♠ The Kac–Wakimoto Conjecture

For any two natural numbers m and n, denote by $\Delta_m(n)$ the number of representations of n as a sum of m triangular numbers (numbers of the form $a(a-1)/2$ with a integral). Since $8a(a-1)/2+1 = (2a-1)^2$, this can also be written as the number $r_m^{\text{odd}}(8n+m)$ of representations of $8n+m$ as a sum of m odd squares. As part of an investigation in the theory of affine superalgebras, Kac and Wakimoto were led to conjecture the formula

$$\Delta_{4s^2}(n) \;=\; \sum_{\substack{r_1,\,a_1,\,\ldots,\,r_s,\,a_s\,\in\,\mathbb{N}_{\text{odd}} \\ r_1a_1+\cdots+r_sa_s\,=\,2n+s^2}} P_s(a_1,\ldots,a_s) \tag{35}$$

for m of the form $4s^2$ (and a similar formula for m of the form $4s(s+1)$), where $\mathbb{N}_{\text{odd}} = \{1,3,5,\ldots\}$ and P_s is the polynomial

$$P_s(a_1,\ldots,a_s) \;=\; \frac{\prod_i a_i \,\cdot\, \prod_{i<j}\bigl(a_i^2-a_j^2\bigr)^2}{4^{s(s-1)}\,s!\,\prod_{j=1}^{2s-1} j!}\,.$$

Two proofs of this were subsequently given, one by S. Milne using elliptic functions and one by myself using modular forms. Milne's proof is very ingenious, with a number of other interesting identities appearing along the way, but is quite involved. The modular proof is much simpler. One first notes that, P_s being a homogeneous polynomial of degree $2s^2-s$ and odd in each argument, the right-hand side of (35) is the coefficient of q^{2n+s^2} in a function $F(z)$ which is a linear combination of products $g_{h_1}(z)\cdots g_{h_s}(z)$ with $h_1+\cdots+h_s = s^2$, where $g_h(z) = \sum_{r,\,a\in\mathbb{N}_{\text{odd}}} a^{2h-1}q^{ra}$ $(h\ge 1)$. Since g_h is a modular form (Eisenstein series) of weight $2h$ on $\Gamma_0(4)$, this function F is a modular form of weight $2s^2$ on the same group. Moreover, its Fourier expansion belongs to $q^{s^2}\mathbb{Q}[[q^2]]$ (because $P_s(a_1,\ldots,a_s)$ vanishes if any two a_i are equal, and the smallest value of $r_1a_1+\cdots+r_sa_s$ with all r_i and a_i in $\mathbb{N}_{\text{odd}}$ and all a_i distinct is $1+3+\cdots+2s-1 = s^2$), and from the formula given in §1 for the number of zeros of a modular form we find that this property characterizes $F(z)$ uniquely in $M_{2s^2}(\Gamma_0(4))$ up to a scalar factor. But $\theta_F(z)^{4s^2}$ has the same property, so the two functions must be proportional. This proves (35) up to a scalar factor, easily determined by setting $n=0$. ♡

3.2 Theta Series in Many Variables

We now consider quadratic forms in an arbitrary number m of variables. Let $Q:\mathbb{Z}^m\to\mathbb{Z}$ be a positive definite quadratic form which takes integral values on $\mathbb{Z}^m$. We associate to Q the theta series

$$\Theta_Q(z) \;=\; \sum_{x_1,\ldots,x_m\in\mathbb{Z}} q^{Q(x_1,\ldots,x_m)} \;=\; \sum_{n=0}^{\infty} R_Q(n)\,q^n\,, \tag{36}$$

where of course $q = e^{2\pi iz}$ as usual and $R_Q(n) \in \mathbb{Z}_{\geq 0}$ denotes the number of representations of n by Q, i.e., the number of vectors $x \in \mathbb{Z}^m$ with $Q(x) = n$. The basic statement is that Θ_Q is always a modular form of weight $m/2$. In the case of even m we can be more precise about the modular transformation behavior, since then we are in the realm of modular forms of integral weight where we have given complete definitions of what modularity means. The quadratic form $Q(x)$ is a linear combination of products $x_i x_j$ with $1 \leq i, j \leq m$. Since $x_i x_j = x_j x_i$, we can write $Q(x)$ uniquely as

