

DEPARTMENT MATHEMATIK/INFORMATIK
MATHEMATISCH – NATURWISSENSCHAFTLICHE FAKULTÄT
UNIVERSITÄT ZU KÖLN

SIEGELSCHER MODULFORMEN

MASTERARBEIT

Vorgelegt von
Titus Pavlovic

Betreuer: Prof. Dr. Sander Zwegers

Köln, 14. Dezember 2022

Vorwort

Die vorliegende Masterarbeit *Siegelsche Modulformen* ist die Abschlussarbeit nach dem Masterstudium der Mathematik am Department Mathematik/Informatik der Universität zu Köln im Wintersemester 2022/2023.

Sie stellt eine Einführung in das Titelthema dar und beschäftigt sich mit Verallgemeinerungen der klassischen Modulformen einer komplexen Variablen.

Hierfür fand ein Studium der im Literaturverzeichnis aufgeführten Bücher, Vorlesungsunterlagen und wissenschaftlichen Artikel statt, deren Bearbeitung sich in dieser Arbeit findet. Sie wurde mithilfe von \LaTeX erstellt.

Mein Dank geht an meine Familie, Freunde sowie Herrn Prof. Dr. Zwegers, die mich in der Zeit der Anfertigung meiner Masterarbeit unterstützten.

Köln, den 14. Dezember 2022

Titus Pavlovic

Inhaltsverzeichnis

1	Einleitung	1
1.1	Thetafunktionen und Modulformen	1
1.2	Siegelsche Modulformen	2
1.3	Notation	4
2	Die symplektische Gruppe $\mathrm{Sp}_n(\mathbb{R})$	7
2.1	Vorbereitungen	7
2.2	Darstellungszahlen und Thetafunktionen	10
2.3	Die symplektische Gruppe $\mathrm{Sp}_n(\mathbb{R})$	15
2.4	Die Operation von $\mathrm{Sp}_n(\mathbb{R})$ auf \mathbb{H}_n	18
2.5	Erzeuger der Siegelschen Modulgruppe Γ_n	23
3	Der Siegelsche Fundamentalbereich \mathcal{F}_n	30
3.1	Die Jacobi – Zerlegung	30
3.2	Die Ungleichung von Hermite	32
3.3	Die Minkowskische Reduktionstheorie	33
3.4	Ungleichungen in der Minkowskischen Reduktionstheorie	39
3.5	Der Siegelsche Fundamentalbereich \mathcal{F}_n	46
3.6	Ungleichungen für siegelreduzierte Matrizen	51
4	Siegelsche Modulformen	54
4.1	Der Vektorraum $M_k(\Gamma_n)$ der Siegelschen Modulformen	54
4.2	Thetafunktionen	58
4.3	Das Prinzip von Koecher	63
4.4	Der Siegelsche Operator Φ	65
4.5	Siegelsche Spitzenformen	70
4.6	Die Endlichdimensionalität von $M_k(\Gamma_n)$	73
4.7	Folgerungen	79
	Literaturverzeichnis	82

Kapitel 1

Einleitung

1.1 Thetafunktionen und Modulformen

Bereits im 18. Jahrhundert wurden immer wieder Integrale der Gestalt

$$F(x) := \int_a^x \frac{dt}{\sqrt{p(t)}}$$

untersucht. Dabei stellt $p(t)$ ein reelles Polynom dritten oder vierten Grades in t dar, das im betrachteten Intervall positiv ist [7, S. 287], [38, S. 1, 2]. Solche Integrale treten beispielsweise bei der Berechnung der Bogenlänge von Ellipsen, Hyperbeln und der Lemniskate auf und werden daher *elliptische Integrale* genannt [38, S. 2].

Die entscheidende Idee zu ihrer Behandlung fand Gauß um 1800 durch Übergang zu deren Umkehrfunktionen [56, S. 225]. Weit verbreitet wurde diese Vorgehensweise aber erst, als die Theorie der *elliptischen Funktionen* durch Abel (in [1] aus dem Jahr 1827) und Jacobi (in [30] aus dem Jahr 1829) nahezu zeitgleich entstand [38, S. 2, 6, 9], [56, S. 225]. Entscheidendes Hilfsmittel für Jacobi waren dazu Reihen der Art

$$\vartheta(z, w) := \sum_{g \in \mathbb{Z}} e^{\pi i g^2 z + 2\pi i g w}$$

für $z \in \mathbb{H} := \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$ und $w \in \mathbb{C}$. Ihm zu Ehren heißt $\vartheta(z, w)$ heute die *Jacobische Thetafunktion* [7, S. 300 – 302], [38, S. 84, 150], [61, S. 10].

Die Bedeutung der Thetafunktionen war aber schon vorher bekannt: Erstmals erscheint nämlich die klassische Thetafunktion

$$\vartheta(z, 0) = \sum_{g \in \mathbb{Z}} e^{\pi i g^2 z}, \quad z \in \mathbb{H}, \quad (1.1)$$

im Jahr 1748 bei Euler [12]. Und Gauß [20] war schon um 1808 eine Transformationsformel für die Thetafunktion bekannt [16, S. 12], [38, S. 150, 255].

Das Quadrat von (1.1) ist

$$\vartheta^2(z, 0) = \sum_{g_1, g_2 \in \mathbb{Z}} e^{\pi i (g_1^2 + g_2^2) z} = 1 + 4e^{\pi i z} + 4e^{2\pi i z} + 0e^{3\pi i z} + \dots$$

Die dabei auftretenden Koeffizienten von $e^{\pi itz}$, $t \in \mathbb{N}_0$, stellen die Anzahl der Darstellungen von t als Summe zweier Quadrate dar [16, S. 5], [38, S. 150, 201, 202], [61, S. 36].

Um geschlossene Formeln für derartige Darstellungszahlen anzugeben, ist eine Untersuchung der Thetafunktionen respektive der Funktionen mit ähnlichen Eigenschaften sinnvoll [3, S. 2, 43]. Das führt zum Studium der *klassischen Modulformen einer komplexen Variablen*: Wie die elliptischen Funktionen unter gewissen Translationen invariant sind, so besitzen Modulformen ein schönes Transformationsverhalten unter den Möbiustransformationen

$$\begin{aligned} \mathbb{H} &\longrightarrow \mathbb{H} \\ z &\longmapsto \frac{az + b}{cz + d}, \end{aligned}$$

wobei $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid ad - bc = 1 \right\}$ ist [7, S. 321], [38, S. 149], [60, S. 1].

1.2 Siegelsche Modulformen

In seiner 1935 veröffentlichten Arbeit [54] untersuchte Siegel allgemeiner die Darstellung von Matrizen durch quadratische Formen. Für eine symmetrische und positiv definite Matrix $a \in M_m(\mathbb{R})$ und eine Matrix $t \in M_n(\mathbb{R})$ sind dann die Darstellungszahlen

$$r_a(t) := \left| \left\{ g \in M_{m,n}(\mathbb{Z}) \mid \frac{1}{2}a[g] = t \right\} \right| \quad (1.2)$$

von Interesse [16, S. 5], [51, S. 1, 2], [54, S. 527 – 606].

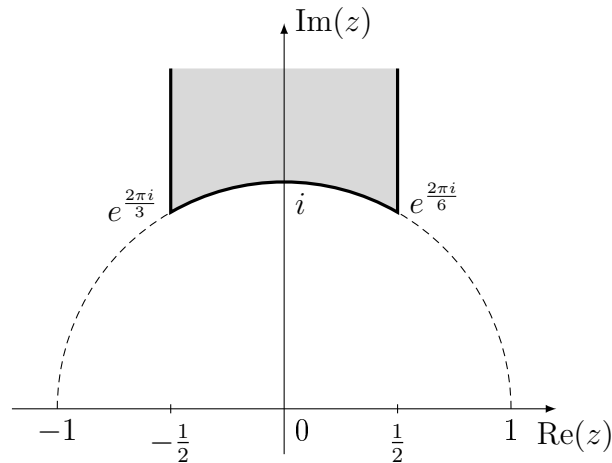
Auch wenn sich bereits dort ein Abschnitt über *Modulfunktionen n -ten Grades* findet [54, S. 595 – 606], so war es erst Siegels Arbeit [55] aus dem Jahr 1939, die eine eingehende Behandlung dieser Thematik darstellte [55, S. 617 – 657]: Dort zeichnete er die Art und Weise vor, wie die *Modulformen n -ten Grades*, die mittlerweile *Siegelsche Modulformen* genannt werden, einzuführen sind. Vieles erscheint dabei als Verallgemeinerung der klassischen Modulformen einer komplexen Variablen [36, S. 399].

Anstatt die Operation von $\Gamma_1 = \mathrm{SL}_2(\mathbb{Z})$ auf \mathbb{H} zu untersuchen, wird die Operation der sogenannten *Siegelschen Modulgruppe* Γ_n betrachtet. An die Stelle von \mathbb{H} tritt dann die sogenannte *Siegelsche Halbebene* \mathbb{H}_n [21, S. 181, 184], [54, S. 595 – 598], [55, S. 620 – 627]. Mit derartigen Ausführungen beschäftigen wir uns im anschließenden zweiten Kapitel, das mit der Untersuchung der Erzeuger von Γ_n endet.

Das dritte Kapitel dieser Masterarbeit behandelt den sogenannten *Siegelschen Fundamentalbereich* \mathcal{F}_n , der den klassischen Fundamentalbereich

$$\mathcal{F} = \left\{ z \in \mathbb{H} \mid |z| \geq 1, |\mathrm{Re}(z)| \leq \frac{1}{2} \right\}$$

der Operation von Γ_1 auf \mathbb{H} verallgemeinert (Abbildung 1.1) [3, S. 44, 45], [7, S. 317, 326]. Durch die größere Allgemeinheit, mit der wir für \mathcal{F}_n konfrontiert sind, ist dies aufwendiger:

Abbildung 1.1: Der Fundamentalbereich \mathcal{F}

Motiviert von Minkowskis Ausführungen in [48] benutzte Siegel dessen Reduktionstheorie, um \mathcal{F}_n angeben zu können [54, S. 598 – 600], [55, S. 627 – 633]. Die dazu für uns nötige Theorie wird im dritten Kapitel dargestellt.

Schließlich ist es dann im vierten Kapitel möglich, *Siegelsche Modulformen* zu definieren und untersuchen [54, S. 600, 601], [55, S. 633 – 645]. Wie im Fall der klassischen Modulformen einer komplexen Variablen beschäftigen wir uns mit Thetafunktionen sowie Spitzenformen und beweisen die Endlichdimensionalität der Vektorräume $M_k(\Gamma_n)$ der Siegelschen Modulformen. Dies gelingt aufgrund eines von Siegel [55] vorgeschlagenen Operators, der $M_k(\Gamma_n)$ mit $M_k(\Gamma_{n-1})$ in Verbindung setzt [35, S. 54], [55, S. 636 – 638]. Als Nebenprodukt des vierten Kapitels können einige Vektorräume explizit angegeben werden.

Siegels eigene Ausführungen dienten als Anlass für viele Mathematiker, die Siegelschen Modulformen genauer zu untersuchen: So war es Koecher, der 1954 in [36] darauf hinwies, dass eine Wachstumsbedingung in der Definition der Siegelschen Modulformen, wie sie Siegel in [55] stellte, für $n \geq 2$ überflüssig ist [36, S. 399].

Die Arbeit weiterer Mathematiker wie Andrianov [2], Eichler [11], Freitag [15], Igusa [26], Klingen [34] und Maaß [44] sowie deren Lehrbücher [3], [16], [28], [35], [47] sorgten dafür, dass Siegelsche Modulformen fundamentale Bedeutung in Zahlentheorie und algebraischer Geometrie erlangten [21, S. 181], [22, S. 7, 8].

Anwendung finden Siegelsche Modulformen beispielsweise in der String – Theorie [8] und in der Kodierungstheorie [9].

1.3 Notation

[3, S. 2, 3, 74], [16, S. 9 – 11, 24, 31, 36, 39, 45], [21, S. 187 – 189, 192], [31, S. 147, 192], [32, S. 4, 6, 16, 17, 19, 24, 33], [60, S. 9], [62, S. 10, 13, 22, 40]

- Die üblichen Zahlenmengen bezeichnen wir mit \mathbb{N} (Natürliche Zahlen), \mathbb{Z} (Ganze Zahlen), \mathbb{Q} (Rationale Zahlen), \mathbb{R} (Reelle Zahlen) und \mathbb{C} (Komplexe Zahlen). Insbesondere seien

$$\mathbb{N} = \{1, 2, 3, \dots\} = \mathbb{Z}_{>0} \quad \text{und} \quad \mathbb{N}_0 = \{0, 1, 2, 3, \dots\} = \mathbb{Z}_{\geq 0}.$$

- Die Teilmengeninklusion „ \subset “ beinhaltet stets auch die Möglichkeit, dass die Mengen gleich sind.
- Die Kardinalität einer Menge A wird mit $|A|$ bezeichnet.
- Die Menge der $m \times n$ – Matrizen mit Einträgen aus einem kommutativen Ring R mit Eins bezeichnen wir mit $M_{m,n}(R)$. Die Einträge einer Matrix $a \in M_{m,n}(R)$ sind $a_{\ell,r}$, $1 \leq \ell \leq m$, $1 \leq r \leq n$. Die Nullmatrix in $M_{m,n}(R)$ wird mit 0 bezeichnet.
- $a = (a_1 | \dots | a_n)$ ist die spaltenweise Darstellung einer Matrix $a \in M_{m,n}(R)$.
- a^T bezeichnet die transponierte Matrix von $a \in M_{m,n}(R)$.
- Statt $M_{m,m}(R)$ schreiben wir kurz $M_m(R)$. I_m ist die Einheitsmatrix in $M_m(R)$.
- Für $0 \leq r \leq m$ kann eine quadratische Matrix $a \in M_m(R)$ geschrieben werden als

$$\begin{pmatrix} a_1^{(r)} & a_2^{(r)} \\ a_3^{(r)} & a_4^{(r)} \end{pmatrix} \tag{1.3}$$

mit $a_1^{(r)} \in M_r(R)$, $a_2^{(r)} \in M_{r,m-r}(R)$, $a_3^{(r)} \in M_{m-r,r}(R)$, $a_4^{(r)} \in M_{m-r}(R)$.

- Sei $z \in M_{m,n}(\mathbb{C})$. Dann meinen wir mit Zerlegungen der Form $z = x + iy$ immer, dass x der (elementweise gebildete) Realteil von z ist und y der (elementweise gebildete) Imaginärteil von z ist.
- Elemente aus $R^m = M_{m,1}(R)$ sind Vektoren, die wir als $v = \begin{pmatrix} v_1 \\ \vdots \\ v_m \end{pmatrix} = (v_1, \dots, v_m)^T$ notieren.
- Für $z \in M_m(\mathbb{C})$ und $w \in M_{m,n}(\mathbb{C})$ benutzen wir die Abkürzungen $z[w] = w^T \cdot z \cdot w$ und $z\{w\} = w^T \cdot z \cdot \bar{w}$ (Notationen 2.1.1 und 2.4.2).
- $z \in M_m(\mathbb{C})$ heißt symmetrisch, falls $z^T = z$ gilt. Sie ist hermitesch, wenn sie $\bar{z}^T = z$ erfüllt.
- Die Bezeichnungen „ \geq “ respektive „ $>$ “ benutzen wir für positive Semidefinitheit respektive positive Definitheit (Definitionen 2.1.3 und 2.4.4, Bemerkungen 2.1.5(a) und 2.4.5(a)).

- Es ist $\text{GL}_m(\mathbb{K}) = \{a \in M_m(\mathbb{K}) \mid \det(a) \neq 0\}$ für einen Körper \mathbb{K} . Die unimodulare Gruppe

$$\text{GL}_m(\mathbb{Z}) = \{u \in M_m(\mathbb{Z}) \mid \text{es gibt ein } v \in M_m(\mathbb{Z}) \text{ mit } uv = vu = I_m\}$$

wird in Lemma 2.5.4 untersucht.

- Die Spur einer Matrix $a \in M_m(R)$ wird mit $\text{Spur}(a) = \sum_{r=1}^m a_{r,r}$ bezeichnet.

- $\|z\|$ bezeichnet die Euklidische Norm $\|z\| = \left(\sum_{r=1}^m |z_r|^2 \right)^{\frac{1}{2}}$ eines Vektors $z \in \mathbb{C}^m$.

- Eine symmetrische Matrix $a \in M_m(\mathbb{R})$ heißt gerade, falls sie nur ganze Einträge hat und ihre Diagonalelemente gerade sind (Definition 2.2.3). Die Hälfte einer geraden Matrix nennen wir halbganz (Definition 2.2.9).

- Für eine symmetrische und positiv definite Matrix $a \in M_m(\mathbb{R})$ und eine Matrix $t \in M_n(\mathbb{R})$ sind die Darstellungszahlen gegeben durch (Definition 2.2.6)

$$r_a(t) = \left| \left\{ g \in M_{m,n}(\mathbb{Z}) \mid \frac{1}{2}a[g] = t \right\} \right|. \quad (1.4)$$

- $\mathbb{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$.

- Die Menge $\mathbb{H}_n = \{z \in M_n(\mathbb{C}) \mid z^T = z, \text{Im}(z) > 0\}$ ist die Siegelsche Halbebene vom Geschlecht n (Definition 2.2.10). Die Menge \mathbb{P}_n ist gegeben durch $\mathbb{P}_n = \{\text{Im}(z) \mid z \in \mathbb{H}_n\}$.

- $e_n(z) = e^{2\pi i \cdot \text{Spur}(z)}$, $z \in M_n(\mathbb{C})$.

- $\mathbb{A}_n = \{t \in M_n(\mathbb{R}) \mid t^T = t, t \text{ halbganz}, t \geq 0\}$ und $\mathbb{A}_n^+ = \{t \in \mathbb{A}_n \mid t > 0\}$.

- Die ℓ -te Teilerpotenzsumme σ_ℓ ist gegeben durch $\sigma_\ell(t) = \sum_{0 < d \mid t} d^\ell$, $t \in \mathbb{N}$.

- Für $j = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \in M_{2n}(\mathbb{R})$ ist $\text{Sp}_n(\mathbb{R}) = \{m \in M_{2n}(\mathbb{R}) \mid j[m] = j\}$ die symplektische Gruppe vom Geschlecht n über \mathbb{R} (Definition 2.3.1).

- $\text{SL}_n(\mathbb{R}) = \{m \in M_n(\mathbb{R}) \mid \det(m) = 1\}$ und $\text{SL}_n(\mathbb{Z}) = \{m \in M_n(\mathbb{Z}) \mid \det(m) = 1\}$.

- Für $m \in \text{Sp}_n(\mathbb{R})$ und $z \in \mathbb{H}_n$ bezeichnet $m\langle z \rangle$ die zugehörige Möbiustransformation (Satz 2.4.1).

- $\mathcal{K}_n = \{m \in \text{Sp}_n(\mathbb{R}) \mid m\langle iI_n \rangle = iI_n\}$ wird in Lemma 2.4.11 untersucht.

- $\Gamma_n = \text{Sp}_n(\mathbb{Z}) = \{m \in M_{2n}(\mathbb{Z}) \mid j[m] = j\}$ ist die Siegelsche Modulgruppe vom Geschlecht n (Definition 2.5.1 und Bemerkung 2.5.5).

- Für $y \in \mathbb{P}_n$ ist $\mu(y) = \min_{g \in \mathbb{Z}^n \setminus \{0\}} y[g]$ (Bemerkung 3.2.1(a)).

- \mathcal{M}_n bezeichnet die Menge aller minkowskireduzierten $n \times n$ -Matrizen (Definition 3.3.2).

- $G_{\ell,n} = \{(g_1, \dots, g_n)^T \in \mathbb{Z}^n \mid \text{ggT}(g_\ell, \dots, g_n) = 1\}$, $1 \leq \ell \leq n$.
- $\mathcal{F} = \{z \in \mathbb{H} \mid |z| \geq 1, |\text{Re}(z)| \leq \frac{1}{2}\}$.
- \mathcal{F}_n bezeichnet den Siegelschen Fundamentalbereich von Γ_n (Definition 3.5.2).
- $f|_k m$ mit $k \in \mathbb{Z}$ und $m \in \text{Sp}_n(\mathbb{R})$ bezeichnet den Strichoperator von $f : \mathbb{H}_n \rightarrow \mathbb{C}$ (Definition 4.1.1).
- $M_k(\Gamma_n)$ ist der Vektorraum der Siegelschen Modulformen vom Geschlecht n und Gewicht k über \mathbb{C} (Definition 4.1.3 und Bemerkung 4.1.5(a)). $S_k(\Gamma_n)$ ist der Vektorraum der Siegelschen Spitzenformen vom Geschlecht n und Gewicht k über \mathbb{C} (Definition 4.5.1).
- $f|\Phi$ bezeichnet den Siegelschen Operator von $f \in M_k(\Gamma_n)$ (Beispiel 4.4.6).
- Die Gauß – Klammer ist $[x] = \max_{\substack{k \in \mathbb{Z} \\ k \leq x}} k$ für $x \in \mathbb{R}$.

Kapitel 2

Die symplektische Gruppe $\mathrm{Sp}_n(\mathbb{R})$

2.1 Vorbereitungen

Wir folgen [21] und benennen Matrizen in der Regel mit kleinen Buchstaben [21, S. 187, 188].

Als eine nützliche Schreibweise erweist sich zunächst die folgende Notation [3, S. 330, 331], [7, S. 348], [16, S. 12], [38, S. 260], [55, S. 619].

Notation 2.1.1. Seien $z \in M_m(\mathbb{C})$ und $w \in M_{m,n}(\mathbb{C})$. Wir definieren

$$z[w] := w^T \cdot z \cdot w \in M_n(\mathbb{C}).$$

Bemerkung 2.1.2. Seien $z \in M_m(\mathbb{C})$ und $w \in M_{m,n}(\mathbb{C})$.

- (a) Wenn wir die ℓ -te Spalte von w mit w_ℓ bezeichnen, so ergibt sich das (ℓ, r) -te Element ($1 \leq \ell, r \leq n$) von $z[w]$ als

$$(z[w])_{\ell,r} = w_\ell^T \cdot z \cdot w_r$$

und insbesondere $(z[w])_{\ell,\ell} = z[w_\ell]$.

- (b) Ist z symmetrisch ($z^T = z$), dann ist auch $z[w]$ symmetrisch.

Mit Notation 2.1.1 können wir folgende Definition für reelle Matrizen angeben [3, S. 330, 331], [7, S. 348], [16, S. 12], [38, S. 260], [55, S. 619].

Definition 2.1.3. Sei $a \in M_m(\mathbb{R})$ symmetrisch. Wir nennen a *positiv semidefinit*, falls

$$a[v] = v^T \cdot a \cdot v \geq 0 \quad \text{für alle } v \in \mathbb{R}^m \text{ gilt.}$$

Falls sogar $a[v] > 0$ für alle $v \in \mathbb{R}^m \setminus \{0\}$ gilt, heißt a *positiv definit*.

Beispiel 2.1.4. [3, S. 331] Sei $d = \mathrm{diag}(\lambda_1, \dots, \lambda_m) \in M_m(\mathbb{R})$ eine Diagonalmatrix. Aus

$$d[v] = \sum_{r=1}^m \lambda_r v_r^2 \quad \text{für } v = (v_1, \dots, v_m)^T \in \mathbb{R}^m$$

ergibt sich, dass d genau dann positiv semidefinit (respektive positiv definit) ist, wenn

$$\lambda_1, \dots, \lambda_m \geq 0 \quad (\text{respektive } \lambda_1, \dots, \lambda_m > 0) \text{ gilt.}$$

Bemerkung 2.1.5. [3, S. 331], [7, S. 348, 349], [16, S. 12], [38, S. 260, 261]

(a) Seien $a, \tilde{a} \in M_m(\mathbb{R})$ symmetrisch. Um auszudrücken, dass $a - \tilde{a}$ positiv semidefinit (beziehungsweise positiv definit) ist, schreiben wir manchmal kurz $a \geq \tilde{a}$ (beziehungsweise $a > \tilde{a}$).

(b) Aus $(a + \tilde{a})[v] = a[v] + \tilde{a}[v]$ für symmetrische $a, \tilde{a} \in M_m(\mathbb{R})$ und $v \in \mathbb{R}^m$ folgt

$$\begin{aligned} a + \tilde{a} \geq 0, & \quad \text{falls } a, \tilde{a} \geq 0; \\ \text{und } a + \tilde{a} > 0, & \quad \text{falls } a > 0, \tilde{a} \geq 0. \end{aligned}$$

(c) Sei $a \in M_m(\mathbb{R})$ symmetrisch und positiv semidefinit und sei $b \in M_{m,n}(\mathbb{R})$. Dann gilt

$$(a[b])[v] = a[bv] \geq 0 \quad \text{für alle } v \in \mathbb{R}^n, \quad (2.1)$$

also ist auch $a[b]$ positiv semidefinit. Wenn a positiv definit und $b \in \mathrm{GL}_m(\mathbb{R})$ invertierbar ist, dann folgt aus (2.1), dass $a[b]$ positiv definit ist.

Entscheidendes Hilfsmittel für weitere Untersuchungen wird der aus der linearen Algebra bekannte folgende Satz sein [3, S. 331], [16, S. 13], [43, S. 83], [62, S. 130, 136].

Satz 2.1.6. *Sei $a \in M_m(\mathbb{R})$ symmetrisch. Dann gibt es ein $g \in \mathrm{GL}_m(\mathbb{R})$, $g^T \cdot g = I_m$, und $\lambda_1, \dots, \lambda_m \in \mathbb{R}$ mit*

$$a[g] = \mathrm{diag}(\lambda_1, \dots, \lambda_m).$$

Dabei sind $\lambda_1, \dots, \lambda_m$ die Eigenwerte von a .

Bemerkung 2.1.7. [3, S. 331], [16, S. 13], [38, S. 261]

Aus Beispiel 2.1.4, Bemerkung 2.1.5(c) und Satz 2.1.6 folgt, dass ein symmetrisches $a \in M_m(\mathbb{R})$ genau dann positiv semidefinit (respektive positiv definit) ist, wenn alle Eigenwerte nichtnegativ (respektive positiv) sind.

Bezeichnen wir die Spur einer Matrix $z \in M_m(\mathbb{C})$ mit $\mathrm{Spur}(z) = \sum_{r=1}^m z_{r,r}$, so haben wir

Lemma 2.1.8. [42, S. 172], [62, S. 73] *Für $z \in M_{n,m}(\mathbb{C})$ und $w \in M_{m,n}(\mathbb{C})$ gilt*

$$\mathrm{Spur}(zw) = \mathrm{Spur}(wz).$$

Beweis. Wir schreiben

$$\mathrm{Spur}(zw) = \sum_{r=1}^n (zw)_{r,r} = \sum_{r=1}^n \sum_{\ell=1}^m z_{r,\ell} w_{\ell,r} = \sum_{\ell=1}^m \sum_{r=1}^n w_{\ell,r} z_{r,\ell} = \sum_{\ell=1}^m (wz)_{\ell,\ell} = \mathrm{Spur}(wz). \quad \square$$

Korollar 2.1.9. [38, S. 261], [42, S. 172] *Für jedes symmetrische $a \in M_m(\mathbb{R})$ mit Eigenwerten $\lambda_1, \dots, \lambda_m$ gilt*

$$\mathrm{Spur}(a) = \sum_{r=1}^m \lambda_r \quad \text{sowie} \quad \det(a) = \prod_{r=1}^m \lambda_r.$$

Beweis. Nach Satz 2.1.6 gibt es ein $g \in \mathrm{GL}_m(\mathbb{R})$ mit den Eigenschaften $g^T \cdot g = I_m$ und $a[g] = \mathrm{diag}(\lambda_1, \dots, \lambda_m)$. Wegen Lemma 2.1.8 erhalten wir

$$\sum_{r=1}^m \lambda_r = \mathrm{Spur}(a[g]) = \mathrm{Spur}(g^T \cdot ag) = \mathrm{Spur}(ag \cdot g^T) = \mathrm{Spur}(a).$$

Der zweite Teil des Korollars ergibt sich aus

$$\prod_{r=1}^m \lambda_r = \det(a[g]) = \det(g^T) \cdot \det(a) \cdot \det(g) = \det(a) \cdot \det(g^T \cdot g) = \det(a). \quad \square$$

Bemerkung 2.1.10. [16, S. 16], [38, S. 261] Sei $a \in M_m(\mathbb{R})$ symmetrisch und positiv definit. Nach Bemerkung 2.1.7 und Korollar 2.1.9 hat a eine positive Determinante und ist daher invertierbar. Bemerkung 2.1.5(c) ergibt nun, dass auch $a^{-1} = a[a^{-1}]$ positiv definit ist.

Korollar 2.1.11. [7, S. 349], [16, S. 13], [38, S. 261]

Sei $a \in M_m(\mathbb{R})$ symmetrisch und positiv semidefinit (respektive positiv definit). Dann gibt es eine symmetrische und positiv semidefinites (respektive positiv definites) $b \in M_m(\mathbb{R})$ mit $b^2 = a$.

In späteren Abschnitten verwenden wir das Korollar meist in der folgenden Fassung: Sei $a \in M_m(\mathbb{R})$ symmetrisch und positiv definit. Dann gibt es ein $b \in \mathrm{GL}_m(\mathbb{R})$ mit $b^T \cdot b = a$.

Beweis des Korollars 2.1.11. Nach Satz 2.1.6 und Bemerkung 2.1.7 existieren ein $g \in \mathrm{GL}_m(\mathbb{R})$, $g^T \cdot g = I_m$, und $\lambda_1, \dots, \lambda_m \geq 0$ (respektive $\lambda_1, \dots, \lambda_m > 0$) mit

$$a[g] = \mathrm{diag}(\lambda_1, \dots, \lambda_m).$$

Definieren wir $b := \mathrm{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_m})[g^{-1}] \in M_m(\mathbb{R})$, so ist b (nach Bemerkungen 2.1.2(b) und 2.1.5(c) sowie Beispiel 2.1.4) eine symmetrische und positiv semidefinite (respektive positiv definite) Matrix. Wegen $g^T \cdot g = I_m$ erhalten wir

$$\begin{aligned} b^2 &= (g^{-1})^T \cdot \mathrm{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_m}) \cdot g^{-1} \cdot (g^{-1})^T \cdot \mathrm{diag}(\sqrt{\lambda_1}, \dots, \sqrt{\lambda_m}) \cdot g^{-1} \\ &= (g^{-1})^T \cdot \mathrm{diag}(\lambda_1, \dots, \lambda_m) \cdot g^{-1} = \mathrm{diag}(\lambda_1, \dots, \lambda_m)[g^{-1}] = (a[g])[g^{-1}] = a[gg^{-1}] = a. \quad \square \end{aligned}$$

Korollar 2.1.12. [3, S. 331], [16, S. 13], [38, S. 261, 262]

Seien $a, \tilde{a} \in M_m(\mathbb{R})$ zwei symmetrische und positiv semidefinite Matrizen. Dann gilt

$$\mathrm{Spur}(a\tilde{a}) \geq 0.$$

Beweis. Gemäß Korollar 2.1.11 gibt es ein $b \in M_m(\mathbb{R})$ mit $b \cdot b^T = a$. Daraus folgt

$$\mathrm{Spur}(a\tilde{a}) = \mathrm{Spur}(b \cdot b^T \tilde{a}) = \mathrm{Spur}(b^T \tilde{a} \cdot b) = \mathrm{Spur}(\tilde{a}[b]) = \sum_{r=1}^m (\tilde{a}[b])_{r,r} = \sum_{r=1}^m (\tilde{a}[b_r]) \geq 0,$$

wobei b_r die r -te Spalte von b bezeichnet. □

Bemerkung 2.1.13. [3, S. 331] Für symmetrische Matrizen $a, \tilde{a}, a^* \in M_m(\mathbb{R})$ mit $a \geq \tilde{a}$ und $a^* \geq 0$ gilt $\mathrm{Spur}((a - \tilde{a}) \cdot a^*) \geq 0$ und daher $\mathrm{Spur}(aa^*) \geq \mathrm{Spur}(\tilde{a}a^*)$.

2.2 Darstellungszahlen und Thetafunktionen

Mithilfe von Satz 2.1.6 können wir jede positiv definite Matrix mit positiven Vielfachen der Einheitsmatrix vergleichen [16, S. 13], [38, S. 261, 262].

Korollar 2.2.1. *Sei $a \in M_m(\mathbb{R})$ symmetrisch und positiv definit. Dann gibt es positive reelle Zahlen $\delta_1, \delta_2 > 0$ mit*

$$\delta_2 I_m > a > \delta_1 I_m.$$

Beweis. Nach Satz 2.1.6 und Bemerkung 2.1.7 gibt es $g \in \mathrm{GL}_m(\mathbb{R})$, $g^T \cdot g = I_m$, und positive $\lambda_1, \dots, \lambda_m > 0$ mit

$$a[g] = \mathrm{diag}(\lambda_1, \dots, \lambda_m).$$

Wir wählen nun $\delta_1, \delta_2 > 0$ mit den Eigenschaften

$$\delta_1 < \min\{\lambda_1, \dots, \lambda_m\} \quad \text{und} \quad \delta_2 > \max\{\lambda_1, \dots, \lambda_m\}.$$

Dann ist $\delta_2 I_m > \mathrm{diag}(\lambda_1, \dots, \lambda_m) > \delta_1 I_m$ nach Beispiel 2.1.4. Wenden wir darauf $[g^{-1}]$ an, so folgt mit Bemerkung 2.1.5(c)

$$\delta_2 I_m [g^{-1}] > \mathrm{diag}(\lambda_1, \dots, \lambda_m) [g^{-1}] > \delta_1 I_m [g^{-1}].$$

Wegen $g^T \cdot g = I_m$ bedeutet dies genau $\delta_2 I_m > a > \delta_1 I_m$. □

Korollar 2.2.2. [7, S. 349], [16, S. 13], [38, S. 262, 263]

Sei $a \in M_m(\mathbb{R})$ eine symmetrische und positiv definite Matrix und seien $v \in \mathbb{R}^m$ sowie $t \in \mathbb{R}$. Dann gibt es nur endlich viele $g \in \mathbb{Z}^m$ mit der Eigenschaft

$$a[v + g] \leq t.$$

Beweis. Korollar 2.2.1 liefert die Existenz eines $\delta > 0$ mit $a > \delta I_m$. Deshalb gilt

$$a[w] \geq \delta \|w\|^2 \quad \text{für alle } w \in \mathbb{R}^m. \tag{2.2}$$

Sei nun $g \in \mathbb{Z}^m$ mit der Eigenschaft $a[v + g] \leq t$. Aus Formel (2.2) folgt

$$\delta \|v + g\|^2 \leq a[v + g] \leq t \quad \text{und daher} \quad \delta \|v + g\|^2 \leq t.$$

Die rechte Ungleichung kann nun aber nur von endlich vielen $g \in \mathbb{Z}^m$ erfüllt werden. □

Für $t \in \mathbb{R}$ sind insbesondere die Darstellungszahlen

$$r_a(t) := \left| \left\{ g \in \mathbb{Z}^m \mid \frac{1}{2} a[g] = t \right\} \right| \tag{2.3}$$

einer symmetrischen und positiv definiten Matrix $a \in M_m(\mathbb{R})$ endlich [38, S. 262], [51, S. 1]. Diesen sind wir bereits in der Theorie der Thetafunktionen begegnet [61, S. 35].

Wir erinnern dazu an die Definition einer *geraden* Matrix [3, S. 65, 66], [16, S. 43], [21, S. 189], [32, S. 44], [38, S. 272], [61, S. 35], [62, S. 120].

Definition 2.2.3. Eine symmetrische Matrix $a \in M_m(\mathbb{R})$ heißt *gerade*, falls sie nur ganze Einträge hat und ihre Diagonalelemente gerade sind.

Eine Charakterisierung gerader Matrizen liefert uns

Lemma 2.2.4. [37, S. 4], [38, S. 272, 273], [55, S. 619], [61, S. 35], [62, S. 20, 120]
 Für eine symmetrische Matrix $a \in M_m(\mathbb{R})$ sind folgende Aussagen äquivalent:

- (a) a ist gerade.
- (b) Für alle symmetrischen $z \in M_m(\mathbb{C})$ ist $\frac{1}{2}\mathrm{Spur}(az)$ eine ganzzahlige Linearkombination von $z_{\ell,r}$, $1 \leq \ell \leq r \leq m$.
- (c) $\mathrm{Spur}(ab) \in 2\mathbb{Z}$ für alle symmetrischen $b \in M_m(\mathbb{Z})$.
- (d) $a[g] \in 2\mathbb{Z}$ für alle $g \in \mathbb{Z}^m$.
- (e) $a[g]$ ist gerade für alle $g \in M_{m,n}(\mathbb{Z})$.

Beweis. (a) \Rightarrow (b): Für eine symmetrische Matrix $z \in M_m(\mathbb{C})$ ist

$$\frac{1}{2}\mathrm{Spur}(az) = \frac{1}{2} \sum_{r=1}^m (az)_{r,r} = \frac{1}{2} \sum_{r=1}^m \sum_{\ell=1}^m a_{r,\ell} z_{\ell,r} = \sum_{r=1}^m \frac{1}{2} a_{r,r} z_{r,r} + \sum_{1 \leq \ell < r \leq m} a_{r,\ell} z_{\ell,r}. \quad (2.4)$$

Da a gerade ist, ist $\frac{1}{2}\mathrm{Spur}(az)$ eine ganzzahlige Linearkombination von $z_{\ell,r}$, $1 \leq \ell \leq r \leq m$.

(b) \Rightarrow (c): Hierfür brauchen wir lediglich $z = b$ setzen.

(c) \Rightarrow (d): Für $g \in \mathbb{Z}^m$ betrachten wir die symmetrische Matrix $b := g \cdot g^T \in M_m(\mathbb{Z})$, womit

$$2\mathbb{Z} \ni \mathrm{Spur}(ab) = \mathrm{Spur}(ag \cdot g^T) = \mathrm{Spur}(g^T \cdot ag) = \mathrm{Spur}(a[g]) = a[g] \quad \text{folgt.}$$

(d) \Rightarrow (e): Wir zeigen zunächst, dass die Matrix a nur ganze Einträge hat: Dazu seien die kanonischen Einheitsvektoren des \mathbb{Z}^m mit e_1, \dots, e_m bezeichnet. Indem wir $g = e_\ell$, $1 \leq \ell \leq m$, in (d) setzen, folgt $a_{\ell,\ell} = a[e_\ell] \in 2\mathbb{Z}$ für alle $1 \leq \ell \leq m$. Für $1 \leq \ell < r \leq m$ erhalten wir außerdem

$$2\mathbb{Z} \ni a[e_\ell + e_r] = a[e_\ell] + e_\ell^T \cdot a \cdot e_r + e_r^T \cdot a \cdot e_\ell + a[e_r] = a_{\ell,\ell} + 2a_{\ell,r} + a_{r,r}.$$

Aus $a_{\ell,\ell}, a_{r,r} \in 2\mathbb{Z}$ ergibt sich $a_{\ell,r} \in \mathbb{Z}$, $1 \leq \ell < r \leq m$. Also gilt insbesondere $a \in M_m(\mathbb{Z})$.

Für $g \in M_{m,n}(\mathbb{Z})$ ist daher $a[g] \in M_n(\mathbb{Z})$ eine ganze Matrix, deren Diagonalelemente nach (d) und Bemerkung 2.1.2(a) gerade ganze Zahlen sind. Daher ist $a[g]$ eine gerade Matrix.

(e) \Rightarrow (a): Dies folgt sofort, indem $n = m$ und $g = I_m$ gewählt wird. \square

Bemerkung 2.2.5. [3, S. 65, 66], [16, S. 43], [18, S. 449], [21, S. 189], [32, S. 44]

Sei $z \in M_m(\mathbb{C})$ symmetrisch. Die Formel (2.4) zeigt, dass die Abbildung

$$\{a \in M_m(\mathbb{Z}) \mid a^T = a, a \text{ gerade}\} \longrightarrow \{\text{ganzzahlige Linearkombination von } z_{\ell,r}, 1 \leq \ell \leq r \leq m\}$$

$$a \longmapsto \frac{1}{2}\mathrm{Spur}(az)$$

bijektiv ist. Jede ganzzahlige Linearkombination von $z_{\ell,r}$, $1 \leq \ell \leq r \leq m$, kann daher in der Form

$$\frac{1}{2}\mathrm{Spur}(az) \quad \text{für genau eine gerade Matrix } a^T = a \in M_m(\mathbb{Z})$$

geschrieben werden.

Sei $a \in M_m(\mathbb{Z})$ symmetrisch, gerade und positiv definit. Wegen Lemma 2.2.4(d) kann die Thetafunktion

$$\vartheta_a(z) := \sum_{g \in \mathbb{Z}^m} e^{\pi i a[g] \cdot z}, \quad z \in \mathbb{H} := \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}, \quad (2.5)$$

(zunächst einmal nur formal) als

$$\vartheta_a(z) = \sum_{t=0}^{\infty} r_a(t) e^{2\pi i t z} = 1 + r_a(1) e^{2\pi i z} + \mathcal{O}(e^{4\pi i z}), \quad z \in \mathbb{H}, \quad (2.6)$$

geschrieben werden [7, S. 349], [16, S. 14], [61, S. 35].

Wir können die Darstellungszahlen (2.3) auf Matrizen $t \in M_n(\mathbb{R})$ verallgemeinern [32, S. 48], [37, S. 3], [51, S. 2].

Definition 2.2.6. Für eine symmetrische und positiv definite Matrix $a \in M_m(\mathbb{R})$ und eine Matrix $t \in M_n(\mathbb{R})$ definieren wir die Darstellungszahlen

$$r_a(t) := \left| \left\{ g \in M_{m,n}(\mathbb{Z}) \mid \frac{1}{2} a[g] = t \right\} \right|. \quad (2.7)$$

Beispiel 2.2.7. [37, S. 3] Für $t = 0$ ist $r_a(0) = 1$: Um dies einzusehen, betrachten wir $g \in M_{m,n}(\mathbb{Z})$ mit $\frac{1}{2} a[g] = 0$. Bezeichnet g_ℓ die ℓ -Spalte von g , so gilt $a[g_\ell] = 0$ für alle $1 \leq \ell \leq n$. Aus der positiven Definitheit von a folgt $g_\ell = 0$ für alle $1 \leq \ell \leq n$, also $g = 0$.

Bemerkung 2.2.8. [16, S. 17], [37, S. 3], [38, S. 262, 273], [51, S. 2]

- (a) Bezeichnen wir die ℓ -te Spalte von g mit g_ℓ , so erhalten wir aus $\frac{1}{2} a[g] = t$ die Beziehung $\frac{1}{2} a[g_\ell] = t_{\ell,\ell}$ für alle $1 \leq \ell \leq n$. Wegen der Endlichkeit der Darstellungszahlen (2.3) gibt es für jede Spalte von g nur endlich viele Möglichkeiten. Daher sind auch die Darstellungszahlen (2.7) endlich.
- (b) Sei $r_a(t) > 0$. Dann muss $t \in M_n(\mathbb{R})$ symmetrisch und positiv semidefinit sein. Falls zusätzlich a gerade ist, so folgt aus Lemma 2.2.4(e), dass $2t$ gerade ist.

Um eine sogenannte *verallgemeinerte Thetafunktion* untersuchen zu können, erscheint es im Hinblick auf Lemma 2.2.4 sowie Bemerkungen 2.2.5 und 2.2.8(b) sinnvoll, die Hälfte von geraden Matrizen zu betrachten [16, S. 18], [35, S. 44], [37, S. 3], [47, S. 182], [51, S. 2], [55, S. 619].

Definition 2.2.9. Eine symmetrische Matrix $a \in M_m(\mathbb{R})$ heißt *halbganz*, falls $2a$ eine gerade Matrix ist.

Eine natürliche Verallgemeinerung der oberen Halbebene \mathbb{H} von \mathbb{C} stellen wir in der folgenden Definition dar [3, S. 4], [16, S. 18], [37, S. 7, 9], [47, S. 32].

Definition 2.2.10. Die Menge

$$\mathbb{H}_n := \{z \in M_n(\mathbb{C}) \mid z^T = z, \mathrm{Im}(z) > 0\}$$

heißt *Siegelsche Halbebene vom Geschlecht n* .

Beispiel 2.2.11. Für $n = 1$ haben wir $\mathbb{H}_1 = \mathbb{H}$.

