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

(1) $$f(\lambda_0) = \frac{1}{2}p^k b'Ab \cdot \lambda_0^2 \equiv 0 \bmod p^{k - v_p(2)}$$

(2) $$v_p(f'(\lambda_0)) = v_p(p^k b'Ab \cdot \lambda_0 + [b'Ac + p^k b'Au]) = \rho$$

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

$$dy_2\wedge.....\wedge dy_n = \sum_{i=1}^{n}\det(T_{1i})dx_1\wedge...\cancel{i}....\wedge dx_n$$

$$= \sum_{i=1}^{n}(-1)^{i+1}\tilde{t}_{i1}dx_1\wedge...\cancel{i}...\wedge dx_n$$

$$= \sum_{i=1}^{n}\tilde{t}_{i1}\frac{(Ax)_i}{(Ax)_1}dx_2\wedge.....\wedge dx_n$$

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

$$\text{(3)} \qquad \frac{\sum_{k=1}^{h} \frac{A(t.M_k)}{|G(M_k)|}}{\sum_{k=1}^{h} \frac{1}{|G(M_k)|}} = (\det A)^{-\frac{1}{2}} t^{\frac{n}{2}-1} \frac{\pi^{\frac{n}{2}}}{\Gamma(\frac{n}{2})} \cdot \prod_p \alpha_p$$

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.