$$Q(x) \;=\; \frac{1}{2}\, x^t A x \;=\; \frac{1}{2} \sum_{i,j=1}^{m} a_{ij} x_i x_j \,, \tag{37}$$

where $A = (a_{ij})_{1 \leq i,j \leq m}$ is a symmetric $m \times m$ matrix and the factor $1/2$ has been inserted to avoid counting each term twice. The integrality of Q on $\mathbb{Z}^m$ is then equivalent to the statement that the symmetric matrix A has integral elements and that its diagonal elements a_{ii} are even. Such an A is called an *even integral matrix*. Since we want $Q(x) > 0$ for $x \neq 0$, the matrix A must be positive definite. This implies that $\det A > 0$. Hence A is non-singular and A^{-1} exists and belongs to $M_m(\mathbb{Q})$. The *level* of Q is then defined as the smallest positive integer $N = N_Q$ such that NA^{-1} is again an even integral matrix. We also have the *discriminant* $\Delta = \Delta_Q$ of A, defined as $(-1)^m \det A$. It is always congruent to 0 or 1 modulo 4, so there is an associated character (Kronecker symbol) χ_Δ, which is the unique Dirichlet character modulo N satisyfing $\chi_\Delta(p) = \left(\dfrac{\Delta}{p}\right)$ (Legendre symbol) for any odd prime $p \nmid N$. (The character χ_Δ in the special cases $\Delta = -4$, 12 and 8 already occurred in §2.2 (eq. (15)) and §3.1.) The precise description of the modular behavior of Θ_Q for $m \in 2\mathbb{Z}$ is then:

Theorem (Hecke, Schoenberg). *Let $Q : \mathbb{Z}^{2k} \to \mathbb{Z}$ be a positive definite integer-valued form in $2k$ variables of level N and discriminant Δ. Then Θ_Q is a modular form on $\Gamma_0(N)$ of weight k and character χ_Δ, i.e., we have $\Theta_Q\left(\frac{az+b}{cz+d}\right) = \chi_\Delta(a)\,(cz+d)^k\,\Theta_Q(z)$ for all $z \in \mathfrak{H}$ and $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.*

The proof, as in the unary case, relies essentially on the Poisson summation formula, which gives the identity $\Theta_Q(-1/Nz) = N^{k/2}(z/i)^k\,\Theta_{Q^*}(z)$, where $Q^*(x)$ is the quadratic form associated to NA^{-1}, but finding the precise modular behavior requires quite a lot of work. One can also in principle reduce the higher rank case to the one-variable case by using the fact that every quadratic form is diagonalizable over $\mathbb{Q}$, so that the sum in (36) can be broken up into finitely many sub-sums over sublattices or translated sublattices of $\mathbb{Z}^m$ on which $Q(x_1, \ldots, x_m)$ can be written as a linear combination of m squares.

There is another language for quadratic forms which is often more convenient, the language of lattices. From this point of view, a quadratic form is no longer a homogeneous quadratic polynomial in m variables, but a function Q

