

Kapitel VI.

Hecke-Theorie

In der Theorie der Modulformen spielen bestimmte Endomorphismen, die so genannten Hecke-Operatoren, eine zentrale Rolle. Die zugehörige Theorie wird in diesem Kapitel beschrieben.

§1. Der abstrakte Hecke-Ring

In diesem Paragraphen beschreiben wir die abstrakte Struktur von Hecke-Ringen.

Ist U eine Untergruppe von G und $g \in G$, so nennt man

$$\begin{aligned} Ug &= \{ug; u \in U\} && \text{die Rechtsnebenklasse von } g, \\ gU &= \{gu; u \in U\} && \text{die Linksnebenklasse von } g, \\ UgU &= \{ugv; u, v \in U\} && \text{die Doppelnebenklasse von } g \end{aligned}$$

bezüglich U . Wir wiederholen aus der (Linearen) Algebra für $g, h \in G$ die Äquivalenz der Aussagen

- (i) $Ug = Uh$.
- (ii) $Ug \cap Uh \neq \emptyset$.
- (iii) Es gibt ein $u \in U$ mit $ug = h$.

Analog erhält man für $g, h \in G$ die Äquivalenz der Aussagen

- (i) $UgU = UhU$.
- (ii) $UgU \cap UhU \neq \emptyset$.
- (iii) Es gibt $u, v \in U$ mit $ugv = h$.

Offenbar können durch Links-, Rechts- und Doppelnebenklassen Äquivalenzrelationen auf G definiert werden. Es bedeutet

$$g: U \backslash G, \quad g: G/U, \quad g: U \backslash G/U,$$

dass g ein Vertretersystem der Rechts-, bzw. Links-, bzw. Doppelnebenklassen bezüglich U in G durchläuft.

Sei $\mathcal{R}(U, G)$ der $\mathbb{Z}$ -Modul mit den Rechtsnebenklassen Ug , $g \in G$, als Basis. Er besteht aus den formalen Linearkombinationen

$$(1) \quad R = \sum_{g: U \backslash G} r(Ug)Ug$$

mit $r(Ug) \in \mathbb{Z}$ und $r(Ug) \neq 0$ nur für endlich viele Rechtsnebenklassen Ug , $g \in G$. Ist

$$S = \sum_{g: U \backslash G} s(Ug)Ug \in \mathcal{R}(U, G)$$

und $\gamma \in \mathbb{Z}$, so hat man

$$\begin{aligned} R = S &\Leftrightarrow r(Ug) = s(Ug) \quad \text{für alle } g \in G, \\ R + S &= \sum_{g: U \backslash G} (r(Ug) + s(Ug))Ug \in \mathcal{R}(U, G), \\ \gamma \cdot R &= \sum_{g: U \backslash G} (\gamma r(Ug))Ug \in \mathcal{R}(U, G). \end{aligned}$$

Darüber hinaus definiert man die Linearform

$$\text{ind}: \mathcal{R}(U, G) \rightarrow \mathbb{Z}, \quad R \mapsto \sum_{g: U \backslash G} r(Ug).$$

G operiert auf $\mathcal{R}(U, G)$ durch Rechtsmultiplikation, d. h. für $h \in G$

$$r_h: \mathcal{R}(U, G) \rightarrow \mathcal{R}(U, G), \quad r_h(R) := \sum_{g: U \backslash G} r(Ug)Ugh.$$

Damit erhalten wir den Untermodul

$$\mathcal{R}(U, G)^U := \{R \in \mathcal{R}(U, G); r_u(R) = R \text{ für alle } u \in U\},$$

der dadurch charakterisiert wird, dass

$$r(Ugu) = r(Ug) \quad \text{für alle } g \in G, u \in U.$$

In völlig analoger Weise definieren wir den freien $\mathbb{Z}$ -Modul $\mathcal{H}(U, G)$ der Doppelnebenklassen in G bezüglich U . Er besteht aus allen formalen Linearkombinationen

$$T = \sum_{g: U \backslash G/U} t(UgU)UgU,$$

wobei $t(UgU) \in \mathbb{Z}$ und $t(UgU) \neq 0$ nur für endlich viele Doppelnebenklassen UgU , $g \in G$. Ist

$$\bar{T} = \sum_{g: UgU} \bar{t}(UgU) UgU \in \mathcal{H}(U, G)$$

so bedeutet die Definition für $\gamma \in \mathbb{Z}$

$$\begin{aligned} T = \bar{T} &\Leftrightarrow t(UgU) = \bar{t}(UgU) \text{ für alle } g \in G, \\ T + \bar{T} &= \sum_{g: UgU} (t(UgU) + \bar{t}(UgU)) UgU, \\ \gamma \cdot T &= \sum_{g: UgU} (\gamma t(UgU)) UgU. \end{aligned}$$

Ist U ein Normalteiler in G , so hat man

$$UgU = Ug = gU \text{ für alle } g \in G,$$

also

$$\mathcal{R}(U, G) = \mathcal{R}(U, G)^U = \mathcal{H}(U, G) = \mathbb{Z}[G/U],$$

wobei der letzte Ausdruck für den Gruppenring von G/U steht.

Wir wollen nun einen Zusammenhang zwischen diesen Moduln formaler Linearkombinationen herstellen. Dazu benötigen wir eine Übersicht über die Zerlegung von Doppelnebenklassen in Rechts- und Linksnebenklassen.

(1.1) Lemma. Sei U eine Untergruppe von G und $g \in G$. Dann gilt

- (i)
$$UgU = \dot{\bigcup}_{u: (U \cap g^{-1}Ug) \setminus U} Ug u = \dot{\bigcup}_{u: U/(U \cap gUg^{-1})} u g U,$$
- (ii)
$$\#(U \setminus UgU) = [U: U \cap g^{-1}Ug], \quad \#(UgU/U) = [U: U \cap gUg^{-1}].$$

Beweis. Sei $\bar{U} := U \cap g^{-1}Ug$. Wir zeigen

$$UgU = \dot{\bigcup}_{u: \bar{U} \setminus U} Ug u.$$

Wegen $g\bar{u}g^{-1} \in U$ für $\bar{u} \in \bar{U}$ ist die rechte Seite unabhängig von der Wahl der Vertreter. Offenbar ist die rechte Seite in UgU enthalten. Sei nun $\bar{g} = u_1 g u_2 \in UgU$, $u_1, u_2 \in U$. Dann gehört u_2 zu einer Rechtsnebenklasse $\bar{U}u$, also $u_2 = \bar{u}u$ für ein $\bar{u} \in \bar{U}$. Es folgt

$$\bar{g} = u_1 g \bar{u} u = u_1 (g \bar{u} g^{-1}) g u \in Ug u,$$

also die Gleichheit.

Seien nun $Ugu = Ug v$ für $u, v \in U$, also $u_1 g u = g v$ für ein $u_1 \in U$. Dann gilt

$$g^{-1} u_1 g = v u^{-1} \in g^{-1} U g \cap U = \overline{U}$$

und damit $\overline{U} u = \overline{U} v$, so dass die Vereinigung disjunkt ist.

Die zweite Gleichung beweist man analog.

(ii) ist eine direkte Folgerung von (i). □

Wir kommen zur zentralen

(1.2) Definition. Sei U eine Untergruppe von G . Man sagt, dass (U, G) die *Hecke-Bedingung* erfüllt und nennt (U, G) ein *Hecke-Paar*, wenn

$$\#(U \setminus U g U) < \infty \quad \text{für alle } g \in G.$$

Der Übergang zum Inversen liefert

$$(2) \quad \#(U \setminus U g^{-1} U) = \#(U g U / U),$$

so dass bei einem Hecke-Paar jede Doppelnebenklasse auch in endlich viele Linksnebenklassen zerfällt.

(1.3) Lemma. Sei (U, G) ein Hecke-Paar.

a) Seien $g \in G$ und $g_\nu \in G$ mit

$$U g U = \bigcup_{\nu=1}^d U g_\nu, \quad d = \#(U \setminus U g U).$$

Dann gilt für alle $u, u_\nu \in U$, $\nu = 1, \dots, d$,

$$U g U = \bigcup_{\nu=1}^d U u_\nu g_\nu u.$$

b) Die Abbildung

$$\iota: \mathcal{H}(U, G) \rightarrow \mathcal{R}(U, G)^U, \quad T = \sum_{g: U \setminus G / U} t(U g U) U g U \mapsto \sum_{g: U \setminus G} t(U g U) U g,$$

ist ein Isomorphismus der $\mathbb{Z}$ -Moduln.

Beweis. a) Die Behauptung folgt aus

$$UgU = (UgU)u = \left(\bigcup_{\nu=1}^d Ug_{\nu} \right) u = \bigcup_{\nu=1}^d Ug_{\nu}u = \bigcup_{\nu=1}^d Uu_{\nu}gu.$$

b) Offenbar ist die Abbildung $\iota: \mathcal{H}(U, G) \rightarrow \mathcal{R}(U, G)$ $\mathbb{Z}$ -linear und injektiv, da paarweise verschiedene Doppelnebenklassen auf paarweise verschiedene Rechtsnebenklassen abgebildet werden. Das Bild ist nach a) in $\mathcal{R}(U, G)^U$ enthalten. Sei nun

$$R = \sum_{g: U \setminus G} r(Ug)Ug \in \mathcal{R}(U, G)^U.$$

Dann gilt

$$r(Ugu) = r(Ug) \quad \text{für alle } g \in G, u \in U$$

und daher

$$R = \sum_{g: U \setminus G/U} r(Ug) \sum_{h: U \setminus UgU} Uh = \iota \left(\sum_{g: U \setminus G/U} r(Ug)UgU \right). \quad \square$$

Wir setzen die Linearform ind in diesem Fall via ι auf $\mathcal{H}(U, G)$ fort und erhalten

$$\text{ind}: \mathcal{H}(U, G) \rightarrow \mathbb{Z}, \quad T \mapsto \text{ind } T := \text{ind } \iota(T) = \sum_{g: U \setminus G} t(UgU).$$

Insbesondere erhält man aus (2)

$$(3) \quad \text{ind } UgU = \sharp(U \setminus UgU), \quad \text{ind } Ug^{-1}U = \sharp(UgU/U).$$

Nun wollen wir ein Produkt definieren. Ist (U, G) ein Hecke-Paar, so ist die Abbildung

$$(UgU) * Uh = \iota(UgU)h = \sum_{\bar{g}: U \setminus UgU} U\bar{g}h \in \mathcal{R}(U, G)$$

nach (1.3) a) wohldefiniert. Diese Operation wird $\mathbb{Z}$ -linear fortgesetzt. Für

$$T = \sum_{g: U \setminus G/U} t(UgU)UgU \in \mathcal{H}(U, G),$$

$$R = \sum_{h: U \setminus G} r(Uh)Uh$$

sei

$$\begin{aligned} T * R &= \sum_{g: U \setminus G/U} \sum_{h: U \setminus G} t(UgU)r(Uh)[(UgU) * Uh] \\ &= \sum_{\bar{g}: U \setminus G} \sum_{h: U \setminus G} t(U\bar{g}U)r(Uh)U\bar{g}h \in \mathcal{R}(U, G). \end{aligned}$$

Die entscheidende Beobachtung liegt in der

(1.4) Proposition. Sei (U, G) ein Hecke-Paar. Für $T \in \mathcal{H}(U, G)$ und $R \in \mathcal{R}(U, G)^U$ gilt

$$T * R \in \mathcal{R}(U, G)^U.$$

Beweis. Seien $u \in U$ und T, R wie oben. Dann gilt wegen der Assoziativität

$$(T * R)u = \sum_{g: U \setminus G} \sum_{h: U \setminus G} t(UgU)r(Uh)Ughu = T * (Ru) = T * R,$$

also $T * R \in \mathcal{R}(U, G)^U$. □

Nun können wir ein Produkt auf $\mathcal{H}(U, G)$ definieren via

$$T_1 \cdot T_2 = \iota^{-1}(T_1 * \iota(T_2)) \in \mathcal{H}(U, G)$$

aufgrund von (1.3) und (1.4).

(1.5) Satz. Sei (U, G) ein Hecke-Paar. Dann ist $\mathcal{H}(U, G)$ mit obigem Produkt ein Ring mit Einselement $U = UeU$.

Man nennt $\mathcal{H}(U, G)$ den Hecke-Ring oder die Hecke-Algebra zum Paar (U, G) .

Beweis. U ist trivialerweise das Einselement:

$$U \cdot UgU = UgU \cdot U = \iota^{-1} \left(\sum_{\bar{g}: U \setminus UgU} U\bar{g}e \right) = \iota^{-1} \left(\sum_{\bar{g}: U \setminus UgU} Ue\bar{g} \right) = UgU.$$

Das Assoziativgesetz folgt aus dem Assoziativgesetz für G :

$$\begin{aligned} \iota(T_1 \cdot (T_2 \cdot T_3)) &= \iota((T_1 \cdot T_2) \cdot T_3) \\ &= \sum_{g_1: U \setminus G} \sum_{g_2: U \setminus G} \sum_{g_3: U \setminus G} t_1(Ug_1U)t_2(Ug_2U)t_3(Ug_3U)Ug_1g_2g_3. \end{aligned} \quad \square$$

Wir diskutieren zwei konkrete

(1.6) Beispiele. a) Sei U ein Normalteiler in G . Dann stimmen Rechts- und Doppelnebenklassen überein: $UgU = Ug$. Also ist der Hecke-Ring genau der Gruppenring $\mathbb{Z}[G/U]$ der Faktorgruppe.

b) Sei $G = S_{n+1}$ und $U = \{\pi \in S_{n+1}; \pi(n+1) = n+1\} \cong S_n$. Man hat

$$\begin{aligned} G &= U \cup \bigcup_{j=1}^n U\langle j, n+1 \rangle = U \cup U\langle 1, n+1 \rangle U, \\ U\langle 1, n+1 \rangle U &= \bigcup_{j=1}^n U\langle j, n+1 \rangle, \\ U\langle j, n+1 \rangle &= \{\pi \in S_{n+1}; \pi(j) = n+1\}. \end{aligned}$$

Nun gilt für $i, j \in \{1, \dots, n\}$

$$\langle j, n+1 \rangle \circ \langle i, n+1 \rangle \in \begin{cases} U\langle j, n+1 \rangle, & \text{falls } i \neq j, \\ U, & \text{falls } i = j. \end{cases}$$

Daraus folgt

$$\begin{aligned} (U\langle 1, n+1 \rangle U)^2 &= \iota^{-1} \left(\sum_{j=1}^n \sum_{i=1}^n U\langle j, n+1 \rangle \circ \langle i, n+1 \rangle \right) \\ &= \iota^{-1} \left((n-1) \sum_{j=1}^n U\langle j, n+1 \rangle + nU \right) \\ &= (n-1)U\langle 1, n+1 \rangle U + nU. \end{aligned}$$

c) Nach I(2.5) ist $(\mathrm{GL}(n; \mathbb{Z}), \mathrm{GL}(n; \mathbb{Q}))$ ebenfalls ein Hecke-Paar, weil sich nach Multiplikation mit einem Vielfachen der Einheitsmatrix auf ganzzahlige Matrizen zurückziehen kann und die Menge

$$\{A \in M(n; \mathbb{Z}); |\det A| = r\}, \quad r \in \mathbb{N},$$

in endlich viele Rechtsnebenklassen zerfällt (vgl. §3).

Wir geben weitere Beschreibungen für das Produkt.

(1.7) Lemma. Sei (U, G) ein Hecke-Paar. Seien $g, h \in G$ mit

$$\begin{aligned} UgU &= \bigcup_{\mu=1}^{d(g)} Sg_{\mu}, & d(g) &= \sharp(U \backslash UgU), \\ UhU &= \bigcup_{\nu=1}^{d(h)} Sh_{\nu}, & d(h) &= \sharp(U \backslash UhU). \end{aligned}$$

Dann gilt

$$UgU \cdot UhU = \sum_{f: U \backslash UgUhU/U} \alpha(g, h; f) UfU,$$

wobei

- (i) $\alpha(g, h; f) = \sharp\{(\mu, \nu); g_{\mu}h_{\nu} \in Uf\} = \{U\tilde{h}; U\tilde{h} \subset UhU, f\tilde{h}^{-1} \in UgU\},$
- (ii) $\mathrm{ind} UfU \cdot \alpha(g, h; f) = \{(\mu, \nu); g_{\mu}h_{\nu} \in UfU\},$
 $= \mathrm{ind} UhU \cdot \sharp\{U\tilde{g}; U\tilde{g} \subset UgU, \tilde{g}h \in UfU\},$
- (iii) $\mathrm{ind} UfU \cdot \mathrm{ind} Uh^{-1}U \cdot \alpha(g, h; f)$
 $= \mathrm{ind} UhU \cdot \sharp\{U\tilde{g}, \tilde{h}U\}; U\tilde{g} \subset UgU, \tilde{h}U \subset UhU, \tilde{g}\tilde{h} \in UfU\}.$

Beweis. (i) Die Definition des Produktes liefert

$$(*) \quad \iota((UgU) \cdot (UhU)) = \sum_{\mu=1}^{d(g)} \sum_{\nu=1}^{d(h)} Ug_{\mu}h_{\nu}.$$

Nun berechne man den Koeffizienten von Uf auf der rechten Seite.

(ii) Jede Rechtsnebenklasse in UfU hat nach (1.4) den gleichen Koeffizienten in (*).

Bei der zweiten Identität wähle man die Repräsentanten in der Form $h_{\nu} = hu_{\nu}$, $u_{\nu} \in U$, $\nu = 1, \dots, d(h)$, und verwende die erste Identität.

(iii) Man verwende $\alpha(g, h; f) = \alpha(g, \tilde{h}; f)$ für alle $\tilde{h} \in UhU$ in (ii) sowie (3). $\square$

Aus (ii) erhält man direkt

$$\begin{aligned} \text{ind}((UgU) \cdot (UhU)) &= \sum_{f: U \backslash UgUhU / U} \alpha(g, h; f) \text{ind } UfU \\ &= \#\{(\mu, \nu)\} = \text{ind } UgU \cdot \text{ind } UhU, \end{aligned}$$

also das

(1.8) Korollar. *Ist (U, G) ein Hecke-Paar, so ist*

$$\text{ind}: \mathcal{H}(U, G) \rightarrow \mathbb{Z}$$

ein Ringhomomorphismus.

Wir suchen insbesondere Elemente mit einem einfachen Multiplikationsgesetz.

(1.9) Lemma. *Sei (U, G) ein Hecke-Paar und $g \in G$ mit $Ug = gU$. Dann gilt für alle $h \in G$*

$$UgU \cdot UhU = UghU, \quad UhU \cdot UgU = UhgU.$$

Beweis. Sei

$$UhU = \bigcup_{\nu=1}^d Uhu_{\nu}, \quad u_{\nu} \in U, \quad d = \text{ind } UhU.$$

Angenommen, es gilt

$$ughu_{\nu} = gh u_{\mu} \quad \text{für ein } u \in U.$$

Wegen $ug = g\bar{u}$ für ein geeignetes $\bar{u} \in U$ aufgrund von $Ug = gU$ folgt

$$\bar{u}hu_{\nu} = hu_{\mu}, \quad \text{also } \nu = \mu,$$

da die Nebenklassen Uhu_{ν} , $\nu = 1, \dots, d$, disjunkt sind. Also sind die $Ughu_{\nu}$ paarweise verschiedene Rechtsnebenklassen in $UghU$ und es folgt

$$UgU \cdot UhU = UghU.$$

Zu u_ν existiert wiederum ein $\bar{u}_\nu \in U$ mit $u_\nu g = g\bar{u}_\nu$. Also sind die Rechtsnebenklassen

$$Uhu_\nu g = Uhg\bar{u}_\nu$$

einerseits paarweise verschieden und andererseits in $UhgU$ enthalten. Es folgt

$$UhU \cdot UgU = UhgU. \quad \square$$

Wir wollen ein zentrales Kommutativitätskriterium für Hecke-Ringe herleiten. Dazu betrachten wir *Antihomomorphismen* von G , d. h. Abbildungen

$$\varphi: G \rightarrow G, \quad \varphi(gh) = \varphi(h)\varphi(g) \quad \text{für alle } g, h \in G.$$

(1.10) Satz. Sei (U, G) ein Hecke-Paar und φ ein Antihomomorphismus von G mit der Eigenschaft

$$\varphi(U) = U, \quad UgU = U\varphi(g)U \quad \text{für alle } g \in G.$$

Dann besitzt jede Doppelnebenklasse ein simultanes Vertretersystem von Rechts- und Linksnebenklassen, d. h. zu jedem $g \in G$ existieren $g_\nu \in G$, $\nu = 1, \dots, d$, $d = \text{ind } UgU$, so dass

$$UgU = \bigcup_{\nu=1}^d Ug_\nu U = \bigcup_{\nu=1}^d g_\nu U \quad (\text{disjunkt}).$$

In diesem Fall ist der Hecke-Ring $\mathcal{H}(U, G)$ kommutativ.