Die Imaginärteile der Elemente $z \in \mathbb{H}_n$ bilden die Menge

$$\mathbb{P}_n := \{\mathrm{Im}(z) \mid z \in \mathbb{H}_n\} = \{y \in M_n(\mathbb{R}) \mid y^T = y, y > 0\}.$$

Mit $\{x \in M_n(\mathbb{R}) \mid x^T = x\} \cong \mathbb{R}^{\frac{n(n+1)}{2}}$ können wir folgendes Lemma beweisen [3, S. 8], [16, S. 39], [32, S. 12, 58], [35, S. 10], [37, S. 7], [38, S. 261], [62, S. 143].

Lemma 2.2.12. \mathbb{P}_n ist eine offene und konvexe Teilmenge von $\mathbb{R}^{\frac{n(n+1)}{2}}$ und \mathbb{H}_n ist eine offene und konvexe Teilmenge von $\mathbb{C}^{\frac{n(n+1)}{2}}$.

Beweis. Das *Hauptminoren – Kriterium für die Definitheit* besagt, dass ein symmetrisches $y \in M_n(\mathbb{R})$ genau dann positiv definit ist, wenn alle Hauptminoren positiv sind. Da die Determinante eine stetige Abbildung ist, ist \mathbb{P}_n in $\mathbb{R}^{\frac{n(n+1)}{2}}$ offen.

Aus

$$\mathbb{H}_n \cong \mathbb{R}^{\frac{n(n+1)}{2}} \times \mathbb{P}_n$$

folgt weiter, dass \mathbb{H}_n eine offene Teilmenge von

$$\mathbb{R}^{\frac{n(n+1)}{2}} \times \mathbb{R}^{\frac{n(n+1)}{2}} \cong \mathbb{C}^{\frac{n(n+1)}{2}} \quad \text{ist.}$$

Für $y, y^* \in \mathbb{P}_n$ und $0 \leq \lambda \leq 1$ ist auch $\lambda y + (1 - \lambda)y^* \in \mathbb{P}_n$ wegen Bemerkung 2.1.5(b). Daher sind \mathbb{P}_n und \mathbb{H}_n konvex. \square

Definition 2.2.13. [3, S. 3, 4, 64], [16, S. 18], [32, S. 47], [51, S. 9]

Sei $a \in \mathbb{P}_m$. Dann heißt

$$\vartheta_{a,n}(z) := \sum_{g \in M_{m,n}(\mathbb{Z})} e^{\pi i \cdot \mathrm{Spur}(a[g] \cdot z)}, \quad z \in \mathbb{H}_n,$$

die (verallgemeinerte) *Thetafunktion vom Geschlecht n zu a* .

Mit den Abkürzungen

$$e_n(z) := e^{2\pi i \cdot \mathrm{Spur}(z)}, \quad z \in M_n(\mathbb{C}), \quad (2.8)$$

$$\text{sowie } \mathbb{A}_n := \{t \in M_n(\mathbb{R}) \mid t^T = t, t \text{ halbganz}, t \geq 0\} \quad (2.9)$$

ergibt sich im folgenden Satz der Zusammenhang zwischen verallgemeinerten Thetafunktionen und den Darstellungszahlen [3, S. 3, 4], [7, S. 101], [16, S. 17, 18], [32, S. 47, 48], [35, S. 46], [51, S. 2, 9], [58, S. 55], [61, S. 11].

Satz 2.2.14. Sei $a \in \mathbb{P}_m$. Die *Thetafunktion*

$$\vartheta_{a,n}(z) = \sum_{g \in M_{m,n}(\mathbb{Z})} e_n\left(\frac{1}{2}a[g] \cdot z\right), \quad z \in \mathbb{H}_n,$$

konvergiert absolut in \mathbb{H}_n und ist in jedem Bereich der Form

$$\{z \in \mathbb{H}_n \mid \mathrm{Im}(z) \geq y_0\}, \quad y_0 \in \mathbb{P}_n,$$

gleichmäßig konvergent. Für gerades $a \in \mathbb{P}_m$ ist

$$\vartheta_{a,n}(z) = \sum_{t \in \mathbb{A}_n} r_a(t) e_n(tz), \quad z \in \mathbb{H}_n. \quad (2.10)$$

Beweis. Für $z = x + iy \in \mathbb{H}_n$ und $g \in M_{m,n}(\mathbb{Z})$ ergibt sich

$$\left| e_n \left(\frac{1}{2} a[g] \cdot z \right) \right| = e^{-\pi \cdot \mathrm{Spur}(a[g] \cdot y)}.$$

Nach Korollar 2.2.1 existieren $\varepsilon, \delta > 0$ mit $y_0 > \varepsilon I_n$ und $a > \delta I_m$. Für jedes $g \in M_{m,n}(\mathbb{Z})$ gilt nach Bemerkung 2.1.5(c) somit

$$a[g] \geq \delta \cdot g^T \cdot g.$$

Mit $y = \mathrm{Im}(z) \geq y_0 > \varepsilon I_n$ und Bemerkung 2.1.13 folgt daher

$$\mathrm{Spur}(a[g] \cdot y) \geq \varepsilon \cdot \mathrm{Spur}(a[g]) \geq \varepsilon \delta \cdot \mathrm{Spur}(g^T \cdot g) = \varepsilon \delta \cdot \sum_{r=1}^n \|g_r\|^2,$$

wobei g_r die r -te Spalte von g bezeichnet.

Nun konvergiert die von z unabhängige Majorante

$$\left(\sum_{v \in \mathbb{Z}^m} e^{-\pi \varepsilon \delta \|v\|^2} \right)^n = \left(\sum_{\ell \in \mathbb{Z}} e^{-\pi \varepsilon \delta \ell^2} \right)^{mn} = \left(-1 + 2 \sum_{\ell=0}^{\infty} e^{-\pi \varepsilon \delta \ell^2} \right)^{mn},$$

denn $\sum_{\ell=0}^{\infty} e^{-\pi \varepsilon \delta \ell^2}$ ist eine Teilreihe der geometrischen Reihe $\sum_{\ell=0}^{\infty} (e^{-\pi \varepsilon \delta})^\ell$ mit $|e^{-\pi \varepsilon \delta}| < 1$.

Also ist $\vartheta_{a,n}$ in \mathbb{H}_n absolut konvergent und in $\{z \in \mathbb{H}_n \mid \mathrm{Im}(z) \geq y_0\}$ gleichmäßig konvergent.

Die Darstellung (2.10) für die Thetafunktion einer geraden Matrix a folgt unter Verwendung der Bemerkung 2.2.8(b). \square

Wir erhalten damit auch

Satz 2.2.15. [3, S. 4], [16, S. 17, 18], [32, S. 47, 48], [51, S. 2, 9]

Sei $a \in \mathbb{P}_m$. Die Thetafunktion $\vartheta_{a,n}$ stellt in \mathbb{H}_n eine holomorphe Funktion dar. Sie ist in jedem Bereich der Form $\{z \in \mathbb{H}_n \mid \mathrm{Im}(z) \geq y_0\}$, $y_0 \in \mathbb{P}_n$, beschränkt.

Für gerades $a \in \mathbb{P}_m$ und $n = 1$ erhalten wir die Thetafunktion (2.5) mit ihrer in \mathbb{H} gültigen Darstellung (2.6).

Beispiel 2.2.16. [37, S. 3], [38, S. 201, 202], [49, S. 198], [51, S. 2, 103], [60, S. 8, 9, 36, 44, 49, 53], [61, S. 36, 38]

Aus der Theorie der Modulformen wissen wir $\dim_{\mathbb{C}}(M_2(\Gamma_0(4))) \leq 2$. Für

$$G_2(z) := -\frac{1}{24} + \sum_{t=1}^{\infty} \sigma_1(t) e^{2\pi i t z} = -\frac{1}{24} + e^{2\pi i z} + \mathcal{O}(e^{4\pi i z}), \quad z \in \mathbb{H},$$

sind nun aber

$$\begin{aligned} M_2(\Gamma_0(4)) \ni \Lambda_2(z) &:= G_2(z) - 2G_2(2z) = \frac{1}{24} + e^{2\pi i z} + \mathcal{O}(e^{4\pi i z}), \quad z \in \mathbb{H}, \\ M_2(\Gamma_0(4)) \ni \Lambda_4(z) &:= G_2(z) - 4G_2(4z) = \frac{1}{8} + e^{2\pi i z} + \mathcal{O}(e^{4\pi i z}), \quad z \in \mathbb{H}, \end{aligned}$$

linear unabhängig und bilden daher eine Basis von $M_2(\Gamma_0(4))$.

Wir betrachten die Modulform

$$\begin{aligned} M_2(\Gamma_0(4)) \ni (\vartheta_{2I_2})^2(z) &= \left(\sum_{g_1, g_2 \in \mathbb{Z}} e^{2\pi i(g_1^2 + g_2^2)z} \right)^2 = \sum_{g_1, \dots, g_4 \in \mathbb{Z}} e^{2\pi i(g_1^2 + \dots + g_4^2)z} \\ &= 1 + 8e^{2\pi iz} + \mathcal{O}(e^{4\pi iz}), \quad z \in \mathbb{H}, \end{aligned}$$

die wir als Linearkombination der Basiselemente darstellen: Um $\alpha, \beta \in \mathbb{C}$ mit der Eigenschaft $(\vartheta_{2I_2})^2 = \alpha\Lambda_2 + \beta\Lambda_4$ zu bestimmen, vergleichen wir die ersten beiden Koeffizienten und erhalten das lineare Gleichungssystem

$$\begin{aligned} 1 &= \frac{1}{24}\alpha + \frac{1}{8}\beta, \\ 8 &= \alpha + \beta, \end{aligned}$$

also $\alpha = 0$, $\beta = 8$ und $(\vartheta_{2I_2})^2 = 8\Lambda_4$. Daraus folgt für alle $t \in \mathbb{N}$ dann

$$|\{g_1, \dots, g_4 \in \mathbb{Z} \mid g_1^2 + \dots + g_4^2 = t\}| = \begin{cases} 8 \cdot \sigma_1(t), & \text{wenn } 4 \nmid t, \\ 8 \cdot (\sigma_1(t) - 4 \cdot \sigma_1(\frac{t}{4})), & \text{wenn } 4 \mid t. \end{cases}$$

Dies können wir schließlich schreiben als

$$|\{g_1, \dots, g_4 \in \mathbb{Z} \mid g_1^2 + \dots + g_4^2 = t\}| = 8 \cdot \sum_{\substack{0 < d \mid t \\ 4 \nmid d}} d, \quad t \in \mathbb{N}. \quad (2.11)$$

Die Formel (2.11), die die Anzahl der Darstellungen von t als Summe vierer Quadrate angibt, geht auf Jacobi [30] zurück [21, S. 27, 100], [51, S. 2].

Insbesondere folgt

Korollar 2.2.17 (Satz von Lagrange). [21, S. 27, 100], [38, S. 202], [51, S. 2]
Jede natürliche Zahl ist als Summe vierer Quadrate darstellbar.

Vermutet wurde diese Aussage bereits 1621 von Bachet; Euler konnte sie 1748 auf Primzahlen reduzieren. Da der erste vollständige Beweis aber auf Lagrange aus dem Jahr 1770 zurückgeht, trägt das Korollar seinen Namen [38, S. 202], [50, S. 198], [56, S. 421].

2.3 Die symplektische Gruppe $\mathrm{Sp}_n(\mathbb{R})$

Definition 2.3.1. [3, S. 6], [35, S. 1], [37, S. 6], [47, S. 31], [54, S. 596]

Sei $j := \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \in M_{2n}(\mathbb{R})$. Wir definieren

$$\mathrm{Sp}_n(\mathbb{R}) := \{m \in M_{2n}(\mathbb{R}) \mid j[m] = j\}.$$

Im Hinblick auf die Zerlegung von j in $n \times n$ -Blöcke schreiben wir auch $m \in M_{2n}(\mathbb{R})$ als $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ mit $a, b, c, d \in M_n(\mathbb{R})$.

Beispiel 2.3.2. [3, S. 5], [32, S. 13], [37, S. 6]

(a) Für $m = \begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix} \in M_{2n}(\mathbb{R})$ mit einer symmetrischen Matrix $b \in M_n(\mathbb{R})$ ist

$$j[m] = m^T \cdot j \cdot m = \begin{pmatrix} I_n & 0 \\ b & I_n \end{pmatrix} \cdot \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \cdot \begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix} = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} = j,$$

also gilt $m = \begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$.

(b) Aus

$$j^2 = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}^2 = \begin{pmatrix} -I_n & 0 \\ 0 & -I_n \end{pmatrix} = -I_{2n}$$

folgt

$$j[j] = j^T \cdot j^2 = -j^T = j.$$

Dies bedeutet $j \in \mathrm{Sp}_n(\mathbb{R})$.

(c) Für $m = \begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix} \in M_{2n}(\mathbb{R})$ mit $u \in \mathrm{GL}_n(\mathbb{R})$ gilt

$$j[m] = m^T \cdot j \cdot m = \begin{pmatrix} u & 0 \\ 0 & (u^{-1})^T \end{pmatrix} \cdot \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \cdot \begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix} = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} = j.$$

Dies heißt $m = \begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$.

Bemerkung 2.3.3. [21, S. 186], [35, S. 2], [37, S. 7], [47, S. 31, 32]

(a) Da j invertierbar ist, erfüllt jedes $m \in \mathrm{Sp}_n(\mathbb{R})$ die Bedingung $(\det(m))^2 = 1$, also $\det(m) = \pm 1$.

(b) Wir werden sogar später feststellen, dass $\det(m) = 1$ für alle $m \in \mathrm{Sp}_n(\mathbb{R})$ gilt. Dies bedeutet

$$\mathrm{Sp}_n(\mathbb{R}) \subset \mathrm{SL}_{2n}(\mathbb{R}) = \{m \in M_{2n}(\mathbb{R}) \mid \det(m) = 1\}.$$

Aus Bemerkung 2.3.3(a) folgt insbesondere $\mathrm{Sp}_n(\mathbb{R}) = \{m \in \mathrm{GL}_{2n}(\mathbb{R}) \mid j[m] = j\}$.

Lemma 2.3.4. [32, S. 4, 5], [35, S. 1], [37, S. 6]

$\mathrm{Sp}_n(\mathbb{R})$ ist eine Untergruppe von $\mathrm{GL}_{2n}(\mathbb{R})$.

$\mathrm{Sp}_n(\mathbb{R})$ heißt die *symplektische Gruppe vom Geschlecht n über \mathbb{R}* [35, S. 1].

Beweis des Lemmas 2.3.4. Offensichtlich gilt $j[I_{2n}] = j$ und daher $I_{2n} \in \mathrm{Sp}_n(\mathbb{R})$.

Seien nun $m, \tilde{m} \in \mathrm{Sp}_n(\mathbb{R})$. Aus $j[\tilde{m}] = j$ folgt $j = j[\tilde{m}^{-1}]$ und

$$j[m\tilde{m}^{-1}] = (j[m])[\tilde{m}^{-1}] = j[\tilde{m}^{-1}] = j.$$

Also ist $m\tilde{m}^{-1} \in \mathrm{Sp}_n(\mathbb{R})$. □

Eine Charakterisierung von symplektischen Matrizen gibt der folgende Satz an [16, S. 25], [32, S. 4, 5], [51, S. 3, 103, 104].

Lemma 2.3.5. Sei $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2n}(\mathbb{R})$ mit Blöcken $a, b, c, d \in M_n(\mathbb{R})$. Dann sind die folgenden Aussagen äquivalent:

(a) $m \in \mathrm{Sp}_n(\mathbb{R})$.

(b) $m^T \in \mathrm{Sp}_n(\mathbb{R})$.

(c) $m \in \mathrm{GL}_{2n}(\mathbb{R})$ und $m^{-1} = \begin{pmatrix} d^T & -b^T \\ -c^T & a^T \end{pmatrix}$.

(d) Die Blöcke a, b, c, d erfüllen

$$a^T \cdot c = c^T \cdot a, \quad b^T \cdot d = d^T \cdot b, \quad a^T \cdot d - c^T \cdot b = I_n.$$

(e) Die Blöcke a, b, c, d erfüllen

$$a \cdot b^T = b \cdot a^T, \quad c \cdot d^T = d \cdot c^T, \quad a \cdot d^T - b \cdot c^T = I_n.$$

Beweis. (a) \Leftrightarrow (b): Aus der Untergruppeneigenschaft von $\mathrm{Sp}_n(\mathbb{R}) \subset \mathrm{GL}_{2n}(\mathbb{R})$ erhalten wir die Äquivalenz

$$m \in \mathrm{Sp}_n(\mathbb{R}) \Leftrightarrow m^{-1} \in \mathrm{Sp}_n(\mathbb{R}) \Leftrightarrow (m^{-1})^T \cdot j \cdot m^{-1} = j[m^{-1}] = j \Leftrightarrow m \cdot j^{-1} \cdot m^T = j^{-1}.$$

Wegen $j^{-1} = -j$ ist dies gleichbedeutend mit $m \cdot j \cdot m^T = j$ und $m^T \in \mathrm{Sp}_n(\mathbb{R})$.

(a) \Leftrightarrow (d): Wir berechnen

$$j[m] = \begin{pmatrix} a^T & c^T \\ b^T & d^T \end{pmatrix} \cdot \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} c^T \cdot a - a^T \cdot c & c^T \cdot b - a^T \cdot d \\ d^T \cdot a - b^T \cdot c & d^T \cdot b - b^T \cdot d \end{pmatrix}.$$

Wegen $d^T \cdot a - b^T \cdot c = (a^T \cdot d - c^T \cdot b)^T$ folgt die Äquivalenz.

(b) \Leftrightarrow (e): Die gerade bewiesene Äquivalenz (a) \Leftrightarrow (d), angewandt auf $m^T = \begin{pmatrix} a^T & c^T \\ b^T & d^T \end{pmatrix}$ statt m , liefert uns (b) \Leftrightarrow (e).

(a) \Leftrightarrow (c): Zunächst berechnen wir

$$-j \cdot m^T \cdot j = \begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix} \cdot \begin{pmatrix} a^T & c^T \\ b^T & d^T \end{pmatrix} \cdot \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} = \begin{pmatrix} d^T & -b^T \\ -c^T & a^T \end{pmatrix}.$$

Damit erhalten wir die Äquivalenz

$$m^{-1} = \begin{pmatrix} d^T & -b^T \\ -c^T & a^T \end{pmatrix} \Leftrightarrow -j \cdot m^T \cdot j = m^{-1} \Leftrightarrow -j = m^{-1} \cdot j^{-1} \cdot (m^T)^{-1} \Leftrightarrow -j^{-1} = m^T \cdot j \cdot m.$$

Wegen $j^{-1} = -j$ bedeutet dies genau $j = j[m]$ und $m \in \mathrm{Sp}_n(\mathbb{R})$. \square

Beispiel 2.3.6. [16, S. 25] Lemma 2.3.5(d) liefert im Fall $n = 1$ sogar die Gleichheit

$$\mathrm{Sp}_1(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R}) \mid ad - bc = 1 \right\} = \mathrm{SL}_2(\mathbb{R}).$$

2.4 Die Operation von $\mathrm{Sp}_n(\mathbb{R})$ auf \mathbb{H}_n

Aus der Theorie der klassischen Modulformen ist bereits bekannt, dass $\mathrm{SL}_2(\mathbb{R})$ auf \mathbb{H} durch Möbiustransformationen

$$\begin{aligned} \mathrm{SL}_2(\mathbb{R}) \times \mathbb{H} &\longrightarrow \mathbb{H} \\ (m, z) &\longmapsto \frac{az + b}{cz + d} \end{aligned}$$

für $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ operiert [16, S. 22], [32, S. 11], [60, S. 2].

Dies verallgemeinern wir im folgenden Satz auf die symplektische Gruppe $\mathrm{Sp}_n(\mathbb{R})$ und die Siegelsche Halbebene \mathbb{H}_n [21, S. 184], [28, S. 194], [32, S. 12, 13], [35, S. 2, 3], [45, S. 19, 20].

Satz 2.4.1. *Die symplektische Gruppe $\mathrm{Sp}_n(\mathbb{R})$ operiert auf \mathbb{H}_n durch Möbiustransformationen*

$$\begin{aligned} \mathrm{Sp}_n(\mathbb{R}) \times \mathbb{H}_n &\longrightarrow \mathbb{H}_n \\ (m, z) &\longmapsto m\langle z \rangle := (az + b)(cz + d)^{-1} \end{aligned}$$

für $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Vor dem Beweis müssen wir zunächst auf *hermitesche Matrizen* und ihre Definitheit eingehen. Dazu führen wir die folgende Schreibweise ein [16, S. 298].

Notation 2.4.2. Für $z \in M_m(\mathbb{C})$ und $w \in M_{m,n}(\mathbb{C})$ schreiben wir

$$z\{w\} := w^T \cdot z \cdot \bar{w} \in M_n(\mathbb{C}).$$

Bemerkung 2.4.3. [16, S. 298] Ist z hermitesch ($\bar{z}^T = z$), so ist auch $z\{w\}$ hermitesch. Für $w \in \mathbb{C}^m$ ist daher $z\{w\} \in \mathbb{R}$.

Definition 2.4.4. [3, S. 330, 331], [7, S. 348], [16, S. 12, 298], [38, S. 260], [55, S. 619] Sei $z \in M_m(\mathbb{C})$ hermitesch. Wir nennen z *positiv semidefinit*, falls

$$z\{w\} \geq 0 \quad \text{für alle } w \in \mathbb{C}^m \text{ gilt.}$$

Falls sogar $z\{w\} > 0$ für alle $w \in \mathbb{C}^m \setminus \{0\}$ gilt, so heißt z *positiv definit*.

Bemerkung 2.4.5. [16, S. 298]

- (a) Die Bemerkung 2.1.5 überträgt sich sinngemäß auf hermitesche Matrizen.
- (b) Für eine symmetrische Matrix $a \in M_m(\mathbb{R})$ und $w = s + it \in \mathbb{C}^m$ berechnen wir

$$\begin{aligned} a\{w\} &= (s + it)^T \cdot a \cdot \overline{(s + it)} = (s^T + it^T) \cdot a \cdot (s - it) \\ &= a[s] + i \cdot (t^T \cdot a \cdot s - s^T \cdot a \cdot t) + a[t] = a[s] + a[t]. \end{aligned}$$

Daher ist a genau dann positiv semidefinit (respektive positiv definit) im Sinne von Definition 2.4.4, wenn a positiv semidefinit (respektive positiv definit) im Sinne von Definition 2.1.3 ist.

Beweis des Satzes 2.4.1. Seien $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$ und $z = x + iy \in \mathbb{H}_n$. Wir führen die Abkürzungen $p := az + b$ sowie $q := cz + d$ ein und bestimmen

$$\begin{aligned} p^T \cdot \bar{q} - q^T \cdot \bar{p} &= (z \cdot a^T + b^T)(c \cdot \bar{z} + d) - (z \cdot c^T + d^T)(a \cdot \bar{z} + b) \\ &= z \cdot (a^T \cdot c - c^T \cdot a) \cdot \bar{z} + z \cdot (a^T \cdot d - c^T \cdot b) - (d^T \cdot a - b^T \cdot c) \cdot \bar{z} + (b^T \cdot d - d^T \cdot b). \end{aligned}$$

Unter Verwendung von Lemma 2.3.5(d) und $d^T \cdot a - b^T \cdot c = (a^T \cdot d - c^T \cdot b)^T$ ergibt sich

$$p^T \cdot \bar{q} - q^T \cdot \bar{p} = z - \bar{z} = 2i \cdot y. \quad (2.12)$$

Hiermit zeigen wir zunächst, dass q invertierbar ist. Dazu sei $v \in \mathbb{C}^n$ mit $qv = 0$. Aus (2.12) folgern wir

$$2i \cdot y\{v\} = 2i \cdot v^T \cdot y \cdot \bar{v} = v^T \cdot (p^T \cdot \bar{q} - q^T \cdot \bar{p}) \cdot \bar{v} = (pv)^T \cdot \overline{(qv)} - (qv)^T \cdot \overline{(pv)} = 0.$$

Da y positiv definit ist, muss $v = 0$ gelten. Dies beweist die Invertierbarkeit von q .

Nun wollen wir $m\langle z \rangle \in \mathbb{H}_n$ zeigen. Mithilfe von Lemma 2.3.5(d) schreiben wir hierfür

$$\begin{aligned} ((m\langle z \rangle)^T - m\langle z \rangle)[q] &= q^T \cdot ((q^{-1})^T \cdot p^T - p \cdot q^{-1}) \cdot q = p^T \cdot q - q^T \cdot p \\ &= z \cdot (a^T \cdot c - c^T \cdot a) \cdot z + z \cdot (a^T \cdot d - c^T \cdot b) - (d^T \cdot a - b^T \cdot c) \cdot z + (b^T \cdot d - d^T \cdot b) \\ &= z - z = 0. \end{aligned}$$

Weil q invertierbar ist, ergibt sich daraus die Symmetrie von $m\langle z \rangle$.

Zur Untersuchung von $\mathrm{Im}(m\langle z \rangle)$ verwenden wir (2.12) und erhalten

$$\begin{aligned} \mathrm{Im}(m\langle z \rangle) &= \frac{1}{2i}(m\langle z \rangle - \overline{m\langle z \rangle}) = \frac{1}{2i}((m\langle z \rangle)^T - \overline{m\langle z \rangle}) = \frac{1}{2i}((q^{-1})^T \cdot p^T - \bar{p} \cdot \bar{q}^{-1}) \\ &= \frac{1}{2i}(q^{-1})^T \cdot (p^T \cdot \bar{q} - q^T \cdot \bar{p}) \cdot \bar{q}^{-1} = y\{q^{-1}\} > 0. \end{aligned} \quad (2.13)$$

Infolgedessen gilt $m\langle z \rangle \in \mathbb{H}_n$ und die im Satz definierte Abbildung ist wohldefiniert.

Es bleibt nachzuweisen, dass sie eine Operation darstellt. Es gilt $I_{2n}\langle z \rangle = z$ für alle $z \in \mathbb{H}_n$.

Für $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$ und $m^* = \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$ ist

$$mm^* = \begin{pmatrix} aa^* + bc^* & ab^* + bd^* \\ ca^* + dc^* & cb^* + dd^* \end{pmatrix}.$$

Daraus ergibt sich für $z \in \mathbb{H}_n$

$$\begin{aligned} m\langle m^*\langle z \rangle \rangle &= m\langle (a^*z + b^*)(c^*z + d^*)^{-1} \rangle \\ &= (a \cdot (a^*z + b^*)(c^*z + d^*)^{-1} + b) \cdot (c \cdot (a^*z + b^*)(c^*z + d^*)^{-1} + d)^{-1} \\ &= (a \cdot (a^*z + b^*) + b \cdot (c^*z + d^*)) \cdot (c^*z + d^*)^{-1} \\ &\quad \cdot \left((c \cdot (a^*z + b^*) + d \cdot (c^*z + d^*)) \cdot (c^*z + d^*)^{-1} \right)^{-1} \\ &= ((aa^* + bc^*) \cdot z + (ab^* + bd^*)) \cdot ((ca^* + dc^*) \cdot z + (cb^* + dd^*))^{-1} \\ &= (mm^*)\langle z \rangle. \end{aligned}$$

□

Beispiel 2.4.6. [3, S. 5], [16, S. 39], [32, S. 13]

(a) Für eine symmetrische Matrix $b \in M_n(\mathbb{R})$ und $z \in \mathbb{H}_n$ ist $\begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix} \langle z \rangle = z + b$.

(b) Es gilt $\begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix} \langle z \rangle = u^T \cdot z \cdot u = z[u]$ für $u \in \mathrm{GL}_n(\mathbb{R})$ und $z \in \mathbb{H}_n$.

Wenden wir Satz 2.4.1 auf $j = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$ an, erhalten wir

Korollar 2.4.7. [16, S. 19], [51, S. 4, 5, 105] Jedes $z \in \mathbb{H}_n$ ist invertierbar und es gilt

$$-z^{-1} \in \mathbb{H}_n.$$

Mithilfe von Satz 2.4.1 können wir auch zu Bemerkung 2.3.3 zurückkehren und zeigen

Korollar 2.4.8. [47, S. 31, 32] Es gilt $\mathrm{Sp}_n(\mathbb{R}) \subset \mathrm{SL}_{2n}(\mathbb{R})$.

Für den Beweis erinnern wir zunächst daran, dass

$$\det \begin{pmatrix} z_1 & z_2 \\ 0 & z_4 \end{pmatrix} = \det(z_1) \cdot \det(z_4) \quad \text{für } z_1, z_2, z_4 \in M_n(\mathbb{C}) \text{ gilt.}$$

Für $z_1, z_2 \in M_n(\mathbb{C})$ folgt daraus

$$\det \begin{pmatrix} z_1 & z_2 \\ I_n & I_n \end{pmatrix} = \det \begin{pmatrix} z_1 - z_2 & z_2 \\ 0 & I_n \end{pmatrix} = \det(z_1 - z_2),$$

indem wir in $\begin{pmatrix} z_1 & z_2 \\ I_n & I_n \end{pmatrix}$ für jedes $1 \leq \ell \leq n$ die $(n + \ell)$ -te Spalte von der ℓ -ten Spalte abziehen.

Beweis des Korollars 2.4.8. Sei $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$. In Bemerkung 2.3.3(a) sahen wir bereits ein, dass $\det(m) = \pm 1$ gilt. Es reicht daher aus, $\det(m) > 0$ zu zeigen.

Sei $z \in \mathbb{H}_n$. Mit $m\langle z \rangle = (az + b)(cz + d)^{-1}$ bestimmen wir

$$\begin{pmatrix} m\langle z \rangle & \overline{m\langle z \rangle} \\ I_n & I_n \end{pmatrix} \cdot \begin{pmatrix} cz + d & 0 \\ 0 & \overline{cz + d} \end{pmatrix} = \begin{pmatrix} az + b & \overline{az + b} \\ cz + d & \overline{cz + d} \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} z & \bar{z} \\ I_n & I_n \end{pmatrix} = m \cdot \begin{pmatrix} z & \bar{z} \\ I_n & I_n \end{pmatrix}$$

und erhalten durch Determinantenbildung daraus

$$\begin{aligned} \det(m\langle z \rangle - \overline{m\langle z \rangle}) \cdot |\det(cz + d)|^2 &= \det(m) \cdot \det(z - \bar{z}), \\ \det(\mathrm{Im}(m\langle z \rangle)) \cdot |\det(cz + d)|^2 &= \det(m) \cdot \det(\mathrm{Im}(z)). \end{aligned} \quad (2.14)$$

Nun sind aber die Matrizen $\mathrm{Im}(m\langle z \rangle)$ und $\mathrm{Im}(z)$ positiv definit und haben daher eine positive Determinante. Da $cz + d$ nach dem Beweis von Satz 2.4.1 invertierbar ist, folgt aus Gleichung (2.14) schließlich $\det(m) > 0$. \square

Lemma 2.4.9. [3, S. 7], [16, S. 28], [25, S. 218], [32, S. 14]

Die Operation von $\mathrm{Sp}_n(\mathbb{R})$ auf \mathbb{H}_n durch Möbiustransformationen im Sinne von Satz 2.4.1 ist transitiv.

Dies bedeutet, dass es nur eine Bahn gibt. Gleichbedeutend damit ist folgende Aussage: Für alle $z, w \in \mathbb{H}_n$ gibt es eine symplektische Matrix $m \in \mathrm{Sp}_n(\mathbb{R})$ mit $m\langle z \rangle = w$.

Beweis des Lemmas 2.4.9. Wir zeigen, dass es zu jedem $z = x + iy \in \mathbb{H}_n$ ein $m \in \mathrm{Sp}_n(\mathbb{R})$ mit $m\langle iI_n \rangle = z$ gibt. Dann nämlich hat die Operation nur eine Bahn und ist transitiv.

Zu der positiv definiten Matrix y gibt es nach Korollar 2.1.11 ein $b \in \mathrm{GL}_n(\mathbb{R})$ mit $b^T \cdot b = y$. Mithilfe der nach Lemma 2.3.5(d) symplektischen Matrix $m := \begin{pmatrix} b^T & xb^{-1} \\ 0 & b^{-1} \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$ gilt

$$m\langle iI_n \rangle = (ib^T + xb^{-1}) \cdot b = ib^T \cdot b + x = iy + x = z. \quad \square$$

Wenn wir den Stabilisator (Fixgruppe) von iI_n mit $\mathcal{K}_n := \{m \in \mathrm{Sp}_n(\mathbb{R}) \mid m\langle iI_n \rangle = iI_n\}$ bezeichnen, ergibt Lemma 2.4.9 eine Bijektion zwischen der Menge der Linksnebenklassen von \mathcal{K}_n in $\mathrm{Sp}_n(\mathbb{R})$ und der Siegelschen Halbebene \mathbb{H}_n [3, S. 7], [16, S. 28], [25, S. 219], [32, S. 14]:

Korollar 2.4.10. Die Abbildung

$$\begin{aligned} \mathrm{Sp}_n(\mathbb{R})/\mathcal{K}_n &\longrightarrow \mathbb{H}_n \\ m\mathcal{K}_n &\longmapsto m\langle iI_n \rangle \end{aligned}$$

ist bijektiv.

Aus welchen Matrizen \mathcal{K}_n konkret besteht, bestimmen wir in

Lemma 2.4.11. [3, S. 7, 8], [16, S. 28], [32, S. 14, 15]

Es gilt

$$\mathcal{K}_n = \{m \in \mathrm{Sp}_n(\mathbb{R}) \mid m^{-1} = m^T\}.$$

\mathcal{K}_n besteht also aus allen symplektischen Matrizen, die orthogonal sind.

Beweis des Lemmas 2.4.11. Schreiben wir $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$, so ist $m\langle iI_n \rangle = iI_n$ gleichbedeutend mit

$$(ia + b)(ic + d)^{-1} = iI_n, \quad \text{also } ia + b = -c + id.$$

Dies wiederum ist äquivalent zu $a = d$, $b = -c$ sowie $m^{-1} = m^T$ (Lemma 2.3.5(c)). \square

Im Fall $n = 1$ wissen wir, dass zwei Matrizen $m, \tilde{m} \in \mathrm{Sp}_1(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})$ genau dann dieselbe Möbiustransformation definieren, wenn $\tilde{m} = \pm m$ gilt [7, S. 158], [60, S. 2].

Wir wollen zeigen, dass dies auch im Allgemeinen gilt. Dazu müssen wir etwas ausholen und beginnen mit der Existenz einer Matrix $y \in \mathbb{P}_n$, deren erste Zeile nur aus Einsen besteht.

Lemma 2.4.12. Es gibt eine symmetrische und positiv definite Matrix $y \in M_n(\mathbb{R})$ mit

$$\begin{aligned} y_{1,\ell} = y_{\ell,1} &= 1 \quad \text{für alle } 1 \leq \ell \leq n \\ \text{und } y_{\ell,r} &= 0 \quad \text{für alle } 2 \leq \ell, r \leq n, \ell \neq r. \end{aligned}$$

Beweis. Wir beweisen das Lemma per Induktion über n . Für $n = 1$ wählen wir $y = (1)$. Sei jetzt $n \geq 2$. Setzen wir voraus, dass ein $x \in M_{n-1}(\mathbb{R})$ mit den gewünschten Eigenschaften existiert (Induktionsvoraussetzung), so definieren wir für $\lambda \in \mathbb{R}$ die symmetrische Matrix

$$y := \begin{pmatrix} & & & 1 \\ & & & 0 \\ & x & & \vdots \\ & & & 0 \\ 1 & 0 \dots 0 & & \lambda \end{pmatrix} \in M_n(\mathbb{R}).$$

Es gilt $\det(y) = \lambda \cdot \det(x) + t$ mit einem $t \in \mathbb{R}$. Nach Induktionsvoraussetzung ist x positiv definit und hat daher eine positive Determinante. Wählen wir $\lambda > -\frac{t}{\det(x)}$, haben wir $\det(y) > 0$. Da die ersten $n-1$ Hauptminoren von y mit denen der positiv definiten Matrix x übereinstimmen, folgt schließlich die positive Definitheit von y . \square

Hiermit können wir untersuchen, welche Matrizen mit allen positiv definiten Matrizen kommutieren [32, S. 13, 40], [35, S. 11], [47, S. 32].

Lemma 2.4.13. *Es gilt*

$$\{a \in M_n(\mathbb{R}) \mid ay = ya \text{ für alle } y \in \mathbb{P}_n\} = \{rI_n \mid r \in \mathbb{R}\}.$$

Beweis. Selbstverständlich kommutieren Matrizen der Gestalt rI_n , $r \in \mathbb{R}$, mit allen Matrizen aus \mathbb{P}_n .

Um die umgekehrte Inklusion zu beweisen, sei $a \in M_n(\mathbb{R})$ eine Matrix mit der Eigenschaft $ay = ya$ für alle $y \in \mathbb{P}_n$. Für $y = \mathrm{diag}(1, 2, 3, \dots, n) \in \mathbb{P}_n$ folgt die Beziehung

$$a_{\ell,r} \cdot r = a_{\ell,r} \cdot y_{r,r} = (ay)_{\ell,r} = (ya)_{\ell,r} = y_{\ell,\ell} \cdot a_{\ell,r} = \ell \cdot a_{\ell,r} \quad \text{für alle } 1 \leq \ell, r \leq n.$$

Für $\ell \neq r$ folgt daraus $a_{\ell,r} = 0$. Also besitzt a die Gestalt $a = \mathrm{diag}(a_{1,1}, \dots, a_{n,n})$. Aufgrund von Lemma 2.4.12 können wir eine Matrix $y \in \mathbb{P}_n$ mit $y_{1,\ell} = 1$ für alle $1 \leq \ell \leq n$ finden. Daraus folgt für alle $1 \leq \ell \leq n$ schließlich

$$a_{1,1} = a_{1,1} \cdot y_{1,\ell} = (ay)_{1,\ell} = (ya)_{1,\ell} = y_{1,\ell} \cdot a_{\ell,\ell} = a_{\ell,\ell}.$$

Dies ergibt $a = a_{1,1}I_n$. \square

Nun sind wir in der Lage, folgenden Satz über Möbiustransformationen zu zeigen [32, S. 13], [47, S. 32], [54, S. 597, 598], [55, S. 626, 627].

Satz 2.4.14. *Zwei symplektische Matrizen $m, \tilde{m} \in \mathrm{Sp}_n(\mathbb{R})$ definieren genau dann dieselbe Möbiustransformation, wenn $\tilde{m} = \pm m$ gilt.*

Beweis. Offenbar liefern m und $-m$ dieselbe Möbiustransformation.

Umgekehrt sei vorausgesetzt, dass $\tilde{m}\langle z \rangle = m\langle z \rangle$ für alle $z \in \mathbb{H}_n$ gilt. Mit der symplektischen Matrix $m^* := m^{-1}\tilde{m} \in \mathrm{Sp}_n(\mathbb{R})$ gilt dann $m^*\langle z \rangle = z$ für alle $z \in \mathbb{H}_n$. Schreiben wir $m^* = \begin{pmatrix} a^* & b^* \\ c^* & d^* \end{pmatrix}$, so bedeutet dies

$$a^* \cdot z + b^* = z \cdot (c^* \cdot z + d^*) \quad \text{für alle } z \in \mathbb{H}_n. \quad (2.15)$$

Für $z = i\lambda I_n \in \mathbb{H}_n$, $\lambda > 0$, erhalten wir nun $i\lambda a^* + b^* = i\lambda \cdot (i\lambda c^* + d^*)$, also

$$0 = \lambda^2 c^* + i\lambda \cdot (a^* - d^*) + b^*. \quad (2.16)$$

Das (ℓ, r) -te Element, $1 \leq \ell, r \leq n$, von (2.16) ergibt sich nun zu

$$0 = c_{\ell,r}^* \lambda^2 + i \cdot (a_{\ell,r}^* - d_{\ell,r}^*) \cdot \lambda + b_{\ell,r}^*.$$

Weil dies für alle $\lambda > 0$ gilt, muss $c_{\ell,r}^* = b_{\ell,r}^* = 0$ und $d_{\ell,r}^* = a_{\ell,r}^*$ für alle $1 \leq \ell, r \leq n$ gelten. Das bedeutet $c^* = b^* = 0$ und $d^* = a^*$. Die Gleichung (2.15) lautet daher $a^* \cdot z = z \cdot a^*$ für alle $z \in \mathbb{H}_n$. Durch Übergang zum Imaginärteil erhalten wir $a^* \cdot y = y \cdot a^*$ für alle $y \in \mathbb{P}_n$, woraus wir die Existenz eines $r \in \mathbb{R}$ mit $a^* = rI_n$ folgern (Lemma 2.4.13). Somit ergibt sich $m^* = \begin{pmatrix} rI_n & 0 \\ 0 & rI_n \end{pmatrix} = rI_{2n}$. Aus Lemma 2.3.5(d) oder Korollar 2.4.8 schließen wir $r = \pm 1$ und $m^* = \pm I_{2n}$. Dies ergibt jetzt $\tilde{m} = \pm m$. \square

Wir können analoge Aussagen von Satz 2.4.1 und Satz 2.4.14 für die Gruppe $\mathrm{GL}_n(\mathbb{R})$ beweisen [32, S. 17], [35, S. 10, 11].

Lemma 2.4.15. *Die Gruppe $\mathrm{GL}_n(\mathbb{R})$ operiert auf \mathbb{P}_n durch*

$$\begin{aligned} \mathrm{GL}_n(\mathbb{R}) \times \mathbb{P}_n &\longrightarrow \mathbb{P}_n \\ (u, y) &\longmapsto y[u^\mathrm{T}]. \end{aligned}$$

Zwei Matrizen $u, \tilde{u} \in \mathrm{GL}_n(\mathbb{R})$ definieren genau dann dieselbe Operation, wenn $\tilde{u} = \pm u$ gilt.

Beweis. Wegen Bemerkung 2.1.5(c) ist $y[u^\mathrm{T}] \in \mathbb{P}_n$. Aus $y[I_n^\mathrm{T}] = y$ und

$$y[(u\tilde{u})^\mathrm{T}] = y[\tilde{u}^\mathrm{T} \cdot u^\mathrm{T}] = (y[\tilde{u}^\mathrm{T}])[u^\mathrm{T}] \quad \text{für alle } y \in \mathbb{P}_n \text{ und alle } u, \tilde{u} \in \mathrm{GL}_n(\mathbb{R})$$

folgt sofort, dass die Abbildung eine Operation darstellt.

Um die zusätzliche Aussage zu zeigen, bemerken wir, dass u und $-u$ offensichtlich dieselbe Operation liefern.

Umgekehrt sei vorausgesetzt, dass $y[\tilde{u}^\mathrm{T}] = y[u^\mathrm{T}]$ für alle $y \in \mathbb{P}_n$ gilt. Mit der Matrix $u^* := \tilde{u}^\mathrm{T} \cdot (u^\mathrm{T})^{-1} \in \mathrm{GL}_n(\mathbb{R})$ erhalten wir dann

$$u^{*\mathrm{T}} \cdot y \cdot u^* = y[u^*] = y \quad \text{für alle } y \in \mathbb{P}_n. \quad (2.17)$$

Für $y = I_n$ ergibt sich insbesondere $u^{*\mathrm{T}} \cdot u^* = I_n$. Multiplikation von (2.17) mit $(u^{*\mathrm{T}})^{-1} = u^*$ von links liefert $y \cdot u^* = u^* \cdot y$ für alle $y \in \mathbb{P}_n$. Dies bedeutet nach Lemma 2.4.13, dass es ein $r \in \mathbb{R} \setminus \{0\}$ mit $u^* = rI_n$ gibt. Nun folgt aus der Bedingung $I_n = u^{*\mathrm{T}} \cdot u^* = r^2 I_n$ schließlich $r^2 = 1$, $r = \pm 1$ sowie $\tilde{u} = \pm u$. \square

2.5 Erzeuger der Siegelschen Modulgruppe Γ_n

Definition 2.5.1. [16, S. 30], [21, S. 184], [35, S. 28], [37, S. 8]

Wir definieren

$$\Gamma_n := \mathrm{Sp}_n(\mathbb{Z}) := \{m \in M_{2n}(\mathbb{Z}) \mid j[m] = j\}.$$

Beispiel 2.5.2. [37, S. 8, 9], [60, S. 1] Aus Beispiel 2.3.6 folgt

$$\Gamma_1 = \mathrm{Sp}_1(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid ad - bc = 1 \right\} = \mathrm{SL}_2(\mathbb{Z}).$$

Vor dem Studium von Γ_n ist es zunächst sinnvoll, die Einheitengruppe $\mathrm{GL}_n(\mathbb{Z})$ des Rings $M_n(\mathbb{Z})$ zu untersuchen [38, S. 256].