from a free $\mathbb{Z}$-module Λ of rank m to $\mathbb{Z}$ such that the associated scalar product $(x, y) = Q(x + y) - Q(x) - Q(y)$ (x, $y \in \Lambda$) is bilinear. Of course we can always choose a $\mathbb{Z}$-basis of Λ, in which case Λ is identified with $\mathbb{Z}^m$ and Q is described in terms of a symmetric matrix A as in (37), the scalar product being given by $(x, y) = x^t Ay$, but often the basis-free language is more convenient. In terms of the scalar product, we have a length function $\|x\|^2 = (x, x)$ (actually this is the square of the length, but one often says simply "length" for convenience) and $Q(x) = \frac{1}{2}\|x\|^2$, so that the integer-valued case we are considering corresponds to lattices in which all vectors have even length. One often chooses the lattice Λ inside the euclidean space $\mathbb{R}^m$ with its standard length function $(x, x) = \|x\|^2 = x_1^2 + \cdots + x_m^2$; in this case the square root of $\det A$ is equal to the volume of the quotient $\mathbb{R}^m/\Lambda$, i.e., to the volume of a fundamental domain for the action by translation of the lattice Λ on $\mathbb{R}^m$. In the case when this volume is 1, i.e., when $\Lambda \in \mathbb{R}^m$ has the same covolume as $\mathbb{Z}^m$, the lattice is called *unimodular*. Let us look at this case in more detail.

♠ Invariants of Even Unimodular Lattices

If the matrix A in (37) is even and unimodular, then the above theorem tells us that the theta series Θ_Q associated to Q is a modular form on the full modular group. This has many consequences.

Proposition 12. *Let $Q : \mathbb{Z}^m \to \mathbb{Z}$ be a positive definite even unimodular quadratic form in m variables. Then*

(i) the rank m is divisible by 8, and
(ii) the number of representations of $n \in \mathbb{N}$ by Q is given for large n by the formula

$$R_Q(n) \;=\; -\frac{2k}{B_k}\,\sigma_{k-1}(n) \;+\; O\big(n^{k/2}\big) \qquad (n \to \infty)\,, \tag{38}$$

where $m = 2k$ and B_k denotes the kth Bernoulli number.

Proof. For the first part it is enough to show that m cannot be an odd multiple of 4, since if m is either odd or twice an odd number then $4m$ or $2m$ is an odd multiple of 4 and we can apply this special case to the quadratic form $Q \oplus Q \oplus Q \oplus Q$ or $Q \oplus Q$, respectively. So we can assume that $m = 2k$ with k even and must show that k is divisible by 4 and that (38) holds. By the theorem above, the theta series Θ_Q is a modular form of weight k on the full modular group $\Gamma_1 = \mathrm{SL}(2, \mathbb{Z})$ (necessarily with trivial character, since there are no non-trivial Dirichlet characters modulo 1). By the results of Section 2, this modular form is a linear combination of $\mathbb{G}_k(z)$ and a cusp form of weight k, and from the Fourier expansion (13) we see that the coefficient of $\mathbb{G}_k$ in this decomposition equals $-2k/B_k$, since the constant term $R_Q(0)$ of Θ_Q equals 1. (The only vector of length 0 is the zero vector.) Now Proposition 8 implies the

Beweis. Wegen des Lemmas darf man umordnen. In c) verwende man zusätzlich Teil (v) des Äquivalenz–Satzes 1.1. □

Damit sind die Theta–Nullwerte $\Theta(\tau; S)$ Klasseninvarianten im Sinne von 1.4(5).

Für $S \in \mathrm{Pos}\,(n;\mathbb{R})$ und $T \in \mathrm{Pos}\,(m;\mathbb{R})$ definiert man die *direkte Summe* durch

$$S \oplus T := \begin{pmatrix} S & 0 \\ 0 & T \end{pmatrix} \in \mathrm{Pos}\,(n+m;\mathbb{R}). \tag{3}$$

Man schreibt $g = \binom{a}{b} \in \mathbb{Z}^{n+m}$ mit $a \in \mathbb{Z}^n$, $b \in \mathbb{Z}^m$ und erhält sofort

$$\Theta(\tau; S \oplus T) = \Theta(\tau; S) \cdot \Theta(\tau; T). \tag{4}$$

Ist $S \in \mathrm{Pos}\,(n;\mathbb{Z}) := \mathrm{Pos}\,(n;\mathbb{R}) \cap \mathrm{Mat}(n;\mathbb{Z})$, so gilt offenbar $S[g] \in \mathbb{Z}$ für alle $g \in \mathbb{Z}^n$. Die Definition impliziert damit

$$\Theta(\tau + 2; S) = \Theta(\tau; S)\ , \quad \tau \in \mathbb{H}. \tag{5}$$

Mit einer Umordnung erhält man die FOURIER–Entwicklung (vgl. **1.4**)

$$\Theta(\tau; S) = \sum_{m=0}^{\infty} \sharp(S, m) \cdot e^{\pi i m \tau}\ , \quad \tau \in \mathbb{H}, \tag{6}$$

wobei natürlich $\sharp(S, 0) = 1$.