Beweis. Wir gehen von zwei disjunkten Zerlegungen

$$UgU = \bigcup_{\nu=1}^d U\bar{g}_\nu U = \bigcup_{\mu=1}^{\delta} g'_\mu U, \quad d = \text{ind } UgU, \quad \delta = \text{ind } Ug^{-1}U,$$

aus. Die Voraussetzungen an φ implizieren

$$\begin{aligned} UgU &= U\varphi(g)U = \varphi(UgU) = \varphi\left(\bigcup_{\nu=1}^d U\bar{g}_\nu U\right) = \bigcup_{\nu=1}^d \varphi(\bar{g}_\nu)U \\ &= \varphi\left(\bigcup_{\mu=1}^{\delta} g'_\mu U\right) = \bigcup_{\mu=1}^{\delta} U\varphi(g'_\mu). \end{aligned}$$

Daraus folgt sowohl $d \geq \delta$ als auch $\delta \geq d$ und damit

$$(*) \quad d = \delta = \text{ind}(UgU) = \text{ind}(Ug^{-1}U) \quad \text{für alle } g \in G.$$

Weil $\bar{g}_\nu$ und g'_ν zu UgU gehören gibt es $u_\nu, \bar{u}_\nu \in U$ mit

$$u_\nu \bar{g}_\nu \bar{u}_\nu = g'_\nu, \quad \text{also} \quad g_\nu := u_\nu \bar{g}_\nu = g'_\nu \bar{u}_\nu^{-1},$$

mit

$$Ug_\nu = U\bar{g}_\nu \quad \text{und} \quad g_\nu U = g'_\nu U \quad \text{für } \nu = 1, \dots, d.$$

Wir gehen nun von einem weiteren simultanen Vertretersystem

$$UhU = \bigcup_{\mu=1}^{\delta} Uh_\mu = \bigcup_{\mu=1}^{\delta} h_\mu U$$

aus. Wegen (*) führt (1.7) (iii) auf

$$UgU \cdot UhU = \sum_{f: U \backslash G/U} \alpha(g, h; f) UfU,$$

$$\text{ind } UfU \cdot \alpha(g, h; f) = \sharp\{(\nu, \mu); g_\nu h_\mu \in S f S\}.$$

Aus

$$U\varphi(g)U = \bigcup_{\nu=1}^d \varphi(g_\nu)U, \quad U\varphi(h)U = \bigcup_{\mu=1}^{\delta} U\varphi(h_\mu)$$

folgt dann

$$UhU \cdot UgU = U\varphi(h)U \cdot U\varphi(g)U = \sum_{f: U \backslash G/U} \alpha(\varphi(h), \varphi(g); f)$$

$$\text{ind } UfU \cdot \alpha(\varphi(h), \varphi(g); f) = \sharp\{(\mu, \nu); \varphi(h_\mu)\varphi(g_\nu) \in UfU\}.$$

Nun gilt

$$\varphi(h_\mu)\varphi(g_\nu) = \varphi(g_\nu h_\mu) \in U\varphi(f)U = UfU \Leftrightarrow g_\nu h_\mu \in UfU,$$

also auch

$$\alpha(g, h; f) = \alpha(\varphi(h), \varphi(g); f) \quad \text{für alle } f \in G$$

und damit

$$UgU \cdot UhU = UhU \cdot UgU. \quad \square$$

In allen Beispielen werden wir diesen Satz anwenden, um die Kommutativität eines Hecke-Rings nachzuweisen.

Ist $U \subset \mathcal{M} \subset G$ und $\mathcal{M}$ multiplikativ abgeschlossen, so ist $\mathcal{H}(U, \mathcal{M})$ ein Unterring von $\mathcal{H}(U, G)$, den wir ebenfalls als Hecke-Ring bezeichnen.

§2. Der Hecke-Ring zu $\mathrm{SL}(2; \mathbb{Z})$

In diesem Paragraphen bestimmen wir die Struktur des Hecke-Rings zum Hecke-Paar $(\mathrm{SL}(2; \mathbb{Z}), \mathrm{GL}^+(2; \mathbb{Q}))$, das in der Theorie der elliptischen Modulformen eine zentrale Rolle spielt.

Dazu sei $\Gamma := \mathrm{SL}(2; \mathbb{Z})$ die elliptische Modulgruppe und

$$\begin{aligned}\mathcal{M} &:= \mathrm{GL}^+(2; \mathbb{Q}) \cap M(2 \times 2; \mathbb{Z}) = \{A \in M(2 \times 2; \mathbb{Z}); \det A > 0\} \\ \mathcal{M}(l) &:= \{A \in M(2 \times 2; \mathbb{Z}); \det A = l\}, \quad l \in \mathbb{N}.\end{aligned}$$

(2.1) Lemma. *Für jedes $A \in \mathcal{M}(l)$ hat die Rechtsnebenklasse ΓA einen eindeutigen Vertreter der Form*

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \quad a, d \in \mathbb{N}, \quad 0 \leq b < d, \quad ad = l.$$

$\mathcal{M}(l)$ zerfällt in $\sigma_1(l)$ Rechtsnebenklassen bezüglich Γ und $(\Gamma, \mathrm{GL}^+(2; \mathbb{Q}))$ ist ein Hecke-Paar.

Beweis. Der erste Teil war schon in I(2.5) bewiesen. Daraus ergibt sich

$$\sharp \Gamma \backslash \mathcal{M}(l) = \sum_{d|l} d = \sigma_1(l).$$

Zu $A \in \mathrm{GL}^+(2; \mathbb{Q})$ wählt man ein $\alpha \in \mathbb{N}$ mit $\alpha A \in \mathcal{M}$. Dann folgt die Behauptung aus

$$\sharp(\Gamma \backslash \Gamma A \Gamma) = \sharp(\Gamma \backslash \Gamma \alpha A \Gamma) \leq \sigma_1(l), \quad l = \alpha^2 \det A \in \mathbb{N}. \quad \square$$

Um Doppelnebenklassen zu behandeln, betrachten wir

$$\delta(A) := \mathrm{ggT}(a, b, c, d), \quad A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}.$$

(2.2) Lemma. *a) Es gilt*

$$(i) \quad \delta(A)\delta(B) \mid \delta(AB) \quad \text{für alle } A, B \in \mathcal{M},$$

$$(ii) \quad \delta(UAV) = \delta(A) \quad \text{für alle } A \in \mathcal{M}, U, V \in \Gamma.$$

b) Zu $A \in \mathcal{M}$ gibt es $U, V \in \Gamma$ und eindeutig bestimmte $a, d \in \mathbb{N}$ mit

$$UAV = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}, \quad a \mid d.$$

Dabei gilt $a = \delta(A)$ und $ad = \det A$.

Beweis. a) Die Matrix

$$\frac{1}{\delta(A)\delta(B)}AB = \left(\frac{1}{\delta(A)}A\right) \cdot \left(\frac{1}{\delta(B)}B\right)$$

ist ganzzahlig. Also gilt (i). In (ii) erhält man aus (i)

$$\delta(A) \mid \delta(UAV), \quad \delta(UAV) \mid \delta(U^{-1} \cdot UAV \cdot V^{-1}) = \delta(A),$$

also die Gleichheit.

b) Das ist ein Spezialfall I(2.8) mit dem Zusatz gemäß a). $\square$

Wesentlich ist nun das

(2.3) Korollar. Seien $A \in \mathcal{M}(k)$, $B \in \mathcal{M}(l)$ mit teilerfremden $k, l \in \mathbb{N}$. Dann gilt

$$\delta(AB) = \delta(A) \cdot \delta(B).$$

Beweis. Wenn man A durch $\frac{1}{\delta(A)}A$ und B durch $\frac{1}{\delta(B)}B$ ersetzt, darf man ohne Einschränkung $\delta(A) = \delta(B) = 1$ annehmen. Wegen (2.2) genügt es daher zu zeigen, dass

$$1 = \delta\left(\begin{pmatrix} 1 & 0 \\ 0 & k \end{pmatrix} U \begin{pmatrix} 1 & 0 \\ 0 & l \end{pmatrix}\right) = \delta\begin{pmatrix} a & lb \\ kc & lkd \end{pmatrix}, \quad U = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

gilt. Sei $p \in \mathbb{P}$, das die Einträge dieser Matrix teilt, also

$$p \mid a, \quad p \mid lb, \quad p \mid kc.$$

Dann ist $p \mid b$ oder $p \mid c$ ein Widerspruch zu $\det U = 1$. Also erhält man $p \mid k$ und $p \mid l$ als Widerspruch zu $\text{ggT}(k, l) = 1$ und damit die Behauptung. $\square$

Damit kommen wir zur Anwendung auf den zugehörigen Hecke-Ring $\mathcal{H} = \mathcal{H}(\Gamma, \mathcal{M})$.

(2.4) Lemma. a) $\mathcal{H}$ ist kommutativ.

b) Für $A \in \mathcal{M}$ und $0 \neq \lambda \in \mathbb{Z}$ gilt

$$\Gamma A \Gamma \cdot \Gamma(\lambda E) \Gamma = \Gamma(\lambda A) \Gamma.$$

c) Für $A \in \mathcal{M}(k)$ und $B \in \mathcal{M}(l)$ mit teilerfremden $k, l \in \mathbb{N}$ gilt

$$\Gamma A \Gamma \cdot \Gamma B \Gamma = \Gamma(AB) \Gamma.$$

Beweis. a) Das Transponieren ist ein Antihomomorphismus von $\mathrm{GL}^+(2; \mathbb{Q})$ mit der Eigenschaft

$$\Gamma A \Gamma = \Gamma A^{tr} \Gamma \quad \text{für alle } A \in \mathcal{M}$$

nach (2.2). Dann folgt die Kommutativität aus (1.10)

b) Man verwende (1.9).

c) Aus (2.3) und (2.2) folgt $\Gamma A \Gamma B \Gamma = \Gamma A B \Gamma$, also

$$\Gamma A \Gamma \cdot \Gamma B \Gamma = t \Gamma A B \Gamma \quad \text{für ein } t \in \mathbb{N}.$$

Nun wählt man Repräsentanten $\overline{B} = \begin{pmatrix} b_1 & b_2 \\ 0 & b_4 \end{pmatrix}$ von $\Gamma \backslash \Gamma B \Gamma$ gemäß (2.1). Man erhält

$$\begin{pmatrix} 1 & 0 \\ 0 & kl \end{pmatrix} \begin{pmatrix} b_1 & b_2 \\ 0 & b_4 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & kl \end{pmatrix} \cdot \frac{1}{l} \begin{pmatrix} b_4 & -b_2 \\ 0 & b_1 \end{pmatrix} = \begin{pmatrix} b_4/l & -b_2/l \\ 0 & kb_1 \end{pmatrix}.$$

Diese Matrix ist genau dann ganzzahlig, wenn $\overline{B} = B$, also $t = 1$. □

Wir zerlegen den Hecke-Ring in Unterringe

$$\mathcal{H}_p = \mathcal{H}(\Gamma, \mathcal{M}_p), \quad \mathcal{M}_p = \bigcup_{l=0}^{\infty} \mathcal{M}(p^l), \quad p \in \mathbb{P}.$$

Man nennt $\mathcal{H}_p$ die *p-primäre Komponente* von $\mathcal{H}$.

(2.5) Satz. $\mathcal{H}$ ist das Tensorprodukt der *p-primären Komponenten*, d. h.

$$\mathcal{H} = \bigotimes_{p \in \mathbb{P}} \mathcal{H}_p.$$

Beweis. Eine Basis von $\mathcal{H}$ bzw. $\mathcal{H}_p$ wird durch die entsprechenden Doppelnebenklassen gegeben. Jede Doppelnebenklasse hat einen eindeutigen Vertreter der Form (2.2), der sich als ein endliches Produkt solcher Matrizen schreiben lässt, deren Determinante eine Primzahlpotenz ist. Dann folgt die Behauptung aus (2.4). □

Wir führen nun geeignete Elemente von $\mathcal{H}$ ein:

$$\mathcal{T}(a, d) := \Gamma \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \Gamma, \quad a, d \in \mathbb{N}, \quad \mathcal{T}(l) := \sum_{A: \Gamma \backslash \mathcal{M}(l) / \Gamma} \Gamma A \Gamma, \quad l \in \mathbb{N}.$$

Für eine Primzahl p hat man speziell

$$\mathcal{T}(1, p) = \mathcal{T}(p) = \mathcal{M}(p).$$

Mit diesen Bezeichnungen reformulieren wir (2.4), (2.3) und (2.1) als

(2.6) Korollar. Für $a, d, l \in \mathbb{N}$ gilt

$$a) \quad \mathcal{T}(l) = \sum_{ad=l, a|d} \mathcal{T}(a, d),$$

$$b) \quad \mathcal{T}(a, d) \cdot \mathcal{T}(l, l) = \mathcal{T}(la, ld),$$

$$c) \quad \text{ind } \mathcal{T}(l) = \sigma_1(l).$$

Nun beschreiben wir die Struktur von $\mathcal{H}_p$.

(2.7) Satz. Sei p eine Primzahl. Dann gilt

$$a) \quad \text{ind } \mathcal{T}(1, p^k) = \text{ind } \mathcal{T}(p^l, p^{k+l}) = p^{k-1}(p+1) \text{ für } k, l \geq 1.$$

$$b) \quad \mathcal{T}(1, p^k) = \mathcal{T}(p^k) - \mathcal{T}(p, p) \cdot \mathcal{T}(p^{k-2}) \text{ für } k \geq 2.$$

$$c) \quad \mathcal{T}(p)^2 = \mathcal{T}(1, p^2) + (p+1)\mathcal{T}(p, p).$$

$$d) \quad \mathcal{T}(p) \cdot \mathcal{T}(p)^k = \mathcal{T}(p^{k+1}) + p\mathcal{T}(p, p) \cdot \mathcal{T}(p^{k-1}) \text{ für } k \geq 1.$$

$$e) \quad \mathcal{T}(p) \cdot \mathcal{T}(1, p^k) = \mathcal{T}(1, p^{k+1}) + p\mathcal{T}(p, p) \cdot \mathcal{T}(1, p^{k-1}) \text{ für } k \geq 2.$$

$$f) \quad \mathcal{T}(p^r) \cdot \mathcal{T}(p^s) = \sum_{\nu=0}^{\min(r,s)} p^\nu \mathcal{T}(p, p)^\nu \cdot \mathcal{T}(p^{r+s-\nu}) \text{ für } r, s \geq 0.$$

$$g) \quad \mathcal{T}(k) \cdot \mathcal{T}(l) = \sum_{d|\text{ggT}(k,l)} d\mathcal{T}(d, d) \cdot \mathcal{T}(kl/d^2) \text{ für } k, l \geq 1.$$

Beweis. a) Nach (2.1) und (2.2) wird ein Vertretersystem von $\Gamma \backslash \mathcal{T}(1, p^k)$ gegeben durch

$$\begin{pmatrix} 1 & b \\ 0 & p^k \end{pmatrix}, \quad 0 \leq b < p^k, \quad \begin{pmatrix} p^k & b \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} p^{k-\nu} & b \\ 0 & p^\nu \end{pmatrix}, \quad 0 \leq b < p^\nu, \quad p \nmid b, \quad \nu = 1, \dots, k-1.$$

Beim zweiten Teil verwende man (2.6) und (1.8).

b) Das ist eine Folgerung aus (2.2).

c) Das ist wegen b) ein Spezialfall von d).

d) Wir berechnen

$$\mathcal{T}(p^k) \cdot \mathcal{T}(p) = \sum_{B: \Gamma \backslash \mathcal{M}(p^{k+1})/\Gamma} t(B) \Gamma B \Gamma.$$

Nach a) wird ein Vertretersystem von $\Gamma \backslash \mathcal{T}(p)$ gegeben durch

$$A_j := \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix}, \quad j = 0, \dots, p-1, \quad A_p := \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}.$$

Ist $B \in \mathcal{M}(p^{k+1})$ mit $p \mid \delta(B)$ dann führt $pA_j^{-1} \in M(2 \times 2; \mathbb{Z})$ zu

$$BA_j^{-1} \in \mathcal{M}(p^k), \quad j = 0, \dots, p,$$

also $t(B) = p + 1$. Es gibt nur eine Doppelnebenklasse $\Gamma B \Gamma$ in $\mathcal{M}(p^{k+1})$ mit $p \nmid \delta(B)$ und wir wählen den Vertreter

$$B = \begin{pmatrix} 1 & 0 \\ 0 & p^{k+1} \end{pmatrix}.$$

Dann bekommt man

$$BA_j^{-1} = \begin{pmatrix} 1 & -i/p \\ 0 & p^k \end{pmatrix} \quad \text{bzw.} \quad \begin{pmatrix} 1/p & 0 \\ 0 & p^{k+1} \end{pmatrix} \in M(2 \times 2; \mathbb{Z})$$

genau dann, wenn $j = 0$. Also gilt $t(B) = 1$. Aus b) erhalten wird

$$\begin{aligned} \mathcal{T}(p^k) \cdot \mathcal{T}(p) &= \mathcal{T}(1, p^{k+1}) + (p+1) \sum_{\substack{B: \Gamma \backslash \mathcal{M}(p^{k+1}) / \Gamma, \\ p \nmid \delta(B)}} \Gamma B \Gamma \\ &= \mathcal{T}(p^{k+1}) + p \mathcal{T}(p, p) \cdot \mathcal{T}(p^{k-1}). \end{aligned}$$

e) Man benutze b) und c) in der folgenden Rechnung

$$\begin{aligned} \mathcal{T}(p) \cdot \mathcal{T}(1, p^2) &= \mathcal{T}(p) \cdot \mathcal{T}(p^2) - \mathcal{T}(p) \cdot \mathcal{T}(p, p) \\ &= \mathcal{T}(p^3) + (p-1) \mathcal{T}(p, p) \cdot \mathcal{T}(p) = \mathcal{T}(1, p^3) + p \mathcal{T}(p, p) \cdot \mathcal{T}(p) \end{aligned}$$

und für $k \geq 3$

$$\begin{aligned} \mathcal{T}(p) \cdot \mathcal{T}(1, p^k) &= \mathcal{T}(p) \cdot \mathcal{T}(p^k) - \mathcal{T}(p) \cdot \mathcal{T}(p, p) \cdot \mathcal{T}(p^{k-2}) \\ &= \mathcal{T}(p^{k+1}) + p \mathcal{T}(p, p) \cdot \mathcal{T}(p^{k-1}) - \mathcal{T}(p, p) \cdot \mathcal{T}(p^{k-1}) - p \mathcal{T}(p, p)^2 \cdot \mathcal{T}(p^{k-3}) \\ &= \mathcal{T}(1, p^{k+1}) + p \mathcal{T}(p, p) \cdot \mathcal{T}(1, p^{k-1}). \end{aligned}$$

f) Wir verwenden eine Induktion nach r , wobei $r = 0$ trivial ist und $r = 1$ aus d) folgt. Sei daher $2 \leq r \leq s$. Dann folgt aus d) und der Induktionsvoraussetzung

$$\begin{aligned} \mathcal{T}(p^r) \cdot \mathcal{T}(p^s) &= \mathcal{T}(p) \cdot \mathcal{T}(p^{r-1}) \cdot \mathcal{T}(p^s) - p \mathcal{T}(p, p) \cdot \mathcal{T}(p^{r-2}) \cdot \mathcal{T}(p^s) \\ &= \sum_{\nu=0}^{r-1} p^\nu \mathcal{T}(p) \cdot \mathcal{T}(p, p)^\nu \cdot \mathcal{T}(p^{r+s-1-1\nu}) - p \sum_{\nu=0}^{r-2} p^\nu \mathcal{T}(p, p)^{\nu+1} \cdot \mathcal{T}(p^{r+s-2-2\nu}) \\ &= \sum_{\nu=0}^{r-1} \left(p^\nu \cdot \mathcal{T}(p, p)^\nu \mathcal{T}(p^{r+s-2\nu}) + p^{\nu+1} \mathcal{T}(p, p)^{\nu+1} \cdot \mathcal{T}(p^{r+s-2-2\nu}) \right) \\ &\quad - \sum_{\nu=0}^{r-2} p^{\nu+1} \mathcal{T}(p, p)^{\nu+1} \cdot \mathcal{T}(p^{r+s-2\nu}) \\ &= \sum_{\nu=0}^r p^\nu \mathcal{T}(p, p)^\nu \cdot \mathcal{T}(p^{r+s-2\nu}). \end{aligned}$$

g) Man kombiniere f) mit (2.4) und benutze $\mathcal{T}(p, p)^\nu = \mathcal{T}(p^\nu, p^\nu)$. □

Das finale Resultat ist der

(2.8) Satz. Sei p eine Primzahl. Dann gilt

$$\mathcal{H}_p = \mathbb{Z}[\mathcal{T}(p), \mathcal{T}(p, p)],$$

wobei $\mathcal{T}(p)$ und $\mathcal{T}(p, p)$ algebraisch unabhängig sind.

Beweis. Eine einfache Rechnung mit (2.7) c) und e) zeigt

$$\mathcal{T}(1, p^k) \in \mathbb{Z}[\mathcal{T}(p), \mathcal{T}(p, p)] \quad \text{für alle } k \geq 1.$$

Dann folgt

$$\mathcal{H}_p = \mathbb{Z}[\mathcal{T}(p), \mathcal{T}(p, p)]$$

mit (2.5). Nach (2.2) gibt es $[l/2] + 1$ Doppelnebenklassen in $\mathcal{M}(p^l)$. Andererseits ist

$$\mathcal{T}(p, p)^\nu \cdot \mathcal{T}(p)^\mu, \quad \nu, \mu \in \mathbb{N}_0,$$

genau dann eine Linearkombination von Doppelnebenklassen in $\mathcal{M}(p^l)$, wenn $2\nu + \mu = l$. Also existieren genau $[l/2] + 1$ solcher Monome. Weil $\mathcal{T}(p)$ und $\mathcal{T}(p, p)$ aber $\mathcal{H}_p$ erzeugen, sind sie somit algebraisch unabhängig. $\square$

Eine Kombination mit (2.5) liefert das

(2.9) Korollar. Die Hecke-Algebra $\tilde{\mathcal{H}} := \mathcal{H} \otimes \mathbb{Q}$ wird erzeugt von

$$\mathcal{T}(l), \quad l \in \mathbb{N}.$$

Beweis. Aus (2.7) d) erhält man

$$\mathcal{T}(p, p) = \frac{1}{p}(\mathcal{T}(p)^2 - \mathcal{T}(p^2)).$$

Nun verwende man (2.8) und (2.5). $\square$

Man betrachte den Hecke-Ring zu $(\Gamma, \mathrm{SL}(2; \mathbb{Q}))$, der nach (2.8) und aus allen Polynomen über $\mathbb{Z}$ in

$$\mathcal{T}(p)^2 \cdot \mathcal{T}(p, p)^{-1} = \Gamma \begin{pmatrix} p^{-1} & 0 \\ 0 & p \end{pmatrix} + (p+1)\Gamma, \quad p \in \mathbb{P},$$

besteht.