Definition 2.5.3. Die Gruppe

$$\mathrm{GL}_n(\mathbb{Z}) := \{u \in M_n(\mathbb{Z}) \mid \text{es gibt ein } v \in M_n(\mathbb{Z}) \text{ mit } uv = vu = I_n\}$$

heißt *unimodulare Gruppe*.

Lemma 2.5.4. [38, S. 256, 257], [61, S. 41] Für eine Matrix $u \in M_n(\mathbb{Z})$ sind folgende Aussagen äquivalent:

- (a) $u \in \mathrm{GL}_n(\mathbb{Z})$.
- (b) $u^T \in \mathrm{GL}_n(\mathbb{Z})$.
- (c) $u \in \mathrm{GL}_n(\mathbb{Q})$ und $u^{-1} \in M_n(\mathbb{Z})$.
- (d) $\det(u) = \pm 1$.
- (e) Die Abbildung

$$\begin{aligned} M_{n,m}(\mathbb{Z}) &\longrightarrow M_{n,m}(\mathbb{Z}) \\ g &\longmapsto ug \end{aligned}$$

ist für jedes $m \in \mathbb{N}$ bijektiv.

- (f) Die Abbildung

$$\begin{aligned} M_{m,n}(\mathbb{Z}) &\longrightarrow M_{m,n}(\mathbb{Z}) \\ g &\longmapsto gu \end{aligned}$$

ist für jedes $m \in \mathbb{N}$ bijektiv.

Beweis. Offensichtlich gelten die Äquivalenzen (a) \Leftrightarrow (b) und (a) \Leftrightarrow (c).

Wir wollen nun einen Ringschluss (c) \Rightarrow (e) \Rightarrow (d) \Rightarrow (c) verwenden, wobei die erste Implikation (c) \Rightarrow (e) offensichtlich gilt.

(e) \Rightarrow (d): Bezeichnen e_1, \dots, e_n die kanonischen Einheitsvektoren des \mathbb{Z}^n , so folgt aus der Surjektivität von

$$\begin{aligned} \mathbb{Z}^n &\longrightarrow \mathbb{Z}^n \\ g &\longmapsto ug, \end{aligned}$$

dass es $v_1, \dots, v_n \in \mathbb{Z}^n$ mit $uv_\ell = e_\ell$, $1 \leq \ell \leq n$, gibt. Für $v := (v_1 \mid \dots \mid v_n) \in M_n(\mathbb{Z})$ gilt also $uv = I_n$. Durch Determinantenbildung erhalten wir, dass $1 = \det(I_n) = \det(u) \cdot \det(v)$ das Produkt zweier ganzer Zahlen ist. Dies ergibt $\det(u) = \pm 1$.

(d) \Rightarrow (c): Berechnen wir die Inverse u^{-1} mithilfe der Cramerschen Regel, so erhalten wir aus $\det(u) = \pm 1$, dass u^{-1} nur ganzzahlige Einträge hat.

Wir können diesen Ringschluss auch mit (f) statt (e) durchführen: In (f) \Rightarrow (d) definieren wir dann die Matrix v zeilenweise.

Hiermit ist schließlich das Lemma bewiesen. □

Bemerkung 2.5.5. [37, S. 6 – 8] Bemerkung 2.3.3(a) und Lemma 2.5.4(d) ergeben

$$\Gamma_n = \mathrm{Sp}_n(\mathbb{Z}) = \{m \in \mathrm{GL}_{2n}(\mathbb{Z}) \mid j[m] = j\} = \mathrm{GL}_{2n}(\mathbb{Z}) \cap \mathrm{Sp}_n(\mathbb{R}).$$

Unter Verwendung von Korollar 2.4.8 gilt sogar

$$\Gamma_n = \mathrm{Sp}_n(\mathbb{Z}) = \{m \in \mathrm{SL}_{2n}(\mathbb{Z}) \mid j[m] = j\} = \mathrm{SL}_{2n}(\mathbb{Z}) \cap \mathrm{Sp}_n(\mathbb{R}).$$

Dies zeigt, dass Γ_n eine Untergruppe von $\mathrm{GL}_{2n}(\mathbb{Z})$ und sogar von $\mathrm{SL}_{2n}(\mathbb{Z})$ ist.

Γ_n heißt die *Siegelsche Modulgruppe vom Geschlecht n* .

Wir richten unsere Aufmerksamkeit nun auf besondere Matrizen von Γ_n [3, S. 5, 14, 17], [32, S. 6, 13], [37, S. 7], [47, S. 162, 163]:

Die von den Matrizen

$$\begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix}, \quad b \in M_n(\mathbb{Z}) \text{ symmetrisch}, \quad (2.18)$$

$$j = \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \quad (2.19)$$

$$\text{und} \quad \begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix}, \quad u \in \mathrm{GL}_n(\mathbb{Z}), \quad (2.20)$$

erzeugte Untergruppe von Γ_n bezeichnen wir mit Γ_n^* .

Beispiel 2.5.6. Die Inversen der in (2.18), (2.19) und (2.20) gegebenen Matrizen sind

$$\begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix}^{-1} = \begin{pmatrix} I_n & -b \\ 0 & I_n \end{pmatrix}, \quad b \in M_n(\mathbb{Z}) \text{ symmetrisch},$$

$$j^{-1} = -j = j^3$$

$$\text{und} \quad \begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix}^{-1} = \begin{pmatrix} (u^T)^{-1} & 0 \\ 0 & u \end{pmatrix}, \quad u \in \mathrm{GL}_n(\mathbb{Z}).$$

Also kann jedes $m \in \Gamma_n^*$ als Produkt von endlich vielen Matrizen der Gestalt (2.18), (2.19) und (2.20) dargestellt werden.

Unser Ziel ist es, $\Gamma_n = \Gamma_n^*$ zu zeigen: Per Definition gilt dabei bereits die Inklusion $\Gamma_n^* \subset \Gamma_n$; um die andere Inklusion zu zeigen, benötigen wir einige Vorbereitungen.

Lemma 2.5.7. [3, S. 17], [4, S. 13], [16, S. 325], [38, S. 257, 258]

Seien $n \in \mathbb{N} \setminus \{1\}$ und $g = (g_1, \dots, g_n)^T \in \mathbb{Z}^n \setminus \{0\}$. Dann gibt es ein $u \in \mathrm{SL}_n(\mathbb{Z})$ mit

$$ug = (d, 0, \dots, 0)^T, \quad d = \mathrm{ggT}(g_1, \dots, g_n).$$

Beweis. Wir führen den Beweis per Induktion über n . Für $n = 2$ gibt es $\alpha, \beta \in \mathbb{Z}$ mit $\alpha g_1 + \beta g_2 = \mathrm{ggT}(g_1, g_2) =: d$. Mit der Matrix $u := \begin{pmatrix} \alpha & \beta \\ -\frac{g_2}{d} & \frac{g_1}{d} \end{pmatrix} \in M_2(\mathbb{Z})$, deren Determinante $\alpha \cdot \frac{g_1}{d} + \beta \cdot \frac{g_2}{d} = 1$ beträgt, folgt dann

$$ug = \begin{pmatrix} \alpha g_1 + \beta g_2 \\ -\frac{g_2}{d} \cdot g_1 + \frac{g_1}{d} \cdot g_2 \end{pmatrix} = \begin{pmatrix} d \\ 0 \end{pmatrix}.$$

Sei $n \geq 3$ und es sei vorausgesetzt, dass die Behauptung für $n - 1$ gilt. Wir machen eine Fallunterscheidung für den Vektor $g = (g_1, \dots, g_n)^T \in \mathbb{Z}^n \setminus \{0\}$:

Fall (a): Falls $g_n \neq 0$ gilt, so wählen wir (nach dem obigen Fall $n = 2$) ein $v \in \mathrm{SL}_2(\mathbb{Z})$, sodass

$$v \cdot \begin{pmatrix} g_{n-1} \\ g_n \end{pmatrix} = \begin{pmatrix} d^* \\ 0 \end{pmatrix}, \quad d^* = \mathrm{ggT}(g_{n-1}, g_n), \quad \text{gilt.}$$

Mit $u_1 := \begin{pmatrix} I_{n-2} & 0 \\ 0 & v \end{pmatrix} \in \mathrm{SL}_n(\mathbb{Z})$ folgt $\tilde{g} := u_1 g = (g_1, \dots, g_{n-2}, d^*, 0)^T$.

Fall (b): Für $g_n = 0$ liefert $u_1 := I_n \in \mathrm{SL}_n(\mathbb{Z})$ den Vektor $\tilde{g} := u_1 g = g = (g_1, \dots, g_{n-1}, 0)^T$.

In beiden Fällen verschwindet der letzte Eintrag des Vektors $\tilde{g} \in \mathbb{Z}^n \setminus \{0\}$. Wenden wir die Induktionsvoraussetzung auf seine ersten $n - 1$ Einträge $(\tilde{g}_1, \dots, \tilde{g}_{n-1})^T \in \mathbb{Z}^{n-1} \setminus \{0\}$ an, so ergibt sich die Existenz eines $\tilde{v} \in \mathrm{SL}_{n-1}(\mathbb{Z})$ mit

$$\tilde{v} \cdot (\tilde{g}_1, \dots, \tilde{g}_{n-1})^T = (\tilde{d}, 0, \dots, 0)^T, \quad \tilde{d} = \mathrm{ggT}(\tilde{g}_1, \dots, \tilde{g}_{n-1}) = \mathrm{ggT}(g_1, \dots, g_n).$$

Daraus folgt, dass $u_2 := \begin{pmatrix} \tilde{v} & 0 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_n(\mathbb{Z})$ nun

$$u_2 u_1 g = u_2 \tilde{g} = \begin{pmatrix} \tilde{v} \cdot (\tilde{g}_1, \dots, \tilde{g}_{n-1})^T \\ 0 \end{pmatrix} = (\tilde{d}, 0, \dots, 0)^T \quad \text{liefert.} \quad \square$$

Durch Berücksichtigung des Falls $n = 1$ folgt sofort

Korollar 2.5.8. [3, S. 17, 47], [4, S. 13], [16, S. 325], [38, S. 257, 258]

Seien $n \in \mathbb{N}$ und $g = (g_1, \dots, g_n)^T \in \mathbb{Z}^n \setminus \{0\}$. Dann gibt es ein $u \in \mathrm{GL}_n(\mathbb{Z})$ mit

$$ug = (d, 0, \dots, 0)^T, \quad d = \mathrm{ggT}(g_1, \dots, g_n).$$

Bemerkung 2.5.9. [38, S. 258] Seien $n \in \mathbb{N}$, $g = (g_1, \dots, g_n)^T \in \mathbb{Z}^n \setminus \{0\}$ und $u \in \mathrm{GL}_n(\mathbb{Z})$. Dann gilt

$$\mathrm{ggT}((ug)_1, \dots, (ug)_n) = \mathrm{ggT}(g_1, \dots, g_n),$$

denn zum einen liefert die Matrixmultiplikation ug , dass die Einträge von ug ganzzahlige Linearkombinationen von g_1, \dots, g_n sind, weshalb $\mathrm{ggT}(g_1, \dots, g_n)$ ein Teiler von $\mathrm{ggT}((ug)_1, \dots, (ug)_n)$ ist. Zum anderen ergibt die Multiplikation von $u^{-1} \cdot (ug) = g$, dass auch $\mathrm{ggT}((ug)_1, \dots, (ug)_n)$ ein Teiler von $\mathrm{ggT}(g_1, \dots, g_n)$ ist.

Lemma 2.5.10. [3, S. 47], [4, S. 13], [16, S. 325], [38, S. 257, 258]

Seien $n \in \mathbb{N}$, $1 \leq k \leq n$ und $g = (g_1, \dots, g_n)^T \in \mathbb{Z}^n \setminus \{0\}$. Dann kommt g genau dann als k -te Spalte eines $u \in \mathrm{GL}_n(\mathbb{Z})$ vor, wenn $\mathrm{ggT}(g_1, \dots, g_n) = 1$ gilt.

Beweis. Sei g die k -te Spalte eines $u \in \mathrm{GL}_n(\mathbb{Z})$. Entwickeln wir die Determinante $\det(u) = \pm 1$ nach der k -ten Spalte von u , so zeigt sich, dass $\mathrm{ggT}(g_1, \dots, g_n)$ die Determinante $\det(u) = \pm 1$ teilt. Also folgt $\mathrm{ggT}(g_1, \dots, g_n) = 1$.

Falls umgekehrt $\mathrm{ggT}(g_1, \dots, g_n) = 1$ vorausgesetzt ist, liefert Korollar 2.5.8 ein $u \in \mathrm{GL}_n(\mathbb{Z})$ mit

$$ug = (1, 0, \dots, 0)^T, \quad \text{also } g = u^{-1} \cdot (1, 0, \dots, 0)^T.$$

Daher ist g die erste Spalte von $u^{-1} \in \mathrm{GL}_n(\mathbb{Z})$. Durch eine Spaltenvertauschung kann erreicht werden, dass g als k -te Spalte einer unimodularen Matrix vorkommt. \square

Lemma 2.5.11. [3, S. 18], [16, S. 326, 327], [32, S. 9, 10]

Seien $n \in \mathbb{N}$ und $g = (g_1, \dots, g_{2n})^T \in \mathbb{Z}^{2n} \setminus \{0\}$. Dann gibt es ein $\tilde{m} \in \Gamma_n^*$ mit

$$\tilde{m}g = (d, 0, \dots, 0)^T, \quad d = \mathrm{ggT}(g_1, \dots, g_{2n}).$$

Beweis. Wir schreiben ganzzahlige Vektoren mit $2n$ Einträgen in der Form $\begin{pmatrix} \alpha \\ \beta \end{pmatrix}$, $\alpha, \beta \in \mathbb{Z}^n$, und zeigen zunächst, dass ein

$$\tilde{g} = \begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} \in \{\tilde{m}g \mid \tilde{m} \in \Gamma_n^*\} \quad \text{mit } \tilde{\alpha} = 0 \text{ oder } \tilde{\beta} = 0 \text{ existiert.}$$

Dies beweisen wir per Widerspruch und nehmen daher an, dass alle $\tilde{g} = \begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} \in \{\tilde{m}g \mid \tilde{m} \in \Gamma_n^*\}$ sowohl $\tilde{\alpha} \neq 0$ als auch $\tilde{\beta} \neq 0$ erfüllen. Definieren wir

$$d_1 := \mathrm{ggT}(\tilde{\alpha}_1, \dots, \tilde{\alpha}_n) \quad \text{und} \quad d_2 := \mathrm{ggT}(\tilde{\beta}_1, \dots, \tilde{\beta}_n),$$

so wählen wir $\tilde{g} = \begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} \in \{\tilde{m}g \mid \tilde{m} \in \Gamma_n^*\}$ derart, dass $d_1 d_2$ minimal ist. Dabei können wir $d_1 \geq d_2$ annehmen, denn ansonsten, falls $d_1 < d_2$ gilt, ersetzen wir \tilde{g} durch $j\tilde{g} = \begin{pmatrix} -\tilde{\beta} \\ \tilde{\alpha} \end{pmatrix}$. Indem wir nun \tilde{g} durch

$$\begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix} \cdot \tilde{g} = \begin{pmatrix} u^T \cdot \tilde{\alpha} \\ u^{-1} \cdot \tilde{\beta} \end{pmatrix}$$

mit einem nach Korollar 2.5.8 geeigneten $u \in \mathrm{GL}_n(\mathbb{Z})$ ersetzen, können wir des Weiteren annehmen, dass $\tilde{\beta}$ von der Gestalt $\tilde{\beta} = (d_2, 0, \dots, 0)^T$ ist. Bei den gemachten Annahmen ändert sich die Minimalbedingung an $d_1 d_2$ wegen Bemerkung 2.5.9 nicht. Nach der Division mit Rest wählen wir $b_{\ell,1} \in \mathbb{Z}$, $1 \leq \ell \leq n$, sodass $0 \leq \tilde{\alpha}_\ell + d_2 b_{\ell,1} < d_2$ gilt. Mit einer symmetrischen Matrix $b \in M_n(\mathbb{Z})$, deren erste Spalte durch den oben gewählten Vektor $(b_{1,1}, \dots, b_{n,1})^T$ gegeben ist, folgt

$$\begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix} \cdot \tilde{g} = \begin{pmatrix} \tilde{\alpha} + b\tilde{\beta} \\ \tilde{\beta} \end{pmatrix} = \begin{pmatrix} \tilde{\alpha} + d_2 b e_1 \\ d_2 e_1 \end{pmatrix}.$$

Der größte gemeinsame Teiler \tilde{d} der Einträge $\tilde{\alpha}_\ell + d_2 b_{\ell,1}$, $1 \leq \ell \leq n$, von $\tilde{\alpha} + d_2 b e_1 \in \mathbb{Z}^n \setminus \{0\}$ erfüllt dann $\tilde{d} < d_2 \leq d_1$, also $\tilde{d} d_2 < d_1 d_2$. Dies ist ein Widerspruch zur Minimalität von $d_1 d_2$. Also ist die Annahme falsch und es muss deshalb ein

$$\tilde{g} = \begin{pmatrix} \tilde{\alpha} \\ \tilde{\beta} \end{pmatrix} \in \{\tilde{m}g \mid \tilde{m} \in \Gamma_n^*\} \quad \text{mit } \tilde{\alpha} = 0 \text{ oder } \tilde{\beta} = 0 \text{ geben.}$$

Indem wir gegebenenfalls \tilde{g} durch $j\tilde{g} = \begin{pmatrix} -\tilde{\beta} \\ \tilde{\alpha} \end{pmatrix}$ ersetzen, können wir $\tilde{\beta} = 0$ annehmen. Mit Korollar 2.5.8 folgt, dass ein $u \in \mathrm{GL}_n(\mathbb{Z})$ mit $u^T \cdot \tilde{\alpha} = (d, 0, \dots, 0)^T$, $d \in \mathbb{N}$, existiert, womit schließlich

$$\begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix} \cdot \tilde{g} = \begin{pmatrix} u^T \cdot \tilde{\alpha} \\ u^{-1} \cdot \tilde{\beta} \end{pmatrix} = (d, 0, \dots, 0)^T \quad \text{folgt.}$$

Dass $d = \mathrm{ggT}(g_1, \dots, g_{2n})$ gilt, ergibt sich aus Bemerkung 2.5.9. \square

Lemma 2.5.12. [3, S. 17 – 19], [16, S. 327, 328], [32, S. 10, 11]

Seien $n \in \mathbb{N}$ und $m \in \Gamma_n$. Dann gibt es ein $\tilde{m} \in \Gamma_n^*$, sodass der linke, untere $n \times n$ – Block von $\tilde{m} \cdot m$ die Nullmatrix ist.

Üblicherweise zerlegen wir $2n \times 2n$ – Matrizen in $n \times n$ – Blöcke, die wir wiederum im folgenden Beweis gemäß (1.3) zerlegen.

Beweis des Lemmas 2.5.12. Zu $m \in \Gamma_n$ wählen wir nach den Lemmata 2.5.10 und 2.5.11 ein $m^* \in \Gamma_n^*$ mit

$$m^* \cdot m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \quad a = \begin{pmatrix} 1 & a_2^{(1)} \\ 0 & a_4^{(1)} \end{pmatrix}, \quad b = \begin{pmatrix} b_1^{(1)} & b_2^{(1)} \\ b_3^{(1)} & b_4^{(1)} \end{pmatrix}, \quad c = \begin{pmatrix} 0 & c_2^{(1)} \\ 0 & c_4^{(1)} \end{pmatrix}, \quad d = \begin{pmatrix} d_1^{(1)} & d_2^{(1)} \\ d_3^{(1)} & d_4^{(1)} \end{pmatrix}.$$

Wir wollen nun die Behauptung per Induktion über n beweisen. Für $n = 1$ ist nichts mehr zu beweisen. Sei also $n \geq 2$ und wir setzen voraus, dass die Behauptung bereits für $n - 1$ gilt. Zunächst zeigen wir, dass die Matrix¹

$$m_4 := \begin{pmatrix} a_4 & b_4 \\ c_4 & d_4 \end{pmatrix} \in M_{2(n-1)}(\mathbb{Z}) \quad \text{ein Element von } \Gamma_{n-1} \text{ ist:}$$

Wegen $m^* \cdot m \in \Gamma_n$ liefert Lemma 2.3.5(d), dass

$$\begin{aligned} a^T \cdot c &= \begin{pmatrix} 1 & 0 \\ a_2^T & a_4^T \end{pmatrix} \cdot \begin{pmatrix} 0 & c_2 \\ 0 & c_4 \end{pmatrix} = \begin{pmatrix} 0 & c_2 \\ 0 & a_2^T \cdot c_2 + a_4^T \cdot c_4 \end{pmatrix} \\ \text{und } c^T \cdot a &= \begin{pmatrix} 0 & 0 \\ c_2^T & c_4^T \end{pmatrix} \cdot \begin{pmatrix} 1 & a_2 \\ 0 & a_4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ c_2^T & c_2^T \cdot a_2 + c_4^T \cdot a_4 \end{pmatrix} \end{aligned}$$

übereinstimmen: Es gilt $c_2 = 0$ und daher auch $a_4^T \cdot c_4 = c_4^T \cdot a_4$. Aus

$$\begin{aligned} I_n = a^T \cdot d - c^T \cdot b &= \begin{pmatrix} 1 & 0 \\ a_2^T & a_4^T \end{pmatrix} \cdot \begin{pmatrix} d_1 & d_2 \\ d_3 & d_4 \end{pmatrix} - \begin{pmatrix} 0 & 0 \\ 0 & c_4^T \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} \\ &= \begin{pmatrix} d_1 & d_2 \\ * & a_2^T \cdot d_2 + a_4^T \cdot d_4 - c_4^T \cdot b_4 \end{pmatrix} \end{aligned}$$

erhalten wir $d_1 = 1$, $d_2 = 0$ und $a_4^T \cdot d_4 - c_4^T \cdot b_4 = I_{n-1}$. Da auch

$$\begin{aligned} b^T \cdot d &= \begin{pmatrix} b_1 & b_3^T \\ b_2^T & b_4^T \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ d_3 & d_4 \end{pmatrix} = \begin{pmatrix} * & * \\ * & b_4^T \cdot d_4 \end{pmatrix} \\ \text{und } d^T \cdot b &= \begin{pmatrix} 1 & d_3^T \\ 0 & d_4^T \end{pmatrix} \cdot \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix} = \begin{pmatrix} * & * \\ * & d_4^T \cdot b_4 \end{pmatrix} \end{aligned}$$

gleich sind, ergibt sich $b_4^T \cdot d_4 = d_4^T \cdot b_4$. Insgesamt ist daher $m_4 \in \Gamma_{n-1}$ bewiesen. Nach der Induktionsvoraussetzung gibt es ein $m_0 = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} \in \Gamma_{n-1}^*$, $a_0, b_0, c_0, d_0 \in M_{n-1}(\mathbb{Z})$, mit

$$m_0 m_4 = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}, \quad \text{das heißt, es gilt } c_0 a_4 + d_0 c_4 = 0.$$

Um aus m_0 ein Element aus Γ_n^* zu konstruieren, betrachten wir die Abbildung

$$\Gamma_{n-1}^* \ni \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = m' \longmapsto \widehat{m'} = \begin{pmatrix} a'' & b'' \\ c'' & d'' \end{pmatrix}$$

¹Der Übersichtlichkeit halber lassen wir die hochstehenden Indices $\cdot^{(1)}$ weg.

mit

$$a'' = \begin{pmatrix} 1 & 0 \\ 0 & a' \end{pmatrix}, \quad b'' = \begin{pmatrix} 0 & 0 \\ 0 & b' \end{pmatrix}, \quad c'' = \begin{pmatrix} 0 & 0 \\ 0 & c' \end{pmatrix}, \quad d'' = \begin{pmatrix} 1 & 0 \\ 0 & d' \end{pmatrix}$$

und zeigen $\widehat{m}' \in \Gamma_n^*$: Da die Abbildung $\widehat{m_1 m_2} = \widehat{m_1} \widehat{m_2}$ für alle $m_1, m_2 \in \Gamma_{n-1}^*$ erfüllt, reicht es, $\widehat{m}' \in \Gamma_n^*$ für die Erzeuger von Γ_{n-1}^* zu überprüfen. Für $\begin{pmatrix} I_{n-1} & b \\ 0 & I_{n-1} \end{pmatrix}$, $b \in M_{n-1}(\mathbb{Z})$ symmetrisch, und $\begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix}$, $u \in \mathrm{GL}_{n-1}(\mathbb{Z})$, ist dies klar und für $j_{n-1} := \begin{pmatrix} 0 & -I_{n-1} \\ I_{n-1} & 0 \end{pmatrix}$ ist

$$\begin{aligned} \widehat{j_{n-1}} &= \begin{pmatrix} \mathrm{diag}(1, 0, \dots, 0) & \mathrm{diag}(0, -1, \dots, -1) \\ \mathrm{diag}(0, 1, \dots, 1) & \mathrm{diag}(1, 0, \dots, 0) \end{pmatrix} \\ &= \begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix}^2 \cdot \left(\begin{pmatrix} 0 & -I_n \\ I_n & 0 \end{pmatrix} \cdot \begin{pmatrix} I_n & \mathrm{diag}(1, 0, \dots, 0) \\ 0 & I_n \end{pmatrix} \right)^3 \in \Gamma_n^*. \end{aligned}$$

Damit ist also $\widehat{m}' \in \Gamma_n^*$ für alle $m' \in \Gamma_{n-1}^*$ bewiesen. Daher gilt $\widehat{m}_0 \in \Gamma_n^*$ und der linke, untere $n \times n$ -Block von $\widehat{m}_0 \cdot (m^* \cdot m)$ ist gegeben durch

$$\begin{pmatrix} 0 & 0 \\ 0 & c_0 \end{pmatrix} \cdot a + \begin{pmatrix} 1 & 0 \\ 0 & d_0 \end{pmatrix} \cdot c = \begin{pmatrix} 0 & 0 \\ 0 & c_0 \end{pmatrix} \cdot \begin{pmatrix} 1 & a_2 \\ 0 & a_4 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & d_0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & c_4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & c_0 a_4 + d_0 c_4 \end{pmatrix} = 0.$$

Dies zeigt die Behauptung mit $\tilde{m} = \widehat{m}_0 \cdot m^* \in \Gamma_n^*$. \square

Hiermit gelingt es uns schließlich, $\Gamma_n = \Gamma_n^*$ zu zeigen [3, S. 17], [16, S. 326, 328], [32, S. 6, 9 – 11], [35, S. 41, 42], [47, S. 162, 163], [49, S. 210].

Satz 2.5.13. *Sei $n \in \mathbb{N}$. Dann wird Γ_n erzeugt von den Matrizen der Gestalt (2.18), (2.19) und (2.20).*

Beweis. Wir müssen $\Gamma_n \subset \Gamma_n^*$ zeigen: Zu $m \in \Gamma_n$ existiert nach Lemma 2.5.12 ein $\tilde{m} \in \Gamma_n^*$ mit

$$\tilde{m} \cdot m = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad a, b, d \in M_n(\mathbb{Z}).$$

Wegen $\tilde{m} \cdot m \in \Gamma_n$ und Lemma 2.3.5(d) gilt $a^T \cdot d = I_n$, also $(a^T)^{-1} = d \in M_n(\mathbb{Z})$. Aus $b^T \cdot d = d^T \cdot b$ folgt durch Multiplikation von links mit $(d^T)^{-1}$ und von rechts mit d^{-1} , dass $(bd^{-1})^T = bd^{-1}$ gilt. Definieren wir nun $u := a^T \in \mathrm{GL}_n(\mathbb{Z})$, dann ist die ganzzahlige Matrix $bu = ba^T = bd^{-1}$ symmetrisch, womit

$$\tilde{m} \cdot m = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} u^T & b \\ 0 & u^{-1} \end{pmatrix} = \begin{pmatrix} I_n & bu \\ 0 & I_n \end{pmatrix} \cdot \begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix} \in \Gamma_n^* \quad \text{folgt.}$$

Hieraus ergibt sich $m \in \Gamma_n^*$. \square

Beispiel 2.5.14. [38, S. 124, 125], [60, S. 2] Sei $n = 1$. Für $b \in \mathbb{Z}$ ist

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^b.$$

Wegen $\mathrm{GL}_1(\mathbb{Z}) = \{\pm 1\}$ sind die durch (2.20) gegebenen Matrizen dann

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 = j^4 \quad \text{und} \quad \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I_2 = j^2.$$

Daher wird Γ_1 erzeugt von

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{und} \quad j = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Kapitel 3

Der Siegelsche Fundamentalbereich \mathcal{F}_n

3.1 Die Jacobi – Zerlegung

Ausgangspunkt für unsere Untersuchungen ist die folgende Identität [3, S. 330], [28, S. 190], [32, S. 18], [35, S. 15], [38, S. 260]:

Lemma 3.1.1 (Quadratische Ergänzung). Sei $y = \begin{pmatrix} y_1 & y_2 \\ y_2^T & y_4 \end{pmatrix} \in M_n(\mathbb{R})$ eine symmetrische Matrix mit einem symmetrischen und invertierbaren Block $y_1 \in \text{GL}_m(\mathbb{R})$, $1 \leq m \leq n-1$. Dann gilt

$$y = \begin{pmatrix} y_1 & 0 \\ 0 & y_4 - y_1^{-1}[y_2] \end{pmatrix} \left[\begin{pmatrix} I_m & y_1^{-1} \cdot y_2 \\ 0 & I_{n-m} \end{pmatrix} \right]. \quad (3.1)$$

Beweis. Die rechte Seite von (3.1) ist

$$\begin{aligned} \begin{pmatrix} I_m & 0 \\ y_2^T \cdot y_1^{-1} & I_{n-m} \end{pmatrix} \cdot \begin{pmatrix} y_1 & 0 \\ 0 & y_4 - y_1^{-1}[y_2] \end{pmatrix} \cdot \begin{pmatrix} I_m & y_1^{-1} \cdot y_2 \\ 0 & I_{n-m} \end{pmatrix} &= \begin{pmatrix} y_1 & y_2 \\ y_2^T & y_1^{-1}[y_2] + y_4 - y_1^{-1}[y_2] \end{pmatrix} \\ &= \begin{pmatrix} y_1 & y_2 \\ y_2^T & y_4 \end{pmatrix} = y. \quad \square \end{aligned}$$

Für positiv definite Matrizen können wir sogar die positive Definitheit wichtiger Bestandteile von (3.1) zeigen [32, S. 18].

Lemma 3.1.2. Sei $y = \begin{pmatrix} y_1 & y_2 \\ y_2^T & y_4 \end{pmatrix} \in \mathbb{P}_n$ mit $y_1 \in M_m(\mathbb{R})$, $1 \leq m \leq n-1$. Dann ist $y_1 \in \mathbb{P}_m$ und y lässt sich gemäß (3.1) mit $y_4 - y_1^{-1}[y_2] \in \mathbb{P}_{n-m}$ zerlegen.

Beweis. Mit y sind auch y_1 und y_4 symmetrisch. Aus $y_1[v] = y \left[\begin{pmatrix} v \\ 0 \end{pmatrix} \right] > 0$, $v \in \mathbb{R}^m \setminus \{0\}$, folgt, dass y_1 positiv definit und somit invertierbar ist. Daher ist Lemma 3.1.1 auf y anwendbar. Um zu zeigen, dass die symmetrische Matrix $y_4 - y_1^{-1}[y_2]$ positiv definit ist, schreiben wir (3.1) als

$$y \left[\begin{pmatrix} I_m & y_1^{-1} \cdot y_2 \\ 0 & I_{n-m} \end{pmatrix}^{-1} \right] = \begin{pmatrix} y_1 & 0 \\ 0 & y_4 - y_1^{-1}[y_2] \end{pmatrix}. \quad (3.2)$$

Nach Bemerkung 2.1.5(c) stellt (3.2) eine positiv definite Matrix dar. Aus

$$(y_4 - y_1^{-1}[y_2])[w] = \begin{pmatrix} y_1 & 0 \\ 0 & y_4 - y_1^{-1}[y_2] \end{pmatrix} \left[\begin{pmatrix} 0 \\ w \end{pmatrix} \right] > 0, \quad w \in \mathbb{R}^{n-m} \setminus \{0\},$$

folgt auch die positive Definitheit von $y_4 - y_1^{-1}[y_2]$. □

Anwendung findet Lemma 3.1.2 im folgenden Satz [28, S. 190], [32, S. 18], [47, S. 129].

Satz 3.1.3 (Jacobi – Zerlegung). *Sei $y \in \mathbb{P}_n$. Dann gibt es $d_\ell > 0$, $1 \leq \ell \leq n$, und eine obere Dreiecksmatrix $b \in \text{GL}_n(\mathbb{R})$ mit*

$$b_{\ell,r} = \begin{cases} 1, & \text{wenn } 1 \leq r = \ell \leq n, \\ 0, & \text{wenn } 1 \leq r < \ell \leq n, \end{cases}$$

sodass

$$y = \text{diag}(d_1, \dots, d_n)[b] \quad \text{gilt.} \quad (3.3)$$

Beweis. Wir beweisen die Aussage per Induktion über n . Für $n = 1$ schreiben wir $y = y[(1)]$. Sei $n \geq 2$ und wir setzen voraus, dass die Aussage für $n - 1$ gilt. Sei $y \in \mathbb{P}_n$. Das Lemma 3.1.2 mit $m = 1$ zeigt die Existenz von $x \in \mathbb{P}_{n-1}$ und $v \in \mathbb{R}^{n-1}$ mit der Eigenschaft

$$y = \begin{pmatrix} y_{1,1} & 0 \\ 0 & x \end{pmatrix} \left[\begin{pmatrix} 1 & v^T \\ 0 & I_{n-1} \end{pmatrix} \right]. \quad (3.4)$$

Nach Induktionsvoraussetzung hat x eine Jacobi – Zerlegung der Gestalt

$$x = \text{diag}(d_1, \dots, d_{n-1})[b], \quad (3.5)$$

wobei $d_\ell > 0$, $1 \leq \ell \leq n - 1$, gilt und $b \in \text{GL}_{n-1}(\mathbb{R})$ eine obere Dreiecksmatrix mit Einsen auf der Diagonalen ist. Damit berechnen wir

$$\begin{aligned} \text{diag}(y_{1,1}, d_1, \dots, d_{n-1}) \left[\begin{pmatrix} 1 & v^T \\ 0 & b \end{pmatrix} \right] &= \begin{pmatrix} y_{1,1} & 0 \\ 0 & x[b^{-1}] \end{pmatrix} \left[\begin{pmatrix} 1 & v^T \\ 0 & b \end{pmatrix} \right] \\ &= \begin{pmatrix} y_{1,1} & 0 \\ 0 & x \end{pmatrix} \left[\begin{pmatrix} 1 & 0 \\ 0 & b^{-1} \end{pmatrix} \cdot \begin{pmatrix} 1 & v^T \\ 0 & b \end{pmatrix} \right] \\ &= \begin{pmatrix} y_{1,1} & 0 \\ 0 & x \end{pmatrix} \left[\begin{pmatrix} 1 & v^T \\ 0 & I_{n-1} \end{pmatrix} \right] = y. \end{aligned}$$

Also hat auch y eine Jacobi – Zerlegung. □

Korollar 3.1.4 (Ungleichung von Hadamard). [28, S. 190, 191] *Sei $y \in \mathbb{P}_n$. Dann gilt*

$$\det(y) \leq \prod_{r=1}^n y_{r,r}.$$

Beweis. Das (ℓ, r) – te Element, $1 \leq \ell \leq r \leq n$, der Jacobi – Zerlegung (3.3) von y ergibt sich zu $y_{\ell,r} = \sum_{k=1}^{\ell} d_k b_{k,\ell} b_{k,r}$. Für $\ell = r$ erhalten wir

$$y_{r,r} = \sum_{k=1}^r d_k b_{k,r}^2 = d_r + \sum_{k=1}^{r-1} d_k b_{k,r}^2 \geq d_r.$$

Mit $\det(b) = 1$ folgt daraus schließlich

$$\det(y) = \det(\text{diag}(d_1, \dots, d_n)) = \prod_{r=1}^n d_r \leq \prod_{r=1}^n y_{r,r}. \quad \square$$

Die Ungleichung von Hadamard (Korollar 3.1.4) kann wie folgt geometrisch interpretiert werden [35, S. 14], [39, S. 262], [62, S. 126, 128]:

Bemerkung 3.1.5. Sei $a = (a_1 | \dots | a_n) \in \text{GL}_n(\mathbb{R})$. Das n -dimensionale Volumen des von den Spalten a_1, \dots, a_n aufgespannten Parallelepipeds im \mathbb{R}^n beträgt $|\det(a)|$. Definieren wir die Matrix $y := a^T \cdot a = I_n[a] \in \mathbb{P}_n$, so gilt nach der Ungleichung von Hadamard

$$(\det(a))^2 = \det(y) \leq \prod_{r=1}^n y_{r,r} = \prod_{r=1}^n \|a_r\|^2 \quad \text{und} \quad |\det(a)| \leq \prod_{r=1}^n \|a_r\|.$$

Das Volumen eines Parallelepipeds, das von Vektoren fester Länge aufgespannt wird, kann also durch paarweise orthogonal aufeinanderstehende Vektoren maximiert werden.

3.2 Die Ungleichung von Hermite

Bemerkung 3.2.1. [16, S. 31], [32, S. 20], [38, S. 263]

- (a) Sei $y \in \mathbb{P}_n$. Nach Korollar 2.2.2 gibt es zu $t \in \mathbb{R}$ nur endlich viele $g \in \mathbb{Z}^n$ mit $y[g] \leq t$. Daher existiert

$$\mu(y) := \min_{g \in \mathbb{Z}^n \setminus \{0\}} y[g]. \tag{3.6}$$

- (b) Für jedes $\tilde{g} \in \mathbb{Z}^n \setminus \{0\}$ gibt es ein $d \in \mathbb{N}$ und einen Vektor $g \in \mathbb{Z}^n \setminus \{0\}$, dessen Einträge teilerfremd sind, mit $\tilde{g} = d \cdot g$. Für $y \in \mathbb{P}_n$ ist dann $y[\tilde{g}] = d^2 \cdot y[g] \geq y[g]$, weshalb das Minimum (3.6) in einem Vektor mit teilerfremden Einträgen angenommen.

Für $y \in \mathbb{P}_n$, $\lambda > 0$, gilt $\mu(\lambda y) = \lambda \cdot \mu(y)$ und $\det(\lambda y) = \lambda^n \cdot \det(y)$. Es erscheint daher sinnvoll, $\mu(y)$ mit $(\det(y))^{\frac{1}{n}}$ zu vergleichen [28, S. 191], [32, S. 19, 20], [35, S. 14, 15], [38, S. 264, 265].

Lemma 3.2.2 (Ungleichung von Hermite). *Sei $y \in \mathbb{P}_n$. Dann gilt*

$$\mu(y) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \cdot (\det(y))^{\frac{1}{n}}.$$

Beweis. Wir führen den Beweis per Induktion über n . Für $n = 1$ gilt die Aussage wegen $\mu(y) = y = \det(y)$. Sei $n \geq 2$. Die Induktionsvoraussetzung besagt, dass die Behauptung für $n - 1$ gilt. Sei $y \in \mathbb{P}_n$. Der Bemerkung 3.2.1(b) zufolge gibt es ein $g \in \mathbb{Z}^n \setminus \{0\}$ mit teilerfremden Einträgen, sodass $y[g] = \mu[y]$ gilt. Aufgrund von Lemma 2.5.10 kommt dieser Vektor g als erste Spalte einer unimodularen Matrix $u \in \text{GL}_n(\mathbb{Z})$ vor. Daher ist

$$\mu(y[u]) = \min_{\tilde{g} \in \mathbb{Z}^n \setminus \{0\}} y[u\tilde{g}] \leq y[ue_1] = y[g] = \mu(y).$$

Andererseits gilt per Definition auch $\mu(y[u]) \geq \mu(y)$, zusammen also $\mu(y[u]) = \mu(y)$. Da auch $\det(y[u]) = \det(y)$ gilt, ändert sich die Aussage des Lemmas nicht, falls wir y durch $y[u]$ ersetzen. Wir können daher annehmen, dass das Minimum $\mu(y)$ in $g = e_1$ angenommen wird, das heißt $y_{1,1} = y[e_1] = \mu(y)$. Wir nutzen jetzt Lemma 3.1.2 mit $m = 1$, um eine Zerlegung von y als

$$y = \begin{pmatrix} y_{1,1} & 0 \\ 0 & x \end{pmatrix} \left[\begin{pmatrix} 1 & v^T \\ 0 & I_{n-1} \end{pmatrix} \right] \quad \text{mit } x \in \mathbb{P}_{n-1} \text{ und } v \in \mathbb{R}^{n-1} \text{ zu erhalten.}$$

Für jedes $w = \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \in \mathbb{R}^n$, $w_1 \in \mathbb{R}$, $w_2 \in \mathbb{R}^{n-1}$, gilt damit

$$\begin{aligned} y[w] &= \begin{pmatrix} y_{1,1} & 0 \\ 0 & x \end{pmatrix} \left[\begin{pmatrix} 1 & v^T \\ 0 & I_{n-1} \end{pmatrix} \cdot \begin{pmatrix} w_1 \\ w_2 \end{pmatrix} \right] = \begin{pmatrix} y_{1,1} & 0 \\ 0 & x \end{pmatrix} \left[\begin{pmatrix} w_1 + v^T \cdot w_2 \\ w_2 \end{pmatrix} \right] \\ &= \begin{pmatrix} w_1 + v^T \cdot w_2 \\ w_2 \end{pmatrix}^T \cdot \begin{pmatrix} y_{1,1} & 0 \\ 0 & x \end{pmatrix} \cdot \begin{pmatrix} w_1 + v^T \cdot w_2 \\ w_2 \end{pmatrix} \\ &= y_{1,1} \cdot (w_1 + v^T \cdot w_2)^2 + x[w_2]. \end{aligned}$$

Wir wählen nun $w_2 \in \mathbb{Z}^{n-1} \setminus \{0\}$ derart, dass das Minimum $\mu(x)$ in w_2 angenommen wird, das heißt $x[w_2] = \mu(x)$. Anschließend wählen wir $w_1 \in \mathbb{Z}$ so, dass $|w_1 + v^T \cdot w_2| \leq \frac{1}{2}$ gilt. Dies liefert nun

$$\mu(y) \leq y[w] = y_{1,1} \cdot (w_1 + v^T \cdot w_2)^2 + x[w_2] \leq \frac{1}{4}y_{1,1} + \mu(x) = \frac{1}{4}\mu(y) + \mu(x).$$

Wir wenden auf x die Induktionsvoraussetzung an und erhalten

$$\mu(y) \leq \frac{4}{3}\mu(x) \leq \left(\frac{4}{3}\right)^{\frac{n}{2}} \cdot (\det(x))^{\frac{1}{n-1}}$$

sowie

$$(\mu(y))^n = y_{1,1} \cdot (\mu(y))^{n-1} \leq \left(\frac{4}{3}\right)^{\frac{n(n-1)}{2}} \cdot y_{1,1} \cdot \det(x) = \left(\frac{4}{3}\right)^{\frac{n(n-1)}{2}} \cdot \det(y).$$

Daraus ergibt sich schließlich

$$\mu(y) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \cdot (\det(y))^{\frac{1}{n}}. \quad \square$$

3.3 Die Minkowskische Reduktionstheorie

Wir betrachten die unimodulare Gruppe $\mathrm{GL}_n(\mathbb{Z})$, die nach Lemma 2.4.15 auf \mathbb{P}_n durch

$$\begin{aligned} \mathrm{GL}_n(\mathbb{Z}) \times \mathbb{P}_n &\longrightarrow \mathbb{P}_n \\ (u, y) &\longmapsto y[u^T] \end{aligned}$$

operiert [35, S. 11], [47, S. 122].