2. Beziehungen zu Gittern. In diesem Abschnitt erläutern wir die zu **1** äquivalente Möglichkeit, Theta–Reihen mit Hilfe von Gittern einzuführen. Sei V ein reeller Vektorraum der Dimension $n < \infty$. Eine Teilmenge G von V heißt ein *Gitter in* V, wenn es linear unabhängige $g_1, \ldots, g_n \in V$ gibt mit

$$G = \mathbb{Z}g_1 + \ldots \mathbb{Z}g_n. \tag{1}$$

$g_1, \ldots, g_n$ nennt man eine *Basis des Gitters* G. Man vergleiche auch mit der Charakterisierung in Bemerkung I.1.3. Ist nun σ eine positiv definite Bilinearform auf V, d. h. (V, σ) ein euklidischer Vektorraum, so definiert man die *Theta–Reihe zum Gitter* G durch

$$\Theta_G(\tau) := \sum_{g \in G} e^{\pi i \tau \cdot \sigma(g,g)}\ , \quad \tau \in \mathbb{H}. \tag{2}$$

Lemma. *Sei (V, σ) ein euklidischer Vektorraum und $G = \mathbb{Z}g_1 + \ldots, +\mathbb{Z}g_n$ ein Gitter in V. Bezeichnet $S = (\sigma(g_\nu, g_\mu))$ die* GRAM*–Matrix zur Basis $g_1, \ldots, g_n$, so gilt*

$$\Theta_G(\tau) = \Theta(\tau; S) \quad \textit{für alle} \quad \tau \in \mathbb{H}.$$

Beweis. Für $g = \gamma_1 g_1 + \cdots + \gamma_n g_n \in G$ definiert man $h = (\gamma_1, \ldots, \gamma_n)^t \in \mathbb{Z}^n$ und erhält aus der Bilinearität von σ

$$\sigma(g, g) = S[h]. \qquad \square$$

Ist umgekehrt ein $S \in \mathrm{Pos}\,(n;\mathbb{R})$ gegeben, so betrachte man den $\mathbb{R}^n$ mit der durch S gegebenen, positiv definiten Bilinearform als euklidischen Vektorraum. Dann gilt

$$\Theta(\tau;S) = \Theta_{\mathbb{Z}^n}(\tau) \quad \text{für alle} \quad \tau \in \mathbb{H}.$$

Bemerkungen. Sei G ein Gitter mit der Basis (1). In Analogie zum Basis–Lemma I.1.6 kann man zeigen, dass $h_1, \ldots, h_n$ aus V genau dann eine Basis von G bilden, wenn es ein $U = (u_{\nu\mu}) \in GL(n;\mathbb{Z})$ gibt mit

$$h_\nu = \sum_{\mu=1}^{n} u_{\mu\nu} g_\mu \ , \ \nu = 1, \ldots, n.$$

Proposition 1c) besagt nun gerade die Unabhängigkeit von der Wahl der Basis im Lemma.