(2.10) Korollar. Der Hecke-Ring $\mathcal{H}(\Gamma, \mathrm{SL}(2; \mathbb{Q}))$ besteht aus den Polynomen in

$$\Gamma \begin{pmatrix} 1/p & 0 \\ 0 & p \end{pmatrix} \Gamma, \quad p \in \mathbb{P},$$

die algebraisch unabhängig sind.

Nun beschreiben wir die Operation des Hecke-Rings auf dem Vektorraum der ganzen elliptischen Modulformen. Für $M \in \mathcal{M}(q)$ und $f \in \mathcal{M}_k(\Gamma)$ sei

$$f \mid_k \Gamma M \Gamma := \sum_{K: \Gamma \backslash \Gamma M \Gamma} f \mid_k K.$$

Wegen $f \mid_k L = f$ für alle $L \in \Gamma$ ist die Abbildung wohldefiniert und $f \mid_k \Gamma M \Gamma$ wieder holomorph und unter Γ invariant. Nimmt man das Vertretersystem $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}_k$ so sieht man, dass $f((az+b)/d)$ wieder eine Potenzreihe in $e^{2\pi iz/q}$ ist und dass somit $f \mid_k \Gamma M \Gamma$ die

Beschränktheitsforderung erfüllt. Diese Abbildung wird linear auf $\tilde{\mathcal{H}}$ fortgesetzt. Die Abbildungen

$$f \mapsto f \mid_k \mathcal{T}, \quad \mathcal{T} \in \tilde{\mathcal{H}}$$

heißen *Hecke-Operatoren*. Insbesondere hat man

$$f \mid_k \mathcal{T}(l, l) = l^{-k} f.$$

Wir schreiben die Fourier-Entwicklung von $f \in \mathcal{M}_k(\Gamma)$ in der Form

$$f(z) = \sum_{m=0}^{\infty} \alpha_f(m) e^{2\pi i m z}, \quad z \in \mathcal{H}_1.$$

(2.11) Satz. *Die Abbildung*

$$\mathcal{H} \rightarrow \mathrm{End} \mathcal{M}_k(\Gamma), \quad \mathcal{T} \mapsto (f \mapsto f \mid_k \mathcal{T}),$$

ist ein Ringhomomorphismus. Jeder Hecke-Operator bildet Spitzenformen auf Spitzenformen ab. Es gilt für $n \in \mathbb{N}$

$$g(z) = f \mid_k \mathcal{T}(n)(z) = \sum_{m=0}^{\infty} \alpha_g(m) e^{2\pi i m z}$$

mit

$$\alpha_g(m) = \sum_{d \mid \mathrm{ggT}(m, n)} (d/n)^{k-1} \alpha_f(mn/d^2), \quad m \in \mathbb{N}_0,$$

insbesondere

$$\alpha_g(0) = \sigma_{1-k}(n) \cdot \alpha_f(0), \quad \alpha_g(1) = n^{1-k} \cdot \alpha_f(n).$$

Beweis. Aus

$$\iota(\Gamma M \Gamma) = \sum_{\mu=1}^{d(M)} \Gamma M_{\mu}, \quad \iota(\Gamma N \Gamma) = \sum_{\nu=1}^{d(N)} \Gamma N_{\nu}$$

folgt mit der Definition des Produktes

$$\iota(\Gamma M \Gamma * \Gamma N \Gamma) = \sum_{\mu=1}^{d(M)} \sum_{\nu=1}^{d(N)} \Gamma M_{\mu} N_{\nu}$$

und damit

$$\begin{aligned} f \Big|_k (\Gamma M \Gamma * \Gamma N \Gamma) &= \sum_{\mu=1}^{d(M)} \sum_{\nu=1}^{d(N)} f \Big|_k (M_{\mu} N_{\nu}) = \sum_{\nu=1}^{d(N)} \left(\sum_{\mu=1}^{d(M)} f \Big|_k M_{\mu} \right) \Big|_k N_{\nu} \\ &= \left(f \Big|_k (\Gamma M \Gamma) \right) \Big|_k \Gamma N \Gamma. \end{aligned}$$

Also ist die Abbildung ein Ringhomomorphismus. Verwendet man für $\mathcal{T}(n)$ das Vertretersystem aus (2.1), so ergibt sich

$$\begin{aligned} g(z) &= f \Big|_k \mathcal{T}(n)(z) = \sum_{ad=n} \sum_{b \bmod m} d^{-k} f((az+b)/d) \\ &= \sum_{ad=n} \sum_{m=0}^{\infty} \alpha_f(m) e^{2\pi i m a z / d} \cdot \sum_{b \bmod d} e^{2\pi i m b / d}. \end{aligned}$$

Mit der geometrischen Reihe kommt man auf

$$\sum_{b \bmod d} e^{2\pi i m b / d} = \begin{cases} 0 & \text{falls } d \nmid m, \\ d & \text{falls } d \mid m. \end{cases}$$

Also muss man nur über $m = dl$ summieren und erhält

$$\begin{aligned} g(z) &= \sum_{ad=n} \sum_{l=0}^{\infty} d^{1-k} \alpha_f(dl) e^{2\pi i l a z} \\ &= \sum_{l=0}^{\infty} \sum_{a|n} (a/n)^{k-1} \alpha_f(nl/a) e^{2\pi i a l z} \\ &= \sum_{r=0}^{\infty} \left(\sum_{a \mid \text{ggT}(r,n)} (a/n)^{k-1} \alpha_f(rn/a^2) \right) e^{2\pi i r z}. \end{aligned}$$

Das liefert die Formel für die Fourier-Koeffizienten, woraus sich sofort die Spezialfälle $r = 0$ und $r = 1$ ergeben. Also werden auch Spitzenformen auf Spitzenformen abgebildet. $\square$

Wir nennen $0 \neq f \in \mathcal{M}_k(\Gamma)$ eine *simultane Eigenform*, wenn es zu jedem $\mathcal{T} \in \mathcal{H}$ ein $\lambda_f(\mathcal{T}) \in \mathbb{C}$ gibt mit

$$f \Big|_k \mathcal{T} = \lambda_f(\mathcal{T}) f.$$

Es genügt wegen Korollar (2.9), die Eigenschaft für alle $\mathcal{T} = \mathcal{T}(n)$, $n \in \mathbb{N}$, mit $\lambda_f(n) := \lambda_f(\mathcal{T}(n))$ nachzuweisen. Aus (2.11) folgt dann

$$\lambda_f(n) \cdot \alpha_f(m) = \alpha_g(m) = \sum_{d \mid \mathrm{ggT}(m,n)} (d/n)^{k-1} \alpha_f(mn/d^2), \quad m \in \mathbb{N}_0$$

und speziell für $m = 1$

$$(*) \quad \lambda_f(n) \cdot \alpha_f(1) = n^{1-k} \alpha_f(n).$$

(2.12) Lemma. Für ein nicht-konstantes $f \in \mathcal{M}_k(\Gamma)$ sind äquivalent

(i) f ist eine simultane Eigenform.

(ii) Es gilt $\alpha_f(1) \neq 0$ und für alle $m \in \mathbb{N}_0$, $n \in \mathbb{N}$

$$\alpha_f(m) \cdot \alpha_f(n) = \alpha_f(1) \cdot \sum_{d \mid \mathrm{ggT}(m,n)} (d/n)^{k-1} \alpha_f(mn/d^2).$$

In diesem Fall sind die Eigenwerte

$$\lambda_f(n) = n^{1-k} \frac{\alpha_f(n)}{\alpha_f(1)}, \quad n \in \mathbb{N},$$

und es gilt

$$\alpha_f(m) \cdot \alpha_f(n) = \alpha_f(1) \cdot \alpha_f(mn)$$

für alle teilerfremden $m, n \in \mathbb{N}$ sowie für $p \in \mathbb{P}$, $r \in \mathbb{N}$

$$\alpha_f(1) \cdot \alpha_f(p^{r+1}) = \alpha_f(p^r) \cdot \alpha_f(p) - p^{k-1} \alpha_f(p^{r-1}) \cdot \alpha_f(1).$$

Beweis. Die Äquivalenz von (i) und (ii) folgt aus Satz (2.11), denn $\alpha_f(1) = 0$ würde wegen (*) auch $\alpha_f(n) = 0$ für alle $n \in \mathbb{N}$ implizieren, woraus folgt, dass f konstant ist. Der erste Zusatz ergibt sich aus (*). Für teilerfremde $m, n \in \mathbb{N}$ liefert (2.7)

$$\lambda_f(m) \cdot \lambda_f(n) = \lambda_f(mn), \quad \lambda_f(p^r) \cdot \lambda_f(p) = \lambda_f(p^{r+1}) - p^{k-1} \lambda_f(p^{r-1}),$$

woraus man wiederum mit (*) die letzte Aussage erhält. $\square$

Wir übersetzen das Lemma (2.12) in eine Eigenschaft der zugehörigen Dirichlet-Reihe

$$D_f(s) = \sum_{m=1}^{\infty} \alpha_f(m) \cdot m^{-s}.$$

(2.13) Korollar. Ist $f \in \mathcal{M}_k(\Gamma)$ eine simultane Eigenform mit $\alpha_f(1) = 1$, so hat $D_f(s)$ eine Entwicklung als Euler-Produkt

$$D_f(s) = \prod_p (1 - \alpha_f(p)p^{-s} + p^{k-1-2s})^{-1}.$$

Beweis. Aus $\alpha_f(m) \cdot \alpha_f(n) = \alpha_f(mn)$ für teilerfremde $m, n \in \mathbb{N}$ gemäß (2.12) ergibt sich

$$D_f(s) = \prod_p \left(\sum_{r=0}^{\infty} \alpha_f(p^r) p^{-rs} \right).$$

Nun berechnet man wieder mit (2.12)

$$\begin{aligned} & \left(\sum_{r=0}^{\infty} \alpha_f(p^r) p^{-rs} \right) \cdot (1 - \alpha_f(p)p^{-s} + p^{k-1-2s}) \\ &= \alpha_f(1) + \sum_{r=2}^{\infty} [\alpha_f(p^r) - \alpha_f(p^{r-1}) \cdot \alpha_f(p) + p^{k-1} \alpha_f(p^{r-2})] p^{-rs} \\ &= 1. \end{aligned}$$

□

Wir wissen, dass Hecke-Operatoren Spitzenformen auf Spitzenformen abbilden. Mit

$$\mathcal{S}_{12}(\Gamma) = \mathbb{C}\Delta^*, \quad \Delta^*(z) = \sum_{m=1}^{\infty} \tau(m) e^{2\pi i m z}, \quad \tau(1) = 1,$$

folgt das

(2.14) Korollar. Die Diskriminante Δ^* ist eine simultane Eigenform

$$\Delta^* \mid_{12} \mathcal{T}(n) = n^{-11} \tau(n) \Delta^*, \quad n \in \mathbb{N}.$$

Die Fourier-Koeffizienten erfüllen

$$\begin{aligned} \tau(m) \cdot \tau(n) &= \tau(mn) \quad \text{für alle teilerfremden } m, n \in \mathbb{N}, \\ \tau(p^{r+1}) &= \tau(p^r) \cdot \tau(p) - p^{11} \tau(p^{r-1}) \quad \text{für alle } p \in \mathbb{P}, r \in \mathbb{N}. \end{aligned}$$

Dieses Korollar war der Ursprung für die Entwicklung der Hecke-Operatoren durch Mordell um 1920. Aber erst Hecke erkannte in den 30er Jahren die universelle Bedeutung dieser Konstruktion.

(2.15) Korollar. Die Eisenstein-Reihen sind simultane Eigenformen: Ist $k > 2$ gerade, so gilt

$$E_k^{(1)} \mid_k \mathcal{T}(n) = \sigma_{1-k}(n) E_k^{(1)}.$$

Beweis. Wir beweisen die Aussage zunächst für eine Primzahl $n = p$. Sei dazu $g := E_k^{(1)} \mid_k \mathcal{T}(p)$. Dann gilt

$$\alpha_g(0) = \sigma_{1-k}(p) = 1 + p^{1-k}$$

nach (2.11). Für $m \in \mathbb{N}$ gilt

$$\alpha_g(m) = \begin{cases} p^{1-k} \alpha_f(pm), & \text{falls } p \nmid m, \\ p^{1-k} \alpha_f(pm) + \alpha_f(m/p), & \text{falls } p \mid m, \end{cases}$$

wobei $\alpha_f(m) = -\frac{2k}{B_k} \sigma_{k-1}(m)$. Weil die Teilersummen multiplikativ sind, hat man im ersten Fall

$$\alpha_g(m) = p^{1-k} \sigma_{k-1}(p) \cdot \alpha_f(m) = \sigma_{1-k}(p) \cdot \alpha_f(m).$$

Im zweiten Fall kann man sich mit demselben Argument auf $m = p^r$, $r \in \mathbb{N}$, zurückziehen. Dann gilt

$$\begin{aligned} -\frac{B_k}{2k} \alpha_g(p^r) &= p^{1-k} \sigma_{k-1}(p^{r+1}) + \sigma_{k-1}(p^{r-1}) \\ &= p^{1-k} \sum_{l=0}^{r+1} p^{l(k-1)} + \sum_{l=0}^{r-1} p^{l(k-1)} \\ &= (p^{1-k} + 1) \sum_{l=0}^r p^{l(k-1)} = \sigma_{1-k}(p) \cdot \sigma_{k-1}(r). \end{aligned}$$

Durch Betrachtung der Fourier-Reihen folgt

$$g = \sigma_{1-k}(p) E_k^{(1)}.$$

Nach (2.7) ist $E_k^{(1)}$ eine simultane Eigenform. Der Eigenwert ergibt sich aus (2.11). $\square$

Wir beschreiben eine weitere Anwendung der Hecke-Theorie auf Modulfunktionen. Dazu bezeichne $j(z)$ die absolute Invariante.

(2.16) Satz. Zu jedem $n \in \mathbb{N}$ existiert ein eindeutig bestimmtes Polynom

$$F_n(X, Y) \in \mathbb{Q}[X, Y]$$

mit der Eigenschaft

$$(*) \quad F_n(X, j(z)) = \prod_{M: \Gamma \backslash \mathcal{M}(n)} (X - j(M\langle z \rangle)) \quad \text{für alle } z \in \mathcal{H}_1.$$

$F_n(X, Y)$ hat als Polynom in X bzw. Y jeweils den Grad $\sigma_1(n)$.

Beweis. Sei

$$F_n(X) := \prod_{M \in \Gamma \backslash \mathcal{M}(n)} (X - j(M\langle z \rangle)).$$

Weil j bereits Γ -invariant ist, hängt die Definition nicht von der Wahl des Vertretersystems ab. Sei $r = \sigma_1(n)$ und $M_1, \dots, M_r$ das Standardvertretersystem aus (2.1). Dann folgt

$$F_n(X) = \sum_{k=0}^r (-1)^k E_k(j(M_1\langle z \rangle), \dots, j(M_r\langle z \rangle)) \cdot X^{r-k},$$

wobei S_k das k -te elementarsymmetrische Polynom in r Unbestimmten ist. Für die Potenzsummen gilt

$$\sum_{\nu=1}^r j(M_\nu\langle z \rangle)^k = j^k \mid \mathcal{T}(n) \in \mathbb{Q}[j(z)],$$

da die Modulfunktion auf der linken Seite holomorph auf $\mathcal{H}_1$ ist und rationale Fourier-Koeffizienten hat. Bekanntlich kann man die elementarsymmetrischen Polynome rational durch Potenzsummen ausdrücken, d. h.

$$(**) \quad S_k(j(M_1\langle z \rangle), \dots, j(M_r\langle z \rangle)) \in \mathbb{Q}[j(z)].$$

Weil $j(z)$ transzendent ist, gibt es ein eindeutig bestimmtes Polynom $F_n(X, Y) \in \mathbb{Q}[X, Y]$ mit der Eigenschaft (*). Offenbar hat $F_n(X, Y)$ in X den Grad r .

Der höchste auftretende Pol in ∞ bei den Funktionen (**) hat die Ordnung $r = \sigma_1(n)$ und dieser tritt nur bei S_r auf, denn in diesem Fall beginnt die Fourier-Entwicklung mit dem Term

$$\prod_{d|n} \prod_{b \pmod{d}} e^{-2\pi i(nz+b)/d^2} = \pm \prod_{d|n} e^{-2\pi inz/d} = \pm e^{-2\pi irz}.$$

Folglich sind alle $S_k(j(M_1\langle z \rangle), \dots, j(M_r\langle z \rangle))$ für $0 \leq k < r$ Polynome in $j(z)$ von einem Grad $< r$ und für $k = r$ ein Polynom in $j(z)$ vom Grad r . Demnach hat $F_n(X, Y)$ in Y ebenfalls den Grad r . $\square$

Man nennt $F_n(X, Y) = 0$ die *Modulargleichung vom Grad n* . Trivialerweise gilt

$$F_1(X, Y) = X - Y.$$

Eine längere Rechnung mit der Fourier-Entwicklung von $j(z)$ liefert

$$\begin{aligned} F_2(X, Y) = & X^3 + Y^3 - X^2Y^2 + 1.488(X^2Y + XY^2) - 162.000(X^2 + Y^2) \\ & + 40.773.375XY + 8.748.000.000(X + Y) - 157.464.000.000.000. \end{aligned}$$

§3. Der Hecke-Ring zur unimodularen Gruppe

Wir verwenden die Abkürzung

$$\mathcal{U}_n := \mathrm{GL}(n; \mathbb{Z})$$

für die *unimodulare Gruppe*. Als Wiederholung aus der Linearen Algebra formulieren wir den

(3.1) Satz. *a) Die unimodulare Gruppe $\mathcal{U}_n$, $n > 1$, wird erzeugt von den Matrizen*

$$P_{\langle 1, j \rangle}, \quad j = 2, \dots, n, \quad E + E_{12}.$$

b) Zu jeder Matrix $A \in M(m \times n; \mathbb{Z})$ mit $\mathrm{Rang} A = r$ gibt es $U \in \mathcal{U}_m$, $V \in \mathcal{U}_n$ und eindeutig bestimmte $d_1, \dots, d_r \in \mathbb{N}$, so dass

$$UAV = \begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix}, \quad D = \mathrm{diag}(d_1, \dots, d_r), \quad d_1 \mid d_2 \mid \dots \mid d_r.$$

Dabei gilt für $k = 1, \dots, r$

$$d_1 \cdot \dots \cdot d_k = \delta_k(A) = \mathrm{ggT} \{k \times k \text{ Unterdeterminanten von } A\}.$$

c) Zu jeder Matrix $A \in M(n; \mathbb{Z})$ mit $\det A \neq 0$ gibt es ein $U, V \in \mathcal{U}_n$ sowie eindeutig bestimmte Matrizen $B = (b_{ij})$, $C = (c_{ij})$, so dass

$$UA = B = \begin{pmatrix} * & & * \\ & \ddots & \\ 0 & & * \end{pmatrix}, \quad b_{ij} = 0 \text{ für } i > j, \quad b_{jj} \in \mathbb{N}, \quad 0 \leq b_{ij} < b_{jj}, \quad 1 \leq i < j \leq n.$$

$$VA = C = \begin{pmatrix} * & & 0 \\ & \ddots & \\ * & & * \end{pmatrix}, \quad c_{ij} = 0 \text{ für } i < j, \quad c_{ii} \in \mathbb{N}, \quad 0 \leq b_{ij} < c_{ii}, \quad 1 \leq i < j \leq n.$$

Als unmittelbare Folgerung erhält man das

(3.2) Korollar. *Für $A, B \in M(n; \mathbb{Z})$ gilt*

$$\mathcal{U}_n A \mathcal{U}_n = \mathcal{U}_n B \mathcal{U}_n \Leftrightarrow \delta_k(A) = \delta_k(B) \quad \text{für } k = 1, \dots, n.$$

Wir interessieren uns nun für die Multiplikativität der Elementarteiler

(3.3) Satz. Seien $A, B \in M(n; \mathbb{Z})$ mit $\det A \neq 0$ und $\det B \neq 0$.

a) Für $1 \leq k \leq n$ gilt (mit der Erweiterung $\delta_0 := 1$)

$$\delta_k(AB) = q_k \delta_k(A) \cdot \delta_k(B) \quad \text{mit einem } q_k \mid \text{ggT} \left(\frac{\det A}{\delta_k(A) \delta_{n-k}(A)}, \frac{\det B}{\delta_k(B) \delta_{n-k}(B)} \right).$$

b) Sind $\det A$ und $\det B$ teilerfremd, so gilt

$$\delta_k(AB) = \delta_k(A) \cdot \delta_k(B) \quad \text{für } k = 1, \dots, n.$$

Beweis. a) Nach (3.1) gilt für $U, V \in \mathcal{U}_n$ und $k = 1, \dots, n$

$$\delta_k(UAV) = \delta_k(A), \quad \delta_k(U) = 1.$$

Also genügt es,

$$\delta_k(AWB), \quad A = \text{diag}(a_1, \dots, a_n), \quad B = \text{diag}(b_1, \dots, b_n), \quad a_i, b_i \in \mathbb{N}, \quad a_i \mid a_{i+1}, \quad b_i \mid b_{i+1}$$

zu betrachten. Sei $I, J \subset \{1, \dots, n\}$, $\#I = \#J = k$. Wir betrachten die $k \times k$ Untermatrix

$$(AWB)_{I,J} = (AWB)_{i \in I, j \in J}.$$

Es folgt

$$\det(AWB)_{I,J} = \prod_{i \in I} a_i \cdot \prod_{j \in J} b_j \cdot \det W_{I,J} \quad \bigg| \quad \prod_{i=n-k+1}^n a_i \cdot \prod_{j=n-k+1}^n b_j \cdot \det W_{IJ}.$$

Wegen

$$\delta_k(W) = \text{ggT} \{ \det W_{I,J}; \quad I, J \subset \{1, \dots, n\}, \quad \#I = \#J = k \} = 1$$

folgt die Behauptung mit

$$\prod_{i=n-k+1}^n a_i = \frac{\det A}{\delta_{n-k}(A)}, \quad \prod_{j=n-k+1}^n b_j = \frac{\det B}{\delta_{n-k}(B)}.$$

b) Das ist eine unmittelbare Konsequenz von a). □

Um den Hecke-Ring zu studieren, verwenden wir die Bezeichnungen

$$\mathcal{D}_n := \{A \in M(n; \mathbb{Z}); \det A \neq 0\}, \quad \mathcal{D}_n(l) = \{A \in M(n; \mathbb{Z}); |\det A| = l\}, \quad l \in \mathbb{N}.$$

(3.4) Korollar. Für jedes $l \in \mathbb{N}$ zerfällt $\mathcal{D}_n(l)$ in endlich viele Rechtsnebenklassen bezüglich $\mathcal{U}_n$. Insbesondere ist $(\mathcal{U}_n, \mathrm{GL}(n; \mathbb{Q}))$ ein Hecke-Paar.

