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.