3. Die Theta–Transformationsformel. Als wesentliches Hilfsmittel zum Beweis der Transformationsformel benötigt man den

Satz von der FOURIER–Entwicklung. *Sei $\varphi : \mathbb{C}^n \to \mathbb{C}$ holomorph und in jeder Komponente periodisch mit der Periode 1, d. h.*

$$\varphi(w+g) = \varphi(w) \quad \textit{für alle} \quad g \in \mathbb{Z}^n.$$

Dann besitzt φ eine abolut und lokal gleichmäßig konvergente FOURIER*–Entwicklung der Form*

$$\varphi(w) = \sum_{h \in \mathbb{Z}^n} c_h \cdot e^{2\pi i h^t w}, \tag{1}$$

wobei die FOURIER*–Koeffizienten*

$$c_h := \int\limits_{[\![0,1]\!]^n} \varphi(z+\xi) \cdot e^{-2\pi i h^t (z+\xi)} d\xi \tag{2}$$

unabhängig von $z \in \mathbb{C}^n$ sind.

Beweis. Wir verwenden eine Induktion nach n, wobei der Fall $n = 1$ aufgrund der klassischen Theorie bekannt ist (vgl. R. REMMERT, G. SCHUMACHER [2002], 12.3.4). Sei also $n > 1$ und

$$w = \begin{pmatrix} w' \\ w_n \end{pmatrix}, \quad z = \begin{pmatrix} z' \\ z_n \end{pmatrix}, \quad \xi = \begin{pmatrix} \xi' \\ \xi_n \end{pmatrix}, \quad h = \begin{pmatrix} h' \\ h_n \end{pmatrix}.$$

Für festes $w_n \in \mathbb{C}$ ist $w' \mapsto \varphi(w)$ holomorph. Nach der Induktionsvoraussetzung existiert eine absolut konvergente FOURIER–Entwicklung

$$\begin{aligned} \varphi(w) &= \sum_{h' \in \mathbb{Z}^{n-1}} c_{h'}(w_n) \cdot e^{2\pi i h'^t w'}, \\ c_{h'}(w_n) &= \int\limits_{[\![0,1]\!]^{n-1}} \varphi\begin{pmatrix} z'+\xi' \\ w_n \end{pmatrix} \cdot e^{-2\pi i h'^t (z'+\xi')} d\xi'. \end{aligned}$$

Mit φ ist dann auch $c_{h'}$ holomorph (vgl. R. REMMERT [1995], 8.2.2) und periodisch mit der Periode 1. Aus der klassischen Theorie erhält man eine FOURIER–Entwicklung

$$\begin{aligned} c_{h'}(w_n) &= \sum_{h_n\in\mathbb{Z}} c_h \cdot e^{2\pi i h_n w_n}, \\ c_h &= \int\limits_{[\![0,1]\!]} c_{h'}(z_n+\xi_n)\cdot e^{-2\pi i h_n(z_n+\xi_n)} d\xi_n \\ &= \int\limits_{[\![0,1]\!]} \left(\int\limits_{[\![0,1]\!]^{n-1}} \varphi(z+\xi)\cdot e^{-2\pi i h^t(z+\xi)} d\xi' \right) d\xi_n. \end{aligned}$$

Da der Integrand stetig ist, erhält man (2) mit dem Satz von FUBINI (vgl. W. WALTER [1992; II], 9.18) und

$$\varphi(w) = \sum_{h'\in\mathbb{Z}^{n-1}} \left(\sum_{h_n\in\mathbb{Z}} c_h \cdot e^{2\pi i h^t w} \right).$$

Sei nun $R>0$ und

$$M := \max\{|\varphi(w)|\ ;\ |w_j| \le 2R+1, j=1,\dots,n\}.$$

Für $h\in\mathbb{Z}^n$ sei $z = -i2R(\operatorname{sgn} h_1,\dots,\operatorname{sgn} h_n)^t$, also

$$h^t z = -i2R(|h_1|+\ldots+|h_n|).$$

Mit diesem z folgt aus (2) für $|w_j|\le R$, $j=1,\dots,n$

$$\begin{aligned} &|c_h\cdot e^{2\pi i h^t w}| \le |c_h|\cdot e^{2\pi(|h_1 w_1|+\ldots+|h_n w_n|)} \\ &\le \int\limits_{[\![0,1]\!]^n} M\cdot e^{-4\pi R(|h_1|+\ldots+|h_n|)} d\xi \cdot e^{2\pi R(|h_1|+\ldots+|h_n|)} \\ &= M\cdot e^{-2\pi R(|h_1|+\ldots+|h_n|)}. \end{aligned}$$