Beweis. Wir wählen die Vertreter in der Form (3.1) c) und erhalten

$$\#(\mathcal{U}_n \backslash \mathcal{D}_n(l)) = \sum_{\substack{(b_1, \dots, b_n) \in \mathbb{N}^n \\ b_1 \cdots b_n = l}} b_1^0 b_2^1 \cdots b_n^{n-1} \leq \sum_{\substack{(b_1, \dots, b_n) \in \mathbb{N}^n \\ b_1 \cdots b_n = l}} l^{n-1} \leq l^{2n-1} < \infty.$$

Für $A \in \mathrm{GL}(n; \mathbb{Q})$ betrachte man $\lambda \in \mathbb{N}$ mit $\lambda A \in \mathcal{D}_n(l)$, $l \in \mathbb{N}$ geeignet. □

Speziell gilt

$$\begin{aligned} \#(\mathcal{U}_2 \backslash \mathcal{D}_2(l)) &= \sum_{d|l} d = \sigma_1(l), \\ \#(\mathcal{U}_3 \backslash \mathcal{D}_3(l)) &= \sum_{d|l} d^2 \sigma_1(l/d) = l^2 \sum_{d|l} \frac{\sigma_1(d)}{d^2}. \end{aligned}$$

Nun betrachten wir den Hecke-Ring

$$\mathcal{H}_n := \mathcal{H}(\mathcal{U}_n, \mathcal{D}_n) \subset \mathcal{H}(\mathcal{U}_n, \mathrm{GL}(n; \mathbb{Q})).$$

(3.5) Lemma. a) $\mathcal{H}_n$ ist ein kommutativer Ring
 b) Für $A \in \mathcal{D}_n$ und $\lambda \in \mathbb{Z}$, $\lambda \neq 0$, gilt

$$\mathcal{U}_n A \mathcal{U}_n \cdot \mathcal{U}_n (\lambda E) \mathcal{U}_n = \mathcal{U}_n (\lambda A) \mathcal{U}_n.$$

c) Sind $A, B \in \mathcal{D}_n$, so dass $\det A$ und $\det B$ teilerfremd sind, dann gilt

$$\mathcal{U}_n A \mathcal{U}_n \cdot \mathcal{U}_n B \mathcal{U}_n = \mathcal{U}_n (AB) \mathcal{U}_n.$$

d) Jede Doppelnebenklasse in $\mathcal{H}_n$ besitzt ein simultanes Vertretersystem der Rechts- und Linksnebenklassen.

Beweis. a) Das Transponieren ist ein Antihomomorphismus von $\mathrm{GL}(n; \mathbb{Q})$, der die Doppelnebenklassen gemäß (3.1) invariant lässt. Dann folgt die Kommutativität aus (1.10).

b) Man verwende (1.9).

c) Aus (3.3) und (3.2) ergibt sich $\mathcal{U}_n A \mathcal{U}_n B \mathcal{U}_n = \mathcal{U}_n A B \mathcal{U}_n$, also

$$\mathcal{U}_n A \mathcal{U}_n \cdot \mathcal{U}_n B \mathcal{U}_n = t \mathcal{U}_n A B \mathcal{U}_n$$

für ein $t \in \mathbb{N}$. Sei nun

$$\iota(\mathcal{U}_n A \mathcal{U}_n) = \sum_{i=1}^d \mathcal{U}_n A_i, \quad \iota(\mathcal{U}_n B \mathcal{U}_n) = \sum_{j=1}^{\delta} \mathcal{U}_n B_j.$$

Es genügt zu zeigen, dass die Rechtsnebenklassen $\mathcal{U}_n A_i B_j$ paarweise verschieden sind. Sei nun $U \in \mathcal{U}_n$ mit

$$U A_i B_j = A_k B_l, \quad \text{also} \quad A_k^{-1} U A_i = B_l B_j^{-1}.$$

Die Nenner auf der linken Seite sind Teiler von $\det A$, auf der rechten Seite von $\det B$. Weil die Determinanten teilerfremd sind, sind beide Seiten ganzzahlig und damit unimodular. Dann gilt $\mathcal{U}_n B_l = \mathcal{U}_n B_j$ und $\mathcal{U}_n A_k = \mathcal{U}_n A_i$, also $j = l$ und $i = k$ und somit $t = 1$.

d) Die Behauptung folgt mit der Argumentation in a) aus (1.10). $\square$

Nun betrachten wir

$$\mathcal{T}_n(l) := \sum_{A: \mathcal{U}_n \backslash \mathcal{D}_n(l) / \mathcal{U}_n} \mathcal{U}_n A \mathcal{U}_n, \quad l \in \mathbb{N}.$$

Weil die Elementarteilmatrizen mit Determinante kl , wobei $k, l \in \mathbb{N}$ teilerfremd sind, sich eindeutig als Produkte von Elementarteilmatrizen mit Determinante k und l schreiben lassen, impliziert (3.5) das

(3.6) Korollar. Für teilerfremde $k, l \in \mathbb{N}$ gilt

$$\mathcal{T}_n(k) \cdot \mathcal{T}_n(l) = \mathcal{T}_n(kl).$$

Analoges gilt natürlich, wenn wir k als Produkt von Primzahlpotenzen schreiben. Sei dazu

$$\mathcal{D}_{n,p} := \bigcup_{\nu=0}^{\infty} \mathcal{D}_n(p^\nu), \quad p \in \mathbb{P},$$

$$\mathcal{H}_{n,p} := \mathcal{H}(\mathcal{U}_n, \mathcal{D}_{n,p}).$$

$\mathcal{H}_{n,p}$ heißt p -primäre Komponente von $\mathcal{H}_n$.

(3.7) Korollar. Der Hecke-Ring $\mathcal{H}_n$ ist das Tensorprodukt der p -primären Komponenten

$$\mathcal{H}_n = \bigotimes_{p \in \mathbb{P}} \mathcal{H}_{n,p}.$$

Beweis. Eine Basis von $\mathcal{H}_n$ bzw. $\mathcal{H}_{n,p}$ wird gegeben durch Doppelnebenklassen, die jeweils eindeutige Vertreter in Elementarteilerform besitzen. Jede solche Matrix kann als Produkt von Elementarteilmatrizen in $\mathcal{D}_{n,p}$ geschrieben werden. Dann folgt die Behauptung aus (3.5). $\square$

Nun beschäftigen wir uns mit $\mathcal{H}_{n,p}$, $p \in \mathbb{P}$. Jede Doppelnebenklasse $\mathcal{U}_n A \mathcal{U}_n$, $A \in \mathcal{D}_{n,p}$, hat einen eindeutigen Vertreter

$$E(A) = \text{diag}(p^{k_1}, \dots, p^{k_n}), \quad 0 \leq k_1 \leq \dots \leq k_n.$$

Für $0 \leq j \leq n$ betrachten wir die Doppelnebenklassen

$$\mathcal{T}_{n,j} := \mathcal{T}_{n,j}(p) = \mathcal{U}_n \text{diag}(\underbrace{1, \dots, 1}_{n-j}, \underbrace{p, \dots, p}_j) \mathcal{U}_n.$$

Insbesondere gilt

$$\mathcal{T}_{n,0}(p) = \mathcal{U}_n, \quad \mathcal{T}_{n,n}(p) = \mathcal{U}_n(pE) \mathcal{U}_n.$$

Für eine ganzzahlige Matrix A sei

$$r_p(A) = \text{Rang } A \text{ über } \mathbb{Z}/p\mathbb{Z}.$$

Offenbar gilt

$$r_p(UAV) = r_p(A) \quad \text{für alle } U, V \in \mathcal{U}_n.$$

Wegen der eindeutigen Vertreter liefert eine Verifikation das

(3.8) Lemma. Für $A \in M(n; \mathbb{Z})$ und $0 \leq j \leq n$ sind äquivalent

(i) $A \in \mathcal{T}_{n,j}(p).$

(ii) $r_p(A) = n - j$ und $\det A = p^j.$

Wir bezeichnen das j -te elementarsymmetrische Polynom in $X_1, \dots, X_n$ mit

$$S_j(X_1, \dots, X_n) = S_j^{(n)}(X_1, \dots, X_n) = \sum_{1 \leq \nu_1 < \dots < \nu_j \leq n} X_{\nu_1} \cdot \dots \cdot X_{\nu_j}$$

$$S_0(X_1, \dots, X_n) := 1, \quad S_1(X_1, \dots, X_n) = X_1 + \dots + X_n,$$

$$S_n(X_1, \dots, X_n) = X_1 \cdot \dots \cdot X_n.$$

(3.9) Proposition. Für $0 \leq j \leq n$ wird ein Vertretersystem der Rechtsnebenklassen von $\mathcal{T}_{n,j}(p)$ bezüglich $\mathcal{U}_n$ gegeben durch

$$(*) \quad A = \begin{pmatrix} p^{k_1} & & a_{\nu\mu} \\ & \ddots & \\ 0 & & p^{k_n} \end{pmatrix}$$

mit den Eigenschaften

(i) $k_\nu \in \{0, 1\}$, $\nu = 1, \dots, n$,

$$(ii) \quad k_1 + \dots + k_n = j,$$

$$(iii) \quad 0 \leq a_{\mu\nu} < p^{k_\nu(1-k_\mu)} \text{ für } 1 \leq \mu < \nu \leq n.$$

Insbesondere gilt

$$\text{ind } \mathcal{T}_{n,j}(p) = p^{-j(j+1)/2} S_j(p, p^2, \dots, p^n).$$

Beweis. Wenn A die Bedingungen (i) - (iii) erfüllt, gilt $\det A = p^j$ und $r_p(A) = n - j$, also $A \in \mathcal{T}_{n,j}(p)$ nach (3.8). Die Vertreter gehören nach (3.1) zu paarweise verschiedenen Rechtsnebenklassen bezüglich $\mathcal{U}_n$. Nun wählt man umgekehrt einen Vertreter A von $\mathcal{U}_n \setminus \mathcal{T}_{n,j}(p)$ in der Form (3.1). Dann hat A die Form (*) mit $0 \leq a_{\mu\nu} < p^{k_\nu}$. Nun folgt (ii) aus der Berechnung der Determinante. Weil pA^{-1} wieder ganzzahlig ist, erhält man (i).

Um (iii) zu beweisen, nehmen wir an, dass ein Paar (μ, ν) existiert mit

$$a_{\mu\nu} \neq 0, \quad k_\mu = k_\nu = 1, \quad 1 \leq \mu < \nu \leq n.$$

Damit gibt es aber mindestens $n - j + 1$ über $\mathbb{Z}/p\mathbb{Z}$ linear unabhängige Zeilen in A , nämlich diejenigen $n - j$ mit $k_l = 0$ sowie die μ -te Zeile. Das widerspricht (3.8).

Sind $k_1, \dots, k_n$ fixiert, so gibt es also

$$\prod_{1 \leq \mu < \nu \leq n} p^{k_\nu(1-k_\mu)}$$

Möglichkeiten für A . Wegen $k_\nu^2 = k_\nu$ folgt daraus

$$\frac{1}{2}j(j+1) = \frac{1}{2} \left(\sum_{\nu=1}^n k_\nu \right) \left(1 + \sum_{\mu=1}^n k_\mu \right) = \sum_{\nu=1}^n k_\nu + \sum_{1 \leq \mu < \nu \leq n} k_\mu k_\nu.$$

Das führt zu

$$p^{-j(j+1)/2} \prod_{\nu=1}^n p^{\nu k_\nu} = \prod_{1 \leq \mu < \nu \leq n} p^{k_\nu(1-k_\mu)}.$$

Schließlich beachte man

$$\begin{aligned} \text{ind } \mathcal{T}_{n,j}(p) &= p^{-j(j+1)/2} \sum_{\substack{(k_1, \dots, k_n) \in \{0,1\}^n \\ k_1 + \dots + k_n = j}} p^{k_1} p^{2k_2} \dots p^{nk_n} \\ &= p^{-j(j+1)/2} S_j(p, p^2, \dots, p^n). \end{aligned} \quad \square$$

Wir beachten, dass $\mathcal{H}_{n,p}$ ein $\mathbb{Z}$ -graduierter Ring ist, d. h.

$$\mathcal{H}_{n,p} = \bigoplus_{k=0}^{\infty} \mathcal{H}_{n,p}^{(k)}, \quad \mathcal{H}_{n,p}^{(k)} = \left\{ \sum_{A: \mathcal{U}_n \setminus \mathcal{D}_n(p^k)/\mathcal{U}_n} t(\mathcal{U}_n A \mathcal{U}_n) \mathcal{U}_n A \mathcal{U}_n; t(\mathcal{U}_n A \mathcal{U}_n) \in \mathbb{Z} \right\}.$$

Das bedeutet

$$\begin{aligned}\mathcal{H}_{n,p}^{(0)} &= \mathcal{U}_n = \mathcal{T}_{n,0}(p), & \mathcal{H}_{n,p}^{(1)} &= \mathbb{Z}\mathcal{T}_{n,1}(p), \\ \mathcal{H}_{n,p}^{(k)} \cdot \mathcal{H}_{n,p}^{(l)} &\subset \mathcal{H}_{n,p}^{(k+l)}.\end{aligned}$$

(3.10) Proposition. $\mathcal{H}_{n,p}$ wird erzeugt von den Doppelnebenklassen

$$\mathcal{T}_{n,0}(p), \mathcal{T}_{n,1}(p), \dots, \mathcal{T}_{n,n}(p).$$

Beweis. Sei $\mathcal{A}$ der von den angegebenen Elementen erzeugte Unterring von $\mathcal{H}_{n,p}$. Wir zeigen durch Induktion nach k , dass

$$\mathcal{H}_{n,p}^{(k)} \subset \mathcal{A},$$

wobei der Induktionsanfang $k = 0$ sowie $k = 1$ klar ist. Ist $k \geq 2$, so zeigen wir sukzessiv

$$\mathcal{H}_{n,p}^{(k,r)} = \left\{ \sum_{\substack{A \cdot \mathcal{U}_n \setminus \mathcal{D}_n(p^k)/\mathcal{U}_n \\ r_p(A)=r}} t(\mathcal{U}_n A \mathcal{U}_n) \mathcal{U}_n A \mathcal{U}_n; t(\mathcal{U}_n A \mathcal{U}_n) \in \mathbb{Z} \right\} \subset \mathcal{A}.$$

Ist $\mathcal{U}_n A \mathcal{U}_n \in \mathcal{H}_{n,p}^{(k,r)}$, so wählen wir einen Vertreter

$$A = \text{diag}(p^{k_1}, \dots, p^{k_n}), \quad 0 = k_1 = \dots = k_r < k_{r+1} \leq \dots \leq k_n, \quad k_1 + \dots + k_n = k.$$

Ist $r = 0$, so gilt $k_1 \geq 1$ und

$$T := \mathcal{U}_n \left(\frac{1}{p} A \right) \mathcal{U}_n \in \mathcal{H}_{n,p}^{(k-n)} \subset \mathcal{A}$$

sowie

$$T \cdot \mathcal{T}_{n,n}(p) = \mathcal{U}_n A \mathcal{U}_n$$

wegen $\mathcal{T}_{n,n}(p) = \mathcal{U}_n(pE)\mathcal{U}_n$ und (3.5). Der Fall $r = n$ führt auf $k = 0$.

Sei also $0 < r < n$ und

$$T := \mathcal{U}_n \text{diag}(1, \dots, 1, p^{k_{r+1}-1}, \dots, p^{k_n-1}) \mathcal{U}_n \in \mathcal{H}_{n,p}^{(k+r-n)} \subset \mathcal{A}.$$

Wir berechnen

$$T \cdot \mathcal{T}_{n,n-r} = \sum_{B: \mathcal{U}_n \setminus \mathcal{D}_n(p^k)/\mathcal{U}_n} t(\mathcal{U}_n B \mathcal{U}_n) \mathcal{U}_n B \mathcal{U}_n \in \mathcal{H}_{n,p}^{(k)}.$$

Zunächst impliziert $t(\mathcal{U}_n B \mathcal{U}_n) \neq 0$ bereits $r_p(B) \leq r$ nach (3.8), da der Rang bei einem Produkt von Matrizen nicht größer werden kann. Betrachtet man $\mathcal{U}_n B \mathcal{U}_n \in \mathcal{H}_{n,p}^{(k,r)}$ mit einem Vertreter

$$B = \text{diag}(1, \dots, 1, p^{l_{r+1}}, \dots, p^{l_n}), \quad 1 \leq l_{r+1} \leq \dots \leq l_n, \quad l_{r+1} + \dots + l_n = k,$$

und wählt man die Vertreter C von $\mathcal{U}_n \setminus \mathcal{T}_{n,n-r}$ nach (3.9), so ist $t(\mathcal{U}_n B \mathcal{U}_n)$ die Anzahl dieser C 's mit der Eigenschaft

$$BC^{-1} \in T.$$

Aber die Wahl von B impliziert, dass nur die Möglichkeit

$$C = \text{diag}(\underbrace{1, \dots, 1}_{n-r}, \underbrace{p, \dots, p}_r)$$

verbleibt. Es folgt

$$T \cdot \mathcal{T}_{n,n-r} = T_1 + \mathcal{U}_n A \mathcal{U}_n, \quad T_1 \in \bigoplus_{l=0}^{r-1} \mathcal{H}_{n,p}^{(k,l)}.$$

Mit der Induktionsvoraussetzung erhält man $\mathcal{A} = \mathcal{H}_{n,p}$. □

Die Strukturaussage folgt aus dem

(3.11) Satz. $\mathcal{H}_{n,p}$ ist der Polynomring über $\mathbb{Z}$ in den n Elementen

$$\mathcal{T}_{n,1}(p), \dots, \mathcal{T}_{n,n}(p),$$

die algebraisch unabhängig sind. Insbesondere enthält $\mathcal{H}_n$ keine Nullteiler.

Beweis. (3.10) impliziert

$$\mathcal{H}_{n,p} = \mathbb{Z}[\mathcal{T}_{n,1}(p), \dots, \mathcal{T}_{n,n}(p)].$$

Aus der Elementarteilergestalt folgert man, dass die Anzahl der Doppelnebenklassen in $\mathcal{D}_n(p^k)$

$$\#\{(k_1, \dots, k_n) \in \mathbb{N}_0^n; 0 \leq k_1 \leq \dots \leq k_n, k_1 + \dots + k_n = k\} = p_n(k)$$

ist, wobei $p_n(k)$ die Anzahl der Partitionen von k in höchstens n Summanden ist. Ein Monom

$$\mathcal{T}_{n,1}^{l_1} \cdot \dots \cdot \mathcal{T}_{n,n}^{l_n}$$

gehört aber genau dann zu $\mathcal{H}_{n,p}^{(k)}$, wenn

$$l_1 + 2l_2 + \dots + nl_n = k.$$

Aus der Elementaren Zahlentheorie weiß man, dass auch diese Zahl gleich $p_n(k)$ ist. Man erhält eine Bijektion durch

$$(k_1, \dots, k_n) \mapsto (l_1, \dots, l_n), \quad l_i := \#\{j; k_j = i\}.$$

Also sind die Monome linear unabhängig (über $\mathbb{Z}$) und $\mathcal{T}_{n,1}, \dots, \mathcal{T}_{n,n}$ somit algebraisch unabhängig. □

Daraus ergibt sich auch sofort die Struktur des größeren Hecke-Ring

$$\begin{aligned}\tilde{\mathcal{H}}_n &= \mathcal{H}(\mathcal{U}_n, \mathrm{GL}(n; \mathbb{Q})) = \bigotimes_{p \in \mathbb{P}} \tilde{\mathcal{H}}_{n,p}, \\ \tilde{\mathcal{H}}_{n,p} &= \mathbb{Z}[\mathcal{T}_{n,1}(p), \dots, \mathcal{T}_{n,n}(p), \mathcal{T}_{n,n}(p)^{-1}].\end{aligned}$$

Mit etwas mehr Aufwand als im Fall $n = 2$ erhält man den

(3.12) Satz. *Ist p eine Primzahl, so gilt*

$$\mathcal{H}_{n,p} \otimes \mathbb{Q} = \mathbb{Q}[\mathcal{T}_n(p), \mathcal{T}_n(p^2), \dots, \mathcal{T}_n(p^n)].$$

§4. Der Hecke-Ring zur Siegelschen Modulgruppe

Für $q \in \mathbb{N}$ definieren wir

$$\Delta_n(q) := \{M \in M(2n; \mathbb{Z}); J[M] = qJ\}, \quad \Delta_n(1) = \Gamma_n.$$

Für $M \in \Delta_n(q)$ gilt

$$\frac{1}{\sqrt{q}} M \in \mathrm{Sp}(n; \mathbb{R}),$$

woraus wir die entsprechenden Grundgleichungen gemäß I(3.2) ableiten können. Offenbar gilt

$$\Delta_n(q) \cdot \Delta_n(r) \subset \Delta_n(qr),$$

so dass

$$\Delta_n := \bigcup_{q=1}^{\infty} \Delta_n(q)$$

ein Γ_n umfassendes Monoid ist. Die von Δ_n erzeugte Gruppe ist

$$\begin{aligned}\overline{\Delta}_n &= \{\tfrac{1}{r}M; M \in \Delta_n, r \in \mathbb{N}\} \\ &= \{M \in M(2n; \mathbb{Q}); J[M] = \nu J \text{ für ein } \nu \in \mathbb{Q}, \nu > 0\} \supset \mathrm{Sp}(n; \mathbb{Q}),\end{aligned}$$

die Gruppe der rationalen symplektischen Ähnlichkeitsmatrizen.