Die Bahnen $\{y[u] \mid u \in \mathrm{GL}_n(\mathbb{Z})\}$, $y \in \mathbb{P}_n$, dieser Operation sind genau die Äquivalenzklassen der Äquivalenzrelation, die durch folgende Definition gegeben ist [25, S. 218, 221], [35, S. 11], [38, S. 263], [61, S. 47]:

Definition 3.3.1. Zwei Matrizen $y, \tilde{y} \in \mathbb{P}_n$ heißen *äquivalent*, falls es ein $u \in \mathrm{GL}_n(\mathbb{Z})$ mit $\tilde{y} = y[u]$ gibt.

Die Aufgabe der Minkowskischen Reduktionstheorie besteht nun darin, aus jeder Bahn $\{y[u] \mid u \in \mathrm{GL}_n(\mathbb{Z})\}$, $y \in \mathbb{P}_n$, einen Repräsentanten auszuwählen [16, S. 30], [35, S. 11].

In [48] führt Minkowski die später nach ihm benannten Reduktionsbedingungen ein [3, S. 13], [16, S. 33], [35, S. 12], [47, S. 123], [48, S. 228]:

Definition 3.3.2. Eine Matrix $y \in \mathbb{P}_n$ heißt *minkowskireduziert*, falls die folgenden Bedingungen gelten:

- (a) $y[g] \geq y_{\ell,\ell}$ für alle $1 \leq \ell \leq n$ und alle $g = (g_1, \dots, g_n)^T \in \mathbb{Z}^n \setminus \{\pm e_\ell\}$, $\text{ggT}(g_\ell, \dots, g_n) = 1$.
- (b) $y_{\ell-1,\ell} \geq 0$ für alle $2 \leq \ell \leq n$.

Die Menge aller minkowskireduzierten $n \times n$ -Matrizen bezeichnen wir mit \mathcal{M}_n .

Bemerkung 3.3.3. [35, S. 23] Wir schließen dabei in Definition 3.3.2(a) den kanonischen Einheitsvektor e_ℓ und sein Negatives aus, da dies die Formulierung späterer Aussagen erleichtert und $y[\pm e_\ell] = y_{\ell,\ell}$ sowieso immer gilt.

Beispiel 3.3.4. [3, S. 53] Wir wollen die Bedingungen aus Definition 3.3.2 für die symmetrische Matrix

$$y := \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \in M_2(\mathbb{R}) \quad \text{überprüfen:}$$

Wegen $y_{1,1} = 1 > 0$ und $\det(y) = 1 - \frac{1}{4} = \frac{3}{4} > 0$ gilt $y \in \mathbb{P}_2$. Da y halbganz ist, folgt unter Verwendung von Lemma 2.2.4(d), dass $y[g] \in \mathbb{Z}_{>0} = \mathbb{N}$ für alle $g \in \mathbb{Z}^2 \setminus \{(0,0)^T\}$ gilt, also $y[g] \geq 1 = y_{1,1} = y_{2,2}$ für alle $g \in \mathbb{Z}^2 \setminus \{(0,0)^T\}$. Dies zeigt Bedingung (a) aus Definition 3.3.2.

Da auch Bedingung (b) wegen $y_{1,2} = \frac{1}{2} \geq 0$ gilt, ist y minkowskireduziert.

Um für $y \in \mathbb{P}_n$ einen geeigneten Repräsentanten aus der Bahn $\{y[u] \mid u \in \text{GL}_n(\mathbb{Z})\}$ auszuwählen, werden die Spalten der unimodularen Matrix $u = (u_1 | \dots | u_n) \in \text{GL}_n(\mathbb{Z})$ sukzessive bestimmt [3, S. 46].

Wir beginnen unsere Untersuchungen mit dem folgenden Lemma [3, S. 46 – 48], [47, S. 122, 123]:

Lemma 3.3.5. *Seien $u, \tilde{u} \in \text{GL}_n(\mathbb{Z})$ und $1 \leq \ell \leq n+1$. Dann stimmen die ersten $\ell-1$ Spalten von u und \tilde{u} genau dann überein, wenn es $b \in M_{\ell-1, n-\ell+1}(\mathbb{Z})$ und $d \in \text{GL}_{n-\ell+1}(\mathbb{Z})$ mit*

$$\tilde{u} = u \cdot \begin{pmatrix} I_{\ell-1} & b \\ 0 & d \end{pmatrix} \quad \text{gibt.}$$

Beweis. Offensichtlich stimmen die ersten $\ell-1$ Spalten von u und $u \cdot \begin{pmatrix} I_{\ell-1} & b \\ 0 & d \end{pmatrix}$ überein.

Umgekehrt sei vorausgesetzt, dass u und \tilde{u} dieselben ersten $\ell-1$ Spalten besitzen. Dann stimmen auch die ersten $\ell-1$ Spalten von $u^{-1} \cdot \tilde{u}$ und $u^{-1} \cdot u = I_n$ überein, weshalb wir

$$\text{GL}_n(\mathbb{Z}) \ni u^{-1} \cdot \tilde{u} = \begin{pmatrix} I_{\ell-1} & b \\ 0 & d \end{pmatrix}$$

mit $b \in M_{\ell-1, n-\ell+1}(\mathbb{Z})$ und $d \in M_{n-\ell+1}(\mathbb{Z})$ schreiben können. Aus $\pm 1 = \det(u^{-1} \cdot \tilde{u}) = \det(d)$ folgt schließlich, dass d unimodular ist. \square

Für $1 \leq \ell \leq n$ definieren wir die Menge

$$\Lambda_{\ell,n} := \{(u_1 | \dots | u_\ell) \in M_{n,\ell}(\mathbb{Z}) \mid (u_1 | \dots | u_\ell | * | \dots | *) \in \text{GL}_n(\mathbb{Z})\}$$

der Matrizen, die aus den ersten ℓ Spalten von unimodularen $n \times n$ -Matrizen bestehen, und

$$G_{\ell,n} := \{(g_1, \dots, g_n)^T \in \mathbb{Z}^n \mid \text{ggT}(g_\ell, \dots, g_n) = 1\}.$$

Lemma 3.3.6. [3, S. 46 – 48], [4, S. 12, 13] Sei $u = (u_1 | \dots | u_n) \in \mathrm{GL}_n(\mathbb{Z})$. Für jedes $1 \leq \ell \leq n$ gilt

$$\{v \in \mathbb{Z}^n \mid (u_1 | \dots | u_{\ell-1} | v) \in \Lambda_{\ell,n}\} = \{ug \mid g \in G_{\ell,n}\}.$$

Beweis. Sei zunächst $v \in \mathbb{Z}^n$ mit $(u_1 | \dots | u_{\ell-1} | v) \in \Lambda_{\ell,n}$. Es gibt also eine unimodulare Matrix $\tilde{u} \in \mathrm{GL}_n(\mathbb{Z})$, deren erste $\ell - 1$ Spalten mit denen von u übereinstimmen und deren $\ell -$ te Spalte genau v ist. Lemma 3.3.5 ergibt nun die Existenz von $b \in M_{\ell-1, n-\ell+1}(\mathbb{Z})$ und $d \in \mathrm{GL}_{n-\ell+1}(\mathbb{Z})$ mit

$$\tilde{u} = u \cdot \begin{pmatrix} I_{\ell-1} & b \\ 0 & d \end{pmatrix}.$$

Bezeichnen wir die erste Spalte von b mit $b_1 \in \mathbb{Z}^{\ell-1}$ und die erste Spalte von d mit $d_1 \in \mathbb{Z}^{n-\ell+1}$, so erhalten wir außerdem, dass für die $\ell -$ te Spalte v von \tilde{u} nun $v = u \cdot \begin{pmatrix} b_1 \\ d_1 \end{pmatrix}$ gilt. Als Spalte einer unimodularen Matrix sind die Einträge von d_1 teilerfremd (Lemma 2.5.10). Daher gilt $v \in \{ug \mid g \in G_{\ell,n}\}$.

Umgekehrt sei $v \in \{ug \mid g \in G_{\ell,n}\}$ vorausgesetzt, das heißt, es gibt $g = (g_1, \dots, g_n)^T \in \mathbb{Z}^n$ mit $\mathrm{ggT}(g_\ell, \dots, g_n) = 1$ und $v = ug$. Nach Lemma 2.5.10 existiert ein $d \in \mathrm{GL}_{n-\ell+1}(\mathbb{Z})$ mit erster Spalte $(g_\ell, \dots, g_n)^T$. Wählen wir ein $b \in M_{\ell-1, n-\ell+1}(\mathbb{Z})$ mit erster Spalte $(g_1, \dots, g_{\ell-1})^T$, so ist v die $\ell -$ te Spalte der unimodularen Matrix

$$u \cdot \begin{pmatrix} I_{\ell-1} & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_n(\mathbb{Z}),$$

deren erste $\ell - 1$ Spalten mit denen von u übereinstimmen. Also ist $(u_1 | \dots | u_{\ell-1} | v) \in \Lambda_{\ell,n}$. \square

Hiermit können wir schließlich beweisen, dass wir aus jedem $\{y[u] \mid u \in \mathrm{GL}_n(\mathbb{Z})\}$, $y \in \mathbb{P}_n$, einen minkowskireduzierten Repräsentanten auswählen können [3, S. 46 – 48], [4, S. 12, 13], [16, S. 32, 33], [32, S. 26], [47, S. 122, 123].

Satz 3.3.7. Zu jedem $y \in \mathbb{P}_n$ gibt es ein $u \in \mathrm{GL}_n(\mathbb{Z})$ mit $y[u] \in \mathcal{M}_n$.

Beweis. Wir konstruieren die gesuchte unimodulare Matrix $u \in \mathrm{GL}_n(\mathbb{Z})$ schrittweise: Im ersten Schritt wählen wir nach Bemerkung 3.2.1(b) einen Vektor $u_1 \in \mathbb{Z}^n \setminus \{0\}$ mit teilerfremden Einträgen, der $y[u_1] = \mu(y)$ erfüllt. Lemma 2.5.10 ergibt dann eine unimodulare Matrix $u^{(1)} = (u_1 | * | \dots | *) \in \mathrm{GL}_n(\mathbb{Z})$ mit erster Spalte u_1 .

Im $\ell -$ ten Schritt, $2 \leq \ell \leq n$, liegen uns bereits die Vektoren $u_1, \dots, u_{\ell-1} \in \mathbb{Z}^n \setminus \{0\}$ und eine unimodulare Matrix $u^{(\ell-1)} = (u_1 | \dots | u_{\ell-1} | * | \dots | *) \in \mathrm{GL}_n(\mathbb{Z})$ vor. Dann wählen wir $u_\ell \in \{u^{(\ell-1)} \cdot g \mid g \in G_{\ell,n}\}$ derart, dass

$$y[u_\ell] \leq y[u^{(\ell-1)} \cdot g] \quad \text{für alle } g \in G_{\ell,n} \text{ gilt.} \quad (3.7)$$

(Nach Korollar 2.2.2 existiert das Minimum.)

Ohne Beschränkung der Allgemeinheit können wir dabei $u_{\ell-1}^T \cdot y \cdot u_\ell \geq 0$ annehmen; ansonsten nämlich ersetzen wir u_ℓ durch $-u_\ell$. Dies ändert die Minimalität in (3.7) nicht. Aus Lemma 3.3.6 folgt die Existenz einer unimodularen Matrix $u^{(\ell)} = (u_1 | \dots | u_{\ell-1} | u_\ell | * | \dots | *) \in \mathrm{GL}_n(\mathbb{Z})$, deren erste ℓ Spalten durch u_1, \dots, u_ℓ gegeben sind.

Nach n Schritten ergibt sich schließlich $u := u^{(n)} = (u_1 | \dots | u_n) \in \mathrm{GL}_n(\mathbb{Z})$.

Wir zeigen nun, dass $y[u] \in \mathbb{P}_n$ minkowskireduziert ist: Da die ersten $\ell - 1$ Spalten von u und $u^{(\ell-1)}$ übereinstimmen, ergibt sich aus Lemma 3.3.6 die Beziehung

$$\{ug \mid g \in G_{\ell,n}\} = \{u^{(\ell-1)} \cdot g \mid g \in G_{\ell,n}\} \quad \text{für alle } 2 \leq \ell \leq n.$$

Für alle $2 \leq \ell \leq n$ und alle $g \in G_{\ell,n}$ folgt daher aus Formel (3.7) die Ungleichung

$$(y[u])_{\ell,\ell} = y[u_\ell] \leq y[ug] = (y[u])[g].$$

Für alle $g \in \mathbb{Z}^n \setminus \{0\}$ ist

$$(y[u])_{1,1} = y[u_1] = \mu(y) \leq y[ug] = (y[u])[g].$$

Daher erfüllt $y[u]$ die Bedingung (a) aus Definition 3.3.2. Nach unserer Wahl der Spalten von u gilt aber auch

$$(y[u])_{\ell-1,\ell} = u_{\ell-1}^T \cdot y \cdot u_\ell \geq 0 \quad \text{für alle } 2 \leq \ell \leq n.$$

Dies ist gerade Bedingung (b) aus Definition 3.3.2 für $y[u]$. Damit ist schließlich $y[u] \in \mathcal{M}_n$ bewiesen. \square

Korollar 3.3.8. [28, S. 191], [32, S. 26], [47, S. 139]

Es gilt

$$\mathbb{P}_n = \bigcup_{u \in \text{GL}_n(\mathbb{Z})} \mathcal{M}_n[u].$$

Wir wenden die Konstruktion aus dem Beweis von Satz 3.3.7 auf ein Beispiel an [32, S. 27]:

Beispiel 3.3.9. Sei $y := \begin{pmatrix} 5 & -\frac{3}{4} \\ -\frac{3}{4} & 1 \end{pmatrix} \in M_2(\mathbb{R})$. Das charakteristische Polynom χ von y ist

$$\chi(\lambda) = \det(y - \lambda I_2) = \det \begin{pmatrix} 5 - \lambda & -\frac{3}{4} \\ -\frac{3}{4} & 1 - \lambda \end{pmatrix} = \lambda^2 - 6\lambda + \frac{71}{16}.$$

Dessen Nullstellen, also die Eigenwerte von y , sind $3 \pm \frac{\sqrt{73}}{4} > 0$. Daher ist $y \in \mathbb{P}_2$. Wegen $y_{1,2} = -\frac{3}{4} < 0$ ist aber y nicht minkowskireduziert.

Um ein $u \in \text{GL}_2(\mathbb{Z})$ mit $y[u] \in \mathcal{M}_2$ zu finden, gehen wir wie im Beweis von Satz 3.3.7 vor: Zunächst müssen wir einen Vektor $u_1 \in \mathbb{Z}^2 \setminus \{(0,0)^T\}$ mit teilerfremden Einträgen finden, der $y[u_1] = \mu(y)$ erfüllt. Dazu nutzen wir Korollar 2.2.1 und dessen Beweis. Wegen $3 \pm \frac{\sqrt{73}}{4} > 3 - \frac{9}{4} = \frac{3}{4}$ gilt $y > \frac{3}{4}I_2$. Für alle $g \in \mathbb{Z}^2 \setminus \{(0,0)^T\}$ ist also $y[g] > \frac{3}{4}\|g\|^2$. Im Fall $\|g\|^2 \geq 2$ erhalten wir

$$y[g] > \frac{3}{4}\|g\|^2 \geq \frac{3}{4} \cdot 2 = \frac{3}{2} > 1 = y_{2,2} = y[\pm e_2].$$

Ansonsten ist $\|g\|^2 \leq 1$ und $g \in \{\pm e_1, \pm e_2\}$. Aus

$$y[\pm e_1] = y_{1,1} = 5 > 1 = y_{2,2} = y[\pm e_2]$$

erhalten wir $u_1 = e_2$ als mögliche Wahl von u_1 . Als $u^{(1)} \in \text{GL}_2(\mathbb{Z})$ mit erster Spalte $u_1 = e_2$ wählen wir $u^{(1)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Im nächsten Schritt betrachten wir die Menge

$$\{u^{(1)} \cdot g \mid g \in G_{2,2}\} = \left\{ \pm u^{(1)} \cdot \begin{pmatrix} g_1 \\ 1 \end{pmatrix} \mid g_1 \in \mathbb{Z} \right\} = \left\{ \pm \begin{pmatrix} 1 \\ g_1 \end{pmatrix} \mid g_1 \in \mathbb{Z} \right\}.$$

Um daraus einen Vektor u_2 auszuwählen, der (3.7) für $\ell = n = 2$ erfüllt, führen wir wieder Abschätzungen durch: Falls $g_1^2 \geq 5$ gilt, erhalten wir

$$y \left[\pm \begin{pmatrix} 1 \\ g_1 \end{pmatrix} \right] > \frac{3}{4} \cdot (1^2 + g_1^2) \geq \frac{3}{4} \cdot (1 + 5) = \frac{9}{2}.$$

Ansonsten ist $g_1^2 \leq 4$, also $g_1 \in \{0, \pm 1, \pm 2\}$ und

$$\pm \begin{pmatrix} 1 \\ g_1 \end{pmatrix} \in \left\{ \pm e_1, \pm \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \pm \begin{pmatrix} 1 \\ -1 \end{pmatrix}, \pm \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \pm \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right\}.$$

Für diese berechnen wir

$$\begin{aligned} y[\pm e_1] &= y_{1,1} = 5, \\ y \left[\pm \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right] &= \frac{9}{2}, \\ y \left[\pm \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right] &= \frac{15}{2}, \\ y \left[\pm \begin{pmatrix} 1 \\ 2 \end{pmatrix} \right] &= 6, \\ y \left[\pm \begin{pmatrix} 1 \\ -2 \end{pmatrix} \right] &= 12. \end{aligned}$$

Die Minimalbedingung (3.7) für $\ell = n = 2$ kann daher durch $u_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ erreicht werden. Wegen $u_1^T \cdot y \cdot u_2 = \frac{1}{4} \geq 0$ können wir schließlich u angeben durch $u = u^{(2)} = (u_1 | u_2) = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$. Damit ist

$$y[u] = \begin{pmatrix} 1 & \frac{1}{4} \\ \frac{1}{4} & \frac{9}{2} \end{pmatrix} \in \mathcal{M}_2.$$

Der Rand $\partial \mathcal{M}_n$ von \mathcal{M}_n in \mathbb{P}_n wird gegeben durch

$$\partial \mathcal{M}_n = \{y \in \mathbb{P}_n \mid y \text{ erfüllt die Ungleichungen in Definition 3.3.2 mit mindestens einem „=“}\}.$$

Das heißt, dass $y \in \mathcal{M}_n$ genau dann ein Randpunkt von \mathcal{M}_n ist, wenn *mindestens eine* der folgenden Bedingungen gilt:

- (a) Es gibt ein $1 \leq \ell \leq n$ und ein $g \in G_{\ell,n} \setminus \{\pm e_\ell\}$ mit $y[g] = y_{\ell,\ell}$.
- (b) Es gibt ein $2 \leq \ell \leq n$ mit $y_{\ell-1,\ell} = 0$.

Insbesondere ist \mathcal{M}_n in \mathbb{P}_n abgeschlossen [3, S. 48], [35, S. 27]. Das Innere $\overset{\circ}{\mathcal{M}}_n$ von \mathcal{M}_n in \mathbb{P}_n ist gegeben durch

$$\overset{\circ}{\mathcal{M}}_n = \{y \in \mathbb{P}_n \mid y \text{ erfüllt alle Ungleichungen in Definition 3.3.2 mit „>“}\}.$$

Satz 3.3.10. [4, S. 14], [35, S. 24, 25], [47, S. 136, 137]

Seien $y, \tilde{y} \in \mathcal{M}_n$ mit $\tilde{y} = y[u]$ für ein $u \in \mathrm{GL}_n(\mathbb{Z}) \setminus \{\pm I_n\}$. Dann gilt $y, \tilde{y} \in \partial\mathcal{M}_n$.

Beweis. Wir machen eine Fallunterscheidung für u :

Fall (a): Falls u eine Diagonalmatrix ist, folgt aus

$$\pm 1 = \det(u) = \det(\mathrm{diag}(u_{1,1}, \dots, u_{n,n})) = \prod_{r=1}^n u_{r,r}$$

und der Ganzzahligkeit der Einträge, dass $u_{r,r} \in \{\pm 1\}$ für alle $1 \leq r \leq n$ gilt. Wegen $u \neq \pm I_n$ gibt es dabei unter $u_{r,r}$, $1 \leq r \leq n$, einen Vorzeichenwechsel. Indem wir gegebenenfalls u durch $-u$ ersetzen, können wir annehmen, dass es ein $2 \leq \ell \leq n$ mit $u_{\ell-1, \ell-1} = -1$ und $u_{\ell, \ell} = 1$ gibt. Da \tilde{y} und y minkowskireduziert sind, folgt

$$0 \leq \tilde{y}_{\ell-1, \ell} = (y[u])_{\ell-1, \ell} = -e_{\ell-1}^T \cdot y \cdot e_\ell = -y_{\ell-1, \ell} \leq 0,$$

also $\tilde{y}_{\ell-1, \ell} = y_{\ell-1, \ell} = 0$. Daraus schließen wir $y, \tilde{y} \in \partial\mathcal{M}_n$.

Fall (b): Sei $u = (u_1 | \dots | u_n)$ keine Diagonalmatrix. Dann existiert

$$\ell := \min_{\substack{1 \leq k \leq n \\ u_k \neq \pm e_k}} k \tag{3.8}$$

und u hat die Gestalt¹

$$u = \begin{pmatrix} u_1^{(\ell-1)} & u_2^{(\ell-1)} \\ 0 & u_4^{(\ell-1)} \end{pmatrix},$$

wobei $u_1^{(\ell-1)} \in M_{\ell-1}(\mathbb{Z})$ eine Diagonalmatrix ist, die $(u_1^{(\ell-1)})_{r,r} \in \{\pm 1\}$ für alle $1 \leq r \leq \ell-1$ erfüllt. Dies ergibt $\pm 1 = \det(u) = \pm \det(u_1^{(\ell-1)})$ und $u_4^{(\ell-1)} \in \mathrm{GL}_{n-\ell+1}(\mathbb{Z})$ ist unimodular. Wegen Lemma 2.5.10 besteht die erste Spalte von $u_4^{(\ell-1)}$ aus teilerfremden Einträgen. Dies bedeutet $u_\ell \in G_{\ell, n} \setminus \{\pm e_\ell\}$, woraus wir mit $y \in \mathcal{M}_n$ die Ungleichung

$$\tilde{y}_{\ell, \ell} = (y[u])_{\ell, \ell} = y[u_\ell] \geq y_{\ell, \ell} \quad \text{bekommen.}$$

Wir können diese Argumentation auch für $u^{-1} = ((u^{-1})_1 | \dots | (u^{-1})_n) \in \mathrm{GL}_n(\mathbb{Z})$ wiederholen: Die Analyse der k -ten Spalten in $u^{-1} \cdot u = I_n = u \cdot u^{-1}$ zeigt zunächst, dass $u_k = \pm e_k$ genau dann gilt, wenn $(u^{-1})_k = \pm e_k$ gilt. Für das in (3.8) definierte ℓ ist daher auch

$$\ell = \min_{\substack{1 \leq k \leq n \\ (u^{-1})_k \neq \pm e_k}} k.$$

Wir erhalten dann $(u^{-1})_\ell \in G_{\ell, n} \setminus \{\pm e_\ell\}$ und

$$y_{\ell, \ell} = (\tilde{y} [u^{-1}])_{\ell, \ell} = \tilde{y} [(u^{-1})_\ell] \geq \tilde{y}_{\ell, \ell}.$$

Insgesamt haben wir damit $u_\ell, (u^{-1})_\ell \in G_{\ell, n} \setminus \{\pm e_\ell\}$ mit

$$y[u_\ell] = \tilde{y}_{\ell, \ell} = y_{\ell, \ell} = \tilde{y} [(u^{-1})_\ell].$$

Daraus schließen wir $y, \tilde{y} \in \partial\mathcal{M}_n$. □

¹Notation gemäß (1.3).

Aus Satz 3.3.10 erhalten wir insbesondere

Korollar 3.3.11. [4, S. 14] *Zwei verschiedene innere Elemente von \mathcal{M}_n gehören nie derselben Bahn an.*

Die Sätze 3.3.7 und 3.3.10 charakterisieren die abgeschlossene Menge \mathcal{M}_n als sogenannten Fundamentalbereich der Operation von $\mathrm{GL}_n(\mathbb{Z})$ auf \mathbb{P}_n [4, S. 14], [47, S. 139], gegeben durch

$$\begin{aligned} \mathrm{GL}_n(\mathbb{Z}) \times \mathbb{P}_n &\longrightarrow \mathbb{P}_n \\ (u, y) &\longmapsto y[u^T]. \end{aligned}$$

3.4 Ungleichungen in der Minkowskischen Reduktionstheorie

Lemma 3.4.1. [4, S. 14], [28, S. 192], [32, S. 28, 29], [45, S. 35], [47, S. 123]

Seien $1 \leq m \leq n-1$ und $y = \begin{pmatrix} y_1^{(m)} & y_2^{(m)} \\ (y_2^{(m)})^T & y_4^{(m)} \end{pmatrix} \in \mathcal{M}_n$. Dann gelten folgende Aussagen:

- (a) $y_1^{(m)} \in \mathcal{M}_m$, $y_4^{(m)} \in \mathcal{M}_{n-m}$.
- (b) $0 < \mu(y) = y_{1,1} \leq y_{2,2} \leq \dots \leq y_{n,n}$.
- (c) $2|y_{\ell,r}| \leq y_{\ell,\ell}$ für alle $1 \leq \ell < r \leq n$.

Beweis. (a): Aus $(y_1^{(m)})[v] = y \begin{bmatrix} v \\ 0 \end{bmatrix} > 0$, $v \in \mathbb{R}^m \setminus \{0\}$, und $(y_4^{(m)})[w] = y \begin{bmatrix} 0 \\ w \end{bmatrix} > 0$, $w \in \mathbb{R}^{n-m} \setminus \{0\}$, folgt zum einen, dass die symmetrischen $y_1^{(m)}$ und $y_4^{(m)}$ positiv definit sind, und zum anderen, dass mit y auch $y_1^{(m)}$ und $y_4^{(m)}$ minkowskireduziert sind.

(b): Nach Definition des Minimums $\mu(y)$ gilt

$$0 < \mu(y) \leq y[e_1] = y_{1,1}.$$

Andererseits wissen wir nach Bemerkung 3.2.1(b), dass es einen Vektor $g \in \mathbb{Z}^n \setminus \{0\}$ mit teilerfremden Einträgen gibt, der $y[g] = \mu(y)$ erfüllt. Für diesen ergibt sich aus Definition 3.3.2(a) mit $\ell = 1$ aber auch die umgekehrte Ungleichung $\mu(y) = y[g] \geq y_{1,1}$. Damit ist zusammen $\mu(y) = y_{1,1}$.

Für die restliche Aussage in (b) betrachten wir $1 \leq \ell \leq n-1$ und wenden Definition 3.3.2(a) auf den $(\ell+1)$ -ten kanonischen Einheitsvektor $e_{\ell+1}$ an, der

$$\mathrm{ggT}((e_{\ell+1})_\ell, \dots, (e_{\ell+1})_n) = \mathrm{ggT}(0, 1, 0, \dots, 0) = 1 \quad \text{erfüllt.}$$

Dies ergibt $y_{\ell+1, \ell+1} = y[e_{\ell+1}] \geq y_{\ell, \ell}$.

(c): Seien $1 \leq \ell < r \leq n$. Die aus den kanonischen Einheitsvektoren gebildeten Vektoren $e_\ell \pm e_r$ erfüllen

$$\mathrm{ggT}((e_\ell \pm e_r)_r, \dots, (e_\ell \pm e_r)_n) = \mathrm{ggT}(\pm 1, 0, \dots, 0) = 1,$$

woraus wir $y[e_\ell \pm e_r] \geq y_{r,r}$ wegen Definition 3.3.2(a) schließen. Mit

$$y[e_\ell \pm e_r] = y[e_\ell] \pm e_\ell^T \cdot y \cdot e_r \pm e_r^T \cdot y \cdot e_\ell + y[e_r] = y_{\ell, \ell} \pm 2y_{\ell, r} + y_{r, r}$$

erhalten wir dann $y_{\ell, \ell} \pm 2y_{\ell, r} \geq 0$ und $2|y_{\ell, r}| \leq y_{\ell, \ell}$. □

Beispiel 3.4.2. [4, S. 15] Für $n = 2$ liefern Definition 3.3.2(b) und Lemma 3.4.1(b) und (c), dass

$$\mathcal{M}_2 \subset \left\{ \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{1,2} & y_{2,2} \end{pmatrix} \in \mathbb{P}_2 \mid 0 \leq 2y_{1,2} \leq y_{1,1} \leq y_{2,2} \right\} \quad \text{gilt.} \quad (3.9)$$

Wir wollen zeigen, dass auch die umgekehrte Inklusion gilt. Sei also $y = \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{1,2} & y_{2,2} \end{pmatrix} \in \mathbb{P}_2$ mit $0 \leq 2y_{1,2} \leq y_{1,1} \leq y_{2,2}$. Für $g = (g_1, g_2)^T \in \mathbb{Z}^2 \setminus \{(0,0)^T\}$ berechnen wir

$$y[g] = g_1^2 \cdot y_{1,1} + g_2^2 \cdot y_{2,2} + 2g_1 \cdot g_2 \cdot y_{1,2}$$

und betrachten zunächst $\ell = 1$ in Definition 3.3.2(a). Wir unterscheiden zwei Fälle:

Fall (a): Falls $g_1 \cdot g_2 \geq 0$ gilt, so ist

$$y[g] \geq g_1^2 \cdot y_{1,1} + g_2^2 \cdot y_{2,2} \begin{cases} \geq g_1^2 \cdot y_{1,1} \geq y_{1,1}, & \text{wenn } g_1 \neq 0, \\ = g_2^2 \cdot y_{2,2} \geq y_{2,2} \geq y_{1,1}, & \text{wenn } g_1 = 0. \end{cases}$$

Fall (b): Falls hingegen $g_1 \cdot g_2 < 0$ ist, erhalten wir

$$2g_1 \cdot g_2 \cdot y_{1,2} \geq g_1 \cdot g_2 \cdot y_{1,1} \geq -\max\{g_1^2, g_2^2\} \cdot y_{1,1}.$$

Dies liefert

$$y[g] \geq (g_1^2 - \max\{g_1^2, g_2^2\}) \cdot y_{1,1} + g_2^2 \cdot y_{2,2} \geq (g_1^2 + g_2^2 - \max\{g_1^2, g_2^2\}) \cdot y_{1,1} \geq y_{1,1}.$$

Also gilt Definition 3.3.2(a) für $\ell = 1$.

Sei jetzt $\ell = 2$. Wir müssen dann Vektoren $\pm \begin{pmatrix} g_1 \\ 1 \end{pmatrix}$, $g_1 \in \mathbb{Z}$, betrachten. Für diese gilt

$$y \left[\pm \begin{pmatrix} g_1 \\ 1 \end{pmatrix} \right] = g_1^2 \cdot y_{1,1} + y_{2,2} + 2g_1 \cdot y_{1,2} = g_1 \cdot (g_1 \cdot y_{1,1} + 2y_{1,2}) + y_{2,2}.$$

Für $g_1 \geq 0$ folgt sofort $y \left[\pm \begin{pmatrix} g_1 \\ 1 \end{pmatrix} \right] \geq y_{2,2}$, weshalb nun $g_1 < 0$ vorausgesetzt sei: Dann ist

$$g_1 \cdot y_{1,1} + 2y_{1,2} \leq g_1 \cdot y_{1,1} + y_{1,1} = (g_1 + 1) \cdot y_{1,1} \leq 0,$$

womit wir auch hier $y \left[\pm \begin{pmatrix} g_1 \\ 1 \end{pmatrix} \right] \geq y_{2,2}$ erhalten. Damit ist Definition 3.3.2(a) erfüllt.

Wegen $y_{1,2} \geq 0$ folgt schließlich $y \in \mathcal{M}_2$. Insgesamt haben wir daher

$$\mathcal{M}_2 = \left\{ \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{1,2} & y_{2,2} \end{pmatrix} \in \mathbb{P}_2 \mid 0 \leq 2y_{1,2} \leq y_{1,1} \leq y_{2,2} \right\}. \quad (3.10)$$

Beispiel 3.4.3. [28, S. 192], [48, S. 230] Aus (3.9) erhalten wir eine Abschätzung der Determinante einer minkowskireduzierten Matrix $y = \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{1,2} & y_{2,2} \end{pmatrix} \in \mathcal{M}_2$ durch ihre Diagonalelemente nach unten: Aus $0 \leq 2y_{1,2} \leq y_{1,1} \leq y_{2,2}$ folgt

$$\begin{aligned} \det(y) &= y_{1,1}y_{2,2} - (y_{1,2})^2 = \frac{1}{4}(3y_{1,1}y_{2,2} + y_{1,1}y_{2,2} - (2y_{1,2})^2) \\ &\geq \frac{1}{4}(3y_{1,1}y_{2,2} + (y_{1,1})^2 - (y_{1,1})^2) = \frac{3}{4}y_{1,1}y_{2,2}. \end{aligned}$$

Bemerkung 3.4.4. [18, S. 481] Die Menge (3.10) können wir auch als

$$\mathcal{M}_2 = \left\{ \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{1,2} & y_{2,2} \end{pmatrix} \in M_2(\mathbb{R}) \mid y_{1,1} > 0, 0 \leq 2y_{1,2} \leq y_{1,1} \leq y_{2,2} \right\} \text{ schreiben.}$$

Der folgende Satz, der auf Minkowski [48] zurückgeht, verallgemeinert das Beispiel 3.4.3 [28, S. 192, 193], [35, S. 13, 16, 17], [48, S. 231, 232]:

Satz 3.4.5 (Ungleichung von Minkowski). *Es gibt eine nur von n abhängige Konstante $c_n > 0$, sodass*

$$\prod_{r=1}^n y_{r,r} \leq c_n \det(y) \quad \text{für alle } y \in \mathcal{M}_n \text{ gilt.}$$

Bemerkung 3.4.6. [16, S. 34], [28, S. 192] In Verbindung mit der Ungleichung von Hadamard (Korollar 3.1.4) erhalten wir für jede minkowskireduzierte Matrix $y \in \mathcal{M}_n$ die Abschätzung

$$\det(y) \leq \prod_{r=1}^n y_{r,r} \leq c_n \det(y).$$

Beweis des Satzes 3.4.5. Wir beweisen den Satz per Induktion über n . Für $n = 1$ gilt die Aussage beispielsweise mit $c_1 = 1$. Sei nun $n \geq 2$ und wir setzen voraus, dass die Aussage für alle $1 \leq k \leq n - 1$ gilt (Induktionsvoraussetzung). Wir betrachten $y \in \mathcal{M}_n$ und führen eine Fallunterscheidung durch:

Fall (a): Falls

$$\frac{y_{\ell+1,\ell+1}}{y_{\ell,\ell}} \leq \frac{n(n-1)}{4} \quad \text{für alle } 1 \leq \ell \leq n-1 \text{ gilt,}$$

so erhalten wir für alle $0 \leq r \leq n-1$

$$\frac{y_{r+1,r+1}}{y_{1,1}} = \prod_{\ell=1}^r \frac{y_{\ell+1,\ell+1}}{y_{\ell,\ell}} \leq \left(\frac{n(n-1)}{4} \right)^r.$$

Mit $y_{1,1} = \mu(y) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \cdot (\det(y))^{\frac{1}{n}}$ nach Lemmata 3.4.1(b) und 3.2.2 erhalten wir

$$\begin{aligned} \prod_{r=1}^n y_{r,r} &= \prod_{r=0}^{n-1} y_{r+1,r+1} \leq \left(\prod_{r=0}^{n-1} \left(\frac{n(n-1)}{4} \right)^r \right) \cdot (y_{1,1})^n = \left(\frac{n(n-1)}{4} \right)^{\frac{n(n-1)}{2}} \cdot (y_{1,1})^n \\ &\leq \left(\frac{n(n-1)}{4} \right)^{\frac{n(n-1)}{2}} \cdot \left(\frac{4}{3} \right)^{\frac{n(n-1)}{2}} \cdot \det(y) = \left(\frac{n(n-1)}{3} \right)^{\frac{n(n-1)}{2}} \cdot \det(y). \end{aligned}$$

Fall (b): Es gibt ein $1 \leq k \leq n-1$ mit

$$\frac{y_{k+1,k+1}}{y_{k,k}} > \frac{n(n-1)}{4}. \quad (3.11)$$

Wir wählen dann $1 \leq k \leq n-1$ maximal mit der Eigenschaft (3.11), das heißt, es gilt

$$\frac{y_{k+1,k+1}}{y_{k,k}} > \frac{n(n-1)}{4} \quad \text{sowie} \quad \frac{y_{i+1,i+1}}{y_{i,i}} \leq \frac{n(n-1)}{4} \quad \text{für alle } k+1 \leq i \leq n-1. \quad (3.12)$$

Schreiben wir $y = \begin{pmatrix} y_1 & y_2 \\ y_2^\top & y_4 \end{pmatrix}$ mit $k \times k$ -Block y_1 , so erhalten wir aus Lemma 3.1.2 (mit $m = k$)

$$y = \begin{pmatrix} y_1 & 0 \\ 0 & x \end{pmatrix} \left[\begin{pmatrix} I_k & b \\ 0 & I_{n-k} \end{pmatrix} \right] \quad \text{mit } x \in \mathbb{P}_{n-k} \text{ und } b \in M_{k,n-k}(\mathbb{R}).$$

Seien $g_1 \in \mathbb{Z}^k$ und $g_2 \in G_{1,n-k}$. Dann ist $g = \begin{pmatrix} g_1 \\ g_2 \end{pmatrix} \in G_{k+1,n}$ und aus $y \in \mathcal{M}_n$ folgt

$$y_{k+1,k+1} \leq y[g] = \begin{pmatrix} y_1 & 0 \\ 0 & x \end{pmatrix} \left[\begin{pmatrix} g_1 + bg_2 \\ g_2 \end{pmatrix} \right] = y_1[g_1 + bg_2] + x[g_2]. \quad (3.13)$$

Aufgrund von Bemerkung 3.2.1(b) können wir $g_2 \in G_{1,n-k}$ so wählen, dass $x[g_2] = \mu(x)$ gilt. Anschließend wählen wir $g_1 \in \mathbb{Z}^k$ derart, dass jeder Eintrag von $g_1 + bg_2$ im Intervall $[-\frac{1}{2}, \frac{1}{2}]$ liegt. Zusammen mit den Ungleichungen (b) und (c) von Lemma 3.4.1 liefert dies

$$\begin{aligned} y_1[g_1 + bg_2] &= |y_1[g_1 + bg_2]| = \left| \sum_{1 \leq \ell, r \leq k} y_{\ell, r} \cdot (g_1 + bg_2)_\ell \cdot (g_1 + bg_2)_r \right| \\ &\leq \sum_{r=1}^k y_{r,r} \cdot |(g_1 + bg_2)_r|^2 + \sum_{1 \leq \ell < r \leq k} 2|y_{\ell, r}| \cdot |(g_1 + bg_2)_\ell| \cdot |(g_1 + bg_2)_r| \\ &\leq k \cdot \frac{y_{k,k}}{4} + \frac{k(k-1)}{2} \cdot \frac{y_{k,k}}{4} = \frac{k(k+1)}{8} \cdot y_{k,k}. \end{aligned}$$

Setzen wir diese Abschätzung und $x[g_2] = \mu(x)$ in (3.13) ein, so erhalten wir mithilfe der Ungleichung von Hermite (Lemma 3.2.2) nun

$$\begin{aligned} y_{k+1,k+1} &\leq y_1[g_1 + bg_2] + x[g_2] \leq \frac{k(k+1)}{8} \cdot y_{k,k} + \mu(x) \\ &\leq \frac{k(k+1)}{8} \cdot y_{k,k} + \left(\frac{4}{3}\right)^{\frac{n-k-1}{2}} \cdot (\det(x))^{\frac{1}{n-k}}. \end{aligned}$$

Unter Verwendung von $-\frac{y_{k+1,k+1}}{2n(n-1)} < -\frac{y_{k,k}}{8}$ (nach dem ersten Teil von (3.12)) ergibt sich daraus

$$\left(1 - \frac{k(k+1)}{2n(n-1)}\right) \cdot y_{k+1,k+1} < y_{k+1,k+1} - \frac{k(k+1)}{8} \cdot y_{k,k} \leq \left(\frac{4}{3}\right)^{\frac{n-k-1}{2}} \cdot (\det(x))^{\frac{1}{n-k}}.$$

Nun ist aber $\frac{k(k+1)}{n(n-1)} \leq \frac{(n-1)n}{n(n-1)} = 1$, also haben wir

$$\frac{1}{2} \cdot y_{k+1,k+1} \leq \left(1 - \frac{k(k+1)}{2n(n-1)}\right) \cdot y_{k+1,k+1} < \left(\frac{4}{3}\right)^{\frac{n-k-1}{2}} \cdot (\det(x))^{\frac{1}{n-k}}. \quad (3.14)$$

Diese Abschätzung nutzen wir, um $\prod_{r=k}^{n-1} y_{r+1,r+1}$ nach oben abzuschätzen: Nach Wahl von k gilt für jedes $k \leq r \leq n-1$

$$\frac{y_{r+1,r+1}}{y_{k+1,k+1}} = \prod_{i=k+1}^r \frac{y_{i+1,i+1}}{y_{i,i}} \leq \left(\frac{n(n-1)}{4}\right)^{r-k}.$$

Mit (3.14) folgt daher

$$\begin{aligned} \prod_{r=k}^{n-1} y_{r+1,r+1} &\leq \left(\prod_{r=k}^{n-1} \left(\frac{n(n-1)}{4} \right)^{r-k} \right) \cdot (y_{k+1,k+1})^{n-k} = \left(\frac{n(n-1)}{4} \right)^{\frac{(n-k)(n-k-1)}{2}} \cdot (y_{k+1,k+1})^{n-k} \\ &< 2^{n-k} \cdot \left(\frac{n(n-1)}{3} \right)^{\frac{(n-k)(n-k-1)}{2}} \cdot \det(x). \end{aligned} \quad (3.15)$$

Um hingegen $\prod_{r=1}^k y_{r,r}$ abzuschätzen, wenden wir die Induktionsvoraussetzung auf die nach Lemma 3.4.1(a) minkowskireduzierte Matrix $y_1 \in \mathcal{M}_k$ an: Es gibt also eine nur von k abhängige Konstante $c_k > 0$ mit

$$\prod_{r=1}^k y_{r,r} \leq c_k \det(y_1). \quad (3.16)$$

Die Formeln (3.15) und (3.16) liefern zusammen

$$\begin{aligned} \prod_{r=1}^n y_{r,r} &< 2^{n-k} \cdot c_k \cdot \left(\frac{n(n-1)}{3} \right)^{\frac{(n-k)(n-k-1)}{2}} \cdot \det(y_1) \cdot \det(x) \\ &= 2^{n-k} \cdot c_k \cdot \left(\frac{n(n-1)}{3} \right)^{\frac{(n-k)(n-k-1)}{2}} \cdot \det(y). \end{aligned}$$

Indem wir nun das Maximum der Konstante

$$\left(\frac{n(n-1)}{3} \right)^{\frac{n(n-1)}{2}}$$

aus Fall (a) und der Konstanten

$$2^{n-k} \cdot c_k \cdot \left(\frac{n(n-1)}{3} \right)^{\frac{(n-k)(n-k-1)}{2}} \quad \text{für alle } 1 \leq k \leq n-1$$

aus Fall (b) bilden, erhalten wir, dass die Ungleichung von Minkowski mit einer nur von n abhängigen Konstanten auch für y gilt. \square

Beispiel 3.4.7. [28, S. 193], [32, S. 31], [35, S. 16]

Offensichtlich ist $c_1 = 1$ die kleinste Konstante, mit der die Ungleichung von Minkowski (Satz 3.4.5) im Fall $n = 1$ gilt.

Beispiel 3.4.8. [4, S. 15], [28, S. 193], [32, S. 31]

Sei $n = 2$. Die nach Beispiel 3.3.4 minkowskireduzierte Matrix $y = \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \in \mathcal{M}_2$ liefert

$$1 = y_{1,1} \cdot y_{2,2} \leq c_2 \det(y) = \frac{3}{4} c_2, \quad \text{also } c_2 \geq \frac{4}{3}.$$

Die Ungleichung von Minkowski (Satz 3.4.5) ist nach Beispiel 3.4.3 bereits mit $c_2 = \frac{4}{3}$ erfüllt, weshalb $c_2 = \frac{4}{3}$ den kleinstmöglichen Wert von c_2 darstellt.