Daraus ergibt sich sofort die absolute und lokal gleichmäßige Konvergenz der Reihe (1), denn man hat

$$\sum_{h\in\mathbb{Z}^n} e^{-2\pi R(|h_1|+\ldots+|h_n|)} = \left(\frac{1+e^{-2\pi R}}{1-e^{-2\pi R}}\right)^n. \qquad \square$$

Damit kommen wir zu der angekündigten

Theta–Transformationsformel. *Für $S\in \operatorname{Pos}(n;\mathbb{R})$, $p,q\in\mathbb{C}^n$ und $\tau\in\mathbb{H}$ gilt*

$$\Theta_{-q,p}(-1/\tau; S^{-1}) = (\tau/i)^{n/2} \cdot \sqrt{\det S} \cdot e^{-2\pi i p^t q} \cdot \Theta_{p,q}(\tau; S). \tag{3}$$

Dabei ist für ungerades n der Zweig der Wurzel zu wählen, der für positive Argumente positiv ist.

Beweis. Aufgrund von Proposition 1 und Lemma 1 können wir den Satz anwenden auf

$$\varphi(p) := \Theta_{p,q}(iy; S).$$

Wegen der absoluten Konvergenz des Integrals erhält man für $h \in \mathbb{Z}^n$

$$\begin{aligned} c_h &= \int\limits_{[\![0,1]\!]^n} \sum_{g\in\mathbb{Z}^n} e^{-\pi y S[g+p]+2\pi i(g+p)^t q} \cdot e^{-2\pi i h^t p} dp \\ &= \sum_{g\in\mathbb{Z}^n} \int\limits_{[\![0,1]\!]^n} e^{-\pi y S[g+p]+2\pi i(g+p)^t (q-h)} dp \\ &= \int\limits_{\mathbb{R}^n} e^{-\pi y S[p]+2\pi i p^t (q-h)} dp \\ &= e^{-\pi (yS)^{-1}[h-q]} \int\limits_{\mathbb{R}^n} e^{-\pi y S[p+i(yS)^{-1}(h-q)]} dp. \end{aligned}$$

Man wählt nach dem Äquivalenz–Satz 1.3 ein $W \in GL(n;\mathbb{R})$ mit $yS[W] = E$ und substitutiert $p = Wu$, also $dp = |\det W| du = y^{-n/2} (\det S)^{-1/2} du$. Mit $W^t(h-q) = v$ ergibt sich

$$\int\limits_{\mathbb{R}^n} e^{-\pi y S[p+i(yS)^{-1}(h-q)]} dp = |\det W| \cdot \int\limits_{\mathbb{R}^n} e^{-\pi (u+iv)^t (u+iv)} du$$

$$= y^{-n/2} \cdot (\det S)^{-1/2} \cdot \prod_{j=1}^{n} \int\limits_{-\infty}^{\infty} e^{-\pi (u_j+iv_j)^2} du_j.$$

Mit Hilfe des Residuensatzes erkennt man, dass hier jedes einzelne Integral gleich 1 ist (vgl. R. Remmert, G. Schumacher [2002], 12.4.3). Damit erhält man

$$y^{n/2} \cdot \sqrt{\det S} \cdot \Theta_{p,q}(iy; S) = \sum_{h\in\mathbb{Z}^n} e^{-\pi (yS)^{-1}[h-q]} \cdot e^{2\pi i h^t p} = e^{2\pi i q^t p} \cdot \Theta_{-q,p}(i/y; S^{-1}).$$

Also gilt (3) für alle $\tau = iy$, $y > 0$. Weil beide Seiten von (3) holomorph in $\tau \in \mathbb{H}$ sind, folgt die Behauptung mit dem Identitätssatz. □