(4.1) Satz. *(Symplektischer Elementarteilersatz)*

Zu $M \in \Delta_n(q)$ gibt es $K, L \in \Gamma_n$ sowie eindeutig bestimmte Zahlen $a_1, \dots, a_n, d_1, \dots, d_n \in \mathbb{N}$, so dass $a_j d_j = q$, $j = 1, \dots, n$ und

$$KML = \mathrm{diag}(a_1, \dots, a_n, d_1, \dots, d_n), \quad a_1 \mid a_2 \mid \dots \mid a_n \mid d_n \mid d_{n-1} \mid \dots \mid d_1.$$

Beweis. Wir verwenden eine Induktion nach n , wobei der Fall $n = 1$ wegen

$$\Delta_1(q) = \{M \in M(2; \mathbb{Z}); \det M = q\}$$

aus (2.1) folgt. Sei also $n > 1$.

Sei $\mathcal{M}$ die Menge aller positiven Koeffizienten von Matrizen, die in $\Gamma_n M \Gamma_n$ auftreten. Wegen $-E \in \Gamma_n$ ist $\mathcal{M} \neq \emptyset$. Sei

$$a := \min \mathcal{M}.$$

Weil man mit J von rechts und/oder links multiplizieren darf, darf man $a \in A$ annehmen. Dann gilt $a = \text{ggT}(a_{ij})$ nach (3.1) und Definition von A . Multipliziert man mit Matrizen der Form $\begin{pmatrix} U^{tr} & 0 \\ 0 & U^{-1} \end{pmatrix}$, $U \in \mathcal{U}_n$, von rechts und links, so darf man von

$$A = \begin{pmatrix} a & 0 \\ 0 & * \end{pmatrix}$$

ausgehen. Nun multipliziert man von rechts mit $\begin{pmatrix} E & S \\ 0 & E \end{pmatrix}$ und von links mit $\begin{pmatrix} E & 0 \\ T & E \end{pmatrix}$, wobei S und T die Form

$$\begin{pmatrix} x_1 & x_2 & \cdots & x_n \\ x_2 & & & \\ \vdots & & 0 & \\ x_n & & & \end{pmatrix} \in \text{Sym}(n; \mathbb{Z})$$

haben. Man wählt $x_i \in \mathbb{Z}$, so dass

$$0 \leq ax_i + m_{n+i,1} < a \quad \text{bzw.} \quad 0 \leq ax_i + m_{1,n+i} < a$$

gilt. Nach Wahl von a sind diese Elemente 0. Also hat M dann die Form

$$\begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & * & & \\ 0 & & & \end{pmatrix}.$$

Nun wendet man die Grundgleichungen I(3.2) auf $\frac{1}{\sqrt{q}} M$ an und erhält

$$M = \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \times M_1, \quad ad = q, \quad M_1 \in \Delta_{n-1}(q).$$

Betrachtet man

$$\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \times E \right) \cdot M = \begin{pmatrix} a & d \\ 0 & d \end{pmatrix} \times M_1,$$

so liefert der obige Schritt $a \mid d$. Nach Induktionsvoraussetzung gibt es $K_1, L_1 \in \Gamma_{n-1}$, so dass

$$(E \times K_1)M \cdot (E \times L_1) = \text{diag}(a, a_2, \dots, a_n, d, d_2, \dots, d_n),$$

$$a_i d_i = q, \quad i = 1, \dots, n, \quad a_2 \mid \dots \mid a_n \mid d_n \mid \dots \mid d_2.$$

Weil a_2 im A -Block einer Matrix in $\Gamma_n M \Gamma_n$ auftritt, liefert der obige Schritt $a \mid a_2$ und $a \mid d$ impliziert dann $d_2 \mid d$. Weil $a_1, \dots, a_n, d_n, \dots, d_1$ die Elementarteiler von M sind, sind sie nach (3.1) eindeutig bestimmt. $\square$

Das letzte Argument führt unmittelbar auf das

(4.2) Korollar. Für $M, N \in \Delta_n$ sind äquivalent:

- (i) $\Gamma_n M \Gamma_n = \Gamma_n N \Gamma_n$.
- (ii) $\mathcal{U}_{2n} M \mathcal{U}_{2n} = \mathcal{U}_{2n} N \mathcal{U}_{2n}$.

Nun kümmern wir uns um Vertreter von Rechtsnebenklassen.

(4.3) Lemma. Zu jedem $0 \neq g \in \mathbb{Z}^{2n}$ existiert ein $M \in \Gamma_n$ mit

$$Mg = (\delta, 0, \dots, 0)^{tr}, \quad \delta = \text{ggT}(g).$$

Beweis. Zunächst wählt man ein $U \in \mathcal{U}_n$, so dass

$$g' = \begin{pmatrix} U^{tr} & 0 \\ 0 & U^{-1} \end{pmatrix} g = (a_1, \dots, a_n, c, 0, \dots, 0)^{tr}.$$

Nun wählt man ein $V \in \text{SL}(2; \mathbb{Z})$ mit

$$V \begin{pmatrix} a_1 \\ c \end{pmatrix} = \begin{pmatrix} \alpha \\ 0 \end{pmatrix}, \quad \text{also } b := (V \times E) \quad g' = (\alpha, a_2, \dots, a_n, 0, \dots, 0)^{tr}.$$

Durch Multiplikation mit einer Matrix $\begin{pmatrix} W^{tr} & 0 \\ 0 & W^{-1} \end{pmatrix}$, $W \in \mathcal{U}_n$, kommt man dann auf die gewünschte Gestalt, wobei $\delta = \text{ggT}(g)$ wegen $\Gamma_n \subset \mathcal{U}_{2n}$ aus (3.1) folgt. $\square$

Mit einer Induktion kommt man auf

(4.4) Lemma. Für $M \in \Delta_n$ enthält $\Gamma_n M$ einen Vertreter

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix},$$

wobei A [oder D] obere Dreiecksgestalt hat.

Beweis. Nach (4.3) darf man davon ausgehen, dass αe_1 die erste Spalte von M ist. Dann ist man fertig für $n = 1$. Sei $n > 1$. Nach den Grundgleichungen I(3.2) angewandt auf $\frac{1}{\sqrt{q}} M$ für $M \in \Delta_n(q)$ hat man dann

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad A = \begin{pmatrix} \alpha & 0 \\ 0 & A_1 \end{pmatrix}, \quad B = \begin{pmatrix} * & * \\ * & B_1 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 \\ 0 & C_1 \end{pmatrix},$$

$$D = \begin{pmatrix} \delta & 0 \\ * & D_1 \end{pmatrix}, \quad \alpha \delta = q, \quad M_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \in \Delta_{n-1}(q).$$

Nach Induktionsvoraussetzung existiert ein $K_1 \in \Gamma_{n-1}$, so dass $K_1 M_1$ die gewünschte Gestalt hat. Man erhält die Behauptung durch Multiplikation mit $E \times K_1$. Der zweite Teil ergibt sich durch Multiplikation mit $\begin{pmatrix} U^{tr} & 0 \\ 0 & U^{-1} \end{pmatrix}$, $U \in \mathcal{U}_n$, aus (3.1). $\square$

Für $M \in \Delta_n(q)$ betrachten wir die nach (4.4) nicht-leere Menge von Matrizen in $\Gamma_n M \Gamma_n$, deren C-Block 0 ist, also

$$\begin{aligned} \mathcal{D}(\Gamma_n M \Gamma_n) &:= \{D \in M(n \times n; \mathbb{Z}); \text{ es existiert } \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Gamma_n M \Gamma_n\} \\ &\subset \{G \in M(n \times n; \mathbb{Z}); \det G \neq 0, qG^{-1} \in M(n \times n; \mathbb{Z})\}. \end{aligned}$$

Diese Menge zerfällt in endlich viele Doppel- und Rechtsnebenklassen bezüglich $\mathcal{U}_n$. Für $D \in \mathcal{D}(\Gamma_n M \Gamma_n)$ sei

$$\mathcal{B}(D, \Gamma_n M \Gamma_n) = \{B \in M(n \times n; \mathbb{Z}); \text{ es existiert } \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Gamma_n M \Gamma_n\}.$$

Die Grundgleichungen I(3.2) implizieren

$$BD^{-1} \in \text{Sym}(n; \mathbb{Q}) \quad \text{für} \quad \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Delta_n(q).$$

Also existiert auf $\mathcal{B}(D, \Gamma_n M \Gamma_n)$ eine Äquivalenzrelation

$$\begin{aligned} B \equiv B^* \bmod D &\Leftrightarrow (B - B^*)D^{-1} \in \text{Sym}(n; \mathbb{Z}). \\ &\Leftrightarrow \Gamma_{n,0} \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} = \Gamma_{n,0} \begin{pmatrix} A & B^* \\ 0 & D \end{pmatrix}. \end{aligned}$$

(4.5) Lemma. Sei $M \in \Delta_n(q)$, $D \in \mathcal{D}(\Gamma_n M \Gamma_n)$. Für alle $U, V \in \mathcal{U}_n$ gilt

$$\begin{aligned} \sharp(\mathcal{B}(D, \Gamma_n M \Gamma_n) \bmod D) &= \sharp(\mathcal{B}(UDV, \Gamma_n M \Gamma_n) \bmod UDV) \\ &\leq d_1^n d_2^{n-1} \cdot \dots \cdot d_n, \end{aligned}$$

falls $\text{diag}(d_1, \dots, d_n)$ die Elementarteilermatrix von D ist.

Beweis. Es gilt

$$\mathcal{B}(UDV, \Gamma_n M \Gamma_n) = U^{tr-1} \mathcal{B}(D, \Gamma_n M \Gamma_n) V.$$

Für $D = \text{diag}(d_1, \dots, d_n)$ hat man wegen $d_1 \mid \dots \mid d_n$ und $BD^{-1} \in \text{Sym}(n; \mathbb{Q})$

$$\mathcal{B}(D, \Gamma_n M \Gamma_n) \subset \{B = (b_{jk}); b_{jk} \in \mathbb{Z} \text{ für } 1 \leq k \leq j \leq n, b_{jk} = b_{kj} d_k d_j^{-1}, j < k\}.$$

Gemäß Äquivalenzrelation können die $b_{jk} \bmod d_k$ reduziert werden. Die Anzahl dieser Matrizen ist dann $d_1^n d_2^{n-1} \cdot \dots \cdot d_n$. $\square$

Nun beschreiben wir ein Rechtsklassenvertretersystem.

(4.6) Satz. a) Sei $M \in \Delta_n(q)$. Dann wird ein Vertretersystem der Rechtsnebenklassen in $\Gamma_n M \Gamma_n$ gegeben durch

$$N = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \quad A = qD^{tr-1},$$

wobei

- (i) D ein Vertretersystem von $\mathcal{U}_n \backslash \mathcal{D}(\Gamma_n M \Gamma_n)$,
- (ii) B bei gegebenem D ein Vertretersystem von $\text{mod } D$ inkongruenten Matrizen in $\mathcal{B}(D, \Gamma_n M \Gamma_n)$

durchläuft.

b) $\Delta_n(q)$ zerfällt in endlich viele Rechtsnebenklassen bezüglich Γ_n , so dass $(\Gamma_n, \overline{\Delta}_n)$ ein Hecke-Paar ist.

Beweis. a) Die obigen Überlegungen zeigen, dass jede Rechtsnebenklasse einen Vertreter der angegebenen Form enthält. Sind nun Vertreter

$$N = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \quad N^* = \begin{pmatrix} A^* & B^* \\ 0 & D^* \end{pmatrix} \quad \text{mit} \quad \Gamma_n N = \Gamma_n N^*$$

gegeben, so folgt

$$N^* N^{-1} \in \Gamma_n, \quad \text{also} \quad N^* N^{-1} \in \Gamma_{n,0}.$$

Die Beschreibung von $\Gamma_{n,0}$ impliziert $\mathcal{U}_n D = \mathcal{U}_n D^*$, also $D = D^*$, sowie $B^* = B + SD$ für ein $S \in \text{Sym}(n; \mathbb{Z})$, also $S = 0$ und $N = N^*$.

b) Die Menge

$$\{G \in M(n \times n; \mathbb{Z}); \det G \neq 0, qG^{-1} \text{ ganz}\}$$

zerfällt in endlich viele Doppel- und Rechtsnebenklassen bezüglich $\mathcal{U}_n$. Dann folgt die Behauptung aus a) und (4.5). $\square$

Sei nun

$$H_n := \mathcal{H}(\Gamma_n, \Delta_n).$$

Für $M, N \in \Delta_n(q)$ gilt $\det M = q^n$ und nach (4.2)

$$\Gamma_n M = \Gamma_n N \Leftrightarrow \mathcal{U}_{2n} M = \mathcal{U}_{2n} N.$$

Dieselben Argumente wie für (3.5) liefern das

(4.7) Lemma. a) H_n ist ein kommutativer Ring.

b) Für $M \in \Delta_n$ und $0 \neq \lambda \in \mathbb{Z}$ gilt

$$\Gamma_n M \Gamma_n \cdot \Gamma_n(\lambda E) \Gamma_n = \Gamma_n(\lambda M) \Gamma_n.$$

c) Für $M \in \Delta_n(q)$ und $N \in \Delta_n(r)$ mit teilerfremden $q, r \in \mathbb{N}$ gilt

$$\Gamma_n M \Gamma_n \cdot \Gamma_n N \Gamma_n = \Gamma_n (MN) \Gamma_n.$$

d) Für jedes $M \in \Delta_n(q)$ existiert ein simultanes Vertretersystem der Rechts- und Linksnebenklassen in $\Gamma_n M \Gamma_n$.

Für $q \in \mathbb{N}$ setzen wir

$$T_n(q) := \sum_{M: \Gamma_n \backslash \Delta_n(q) / \Gamma_n} \Gamma_n M \Gamma_n.$$

Analog zu (3.6) erhält man das

(4.8) Korollar. Für teilerfremde $q, r \in \mathbb{N}$ gilt

$$T_n(q) \cdot T_n(r) = T_n(qr).$$

Für eine Primzahl p betrachten wir das Monoid

$$\Delta_{n,p} := \bigcup_{l=0}^{\infty} \Delta_n(p^l)$$

und den Unterring

$$H_{n,p} := H(\Gamma_n, \Delta_{n,p}).$$

Man nennt $H_{n,p}$ die p -primäre Komponente von H_n . Wie zuvor folgt der

(4.9) Satz. Der Hecke-Ring H_n ist das Tensorprodukt seiner p -primären Komponenten

$$H_n = \bigotimes_{p \in \mathbb{P}} H_{n,p}.$$

Jede Doppelnebenklasse $\Gamma_n M \Gamma_n \subset \Delta_n(p^l)$ hat einen eindeutigen Vertreter

$$M = \text{diag}(p^{k_1}, \dots, p^{k_n}, p^{l-k_1}, \dots, p^{l-k_n}), \quad 0 \leq k_1 \leq \dots \leq k_n \leq l/2.$$

Also besteht $\Delta_n(p)$ aus einer einzigen Doppelnebenklasse

$$T_n(p) = \Delta_n(p) = \Gamma_n \begin{pmatrix} E & 0 \\ 0 & pE \end{pmatrix} \Gamma_n.$$

Aus obigen Überlegungen folgt mit §3

$$\mathcal{D}(T_n(p)) = \bigcup_{j=0}^n \mathcal{T}_{n,j}(p).$$

Für $D = \begin{pmatrix} E^{(n-j)} & 0 \\ 0 & pE^{(j)} \end{pmatrix}$, $0 \leq j \leq n$ gilt

$$\mathcal{B}(D, T_n(p)) = \left\{ \begin{pmatrix} B_1 & pB_3^{tr} \\ B_3 & B_4 \end{pmatrix}; \begin{matrix} B_1 \in \text{Sym}(n-j; \mathbb{Z}), B_4 \in \text{Sym}(j; \mathbb{Z}) \\ B_3 \in M(j \times (n-j); \mathbb{Z}) \end{matrix} \right\}$$

Repräsentanten von $\mathcal{B}(D, T_n(p))$ werden gegeben durch

$$\begin{pmatrix} 0 & 0 \\ 0 & S \end{pmatrix}, \quad S \in \text{Sym}(j; \mathbb{Z}) \bmod p,$$

also

$$\sharp(\mathcal{B}(D, T_n(p)) \bmod D) = p^{j(j+1)/2} \quad \text{für } D \in \mathcal{T}_{n,j}(p).$$

Aus (3.9) und

$$\sum_{j=0}^n S_j(p, p^2, \dots, p^n) = \prod_{j=1}^n (p^j + 1)$$

ergibt sich das

(4.10) Lemma. Für $p \in \mathbb{P}$ gilt

$$\text{ind } T_n(p) = \prod_{j=1}^n (p^j + 1).$$

Nun betrachten wir $\Delta_n(p^2)$ und erhalten

$$\Delta_n(p^2) = \bigcup_{j=0}^n T_{n,j}(p^2), \quad T_{n,j}(p^2) = \Gamma_n \text{diag}(E^{(n-j)}, pE^{(j)}, p^2 E^{(n-j)}, pE^{(j)}) \Gamma_n.$$

Mit der Bezeichnung des p -Rangs ergibt sich das

(4.11) Lemma. Für $M \in \Delta_n(p^2)$, $p \in \mathbb{P}$, und $0 \leq j \leq n$ gilt

$$M \in T_{n,j}(p^2) \Leftrightarrow r_p(M) = n - j.$$

Damit bekommt man das

(4.12) Lemma. Für $p \in \mathbb{P}$ gilt

$$T_n(p)^2 = T_{n,0}(p^2) + \sum_{j=1}^n (\text{ind } T_j(p)) \cdot T_{n,j}(p^2).$$

Beweis. Es gilt

$$T_n(p)^2 = \sum_{j=0}^n t_j T_{n,j}(p^2),$$

wobei t_j die Anzahl der Repräsentanten $M : \Gamma_n \backslash T_n(p)$ ist mit der Eigenschaft

$$M_j M^{-1} \in M(2n \times 2n; \mathbb{Z}),$$

wenn M_j ein beliebiger, aber fester Vertreter von $T_{n,j}(p^2)$ ist. Wählt man

$$M_j = \text{diag}(p^2 E^{(n-j)}, p E^{(j)}, E^{(n-j)}, p E^{(j)})$$

und wählt man M in der Form (4.6) mit oberer Dreiecksmatrix D , so folgt

$$M = \begin{pmatrix} p E^{(n-j)} & 0 \\ 0 & E \end{pmatrix} \times M_1,$$

wobei M_1 ein Vertretersystem von $\Gamma_j \backslash T_j(p)$ durchläuft, da dann $p M_j^{-1}$ immer ganzzahlig ist. $\square$

Nun betrachten wir die Graduierung

$$H_{n,p} = \bigotimes_{l=0}^{\infty} H_{n,p}^{(l)},$$

$$H_{n,p}^{(l)} := \left\{ \sum_{M: \Gamma_n \backslash \Delta_n(p^l)/\Gamma_n} t(\Gamma_n M \Gamma_n) \Gamma_n M \Gamma_n; t(\Gamma_n M \Gamma_n) \in \mathbb{Z} \right\}.$$

Insbesondere gilt

$$(*) \quad \begin{cases} H_{n,p}^{(0)} = \mathbb{Z} \Gamma_n \\ H_{n,p}^{(1)} = \mathbb{Z} T_n(p) \\ H_{n,p}^{(2)} = \mathbb{Z} T_{n,0}(p^2) + \dots + \mathbb{Z} T_{n,n}(p^2) \\ H_{n,p}^{(k)} \cdot H_{n,p}^{(l)} \subset H_{n,p}^{(k+l)}. \end{cases}$$

(4.13) Proposition. Für eine Primzahl p gilt

$$H_{n,p} = \mathbb{Z}[T_n(p), T_{n,1}(p^2), T_{n,2}(p^2), \dots, T_{n,n}(p^2)].$$