Definieren wir nun

$$a_n := \sup_{y \in \mathcal{M}_n} \left((\det(y))^{-1} \cdot \prod_{r=1}^n y_{r,r} \right), \quad n \in \mathbb{N},$$

so ergeben die Beispiele 3.4.7 und 3.4.8, dass $a_1 = 1$ und $a_2 = \frac{4}{3}$ gilt.

Satz 3.4.9. [3, S. 52] Die Folge a_n , $n \in \mathbb{N}$, ist monoton wachsend.

Der Beweis des Satzes 3.4.9 beruht auf

Lemma 3.4.10. [3, S. 52] Für $n \in \mathbb{N} \setminus \{1\}$ gilt

$$B_n := \left\{ \begin{pmatrix} \tilde{y} & 0 \\ 0 & \lambda \end{pmatrix} \mid \tilde{y} \in \mathcal{M}_{n-1}, \lambda \geq \max\{\tilde{y}_{1,1}, \dots, \tilde{y}_{n-1,n-1}\} \right\} \subset \mathcal{M}_n.$$

Beweis. Wir überprüfen Definition 3.3.2 für $y \in B_n$: Für alle $v = \begin{pmatrix} \tilde{v} \\ v_{n,n} \end{pmatrix} \in \mathbb{R}^n \setminus \{0\}$, $v_{n,n} \in \mathbb{R}$, gilt

$$y[v] = \begin{pmatrix} \tilde{y} & 0 \\ 0 & \lambda \end{pmatrix} \left[\begin{pmatrix} \tilde{v} \\ v_{n,n} \end{pmatrix} \right] = \tilde{y}[\tilde{v}] + \lambda v_{n,n}^2.$$

Für $v_{n,n} \neq 0$ ergibt sich $y[v] \geq \lambda v_{n,n}^2 > 0$; ansonsten ist $v_{n,n} = 0$, woraus $\tilde{v} \neq 0$ und $y[v] = \tilde{y}[\tilde{v}] > 0$ folgt. Daher gilt $y \in \mathbb{P}_n$.

Um Bedingung (a) aus Definition 3.3.2 nachzuprüfen, betrachten wir für $1 \leq \ell \leq n$ den Vektor $g = \begin{pmatrix} \tilde{g} \\ g_{n,n} \end{pmatrix} \in G_{\ell,n}$, $g_{n,n} \in \mathbb{Z}$, und machen eine Fallunterscheidung:

Fall (a): Falls $g_{n,n} \neq 0$ gilt, so erhalten wir

$$y[g] = \tilde{y}[\tilde{g}] + \lambda g_{n,n}^2 \geq \lambda g_{n,n}^2 \geq \lambda \geq y_{\ell,\ell}.$$

Fall (b): Falls hingegen $g_{n,n} = 0$ ist, so folgern wir $\ell < n$ und $\tilde{g} \in G_{\ell,n-1}$. Da \tilde{y} minkowskireduziert ist, erhalten wir

$$y[g] = \tilde{y}[\tilde{g}] \geq \tilde{y}_{\ell,\ell} = y_{\ell,\ell}.$$

Damit erfüllt y die Bedingung (a) aus Definition 3.3.2. Per Konstruktion ist auch Bedingung (b) erfüllt, weshalb $y \in \mathcal{M}_n$ gilt. \square

Beweis des Satzes 3.4.9. Für $n \in \mathbb{N} \setminus \{1\}$ erhalten wir mithilfe der in Lemma 3.4.10 definierten Menge $B_n \subset \mathcal{M}_n$ die Abschätzung

$$\begin{aligned} a_n &= \sup_{y \in \mathcal{M}_n} \left((\det(y))^{-1} \cdot \prod_{r=1}^n y_{r,r} \right) \\ &\geq \sup_{\begin{pmatrix} \tilde{y} & 0 \\ 0 & \lambda \end{pmatrix} \in B_n} \left((\det(\tilde{y}))^{-1} \cdot \lambda^{-1} \cdot \lambda \cdot \prod_{r=1}^{n-1} \tilde{y}_{r,r} \right) \\ &= \sup_{\tilde{y} \in \mathcal{M}_{n-1}} \left((\det(\tilde{y}))^{-1} \cdot \prod_{r=1}^{n-1} \tilde{y}_{r,r} \right) = a_{n-1}. \end{aligned} \quad \square$$

Mithilfe der Ungleichung von Minkowski (Satz 3.4.5) können wir jede minkowskireduzierte Matrix mit der durch ihre Diagonalelemente gebildeten Diagonalmatrix vergleichen [3, S. 51, 52], [4, S. 14, 15], [28, S. 193, 194], [32, S. 30], [47, S. 128, 129].

Korollar 3.4.11. *Für jedes $y \in \mathcal{M}_n$ gilt*

$$n \cdot \text{diag}(y_{1,1}, \dots, y_{n,n}) \geq y \geq \frac{1}{n^{n-1} \cdot c_n} \cdot \text{diag}(y_{1,1}, \dots, y_{n,n}),$$

wobei c_n die Konstante aus der Ungleichung von Minkowski (Satz 3.4.5) ist.

Beweis. Wir definieren $d := \text{diag}(\sqrt{y_{1,1}}, \dots, \sqrt{y_{n,n}})$ und wenden Satz 2.1.6 auf $y[d^{-1}] \in \mathbb{P}_n$ an: Es gibt $g \in \text{GL}_n(\mathbb{R})$, $g^T \cdot g = I_n$, und $\lambda_1, \dots, \lambda_n > 0$ mit

$$y[d^{-1}g] = \text{diag}(\lambda_1, \dots, \lambda_n).$$

Da $\lambda_1, \dots, \lambda_n$ die Eigenwerte von $y[d^{-1}]$ sind, gilt (Korollar 2.1.9)

$$\sum_{r=1}^n \lambda_r = \text{Spur}(y[d^{-1}]) = \sum_{r=1}^n (y[d^{-1}])_{r,r} = \sum_{r=1}^n y[(y_{r,r})^{-\frac{1}{2}} \cdot e_r] = \sum_{r=1}^n (y_{r,r})^{-1} \cdot y[e_r] = \sum_{r=1}^n 1 = n,$$

woraus

$$\lambda_k \leq n \quad \text{für alle } 1 \leq k \leq n \text{ folgt.} \quad (3.17)$$

Aus der Ungleichung von Minkowski (Satz 3.4.5) erhalten wir des Weiteren

$$\prod_{k=1}^n \lambda_k = \det(y[d^{-1}]) = \left(\prod_{k=1}^n (y_{k,k})^{-\frac{1}{2}} \right)^2 \cdot \det(y) = \left(\prod_{k=1}^n y_{k,k} \right)^{-1} \cdot \det(y) \geq \frac{1}{c_n}.$$

Mithilfe von (3.17) schließen wir daraus nun $n^{n-1} \cdot \lambda_i \geq \prod_{k=1}^n \lambda_k \geq \frac{1}{c_n}$ und

$$\lambda_i \geq \frac{1}{n^{n-1} \cdot c_n} \quad \text{für alle } 1 \leq i \leq n. \quad (3.18)$$

Mit den Abschätzungen (3.17) und (3.18) ergibt sich

$$n \cdot I_n \geq y[d^{-1}g] = \text{diag}(\lambda_1, \dots, \lambda_n) \geq \frac{1}{n^{n-1} \cdot c_n} \cdot I_n.$$

Wenden wir darauf $[g^{-1}d]$ an, so erhalten wir wegen $g^T \cdot g = I_n$ die Behauptung

$$n \cdot d^2 \geq y \geq \frac{1}{n^{n-1} \cdot c_n} \cdot d^2. \quad \square$$

Zum Abschluss dieses Abschnitts zeigen wir, dass es unter bestimmten Voraussetzungen an $y \in \mathbb{P}_n$ nur endlich viele Bahnen $\{y[u] \mid u \in \text{GL}_n(\mathbb{Z})\}$ gibt [3, S. 52], [16, S. 36].

Korollar 3.4.12. *Sei $d > 0$. Dann gibt es nur endlich viele Bahnen*

$$\{y[u] \mid u \in \text{GL}_n(\mathbb{Z})\}$$

zu halbganzen Matrizen $y \in \mathbb{P}_n$ mit fester Determinante $\det(y) = d$.

Beweis. Wegen Satz 3.3.7 besitzt jede solche Bahn einen minkowskireduzierten Repräsentanten $w \in \mathcal{M}_n$, der auch halbganz ist (Lemma 2.2.4(e)) und $\det(w) = d$ erfüllt. Die Ungleichung von Minkowski (Satz 3.4.5) für w ergibt

$$w_{\ell,\ell} \leq \prod_{r=1}^n w_{r,r} \leq c_n \det(w) = c_n d \quad \text{für alle } 1 \leq \ell \leq n.$$

Wegen Lemma 3.4.1(c) zeigt dies die Beschränktheit aller Einträge von w durch eine nur von n und d abhängige Konstante. Da w halbganz ist, gibt es also für w nur endlich viele Möglichkeiten. Daher ist die Anzahl der Bahnen endlich. \square

3.5 Der Siegelische Fundamentalbereich \mathcal{F}_n

Aus der Theorie der klassischen Modulformen wissen wir bereits, dass die Operation von $\mathrm{SL}_2(\mathbb{Z})$ auf \mathbb{H} durch

$$\begin{aligned} \mathrm{SL}_2(\mathbb{Z}) \times \mathbb{H} &\longrightarrow \mathbb{H} \\ (m, z) &\longmapsto m\langle z \rangle = \frac{az + b}{cz + d} \end{aligned}$$

für $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ einen Fundamentalbereich

$$\mathcal{F} := \left\{ z = x + iy \in \mathbb{H} \mid |z| \geq 1, |x| \leq \frac{1}{2} \right\} \tag{3.19}$$

besitzt (Abbildung 3.1), der das Folgende erfüllt [3, S. 44, 45], [7, S. 317, 326], [10, S. 34 – 37], [37, S. 9], [60, S. 2 – 4]:

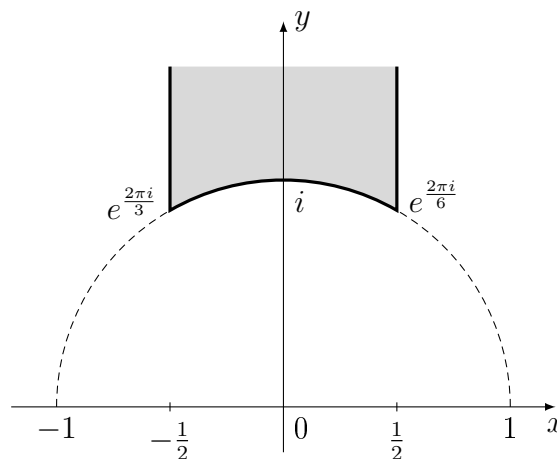


Abbildung 3.1: Der Fundamentalbereich \mathcal{F}

Satz 3.5.1. (a) Zu jedem $z \in \mathbb{H}$ gibt es ein $m \in \mathrm{SL}_2(\mathbb{Z})$ mit $m\langle z \rangle \in \mathcal{F}$.

(b) Seien $z, \tilde{z} \in \mathcal{F}$ mit $\tilde{z} = m\langle z \rangle$ für ein $m \in \mathrm{SL}_2(\mathbb{Z}) \setminus \{\pm I_2\}$. Dann gilt $z, \tilde{z} \in \partial\mathcal{F}$. Insbesondere gehören zwei verschiedene innere Punkte von \mathcal{F} nie derselben Bahn an.

Das Ziel ist es, dies zu verallgemeinern [16, S. 30, 31]. Satz 2.4.1 beschreibt bereits die Operation von Γ_n auf \mathbb{H}_n durch

$$\begin{aligned} \Gamma_n \times \mathbb{H}_n &\longrightarrow \mathbb{H}_n \\ (m, z) &\longmapsto m\langle z \rangle = (az + b)(cz + d)^{-1} \end{aligned}$$

für $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Ihre Bahnen sind gegeben durch

$$\Gamma_n\langle z \rangle := \{m\langle z \rangle \mid m \in \Gamma_n\}, \quad z \in \mathbb{H}_n.$$

Definition 3.5.2. [21, S. 185, 186], [54, S. 599], [55, S. 628]

Eine Matrix $z = x + iy \in \mathbb{H}_n$ heißt *siegelreduziert*, falls die folgenden Bedingungen gelten:

- (a) $|\det(cz + d)| \geq 1$ für alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_n$.
- (b) $y \in \mathcal{M}_n$.
- (c) $|x_{\ell,r}| \leq \frac{1}{2}$ für alle $1 \leq \ell \leq r \leq n$.

Die Menge aller siegelreduzierten $n \times n$ -Matrizen bezeichnen wir mit \mathcal{F}_n .

Bemerkung 3.5.3. [16, S. 38], [28, S. 194] Da \mathcal{M}_n in \mathbb{P}_n abgeschlossen ist, ist \mathcal{F}_n in \mathbb{H}_n abgeschlossen.

Beispiel 3.5.4. [3, S. 44, 45], [37, S. 9] Im Fall $n = 1$ ergibt Definition 3.5.2

$$\begin{aligned} \mathcal{F}_1 &= \left\{ z = x + iy \in \mathbb{H} \mid |cz + d| \geq 1 \text{ für alle } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}), |x| \leq \frac{1}{2} \right\} \\ &= \left\{ z = x + iy \in \mathbb{H} \mid |cz + d| \geq 1 \text{ für alle } c, d \in \mathbb{Z} \text{ mit } \text{ggT}(c, d) = 1, |x| \leq \frac{1}{2} \right\}. \end{aligned}$$

Wir wollen zeigen, dass dies mit dem in (3.19) definierten Fundamentalbereich \mathcal{F} übereinstimmt:

Mit $(c, d) = (1, 0)$ sehen wir $\mathcal{F}_1 \subset \mathcal{F}$. Um die umgekehrte Inklusion zu zeigen, betrachten wir die symmetrischen, nach dem Hauptminoren-Kriterium für die Definitheit auch positiv definiten Matrizen

$$\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \in \mathbb{P}_2 \quad \text{und} \quad \begin{pmatrix} 1 & -\frac{1}{2} \\ -\frac{1}{2} & 1 \end{pmatrix} \in \mathbb{P}_2.$$

Die zugehörigen quadratischen Formen erfüllen

$$c^2 \pm cd + d^2 \in \mathbb{Z}_{>0} = \mathbb{N} \quad \text{für alle } (c, d)^T \in \mathbb{Z}^2 \setminus \{(0, 0)^T\}.$$

Für alle $z \in \mathcal{F}$ und alle $(c, d)^T \in \mathbb{Z}^2 \setminus \{(0, 0)^T\}$ gilt daher

$$\begin{aligned} |cz + d|^2 &= (cz + d)(c\bar{z} + d) = c^2|z|^2 + 2cdx + d^2 \\ &\geq c^2 + 2cdx + d^2 \geq c^2 - 2|cd||x| + d^2 \geq c^2 - |cd| + d^2 \geq 1. \end{aligned}$$

Dies zeigt $z \in \mathcal{F}_1$, also $\mathcal{F} \subset \mathcal{F}_1$. Insgesamt ergibt sich $\mathcal{F} = \mathcal{F}_1$.

Der Beweis von Satz 3.5.1 basiert darauf, dass jede Bahn $\Gamma_1\langle z \rangle$, $z \in \mathbb{H}$, einen Punkt maximaler Höhe besitzt. Die Höhe wird dabei durch den Imaginärteil gegeben [3, S. 43, 44], [10, S. 34, 35], [32, S. 34], [37, S. 9].

Dies übertragen wir auf $n \in \mathbb{N}$ [16, S. 36], [37, S. 9], [55, S. 627].

Definition 3.5.5. Für $z = x + iy \in \mathbb{H}_n$ heißt $h(z) := \det(y)$ die *Höhe* von z .

Bemerkung 3.5.6. [16, S. 26, 37], [32, S. 34], [35, S. 28], [47, S. 168, 169]

(a) Für $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_n$ und $z = x + iy \in \mathbb{H}_n$ gilt nach (2.13)

$$\begin{aligned} h(m\langle z \rangle) &= \det(\operatorname{Im}(m\langle z \rangle)) = \det(y\{(cz + d)^{-1}\}) \\ &= \det\left(\left((cz + d)^{-1}\right)^T \cdot y \cdot \overline{(cz + d)^{-1}}\right) = |\det(cz + d)|^{-2} \cdot h(z). \end{aligned}$$

(b) Für $m = \begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix} \in \Gamma_n$, $b \in M_n(\mathbb{Z})$ symmetrisch, und $z \in \mathbb{H}_n$ ergibt sich

$$h(z + b) = h(m\langle z \rangle) = h(z).$$

(c) Für $m = \begin{pmatrix} u^T & 0 \\ 0 & u^{-1} \end{pmatrix} \in \Gamma_n$, $u \in \operatorname{GL}_n(\mathbb{Z})$, und $z \in \mathbb{H}_n$ erhalten wir

$$h(z[u]) = h(m\langle z \rangle) = h(z).$$

Lemma 3.5.7. [4, S. 15, 16], [16, S. 37], [32, S. 34, 35], [35, S. 29]

Seien $m \in \Gamma_n$ und $z \in \mathbb{H}_n$. Dann gibt es ein $\tilde{m} \in \Gamma_n$ mit

$$h(\tilde{m}\langle z \rangle) = h(m\langle z \rangle) \quad \text{und} \quad (\operatorname{Im}(\tilde{m}\langle z \rangle))^{-1} \in \mathcal{M}_n.$$

Beweis. Wir schreiben $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ und $z = x + iy$. Aus (2.13) ergibt sich

$$\begin{aligned} y^* &:= \operatorname{Im}(m\langle z \rangle) = y\{(cz + d)^{-1}\} = \left((cz + d)^{-1}\right)^T \cdot y \cdot \overline{(cz + d)^{-1}}, \\ \text{also } (y^*)^{-1} &= \overline{(cz + d)} \cdot y^{-1} \cdot (cz + d)^T = y^{-1} \left\{ \overline{(cz + d)}^T \right\}. \end{aligned} \tag{3.20}$$

Nach Satz 3.3.7 existiert ein $u \in \operatorname{GL}_n(\mathbb{Z})$ mit $(y^*)^{-1}[u] \in \mathcal{M}_n$. Mit der Matrix

$$\Gamma_n \ni \tilde{m} := \begin{pmatrix} u^{-1} & 0 \\ 0 & u^T \end{pmatrix} \cdot m = \begin{pmatrix} u^{-1} & 0 \\ 0 & u^T \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} u^{-1} \cdot a & u^{-1} \cdot b \\ u^T \cdot c & u^T \cdot d \end{pmatrix}$$

gilt wegen Bemerkung 3.5.6(c)

$$h(\tilde{m}\langle z \rangle) = h((m\langle z \rangle)[(u^{-1})^T]) = h(m\langle z \rangle).$$

Mit (3.20) folgt schließlich auch

$$\begin{aligned} (\operatorname{Im}(\tilde{m}\langle z \rangle))^{-1} &= y^{-1} \left\{ \overline{(u^T \cdot cz + u^T \cdot d)}^T \right\} = y^{-1} \left\{ \overline{(cz + d)}^T \cdot u \right\} \\ &= \left(y^{-1} \left\{ \overline{(cz + d)}^T \right\} \right) [u] = (y^*)^{-1}[u] \in \mathcal{M}_n. \end{aligned} \quad \square$$

Mithilfe von Lemma 3.5.7 gelingt es schließlich zu zeigen, dass jede Bahn $\Gamma_n\langle z \rangle$, $z \in \mathbb{H}_n$, ein Element maximaler Höhe besitzt [4, S. 15, 16], [16, S. 37], [32, S. 34, 35], [35, S. 29]:

Lemma 3.5.8. *Seien $z \in \mathbb{H}_n$ und $\varepsilon > 0$. Dann gibt es nur endlich viele $h_0 > 0$ mit*

$$h_0 \geq \varepsilon \quad \text{und} \quad h_0 = h(m\langle z \rangle) \quad \text{für ein } m \in \Gamma_n.$$

Beweis. Sei $h(m\langle z \rangle) \geq \varepsilon$ mit $m \in \Gamma_n$. Aufgrund von Lemma 3.5.7 können wir annehmen, dass $(\text{Im}(m\langle z \rangle))^{-1} \in \mathcal{M}_n$ minkowskireduziert ist. Wir bezeichnen die Diagonalelemente von $(\text{Im}(m\langle z \rangle))^{-1}$ mit $t_{1,1}, \dots, t_{n,n}$. Nach der Ungleichung von Minkowski (Satz 3.4.5) gilt

$$\prod_{r=1}^n t_{r,r} \leq c_n \cdot \det(\text{Im}(m\langle z \rangle))^{-1} = c_n \cdot (h(m\langle z \rangle))^{-1} \leq \frac{c_n}{\varepsilon}. \quad (3.21)$$

Schreiben wir $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ und $z = x + iy$, erhalten wir mit (3.20) andererseits

$$\begin{aligned} (\text{Im}(m\langle z \rangle))^{-1} &= (c\bar{z} + d) \cdot y^{-1} \cdot (cz + d)^T = (c \cdot (x - iy) + d) \cdot y^{-1} \cdot (c \cdot (x + iy) + d)^T \\ &= ((cx + d) - icy) \cdot y^{-1} \cdot ((cx + d)^T + icy^T) \\ &= y^{-1}[(cx + d)^T] + i((cx + d) \cdot c^T - c \cdot (cx + d)^T) + y[c^T] \\ &= y^{-1}[(cx + d)^T] + y[c^T] \\ &= y^{-1}[x \cdot c^T + d^T] + y[c^T], \end{aligned}$$

denn $(cx + d) \cdot c^T = x[c^T] + d \cdot c^T$ ist nach Lemma 2.3.5(e) symmetrisch.

Bezeichnen wir die ℓ -te Zeile von c (respektive d) mit c_ℓ (respektive d_ℓ), $1 \leq \ell \leq n$, so folgt

$$t_{\ell,\ell} = y^{-1}[x \cdot c_\ell^T + d_\ell^T] + y[c_\ell^T] \quad \text{für alle } 1 \leq \ell \leq n. \quad (3.22)$$

Wir unterscheiden nun zwei Fälle:

Fall (a): Wenn $c_\ell \neq 0$ gilt, ergibt sich

$$t_{\ell,\ell} \geq y[c_\ell^T] \geq \mu(y) \geq \min\{\mu(y), \mu(y^{-1})\} =: K.$$

Fall (b): Sei $c_\ell = 0$. Dann muss $d_\ell \neq 0$ gelten; denn ansonsten wäre nämlich die $(n + \ell)$ -te Zeile der invertierbaren Matrix m eine Nullzeile. Wir erhalten

$$t_{\ell,\ell} = y^{-1}[d_\ell^T] \geq \mu(y^{-1}) \geq \min\{\mu(y), \mu(y^{-1})\} = K.$$

Jedes $t_{\ell,\ell}$, $1 \leq \ell \leq n$, ist also immer nach unten durch eine positive Konstante $K > 0$ beschränkt, die unabhängig von m ist. Zusammen mit (3.21) schließen wir daraus

$$\begin{aligned} t_{\ell,\ell} \cdot K^{n-1} &\leq \prod_{r=1}^n t_{r,r} \leq \frac{c_n}{\varepsilon}, \\ \text{also } t_{\ell,\ell} &\leq \frac{c_n}{K^{n-1} \cdot \varepsilon} \quad \text{für alle } 1 \leq \ell \leq n, \end{aligned} \quad (3.23)$$

wobei die obere Schranke $\frac{c_n}{K^{n-1} \cdot \varepsilon}$ unabhängig von m ist. Wegen (3.22) und (3.23) müssen die Zeilen c_ℓ , $1 \leq \ell \leq n$, daher die Ungleichung

$$y[c_\ell^T] \leq \frac{c_n}{K^{n-1} \cdot \varepsilon}$$

erfüllen, die nach Korollar 2.2.2 nur für endlich viele ganze Vektoren erfüllt sein kann. Für jede dieser endlich vielen Möglichkeiten von c_ℓ gibt es (wieder nach Korollar 2.2.2) nun aber auch nur endlich viele Möglichkeiten von ganzzahligen Vektoren d_ℓ mit der Eigenschaft

$$y^{-1}[x \cdot c_\ell^\top + d_\ell^\top] \leq \frac{c_n}{K^{n-1} \cdot \varepsilon}.$$

Daher durchlaufen die Blöcke c und d von m eine endliche Menge, woraus mit Bemerkung 3.5.6(a) schließlich die Behauptung folgt. \square

Damit können wir nun Satz 3.5.1(a) verallgemeinern [3, S. 59], [16, S. 36, 37], [28, S. 194, 195], [47, S. 169].

Satz 3.5.9. *Zu jedem $z \in \mathbb{H}_n$ gibt es ein $m \in \Gamma_n$ mit $m\langle z \rangle \in \mathcal{F}_n$.*

Beweis. Nach Lemma 3.5.8 existiert ein $\tilde{z} = \tilde{x} + i\tilde{y} \in \Gamma_n\langle z \rangle$, das maximale Höhe unter allen Elementen der Bahn $\Gamma_n\langle z \rangle$ besitzt. Wegen Satz 3.3.7 gibt es ein $u \in \mathrm{GL}_n(\mathbb{Z})$ mit $\tilde{y}[u] \in \mathcal{M}_n$. Anschließend wählen wir ein symmetrisches $b \in M_n(\mathbb{Z})$ derart, dass jeder Eintrag von $\tilde{x}[u] + b$ im Intervall $[-\frac{1}{2}, \frac{1}{2}]$ liegt. Wir betrachten die Matrix $\tilde{m} := \begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix} \cdot \begin{pmatrix} u^\top & 0 \\ 0 & u^{-1} \end{pmatrix} \in \Gamma_n$ und das Element

$$z^* := \tilde{m}\langle \tilde{z} \rangle = \begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix} \langle \tilde{z}[u] \rangle = \tilde{z}[u] + b = \tilde{x}[u] + b + i\tilde{y}[u],$$

das in derselben Bahn wie z liegt. Wir zeigen, dass z^* siegelreduziert ist: Wegen

$$h(z^*) = h(\tilde{z}[u] + b) = h(\tilde{z}[u]) = h(\tilde{z})$$

hat auch z^* maximale Höhe unter allen Elementen der Bahn $\Gamma_n\langle z \rangle = \Gamma_n\langle z^* \rangle$, das heißt $h(z^*) \geq h(m\langle z^* \rangle)$ für alle $m \in \Gamma_n$. Aus Bemerkung 3.5.6(a) folgt daher

$$h(z^*) \geq h(m\langle z^* \rangle) = |\det(cz^* + d)|^{-2} \cdot h(z^*)$$

und $|\det(cz^* + d)| \geq 1$ für alle $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_n$.

Des Weiteren gilt $\mathrm{Im}(z^*) = \tilde{y}[u] \in \mathcal{M}_n$ und jeder Eintrag von $\mathrm{Re}(z^*) = \tilde{x}[u] + b$ liegt per Konstruktion im Intervall $[-\frac{1}{2}, \frac{1}{2}]$. Daher ist z^* siegelreduziert. \square

Korollar 3.5.10. [28, S. 195] *Es gilt $\mathbb{H}_n = \bigcup_{m \in \Gamma_n} m\langle \mathcal{F}_n \rangle$.*

Auch Aussage (b) von Satz 3.5.1 wird verallgemeinert durch

Satz 3.5.11. [3, S. 59], [32, S. 38], [35, S. 33], [47, S. 176, 177]

Seien $z, \tilde{z} \in \mathcal{F}_n$ mit $\tilde{z} = m\langle z \rangle$ für ein $m \in \Gamma_n \setminus \{\pm I_{2n}\}$. Dann gilt $z, \tilde{z} \in \partial\mathcal{F}_n$.

Beweis. Wir schreiben $z = x + iy$, $\tilde{z} = \tilde{x} + i\tilde{y}$ und $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, deren inverse Matrix nach

Lemma 2.3.5(c) durch $m^{-1} = \begin{pmatrix} d^\top & -b^\top \\ -c^\top & a^\top \end{pmatrix}$ gegeben ist. Aus $z \in \mathcal{F}_n$ erhalten wir

$$h(\tilde{z}) = h(m\langle z \rangle) = |\det(cz + d)|^{-2} \cdot h(z) \leq h(z).$$

Andererseits ist auch $\tilde{z} \in \mathcal{F}_n$, woraus

$$h(z) = h(m^{-1}\langle \tilde{z} \rangle) = |\det(-c^T \cdot \tilde{z} + a^T)|^{-2} \cdot h(\tilde{z}) \leq h(\tilde{z}) \quad \text{folgt.}$$

Daher erhalten wir $h(\tilde{z}) = h(z)$ und $|\det(cz + d)| = 1 = |\det(-c^T \cdot \tilde{z} + a^T)|$. Wir machen eine Fallunterscheidung:

Fall (a): Sei $c \neq 0$. Wäre $z \in \overset{\circ}{\mathcal{F}}_n$, so könnte $\det(cz + d)$ als nichtkonstante holomorphe Funktion aufgefasst werden. Nach dem Minimumprinzip dürfte sie in z kein Betragsminimum besitzen, das heißt, es gäbe ein $z^* \in \mathcal{F}_n$ mit

$$|\det(cz^* + d)| < |\det(cz + d)| = 1.$$

Da dies ein Widerspruch zu Definition 3.5.2(a) wäre, muss also $z \in \partial\mathcal{F}_n$ gelten. Eine analoge Argumentation ergibt auch $\tilde{z} \in \partial\mathcal{F}_n$.

Fall (b): Falls $c = 0$ gilt, so folgt $a^T \cdot d = I_n$ aus Lemma 2.3.5(d), also $(a^T)^{-1} = d \in M_n(\mathbb{Z})$. Dann können wir $u := a^T \in \text{GL}_n(\mathbb{Z})$ setzen, womit $m = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} u^T & b \\ 0 & u^{-1} \end{pmatrix}$ gilt. Damit erhalten wir

$$\begin{aligned} \tilde{x} + i\tilde{y} = \tilde{z} = m\langle z \rangle &= (u^T \cdot z + b) \cdot u = z[u] + bu = x[u] + bu + iy[u], \\ \text{also } \tilde{x} &= x[u] + bu \quad \text{und} \quad \tilde{y} = y[u]. \end{aligned}$$

Falls $u \neq \pm I_n$ ist, so impliziert Satz 3.3.10 sofort $y, \tilde{y} \in \partial\mathcal{M}_n$ und $z, \tilde{z} \in \partial\mathcal{F}_n$.

Falls hingegen $u = \pm I_n$ gilt, ist $b \neq 0$ wegen $m \neq \pm I_{2n}$. Daher ist $\tilde{x} = x[u] + bu = x \pm b$ eine nichttriviale Translation mit ganzzahligen Einträgen. Unter Berücksichtigung, dass alle Einträge von x und \tilde{x} im Intervall $[-\frac{1}{2}, \frac{1}{2}]$ liegen, folgt, dass es ein $1 \leq \ell \leq r \leq n$ gibt mit $x_{\ell,r} = \pm \frac{1}{2}$ und $\tilde{x}_{\ell,r} = -x_{\ell,r}$. Auch hier ergibt sich daher $z, \tilde{z} \in \partial\mathcal{F}_n$. \square

Aus Satz 3.5.11 ergibt sich

Korollar 3.5.12. [4, S. 16], [37, S. 10] *Zwei verschiedene innere Elemente von \mathcal{F}_n gehören nie derselben Bahn an.*

Die Sätze 3.5.9 und 3.5.11 charakterisieren die abgeschlossene Menge \mathcal{F}_n als Fundamentalbereich der Operation von Γ_n auf \mathbb{H}_n , gegeben durch

$$\begin{aligned} \Gamma_n \times \mathbb{H}_n &\longrightarrow \mathbb{H}_n \\ (m, z) &\longmapsto m\langle z \rangle = (az + b)(cz + d)^{-1} \end{aligned}$$

für $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Wir nennen \mathcal{F}_n den *Siegelschen Fundamentalbereich* von Γ_n [4, S. 16], [16, S. 36].

3.6 Ungleichungen für siegelreduzierte Matrizen

Die im Abschnitt 3.4 hergeleiteten Ungleichungen für minkowskireduzierte Matrizen ergeben wichtige Abschätzungen für siegelreduzierte Matrizen [3, S. 59, 60], [16, S. 37, 38], [35, S. 30].

Lemma 3.6.1. *Sei $x + iy \in \mathcal{F}_n$. Dann gilt*

$$y_{n,n} \geq y_{n-1,n-1} \geq \dots \geq y_{1,1} \geq \frac{\sqrt{3}}{2}.$$

Beweis. Definieren wir

$$a := d := \begin{pmatrix} 0 & 0 \\ 0 & I_{n-1} \end{pmatrix} \in M_n(\mathbb{Z}), \quad b := \begin{pmatrix} -1 & 0 \\ 0 & 0 \end{pmatrix} \in M_n(\mathbb{Z}), \quad c := -b$$

und $m := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2n}(\mathbb{Z})$, dann sind $a^T \cdot c = 0$ und $b^T \cdot d = 0$ symmetrisch. Außerdem ist

$$a^T \cdot d - c^T \cdot b = \begin{pmatrix} 0 & 0 \\ 0 & I_{n-1} \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = I_n.$$

Nach Lemma 2.3.5(d) gilt daher $m \in \Gamma_n$. Dies ermöglicht es, Definition 3.5.2(a) auf m und $z = x + iy \in \mathcal{F}_n$ anzuwenden:

$$1 \leq |\det(cz + d)| = \left| \det \left(\begin{pmatrix} z_{1,1} & * \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & 0 \\ 0 & I_{n-1} \end{pmatrix} \right) \right| = \left| \det \begin{pmatrix} z_{1,1} & * \\ 0 & I_{n-1} \end{pmatrix} \right| = |z_{1,1}|.$$

Wegen $|x_{1,1}| \leq \frac{1}{2}$ nach Definition 3.5.2(c) ergibt sich

$$1 \leq |z_{1,1}|^2 = x_{1,1}^2 + y_{1,1}^2 \leq \frac{1}{4} + y_{1,1}^2, \quad \text{also } y_{1,1}^2 \geq \frac{3}{4} \text{ und } y_{1,1} \geq \frac{\sqrt{3}}{2}.$$

Mit Lemma 3.4.1(b) erhalten wir die Behauptung. \square

Beispiel 3.6.2. Für $n = 1$ besagt Lemma 3.6.1, dass $y \geq \frac{\sqrt{3}}{2}$ für alle $x + iy \in \mathcal{F}_1 = \mathcal{F}$ gilt. Eine größere Konstante als $\frac{\sqrt{3}}{2}$ gibt es dabei nicht, denn die beiden „unteren Ecken“

$$e^{\frac{2\pi i}{3}} = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \quad \text{und} \quad e^{\frac{2\pi i}{6}} = \frac{1}{2} + i\frac{\sqrt{3}}{2}$$

des Fundamentalbereichs $\mathcal{F}_1 = \mathcal{F}$ aus Abbildung 3.1 besitzen ja genau den Imaginärteil $\frac{\sqrt{3}}{2}$.

Satz 3.6.3. [3, S. 59, 60], [16, S. 51], [32, S. 33]

Sei $x + iy \in \mathcal{F}_n$. Dann gilt

$$y \geq \frac{\sqrt{3}}{2 \cdot n^{n-1} \cdot c_n} \cdot I_n \quad \text{sowie} \quad \text{Spur}(y^{-1}) \leq \frac{2 \cdot n^n \cdot c_n}{\sqrt{3}},$$

wobei c_n die Konstante aus der Ungleichung von Minkowski (Satz 3.4.5) ist.

Beweis. Aus Korollar 3.4.11 und Lemma 3.6.1 erhalten wir für jedes $x + iy \in \mathcal{F}_n$

$$y \geq \frac{1}{n^{n-1} \cdot c_n} \cdot \text{diag}(y_{1,1}, \dots, y_{n,n}) \geq \frac{\sqrt{3}}{2 \cdot n^{n-1} \cdot c_n} \cdot I_n.$$

Dies zeigt die erste Behauptung des Satzes, woraus auch die zweite folgt: Wir nutzen Bemerkung 2.1.13 und schreiben

$$n = \text{Spur}(I_n) = \text{Spur}(y \cdot y^{-1}) \geq \frac{\sqrt{3}}{2 \cdot n^{n-1} \cdot c_n} \text{Spur}(y^{-1}).$$

Dies ergibt die zweite Behauptung. \square

Beispiel 3.6.4. [45, S. 83], [47, S. 189, 195] Wir betrachten den Fall $n = 1$. Mit $c_1 = 1$ folgt

$$y^{-1} = \text{Spur}(y^{-1}) \leq \frac{2}{\sqrt{3}} \quad \text{für alle } x + iy \in \mathcal{F}_1.$$

In dieser Ungleichung ist $\frac{2}{\sqrt{3}}$ nach Beispiel 3.6.2 die kleinstmögliche Konstante und es gilt $\sup_{x+iy \in \mathcal{F}_1} (y^{-1}) = \frac{2}{\sqrt{3}}$.

Sei $n = 2$. Die wegen Satz 3.6.3 und Beispiel 3.4.8 gültige Abschätzung

$$\text{Spur}(y^{-1}) \leq \frac{2 \cdot 2^2 \cdot \frac{4}{3}}{\sqrt{3}} = \frac{32}{3\sqrt{3}} \quad \text{für alle } x + iy \in \mathcal{F}_2$$

kann wie folgt verbessert werden [45, S. 83 – 84], [47, S. 195, 196]:

Beispiel 3.6.5. Sei $y = \begin{pmatrix} y_{1,1} & y_{1,2} \\ y_{1,2} & y_{2,2} \end{pmatrix} \in \mathcal{M}_2$. Dann gilt $y^{-1} = \frac{1}{\det(y)} \cdot \begin{pmatrix} y_{2,2} & -y_{1,2} \\ -y_{1,2} & y_{1,1} \end{pmatrix}$ und Beispiel 3.4.8 liefert

$$\text{Spur}(y^{-1}) = \frac{1}{\det(y)} \cdot (y_{2,2} + y_{1,1}) \leq \frac{4}{3} \cdot \frac{y_{2,2} + y_{1,1}}{y_{1,1} \cdot y_{2,2}} = \frac{4}{3} \cdot \left(\frac{1}{y_{1,1}} + \frac{1}{y_{2,2}} \right).$$

Mit Lemma 3.6.1 folgt für alle $x + iy \in \mathcal{F}_2$ schließlich

$$\text{Spur}(y^{-1}) \leq \frac{4}{3} \cdot \left(\frac{1}{y_{1,1}} + \frac{1}{y_{2,2}} \right) \leq \frac{4}{3} \cdot \left(\frac{2}{\sqrt{3}} + \frac{2}{\sqrt{3}} \right) = \frac{16}{3\sqrt{3}}.$$

Wir kehren zu Satz 3.6.3 zurück und notieren eine unmittelbare Folgerung [3, S. 59, 60], [16, S. 38], [28, S. 196]:

Korollar 3.6.6. \mathcal{F}_n ist in der Menge $\{z \in M_n(\mathbb{C}) \mid z^T = z\}$ abgeschlossen.

Korollar 3.6.7. [3, S. 93], [4, S. 31], [16, S. 38], [28, S. 196], [32, S. 57]
Sei $c > 0$. Dann ist die Menge $\mathcal{F}_n(c) := \{x + iy \in \mathcal{F}_n \mid \det(y) \leq c\}$ kompakt.

Beweis. Wegen Korollar 3.6.6 ist $\mathcal{F}_n(c)$ abgeschlossen. Es bleibt daher die Beschränktheit zu zeigen: Mit Lemma 3.6.1 und der Ungleichung von Minkowski (Satz 3.4.5) ergibt sich für $x + iy \in \mathcal{F}_n(c)$ die Abschätzung

$$\left(\frac{\sqrt{3}}{2} \right)^{n-1} \cdot y_{\ell,\ell} \leq \prod_{r=1}^n y_{r,r} \leq c_n \det(y) \leq c_n c \quad \text{für alle } 1 \leq \ell \leq n.$$

Wegen Lemma 3.4.1(c) ist jeder Eintrag von y beschränkt. Nun sind aber auch die Einträge von x (per Definition) beschränkt, woraus die Behauptung folgt. \square

Kapitel 4

Siegelsche Modulformen

4.1 Der Vektorraum $M_k(\Gamma_n)$ der Siegelschen Modulformen

Definition 4.1.1 (Strichoperator). [32, S. 43], [60, S. 7] Seien $n \in \mathbb{N}$ und $k \in \mathbb{Z}$. Für eine Funktion $f : \mathbb{H}_n \rightarrow \mathbb{C}$ und eine symplektische Matrix $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Sp}_n(\mathbb{R})$ definieren wir $f|_k m : \mathbb{H}_n \rightarrow \mathbb{C}$ durch

$$(f|_k m)(z) = \det(cz + d)^{-k} \cdot f(m\langle z \rangle) = \det(cz + d)^{-k} \cdot f((az + b)(cz + d)^{-1}).$$

Beispiel 4.1.2. Es ist $f|_k I_{2n} = f$.

Definition 4.1.3. [3, S. 62, 63], [4, S. 20], [16, S. 39], [21, S. 187], [32, S. 43], [37, S. 11], [51, S. 5], [60, S. 7]

Seien $n \in \mathbb{N}$ und $k \in \mathbb{Z}$. Eine Funktion $f : \mathbb{H}_n \rightarrow \mathbb{C}$ heißt *Siegelsche Modulform vom Geschlecht n und Gewicht k* , falls die folgenden Bedingungen gelten:

- (a) f ist holomorph.
- (b) Es gilt $f|_k m = f$ für alle $m \in \Gamma_n$.
- (c) f ist in jedem Bereich der Form $\{z \in \mathbb{H}_n \mid \mathrm{Im}(z) \geq y_0\}$, $y_0 \in \mathbb{P}_n$, beschränkt.

Beispiel 4.1.4. [38, S. 155], [60, S. 7] Für $n = 1$ erhalten wir die klassischen Modulformen einer komplexen Variablen.

Bemerkung 4.1.5. [3, S. 62, 63], [4, S. 20], [16, S. 39], [21, S. 188], [32, S. 43, 44], [35, S. 43], [37, S. 11], [51, S. 5], [60, S. 7, 8]

- (a) Die Menge aller Siegelschen Modulformen vom Geschlecht n und Gewicht k bilden einen Vektorraum über \mathbb{C} , der mit $M_k(\Gamma_n)$ bezeichnet wird.
- (b) Nach Korollar 2.2.1 gibt es zu jedem $y_0 \in \mathbb{P}_n$ ein $\delta > 0$ mit $y_0 > \delta I_n$. Daher kann die Bedingung (c) aus Definition 4.1.3 ersetzt werden durch folgende Aussage:
 f ist in jedem Bereich der Form $\{z \in \mathbb{H}_n \mid \mathrm{Im}(z) \geq \delta I_n\}$, $\delta > 0$, beschränkt.
- (c) Für $f \in M_k(\Gamma_n)$ und $g \in M_\ell(\Gamma_n)$ ist $f \cdot g \in M_{k+\ell}(\Gamma_n)$.

