n(p)p^{-\frac{n-1}{2}}) \cdot \prod_{p|t}(1-p^{-(n-1)})$$

$$= \prod_{p\dagger 2t} \frac{1-p^{-(n-1)}}{1-\psi_n(p)p^{-\frac{n-1}{2}}} \cdot \prod_{p|t}(1-p^{-(n-1)})$$

$$= L(\frac{n-1}{2},\psi_n) \cdot \frac{1}{1-2^{-(n-1)}} \cdot \zeta(n-1)^{-1}$$

Wie eingangs bemerkt, ist das Geschlecht von $\mathbb{Z}^n$ einklassig für $n \leq 8$, und die Siegel'sche Formel lautet jetzt

$$A(\mathbb{Z}^n,t) = t^{\frac{n}{2}-1} \cdot \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})} \cdot \prod_p \alpha_p$$

Wir haben sie bewiesen für $n \geq 4$ (wir haben die Tamagawa-Zahl des Stabilisators eines Vektors eingesetzt).

$n = 4$:

$$A(\mathbb{Z}^4,t) = t \cdot \frac{\pi^2}{\Gamma(2)} \cdot \alpha_2 \cdot \prod_{p\neq 2} \alpha_p$$

$$= t \cdot \pi^2 \cdot \frac{1}{1-2^{-2}} \cdot \frac{1}{\zeta(2)} \cdot \prod_{p|t}(1+p^{-1})$$

$$= 8 \prod_{p|t} (p+1)$$

$n = 6$:

$$A(\mathbb{Z}^6, t) = t^2 \cdot \frac{\pi^3}{\Gamma(3)} \cdot \frac{3}{4} \cdot L(3,\chi)^{-1} \prod_{p|t} (1 + \chi(p) p^{-2})$$

$$= \frac{3}{8} \cdot \frac{\pi^3}{L(3,\chi)} \prod_{p|t} (p^2 + \chi(p))$$

$n = 8$:

$$A(\mathbb{Z}^8, t) = t^3 \cdot \frac{\pi^4}{\Gamma(4)} \cdot \frac{1}{1 - 2^{-4}} \cdot \frac{1}{\zeta(4)} \cdot \prod_{p|t} (1 + p^{-3})$$

$$= 16 \cdot \prod_{p|t} (p^3 + 1)$$

Die Formeln für $n = 4$ und 8 sind aus der Elementaren Zahlentheorie wohlbekannt.

Nun zu den ungeraden n:

$$A(\mathbb{Z}^5, t) = t^{\frac{3}{2}} \cdot \frac{\pi^{\frac{5}{2}}}{\Gamma(\frac{5}{2})} \cdot \frac{5}{8} \cdot \prod_{p \neq 2} (1 - p^{-4}) \cdot L(2, \psi)$$

$$= 80 \frac{t^{\frac{3}{2}}}{\pi^2} \cdot L(2, \psi)$$

mit $\psi(p) = (\frac{t}{p})$ für $p \dagger 2t$ (und $= 0$ sonst). Dies ist das zweite Beispiel in [S],Seite 569.

$$A(t, \mathbb{Z}^7) = t^{\frac{5}{2}} \cdot \frac{\pi^{\frac{7}{2}}}{\Gamma(\frac{7}{2})} \cdot \frac{7}{8} \cdot \frac{2^6}{2^6 - 1} \cdot \zeta(6)^{-1} L(3, \psi')$$

$$= 448 t^{\frac{5}{2}} \cdot \frac{L(3, \psi')}{\pi^3}$$

mit $\psi'(p) = (\frac{-t}{p})$ für $p \dagger 2t$.

Bemerkungen: 1. Die Voraussetzung $t \equiv 1 \bmod 8$ berührt nur α_2 und nicht die α_p für $p \neq 2$. Wenn $t \equiv 3, 5$ oder $7 \bmod 8$, so finden wir für $A_8(\mathbb{Z}^n, t)$ für $n = 4, 5, 6, 7, 8$ die Werte

$t \backslash n$	4	5	6	7	8
3	2^9	$5 \cdot 2^{10}$	$5 \cdot 2^{13}$	$5 \cdot 7 \cdot 2^{13}$	2^{21}
5	2^9	$7 \cdot 2^9$	$3 \cdot 2^{13}$	$7 \cdot 2^{15}$	2^{21}
7	2^9	$5 \cdot 2^{10}$	$5 \cdot 2^{13}$	$37 \cdot 2^{13}$	2^{21}

Für $n = 5$ zum Beispiel müssen wir in der Formel für $A(\mathbb{Z}^5, t)$ nur den Faktor 80 durch 160 ersetzen, wenn $t \equiv 3$ oder $7 \bmod 8$ ist und durch $\frac{7}{5} \cdot 80 = 112$, wenn $t \equiv 5 \bmod 8$.

