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.