(d) Für $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_n$ und $\tilde{m} = \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \in \Gamma_n$ ist

$$m\tilde{m} = \begin{pmatrix} * & * \\ c\tilde{a} + d\tilde{c} & c\tilde{b} + d\tilde{d} \end{pmatrix}.$$

Für $z \in \mathbb{H}_n$ bestimmen wir

$$\begin{aligned} & \det((c\tilde{a} + d\tilde{c}) \cdot z + (c\tilde{b} + d\tilde{d})) \\ &= \det(c \cdot (\tilde{a}z + \tilde{b}) + d \cdot (\tilde{c}z + \tilde{d})) \\ &= \det(c \cdot (\tilde{a}z + \tilde{b})(\tilde{c}z + \tilde{d})^{-1} + d) \cdot \det(\tilde{c}z + \tilde{d}) \\ &= \det(c \cdot \tilde{m}\langle z \rangle + d) \cdot \det(\tilde{c}z + \tilde{d}). \end{aligned}$$

Daher ergibt sich

$$\begin{aligned} (f|_k(m\tilde{m}))(z) &= \det(c \cdot \tilde{m}\langle z \rangle + d)^{-k} \cdot \det(\tilde{c}z + \tilde{d})^{-k} \cdot f((m\tilde{m})\langle z \rangle) \\ &= \det(c \cdot \tilde{m}\langle z \rangle + d)^{-k} \cdot \det(\tilde{c}z + \tilde{d})^{-k} \cdot f(m\langle \tilde{m}\langle z \rangle \rangle) \\ &= \det(\tilde{c}z + \tilde{d})^{-k} \cdot (f|_k m)(\tilde{m}\langle z \rangle) \\ &= ((f|_k m)|_k \tilde{m})(z). \end{aligned}$$

(e) Wegen Teil (d) muss die Transformationseigenschaft $f|_k m = f$ aus Definition 4.1.3(b) nur für die Erzeuger (2.18), (2.19) und (2.20) von Γ_n überprüft werden: Wir müssen also lediglich

$$\begin{aligned} f(z + b) &= f(z), \quad b \in M_n(\mathbb{Z}) \text{ symmetrisch,} \\ f(-z^{-1}) &= (\det(z))^k \cdot f(z) \\ \text{und } f(z[u]) &= (\det(u))^k \cdot f(z), \quad u \in \text{GL}_n(\mathbb{Z}), \text{ überprüfen.} \end{aligned}$$

Bemerkung 4.1.6. [7, S. 149, 350, 351], [18, S. 449], [21, S. 189, 190], [32, S. 44, 45], [35, S. 44], [38, S. 269], [51, S. 6]

Sei $f : \mathbb{H}_n \rightarrow \mathbb{C}$ eine holomorphe Funktion, die $f(z + b) = f(z)$ für alle symmetrischen $b \in M_n(\mathbb{Z})$ erfüllt. Dann ist f in jedem $z_{\ell,r}$, $1 \leq \ell \leq r \leq n$, periodisch mit Periode 1 und lässt daher eine Fourierreiheentwicklung in diesen Variablen zu. Da jede ganzzahlige Linearkombination von $z_{\ell,r}$, $1 \leq \ell \leq r \leq n$, in der Form

$$\text{Spur}(tz) \quad \text{für genau eine halbganze Matrix } t^T = t \in M_n(\mathbb{R})$$

dargestellt werden kann (Bemerkung 2.2.5), können wir die Fourierreiheentwicklung mithilfe der Notation (2.8) als

$$f(z) = \sum_{\substack{t^T = t \in M_n(\mathbb{R}) \\ t \text{ halbganz}}} a(t) e^{2\pi i \cdot \text{Spur}(tz)} = \sum_{\substack{t^T = t \in M_n(\mathbb{R}) \\ t \text{ halbganz}}} a(t) e_n(tz), \quad z \in \mathbb{H}_n, \quad (4.1)$$

schreiben. Sie stellt eine absolut und auf Kompakta von \mathbb{H}_n gleichmäßig konvergente Reihe dar.

Einige der folgenden Ergebnisse können wir nicht nur für Siegelsche Modulformen beweisen; es reicht sogar, für holomorphe Funktionen lediglich die „richtigen“ Transformationen unter (2.18) und (2.20) vorauszusetzen [21, S. 190], [32, S. 45, 46], [35, S. 44, 45].

Lemma 4.1.7. [16, S. 43], [21, S. 190], [32, S. 45, 46], [35, S. 44, 45], [47, S. 182, 183], [54, S. 601], [55, S. 635]

Seien $n \in \mathbb{N}$, $k \in \mathbb{Z}$ und $f : \mathbb{H}_n \rightarrow \mathbb{C}$ holomorph mit der Eigenschaft

$$f(z[u] + b) = (\det(u))^k \cdot f(z)$$

für alle $z \in \mathbb{H}_n$, $u \in \mathrm{GL}_n(\mathbb{Z})$ und symmetrischen $b \in M_n(\mathbb{Z})$. Für die Fourierkoeffizienten von

$$f(z) = \sum_{\substack{t^T = t \in M_n(\mathbb{R}) \\ t \text{ halbganz}}} a(t) e_n(tz), \quad z \in \mathbb{H}_n,$$

gilt dann die Beziehung

$$a(t[u]) = (\det(u))^k \cdot a(t)$$

für alle halbganzen $t^T = t \in M_n(\mathbb{R})$ und alle $u \in \mathrm{GL}_n(\mathbb{Z})$.

Beweis. Zunächst gilt

$$\mathrm{Spur}(t \cdot z[u]) = \mathrm{Spur}(tu^T z \cdot u) = \mathrm{Spur}(u \cdot tu^T z) = \mathrm{Spur}(t[u^T] \cdot z).$$

Wir erhalten damit

$$\begin{aligned} (\det(u))^k \cdot f(z) = f(z[u]) &= \sum_{\substack{t^T = t \in M_n(\mathbb{R}) \\ t \text{ halbganz}}} a(t) e_n(t \cdot z[u]) \\ &= \sum_{\substack{t^T = t \in M_n(\mathbb{R}) \\ t \text{ halbganz}}} a(t) e_n(t[u^T] \cdot z) \\ &= \sum_{\substack{t^T = t \in M_n(\mathbb{R}) \\ t \text{ halbganz}}} a(t[(u^T)^{-1}]) e_n(tz), \end{aligned}$$

wobei die letzte Gleichheit aus der Bijektion $t \mapsto t[u^T]$ zwischen den halbganzen Matrizen t und $t[u^T]$ folgt (Lemma 2.2.4). Daraus schließen wir $a(t[(u^T)^{-1}]) = (\det(u))^k \cdot a(t)$. Indem wir u durch $(u^{-1})^T$ ersetzen, ergibt sich

$$a(t[u]) = (\det(u^{-1})^T)^k \cdot a(t) = (\det(u))^k \cdot a(t). \quad \square$$

Korollar 4.1.8. [35, S. 45], [47, S. 183] Seien $n \in \mathbb{N}$ und $k \in \mathbb{Z}$ mit ungeradem nk . Die Funktion $f : \mathbb{H}_n \rightarrow \mathbb{C}$ sei holomorph mit der Eigenschaft

$$f(z[u] + b) = (\det(u))^k \cdot f(z)$$

für alle $z \in \mathbb{H}_n$, $u \in \mathrm{GL}_n(\mathbb{Z})$ und symmetrischen $b \in M_n(\mathbb{Z})$. Dann ist f die Nullfunktion.

Beweis. Für

$$f(z) = \sum_{\substack{t^T = t \in M_n(\mathbb{R}) \\ t \text{ halbganz}}} a(t) e_n(tz), \quad z \in \mathbb{H}_n,$$

folgt aus Lemma 4.1.7 (mit $u = -I_n \in \mathrm{GL}_n(\mathbb{Z})$)

$$a(t) = a(t[-I_n]) = (\det(-I_n))^k \cdot a(t) = (-1)^{nk} \cdot a(t) = -a(t).$$

Es folgt $a(t) = 0$ für alle halbganzen Matrizen $t^T = t \in M_n(\mathbb{R})$. □

Da Siegelsche Modulformen vom Geschlecht n und Gewicht k mit ungeradem nk die Voraussetzungen von Korollar 4.1.8 erfüllen, ergibt sich unmittelbar

Korollar 4.1.9. [16, S. 39], [35, S. 45] Seien $n \in \mathbb{N}$ und $k \in \mathbb{Z}$ mit ungeradem nk . Dann ist $M_k(\Gamma_n) = \{0\}$.

Beispiel 4.1.10. [60, S. 8] Für $n = 1$ und ungerades $k \in \mathbb{Z}$ erhalten wir die bekannte Aussage $M_k(\Gamma_1) = \{0\}$.

Wir kehren zu (4.1) zurück. Die Fourierkoeffizienten können zurückgewonnen werden durch die für alle $y \in \mathbb{P}_n$ gültige Formel ($z = x + iy$)

$$\begin{aligned} a(t) &= \int_0^1 \cdots \int_0^1 f(z) e^{-2\pi i \cdot \text{Spur}(tz)} dx = e^{2\pi \cdot \text{Spur}(ty)} \int_0^1 \cdots \int_0^1 f(z) e^{-2\pi i \cdot \text{Spur}(tx)} dx \\ &= e^{2\pi \cdot \text{Spur}(ty)} \int_0^1 \cdots \int_0^1 f(z) e_n(-tx) dx. \end{aligned} \quad (4.2)$$

Dabei bezeichnet $dx = \prod_{1 \leq \ell \leq r \leq n} dx_{\ell,r}$ das Euklidische Volumenelement im $\mathbb{R}^{\frac{n(n+1)}{2}}$ [7, S. 149], [16, S. 20], [32, S. 45], [35, S. 44], [38, S. 269].

Wir benutzen die Darstellung (4.2), um zu zeigen, dass jede Siegelsche Modulform negativen Gewichts verschwindet. Zunächst sei dazu an die Höhe $h(z) = \det(y)$ eines Elements $z = x + iy \in \mathbb{H}_n$ erinnert.

Bemerkung 4.1.11. [32, S. 45], [35, S. 47], [45, S. 70, 71], [47, S. 192]

Seien $n \in \mathbb{N}$, $k \in \mathbb{Z}$ und sei $f : \mathbb{H}_n \rightarrow \mathbb{C}$ eine Funktion, die $f|_k m = f$ für alle $m \in \Gamma_n$ erfüllt. Sei

$$g(z) := (\det(y))^{\frac{k}{2}} \cdot |f(z)| = h(z)^{\frac{k}{2}} \cdot |f(z)|, \quad z = x + iy \in \mathbb{H}_n.$$

Für alle $m = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_n$ und alle $z \in \mathbb{H}_n$ gilt mit Bemerkung 3.5.6(a)

$$\begin{aligned} g(m\langle z \rangle) &= h(m\langle z \rangle)^{\frac{k}{2}} \cdot |f(m\langle z \rangle)| \\ &= |\det(cz + d)|^{-k} \cdot h(z)^{\frac{k}{2}} \cdot |\det(cz + d)|^k \cdot |f(z)| \\ &= h(z)^{\frac{k}{2}} \cdot |f(z)| = g(z). \end{aligned}$$

Satz 4.1.12. [21, S. 191], [28, S. 200], [32, S. 45], [35, S. 47], [45, S. 52, 70, 71], [55, S. 626, 637, 638]

Seien $n \in \mathbb{N}$ und $k \in -\mathbb{N}$. Dann gilt $M_k(\Gamma_n) = \{0\}$.

Beweis. Für $f \in M_k(\Gamma_n)$ betrachten wir

$$g(z) = (\det(y))^{\frac{k}{2}} \cdot |f(z)|, \quad z = x + iy \in \mathbb{H}_n,$$

und zeigen zunächst, dass g auf dem Siegelschen Fundamentalbereich \mathcal{F}_n beschränkt ist: Nach der Ungleichung von Minkowski (Satz 3.4.5) und Lemma 3.6.1 gilt für $x + iy \in \mathcal{F}_n$

$$\det(y) \geq c_n^{-1} \cdot \prod_{r=1}^n y_{r,r} \geq c_n^{-1} \cdot \left(\frac{\sqrt{3}}{2}\right)^n \quad \text{und} \quad (\det(y))^{\frac{k}{2}} \leq c_n^{-\frac{k}{2}} \cdot \left(\frac{\sqrt{3}}{2}\right)^{\frac{nk}{2}} \quad \text{wegen } k < 0.$$

Also ist $\mathcal{F}_n \ni x + iy \mapsto (\det(y))^{\frac{k}{2}}$ beschränkt. Um zu zeigen, dass f auf \mathcal{F}_n beschränkt ist, bemerken wir, dass \mathcal{F}_n nach Satz 3.6.3 eine Teilmenge von

$$\left\{ x + iy \in \mathbb{H}_n \mid y \geq \frac{\sqrt{3}}{2 \cdot n^{n-1} \cdot c_n} \cdot I_n \right\} \quad \text{ist.} \quad (4.3)$$

Als Siegelsche Modulform ist f nun auf (4.3) und daher auch auf \mathcal{F}_n beschränkt. Insgesamt ergibt sich die Beschränktheit von g auf \mathcal{F}_n . Wegen Bemerkung 4.1.11 und Satz 3.5.9 ist g dann sogar auf \mathbb{H}_n beschränkt. Es gibt also eine Konstante $c \geq 0$, sodass

$$|f(z)| \leq c \cdot (\det(y))^{-\frac{k}{2}} \quad \text{für alle } z = x + iy \in \mathbb{H}_n \text{ gilt.}$$

Für die Fourierkoeffizienten $a(t)$ von f erhalten wir aus (4.2) die Abschätzung

$$|a(t)| \leq e^{2\pi \cdot \text{Spur}(ty)} \int_0^1 \dots \int_0^1 |f(z)| dx \leq c \cdot e^{2\pi \cdot \text{Spur}(ty)} \cdot (\det(y))^{-\frac{k}{2}}.$$

Für $y = \varepsilon I_n$, $\varepsilon > 0$, ergibt sich schließlich

$$|a(t)| \leq c \cdot e^{2\pi\varepsilon \cdot \text{Spur}(t)} \cdot \varepsilon^{-\frac{nk}{2}} \xrightarrow{\varepsilon \downarrow 0} 0.$$

Daher verschwinden alle Fourierkoeffizienten von f . □

4.2 Thetafunktionen

Wir kehren zur Thetafunktion aus Definition 2.2.13 zurück und wollen zeigen, dass sie unter gewissen Voraussetzungen eine Siegelsche Modulform darstellt. Nach Satz 2.2.15 ist dazu lediglich noch die Transformationseigenschaft (b) aus Definition 4.1.3 zu beweisen, die wir mithilfe von Bemerkung 4.1.5(e) überprüfen werden [16, S. 39, 40].

Lemma 4.2.1. [16, S. 40], [32, S. 48, 49]

(a) Seien $a \in \mathbb{P}_m$ gerade und $b \in M_n(\mathbb{Z})$ symmetrisch. Dann gilt

$$\vartheta_{a,n}(z + b) = \vartheta_{a,n}(z), \quad z \in \mathbb{H}_n.$$

(b) Seien $a \in \mathbb{P}_m$ und $u \in \text{GL}_n(\mathbb{Z})$. Dann gilt

$$\vartheta_{a,n}(z[u]) = \vartheta_{a,n}(z), \quad z \in \mathbb{H}_n.$$

(c) Seien $a \in \mathbb{P}_m$ und $u \in \text{GL}_m(\mathbb{Z})$. Dann gilt

$$\vartheta_{a[u],n}(z) = \vartheta_{a,n}(z), \quad z \in \mathbb{H}_n.$$

Beweis. (a): Für alle $g \in M_{m,n}(\mathbb{Z})$ ist $a[g]$ eine gerade Matrix (Lemma 2.2.4(e)), weshalb $\text{Spur}(a[g] \cdot b) \in 2\mathbb{Z}$ und $e_n(\frac{1}{2}a[g] \cdot b) = e^{\pi i \cdot \text{Spur}(a[g] \cdot b)} = 1$ gilt (Lemma 2.2.4(c)). Daher ergibt sich

$$\begin{aligned} \vartheta_{a,n}(z + b) &= \sum_{g \in M_{m,n}(\mathbb{Z})} e_n\left(\frac{1}{2}a[g] \cdot (z + b)\right) = \sum_{g \in M_{m,n}(\mathbb{Z})} e_n\left(\frac{1}{2}a[g] \cdot z\right) \cdot e_n\left(\frac{1}{2}a[g] \cdot b\right) \\ &= \sum_{g \in M_{m,n}(\mathbb{Z})} e_n\left(\frac{1}{2}a[g] \cdot z\right) = \vartheta_{a,n}(z). \end{aligned}$$

(b): Für alle $g \in M_{m,n}(\mathbb{Z})$ gilt

$$\text{Spur}(a[g] \cdot z[u]) = \text{Spur}(g^T a g u^T z \cdot u) = \text{Spur}(u \cdot g^T a g u^T z) = \text{Spur}(a[gu^T] \cdot z).$$

Mit Lemma 2.5.4(f) folgt

$$\begin{aligned} \vartheta_{a,n}(z[u]) &= \sum_{g \in M_{m,n}(\mathbb{Z})} e_n\left(\frac{1}{2}a[g] \cdot z[u]\right) = \sum_{g \in M_{m,n}(\mathbb{Z})} e_n\left(\frac{1}{2}a[gu^T] \cdot z\right) \\ &= \sum_{g \in M_{m,n}(\mathbb{Z})} e_n\left(\frac{1}{2}a[g] \cdot z\right) = \vartheta_{a,n}(z). \end{aligned}$$

(c): Mit Lemma 2.5.4(e) erhalten wir

$$\vartheta_{a[u],n}(z) = \sum_{g \in M_{m,n}(\mathbb{Z})} e_n\left(\frac{1}{2}a[ug] \cdot z\right) = \sum_{g \in M_{m,n}(\mathbb{Z})} e_n\left(\frac{1}{2}a[g] \cdot z\right) = \vartheta_{a,n}(z). \quad \square$$

Aufwendiger wird es hingegen sein, eine Formel für die Transformation der Thetafunktion unter

$$\begin{aligned} \mathbb{H}_n &\longrightarrow \mathbb{H}_n \\ z &\longmapsto -z^{-1} \end{aligned}$$

herzuleiten. Wir starten dazu mit

Lemma 4.2.2. [16, S. 21], [32, S. 49] Seien $a \in \mathbb{P}_m$, $\tilde{g} \in M_{m,n}(\mathbb{Z})$, $z \in \mathbb{H}_n$ und $w \in M_{m,n}(\mathbb{C})$. Dann gilt

$$e_n\left(\frac{1}{2}a[w] \cdot z - \tilde{g}^T \cdot w\right) = e_n\left(-\frac{1}{2}a^{-1}[\tilde{g}] \cdot z^{-1}\right) \cdot e_n\left(\frac{1}{2}a[w - a^{-1} \cdot \tilde{g} \cdot z^{-1}] \cdot z\right).$$

Beweis. Wir berechnen

$$\begin{aligned} &\text{Spur}(-a^{-1}[\tilde{g}] \cdot z^{-1} + a[w - a^{-1} \cdot \tilde{g} \cdot z^{-1}] \cdot z) \\ &= \text{Spur}(-\tilde{g}^T a^{-1} \tilde{g} \cdot z^{-1} + (w^T - z^{-1} \cdot \tilde{g}^T \cdot a^{-1}) \cdot a \cdot (w - a^{-1} \cdot \tilde{g} \cdot z^{-1}) \cdot z) \\ &= \text{Spur}(-z^{-1} \cdot \tilde{g}^T a^{-1} \tilde{g} + w^T \cdot a \cdot w \cdot z - w^T \cdot \tilde{g} - z^{-1} \cdot \tilde{g}^T w z + z^{-1} \cdot \tilde{g}^T \cdot a^{-1} \cdot \tilde{g}) \\ &= \text{Spur}(a[w] \cdot z - \tilde{g}^T \cdot w - \tilde{g}^T w z \cdot z^{-1}) \\ &= \text{Spur}(a[w] \cdot z - 2\tilde{g}^T \cdot w). \end{aligned} \quad \square$$

Lemma 4.2.3. [3, S. 332, 333], [16, S. 13, 21], [32, S. 50, 51]

Zu jedem $z \in \mathbb{H}_n$ gibt es ein $b \in \text{GL}_n(\mathbb{R})$, sodass $z[b]$ eine Diagonalmatrix ist.

Beweis. Zu $z = x + iy \in \mathbb{H}_n$ gibt es nach Korollar 2.1.11 ein $\tilde{b} \in \text{GL}_n(\mathbb{R})$ mit $\tilde{b}^T \cdot \tilde{b} = y$. Wir wenden Satz 2.1.6 auf die symmetrische Matrix $x[\tilde{b}^{-1}] \in M_n(\mathbb{R})$ an und erhalten $b^* \in \text{GL}_n(\mathbb{R})$, $b^{*T} \cdot b^* = I_n$, sowie $\lambda_1, \dots, \lambda_n \in \mathbb{R}$ mit $x[\tilde{b}^{-1} \cdot b^*] = \text{diag}(\lambda_1, \dots, \lambda_n)$. Daraus folgt

$$\begin{aligned} z[\tilde{b}^{-1} \cdot b^*] &= x[\tilde{b}^{-1} \cdot b^*] + iy[\tilde{b}^{-1} \cdot b^*] = x[\tilde{b}^{-1} \cdot b^*] + iI_n[\tilde{b} \cdot \tilde{b}^{-1} \cdot b^*] \\ &= x[\tilde{b}^{-1} \cdot b^*] + ib^{*T} \cdot b^* \\ &= \text{diag}(\lambda_1, \dots, \lambda_n) + iI_n. \end{aligned} \quad \square$$

Jetzt können wir die für uns entscheidende Transformationsformel beweisen [3, S. 10 – 14], [7, S. 343 – 352], [16, S. 15 – 21], [32, S. 48 – 51], [46, S. 1 – 8], [49, S. 189 – 197], [61, S. 42].

Satz 4.2.4. *Seien $n \in \mathbb{N}$, $m \in 2\mathbb{N}$ und $a \in \mathbb{P}_m$. Dann gilt*

$$\vartheta_{a^{-1},n}(-z^{-1}) = (\det(a))^{\frac{n}{2}} \cdot \left(\det \begin{pmatrix} z \\ i \end{pmatrix} \right)^{\frac{m}{2}} \cdot \vartheta_{a,n}(z), \quad z \in \mathbb{H}_n.$$

Beweis. Für festes $z \in \mathbb{H}_n$ betrachten wir die Funktion

$$F(w) = \sum_{g \in M_{m,n}(\mathbb{Z})} e_n \left(\frac{1}{2} a[g+w] \cdot z \right), \quad w \in M_{m,n}(\mathbb{C}),$$

die $F(w+\tilde{g}) = F(w)$ für alle $\tilde{g} \in M_{m,n}(\mathbb{Z})$ erfüllt. F ist also in jedem $w_{\ell,r}$, $1 \leq \ell \leq m$, $1 \leq r \leq n$, periodisch mit Periode 1 und lässt daher eine Fourierentwicklung in diesen Variablen zu. Da jede ganzzahlige Linearkombination $\sum_{\ell=1}^m \sum_{r=1}^n \tilde{g}_{\ell,r} w_{\ell,r}$, $\tilde{g}_{\ell,r} \in \mathbb{Z}$, von $w_{\ell,r}$, $1 \leq \ell \leq m$, $1 \leq r \leq n$, als

$$\text{Spur}(\tilde{g}^T \cdot w) \quad \text{für genau eine Matrix } \tilde{g} \in M_{m,n}(\mathbb{Z})$$

geschrieben werden kann, können wir die Fourierentwicklung darstellen als

$$F(w) = \sum_{\tilde{g} \in M_{m,n}(\mathbb{Z})} a(\tilde{g}) e^{2\pi i \cdot \text{Spur}(\tilde{g}^T \cdot w)} = \sum_{\tilde{g} \in M_{m,n}(\mathbb{Z})} a(\tilde{g}) e_n(\tilde{g}^T \cdot w).$$

Schreiben wir $w = u + iv$, so sind die Fourierkoeffizienten für alle $v \in M_{m,n}(\mathbb{R})$ gegeben durch

$$\begin{aligned} a(\tilde{g}) &= \int_0^1 \cdots \int_0^1 F(w) e^{-2\pi i \cdot \text{Spur}(\tilde{g}^T \cdot w)} du \\ &= \int_0^1 \cdots \int_0^1 \sum_{g \in M_{m,n}(\mathbb{Z})} e_n \left(\frac{1}{2} a[g+w] \cdot z - \tilde{g}^T \cdot w \right) du \\ &= \int_{M_{m,n}(\mathbb{R})} e_n \left(\frac{1}{2} a[w] \cdot z - \tilde{g}^T \cdot w \right) du. \end{aligned}$$

Nach Lemma 4.2.2 stimmt dies überein mit

$$e_n \left(-\frac{1}{2} a^{-1}[\tilde{g}] \cdot z^{-1} \right) \cdot \int_{M_{m,n}(\mathbb{R})} e_n \left(\frac{1}{2} a[w - a^{-1} \cdot \tilde{g} \cdot z^{-1}] \cdot z \right) du.$$

Wählen wir $v = \text{Im}(a^{-1} \cdot \tilde{g} \cdot z^{-1})$, so ist $w - a^{-1} \cdot \tilde{g} \cdot z^{-1} = u - \text{Re}(a^{-1} \cdot \tilde{g} \cdot z^{-1})$ reell. Substituieren wir dies durch u , folgt

$$a(\tilde{g}) = e_n \left(-\frac{1}{2} a^{-1}[\tilde{g}] \cdot z^{-1} \right) \cdot \int_{M_{m,n}(\mathbb{R})} e_n \left(\frac{1}{2} a[u] \cdot z \right) du.$$

Um

$$\int_{M_{m,n}(\mathbb{R})} e_n \left(\frac{1}{2} a[u] \cdot z \right) du \tag{4.4}$$

zu berechnen, betrachten wir zunächst den Fall $n = 1$: Nach Korollar 2.1.11 gibt es eine Matrix $\tilde{b} \in \mathbb{P}_m$ mit $\tilde{b}^T \cdot \tilde{b} = a$. Indem wir u durch $\tilde{b}^{-1} \cdot u$ substituieren, erhalten wir

$$\begin{aligned} \int_{\mathbb{R}^m} e_1\left(\frac{1}{2}a[u] \cdot z\right) du &= \int_{\mathbb{R}^m} e_1\left(\frac{1}{2}I_m[\tilde{b}u] \cdot z\right) du \\ &= (\det(\tilde{b}))^{-1} \cdot \int_{\mathbb{R}^m} e_1\left(\frac{1}{2}I_m[u] \cdot z\right) du \\ &= (\det(\tilde{b}))^{-1} \cdot \left(\int_{\mathbb{R}} e^{\pi i t^2 z} dt\right)^m. \end{aligned}$$

Für $z = iy$, $y > 0$, ergibt sich daraus

$$(\det(\tilde{b}))^{-1} \cdot \left(\int_{\mathbb{R}} e^{-\pi t^2 y} dt\right)^m = (\det(\tilde{b}))^{-1} \cdot y^{-\frac{m}{2}} \cdot \left(\frac{1}{\sqrt{\pi}} \int_{\mathbb{R}} e^{-t^2} dt\right)^m = (\det(a))^{-\frac{1}{2}} \cdot \left(\frac{z}{i}\right)^{-\frac{m}{2}}.$$

Durch analytische Fortsetzung folgt

$$\int_{\mathbb{R}^m} e_1\left(\frac{1}{2}a[u] \cdot z\right) du = (\det(a))^{-\frac{1}{2}} \cdot \left(\frac{z}{i}\right)^{-\frac{m}{2}} \quad \text{für alle } z \in \mathbb{H}.$$

Dies nutzen wir jetzt aus, um (4.4) für beliebiges $n \in \mathbb{N}$ zu berechnen. Nach Lemma 4.2.3 gibt es ein $b \in \text{GL}_n(\mathbb{R})$, sodass $z[b]$ eine Diagonalmatrix ist. Dann gilt

$$\begin{aligned} (\det(b))^{-m} \cdot (\det(a))^{-\frac{n}{2}} \cdot \left(\det\left(\frac{z}{i}\right)\right)^{-\frac{m}{2}} &= (\det(a))^{-\frac{n}{2}} \cdot \left(\det\left(\frac{z[b]}{i}\right)\right)^{-\frac{m}{2}} \\ &= (\det(a))^{-\frac{n}{2}} \cdot \prod_{r=1}^n \left(\frac{(z[b])_{r,r}}{i}\right)^{-\frac{m}{2}} \\ &= \prod_{r=1}^n \int_{\mathbb{R}^m} e_1\left(\frac{1}{2}a[\tilde{u}] \cdot (z[b])_{r,r}\right) d\tilde{u} \\ &= \int_{M_{m,n}(\mathbb{R})} e_n\left(\frac{1}{2}a[u] \cdot z[b]\right) du \\ &= \int_{M_{m,n}(\mathbb{R})} e_n\left(\frac{1}{2}a[ub^T] \cdot z\right) du \\ &= (\det(b))^{-m} \cdot \int_{M_{m,n}(\mathbb{R})} e_n\left(\frac{1}{2}a[u] \cdot z\right) du. \end{aligned}$$

Damit ist insgesamt

$$\int_{M_{m,n}(\mathbb{R})} e_n\left(\frac{1}{2}a[u] \cdot z\right) du = (\det(a))^{-\frac{n}{2}} \cdot \left(\det\left(\frac{z}{i}\right)\right)^{-\frac{m}{2}}$$

bewiesen. Es gilt also

$$a(\tilde{g}) = e_n\left(-\frac{1}{2}a^{-1}[\tilde{g}] \cdot z^{-1}\right) \cdot (\det(a))^{-\frac{n}{2}} \cdot \left(\det\left(\frac{z}{i}\right)\right)^{-\frac{m}{2}}$$

sowie

$$\vartheta_{a,n}(z) = F(0) = \sum_{\tilde{g} \in M_{m,n}(\mathbb{Z})} a(\tilde{g}) = (\det(a))^{-\frac{n}{2}} \cdot \left(\det\left(\frac{z}{i}\right)\right)^{-\frac{m}{2}} \cdot \vartheta_{a^{-1},n}(-z^{-1}). \quad \square$$

Hiermit können wir das zentrale Ergebnis dieses Abschnitts angeben.

Satz 4.2.5. [3, S. 29], [16, S. 39], [32, S. 51 – 53], [38, S. 272, 273], [61, S. 41 – 43]
 Seien $n \in \mathbb{N}$, $m \in 2\mathbb{N}$ und $a \in M_m(\mathbb{Z})$ eine symmetrische, gerade, positiv definite und unimodulare Matrix. Dann ist m durch 8 teilbar und $\vartheta_{a,n} \in M_{\frac{m}{2}}(\Gamma_n)$.

Beweis. Mit Lemma 4.2.1(c) folgt zunächst $\vartheta_{a,n} = \vartheta_{a^{-1}[a],n} = \vartheta_{a^{-1},n}$. Wegen $\det(a) = 1$ lautet Satz 4.2.4 nun

$$\begin{aligned}\vartheta_{a,n}(-z^{-1}) &= \left(\det\left(\frac{z}{i}\right)\right)^{\frac{m}{2}} \cdot \vartheta_{a,n}(z), \quad z \in \mathbb{H}_n, \\ \vartheta_{a,n}\Big|_{\frac{m}{2}}j &= (-i)^{\frac{nm}{2}} \cdot \vartheta_{a,n}.\end{aligned}\tag{4.5}$$

Des Weiteren gilt nach Lemma 4.2.1(a)

$$\vartheta_{a,n}\Big|_{\frac{m}{2}}\begin{pmatrix} I_n & b \\ 0 & I_n \end{pmatrix} = \vartheta_{a,n}, \quad b \in M_n(\mathbb{Z}) \text{ symmetrisch.}$$

Für $n = 1$ ist $\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot j\right)^3 = -I_2$, woraus

$$(-1)^{\frac{m}{2}} \cdot \vartheta_{a,1} = \vartheta_{a,1}\Big|_{\frac{m}{2}}(-I_2) = \vartheta_{a,1}\Big|_{\frac{m}{2}}\left(\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot j\right)^3\right) = (-i)^{\frac{3m}{2}} \cdot \vartheta_{a,1} = i^{\frac{m}{2}} \cdot \vartheta_{a,1} \quad \text{folgt.}$$

Damit muss $(-1)^{\frac{m}{2}} = i^{\frac{m}{2}}$ gelten. Dies bedeutet $4 \mid \frac{m}{2}$, also ist m durch 8 teilbar und (4.5) ergibt dann $\vartheta_{a,n}\Big|_{\frac{m}{2}}j = \vartheta_{a,n}$. Mit Lemma 4.2.1(b) und Bemerkung 4.1.5(e) erhalten wir, dass $\vartheta_{a,n}$ wie eine Siegelsche Modulform vom Geschlecht n und Gewicht $\frac{m}{2}$ transformiert. Aus Satz 2.2.15 folgt schließlich die Behauptung. \square

Die Aussage von Satz 4.2.5 hängt entscheidend davon ab, ob es Matrizen der geforderten Art gibt. Für $m = 8$ stellen wir ein Beispiel dar in

Lemma 4.2.6. [38, S. 274], [61, S. 45, 46] Sei

$$b := \begin{pmatrix} 0 & 1 & 1 & 1 \\ -1 & 0 & -1 & 1 \\ -1 & 1 & 0 & -1 \\ -1 & -1 & 1 & 0 \end{pmatrix} \in M_4(\mathbb{Z}).$$

Dann ist

$$a_8 := \begin{pmatrix} 2I_4 & b \\ -b & 2I_4 \end{pmatrix} \in M_8(\mathbb{Z})$$

symmetrisch, gerade, positiv definit und unimodular.

Beweis. Aus $b^T = -b$ folgt, dass a_8 eine symmetrische Matrix ist, welche per Konstruktion gerade ist.

Wenden wir Lemma 3.1.1 auf a_8 an, so erhalten wir

$$a_8 = \begin{pmatrix} 2I_4 & 0 \\ 0 & 2I_4 - \frac{1}{2}b^T \cdot b \end{pmatrix} \left[\begin{pmatrix} I_4 & \frac{1}{2}b \\ 0 & I_4 \end{pmatrix} \right] = \begin{pmatrix} 2I_4 & 0 \\ 0 & \frac{1}{2}I_4 \end{pmatrix} \left[\begin{pmatrix} I_4 & \frac{1}{2}b \\ 0 & I_4 \end{pmatrix} \right], \tag{4.6}$$

wobei $b^T \cdot b = -b^2 = 3I_4$ ausgenutzt wurde. Aus (4.6) folgt einerseits $\det(a_8) = 1$ und andererseits, dass a_8 positiv definit ist. \square

Beispiel 4.2.7. [38, S. 275], [60, S. 8, 9, 10, 21], [61, S. 44, 46]

Es gilt $\vartheta_{a_8} = \vartheta_{a_8,1} \in M_4(\Gamma_1)$. Dieser Vektorraum wird aufgespannt von

$$G_4(z) := \frac{1}{240} + \sum_{t=1}^{\infty} \sigma_3(t) e^{2\pi itz}, \quad z \in \mathbb{H}.$$

Aus (2.6) erhalten wir

$$\vartheta_{a_8} = 240 \cdot G_4 \quad \text{sowie} \quad r_{a_8}(t) = 240 \cdot \sigma_3(t) \quad \text{für alle } t \in \mathbb{N}.$$

Der erste Teil von Satz 4.2.5 und Beispiel 4.2.7 gehen auf Schoeneberg [53] zurück [38, S. 275], [53, S. 511, 520, 521].

Bemerkung 4.2.8. [38, S. 268, 274] Seien $a_1 \in M_{m_1}(\mathbb{Z})$ und $a_2 \in M_{m_2}(\mathbb{Z})$ symmetrisch, gerade, positiv definit und unimodular. Dann ist auch die *direkte Summe*

$$a_1 \oplus a_2 := \begin{pmatrix} a_1 & 0 \\ 0 & a_2 \end{pmatrix} \in M_{m_1+m_2}(\mathbb{Z})$$

symmetrisch, gerade und unimodular. Wegen $(a_1 \oplus a_2) \left[\begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \right] = a_1[v_1] + a_2[v_2]$ für $v_1 \in \mathbb{R}^{m_1}$ und $v_2 \in \mathbb{R}^{m_2}$ ist auch $a_1 \oplus a_2$ positiv definit.

Indem wir direkte Summen von a_8 bilden, folgt die Existenz einer symmetrischen, geraden, positiv definiten und unimodularen Matrix $a \in M_m(\mathbb{Z})$ für jedes durch 8 teilbare m [38, S. 274].

4.3 Das Prinzip von Koecher

In der Theorie der klassischen Modulformen stellt es sich als nützlich heraus, die klassische Wachstumsbedingung abzuschwächen, um auch schwach holomorphe Modulformen wie die absolute Invariante j zu untersuchen [21, S. 191], [35, S. 45, 46], [36, S. 399], [60, S. 24, 25].

Daher widmen wir uns der Wachstumsbedingung (c) aus Definition 4.1.3. Erstaunlicherweise wird sich diese für $n \geq 2$ als überflüssig herausstellen. Das heißt, sie folgt bereits aus den Bedingungen (a) und (b) von Definition 4.1.3. Dieses Erkenntnis fand allgemein Bedeutung durch Koechers Arbeit [36], wurde aber schon vorher von Götzky im Zusammenhang mit Hilbertschen Modulformen in [23] bemerkt [21, S. 191], [35, S. 45, 46], [36, S. 399].

Satz 4.3.1 (Das Prinzip von Koecher). [3, S. 3, 65 – 69], [16, S. 44, 45], [21, S. 191, 192], [28, S. 198 – 200], [32, S. 46, 47], [35, S. 45, 46], [37, S. 11]

Seien $n \in \mathbb{N} \setminus \{1\}$, $k \in \mathbb{Z}$ und $f : \mathbb{H}_n \rightarrow \mathbb{C}$ holomorph mit der Eigenschaft

$$f(z[u] + b) = (\det(u))^k \cdot f(z)$$

für alle $z \in \mathbb{H}_n$, $u \in \text{GL}_n(\mathbb{Z})$ und symmetrischen $b \in M_n(\mathbb{Z})$. Dann gelten folgende Aussagen:

(a) f besitzt die in \mathbb{H}_n absolut konvergente Fourierentwicklung

$$f(z) = \sum_{t \in \mathbb{A}_n} a(t) e_n(tz), \quad z \in \mathbb{H}_n, \tag{4.7}$$

wobei $\mathbb{A}_n = \{t \in M_n(\mathbb{R}) \mid t^T = t, t \text{ halbganz}, t \geq 0\}$ in (2.9) definiert wurde.

(b) Die Reihe (4.7) ist in jedem Bereich der Form

$$\{z \in \mathbb{H}_n \mid \operatorname{Im}(z) \geq y_0\}, \quad y_0 \in \mathbb{P}_n, \quad (4.8)$$

gleichmäßig konvergent.

(c) f ist in jedem Bereich der Form (4.8) beschränkt.

(d) f ist in \mathcal{F}_n beschränkt.

Beweis. Zum Beweis von (a) betrachten wir die absolut konvergente Fourierreihe

$$f(z) = \sum_{\substack{t^T = t \in M_n(\mathbb{R}) \\ t \text{ halbganz}}} a(t)e_n(tz), \quad z \in \mathbb{H}_n.$$

Sie konvergiert insbesondere in $z = iI_n \in \mathbb{H}_n$, weshalb die zugehörige Folge

$$a(t)e_n(it) = a(t)e^{-2\pi \cdot \operatorname{Spur}(t)}, \quad t^T = t \in M_n(\mathbb{R}) \text{ halbganz,}$$

beschränkt ist. Dies bedeutet, es gibt ein $c \geq 0$ mit der Eigenschaft

$$|a(t)| \leq c \cdot e^{2\pi \cdot \operatorname{Spur}(t)} \quad \text{für alle halbganzen } t^T = t \in M_n(\mathbb{R}). \quad (4.9)$$

Sei $t \in M_n(\mathbb{R})$ eine symmetrische und halbganze Matrix, die *nicht* positiv semidefinit ist. Zu zeigen ist dann, dass $a(t) = 0$ gilt. Da t nicht positiv semidefinit ist, muss es einen Vektor $v \in \mathbb{R}^n \setminus \{0\}$ mit $t[v] < 0$ geben. Durch Approximation (\mathbb{Q}^n liegt dicht in \mathbb{R}^n) können wir sogar $v \in \mathbb{Q}^n \setminus \{0\}$ annehmen. Anschließendes Multiplizieren mit dem Produkt der Nenner der Einträge von v liefert sogar einen ganzzahligen Vektor, aus dem wir den größten gemeinsamen Teiler herausteilen: Wir können also annehmen, dass es einen Vektor $v \in \mathbb{Z}^n \setminus \{0\}$ mit teilerfremden Einträgen gibt, der $t[v] < 0$ erfüllt.

Nach Lemma 2.5.10 existiert ein $u \in \operatorname{GL}_n(\mathbb{Z})$ mit erster Spalte v . Das erste Diagonalelement der symmetrischen und halbganzen Matrix $\tilde{t} := t[u] \in M_n(\mathbb{R})$ ist dann $\tilde{t}_{1,1} = (t[u])_{1,1} = t[v] < 0$.

Betrachten wir für $m \in \mathbb{Z}$ die obere Dreiecksmatrix $\tilde{u} \in \operatorname{GL}_n(\mathbb{Z})$, definiert durch

$$\tilde{u}_{\ell,r} := \begin{cases} 1, & \text{wenn } 1 \leq \ell = r \leq n, \\ m, & \text{wenn } \ell = 1, r = 2, \\ 0, & \text{andernfalls,} \end{cases}$$

so ist $\tilde{t}[\tilde{u}] \in M_n(\mathbb{R})$ eine symmetrische und halbganze Matrix. Es gilt

$$\begin{aligned} \operatorname{Spur}(\tilde{t}[\tilde{u}]) &= \sum_{r=1}^n (\tilde{t}[\tilde{u}])_{r,r} = \tilde{t}[(m, 1, 0, \dots, 0)^T] + \sum_{\substack{r=1 \\ r \neq 2}}^n \tilde{t}[e_r] \\ &= \tilde{t}[me_1 + e_2] + \sum_{\substack{r=1 \\ r \neq 2}}^n \tilde{t}[e_r] = m^2 \cdot \tilde{t}[e_1] + me_1^T \cdot \tilde{t} \cdot e_2 + me_2^T \cdot \tilde{t} \cdot e_1 + \tilde{t}[e_2] + \sum_{\substack{r=1 \\ r \neq 2}}^n \tilde{t}[e_r] \\ &= m^2 \cdot \tilde{t}_{1,1} + 2m\tilde{t}_{1,2} + \sum_{r=1}^n \tilde{t}_{r,r} = m^2 \cdot \tilde{t}_{1,1} + 2m\tilde{t}_{1,2} + \operatorname{Spur}(\tilde{t}) \xrightarrow{m \rightarrow \infty} -\infty \end{aligned}$$

wegen $\tilde{t}_{1,1} < 0$. Mit Lemma 4.1.7 und (4.9) folgt daraus

$$|a(t)| = |a(t[u\tilde{u}])| = |a(\tilde{t}[\tilde{u}])| \leq c \cdot e^{2\pi \cdot \text{Spur}(\tilde{t}[\tilde{u}])} \xrightarrow{m \rightarrow \infty} 0.$$

Damit ist Aussage (a) gezeigt, die wir zum Beweis von (b) und (c) nutzen:

Sei $y_0 \in \mathbb{P}_n$. Für alle $z = x + iy \in \mathbb{H}_n$ mit $y \geq y_0$ und alle $t \in \mathbb{A}_n$ gilt $\text{Spur}(ty) \geq \text{Spur}(ty_0)$ nach Bemerkung 2.1.13, woraus

$$|a(t)e_n(tz)| = |a(t)|e^{-2\pi \cdot \text{Spur}(ty)} \leq |a(t)|e^{-2\pi \cdot \text{Spur}(ty_0)} \quad \text{folgt.} \quad (4.10)$$

Die absolute Konvergenz von (4.7) in $iy_0 \in \mathbb{H}_n$ liefert die von z unabhängige konvergente Reihe $\sum_{t \in \mathbb{A}_n} |a(t)|e^{-2\pi \cdot \text{Spur}(ty_0)}$, die nun die Reihe (4.7) (wegen (4.10)) majorisiert. Damit sind auch die

Aussagen (b) und (c) bewiesen.

Die Aussage (d) folgt aus (c), da \mathcal{F}_n eine Teilmenge von (4.3) ist. □

Offensichtlich geht die Voraussetzung $n \geq 2$ bei der Definition von \tilde{u} im Beweis von (a) ein [35, S. 46].

Korollar 4.3.2. [3, S. 65 – 69], [7, S. 99, 101, 149], [16, S. 43 – 45], [38, S. 153 – 156], [47, S. 187], [60, S. 8]

Seien $n \in \mathbb{N}$, $k \in \mathbb{Z}$ und $f \in M_k(\Gamma_n)$. Dann hat f die in \mathbb{H}_n absolut konvergente Fourierentwicklung

$$f(z) = \sum_{t \in \mathbb{A}_n} a(t)e_n(tz), \quad z \in \mathbb{H}_n, \quad (4.11)$$

die in jedem Bereich der Form $\{z \in \mathbb{H}_n \mid \text{Im}(z) \geq y_0\}$, $y_0 \in \mathbb{P}_n$, gleichmäßig konvergiert.