2. In der Formel für $A(\mathbb{Z}^6, t)$ setzen wir $t = 1$. Offenbar ist $A(\mathbb{Z}^6, 1) = 2 \cdot 6$, und das Produkt ist leer. Wir erhalten

$$2 \cdot 6 = \frac{3}{8} \cdot \frac{\pi^3}{L(3, \chi)}$$

also

$$L(3, \chi) = \frac{\pi^3}{32} \quad \text{(siehe auch Seite 78)}$$

Dies können wir in die Formel einsetzen und erhalten

$$A(\mathbb{Z}^6, t) = 12 \cdot \prod_{p|t} (p^2 + \chi(p)) \text{ wenn } t \equiv 1 \bmod 8$$

Aus der obigen Tabelle entnehmen wir (weil $\chi(p) = (\frac{-1}{p})$): Für ungerade quadratfreie t gilt

$$A(\mathbb{Z}^6, t) = \begin{cases} 12 \cdot \prod_{p|t} (p^2 + (\frac{-1}{p})) & \text{wenn } t \equiv 1 \bmod 4 \\ 20 \cdot \prod_{p|t} (p^2 + (\frac{-1}{p})) & \text{wenn } t \equiv 3 \bmod 4 \end{cases}$$

Diese Formel findet sich (als Summe über die Teiler von t geschrieben) zum Beispel in [H W], Seite 314.

Als letztes Beispiel zählen wir im Gitter E_8 die sogenannten Wurzeln, das sind die x mit $(x, x) = 2$.

Für alle $p \neq 2$ wird es $\mathfrak{o}_p^8$, und wir können die α_p von oben übernehmen:

$$\alpha_p = 1 - p^{-4} \text{ für } p \neq 2$$

Für $p = 2$ wird E_8 nach Kapitel 14 direkte Summe von vier hyperbolischen Gittern. Wir müssen bestimmen

$$|\{(\lambda_1, ..., \lambda_4, \mu_1, ...\mu_4) \bmod 2^m \mid 2 \sum_{i=1}^{4} \lambda_i \mu_i \equiv 2 \bmod 2^m\}|$$

$$= |\{(\lambda_1, ..., \lambda_4, \mu_1, ..., \mu_4) \bmod 2^m \mid \sum_{i=1}^{4} \lambda_i \mu_i \equiv 1 \bmod 2^{m-1}\}|$$

Für ein solches 8-Tupel sind nicht alle μ_i durch 2 teilbar. Es gibt also mod 2^m gerade $2^{4m} - 2^{4(m-1)}$ zulässige Quadrupel μ. In jedem solchen ist mindestens ein μ_i Einheit, etwa μ_1. Dann kann man $\lambda_2, \lambda_3, \lambda_4$ beliebig wählen, für jedes gibt es 2^m Möglichkeiten, und λ_1 muß die Kongruenz $\lambda_1 \mu_1 \equiv 1 - \sum_{i=2}^{4} \lambda_i \mu_i \bmod 2^{m-1}$ erfüllen, hat also mod 2^m zwei Möglichkeiten. Das ergibt

$$\alpha_2 = 2^{-7m} \cdot (2^{4m} - 2^{4(m-1)}) \cdot 2^{3m} \cdot 2 = \frac{15}{8}$$

Jetzt liefert die Formel

$$A(E_8, 2) = 2^3 \cdot \frac{\pi^4}{\Gamma(4)} \cdot \frac{15}{8} \cdot \prod_{p \neq 2} (1 - p^{-4}) = 240$$

und das ist in der Tat die Anzahl der Wurzeln in E_8 (wie man durch unmittelbares Abzählen anhand einer geeigneten Beschreibung von E_8 bestätigt).

Literaturverzeichnis

[Bö] S. Böge, Vorlesung über Quadratische Formen, WS 2000/2001

[Bo] A. Borel, Introduction aux Groupes arithmetiques, Hermann, Paris 1969

[E] W. Ebeling, Lattices and Codes, Vieweg 1994

[F B] E.Freitag, R.Busam, Funktionentheorie, Springer 2000, dritte Auflage

[H W] G.H.Hardy-E.M.Wright, Introduction to the Theory of Numbers, Oxford 1938

[K] M.Kneser, Quadratische Formen, Springer 2001

[L] L.H. Loomis, Abstract Harmonic Analysis, D.Van Nostrand 1953

[Sch] H.Schubert, Topologie: Eine Einführung, Teubner 1964

[S] C.L. Siegel, Über die analytische Theorie der quadratischen Formen, Annals of Math. 36 (1935)

[T] J. Tate, Fourier Analysis in Number Fields, Thesis 1950

[W1] A. Weil, L'integration dans les groupes topologiques et ses applications, Hermann, Paris 1951

[W2] A. Weil, Adeles and Algebraic Groups, Princeton 1961

[Z] D.B. Zagier, Zetafunktionen und quadratische Körper, Springer 1981

Dieses Manuskript ist aus einer Vorlesung entstanden, die ich im Wintersemester 2016/17 in Heidelberg gehalten habe. Der Reiz für mich bestand darin, wirklich im Einzelnen und mit allen Formeln in Evidenz zu setzen, daß die Minkowski-Siegel'sche Formel in der großen Arbeit von Siegel aus dem Jahre 1935 äquivalent ist zu der Aussage, daß die Tamagawazahl der orthogonalen Gruppe (zunächst zu einer positiv definiten quadratischen Form) gleich 2 ist. Jeder weiß das, aber niemand hat das genau vorgerechnet. Man kann die Formeln auch benutzen, um Darstellungen von Zahlen durch Formen zu betrachten. Den Ansatz dazu habe ich dem Buch „Quadratische Formen“ von M. Kneser entnommen. Außerdem werden die Minkowski'schen Ungleichungen in orthogonalen Gruppen bewiesen und Siegelbereiche beschrieben und ihr Volumen abgeschätzt.

UNIVERSITÄT
HEIDELBERG
ZUKUNFT
SEIT 1386

ISBN 978-3-946531-86-9