Den Spezialfall der Theta–Nullwerte, also $p = q = 0$, notieren wir als

Korollar A. *Für $S \in \mathrm{Pos}\,(n;\mathbb{R})$ und $\tau \in \mathbb{H}$ gilt*

$$\Theta(-1/\tau; S^{-1}) = (\tau/i)^{n/2} \cdot \sqrt{\det S} \cdot \Theta(\tau; S).$$

Einen weiteren wichtigen Spezialfall formulieren wir in

Korollar B. *Ist* $S \in \mathrm{Pos}\,(n;\mathbb{Z})$ *mit* $\det S = 1$, *so gilt*

$$\Theta\,(-1/\tau;S) = (\tau/i)^{n/2} \cdot \Theta(\tau;S) \quad \textit{für alle } \tau \in \mathbb{H}.$$

Beweis. Es gilt $S^{-1}[S] = S$ mit $S \in GL(n;\mathbb{Z})$. Nun verwendet man Korollar A und Proposition 1c). □

Bemerkungen. a) Sei G von der Form 2(1) ein Gitter in dem euklidischen Vektorraum (V,σ). Bis auf Normierung des Maßes ist das Volumen einer Fundamentalmasche

$$\{\gamma_1 g_1 + \ldots + \gamma_n g_n\ ;\ 0 \le \gamma_\nu \le 1\ ,\ 1 \le \nu \le n\}$$

von G gleich $\sqrt{\det S}$, wobei S die zugehörige GRAM–Matrix ist. Wir verwenden dafür die Abkürzung $\mathrm{vol}(G)$. Die Menge

$$G^\sigma := \{v \in V\ ;\ \sigma(v,g) \in \mathbb{Z} \ \text{ für alle } \ g \in G\}$$

ist wiederum ein Gitter, das zu G *duale Gitter* (bezüglich σ). Wählt man $h_1, \ldots h_n \in V$ mit $\sigma(h_i, g_j) = \delta_{ij}$, so ist $h_1, \ldots, h_n$ eine Basis von G^σ und S^{-1} die zugehörige GRAM–Matrix. Damit kann man Korollar A auch äquivalent formulieren als

$$\Theta_{G^\sigma}\,(-1/\tau) = (\tau/i)^{n/2} \cdot \mathrm{vol}(G) \cdot \Theta_G(\tau).$$

Im Fall $G = G^\sigma$ nennen wir G *selbstdual* und haben dann auch $\mathrm{vol}(G) = 1$.
b) In der Bezeichnung E(2) gilt $\Theta_{p,q}(\tau;S) = \vartheta(\tau S, p, q)$. Damit wird (3) zu einem Spezialfall von E(3). Andererseits hat man E(3) für alle $Z = iS$, $S \in \mathrm{Pos}\,(n;\mathbb{R})$, in (3) bewiesen, so dass die Aussage mit dem Identitätssatz für Z folgt.

4. Gerade Matrizen. Eine Matrix $S \in \mathrm{Sym}\,(n;\mathbb{R})$ heißt *gerade*, wenn

$$S[g] = g^t S g \in 2\mathbb{Z} \quad \text{für alle} \quad g \in \mathbb{Z}^n. \tag{1}$$

Eine Charakterisierung gibt das

Lemma. *Für eine Matrix* $S = (s_{\nu\mu}) \in \mathrm{Sym}\,(n;\mathbb{R})$ *sind äquivalent:*

(i) S *ist gerade.*

(ii) $s_{\nu\nu} \in 2\mathbb{Z}$ *für* $\nu = 1, \ldots, n$ *und* $s_{\nu\mu} \in \mathbb{Z}$ *für alle* $\nu \neq \mu$.

(iii) $\mathrm{Sp}(ST) \in 2\mathbb{Z}$ *für alle* $T \in \mathrm{Sym}\,(n;\mathbb{Z})$.