Beweis. Es bezeichne $\mathcal{A}$ den Unterring auf der rechten Seite. Wir zeigen

$$H_{n,p}^{(l)} \subset \mathcal{A} \quad \text{für alle } l \in \mathbb{N}_0$$

durch Induktion nach l , wobei $l = 0, 1, 2$ mit (4.12) und (*) klar sind. Sei $l \geq 3$ und

$$H_{n,p}^{(l,r)} = \left\{ \sum_{\substack{M: \Gamma_n \backslash \Delta_n(p^l)/\Gamma_n \\ r_p(M)=r}} t(\Gamma_n M \Gamma_n) \Gamma_n M \Gamma_n; t(\Gamma_n M \Gamma_n) \in \mathbb{Z} \right\}$$

für $0 \leq r \leq n$. Sei $\Gamma_n M \Gamma_n \in H_{n,p}^{(l,r)}$. Dann kann man M wählen als

$$M = \text{diag}(p^{k_1}, \dots, p^{k_n}, p^{l-k_1}, \dots, p^{l-k_n}), \quad 0 = k_1 = \dots = k_r < k_{r+1} \leq \dots \leq k_n \leq l/2.$$

Im Fall $r = 0$ haben wir $k_1 \geq 1$ und

$$T := \Gamma_n \left(\frac{1}{p} M \right) \Gamma_n \in H_{n,p}^{(l-n)} \subset \mathcal{A}.$$

Mit $T_{n,n}(p^2) = \Gamma_n(pE)\Gamma_n$ und (4.7) folgt

$$\Gamma_n M \Gamma_n = T \cdot T_{n,n}(p^2) \in \mathcal{A}.$$

Sei daher $0 < r \leq n$ und

$$T := \Gamma_n \text{diag}(1, \dots, 1, p^{k_{r+1}-1}, \dots, p^{k_n-1}, p^{l-2}, \dots, p^{l-2}, p^{l-k_{r+1}-1}, \dots, p^{l-k_n-1}) \Gamma_n.$$

Es gilt $T \in \mathcal{A}$ und

$$T \cdot T_{n,n-r}(p^2) = \sum_{N: \Gamma_n \backslash \Delta_n(p^l)/\Gamma_n} t(\Gamma_n N \Gamma_n) \Gamma_n N \Gamma_n \in H_{n,p}^{(l)}.$$

Zunächst impliziert $t(\Gamma_n N \Gamma_n) \neq 0$ sogleich $r_p(N) \leq r$, da der Ring bei einem Produkt von Matrizen nicht größer werden kann. Nun betrachten wir ein N mit $r_p(N) = r$, also ohne Einschränkung

$$N = \text{diag}(p^l, \dots, p^l, p^{l-j_{r+1}}, \dots, p^{l-j_n}, 1, \dots, 1, p^{j_{r+1}}, \dots, p^{j_n})$$

$$1 \leq j_{r+1} \leq \dots \leq j_n \leq l/2.$$

Wir wählen Vertreter K von $\Gamma_n \backslash T_{n,n-r}(p^2)$ in der Form (4.6) mit oberer Dreiecksmatrix D . Dann stimmt $t(\Gamma_n N \Gamma_n)$ mit der Anzahl der K überein, für die

$$NK^{-1} \in T.$$

Man erhält sogleich

$$K = \begin{pmatrix} p^2 E^{(r)} & 0 \\ 0 & E^{(r)} \end{pmatrix} \times K_1, \quad K_1 \in \Delta_{n-r}(p^2).$$

Aber (4.11) impliziert $K_1 = pE$. Es folgt

$$T \cdot T_{n,n-r}(p^2) = T_1 + \Gamma_n M \Gamma_n,$$

$$T_1 \in \bigoplus_{s=0}^{r-1} H_{n,p}^{(l,s)} \subset \mathcal{A}.$$

Also gilt $\mathcal{A} = H_{n,p}$. □

Die Strukturbeschreibung folgt in dem

(4.14) Satz. Für $p \in \mathbb{P}$ ist $H_{n,p}$ der Polynomring über $\mathbb{Z}$ in den $n+1$ Elementen

$$T_n(p), T_{n,1}(p^2), \dots, T_{n,n}(p^2),$$

die algebraisch unabhängig sind. Insbesondere enthält H_n keine Nullteiler.

Beweis. Zu zeigen bleibt die algebraische Unabhängigkeit. Die Anzahl der Doppelnebenklassen in $H_{n,p}^{(l)}$ ist

$$\#\{(k_1, \dots, k_n) \in \mathbb{N}_0^n; 0 \leq k_1 \leq \dots \leq k_n \leq [l/2]\} = \binom{n + [l/2]}{n}.$$

Ein Monom

$$T_n^{m_0} \cdot T_{n,1}^{m_1} \cdot \dots \cdot T_{n,n}^{m_n}$$

gehört genau dann zu $H_{n,p}^{(l)}$, wenn

$$m_0 + 2m_1 + \dots + 2m_n = l.$$

Die gesuchte Anzahl ist somit

$$\#\{(l_0, \dots, l_n) \in \mathbb{N}_0^{n+1}; l_0 + \dots + l_n = [l/2]\} = \binom{n + [l/2]}{n}.$$

Also sind die Monome linear unabhängig über $\mathbb{Z}$ und die Elemente somit algebraisch unabhängig. $\square$

Wegen $T_{n,n}(p^2) = \Gamma_n(pE)\Gamma_n$ ergibt eine einfache Rechnung

$$\mathcal{H}(\Gamma_n, \mathrm{Sp}(n; \mathbb{Q})) = \mathbb{Z}[T_{n,0}(p^2)T_{n,n}(p^2)^{-1}, \dots, T_{n,n-1}(p^2)T_{n,n}(p^2)^{-1}].$$

Zum Abschluss dieses Paragraphen wollen wir die Vertauschungsrelation zwischen Hecke-Operatoren und dem Siegelschen ϕ -Operator beweisen. Dazu sei

$$\tilde{H}_n = H_n \otimes_{\mathbb{Z}} \mathbb{Q}, \quad \tilde{R}_n = \mathcal{R}(\Gamma_n, \Delta_n) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Für $n > 1$ und jede Rechtsnebenklasse $\Gamma_n M \subset \Delta_n(q)$ wählen wir einen Vertreter M mit $(0, \dots, 0, *)$ als letzter Zeile. Nach den Grundgleichungen I(3.2) bedeutet das

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}, \quad A = \begin{pmatrix} A_1 & 0 \\ a^{tr} & \alpha \end{pmatrix}, \quad B = \begin{pmatrix} B_1 & * \\ * & * \end{pmatrix}, \quad C = \begin{pmatrix} C_1 & 0 \\ 0 & 0 \end{pmatrix},$$

$$D = \begin{pmatrix} D_1 & d \\ 0 & \delta \end{pmatrix}, \quad M_1 = \begin{pmatrix} A_1 & B_1 \\ C_1 & D_1 \end{pmatrix} \in \Delta_{n-1}(q), \quad \alpha\delta = q.$$

Für gerades $k \in \mathbb{Z}$ sei nun

$$\phi_k(\Gamma_n M) := \delta^{-k} \Gamma_{n-1} M_1 \in \widetilde{R}_{n-1}.$$

Diese Abbildung ist wohldefiniert, da für $M \in \Gamma_{n,n-1}$ stets $\delta = \pm 1$ gilt. Die Abbildung wird linear auf $\widetilde{R}_n$ fortgesetzt. Multiplikation mit Matrizen $K_1 \times E$, $K_1 \in \Gamma_{n-1}$, von rechts impliziert

$$\phi_k(\widetilde{R}_n^{\Gamma_n}) \subset R_{n-1}^{\Gamma_{n-1}}, \quad \text{also} \quad \phi_k(\widetilde{H}_n) \subset \widetilde{H}_{n-1}.$$

Die Definition der Abbildung führt direkt auf

$$\phi_k(T * S) = \phi_k(T) * \phi_k(S) \quad \text{für } T \in \widetilde{H}_n, S \in \widetilde{R}_n.$$

Also ist ϕ_k ein Homomorphismus der $\mathbb{Q}$ -Algebren.

(4.15) Satz. Sei $p \in \mathbb{P}$, $n \in \mathbb{N}$, $n > 1$ und $k \in \mathbb{Z}$ gerade. Dann gilt

a) $\phi_k(T_n(p)) = (p^{n-k} + 1)T_{n-1}(p).$

b) $\phi_r(T_{n,j}(p)) = \sum_{\substack{i=j-1, j, j+1 \\ 0 \leq i \leq n-1}} t_i T_{n-1,i}(p)$

für $0 \leq j \leq n$, wobei

$$t_{j-1} = p^{n-j-k}, \quad t_j = 1 + (p-1)p^{n-j-1-k}, \quad t_{j+1} = (p^{2j+2} - 1)p^{n-j-1-k}.$$

Beweis. a) Vertreter der Rechtsnebenklassen $\Gamma_n M \subset \Delta_n(p)$, für die $\phi_k(\Gamma_n M)$ ein Vielfaches von $\Gamma_{n-1} \begin{pmatrix} E & 0 \\ 0 & pE \end{pmatrix}$, $E = E^{(n-1)}$, ist werden gemäß (4.6) gegeben durch

$$M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \quad A = pD^{tr-1}$$

$$D = \begin{pmatrix} pE & 0 \\ 0 & 1 \end{pmatrix}, \quad B = 0, \quad D = \begin{pmatrix} pE & 0 \\ 0 & p \end{pmatrix}, \quad B = \begin{pmatrix} 0 & b \\ b^{tr} & \beta \end{pmatrix}, \quad \begin{pmatrix} b \\ \beta \end{pmatrix} \in \mathbb{Z}^n \bmod p.$$

Damit kommt man direkt auf die Behauptung.

b) Sei $0 \leq r \leq n-1$, $s = n-1-r$ und

$$N = \text{diag}(E^{(r)}, pE^{(s)}, pE^{(r)}, p^2E^{(s)}) \in \Delta_{n-1}(p^2).$$

Nun bestimmen wir alle Rechtsnebenklassen $\Gamma_n M \subset \Delta_n(p^2)$, für die $\phi_k(\Gamma_n M)$ ein Vielfaches von $\Gamma_{n-1} N$ ist. Die Form der letzten Spalte von D ergibt sich aus $A = p^2 D^{tr-1} \in M(n \times n; \mathbb{Z})$. Ein Vertretersystem wird gegeben durch

$$M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \quad A = p^2 D^{tr-1},$$

wobei

$$(1) \quad D = \text{diag}(p^2 E^{(r)}, p E^{(s)}, 1), \quad B = 0,$$

$$(2) \quad D = \begin{pmatrix} p^2 E & 0 & 0 \\ 0 & p E & d \\ 0 & 0 & p \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & b_1 \\ 0 & 0 & b_2 \\ p b_1^{tr} & b_2^{tr} & \beta \end{pmatrix}, \quad \begin{matrix} b_1 \in \mathbb{Z}^r \bmod p, \beta \in \mathbb{Z} \bmod p \\ b_2, d \in \mathbb{Z}^s \bmod p \end{matrix},$$

$$(3) \quad D = \begin{pmatrix} p^2 E & 0 & 0 \\ 0 & p E & p d \\ 0 & 0 & p^2 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & b_1 \\ 0 & 0 & p b_2 \\ p b_1^{tr} & b_2^{tr} & \beta \end{pmatrix}, \quad \begin{matrix} b_1 \in \mathbb{Z}^r \bmod p^2, \beta \in \mathbb{Z} \bmod p^2 \\ b_2, d \in \mathbb{Z}^s \bmod p \end{matrix}.$$

Mit Hilfe von (4.11) verifiziert man, dass die Matrix (1) und die p^{2n} Matrizen (3) zu $T_{n,s}(p^2)$ gehören. In (2) gehören die p^r Matrizen mit $(d^{tr}, b_2^{tr}, \beta) \equiv 0 \bmod p$ zu $T_{n,s+1}(p)$. Alle $p^r(p-1)$ Matrizen mit $(d^{tr}, b_2^{tr}) \equiv 0 \bmod p$ und $\beta \not\equiv 0 \bmod p$ sind in $T_{n,s}(p^2)$ enthalten. Die verbleibenden $(p^{2s}-1)p^{r+1}$ Matrizen mit $(d^{tr}, b_2^{tr}) \not\equiv 0 \bmod p$ gehören zu $T_{n,s-1}(p^2)$.

Mit (1), (2), (3) haben wir somit das Urbild $\phi_k^{-1}(\Gamma_{n-1}N)$ beschrieben. Nun folgt daraus die Behauptung durch Berechnung der entsprechenden Koeffizienten. $\square$

Mit (4.9) und (4.13) ergibt sich daraus das

(4.16) Korollar. Für jedes gerade $k \in \mathbb{N}$ und $n > 1$ ist der Algebrenhomomorphismus

$$\phi_k : \tilde{H}_n \rightarrow \tilde{H}_{n-1}$$

surjektiv.

§5. Hecke-Operatoren für Siegelsche Modulformen

Wir beschreiben nun die Operation des Hecke-Rings H_n aus §4 auf dem Vektorraum $\mathcal{M}_k(\Gamma_n)$ der Siegelschen Modulformen vom Grad n und Gewicht k . Für $M \in \Delta_n(l)$ und $f \in \mathcal{M}_k(\Gamma_n)$ sei

$$f \Big|_k \Gamma_n M \Gamma_n := \sum_{K: \Gamma_n \backslash \Gamma_n M \Gamma_n} f \Big|_k K.$$

Wegen $f \Big|_k L = f$ für alle $L \in \Gamma_n$ ist die Abbildung wohldefiniert und das Bild wieder holomorph auf $\mathcal{H}_n$ und invariant unter Γ_n . Diese Definition wird linear auf H_n fortgesetzt. Man nennt die Abbildungen

$$f \mapsto f \Big|_k \mathcal{T}, \quad \mathcal{T} \in H_n,$$

Hecke-Operatoren.

(5.1) Satz. Die Abbildung

$$H_n \rightarrow \text{End } \mathcal{M}_k(\Gamma_n), \quad \mathcal{T} \mapsto (f \mapsto f|_k \mathcal{T}),$$

ist ein Ringhomomorphismus. Jeder Hecke-Operator bildet Spitzenformen auf Spitzenformen ab. Für $M \in \Delta_n(l)$ und $f \in \mathcal{M}_k(\Gamma_n)$ gilt

$$g(Z) = f|_k \Gamma_n M \Gamma_n(Z) = \sum_{R \in \Lambda_n, R \geq 0} \alpha_g(R) e^{\pi i \text{Sp}(RZ)},$$

$$\alpha_g(R) = \sum_{\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} : \Gamma_n \backslash \Gamma_n M \Gamma_n} (\det D)^{-k} \alpha_f\left(\frac{1}{l} R[D^{tr}]\right) e^{\pi i \text{Sp}(RD^{tr}B)/l},$$

wenn man $\alpha_f(T) = 0$ für $T \notin \Lambda_n$ setzt.

Beweis. Wenn man für $n = 1$ zusätzlich (2.11) verwendet, folgt $f|_k \mathcal{T} \in \mathcal{M}_k(\Gamma_n)$ aus den obigen Überlegungen. Dass die Abbildung ein Ringhomomorphismus ist, zeigt man wörtlich wie in (2.11). Wir berechnen

$$g(Z) = \sum_{\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} : \Gamma_n \backslash \Gamma_n M \Gamma_n} \sum_{T \in \Lambda_n, T \geq 0} (\det D)^{-k} \alpha_f(T) e^{\pi i \text{Sp}(T(AZ+B)D^{-1})}$$

$$= \sum_{R \in \Lambda_n, R \geq 0} \alpha_g(R) e^{\pi i \text{Sp}(RZ)},$$

wobei wir aus $R = D^{-1}TA$ mit den Grundgleichungen I(3.2) sofort

$$T = DRA^{-1} = \frac{1}{l} R[D^{tr}]$$

und damit

$$\alpha_g(R) = \sum_{\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}} (\det D)^{-k} \alpha_f\left(\frac{1}{l} R[D^{tr}]\right) e^{\pi i \text{Sp}(RD^{tr}B)/l}$$

erhalten. Treten in der Fourier-Entwicklung von f nur positiv definite Matrizen auf, so auch in der von g . Also werden Spitzenformen auf Spitzenformen abgebildet. $\square$

Eine einfache Folgerung aus der Formel für die Fourier-Entwicklung ist das

(5.2) Korollar. Sei $M \in \Delta_n(l)$ und $f \in \mathcal{M}_k(\Gamma_n)$ mit

$$f|_k \Gamma_n M \Gamma_n = \lambda f.$$

Gilt $\alpha_f(0) \neq 0$, so hat man

$$\lambda = \sum_{\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} : \Gamma_n \backslash \Gamma_n M \Gamma_1} (\det D)^{-k}.$$

Im Fall $\Gamma_n M \Gamma_n = T_n(p)$, $p \in \mathbb{P}$, gilt in diesem Fall speziell

$$\lambda = \prod_{j=1}^n (p^{j-k} + 1).$$

Beweis. Man berechnet

$$\alpha_g(0) = \sum_{\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} : \Gamma_n \backslash \Gamma_n M \Gamma_1} (\det D)^{-k} \alpha_f(0)$$

aus (5.1). Für den Zusatz verwende man den Beweis von (4.10). $\square$

Wir nennen $0 \neq f \in \mathcal{M}_k(\Gamma_n)$ wieder eine *simultane Hecke-Eigenform*, wenn es zu jedem $\mathcal{T} \in \mathcal{H}$ ein $\lambda(\mathcal{T}) \in \mathbb{C}$ gibt mit

$$f \Big|_k \mathcal{T} = \lambda(\mathcal{T}) \cdot f.$$

(5.3) Satz. Sei $k > n + 1$ gerade. Dann ist die Siegelsche Eisenstein-Reihe $E_k^{(n)}$ eine simultane Hecke-Eigenform.

Beweis. Sei $M \in \Delta_n(l)$ und

$$\Gamma_n M \Gamma_n = \bigcup_{\nu=1}^d M_\nu \Gamma_n, \quad M_\nu = \begin{pmatrix} A_\nu & B_\nu \\ 0 & D_\nu \end{pmatrix}, \quad d = \text{ind } \Gamma_n M^{-1} \Gamma_n.$$

Wir betrachten die Untergruppe

$$\Gamma'_n := \Gamma_{n,0} \cap \Gamma_n[l] = \left\{ M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Gamma_{n,0}; \ M \equiv E \pmod{l} \right\}$$

von endlichem Index in $\Gamma_{n,0}$. Wegen $lM_\nu^{-1} \in M(2n \times 2n; \mathbb{Z})$ ist

$$\Gamma_{n,0} \cap \Gamma_n[l^2] \subset M_\nu^{-1} \Gamma'_n M_\nu \subset \Gamma_{n,0} \quad \text{für } \nu = 1, \dots, d,$$

so dass auch die konjugierte Gruppe endlichen Index in $\Gamma_{n,0}$ hat. Nun verifiziert man sofort

$$\Gamma'_n M_\nu \Gamma_n \subset M_\nu \Gamma_n = \bigcup_{L: \Gamma'_n \backslash M_\nu \Gamma_n} \Gamma'_n L = \bigcup_{K: M_\nu^{-1} \Gamma'_n M_\nu \backslash \Gamma_n} \Gamma'_n M_\nu K.$$

Damit berechnet man

$$\begin{aligned}
E_k^{(n)} \big|_k \Gamma_n M \Gamma_n &= \sum_{L: \Gamma_n \backslash \Gamma_n M \Gamma_n} \sum_{K: \Gamma_{n,0} \backslash \Gamma_n} 1 \big|_k K \big|_k L \\
&= \sum_{\tilde{L}: \Gamma_{n,0} \backslash \Gamma_n M \Gamma_0} 1 \big|_k \tilde{L} \\
&= \frac{1}{[\Gamma_{n,0} : \Gamma'_n]} \sum_{L': \Gamma'_n \backslash \Gamma_n M \Gamma_n} 1 \big|_k L' \\
&= \frac{1}{[\Gamma_{n,0} : \Gamma'_n]} \sum_{\nu=1}^d \sum_{L: \Gamma'_n \backslash M_\nu \Gamma_n} 1 \big|_k L \\
&= \frac{1}{[\Gamma_{n,0} : \Gamma'_n]} \sum_{\nu=1}^d \sum_{K: M_\nu^{-1} \Gamma'_n M_\nu \backslash \Gamma_n} 1 \big|_k M_\nu K \\
&= \sum_{\nu=1}^d \frac{[\Gamma_{n,0} : M_\nu^{-1} \Gamma'_n M_\nu]}{[\Gamma_{n,0} : \Gamma'_n]} \sum_{\nu=1}^d (\det D_\nu)^{-k} 1 \big|_k K \\
&= \left(\sum_{\nu=1}^d \frac{[\Gamma_{n,0} : M_\nu^{-1} \Gamma'_n M_\nu]}{[\Gamma_{n,0} : \Gamma'_n]} (\det D_\nu)^{-k} \right) \cdot E_k^{(n)},
\end{aligned}$$

da $1 \big|_k M_\nu = (\det D_\nu)^{-k}$. Weil die Doppelnebenklassen eine $\mathbb{Z}$ -Basis von H_n bilden, folgt die Behauptung. $\square$

Nun beschäftigen wir uns mit dem Vertauschungsgesetz mit dem Siegelschen ϕ -Operator. Dazu sei für $n > 1$

$$M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Delta_n(l), \quad A = \begin{pmatrix} A_1 & 0 \\ a^{tr} & \alpha \end{pmatrix}, \quad B = \begin{pmatrix} B_1 & * \\ * & * \end{pmatrix}, \quad D = \begin{pmatrix} D_1 & * \\ 0 & \delta \end{pmatrix}.$$

Wegen

$$\begin{aligned}
M \left\langle \begin{pmatrix} Z_1 & 0 \\ 0 & it \end{pmatrix} \right\rangle &= A \begin{pmatrix} Z_1 & 0 \\ 0 & it \end{pmatrix} D^{-1} + B D^{-1} = \frac{1}{l} \begin{pmatrix} Z_1 & 0 \\ 0 & it \end{pmatrix} [A^{tr}] + B D^{-1} \\
&= \frac{1}{l} \begin{pmatrix} Z_1 [A_1^{tr}] & A_1 Z_1 a \\ * & Z_1 [a] + it \alpha^2 \end{pmatrix} + B D^{-1}
\end{aligned}$$

folgt man durch Einsetzen der Fourier-Entwicklung

$$\lim_{t \rightarrow \infty} f \big|_k M \begin{pmatrix} Z_1 & 0 \\ 0 & it \end{pmatrix} = \delta^{-k} (f \big| \phi) \big|_k M_1(Z_1), \quad M_1 = \begin{pmatrix} A_1 & B_1 \\ 0 & D_1 \end{pmatrix}.$$

Mit (4.15) und (4.16) ergibt sich daraus der

(5.4) Satz. Sei $n > 1$, $\mathcal{T} \in \tilde{H}_n$ und $\mathcal{T}^* = \phi_k(\mathcal{T}) \in \tilde{H}_{n-1}$. Dann gilt für alle $f \in \mathcal{M}_k(\Gamma_n)$

$$\left(f \mid_k \mathcal{T} \right) \mid \phi = (f \mid \phi) \mid_k \mathcal{T}^*,$$

insbesondere für jede Primzahl p

$$\left(f \mid_k T_n(p) \right) \mid \phi = (p^{n-k} + 1)(f \mid \phi) \mid_k T_{n-1}(p).$$

Ist f eine simultane Hecke-Eigenform, so ist $f \mid \phi \equiv 0$ oder $f \mid \phi$ ist ebenfalls eine simultane Hecke-Eigenform.

