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.