Beweis. (i) $\Longrightarrow$ (ii): Wählt man für g den ν–ten Einheitsvektor e_ν in (1), so ergibt sich $s_{\nu\nu} \in 2\mathbb{Z}$. Für $\nu \neq \mu$ folgt dann aus

$$S[e_\nu + e_\mu] = s_{\nu\nu} + s_{\mu\mu} + 2s_{\nu\mu} \in 2\mathbb{Z}$$

sofort $s_{\nu\mu} \in \mathbb{Z}$.
(ii) $\Longrightarrow$ (iii): Schreibt man $T = (t_{\nu\mu})$, so berechnet man

$$\mathrm{Sp}(ST) = \sum_{1\le\nu\le n} s_{\nu\nu}t_{\nu\nu} + 2\sum_{1\le\nu<\mu\le n} s_{\nu\mu}t_{\nu\mu} \in 2\mathbb{Z}.$$

(iii) $\Longrightarrow$ (i): Ist $g \in \mathbb{Z}^n$, so folgt $T = gg^t \in \mathrm{Sym}\,(n;\mathbb{Z})$ und es gilt

$$\mathrm{Sp}(ST) = S[g]. \qquad \square$$

Insbesondere folgert man sofort

$$(2) \qquad S \text{ gerade, } G \in \mathrm{Mat}(n,m;\mathbb{Z}) \quad \Longrightarrow \quad S[G] \text{ gerade.}$$

Nun betrachten wir Theta–Reihen zu geraden, positiv definiten Matrizen. Als unmittelbare Folgerung aus (1) und 1(6) notieren wir die

Proposition. *Sei $S \in \mathrm{Pos}\,(n;\mathbb{Z})$ gerade. Dann gilt:*

$$\Theta(\tau+1;S) = \Theta(\tau;S) \quad \textit{für alle} \quad \tau \in \mathbb{H}.$$

$\Theta(\cdot;S)$ *besitzt die* FOURIER*–Entwicklung*

$$\Theta(\tau;S) = \sum_{m=0}^{\infty} \sharp(S,2m)\cdot e^{2\pi i m\tau}\ , \quad \tau \in \mathbb{H}.$$

5. Gerade, unimodulare, positiv definite Matrizen. In diesem Abschnitt beschreiben wir notwendige und hinreichende Bedingungen an das Format für die Existenz solcher Matrizen. Diese erhält man mit Hilfe der zugehörigen Theta–Reihen.

Satz. *Ist $S \in \mathrm{Pos}\,(n;\mathbb{Z})$ gerade und unimodular, dann ist n durch 8 teilbar.*

Beweis. Für $\tau \in \mathbb{H}$ definiert man

$$\tau_1 = -\frac{1}{\tau}\ , \quad \tau_2 = \tau_1 + 1 = \frac{\tau-1}{\tau}\ , \quad \tau_3 = -\frac{1}{\tau_2} = \frac{\tau}{1-\tau}\ ,$$
$$\tau_4 = \tau_3 + 1 = \frac{1}{1-\tau}\ , \quad \tau_5 = -\frac{1}{\tau_4} = \tau - 1\ , \quad \tau_6 = \tau_5 + 1 = \tau.$$

Nun wendet man Proposition 4 und Korollar 3B an und erhält

$$\Theta(\tau;S) = \Theta(\tau_6;S) = (\tau/i)^{n/2}\cdot(\tau_2/i)^{n/2}\cdot(\tau_4/i)^{n/2}\cdot\Theta(\tau;S).$$

Wählt man nun $\tau = i$ und benutzt die Tatsache, dass $\Theta(i;S)$ eine positive reelle Zahl ist, so folgt

$$1 = (1+i)^{n/2}\left(\frac{1+i}{2}\right)^{n/2} = e^{\pi i n/4},$$

wenn man berücksichtigt, dass man den Zweig der Wurzel zu wählen hat, der für positive Argumente positiv ist. Folglich ist n durch 8 teilbar. $\square$

Für $n = 8$ geben wir nun ein Beispiel an.