Im nächsten Schritt untersuchen wir Spitzenformen.

(5.5) Lemma. Sei $0 \neq f \in \mathcal{S}_k(\Gamma_n)$ und $M \in \Delta_n(l)$ mit

$$f \mid_k \Gamma_n M \Gamma = \lambda f.$$

Dann gilt

$$|\lambda| \leq l^{-nk/2} \text{ind } \Gamma_n M \Gamma.$$

Für $\Gamma_n M \Gamma_n = T_n(p)$, $p \in \mathbb{P}$, hat man speziell

$$|\lambda| \leq p^{-nk/2} \prod_{j=1}^n (p^j + 1).$$

Beweis. Da f eine Spitzenform ist, nimmt die Funktion

$$\mathcal{H}_n \rightarrow \mathbb{R}, \quad Z \mapsto (\det Y)^{k/2} |f(Z)|,$$

nach II(2.5) ihr Maximum in einem Punkt $Z_0 \in \mathcal{H}_n$ an, also

$$|f(Z)| \leq \left(\frac{\det Y_0}{\det Y} \right)^{k/2} |f(Z_0)| \quad \text{für alle } Z \in \mathcal{H}_n.$$

Für $M = \begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Delta_n(l)$ gilt somit

$$|f(M \langle Z_0 \rangle)| \leq \det \left(\frac{1}{l} D^{tr} D \right)^{k/2} |f(Z_0)|.$$

Daraus ergibt sich

$$\begin{aligned}
 |\lambda f(Z_0)| &= \left| \sum_{M=\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} : \Gamma_n \backslash \Gamma_n M \Gamma_n} (\det D)^{-k} \cdot f(M\langle Z_0 \rangle) \right| \\
 &\leq \sum_{M=\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} : \Gamma_n \backslash \Gamma_n M \Gamma_n} |\det D|^{-k} \cdot |f(M\langle Z_0 \rangle)| \\
 &\leq \sum_{M=\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} : \Gamma_n \backslash \Gamma_n M \Gamma_n} l^{-nk/2} \cdot |f(Z_0)| \\
 &= l^{-nk/2} \text{ind } \Gamma_n M \Gamma_n \cdot |f(Z_0)|.
 \end{aligned}$$

Wegen $f(Z_0) \neq 0$ folgt damit die Behauptung. $\square$

Daraus erhalten wir das überraschende

(5.6) Korollar. *Sei $k > n+1$ gerade. Für $f \in \mathcal{M}_k(\Gamma_n)$ mit $\alpha_f(0) = 1$ sind äquivalent:*

(i) *Es gibt eine Primzahl p mit einem $\lambda \in \mathbb{C}$ mit*

$$f \mid_k \mathcal{T}_n(p) = \lambda f.$$

(ii) $f = E_k^{(n)}$.

Beweis. (ii) $\Rightarrow$ (i) Man verwende (5.3) und II(3.8).

(i) $\Rightarrow$ (ii) Für den Eigenwert λ gilt nach (5.2)

$$\lambda = \prod_{j=1}^n (p^{j-k} + 1).$$

Wir verwenden eine Induktion nach n und betrachten $g = f - E_k^{(n)}$ mit

$$g \mid_k \mathcal{T}_n(p) = \lambda g.$$

Im Fall $n = 1$ ist g eine Spitzenform. Aus $g \neq 0$ erhält man

$$\lambda = p^{1-k} + 1 \leq p^{-k/2}(p+1)$$

gemäß (5.5). Es gilt aber

$$p^{1-k} + 1 - p^{-k/2}(p+1) = (1 - p^{-k/2})(1 - p^{1-k/2}) > 0$$

wegen $k > 2$.

Sei nun $n > 1$. Weil $f \mid \phi$ nach (5.4) die gleiche Eigenschaft hat und nach Induktionsvoraussetzung mit $E_k^{(n-1)}$ übereinstimmt, ist g eine Spitzenform. Nach (5.2) und (5.5) gilt für $g \not\equiv 0$ dann wieder

$$\lambda = \prod_{j=1}^n (p^{j-k} + 1) \leq p^{-nk/2} \prod_{j=1}^n (p^j + 1) \leq p^{-n(n+2)/2} \prod_{j=1}^n (p^j + 1),$$

wegen $k > n + 1$. Es gilt $\lambda > 1$, aber

$$p^{-n(n+2)/2} \prod_{j=1}^n (p^j + 1) \leq 1 \quad \text{für alle } n \geq 2,$$

wie man durch Induktion nach n sofort nachweist. Das ist ein Widerspruch, so dass $g \equiv 0$ die Behauptung liefert. $\square$

Nun beschreiben wir den Zusammenhang mit dem Petersson Skalarprodukt aus II(4.13).

(5.7) Satz. Seien $M \in \Delta_n(l)$ und $f, g \in \mathcal{M}_k(\Gamma_n)$, wobei f oder g eine Spitzenform ist. Dann gilt

$$\langle f \mid \Gamma_n M \Gamma_n, g \rangle = \langle f, g \mid \Gamma_n M \Gamma_n \rangle.$$

Beweis. Wir beweisen die Aussage in mehreren Schritten. Zunächst sei $\varphi : \mathcal{H}_n \rightarrow \mathbb{C}$ eine beliebige beschränkte stetige Funktion und

$$\Gamma(\varphi) := \{M \in \Gamma_n; \varphi(M\langle Z \rangle) = \varphi(Z) \text{ für alle } Z\}$$

die Invarianzgruppe von φ , die nach Voraussetzung endlichen Index in Γ_n habe.

Beh. 1. Ist Λ eine Untergruppe von $\Gamma(\varphi)$ von endlichem Index und sind $\mathcal{F}_1$ sowie $\mathcal{F}_2$ zwei Fundamentalbereiche bezüglich Λ , so gilt

$$\int_{\mathcal{F}_1} \varphi \, d\mu_n = \int_{\mathcal{F}_2} \varphi \, d\mu_n.$$

Bew. $\mathcal{F}_1$ und $\mathcal{F}_2$ sind als (relativ) abgeschlossene Mengen Lebesgue-messbar. Für jedes $M \in \Gamma(\varphi)$ gilt

$$\int_{M\langle \mathcal{F}_1 \rangle} \varphi \, d\mu_n = \int_{\mathcal{F}_1} \varphi(M\langle Z \rangle) \, d\mu_n = \int_{\mathcal{F}_1} \varphi \, d\mu_n.$$

Nimmt man $-E \in \Lambda$ an, so folgt daraus

$$\begin{aligned} \int_{\mathcal{F}_1} \varphi \, d\mu_n &= \frac{1}{2} \sum_{M \in \Lambda} \int_{M\langle \mathcal{F}_2 \rangle \cap \mathcal{F}_1} \varphi \, d\mu_n \\ &= \frac{1}{2} \sum_{M \in \Lambda} \int_{\mathcal{F}_2 \cap M^{-1}\langle \mathcal{F}_1 \rangle} \varphi \, d\mu_n \\ &= \int_{\mathcal{F}_2} \varphi \, d\mu_n, \end{aligned}$$

da mit M auch M^{-1} die gesamte Gruppe Λ durchläuft. □

Wir schreiben dafür

$$\int_{\Lambda \backslash \mathcal{H}_n} \varphi \, d\mu_n := \int_{\mathcal{F}_1} \varphi \, d\mu_n.$$

Beh. 2. Ist Λ eine Untergruppe von endlichem Index in $\Gamma(\varphi)$ mit $-E \in \Lambda$, so gilt

$$\frac{1}{[\Gamma(\varphi) : \Lambda]} \int_{\Lambda \backslash \mathcal{H}_n} \varphi \, d\mu_n = \int_{\Gamma(\varphi) \backslash \mathcal{H}_n} \varphi \, d\mu_n.$$

Bew. Sei $\mathcal{F}$ ein Fundamentalbereich bezüglich $\Gamma(\varphi)$ und

$$\Gamma(\varphi) = \bigcup_{\nu=1}^r \Lambda M_\nu, \quad r = [\Gamma(\varphi) : \Lambda],$$

eine direkte Zerlegung in Nebenklassen. Dann ist

$$\mathcal{G} := \bigcup_{\nu=1}^r M_\nu \langle \mathcal{F} \rangle$$

ein Fundamentalbereich bezüglich Λ . Aus Beh. 1 folgt

$$\begin{aligned} \int_{\Lambda \backslash \mathcal{H}_n} \varphi \, d\mu_n &= \int_{\mathcal{G}} \varphi \, d\mu_n = \sum_{\nu=1}^r \int_{M_\nu \langle \mathcal{F} \rangle} \varphi \, d\mu_n \\ &= \sum_{\nu=1}^r \int_{\mathcal{F}} \varphi \, d\mu_n = r \cdot \int_{\Gamma(\varphi) \backslash \mathcal{H}_n} \varphi \, d\mu_n. \end{aligned} \quad \square$$

Nun betrachten wir $M \in \Delta_n(q)$ mit

$$M^\sharp = \begin{pmatrix} D^{tr} & -B^{tr} \\ -C^{tr} & A^{tr} \end{pmatrix} = qM^{-1}$$

sowie

$$\varphi := \varphi_{f,g} : \mathcal{H}_n \rightarrow \mathbb{R}, \quad Z \mapsto f(Z)\overline{g(Z)}(\det Y)^k,$$

und die erweiterte Kongruenzgruppe

$$\Gamma_n[q] := \{K \in \Gamma_n; K \equiv \pm E \pmod{q}\}.$$

Wegen $MM^\sharp = M^\sharp M = qE$ liefert eine Verifikation

$$(*) \quad \varphi_{f|_{M,g}}(M^{-1}\langle Z \rangle) = \varphi_{fg|_{M^\sharp}}(Z), \quad Z \in \mathcal{H}_n.$$

Beh. 3. $\Gamma_n[q]$ und $M\Gamma_n[q]M^{-1}$ sind Untergruppen von endlichem Index in $\Gamma(\varphi_{f|_{M,g}})$ und in $\Gamma(\varphi_{f,g|M^\sharp})$.

Bew. Für $L \in \Gamma_n[q]$, $L = \pm E + qA$, $A \in M(2n \times 2n; \mathbb{Z})$ folgt

$$L_0 = MLM^{-1} = \pm E + MAM^\sharp \in M(2n \times 2n; \mathbb{Z}),$$

also $L_0 \in \Gamma_n$ mit $ML = L_0M$ und somit

$$f|_{\underset{k}{M}}|_{\underset{k}{L}} = f|_{\underset{k}{(ML)}} = f|_{\underset{k}{L_0}}|_{\underset{k}{M}} = f|_{\underset{k}{M}} \quad \text{und} \quad g|_{\underset{k}{L}} = g.$$

Dann folgt

$$\varphi_{f|M,g}(L\langle Z \rangle) = \varphi_{f|M|L,g|L}(Z) = \varphi_{f|M,g}(Z),$$

also $\Gamma_n[q] \subset \Gamma(\varphi_{f|M,g})$. Der Index ist wegen $[\Gamma_n : \Gamma_n[q]] < \infty$ ebenfalls endlich. Für $M^{-1}\Gamma_n[q]M \supset \Gamma_n[q^2]$ ist die Behauptung unmittelbar klar. Die analoge Aussage für $\Gamma(\varphi_{f,g|M^\sharp})$ zeigt man in gleicher Weise. $\square$

Beh. 4. Es gilt

$$[\Gamma : \Gamma_n[q]] = [\Gamma : M^{-1}\Gamma_n[q]M].$$

Bew. Sei $\mathcal{F}$ ein Fundamentalbereich bezüglich $\Gamma_n[q]$. Dann ist $M^{-1}\langle \mathcal{F} \rangle$ ein Fundamentalbereich bezüglich $M^{-1}\Gamma_n[q]M$. Aus Beh. 1 und 2 erhält man

$$\begin{aligned} [\Gamma_n : M^{-1}\Gamma_n[q]\Gamma] \text{vol}(\mathcal{F}_n) &= \int_{M^{-1}\Gamma_n[q]M \setminus \Gamma_n} d\mu_n \\ &= \int_{M^{-1}\langle \mathcal{F} \rangle} d\mu_n = \int_{\mathcal{F}} d\mu_n = [\Gamma_n : \Gamma_n[q]] \text{vol}(\mathcal{F}_n), \end{aligned}$$

wenn $\mathcal{F}_n$ den Siegelschen Fundamentalbereich bezüglich Γ_n bezeichnet. Die Aussage folgt dann aus $\text{vol}(\mathcal{F}_n) < \infty$. $\square$

Aus Behauptung 2 und 3 ergibt sich nun für ein beliebiges Vertretersystem $M_1, \dots, M_r$

von $\Gamma_n \backslash \Gamma_n M \Gamma_n$

$$\begin{aligned}
\langle f \mid_k \Gamma_n M \Gamma_n, g \rangle &= \int_{\mathcal{F}_n} \sum_{\nu=1}^r f \mid_k M_\nu(Z) \overline{g(Z)} (\det Y)^k d\mu_n \\
&= \int_{\mathcal{F}_n} \sum_{\nu=1}^r \varphi_{f \mid M_\nu, g}(Z) d\mu_n \\
&= \frac{1}{[\Gamma_n : \Gamma_n[q]]} \int_{\Gamma_n[q] \backslash \Gamma_n} \sum_{\nu=1}^r \varphi_{f \mid M_\nu, g}(Z) d\mu_n \\
&= \frac{1}{[\Gamma_n : \Gamma_n[q]]} \sum_{\nu=1}^r \int_{\Gamma_n[q] \backslash \mathcal{H}_n} \varphi_{f \mid M_\nu, g}(Z) d\mu_n \\
&= \frac{1}{[\Gamma_n : \Gamma_n[q]]} \sum_{\nu=1}^r \int_{\Gamma_n[q] \backslash \mathcal{H}_n} \varphi_{f, g \mid M_\nu^\#}(M_\nu \langle Z \rangle) d\mu_n
\end{aligned}$$

wenn man (*) verwendet. Nach (4.5) können wir die M_ν als simultanes Vertretersystem der Rechts- und Linksnebenklassen wählen. Aus dem symplektischen Elementarteilersatz (4.1) erhält man dann

$$\Gamma_n M \Gamma_n = \bigcup_{\nu=1}^r \Gamma_n M_\nu = \bigcup_{\nu=1}^r M_\nu \Gamma_n = \Gamma_n M^\# \Gamma_n = \bigcup_{\nu=1}^r M_\nu^\# \Gamma_n = \bigcup_{\nu=1}^r \Gamma_n M_\nu^\#.$$

Daraus ergibt sich dann, wenn $\mathcal{F}$ einen Fundamentalbereich bezüglich $\Gamma_n[q]$ bezeichnet, zusammen mit (*)

$$\begin{aligned}
\langle f \mid_k \Gamma_n M \Gamma_n, g \rangle &= \frac{1}{[\Gamma_n : \Gamma_n[q]]} \sum_{\nu=1}^r \int_{M_\nu^{-1} \langle \mathcal{F} \rangle} \varphi_{f, g \mid M_\nu^\#}(Z) d\mu_n \\
&= \frac{1}{[\Gamma_n : \Gamma_n[q]]} \sum_{\nu=1}^r \int_{M_\nu^{-1} \Gamma_n[q] M_\nu \backslash \mathcal{H}_n} \varphi_{f, g \mid M_\nu^\#} d\mu_n \\
&= \int_{\Gamma_n \backslash \mathcal{H}_n} \sum_{\nu=1}^r \varphi_{f, g \mid M_\nu^\#} d\mu_n \\
&= \int_{\Gamma_n \backslash \mathcal{H}_n} f(Z) \overline{g \mid_k \Gamma_n M \Gamma_n(Z)} d\mu_n \\
&= \langle f, g \mid_k \Gamma_n M \Gamma_n \rangle
\end{aligned}$$

□

Wir wiederholen aus II(4.14) die Definition

$$\mathcal{N}_k(\Gamma_n) = \{f \in \mathcal{M}_k(\Gamma_n); \langle f, g \rangle = 0 \text{ für alle } g \in \mathcal{S}_k(\Gamma_n)\},$$

$$\mathcal{M}_k^{(n,j)} = \begin{cases} \mathcal{S}_k(\Gamma_n) & \text{für } j = n, \\ \{f \in \mathcal{N}_k(\Gamma_n); f \mid \phi \in \mathcal{M}_k^{(n-1,j)}\} & \text{für } 0 \leq j < n, \end{cases}$$

wenn man $\mathcal{M}_k^{(0,0)} := \mathbb{C}$ ergänzt.

(5.8) Lemma. Die Räume $\mathcal{N}_k(\Gamma_n)$ und $\mathcal{M}_k^{(n,j)}$, $0 \leq j \leq n$, sind unter allen Hecke-Operatoren $\mathcal{T} \in \tilde{H}_n$ invariant.

Beweis. Die Invarianz von $\mathcal{N}_k(\Gamma_n)$ folgt direkt aus (5.7) und der Tatsache, dass $\mathcal{M}_k^{(n,n)} = \mathcal{S}_k(\Gamma_n)$ nach (5.1) unter allen Hecke-Operatoren invariant ist. Wegen $\mathcal{N}_k(\Gamma_1) = \mathcal{M}_k^{(1,1)}$ ist die Behauptung damit auch für $n = 1$ bewiesen. Sei also $n > 1$ und $0 \leq j < n$, $\mathcal{T} \in \tilde{H}_n$. Die Abbildung

$$\phi : \mathcal{N}_k(\Gamma_n) \rightarrow \mathcal{M}_k(\Gamma_{n-1})$$

ist wegen $\text{Kern } \phi = \mathcal{N}_k(\Gamma_n) \cap \mathcal{S}_k(\Gamma_n) = \{0\}$ injektiv, also auch

$$\phi : \mathcal{M}_k^{(n,j)} \rightarrow \mathcal{M}_k^{(n-1,j)}.$$

Mit $\mathcal{T}^* = \phi_k(\mathcal{T}) \in \tilde{H}_{n-1}$ folgt für $f \in \mathcal{M}_k^{(n,j)}$ nach (5.4)

$$f \mid_k \mathcal{T} \mid \phi = f \mid \phi \mid_k \mathcal{T}^* \in \mathcal{M}_k^{(n-1,j)},$$

weil $\mathcal{M}_k^{(n-1,j)}$ nach Induktionsvoraussetzung unter $\mathcal{T}^*$ invariant ist. Da $f \mid_k \mathcal{T} \in \mathcal{N}_k(\Gamma_n)$ gilt, liefert die Injektivität von ϕ auch $f \mid_k \mathcal{T} \in \mathcal{M}_k^{(n,j)}$. $\square$

Für gerades $k > n + j + 1$, $0 \leq j < n$ gilt nach II(4.17)

$$\mathcal{M}_k^{(n,j)} = \{E_k^{(n,j)}(\cdot, g); g \in \mathcal{S}_k(\Gamma_j)\}.$$

Mit dem Vertauschungsgesetz aus (5.4) erhalten wir das

(5.9) Korollar. Sei $k > n + j + 1$ gerade und $0 < j < n$. Ist $\mathcal{T} \in \tilde{H}_n$ und

$$\mathcal{T}^* := \phi_k^{n-j}(\mathcal{T}) \in \tilde{H}_j,$$

so gilt für alle $g \in \mathcal{S}_k(\Gamma_j)$

$$E_k^{(n,j)}(\cdot, g) \mid \mathcal{T} = E_k^{(n,j)}(\cdot, g \mid \mathcal{T}^*).$$

Nun wenden wir uns der Existenz von simultanen Eigenformen zu.

(5.10) Satz. $\mathcal{M}_k(\Gamma_n)$ besitzt eine Basis aus simultanen Eigenformen aller Hecke-Operatoren aus $\tilde{H}_n$.