Beweis. Für $n \in \mathbb{N} \setminus \{1\}$ ergibt sich das Korollar sofort aus Satz 4.3.1. Im Fall $n = 1$ ist f eine klassische Modulform: Aus Bedingung (c) von Definition 4.1.3 folgt, dass f die absolut konvergente Fourierentwicklung $f(z) = \sum_{t=0}^{\infty} a(t)e^{2\pi itz}$, $z \in \mathbb{H}$, hat. Diese Reihe ist für $z = x + iy \in \mathbb{H}$

mit $y \geq y_0 > 0$ gleichmäßig konvergent, da der Beweis von Satz 4.3.1(b) auch für $n = 1$ gültig ist. □

4.4 Der Siegelsche Operator Φ

Im Fall $n = 1$ sind Spitzenformen aus $M_k(\Gamma_1)$ dadurch charakterisiert, dass der konstante Term ihrer Fourierentwicklung verschwindet [38, S. 156], [60, S. 10]. Im Hinblick auf Korollar 4.3.2 ist für *Siegelsche Spitzenformen* dementsprechend zu erwarten, dass nur über positiv definite Matrizen

$$t \in \mathbb{A}_n^+ := \{t \in \mathbb{A}_n \mid t > 0\} = \{t \in M_n(\mathbb{R}) \mid t^T = t, t \text{ halbganz}, t > 0\}$$

in (4.11) zu summieren ist [16, S. 46], [32, S. 54], [35, S. 56].

Anstatt aber Siegelsche Spitzenformen derart einzuführen, ist es für weitere Resultate vorteilhaft, sie als Kern eines von Siegel [55] eingeführten Operators zu definieren [32, S. 54], [35, S. 54, 56], [55, S. 636 – 638]. Mit diesem Operator beschäftigen wir uns zunächst.

Lemma 4.4.1. [3, S. 74, 75], [16, S. 45], [24, S. 554], [35, S. 54 – 56], [45, S. 72, 73], [55, S. 636 – 638]

Seien $n \in \mathbb{N}$, $k, r \in \mathbb{Z}$ mit $0 \leq r \leq n - 1$ und sei $f \in M_k(\Gamma_n)$ mit Fourierentwicklung

$$f(z) = \sum_{t \in \mathbb{A}_n} a(t) e_n(tz), \quad z \in \mathbb{H}_n. \quad (4.12)$$

Dann existiert

$$(f|_{\Phi^{n-r}})(\tilde{z}) := \lim_{\lambda \rightarrow \infty} f \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix}, \quad \tilde{z} \in \mathbb{H}_r, \quad (4.13)$$

und besitzt die Fourierentwicklung

$$(f|_{\Phi^{n-r}})(\tilde{z}) = \sum_{\tilde{t} \in \mathbb{A}_r} a \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix} e_r(\tilde{t}\tilde{z}), \quad \tilde{z} \in \mathbb{H}_r. \quad (4.14)$$

Für $r \geq 1$ ist (4.14) in \mathbb{H}_r absolut konvergent und in jedem Bereich der Form

$$\{\tilde{z} \in \mathbb{H}_r \mid \text{Im}(\tilde{z}) \geq \tilde{y}_0\}, \quad \tilde{y}_0 \in \mathbb{P}_r,$$

gleichmäßig konvergent und beschränkt. $f|_{\Phi^{n-r}}$ stellt in \mathbb{H}_r eine holomorphe Funktion dar.

Im Hinblick auf (4.13) ist es sinnvoll, $f|_{\Phi^0} := f$ für $f \in M_k(\Gamma_n)$ zu definieren.

Zum Beweis des Lemmas 4.4.1 benötigen wir

Lemma 4.4.2. [16, S. 45], [38, S. 265], [61, S. 76]

Seien $n \in \mathbb{N}$, $r \in \mathbb{Z}$ mit $0 \leq r \leq n - 1$. Dann sind folgende Aussagen äquivalent:

(a) $t = \begin{pmatrix} t_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix} \in M_n(\mathbb{R})$ mit $t_1^{(r)} \in \mathbb{A}_r$.

(b) $t \in \mathbb{A}_n$ mit $t_{\ell,\ell} = 0$ für alle $r + 1 \leq \ell \leq n$.

Beweis. (a) \Rightarrow (b): Für $t_1^{(r)} \in \mathbb{A}_r$ ist $t = \begin{pmatrix} t_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix} \in M_n(\mathbb{R})$ offensichtlich symmetrisch und

halbganzz. Für $v_1 \in \mathbb{R}^r$ und $v_2 \in \mathbb{R}^{n-r}$ gilt $t \begin{bmatrix} v_1 \\ v_2 \end{bmatrix} = t_1^{(r)}[v_1] \geq 0$, also ist t auch positiv semidefinit, das heißt $t \in \mathbb{A}_n$.

(b) \Rightarrow (a): Die zu $t \in \mathbb{A}_n$ gehörige quadratische Form $t[v]$, $v \in \mathbb{R}^n$, ist auch auf dem zweidimensionalen linearen Spann $\text{span}_{\mathbb{R}}\{e_i, e_j\}$, $1 \leq i, j \leq n$, $i \neq j$, positiv semidefinit. Daher hat die Matrix

$$\begin{pmatrix} t[e_i] & e_i^T \cdot t \cdot e_j \\ e_j^T \cdot t \cdot e_i & t[e_j] \end{pmatrix} = \begin{pmatrix} t_{i,i} & t_{i,j} \\ t_{i,j} & t_{j,j} \end{pmatrix}$$

eine nichtnegative Determinante $t_{i,i}t_{j,j} - t_{i,j}^2 \geq 0$. Für $r + 1 \leq i \leq n$ ist $t_{i,i} = 0$, weshalb nun $t_{i,j} = 0$ für alle $j \neq i$ folgt. Daher verschwinden alle Einträge von t in den Zeilen $r + 1, \dots, n$. Da

die Matrix t symmetrisch und halbganzz ist, hat es die Gestalt $t = \begin{pmatrix} t_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix}$ mit symmetrischer

und halbganzz Matrix $t_1^{(r)} \in M_r(\mathbb{R})$. Wegen $t_1^{(r)}[v_1] = t \begin{bmatrix} v_1 \\ 0 \end{bmatrix} \geq 0$ für alle $v_1 \in \mathbb{R}^r$ ist $t_1^{(r)}$

auch positiv semidefinit, also $t_1^{(r)} \in \mathbb{A}_r$. □

Beweis des Lemmas 4.4.1. Seien $\tilde{z} \in \mathbb{H}_r$, $\lambda > 0$ und sei $t = \begin{pmatrix} t_1^{(r)} & t_2^{(r)} \\ (t_2^{(r)})^\top & t_4^{(r)} \end{pmatrix} \in \mathbb{A}_n$ zerlegt gemäß (1.3). Dann ist

$$\begin{aligned} \text{Spur} \left(t \cdot \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \right) &= \text{Spur} \begin{pmatrix} t_1^{(r)} \cdot \tilde{z} & * \\ * & i\lambda t_4^{(r)} \end{pmatrix} = \text{Spur}(t_1^{(r)} \cdot \tilde{z}) + i\lambda \cdot \text{Spur}(t_4^{(r)}) \\ &= \text{Spur}(t_1^{(r)} \cdot \tilde{z}) + i\lambda \cdot \sum_{\ell=r+1}^n t_{\ell,\ell}. \end{aligned} \quad (4.15)$$

Um Lemma 4.4.2 anzuwenden, machen wir eine Fallunterscheidung:

Fall (a): Falls $t_{\ell,\ell} = 0$ für alle $r+1 \leq \ell \leq n$ gilt, so liefert (4.15) den von λ unabhängigen Ausdruck $\text{Spur} \left(t \cdot \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \right) = \text{Spur}(t_1^{(r)} \cdot \tilde{z})$. Nach Lemma 4.4.2 hat t die Gestalt $t = \begin{pmatrix} t_1^{(r)} & 0 \\ 0 & 0 \end{pmatrix}$ mit $t_1^{(r)} \in \mathbb{A}_r$.

Fall (b): Falls hingegen ein $r+1 \leq \ell \leq n$ mit $t_{\ell,\ell} > 0$ existiert, so ist $\sum_{\ell=r+1}^n t_{\ell,\ell} > 0$, woraus

$$e_n \left(t \cdot \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \right) = e_r(t_1^{(r)} \cdot \tilde{z}) \cdot e^{-2\pi\lambda \cdot \sum_{\ell=r+1}^n t_{\ell,\ell}} \xrightarrow{\lambda \rightarrow \infty} 0 \quad \text{folgt.}$$

Nach Korollar 2.2.1 gibt es ein $\delta > 0$ mit $\text{Im}(\tilde{z}) \geq \delta I_r$. Für $\lambda \geq \delta$ ist daher

$$\begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \in \{z \in \mathbb{H}_n \mid \text{Im}(z) \geq \delta I_n\}.$$

Wegen der gleichmäßigen Konvergenz von (4.12) in $\{z \in \mathbb{H}_n \mid \text{Im}(z) \geq \delta I_n\}$ (Korollar 4.3.2) können wir den Limes in (4.13) gliedweise bilden und erhalten

$$(f|\Phi^{n-r})(\tilde{z}) = \sum_{t \in \mathbb{A}_n} a(t) \lim_{\lambda \rightarrow \infty} e_n \left(t \cdot \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \right) = \sum_{\tilde{t} \in \mathbb{A}_r} a \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix} e_r(\tilde{t}\tilde{z}).$$

Dies ist eine Teilreihe von (4.12), woraus auch die Aussagen über die Konvergenz und Beschränktheit folgen. Also ist $f|\Phi^{n-r}$ in \mathbb{H}_r holomorph. \square

Beispiel 4.4.3. [3, S. 75], [38, S. 156], [55, S. 637]

Sei $f \in M_k(\Gamma_n)$ mit Fourierentwicklung $f(z) = \sum_{t \in \mathbb{A}_n} a(t)e_n(tz)$, $z \in \mathbb{H}_n$. Für $r = 0$ verstehen wir unter (4.13) den Grenzwert $f|\Phi^n = \lim_{\lambda \rightarrow \infty} f(i\lambda I_n)$, der den Term $a(0)$ der Fourierentwicklung von f liefert: $f|\Phi^n = a(0)$.

Beispiel 4.4.4. [3, S. 77] Seien $n = 1$, $m \in 8\mathbb{N}$ und sei $a \in M_m(\mathbb{Z})$ symmetrisch, gerade, positiv definit und unimodular. Für die Thetafunktion $\vartheta_a \in M_{\frac{m}{2}}(\Gamma_1)$ gilt $\vartheta_a|\Phi = r_a(0) = 1$.

Für $n = 0$ und $k \in \mathbb{Z}$ erweitern wir Definition 4.1.3 durch

$$M_k(\Gamma_0) := \begin{cases} \mathbb{C}, & \text{wenn } k \geq 0, \\ \{0\}, & \text{wenn } k < 0. \end{cases} \quad (4.16)$$

Satz 4.4.5. [3, S. 75, 76], [16, S. 45, 46], [35, S. 54 – 56], [45, S. 73, 74], [47, S. 187 – 189], [51, S. 7], [55, S. 637]

Seien $n \in \mathbb{N}$, $k, r \in \mathbb{Z}$ mit $0 \leq r \leq n$ und sei $f \in M_k(\Gamma_n)$. Dann ist $f|_{\Phi^{n-r}} \in M_k(\Gamma_r)$.

Beweis. Für $r = n$ ist nichts zu beweisen. Die Aussage für $r = 0$ ergibt sich aus Beispiel 4.4.3 und Satz 4.1.12. Für $1 \leq r \leq n - 1$ müssen wir nach Lemma 4.4.1 nur noch die Transformationseigenschaft von $f|_{\Phi^{n-r}}$ nachweisen: Sei dazu $\tilde{m} = \begin{pmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{pmatrix} \in \Gamma_r$, $\tilde{a}, \tilde{b}, \tilde{c}, \tilde{d} \in M_r(\mathbb{Z})$, und wir definieren die $n \times n$ -Matrizen

$$a := \begin{pmatrix} \tilde{a} & 0 \\ 0 & I_{n-r} \end{pmatrix}, \quad b := \begin{pmatrix} \tilde{b} & 0 \\ 0 & 0 \end{pmatrix}, \quad c := \begin{pmatrix} \tilde{c} & 0 \\ 0 & 0 \end{pmatrix}, \quad d := \begin{pmatrix} \tilde{d} & 0 \\ 0 & I_{n-r} \end{pmatrix}.$$

Betrachten wir $m := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2n}(\mathbb{Z})$, so gilt mit Lemma 2.3.5(d)

$$\begin{aligned} a^T \cdot c &= \begin{pmatrix} \tilde{a}^T \cdot \tilde{c} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \tilde{c}^T \cdot \tilde{a} & 0 \\ 0 & 0 \end{pmatrix} = c^T \cdot a, \\ b^T \cdot d &= \begin{pmatrix} \tilde{b}^T \cdot \tilde{d} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \tilde{d}^T \cdot \tilde{b} & 0 \\ 0 & 0 \end{pmatrix} = d^T \cdot b, \\ a^T \cdot d - c^T \cdot b &= \begin{pmatrix} \tilde{a}^T \cdot \tilde{d} & 0 \\ 0 & I_{n-r} \end{pmatrix} - \begin{pmatrix} \tilde{c}^T \cdot \tilde{b} & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} \tilde{a}^T \cdot \tilde{d} - \tilde{c}^T \cdot \tilde{b} & 0 \\ 0 & I_{n-r} \end{pmatrix} = \begin{pmatrix} I_r & 0 \\ 0 & I_{n-r} \end{pmatrix} = I_n. \end{aligned}$$

Daher ist $m \in \Gamma_n$. Für alle $\tilde{z} \in \mathbb{H}_r$ und $\lambda > 0$ ist

$$\begin{aligned} m \left\langle \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \right\rangle &= \left(a \cdot \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} + b \right) \cdot \left(c \cdot \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} + d \right)^{-1} \\ &= \begin{pmatrix} \tilde{a}\tilde{z} + \tilde{b} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \cdot \begin{pmatrix} \tilde{c}\tilde{z} + \tilde{d} & 0 \\ 0 & I_{n-r} \end{pmatrix}^{-1} \\ &= \begin{pmatrix} \tilde{a}\tilde{z} + \tilde{b} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \cdot \begin{pmatrix} (\tilde{c}\tilde{z} + \tilde{d})^{-1} & 0 \\ 0 & I_{n-r} \end{pmatrix} = \begin{pmatrix} \tilde{m}(\tilde{z}) & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix}. \end{aligned}$$

Außerdem haben wir

$$\det \left(c \cdot \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} + d \right) = \det \begin{pmatrix} \tilde{c}\tilde{z} + \tilde{d} & 0 \\ 0 & I_{n-r} \end{pmatrix} = \det(\tilde{c}\tilde{z} + \tilde{d}).$$

Damit erhalten wir schließlich

$$\begin{aligned} ((f|_{\Phi^{n-r}})|_k \tilde{m})(\tilde{z}) &= \det(\tilde{c}\tilde{z} + \tilde{d})^{-k} \cdot (f|_{\Phi^{n-r}})(\tilde{m}(\tilde{z})) \\ &= \lim_{\lambda \rightarrow \infty} \det(\tilde{c}\tilde{z} + \tilde{d})^{-k} \cdot f \left(\begin{pmatrix} \tilde{m}(\tilde{z}) & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \right) \\ &= \lim_{\lambda \rightarrow \infty} \det \left(c \cdot \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} + d \right)^{-k} \cdot f \left(m \left\langle \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \right\rangle \right) \\ &= \lim_{\lambda \rightarrow \infty} (f|_k m) \left(\begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \right) = \lim_{\lambda \rightarrow \infty} f \left(\begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda I_{n-r} \end{pmatrix} \right) = (f|_{\Phi^{n-r}})(\tilde{z}). \quad \square \end{aligned}$$

Beispiel 4.4.6. [16, S. 45, 46], [35, S. 54 – 56] Für $r = n - 1$ erhalten wir den *Siegelschen Operator*

$$\begin{aligned} \Phi : M_k(\Gamma_n) &\longrightarrow M_k(\Gamma_{n-1}) \\ f &\longmapsto f|\Phi \end{aligned}$$

mit $(f|\Phi)(\tilde{z}) = \lim_{\lambda \rightarrow \infty} f \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda \end{pmatrix}$, $\tilde{z} \in \mathbb{H}_{n-1}$. Hat f die Fourierentwicklung $f(z) = \sum_{t \in \mathbb{A}_n} a(t)e_n(tz)$, $z \in \mathbb{H}_n$, so besitzt $f|\Phi$ die Fourierentwicklung

$$(f|\Phi)(\tilde{z}) = \sum_{\tilde{t} \in \mathbb{A}_{n-1}} a \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix} e_{n-1}(\tilde{t}\tilde{z}), \quad \tilde{z} \in \mathbb{H}_{n-1}. \quad (4.17)$$

Beispiel 4.4.7. [3, S. 77], [16, S. 46], [32, S. 55, 56]

Seien $n \in \mathbb{N} \setminus \{1\}$, $m \in 8\mathbb{N}$ und sei $a \in M_m(\mathbb{Z})$ eine symmetrische, gerade, positiv definite und unimodulare Matrix. Für $\vartheta_{a,n}(z) = \sum_{t \in \mathbb{A}_n} r_a(t)e_n(tz) \in M_{\frac{m}{2}}(\Gamma_n)$ ergibt (4.17) die Darstellung

$$(\vartheta_{a,n}|\Phi)(\tilde{z}) = \sum_{\tilde{t} \in \mathbb{A}_{n-1}} r_a \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix} e_{n-1}(\tilde{t}\tilde{z}), \quad \tilde{z} \in \mathbb{H}_{n-1}. \quad (4.18)$$

Wir zeigen nun, dass

$$r_a \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix} = r_a(\tilde{t}) \quad \text{für alle } \tilde{t} \in \mathbb{A}_{n-1} \text{ gilt.} \quad (4.19)$$

Für $\tilde{g} \in M_{m,n-1}(\mathbb{Z})$ mit $\frac{1}{2}a[\tilde{g}] = \tilde{t}$ ergibt sich $\frac{1}{2}a[(\tilde{g}|0)] = \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix}$. Wir betrachten daher die injektive Abbildung

$$\begin{aligned} \left\{ \tilde{g} \in M_{m,n-1}(\mathbb{Z}) \mid \frac{1}{2}a[\tilde{g}] = \tilde{t} \right\} &\longrightarrow \left\{ g \in M_{m,n}(\mathbb{Z}) \mid \frac{1}{2}a[g] = \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix} \right\} \\ \tilde{g} &\longmapsto (\tilde{g}|0). \end{aligned}$$

Um zu zeigen, dass sie surjektiv ist, betrachten wir $g = (g_1 | \dots | g_n) \in M_{m,n}(\mathbb{Z})$ mit der Eigenschaft $\frac{1}{2}a[g] = \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix}$. Hieraus folgt einerseits $\frac{1}{2}a[(g_1 | \dots | g_{n-1})] = \tilde{t}$, andererseits ist $\frac{1}{2}a[g_n] = 0$, also $g_n = 0$. Dies zeigt schließlich die Surjektivität. Damit ist die Abbildung bijektiv, woraus (4.19) folgt.

Die Darstellung (4.18) ergibt für alle $\tilde{z} \in \mathbb{H}_{n-1}$ daher

$$(\vartheta_{a,n}|\Phi)(\tilde{z}) = \sum_{\tilde{t} \in \mathbb{A}_{n-1}} r_a(\tilde{t})e_{n-1}(\tilde{t}\tilde{z}) = \vartheta_{a,n-1}(\tilde{z}).$$

Wegen der Linearität des Grenzwertes ist der Siegelsche Operator Φ eine lineare Abbildung. Der Kern von Φ , nämlich die sogenannten *Siegelschen Spitzenformen*, ist von besonderem Interesse [35, S. 54, 56], [37, S. 14].

4.5 Siegelsche Spitzenformen

Definition 4.5.1. [35, S. 54, 56], [37, S. 14] Für $n \in \mathbb{N}$ und $k \in \mathbb{Z}$ definieren wir den Vektorraum der *Siegelschen Spitzenformen vom Geschlecht n und Gewicht k* durch

$$S_k(\Gamma_n) := \text{Ker}(\Phi) = \{f \in M_k(\Gamma_n) \mid f|_k\Phi = 0\}.$$

Für $n = 0$ setzen wir $S_k(\Gamma_0) := M_k(\Gamma_0)$.

Im Fall $n = 1$ ergibt sich die Definition einer Spitzenform, wie wir sie aus der Theorie der klassischen Modulformen kennen [38, S. 156]:

Beispiel 4.5.2. Für $n = 1$ erhalten wir aus Beispiel 4.4.3

$$S_k(\Gamma_1) = \{f \in M_k(\Gamma_1) \mid f|_k\Phi = 0\} = \left\{ \sum_{t=0}^{\infty} a(t)e^{2\pi itz} \in M_k(\Gamma_1) \mid a(0) = 0 \right\}.$$

Die Charakterisierung von Spitzenformen durch die besondere Gestalt ihrer Fourierreentwicklung ist auch im allgemeinen Fall möglich [3, S. 78, 79], [16, S. 46], [32, S. 56], [35, S. 56], [51, S. 7]:

Satz 4.5.3. Seien $n \in \mathbb{N}$, $k \in \mathbb{Z}$ und $f \in M_k(\Gamma_n)$ mit Fourierreentwicklung

$$f(z) = \sum_{t \in \mathbb{A}_n} a(t)e_n(tz), \quad z \in \mathbb{H}_n.$$

Dann sind folgende Aussagen äquivalent:

- (a) $f \in S_k(\Gamma_n)$.
- (b) $a(t) = 0$ für alle $t \in \mathbb{A}_n \setminus \mathbb{A}_n^+$.
- (c) $f(z) = \sum_{t \in \mathbb{A}_n^+} a(t)e_n(tz)$, $z \in \mathbb{H}_n$.

Beweis. Die Äquivalenz zwischen (b) und (c) ist klar.

(a) \Rightarrow (b): Sei $f \in S_k(\Gamma_n)$ und wir betrachten $t \in \mathbb{A}_n \setminus \mathbb{A}_n^+ \subset M_n(\mathbb{Q})$. Eine solche Matrix t besitzt den Eigenwert 0. Es gibt also einen Eigenvektor $v \in \mathbb{Q}^n \setminus \{0\}$ mit $tv = 0$. Durch Multiplizieren mit dem Produkt der Nenner der Einträge von v können wir $v \in \mathbb{Z}^n \setminus \{0\}$ annehmen. Durch Herausteilen des größten gemeinsamen Teilers der Einträge ist es sogar möglich anzunehmen, dass $tv = 0$ von einem Vektor $v \in \mathbb{Z}^n \setminus \{0\}$ mit teilerfremden Einträgen erfüllt wird.

Nach Lemma 2.5.10 gibt es ein $u \in \text{GL}_n(\mathbb{Z})$ mit letzter Spalte v . Das letzte Diagonalelement der Matrix $t[u] \in \mathbb{A}_n$ ist dann $(t[u])_{n,n} = t[v] = v^T \cdot tv = 0$. Unter Verwendung von Lemma 4.4.2 folgt

$$t[u] = \begin{pmatrix} (t[u]_1^{(n-1)}) & 0 \\ 0 & 0 \end{pmatrix} \quad \text{mit} \quad (t[u]_1^{(n-1)}) \in \mathbb{A}_{n-1}.$$

Nach (4.17) gilt

$$0 = (f|_k\Phi)(\tilde{z}) = \sum_{\tilde{t} \in \mathbb{A}_{n-1}} a \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix} e_{n-1}(\tilde{t}\tilde{z}), \quad \tilde{z} \in \mathbb{H}_{n-1},$$

und daher $a(t[u]) = 0$. Mit Lemma 4.1.7 ergibt sich die gewünschte Aussage $a(t) = 0$.

(b) \Rightarrow (a): Gilt $a(t) = 0$ für alle $t \in \mathbb{A}_n \setminus \mathbb{A}_n^+$, so folgt auch $a \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix} = 0$ für alle $\tilde{t} \in \mathbb{A}_{n-1}$. Mit (4.17) ergibt sich

$$(f|\Phi)(\tilde{z}) = \sum_{\tilde{t} \in \mathbb{A}_{n-1}} a \begin{pmatrix} \tilde{t} & 0 \\ 0 & 0 \end{pmatrix} e_{n-1}(\tilde{t}\tilde{z}) = 0, \quad \tilde{z} \in \mathbb{H}_{n-1}.$$

Daraus schließen wir $f \in \text{Ker}(\Phi) = S_k(\Gamma_n)$. □

Eine weitere Charakterisierung von Siegelschen Spitzenformen besagt, dass sie exponentiell schnell gegen 0 konvergieren, wenn $\text{Im}(z)$ „wächst“ [35, S. 56]. Genauer gesagt beweisen wir

Lemma 4.5.4. [3, S. 79, 80], [4, S. 26], [28, S. 204, 205], [32, S. 58], [35, S. 56, 57]
 Seien $n \in \mathbb{N}$, $k \in \mathbb{Z}$, $y_0 \in \mathbb{P}_n$ und $f \in S_k(\Gamma_n)$. Dann gibt es $\alpha_1, \alpha_2 > 0$, sodass die Abschätzung

$$|f(z)| \leq \alpha_1 \cdot e^{-\alpha_2 \cdot \text{Spur}(y)}$$

für alle $z = x + iy \in \mathbb{H}_n$ mit $y \in \mathcal{M}_n$ und $y \geq y_0$ gilt. α_2 hängt dabei lediglich von n ab.

Beweis. Seien $t \in \mathbb{A}_n^+$ und $y \in \mathcal{M}_n$ mit $y \geq y_0$. Wir wollen $\text{Spur}(ty)$ auf zwei Arten nach unten abschätzen. Nach Bemerkung 2.1.13 gilt einerseits

$$\text{Spur}(ty) \geq \text{Spur}(ty_0). \tag{4.20}$$

Andererseits nutzen wir $y \in \mathcal{M}_n$ und Korollar 3.4.11 aus, um

$$\text{Spur}(ty) \geq \frac{1}{n^{n-1} \cdot c_n} \cdot \text{Spur}(t \cdot \text{diag}(y_{1,1}, \dots, y_{n,n})) = \frac{1}{n^{n-1} \cdot c_n} \cdot \sum_{\ell=1}^n t_{\ell,\ell} y_{\ell,\ell} \quad \text{zu schreiben.}$$

Für $t \in \mathbb{A}_n^+$ sind die Diagonalelemente $t_{\ell,\ell} = t[e_\ell] \in \mathbb{N}$. Deshalb erhalten wir sogar

$$\text{Spur}(ty) \geq \frac{1}{n^{n-1} \cdot c_n} \cdot \sum_{\ell=1}^n t_{\ell,\ell} y_{\ell,\ell} \geq \frac{1}{n^{n-1} \cdot c_n} \cdot \sum_{\ell=1}^n y_{\ell,\ell} = \frac{1}{n^{n-1} \cdot c_n} \cdot \text{Spur}(y). \tag{4.21}$$

Die Abschätzungen (4.20) und (4.21) ergeben zusammen

$$2 \cdot \text{Spur}(ty) = \text{Spur}(ty) + \text{Spur}(ty) \geq \text{Spur}(ty_0) + \frac{1}{n^{n-1} \cdot c_n} \cdot \text{Spur}(y).$$

Mit der Fourierreentwicklung aus Satz 4.5.3(c) folgt

$$|f(z)| \leq \sum_{t \in \mathbb{A}_n^+} |a(t) e_n(tz)| = \sum_{t \in \mathbb{A}_n^+} |a(t)| e^{-2\pi \cdot \text{Spur}(ty)} \leq e^{-\pi \cdot n^{1-n} \cdot c_n^{-1} \cdot \text{Spur}(y)} \cdot \sum_{t \in \mathbb{A}_n^+} |a(t)| e^{-\pi \cdot \text{Spur}(ty_0)}.$$

Da die Fourierreentwicklung von f in $i \cdot \frac{y_0}{2} \in \mathbb{H}_n$ absolut konvergiert, ist dabei

$$\sum_{t \in \mathbb{A}_n^+} |a(t)| e^{-\pi \cdot \text{Spur}(ty_0)} < \infty, \quad \text{woraus die Behauptung folgt.} \quad \square$$

Damit können wir ein wichtiges Verhalten der in Bemerkung 4.1.11 definierten Funktion g beweisen [16, S. 47], [28, S. 205], [32, S. 56 – 58], [40, S. 108]:

Lemma 4.5.5. *Seien $n \in \mathbb{N}$, $k \in \mathbb{Z}$ und $f \in S_k(\Gamma_n)$. Dann besitzt die in \mathbb{H}_n definierte Funktion*

$$g(z) = (\det(y))^{\frac{k}{2}} \cdot |f(z)|, \quad z = x + iy \in \mathbb{H}_n,$$

ein Maximum, das bereits in \mathcal{F}_n angenommen wird.

Beweis. Für $k \in -\mathbb{N}$ ist $g = 0$ wegen Satz 4.1.12, wofür die Behauptung trivial ist. Sei also $k \in \mathbb{N}_0$. Wegen Bemerkung 4.1.11 und Satz 3.5.9 reicht es zu zeigen, dass g in \mathcal{F}_n ein Maximum besitzt. Wir zeigen dazu

$$\lim_{\substack{z=x+iy \in \mathcal{F}_n \\ \det(y) \rightarrow \infty}} g(z) = 0, \quad (4.22)$$

denn dann ist das Maximum, das die stetige Funktion g auf dem Kompaktum (Korollar 3.6.7)

$$\mathcal{F}_n(c) = \{x + iy \in \mathcal{F}_n \mid \det(y) \leq c\} \quad \text{für } c > 0 \text{ groß genug}$$

annimmt, sogar das Maximum in \mathcal{F}_n und auch in \mathbb{H}_n .

Zum Beweis von (4.22) bemerken wir, dass \mathcal{F}_n eine Teilmenge von (4.3) ist (Satz 3.6.3). Mit der Ungleichung von Hadamard (Korollar 3.1.4) und Lemma 4.5.4 folgt dann

$$g(z) = (\det(y))^{\frac{k}{2}} \cdot |f(z)| \leq \alpha_1 \cdot \left(\prod_{\ell=1}^n y_{\ell,\ell} \right)^{\frac{k}{2}} \cdot e^{-\alpha_2 \cdot \text{Spur}(y)} = \alpha_1 \cdot \prod_{\ell=1}^n (y_{\ell,\ell})^{\frac{k}{2}} \cdot e^{-\alpha_2 \cdot y_{\ell,\ell}}$$

für alle $z = x + iy \in \mathcal{F}_n$. Falls $\det(y) \rightarrow \infty$ gilt, muss es wegen der Ungleichung von Hadamard (Korollar 3.1.4) ein $1 \leq j \leq n$ mit $y_{j,j} \rightarrow \infty$ geben. Aus $\lim_{y_{j,j} \rightarrow \infty} (y_{j,j})^{\frac{k}{2}} \cdot e^{-\alpha_2 \cdot y_{j,j}} = 0$ ergibt sich somit

$$0 \leq g(z) \leq \alpha_1 \cdot \prod_{\ell=1}^n (y_{\ell,\ell})^{\frac{k}{2}} \cdot e^{-\alpha_2 \cdot y_{\ell,\ell}} \xrightarrow{\det(y) \rightarrow \infty} 0, \quad z = x + iy \in \mathcal{F}_n,$$

also ist (4.22) bewiesen. \square

Als Anwendung untersuchen wir die Vektorräume $S_0(\Gamma_n)$ und $M_0(\Gamma_n)$ [16, S. 48], [32, S. 58], [37, S. 15].

Satz 4.5.6. *Für $n \in \mathbb{N}$ gilt $S_0(\Gamma_n) = \{0\}$.*

Beweis. Sei $f \in S_0(\Gamma_n)$. Nach Lemma 4.5.5 besitzt $g = |f|$ ein Maximum in \mathbb{H}_n . Da \mathbb{H}_n ein Gebiet ist (Lemma 2.2.12), liefert das Maximumprinzip, dass f konstant ist: Es gibt ein $c \in \mathbb{C}$, sodass $f(z) = c$ für alle $z \in \mathbb{H}_n$ gilt. Aus

$$0 = (f|\Phi)(\tilde{z}) = \lim_{\lambda \rightarrow \infty} f \begin{pmatrix} \tilde{z} & 0 \\ 0 & i\lambda \end{pmatrix} = c, \quad \tilde{z} \in \mathbb{H}_{n-1},$$

folgt die gewünschte Aussage $f = 0$. \square

Korollar 4.5.7. *Für $n \in \mathbb{N}_0$ gilt $M_0(\Gamma_n) = \mathbb{C}$.*

Beweis. Wir zeigen die Behauptung per Induktion über n . Für $n = 0$ ist $M_0(\Gamma_0) = \mathbb{C}$ nach (4.16). Sei also $n \geq 1$ und wir setzen $M_0(\Gamma_{n-1}) = \mathbb{C}$ voraus (Induktionsvoraussetzung). Betrachten wir $f \in M_0(\Gamma_n)$, so ergibt sich $f|\Phi \in M_0(\Gamma_{n-1}) = \mathbb{C}$. Daher gibt es ein $c \in \mathbb{C}$ mit $f|\Phi = c$, also $(f - c)|\Phi = f|\Phi - c = 0$. Dies bedeutet $f - c \in \text{Ker}(\Phi) = S_0(\Gamma_n) = \{0\}$, das heißt, f ist konstant. \square

4.6 Die Endlichdimensionalität von $M_k(\Gamma_n)$

Aus der Theorie der klassischen Modulformen wissen wir, dass eine Modulform bereits die Nullfunktion ist, wenn ausreichend viele Fourierkoeffizienten verschwinden [3, S. 91], [7, S. 342], [38, S. 175], [60, S. 31]:

Satz 4.6.1. *Sei $k \geq 4$ gerade, $d := \dim_{\mathbb{C}}(M_k(\Gamma_1))$ und $f(z) = \sum_{t=0}^{\infty} a(t)e^{2\pi itz} \in M_k(\Gamma_1)$. Wenn $a(t) = 0$ für alle $0 \leq t \leq d - 1$ gilt, dann ist f die Nullfunktion.*

Wir werden eine ähnliche Eigenschaft auch für Siegelische Spitzenformen beweisen, womit wir zeigen können, dass $S_k(\Gamma_n)$ und $M_k(\Gamma_n)$ als Vektorräume über \mathbb{C} endlichdimensional sind [3, S. 91].

Da $M_k(\Gamma_n)$ und $S_k(\Gamma_n)$ für nichtpositive Gewichte k bereits vollständig bestimmt sind (Sätze 4.1.12 und 4.5.6 sowie Korollar 4.5.7), können wir $k \in \mathbb{N}$ voraussetzen.

Lemma 4.6.2. [4, S. 31], [7, S. 124, 125], [16, S. 48], [32, S. 59, 60]
 Seien $\ell \in \mathbb{N}$ und $\delta > 0$. Sei

$$h(\zeta) = \sum_{r=\ell}^{\infty} b_r e^{2\pi i \zeta r}$$

eine Fourierreihe, die für alle $\zeta \in \mathbb{C}$ mit $\text{Im}(\zeta) > -\delta$ konvergiert. Dann existiert zu jedem $0 < \varepsilon < \delta$ ein Punkt $\zeta_\varepsilon \in \mathbb{C}$ mit den Eigenschaften

$$\text{Im}(\zeta_\varepsilon) = -\varepsilon \quad \text{und} \quad |h(0)| \leq e^{-2\pi\ell\varepsilon} \cdot |h(\zeta_\varepsilon)|.$$

Beweis. Sei $q := e^{2\pi i \zeta}$. Wir definieren die Funktion $\tilde{h}(q) := q^{-\ell} \cdot h(\zeta)$. Da $\text{Im}(\zeta) > -\delta$ gleichbedeutend mit $|q| = e^{-2\pi \text{Im}(\zeta)} < e^{2\pi\delta}$ ist, ist \tilde{h} für $|q| < e^{2\pi\delta}$ holomorph. Nach dem Maximumprinzip wird das Betragsmaximum von \tilde{h} , das die Funktion im Bereich $|q| \leq e^{2\pi\varepsilon}$ annimmt, auf dem Rand angenommen: Es gibt einen Punkt $\zeta_\varepsilon \in \mathbb{C}$ mit $|e^{2\pi i \zeta_\varepsilon}| = e^{2\pi\varepsilon}$, das heißt $\text{Im}(\zeta_\varepsilon) = -\varepsilon$, für den insbesondere $|\tilde{h}(1)| \leq |\tilde{h}(e^{2\pi i \zeta_\varepsilon})|$ gilt. Daraus erhalten wir

$$|h(0)| = |\tilde{h}(1)| \leq |\tilde{h}(e^{2\pi i \zeta_\varepsilon})| = |e^{-2\pi i \zeta_\varepsilon \ell}| \cdot |h(\zeta_\varepsilon)| = e^{-2\pi\ell\varepsilon} \cdot |h(\zeta_\varepsilon)|. \quad \square$$

Lemma 4.6.3. [5, S. 210], [32, S. 60], [62, S. 73]
 Seien $n, k \in \mathbb{N}$, $\beta > 0$ und $a \in M_n(\mathbb{R})$. Dann gilt

$$e^{\beta\varepsilon} \cdot \det(I_n - \varepsilon a)^k = 1 + (\beta - k \cdot \text{Spur}(a)) \cdot \varepsilon + \mathcal{O}(\varepsilon^2), \quad \varepsilon \downarrow 0.$$

Beweis. Das charakteristische Polynom von a kann dargestellt werden als

$$\det(a - \lambda I_n) = (-1)^n \cdot \lambda^n + (-1)^{n+1} \cdot \text{Spur}(a) \cdot \lambda^{n-1} + \dots$$

Für $\lambda := \varepsilon^{-1}$, $\varepsilon > 0$, ergibt eine Multiplikation mit $(-\varepsilon)^n$

$$\det(I_n - \varepsilon a) = (-\varepsilon)^n \cdot \det(a - \varepsilon^{-1} I_n) = 1 - \text{Spur}(a) \cdot \varepsilon + \mathcal{O}(\varepsilon^2), \quad \varepsilon \downarrow 0,$$

$$\text{und} \quad \det(I_n - \varepsilon a)^k = 1 - k \cdot \text{Spur}(a) \cdot \varepsilon + \mathcal{O}(\varepsilon^2), \quad \varepsilon \downarrow 0.$$

Durch Multiplikation mit $e^{\beta\varepsilon} = 1 + \beta\varepsilon + \mathcal{O}(\varepsilon^2)$, $\varepsilon \downarrow 0$, folgt schließlich die Behauptung. \square

Die beiden Lemmata 4.6.2 und 4.6.3 dienen uns dazu, eine entscheidende Ungleichung im folgenden Lemma herzuleiten [4, S. 31, 32], [7, S. 111], [16, S. 48 – 50], [24, S. 257 – 258], [35, S. 59, 60].

Lemma 4.6.4. *Seien $n, k \in \mathbb{N}$, $f \in S_k(\Gamma_n) \setminus \{0\}$ mit Fourierentwicklung*

$$f(z) = \sum_{t \in \mathbb{A}_n^+} a(t) e_n(tz), \quad z \in \mathbb{H}_n,$$

und sei $m \in M_n(\mathbb{Z})$ symmetrisch und positiv semidefinit. Sei $z_0 = x_0 + iy_0 \in \mathcal{F}_n$ eine Stelle, in der die Funktion

$$g(z) = (\det(y))^{\frac{k}{2}} \cdot |f(z)|, \quad z = x + iy \in \mathbb{H}_n,$$

ihr Maximum annimmt. Des Weiteren seien

$$b_r := \sum_{\substack{t \in \mathbb{A}_n^+ \\ \text{Spur}(tm)=r}} a(t) e_n(tz_0), \quad r \in \mathbb{N}_0,$$

definiert. Falls es ein $\ell \in \mathbb{N}$ mit $b_r = 0$ für alle $r \leq \ell - 1$ gibt, so gilt

$$k \cdot \text{Spur}(my_0^{-1}) \geq 4\pi\ell.$$

Beweis. Nach Lemma 4.5.5 existiert eine Stelle $z_0 = x_0 + iy_0 \in \mathcal{F}_n$, in der die Funktion g ihr Maximum annimmt. Für den Imaginärteil y_0 gilt nach Satz 3.6.3

$$y_0 \geq \frac{\sqrt{3}}{2 \cdot n^{n-1} \cdot c_n} \cdot I_n. \quad (4.23)$$

Für m erhalten wir mithilfe von Satz 2.1.6 ein $g \in \text{GL}_n(\mathbb{R})$, $g^T \cdot g = I_n$, und $\lambda_1, \dots, \lambda_n \geq 0$ mit $m[g] = \text{diag}(\lambda_1, \dots, \lambda_n)$. Wählen wir nun $\delta > 0$ derart, dass

$$\delta \cdot \max\{\lambda_1, \dots, \lambda_n\} < \frac{\sqrt{3}}{2 \cdot n^{n-1} \cdot c_n} \quad \text{gilt,}$$

$$\text{so folgt} \quad \frac{\sqrt{3}}{2 \cdot n^{n-1} \cdot c_n} \cdot I_n > \delta \cdot \text{diag}(\lambda_1, \dots, \lambda_n).$$

Durch Anwendung von $[g^{-1}]$ ergibt sich

$$\frac{\sqrt{3}}{2 \cdot n^{n-1} \cdot c_n} \cdot I_n > \delta m. \quad (4.24)$$

Die Formeln (4.23) und (4.24) liefern nun $y_0 > \delta m$.

Sei $\zeta \in \mathbb{C}$ mit $\text{Im}(\zeta) > -\delta$. Wegen

$$\text{Im}(z_0 + \zeta m) = y_0 + \text{Im}(\zeta) \cdot m \geq y_0 - \delta m > 0$$

gilt $z_0 + \zeta m \in \mathbb{H}_n$ und die Funktion $h(\zeta) := f(z_0 + \zeta m)$ ist in $\{\zeta \in \mathbb{C} \mid \text{Im}(\zeta) > -\delta\}$ holomorph. Da $\text{Spur}(tm) \in \mathbb{N}_0$ für alle $t \in \mathbb{A}_n^+$ nach Korollar 2.1.12 und Lemma 2.2.4(c) gilt, schreiben wir

$$\begin{aligned} h(\zeta) &= f(z_0 + \zeta m) \\ &= \sum_{t \in \mathbb{A}_n^+} a(t) e_n(tz_0 + \zeta tm) = \sum_{r=0}^{\infty} \left(\sum_{\substack{t \in \mathbb{A}_n^+ \\ \text{Spur}(tm)=r}} a(t) e_n(tz_0) \right) e^{2\pi i \zeta r} = \sum_{r=0}^{\infty} b_r e^{2\pi i \zeta r}. \end{aligned}$$

Wegen $b_r = 0$ für alle $r \leq \ell - 1$ existiert zu jedem $0 < \varepsilon < \delta$ ein Punkt $\zeta_\varepsilon \in \mathbb{C}$ mit $\text{Im}(\zeta_\varepsilon) = -\varepsilon$ und $|h(0)| \leq e^{-2\pi\ell\varepsilon} \cdot |h(\zeta_\varepsilon)|$ (Lemma 4.6.2).

Aus $y_0 > \delta m$ schließen wir $y_0 > \varepsilon m$ und $\det(y_0 - \varepsilon m) > 0$. Daraus ergibt sich

$$\begin{aligned} (\det(y_0 - \varepsilon m))^{\frac{k}{2}} \cdot |f(z_0)| &= (\det(y_0 - \varepsilon m))^{\frac{k}{2}} \cdot |h(0)| \\ &\leq e^{-2\pi\ell\varepsilon} \cdot (\det(y_0 - \varepsilon m))^{\frac{k}{2}} \cdot |h(\zeta_\varepsilon)| \\ &= e^{-2\pi\ell\varepsilon} \cdot (\det(y_0 + \text{Im}(\zeta_\varepsilon) \cdot m))^{\frac{k}{2}} \cdot |f(z_0 + \zeta_\varepsilon m)| \\ &= e^{-2\pi\ell\varepsilon} \cdot g(z_0 + \zeta_\varepsilon m) \\ &\leq e^{-2\pi\ell\varepsilon} \cdot g(z_0) \\ &= e^{-2\pi\ell\varepsilon} \cdot (\det(y_0))^{\frac{k}{2}} \cdot |f(z_0)|. \end{aligned}$$

Aus $f \neq 0$ folgt $g(z_0) \neq 0$ und $f(z_0) \neq 0$. Eine Division durch $|f(z_0)| > 0$ liefert daher

$$(\det(y_0 - \varepsilon m))^{\frac{k}{2}} \leq e^{-2\pi\ell\varepsilon} \cdot (\det(y_0))^{\frac{k}{2}}.$$

Durch Quadrieren und Umstellen erhalten wir daraus $e^{4\pi\ell\varepsilon} \cdot \det(I_n - \varepsilon m y_0^{-1})^k \leq 1$, also

$$e^{4\pi\ell\varepsilon} \cdot \det(I_n - \varepsilon m y_0^{-1})^k - 1 \leq 0. \quad (4.25)$$

Nach Lemma 4.6.3 hat die linke Seite von (4.25) die Form

$$(4\pi\ell - k \cdot \text{Spur}(m y_0^{-1})) \cdot \varepsilon + \mathcal{O}(\varepsilon^2), \quad \varepsilon \downarrow 0.$$

Division durch ε und anschließender Grenzübergang für $\varepsilon \downarrow 0$ ergeben schließlich

$$4\pi\ell - k \cdot \text{Spur}(m y_0^{-1}) \leq 0. \quad \square$$

Nach Satz 3.6.3 existiert $\sup_{x+iy \in \mathcal{F}_n} \text{Spur}(y^{-1})$ und wir beweisen nun einen auf Siegel [55] zurückgehenden Satz, der dem Satz 4.6.1 ähnelt [28, S. 205, 206], [55, S. 642].

Satz 4.6.5. [4, S. 31], [11, S. 286, 287], [16, S. 51], [28, S. 197, 206], [32, S. 59 – 61], [47, S. 189 – 194], [55, S. 642]

Seien $n, k \in \mathbb{N}$, $f \in S_k(\Gamma_n)$ mit Fourierentwicklung

$$f(z) = \sum_{t \in \mathbb{A}_n^+} a(t) e_n(tz), \quad z \in \mathbb{H}_n.$$

Falls $a(t) = 0$ für alle $t \in \mathbb{A}_n^+$ mit

$$\text{Spur}(t) \leq \frac{k}{4\pi} \cdot \sup_{x+iy \in \mathcal{F}_n} \text{Spur}(y^{-1})$$

gilt, dann ist f die Nullfunktion.

Beweis. Wir beweisen den Satz per Widerspruch und nehmen daher $f \neq 0$ an. Um Lemma 4.6.4 anzuwenden, setzen wir $m = I_n$ und definieren

$$\ell := \left\lfloor \frac{k}{4\pi} \cdot \sup_{x+iy \in \mathcal{F}_n} \text{Spur}(y^{-1}) \right\rfloor + 1,$$

das $b_r = 0$ für alle $r \leq \ell - 1$ erfüllt. Lemma 4.6.4 besagt $k \cdot \text{Spur}(y_0^{-1}) \geq 4\pi\ell$, woraus die Ungleichung

$$\begin{aligned} 4\pi\ell &\leq k \cdot \text{Spur}(y_0^{-1}) \leq 4\pi \cdot \frac{k}{4\pi} \cdot \sup_{x+iy \in \mathcal{F}_n} \text{Spur}(y^{-1}) \\ &< 4\pi \cdot \left(\left\lfloor \frac{k}{4\pi} \cdot \sup_{x+iy \in \mathcal{F}_n} \text{Spur}(y^{-1}) \right\rfloor + 1 \right) = 4\pi\ell \quad \text{folgt.} \end{aligned}$$

Diese Ungleichung stellt einen Widerspruch dar. □

Jedes $t \in \mathbb{A}_n^+$ erfüllt $\text{Spur}(t) \geq n$. Wenn also

$$\frac{k}{4\pi} \cdot \sup_{x+iy \in \mathcal{F}_n} \text{Spur}(y^{-1}) < n$$

gilt, dann erfüllt jedes $f \in S_k(\Gamma_n)$ die leeren Voraussetzungen des Satzes 4.6.5, womit $f = 0$ und $S_k(\Gamma_n) = \{0\}$ folgt [4, S. 16, 18, 34], [11, S. 286, 287], [47, S. 195, 196], [59, S. 11].

Diese Argumentation nutzen wir in den folgenden Beispielen aus.

Beispiel 4.6.6. [4, S. 16, 18, 34], [16, S. 50], [45, S. 83, 84], [47, S. 195, 196]

Sei $n = 1$. Nach Beispiel 3.6.4 haben wir $\sup_{x+iy \in \mathcal{F}_1} (y^{-1}) = \frac{2}{\sqrt{3}}$. Wenn wir $k \in \mathbb{N}$ derart wählen, dass

$$\frac{k}{4\pi} \cdot \frac{2}{\sqrt{3}} < 1 \tag{4.26}$$

gilt, dann erfüllt jedes $f \in S_k(\Gamma_1)$ die leeren Voraussetzungen des Satzes 4.6.5, woraus $f = 0$ folgt. Da (4.26) äquivalent zu $k \leq 10$ ist, folgt $S_k(\Gamma_1) = \{0\}$ für $k \in \{2, 4, 6, 8, 10\}$.

Sei jetzt $k = 12$. Dann ist $1 < \frac{12}{4\pi} \cdot \frac{2}{\sqrt{3}} < 2$. Falls also $f(z) = \sum_{t=1}^{\infty} a(t)e^{2\pi itz} \in S_{12}(\Gamma_1)$ die

Bedingung $a(1) = 0$ erfüllt, so muss $f = 0$ nach Satz 4.6.5 sein.

Dies nutzen wir aus, um $\dim_{\mathbb{C}}(S_{12}(\Gamma_1)) \leq 1$ zu zeigen: Im Fall $S_{12}(\Gamma_1) \neq \{0\}$ gibt es nämlich eine Spitzenform $f(z) = \sum_{t=1}^{\infty} a(t)e^{2\pi itz} \in S_{12}(\Gamma_1) \setminus \{0\}$, die $a(1) \neq 0$ erfüllt. Betrachten wir ein beliebiges $g(z) = \sum_{t=1}^{\infty} b(t)e^{2\pi itz} \in S_{12}(\Gamma_1)$, so wählen wir $\lambda \in \mathbb{C}$ derart, dass $b(1) = \lambda \cdot a(1)$ gilt. Dann ist $g - \lambda \cdot f \in S_{12}(\Gamma_1)$ eine Spitzenform, deren erster Fourierkoeffizient¹ $b(1) - \lambda \cdot a(1) = 0$ verschwindet. Daher muss $g - \lambda \cdot f = 0$ sein, das heißt $g = \lambda \cdot f$. Dies zeigt insgesamt $\dim_{\mathbb{C}}(S_{12}(\Gamma_1)) \leq 1$.

Bemerkung 4.6.7. [60, S. 10, 18, 19] Aus der Theorie der klassischen Modulformen ist schon $\Delta \in S_{12}(\Gamma_1) \setminus \{0\}$ bekannt, womit Beispiel 4.6.6 dann $S_{12}(\Gamma_1) = \mathbb{C} \cdot \Delta$ ergibt.

Beispiel 4.6.8. [3, S. 96], [16, S. 50], [45, S. 83, 84], [47, S. 195, 196]

Für $n = 2$ liefert Beispiel 3.6.5 die Abschätzung

$$\sup_{x+iy \in \mathcal{F}_2} \text{Spur}(y^{-1}) \leq \frac{16}{3\sqrt{3}}.$$

¹Gemeint ist der Fourierkoeffizient zu $t = 1$.

Wenn wir $k \in \mathbb{N}$ derart wählen, dass

$$\frac{k}{4\pi} \cdot \frac{16}{3\sqrt{3}} < 2 \quad (4.27)$$

gilt, dann erfüllt jedes $f \in S_k(\Gamma_2)$ die leeren Voraussetzungen des Satzes 4.6.5, woraus $f = 0$ folgt. Da (4.27) äquivalent zu $k \leq 8$ ist, folgt $S_k(\Gamma_2) = \{0\}$ für $1 \leq k \leq 8$.

Aus den Sätzen 4.6.5 und 3.6.3 folgt

Korollar 4.6.9. [4, S. 31], [11, S. 286, 287], [16, S. 51], [28, S. 197, 206], [32, S. 59 – 61], [47, S. 189 – 194], [55, S. 642]

Seien $n, k \in \mathbb{N}$, $f \in S_k(\Gamma_n)$ mit Fourierentwicklung

$$f(z) = \sum_{t \in \mathbb{A}_n^+} a(t) e_n(tz), \quad z \in \mathbb{H}_n.$$

Falls $a(t) = 0$ für alle $t \in \mathbb{A}_n^+$ mit

$$\text{Spur}(t) \leq \left\lfloor \frac{k \cdot n^n \cdot c_n}{2\sqrt{3} \cdot \pi} \right\rfloor$$

gilt, dann ist f die Nullfunktion. Dabei ist c_n die Konstante aus der Ungleichung von Minkowski (Satz 3.4.5).

Um mit Korollar 4.6.9 die Endlichdimensionalität von $S_k(\Gamma_n)$ über \mathbb{C} zu zeigen, benötigen wir

Lemma 4.6.10. [3, S. 68], [28, S. 208], [32, S. 59], [38, S. 265]

Für $n, r \in \mathbb{N}$ gilt

$$|\{t \in \mathbb{A}_n^+ \mid \text{Spur}(t) \leq r\}| \leq r^n \cdot (4r - 1)^{\frac{n(n-1)}{2}} < (4r - 1)^{\frac{n(n+1)}{2}}.$$

Beweis. Die zu $t \in \mathbb{A}_n^+$ gehörige quadratische Form $t[v]$, $v \in \mathbb{R}^n$, ist auch auf dem zweidimensionalen linearen Spann $\text{span}_{\mathbb{R}}\{e_i, e_j\}$, $1 \leq i, j \leq n$, $i \neq j$, positiv definit. Daher hat die Matrix

$$\begin{pmatrix} t[e_i] & e_i^T \cdot t \cdot e_j \\ e_j^T \cdot t \cdot e_i & t[e_j] \end{pmatrix} = \begin{pmatrix} t_{i,i} & t_{i,j} \\ t_{i,j} & t_{j,j} \end{pmatrix}$$

eine positive Determinante $t_{i,i}t_{j,j} - t_{i,j}^2 > 0$. Aus $t_{i,i} \leq \text{Spur}(t)$, $1 \leq i \leq n$, folgt

$$t_{i,j}^2 < t_{i,i}t_{j,j} \leq (\text{Spur}(t))^2 \quad \text{und} \quad |t_{i,j}| < \text{Spur}(t) \quad \text{für alle } 1 \leq i, j \leq n, i \neq j.$$

Ist nun $r \in \mathbb{N}$ mit $\text{Spur}(t) \leq r$ vorgegeben, so gibt es, da t halbganz ist, für jeden Diagonaleintrag höchstens r Möglichkeiten und für jeden anderen Eintrag höchstens $4r - 1$ Möglichkeiten. Insgesamt folgt daraus die Behauptung. \square

Satz 4.6.11. [13, S. 107], [16, S. 51], [28, S. 208], [31, S. 87], [32, S. 59 – 61], [35, S. 51], [62, S. 56, 59]

Seien $n, k \in \mathbb{N}$ und c_n die Konstante aus der Ungleichung von Minkowski (Satz 3.4.5). Mit der

Abkürzung $r_{n,k} := \left\lfloor \frac{k \cdot n^n \cdot c_n}{2\sqrt{3} \cdot \pi} \right\rfloor$ gilt

$$\dim_{\mathbb{C}}(S_k(\Gamma_n)) \leq d_{n,k} := |\{t \in \mathbb{A}_n^+ \mid \text{Spur}(t) \leq r_{n,k}\}| \leq \max \left\{ 0, (4r_{n,k} - 1)^{\frac{n(n+1)}{2}} \right\}. \quad (4.28)$$

Es gibt daher eine nur von n abhängige Konstante $\tilde{d}_n > 0$, sodass

$$\dim_{\mathbb{C}}(S_k(\Gamma_n)) < \tilde{d}_n \cdot k^{\frac{n(n+1)}{2}} \quad \text{gilt.}$$

Beweis. Für $d_{n,k} = 0$ liefert Korollar 4.6.9 $S_k(\Gamma_n) = \{0\}$, weshalb die Aussagen des Satzes in diesem Fall stimmen.

Ansonsten ist $d_{n,k} \in \mathbb{N}$ und es muss $r_{n,k} \in \mathbb{N}$ gelten. Daher ergibt sich die zweite Ungleichung von (4.28) aus Lemma 4.6.10. Um die erste Abschätzung von (4.28) zu beweisen, betrachten wir die Abbildung $\psi : S_k(\Gamma_n) \rightarrow \mathbb{C}^{d_{n,k}}$, die einer Siegelschen Spitzenform $f(z) = \sum_{t \in \mathbb{A}_n^+} a(t)e_n(tz)$, $z \in \mathbb{H}_n$, den Vektor mit Einträgen $a(t)$, $t \in \mathbb{A}_n^+$ mit $\text{Spur}(t) \leq r_{n,k}$, zuordnet. Diese ist eine lineare Abbildung, die nach Korollar 4.6.9 den Kern $\text{Ker}(\psi) = \{0\}$ besitzt und daher injektiv ist. Insbesondere ist $S_k(\Gamma_n)$ endlichdimensional und der Rangsatz liefert²

$$\dim_{\mathbb{C}}(S_k(\Gamma_n)) = \dim_{\mathbb{C}}(\text{Ker}(\psi)) + \dim_{\mathbb{C}}(\text{Bild}(\psi)) = \dim_{\mathbb{C}}(\text{Bild}(\psi)) \leq \dim_{\mathbb{C}}(\mathbb{C}^{d_{n,k}}) = d_{n,k}.$$

Damit gilt (4.28), woraus wir des Weiteren

$$\dim_{\mathbb{C}}(S_k(\Gamma_n)) \leq (4r_{n,k} - 1)^{\frac{n(n+1)}{2}} < (4r_{n,k})^{\frac{n(n+1)}{2}} \leq \tilde{d}_n \cdot k^{\frac{n(n+1)}{2}}$$

mit $\tilde{d}_n := \left(\frac{2 \cdot n^n \cdot c_n}{\sqrt{3} \cdot \pi}\right)^{\frac{n(n+1)}{2}}$ erhalten. □

Im Beweis von Satz 4.6.11 wurde der Rangsatz aus der linearen Algebra unter der üblichen Voraussetzung benutzt, dass der Vektorraum, der den Definitionsbereich der linearen Abbildung darstellt, *endlichdimensional* ist [31, S. 87], [62, S. 59].

Diese Voraussetzung ersetzen wir durch Bedingungen an Wertebereich und Kern, um die Endlichdimensionalität von $M_k(\Gamma_n)$ über \mathbb{C} beweisen zu können.

Satz 4.6.12. [31, S. 87], [62, S. 59] *Seien V und W zwei \mathbb{K} -Vektorräume mit endlichdimensionalem W und sei $\varphi : V \rightarrow W$ eine lineare Abbildung mit endlichdimensionalem $\text{Ker}(\varphi)$. Dann ist V endlichdimensional und es gilt*

$$\dim_{\mathbb{K}}(V) = \dim_{\mathbb{K}}(\text{Ker}(\varphi)) + \dim_{\mathbb{K}}(\text{Bild}(\varphi)).$$

Beweis. Mit W ist auch $\text{Bild}(\varphi)$ endlichdimensional mit $k := \dim_{\mathbb{K}}(\text{Bild}(\varphi)) \in \mathbb{N}_0$. Wir betrachten eine Basis $\{w_1, \dots, w_k\}$ von $\text{Bild}(\varphi)$. Für alle $1 \leq \ell \leq k$ gibt es per Definition ein $v_\ell \in V$ mit $\varphi(v_\ell) = w_\ell$. Mithilfe einer r -dimensionalen Basis $\{v_{k+1}, \dots, v_{k+r}\}$ von $\text{Ker}(\varphi)$ erhalten wir eine Menge $\{v_1, \dots, v_k, v_{k+1}, \dots, v_{k+r}\} \subset V$, von der wir zeigen, dass sie eine Basis von V darstellt. Zunächst zeigen wir, dass die Vektoren dieser Menge linear unabhängig sind: Aus

$$\lambda_1 v_1 + \dots + \lambda_{k+r} v_{k+r} = 0 \tag{4.29}$$

folgt unter Anwendung von φ und Beachtung von $v_{k+1}, \dots, v_{k+r} \in \text{Ker}(\varphi)$ zunächst $\lambda_1 w_1 + \dots + \lambda_k w_k = 0$. Da w_1, \dots, w_k linear unabhängig sind, folgt $\lambda_1 = \dots = \lambda_k = 0$. Also ergibt (4.29) jetzt $\lambda_{k+1} v_{k+1} + \dots + \lambda_{k+r} v_{k+r} = 0$, woraus $\lambda_{k+1} = \dots = \lambda_{k+r} = 0$ wegen der linearen Unabhängigkeit von v_{k+1}, \dots, v_{k+r} folgt. Daher sind v_1, \dots, v_{k+r} linear unabhängig.

Schließlich ist noch zu zeigen, dass sich jedes $v \in V$ als Linearkombination von v_1, \dots, v_{k+r} schreiben lässt: Zum Vektor $v \in V$ betrachten wir dessen Bild $\varphi(v)$ und stellen es dar als

$$\varphi(v) = \lambda_1 w_1 + \dots + \lambda_k w_k \quad \text{mit } \lambda_1, \dots, \lambda_k \in \mathbb{K}.$$

Dann ist

$$\varphi(v - \lambda_1 v_1 - \dots - \lambda_k v_k) = \varphi(v) - \lambda_1 w_1 - \dots - \lambda_k w_k = 0,$$

²Das Bild der linearen Abbildung ψ wird mit $\text{Bild}(\psi)$ bezeichnet.

also $v - \lambda_1 v_1 - \dots - \lambda_k v_k \in \text{Ker}(\varphi)$. Es gibt daher $\lambda_{k+1}, \dots, \lambda_{k+r} \in \mathbb{K}$ mit

$$v - \lambda_1 v_1 - \dots - \lambda_k v_k = \lambda_{k+1} v_{k+1} + \dots + \lambda_{k+r} v_{k+r}.$$

Damit ist $v = \lambda_1 v_1 + \dots + \lambda_k v_k + \lambda_{k+1} v_{k+1} + \dots + \lambda_{k+r} v_{k+r}$ als Linearkombination der v_1, \dots, v_{k+r} dargestellt.

Also ist V ein $(k+r)$ -dimensionaler Vektorraum mit Basis $\{v_1, \dots, v_{k+r}\}$, für den

$$\dim_{\mathbb{K}}(V) = k+r = \dim_{\mathbb{K}}(\text{Bild}(\varphi)) + \dim_{\mathbb{K}}(\text{Ker}(\varphi)) \quad \text{gilt.} \quad \square$$

Die Endlichdimensionalität von $M_k(\Gamma_n)$ über \mathbb{C} ergibt sich nun im

Satz 4.6.13. [16, S. 52], [29, S. 79], [32, S. 61], [35, S. 51], [37, S. 15], [47, S. 194]
 Seien $n \in \mathbb{N}_0$ und $k \in \mathbb{N}$. Dann gibt es eine nur von n abhängige Konstante $d_n^* > 0$, sodass

$$\dim_{\mathbb{C}}(M_k(\Gamma_n)) < d_n^* \cdot k^{\frac{n(n+1)}{2}} \quad \text{gilt.}$$

Beweis. Wir beweisen die Aussage per Induktion über n . Für $n=0$ ist $M_k(\Gamma_0) = \mathbb{C}$ und die Behauptung gilt mit jedem $d_0^* > 1$. Sei nun $n \geq 1$ und wir setzen voraus, dass die Aussage des Satzes bereits für $n-1$ gilt (Induktionsvoraussetzung). Insbesondere ist also $M_k(\Gamma_{n-1})$ endlichdimensional. Zum Beweis der Aussage für n betrachten wir den Siegelischen Operator

$$\begin{aligned} \Phi : M_k(\Gamma_n) &\longrightarrow M_k(\Gamma_{n-1}) \\ f &\longmapsto f|_{\Phi} \end{aligned}$$

aus Beispiel 4.4.6: Er ist eine lineare Abbildung, deren Wertebereich $M_k(\Gamma_{n-1})$ endlichdimensional ist und deren Kern $S_k(\Gamma_n)$ dies auch ist (Satz 4.6.11). Nach Satz 4.6.12 ist $M_k(\Gamma_n)$ endlichdimensional mit

$$\begin{aligned} \dim_{\mathbb{C}}(M_k(\Gamma_n)) &= \dim_{\mathbb{C}}(\text{Ker}(\Phi)) + \dim_{\mathbb{C}}(\text{Bild}(\Phi)) \leq \dim_{\mathbb{C}}(S_k(\Gamma_n)) + \dim_{\mathbb{C}}(M_k(\Gamma_{n-1})) \\ &< \tilde{d}_n \cdot k^{\frac{n(n+1)}{2}} + d_{n-1}^* \cdot k^{\frac{n(n-1)}{2}} \\ &< (\tilde{d}_n + d_{n-1}^*) \cdot k^{\frac{n(n+1)}{2}}. \quad \square \end{aligned}$$

4.7 Folgerungen

Aufgrund von Lemma 4.6.4 gelingt es uns auch, einige Vektorräume $S_k(\Gamma_n)$ und $M_k(\Gamma_n)$ explizit anzugeben.

Lemma 4.7.1. [16, S. 50] Seien $n, k \in \mathbb{N}$ und $S_k(\Gamma_n) \neq \{0\}$. Dann gilt

$$k \geq 2\sqrt{3} \cdot \left(\frac{3}{4}\right)^{n-1} \cdot \pi.$$

Beweis. Wir wählen ein $f \in S_k(\Gamma_n) \setminus \{0\}$ und wenden Lemma 4.6.4 an: Nach Bemerkung 3.2.1(a) wählen wir zunächst einen Vektor $g \in \mathbb{Z}^n \setminus \{0\}$ mit $y_0^{-1}[g] = \mu(y_0^{-1})$ und definieren die symmetrische und positiv semidefinite Matrix $m := g \cdot g^T \in M_n(\mathbb{Z})$. Für alle $t \in \mathbb{A}_n^+$ gilt

$$\text{Spur}(tm) = \text{Spur}(tg \cdot g^T) = \text{Spur}(g^T \cdot tg) = \text{Spur}(t[g]) = t[g].$$

Aus Lemma 2.2.4(d) folgt $\text{Spur}(tm) = t[g] \in \mathbb{N}$ für alle $t \in \mathbb{A}_n^+$, weshalb Lemma 4.6.4 mit $\ell = 1$ angewandt werden kann: Es gilt dann

$$k \cdot \text{Spur}(my_0^{-1}) \geq 4\pi. \quad (4.30)$$

Wir schätzen $\text{Spur}(my_0^{-1}) = y_0^{-1}[g] = \mu(y_0^{-1})$ mithilfe der Ungleichung von Hermite (Lemma 3.2.2) durch

$$\mu(y_0) \cdot \mu(y_0^{-1}) \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \cdot (\det(y_0))^{\frac{1}{n}} \cdot \left(\frac{4}{3}\right)^{\frac{n-1}{2}} \cdot (\det(y_0^{-1}))^{\frac{1}{n}} = \left(\frac{4}{3}\right)^{n-1} \quad \text{ab.}$$

Mit den Lemmata 3.4.1(b) und 3.6.1 gilt $\mu(y_0) = (y_0)_{1,1} \geq \frac{\sqrt{3}}{2}$, womit sich

$$\mu(y_0^{-1}) \leq \left(\frac{4}{3}\right)^{n-1} \cdot (\mu(y_0))^{-1} \leq \frac{2}{\sqrt{3}} \cdot \left(\frac{4}{3}\right)^{n-1} \quad \text{ergibt.}$$

Die Ungleichung (4.30) liefert nun

$$4\pi \leq k \cdot \text{Spur}(my_0^{-1}) = k \cdot \mu(y_0^{-1}) \leq \frac{2k}{\sqrt{3}} \cdot \left(\frac{4}{3}\right)^{n-1}. \quad \square$$

Vernachlässigen wir die Vektorräume der Siegelschen Modulformen, die bereits nach Korollar 4.1.9 trivial sind, so ergibt Lemma 4.7.1 das folgende

Korollar 4.7.2. [3, S. 96], [11, S. 286, 287], [16, S. 50], [29, S. 77], [59, S. 11]
Es gilt

$$S_k(\Gamma_n) = \{0\} \quad \text{für} \quad \begin{cases} n = 1 \text{ und } k \in \{2, 4, 6, 8, 10\}, \\ n = 2 \text{ und } 1 \leq k \leq 8, \\ n = 3 \text{ und } k \in \{2, 4, 6\}, \\ n = 4 \text{ und } 1 \leq k \leq 4, \\ n = 5 \text{ und } k = 2, \\ n = 6 \text{ und } k \in \{1, 2\}, \\ n = 8 \text{ und } k = 1. \end{cases}$$

Bemerkung 4.7.3. Hierbei ergeben sich die aus den Beispielen 4.6.6 und 4.6.8 bekannten Fälle $n = 1$ und $n = 2$ erneut.

Korollar 4.7.4. [3, S. 91], [4, S. 34], [11, S. 286, 287], [60, S. 10]
Es gilt

$$\dim_{\mathbb{C}}(M_k(\Gamma_1)) \leq 1 \quad \text{für } k \in \{2, 4, 6, 8, 10\}.$$

Beweis. Für $n = 1$ betrachten wir den Siegelschen Operator

$$\begin{aligned} \Phi : M_k(\Gamma_1) &\longrightarrow M_k(\Gamma_0) = \mathbb{C} \\ f &\longmapsto f|_{\Phi}, \end{aligned}$$

für den der Rangsatz

$$\dim_{\mathbb{C}}(M_k(\Gamma_1)) \leq \dim_{\mathbb{C}}(S_k(\Gamma_1)) + \dim_{\mathbb{C}}(\mathbb{C}) = 0 + 1 = 1 \quad \text{liefert.} \quad \square$$

Bemerkung 4.7.5. [11, S. 286, 287], [38, S. 173], [60, S. 10, 30]

- (a) Es gilt sogar $M_2(\Gamma_1) = \{0\}$.
- (b) Außerdem besteht die Gleichheit $\dim_{\mathbb{C}}(M_k(\Gamma_1)) = 1$ für $k \in \{4, 6, 8, 10\}$.

Setzen wir alle uns jetzt bekannten Bausteine zusammen, erhalten wir

Korollar 4.7.6. [3, S. 96], [11, S. 286, 287], [29, S. 77, 79], [47, S. 194]
Es gilt

$$\begin{aligned}
 M_k(\Gamma_2) &= \{0\} \text{ für } k \in \{1, 2, 3, 5, 7\}, \\
 \dim_{\mathbb{C}}(M_k(\Gamma_2)) &= 1 \text{ für } k \in \{4, 8\}, \\
 \dim_{\mathbb{C}}(M_6(\Gamma_2)) &\leq 1, \\
 M_2(\Gamma_3) &= \{0\}, \\
 \dim_{\mathbb{C}}(M_4(\Gamma_3)) &= 1, \\
 \dim_{\mathbb{C}}(M_6(\Gamma_3)) &\leq 1, \\
 M_k(\Gamma_4) &= \{0\} \text{ für } k \in \{1, 2, 3\}, \\
 \dim_{\mathbb{C}}(M_4(\Gamma_4)) &= 1, \\
 M_2(\Gamma_5) &= \{0\}, \\
 M_k(\Gamma_6) &= \{0\} \text{ für } k \in \{1, 2\}, \\
 M_1(\Gamma_8) &= \{0\}.
 \end{aligned}$$

Beweis. Der Rangsatze, angewandt auf den Siegelschen Operator

$$\begin{aligned}
 \Phi : M_k(\Gamma_n) &\longrightarrow M_k(\Gamma_{n-1}) \\
 f &\longmapsto f|\Phi,
 \end{aligned}$$

liefert

$$\dim_{\mathbb{C}}(M_k(\Gamma_n)) \leq \dim_{\mathbb{C}}(S_k(\Gamma_n)) + \dim_{\mathbb{C}}(M_k(\Gamma_{n-1})).$$

Daraus folgt für $n \in \mathbb{N}$ induktiv

$$\dim_{\mathbb{C}}(M_k(\Gamma_n)) \leq \left(\sum_{m=2}^n \dim_{\mathbb{C}}(S_k(\Gamma_m)) \right) + \dim_{\mathbb{C}}(M_k(\Gamma_1)). \quad (4.31)$$

Aus (4.31), den Korollaren 4.7.2, 4.7.4, Bemerkung 4.7.5(a), Beispiel 4.1.10 und Satz 4.2.5 erhalten wir dann die Behauptung. \square

Beispiel 4.7.7. [11, S. 286, 287], [29, S. 77, 79] Mit der in Lemma 4.2.6 definierten Matrix a_8 erhalten wir insbesondere

$$\begin{aligned}
 M_4(\Gamma_1) &= \mathbb{C} \cdot \vartheta_{a_8}, \\
 M_8(\Gamma_1) &= \mathbb{C} \cdot \vartheta_{a_8 \oplus a_8}, \\
 M_4(\Gamma_2) &= \mathbb{C} \cdot \vartheta_{a_8, 2}, \\
 M_8(\Gamma_2) &= \mathbb{C} \cdot \vartheta_{a_8 \oplus a_8, 2}, \\
 M_4(\Gamma_3) &= \mathbb{C} \cdot \vartheta_{a_8, 3}, \\
 M_4(\Gamma_4) &= \mathbb{C} \cdot \vartheta_{a_8, 4}.
 \end{aligned}$$

Literaturverzeichnis

- [1] Niels Henrik Abel. „Recherches sur les fonctions elliptiques“. In: *Journal für die reine und angewandte Mathematik* Heft 2 (1827). S. 101 – 181. Springer – Verlag. Abgerufen am 28.10.2022. URL: https://gdz.sub.uni-goettingen.de/download/pdf/PPN243919689_0002/LOG_0018.pdf.
- [2] Anatolij Nikolaevich Andrianov. „Euler products corresponding to Siegel modular forms of genus 2“. In: *Uspekhi Matematicheskikh Nauk* Heft 29 (1974). S. 43 – 110. Abgerufen am 31.10.2022. URL: https://www.mathnet.ru/php/getFT.phtml?jrnid=rm&paperid=4375&what=fullt&option_lang=eng.
- [3] Anatolij Nikolaevich Andrianov. *Quadratic forms and Hecke operators*. Springer – Verlag, 1987.
- [4] Anatolij Nikolaevich Andrianov. *Introduction to Siegel modular forms and Dirichlet series*. Springer – Verlag, 2009.
- [5] Christian Blatter. *Analysis I*. Dritte Auflage. Springer – Verlag, 1980.
- [6] Peter Bundschuh. *Einführung in die Zahlentheorie*. Zweite Auflage. Springer – Verlag, 1992.
- [7] Eberhard Freitag; Rolf Busam. *Funktionentheorie*. Zweite Auflage. Springer – Verlag, 1995.
- [8] Gottfried Curio. *$N = 2$ String-String Duality and Holomorphic couplings*. Humboldt – Universität zu Berlin, 1997. Abgerufen am 31.10.2022. URL: <https://arxiv.org/pdf/hep-th/9708009>.
- [9] William Duke. „On Codes and Siegel Modular Forms“. In: *International Mathematics Research Notices* Band 1993. Heft 5 (1993). S. 125 – 136. Abgerufen am 31.10.2022. URL: <https://www.math.ucla.edu/~wdduke/preprints/codes.pdf>.
- [10] Wolfgang Ebeling. *Lattices and Codes: A Course Partially Based on Lectures by Friedrich Hirzebruch*. Dritte Auflage. Springer – Verlag, 2013.
- [11] Martin Eichler. „Über die Anzahl der linear unabhängigen Siegelschen Modulformen von gegebenem Gewicht“. In: *Mathematische Annalen* Band 213 (1975). S. 281 – 291. Springer – Verlag. Abgerufen am 22.7.2022. URL: https://www.digizeitschriften.de/download/pdf/235181684_0213/log42.pdf.
- [12] Leonhard Euler. Brief an Goldbach, 4.5.1748. Abgerufen am 28.10.2022. URL: <http://eulerarchive.maa.org/correspondence/letters/000841.pdf>.
- [13] Gerd Fischer. *Lineare Algebra*. Zehnte Auflage. Vieweg – Verlag, 1995.
- [14] Otto Forster. *Analysis 1*. Neunte Auflage. Vieweg – Verlag, 2008.

- [15] Eberhard Freitag. „Siegel'sche Modulformen“. In: *Jahresbericht der Deutschen Mathematiker – Vereinigung* Band 79 (1977). S. 79 – 86. Teubner – Verlag. Abgerufen am 31.10.2022. URL: https://gdz.sub.uni-goettingen.de/download/pdf/PPN37721857X_0079/PPN37721857X_0079.pdf.
- [16] Eberhard Freitag. *Siegel'sche Modulformen*. Springer – Verlag, 1983.
- [17] Eberhard Freitag. *Singular Modular Forms and Theta Relations*. Springer – Verlag, 1991. Abgerufen am 16.9.2022. URL: <https://link.springer.com/content/pdf/10.1007/BFb0093829.pdf>.
- [18] Eberhard Freitag. *Funktionentheorie 2: Riemann'sche Flächen, Mehrere komplexe Variable, Abel'sche Funktionen, Höhere Modulformen*. Springer – Verlag, 2009. Abgerufen am 8.10.2022. URL: <https://link.springer.com/content/pdf/10.1007/978-3-540-87899-5.pdf>.
- [19] Eberhard Freitag. *Funktionentheorie 2: Riemann'sche Flächen, Mehrere komplexe Variable, Abel'sche Funktionen, Höhere Modulformen*. Springer – Verlag, 2014. Abgerufen am 8.10.2022. URL: <https://link.springer.com/content/pdf/10.1007/978-3-642-45307-6.pdf>.
- [20] Johann Carl Friedrich Gauß. „Zur Theorie der transscendenten Functionen gehörig“. In: *Johann Carl Friedrich Gauß. Werke* Band 3 (1866). S. 436 – 445. Königliche Gesellschaft der Wissenschaften zu Göttingen. Abgerufen am 28.10.2022. URL: https://archive.org/download/bub_gb_guYGAAAYAAJ/bub_gb_guYGAAAYAAJ.pdf.
- [21] Jan Hendrik Bruinier; Gerard van der Geer; Günter Harder; Don Zagier. *The 1 – 2 – 3 of Modular Forms*. Springer – Verlag, 2008.
- [22] Alexandru Ghitza. *An Elementary Introduction to Siegel Modular Forms*. McGill University, Montréal, 2004. Abgerufen am 31.10.2022. URL: https://aghitza.org/publications/An_elementary_introduction_to_Siegel_modular_forms.pdf.
- [23] Fritz Götzky. „Über eine zahlentheoretische Anwendung von Modulformen zweier Veränderlicher“. In: *Mathematische Annalen* Band 100 (1928). S. 411 – 437. Springer – Verlag. Abgerufen am 28.9.2022. URL: https://gdz.sub.uni-goettingen.de/download/pdf/PPN235181684_0100/LOG_0020.pdf.
- [24] Harro Heuser. *Lehrbuch der Analysis Teil 1*. 15. Auflage. Teubner – Verlag, 2003.
- [25] Michael Holz. *Repetitorium Algebra*. Dritte Auflage. Binomi – Verlag, 2010.
- [26] Jun-Ichi Igusa. „On Siegel Modular Forms of Genus Two“. In: *American Journal of Mathematics* Heft 84 (1962). S. 175 – 200. The Johns Hopkins University Press. Abgerufen am 31.10.2022. URL: <https://www.jstor.org/stable/2372812>.
- [27] Jun-Ichi Igusa. „On Siegel Modular Forms of Genus Two (II)“. In: *American Journal of Mathematics* Heft 86 (1964). S. 392 – 412. The Johns Hopkins University Press. Abgerufen am 31.10.2022. URL: <https://www.jstor.org/stable/2373172>.
- [28] Jun-Ichi Igusa. *Theta functions*. Springer – Verlag, 1972.
- [29] William Duke; Özlem Imamoglu. „Siegel modular forms of small weight“. In: *Mathematische Annalen* Band 310 (1998). S. 73 – 82. Springer – Verlag. Abgerufen am 28.7.2022. URL: <https://link.springer.com/content/pdf/10.1007/s002080050137.pdf>.

- [30] Carl Gustav Jacob Jacobi. *Fundamenta nova theoriae functionum ellipticarum*. Cambridge University Press, 1829. Abgerufen am 28.10.2022. URL: <https://www.cambridge.org/core/books/fundamenta-nova-theoriae-functionum-ellipticarum/B4C05290013C41B0CF8C69F14ADB313D>.
- [31] Klaus Jänich. *Lineare Algebra*. Neunte Auflage. Springer – Verlag, 2002.
- [32] Hendrik Kasten. *Siegel'sche Modulformen. Vorlesungsskript*. Universität Heidelberg, 2021. Abgerufen am 21.4.2022. URL: <https://www.mathi.uni-heidelberg.de/~kasten/files/Skripte/ss17siegel.pdf>.
- [33] Hendrik Kasten. *Siegel'sche Modulformen. Vorlesungsskript*. Universität Heidelberg, 2022. Abgerufen am 18.10.2022. URL: <https://www.mathi.uni-heidelberg.de/~kasten/files/Skripte/ss17siegel.pdf>.
- [34] Helmut Klingen. „Zur Struktur der Siegelschen Modulgruppe“. In: *Mathematische Zeitschrift* Heft 136 (1974). S. 169 – 178. Springer – Verlag. Abgerufen am 31.10.2022. URL: <https://link.springer.com/content/pdf/10.1007/BF01214351.pdf>.
- [35] Helmut Klingen. *Introductory lectures on Siegel modular forms*. Cambridge University Press, 1990. Abgerufen am 3.6.2022. URL: <https://www.cambridge.org/core/books/introductory-lectures-on-siegel-modular-forms/B20895BD1982A4D4BDD63BBC1D7C16C8>.
- [36] Max Koecher. „Zur Theorie der Modulformen n – ten Grades. I.“ In: *Mathematische Zeitschrift* Heft 59 (1954). S. 399 – 416. Springer – Verlag. Abgerufen am 22.7.2022. URL: https://gdz.sub.uni-goettingen.de/download/pdf/PPN266833020_0059/LOG_0038.pdf.
- [37] Winfried Kohlen. *A short course on Siegel modular forms. Lecture Notes*. Universität Heidelberg, 2007. Abgerufen am 21.4.2022. URL: <https://www.mathi.uni-heidelberg.de/~kohlen/siegel2.pdf>.
- [38] Max Koecher; Aloys Krieg. *Elliptische Funktionen und Modulformen*. Zweite Auflage. Springer – Verlag, 2007. Abgerufen am 16.7.2020. URL: <https://link.springer.com/content/pdf/10.1007/978-3-540-49325-9.pdf>.
- [39] Konrad Königsberger. *Analysis 2*. Vierte Auflage. Springer – Verlag, 2002.
- [40] Konrad Königsberger. *Analysis 1*. Sechste Auflage. Springer – Verlag, 2004.
- [41] Wolfgang Fischer; Ingo Lieb. *Funktionentheorie*. Fünfte Auflage. Vieweg – Verlag, 1988.
- [42] Falko Lorenz. *Lineare Algebra 1*. Zweite Auflage. BI – Wissenschaftsverlag, 1988.
- [43] Falko Lorenz. *Lineare Algebra 2*. Dritte Auflage. BI – Wissenschaftsverlag, 1992.
- [44] Hans Maaß. „Über die Darstellung der Modulformen n – ten Grades durch Poincarésche Reihen“. In: *Mathematische Annalen* Band 123 (1951). S. 125 – 151. Springer – Verlag. Abgerufen am 31.10.2022. URL: <https://www.mathi.uni-heidelberg.de/~freitag/maass/data/17/maass17.pdf>.
- [45] Hans Maaß. *Lectures on Siegel's Modular Functions. Notes by T.P. Srinivasan*. Tata Institute of Fundamental Research Bombay, 1954 – 1955. Abgerufen am 3.10.2022. URL: www.math.tifr.res.in/~publ/ln/tifr03.pdf.
- [46] Hans Maaß. „Zetafunktionen mit Größencharakteren und Kugelfunktionen“. In: *Mathematische Annalen* Band 134 (1957). S. 1 – 32. Springer – Verlag. Abgerufen am 21.10.2022. URL: <https://link.springer.com/content/pdf/10.1007/BF01342828.pdf>.

- [47] Hans Maaß. *Siegel's Modular Forms and Dirichlet Series: Course Given at the University of Maryland, 1969 – 1970*. Springer – Verlag, 1971. Abgerufen am 8.7.2022. URL: <https://link.springer.com/content/pdf/10.1007/BFb0058625.pdf>.
- [48] Hermann Minkowski. „Diskontinuitätsbereich für arithmetische Äquivalenz“. In: *Journal für die reine und angewandte Mathematik* Heft 129 (1905). S. 220 – 274. De Gruyter – Verlag. Abgerufen am 5.8.2022. URL: https://gdz.sub.uni-goettingen.de/download/pdf/PPN243919689_0129/LOG_0017.pdf.
- [49] David Mumford. *Tata Lectures on Theta I*. Birkhäuser – Verlag, 1983. Abgerufen am 22.10.2022. URL: https://www.dam.brown.edu/people/mumford/alg_geom/papers/Tata1.pdf.
- [50] Öystein Ore. *Number Theory and Its History*. McGraw – Hill Book Company, 1948.
- [51] Ameya Pitale. *Siegel Modular Forms*. Springer – Verlag, 2019. Abgerufen am 16.9.2022. URL: <https://link.springer.com/content/pdf/10.1007/978-3-030-15675-6.pdf>.
- [52] Andreas Herz; Martin Schalk. *Repetitorium Funktionentheorie*. Vieweg – Verlag, 1996.
- [53] Bruno Schoeneberg. „Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen“. In: *Mathematische Annalen* Band 116 (1939). S. 511 – 523. Springer – Verlag. Abgerufen am 16.8.2022. URL: https://gdz.sub.uni-goettingen.de/download/pdf/PPN235181684_0116/PPN235181684_0116.pdf.
- [54] Carl Ludwig Siegel. „Über die analytische Theorie der quadratischen Formen“. In: *Annals of Mathematics* Heft 36 (1935). S. 527 – 606. Princeton University. Abgerufen am 19.10.2022. URL: <https://www.jstor.org/stable/1968644>.
- [55] Carl Ludwig Siegel. „Einführung in die Theorie der Modulfunktionen n -ten Grades“. In: *Mathematische Annalen* Band 116 (1939). S. 617 – 657. Springer – Verlag. Abgerufen am 16.8.2022. URL: https://gdz.sub.uni-goettingen.de/download/pdf/PPN235181684_0116/PPN235181684_0116.pdf.
- [56] John Stillwell. *Mathematics and Its History*. Dritte Auflage. Springer – Verlag, 2010.
- [57] Steffen Timmann. *Repetitorium der Analysis, Teil 1*. Dritte Auflage. Binomi – Verlag, 2006.
- [58] Steffen Timmann. *Repetitorium der Funktionentheorie*. Binomi – Verlag, 2007.
- [59] Chris Poor; David S. Yuen. *Linear Dependence among Siegel Modular Forms*. Fordham University New York; Lake Forest College, 2000. Abgerufen am 26.6.2022. URL: <https://faculty.fordham.edu/poor/files/Semihull100.pdf>.
- [60] Sander Zwegers. *Modular Forms. Lecture Notes*. Universität zu Köln, 2021. Abgerufen am 19.9.2022. URL: https://www.ilias.uni-koeln.de/ilias/goto_uk_file_4022714_download.html.
- [61] Sander Zwegers. *Theta Functions. Lecture Notes*. Universität zu Köln, 2021. Abgerufen am 19.9.2022. URL: https://www.ilias.uni-koeln.de/ilias/goto_uk_file_3972575_download.html.
- [62] Sander Zwegers. *Lineare Algebra. Notizen zur Vorlesung*. Universität zu Köln, 2022. Stand 30.5.2022.

Eigenständigkeitserklärung

Hiermit versichere ich an Eides statt, dass ich die vorliegende Arbeit selbstständig und ohne die Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten und nicht veröffentlichten Schriften entnommen wurden, sind als solche kenntlich gemacht. Die Arbeit ist in gleicher oder ähnlicher Form oder auszugsweise im Rahmen einer anderen Prüfung noch nicht vorgelegt worden. Ich versichere, dass die eingereichte elektronische Fassung der eingereichten Druckfassung vollständig entspricht.

Köln, den 14. Dezember 2022

Titus Pavlovic