Beweis. $(\mathcal{S}_k(\Gamma_n), <, >)$ ist ein unitärer Vektorraum und die Hecke-Operatoren sind nach (5.7) selbstadjungiert sowie paarweise vertauschbar, da der Hecke Ring nach (4.7) kommutativ ist. Nach einem Satz der Linearen Algebra existiert dann eine Basis, die aus simultanen Eigenvektoren besteht. Wegen

$$\mathcal{M}_k(\Gamma_n) = \mathcal{N}_k(\Gamma_n) \oplus \mathcal{S}_k(\Gamma_n), \quad \mathcal{N}_k(\Gamma_1) = \begin{cases} \mathbb{C}E_k^{(1)}, & k > 2 \text{ gerade} \\ \{0\}, & \text{sonst,} \end{cases}$$

folgt die Behauptung für $n = 1$. Ist $n > 1$, so ist

$$\phi : \mathcal{N}_k(\Gamma_n) \rightarrow \mathcal{M}_k(\Gamma_{n-1})$$

injektiv. Nach dem Vertauschungsgesetz (5.4) und der Surjektivität gemäß (4.16) ist $\phi(\mathcal{N}_k(\Gamma_n))$ ein Unterraum von $\mathcal{M}_k(\Gamma_{n-1})$, der unter allen Hecke-Operatoren invariant ist. Dieser Unterraum besitzt nach Induktionsvoraussetzung eine Basis aus simultanen Eigenformen. Deren Urbilder unter ϕ bilden dann eine Basis von $\mathcal{N}_k(\Gamma_n)$, die aus simultanen Eigenformen besteht. $\square$

Als Nächstes wenden wir uns den Theta-Reihen zu. Für $k \equiv 0 \pmod{4}$ bezeichne $\mathcal{M}_k(\Gamma_n)_\Theta$ den von den Theta-Reihen zu positiv-definiten, geraden unimodularen $2k \times 2k$ Matrizen S aufgespannten Unterraum von $\mathcal{M}_k(\Gamma_n)$.

(5.11) Satz. $\mathcal{M}_k(\Gamma_n)_\Theta$ ist unter allen Hecke-Operatoren invariant.

Beweis. Sei $f \in \mathcal{M}_k(\Gamma_n)_\Theta$. Dann existiert nach IV(3.12) zu $N > \max\{n, 2k\}$ ein $F \in \mathcal{M}_k(\Gamma_N)$ mit $\phi^{N-n}(F) = f$. Ist $\mathcal{T} \in \tilde{H}_n$, so existiert nach (4.16) ein $\mathcal{T}^* \in \tilde{H}_N$ mit

$$\phi_k^{N-n}(\mathcal{T}^*) = \mathcal{T}, \quad \text{also} \quad \phi^{N-n} \left(F \mid_k \mathcal{T}^* \right) = \phi^{N-n}(F) \mid_k \phi_r^{N-n}(\mathcal{T}^*) = f \mid_k \mathcal{T}$$

nach (5.4). Es folgt $f \mid_k \mathcal{T} \in \mathcal{M}_k(\Gamma_n)_\Theta$ nach IV(3.12). $\square$

Nun beschäftigen wir uns speziell mit der Wirkung von $\mathcal{T}_n(p)$ für eine Primzahl p . Dazu sei im Folgenden stets

$S_1, \dots, S_h$ ein Vertretersystem der Klassen gerader, unimodularer, positiv definiter $2k \times 2k$ Matrizen.

Ist p eine (feste) Primzahl, so sei für $0 \leq j \leq n$ wieder

$$\begin{aligned} \mathcal{T}_{n,j}(p) &= \{D \in M(n \times n; \mathbb{Z}); \det D = p^j, r_p(D) = n - j\} \\ &= \mathcal{U}_n \begin{pmatrix} E & 0 \\ 0 & pE^{(j)} \end{pmatrix} \mathcal{U}_n \end{aligned}$$

wie in (3.8).

(5.12) Lemma. Für $p \in \mathbb{P}$ und $1 \leq \mu \leq h$ und $n = 2k$ gibt es eine eindeutige Darstellung

$$\Theta^{(n)}(\cdot, S_\mu) \Big|_k T_n(p) = \sum_{\nu=1}^h c_{\mu\nu} \Theta^{(n)}(\cdot, S_\nu)$$

mit

$$c_{\mu\nu} = \sum_{j=k}^{2k} p^{j(j+1-2k)/2} \sum_{D: \mathcal{U}_n \setminus \mathcal{T}_{n,j}(p)} \frac{\#(S_\mu, \frac{1}{p}S_\nu[D^{tr}])}{\#(S_\nu, S_\nu)}.$$

Beweis. Nach (5.11) haben wir eine Darstellung

$$F := \Theta^{(2k)}(\cdot, S_\mu) \Big|_k T_n(p) = \sum_{\nu=1}^h c_{\mu\nu} \Theta^{(2k)}(\cdot, S_\nu).$$

Wegen der linearen Unabhängigkeit der Theta-Reihen folgt

$$\alpha_F(S_\nu) = c_{\mu\nu} \cdot \#(S_\nu, S_\nu).$$

Aus (5.1) erhält man

$$\alpha_F(S_\nu) = \sum_{\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \Gamma_n \setminus T_n(p)} (\det D)^{-k} \#(S_\mu, \frac{1}{p}S_\nu[D^{tr}]) e^{\pi i \operatorname{Sp}(S_\mu D^{tr} B)/p}.$$

Nach (3.8) folgt $D \in \mathcal{T}_{n,j}(p)$, $0 \leq j \leq n$. Die auftretende Darstellungsanzahl ist 0, wenn $\frac{1}{p}S_\nu[D^{tr}]$ nicht gerade ist. Die Betrachtung der Determinante liefert $j \geq k$. Nun kann man die Vertreter in der Form

$$\begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \quad A = pD^{tr-1}, \quad D = \begin{pmatrix} E & 0 \\ 0 & pE^{(j)} \end{pmatrix} V, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & S \end{pmatrix} V,$$

mit $S \in \operatorname{Sym}(j; \mathbb{Z}) \bmod p$, $k \leq j \leq 2k$ und geeigneten $V \in \mathcal{U}_n$ wählen. Dann ist

$$\frac{1}{p}D^{tr} B = \begin{pmatrix} 0 & 0 \\ 0 & S \end{pmatrix} [V] \in \Lambda_n$$

und der Exponentialterm somit 1. Es folgt

$$\alpha_F(S_\nu) = \sum_{j=k}^{2k} p^{j(j+1-2k)/2} \sum_{D: \mathcal{U}_n \setminus \mathcal{T}_{n,j}(p)} \#(S_\mu, \frac{1}{p}S_\nu[D^{tr}]).$$

□

Für symmetrische Matrizen $S \in \text{Sym}(m; \mathbb{R})$, $T \in \text{Sym}(n; \mathbb{R})$ sei

$$\mathcal{D}(S, T) := \{G \in M(m \times n; \mathbb{Z}); S[G] = T\}.$$

Einen weiteren Zwischenschritt formulieren wir in dem

(5.13) Lemma. Für $k \leq j \leq 2k = n$ und $1 \leq \mu, \nu \leq h$ gilt

$$\text{ind } \mathcal{T}_{k, j-k}(p) \cdot \sharp(S_\mu, pS_\nu) = \sum_{D: \mathcal{U}_n \setminus \mathcal{T}_{n, j}(p)} \sharp(S_\mu, \frac{1}{p}S_\nu[D^{tr}]).$$

Beweis. Für jedes $D \in \mathcal{T}_{n, j}(p)$ ist die Abbildung

$$\mathcal{D}(S_\mu \frac{1}{p}S_\nu[D^{tr}]) \rightarrow \mathcal{D}(S_\mu, pS_\nu), \quad H \mapsto G := pH D^{tr-1},$$

injektiv. Wegen $H = \frac{1}{p}GD^{tr}$ bestimmen wir für festes $G \in \mathcal{D}(S_\mu, pS_\nu)$ die Anzahl

$$r = r(G) = \sharp\{\mathcal{U}_n D \subset \mathcal{T}_{n, j}(p); GD^{tr} \equiv 0 \pmod{p}\}.$$

Offenbar gilt $r(G) = r(UGV)$ für alle $U, V \in \mathcal{U}_n$. Wegen $|\det G| = p^k$ und $pG^{-1} = S_\nu^{-1}G^{tr}S_\mu \in M(n \times n; \mathbb{Z})$ folgt

$$G \in \mathcal{T}_{2k, k}(p), \text{ also ohne Einschränkung } G = \begin{pmatrix} E & 0 \\ 0 & pE \end{pmatrix}, \quad E = E^{(k)}.$$

Wählt man nun die Vertreter D in oberer Dreiecksform, so hat man

$$\begin{aligned} r &= \sharp\left\{\mathcal{U}_n \begin{pmatrix} E^{(k)} & 0 \\ 0 & D \end{pmatrix} \subset \mathcal{T}_{n, j}(p)\right\} = \sharp\{\mathcal{U}_k \tilde{D} \subset \mathcal{T}_{k, j-k}(p)\} \\ &= \text{ind } \mathcal{T}_{k, j-k}(p). \end{aligned}$$

Da die Anzahl unabhängig von G ist, folgt die Behauptung. $\square$

Die Anwendung ist der

(5.14) Satz. Für $1 \leq \mu \leq h$ und $p \in \mathbb{P}$ gilt

$$\Theta^{(n)}(\cdot, S_\mu) \Big|_k T_n(p) = \beta_n \sum_{\nu=1}^n \frac{\sharp(S_\mu, pS_\nu)}{\sharp(S_\nu, S_\nu)} \Theta^{(n)}(\cdot, S_\nu)$$

mit

$$\beta_n = p^{n(n+1-2k)/2} \cdot \begin{cases} \prod_{j=1}^{k-n} (1 + p^{j-1})^{-1} & \text{für } n \leq k, \\ \prod_{j=1}^{n-k} (1 + p^{-j}) & \text{für } k \leq n. \end{cases}$$

Beweis. Zunächst sei $n = 2k$. Dann folgt die Behauptung aus (5.12) und (5.13) mit

$$\begin{aligned}
 \beta &= \sum_{j=k}^{2k} p^{j(j+1-2k)/2} \text{ind } T_{k,j-k}(p) \\
 &= \sum_{j=k}^{2k} p^{j(j+1-2k)/2} p^{-(j-k)(j-k-1)/2} S_{j-k}(p, \dots, p^k) \\
 &= p^{k(1-k)/2} \sum_{l=0}^k S_l(p, \dots, p^k) \\
 &= p^{k(1-k)/2} \prod_{l=1}^k (p^l + 1) \\
 &= p^k \prod_{l=1}^k (1 + p^{-l}).
 \end{aligned}$$

Das ist die Behauptung. Die anderen Fälle folgen nun durch das Vertauschungsgesetz mit dem ϕ -Operator in (5.4), das auf $\beta_n = (1 + p^{n-k})\beta_{n-1}$ führt. $\square$

Sei nun $S \in \Lambda_{2k} \cap \mathcal{P}_{2k} \cap \mathcal{U}_{2k}$ beliebig und für $p \in \mathbb{P}$

$$A_p(S) := \{H\mathcal{U}_{2k} \subset \mathcal{T}_{2k,k}(p); S[H] \in p\Lambda_{2k}\}.$$

(5.15) Lemma. a) Ist $H \in M(2k \times 2k; \mathbb{Z})$ mit $|\det H| = p^k$ und $S[H] \in p\Lambda_{2k}$, so gilt $pH^{-1} \in M(2k \times 2k; \mathbb{Z})$ und $H \in \mathcal{T}_{2k,k}(p)$.

b) Die Abbildung

$$\bigcup_{\nu=1}^h \{G \text{ Aut } S_\nu; G \in \mathcal{D}(S, pS_\nu)\} \rightarrow A_p(S), \quad G \text{ Aut } S_\nu \mapsto G\mathcal{U}_{2k},$$

ist eine Bijektion.

c) Die Abbildung

$$\bigcup_{\nu=1}^h \{(\text{Aut } S_\nu)G; G \in \mathcal{D}(S_\nu, pS)\} \rightarrow A_p(S), \quad (\text{Aut } S_\nu)G \mapsto pG^{-1}\mathcal{U}_{2k},$$

ist eine Bijektion.

Beweis. a) Sei $S[H] = pT$, $T \in \Lambda_{2k}$. Aus der Berechnung der Determinante folgt $T \in \mathcal{U}_{2k}$, also

$$pH^{-1} = T^{-1}H^{tr}S \in M(2k \times 2k; \mathbb{Z}).$$

b) Aus $S[G] = pS_\nu$ und $\det S = \det S_\nu = 1$ folgt $|\det G| = p^k$. Wegen a) und $\text{Aut } S_\nu \subset \mathcal{U}_n$ ist die Abbildung, die wir ψ nennen, wohldefiniert. Seien nun $G \in \mathcal{D}(S, pS_\nu)$ und $H \in \mathcal{D}(S, pS_\mu)$ mit $G\mathcal{U}_n = H\mathcal{U}_{2k}$, also $G = HU$ für ein geeignetes $U \in \mathcal{U}_{2k}$. Damit folgt

$$S_\nu = \frac{1}{p}S[G] = \frac{1}{p}S[HU] = S_\mu[U].$$

Da es sich um Vertreter der Klassen handelt, schließen wir $\nu = \mu$ und $U \in \text{Aut } S_\nu$, also

$$G \text{ Aut } S_\nu = H \text{ Aut } S_\nu.$$

Demnach ist ψ injektiv.

Sei nun $H\mathcal{U}_n \in Ap(S)$. Dann ist $T := \frac{1}{p}S[H] \in \Lambda_{2k} \cap \mathcal{P}_{2k} \cap \mathcal{U}_{2k}$. Also existieren ein ν und ein $U \in \mathcal{U}_{2k}$ mit

$$S_\nu = T[U].$$

Daraus ergibt sich $HU \in \mathcal{D}(S, pS_\nu)$ und

$$\psi(HU \text{ Aut } S_\nu) = H\mathcal{U}_{2k}.$$

Also ist ψ auch surjektiv.

c) Der Beweis verläuft analog. □

Indem wir die Ordnung von $A_p(S)$ in b) und c) berechnen, bekommen wir das

(5.16) Korollar. Sei $S \in \Lambda_{2k} \cap \mathcal{U}_{2k} \cap \mathcal{P}_{2k}$ und $p \in \mathbb{P}$. Dann gilt

$$\#A_p(S) = \sum_{\nu=1}^h \frac{\#(S, pS_\nu)}{\#(S_\nu, S_\nu)} = \sum_{\nu=1}^h \frac{\#(S_\nu, pS)}{\#(S_\nu, S_\nu)}.$$

Als Folgerung notieren wir den

(5.17) Satz. Die Siegelsche Modulformen

$$F(Z) := \sum_{\mu=1}^h \frac{1}{\#(S_\mu, S_\mu)} \Theta^{(n)}(Z, S_\mu) \in \mathcal{M}_k(\Gamma_n)$$

ist eine simultane Eigenform aller Hecke-Operatoren $T_n(p)$, $p \in \mathbb{P}$.

Beweis. Aus (5.14) erhält man

$$\begin{aligned}
 F \mid_k T_n(p) &= \sum_{\mu=1}^h \frac{1}{\sharp(S_\mu, S_\mu)} \Theta^{(n)}(\cdot, S_\mu) \mid_k T_n(p) \\
 &= \sum_{\nu=1}^h \sum_{\mu=1}^h \beta_n \frac{\sharp(S_\mu, pS_\nu)}{\sharp(S_\nu, S_\nu) \cdot \sharp(S_\mu, S_\mu)} \Theta^{(n)}(\cdot, S_\nu) \\
 &= \sharp A_p(S) \cdot \beta_n \sum_{\nu=1}^h \frac{1}{\sharp(S_\nu, S_\nu)} \Theta^{(n)}(\cdot, S_\nu) \\
 &= \sharp A_p(S) \cdot \beta_n \cdot F,
 \end{aligned}$$

wenn man (5.16) verwendet. □

Der konstante Fourier-Koeffizient von F ist

$$\alpha_F(0) = \frac{1}{\sharp(S_1, S_1)} + \cdots + \frac{1}{\sharp(S_h, S_h)}.$$

Mit (5.6) folgt daraus sofort der

(5.18) Satz. Sei $k > n + 1$, $k \equiv 0 \pmod{4}$. Dann gilt

$$E_k^{(n)} = \sum_{\nu=1}^h m_\nu \Theta^{(n)}(\cdot, S_\nu), \quad m_\nu = \frac{\frac{1}{\sharp(S_\nu, S_\nu)}}{\frac{1}{\sharp(S_1, S_1)} + \cdots + \frac{1}{\sharp(S_h, S_h)}}.$$

Die Fourier-Koeffizienten von $E_k^{(n)}$ sind rationale Zahlen mit beschränktem Nenner.

Dieser Satz ist ein Spezialfall des so genannten *Siegelschen Hauptsatzes*.

(5.19) Bemerkungen. a) Für $k \equiv 2 \pmod{4}$, $k > n + 1$ sind die Fourier-Koeffizienten von $E_k^{(n)}$ ebenfalls rational mit beschränktem Nenner.

b) Die im Nenner auftretende Größe

$$M(2k) = \frac{1}{\sharp(S_1, S_1)} + \cdots + \frac{1}{\sharp(S_h, S_h)},$$

heißt *Maß* des Geschlechts der geraden, unimodularen, positiv definiten $2k \times 2k$ Matrizen. Die Minkowski-Siegelsche Maßformel gibt die Größe an

$$M(2k) = \frac{B_k}{2k} \prod_{j=1}^{k-1} \frac{B_{2j}}{4j}.$$

Schließlich wenden wir uns dem Maaß-Raum $\mathcal{M}_k^*$ in $\mathcal{M}_k(\Gamma_2)$ zu, der gemäß V(2.1) aus allen $f \in \mathcal{M}_k(\Gamma_2)$ besteht, die

$$(*) \quad \alpha_f(T) = \sum_{d|\varepsilon(T)} d^{k-1} \alpha_f \begin{pmatrix} 2mn/d^2 & t/d \\ t/d & 2 \end{pmatrix}$$

für alle $0 \neq T = \begin{pmatrix} 2n & t \\ t & 2m \end{pmatrix} \in \Lambda_2$, $T \geq 0$ mit $\varepsilon(T) = \text{ggT}(m, n, t)$ erfüllen. Wir geben eine für unsere Zwecke etwas handlichere Beschreibung in dem folgenden

(5.20) Lemma. *a) $f \in \mathcal{M}_k(\Gamma_2)$ liegt genau dann im Maaß-Raum, wenn es eine Funktion*

$$\alpha_f^* : \mathbb{N} \times \{N \in \mathbb{N}_0; N \equiv 0, 3 \pmod{4}\} \rightarrow \mathbb{C}$$

gibt mit den Eigenschaften

$$(i) \quad \alpha_f(T) = \alpha_f^*(\varepsilon(T), \det T) \quad \text{für alle } 0 \neq T \in \Lambda_2, T \geq 0,$$

$$(ii) \quad \alpha_f^*(r, N) = \sum_{d|r} d^{k-1} \alpha_f^*(1, r^2 N/d^2) \quad \text{für alle } (r, N).$$

b) Eine Funktion $\alpha_f^ : \mathbb{N} \times \{N \in \mathbb{N}_0; N \equiv 0, 3 \pmod{4}\} \rightarrow \mathbb{C}$ erfüllt genau dann (ii), wenn*

$$\alpha_f^*(q^s r, N) = \sum_{\nu=0}^s q^{\nu(k-1)} \alpha_f^*(r, q^{2(s-\nu)} N)$$

für alle $q \in \mathbb{P}$, $s, r \in \mathbb{N}$, $q \nmid r$, $N \in \mathbb{N}_0$ mit $N \equiv 0, 3 \pmod{4}$.

Beweis. a) Offenbar erfüllt ein $f \in \mathcal{M}_k(\Gamma_2)$, das (i) und (ii) genügt, auch die Bedingung (*) und gehört damit zu $\mathcal{M}_k^*$.

Geht man umgekehrt von einem $f \in \mathcal{M}_k^*$ aus, so definiert man

$$\alpha_f^*(r, N) = \begin{cases} \alpha_f \left(r \begin{pmatrix} 2m & 0 \\ 0 & 2 \end{pmatrix} \right), & \text{falls } N = 4m, m \in \mathbb{N}_0, \\ \alpha_f \left(r \begin{pmatrix} 2m & 1 \\ 1 & 2 \end{pmatrix} \right), & \text{falls } N = 4m - 1, m \in \mathbb{N}. \end{cases}$$

Aufgrund von

$$\alpha_f \begin{pmatrix} 2m & t \\ t & 2 \end{pmatrix} = \alpha_f \begin{pmatrix} 2m' & t' \\ t' & 2 \end{pmatrix}, \quad \text{falls } t \equiv t' \pmod{2} \quad \text{und} \quad 4m - t^2 = 4m' - t'^2,$$

erfüllt die so definierte Funktion auch (i) und (ii).

b) Erfüllt α_f^* die Bedingung (ii), so liefert deren zweimalige Anwendung auch

$$\begin{aligned}\alpha_f^*(q^s r, N) &= \sum_{d|q^s r} d^{k-1} \alpha_f^*(1, q^{2s} r^2 N/d^2) \\ &= \sum_{\substack{\nu=0, \dots, s \\ d|r}} (q^\nu d)^{k-1} \alpha_f^*(1, q^{2(s-\nu)} r^2 N/d^2) \\ &= \sum_{\nu=0}^s q^{\nu(k-1)} \alpha_f^*(r, q^{2(s-\nu)} N).\end{aligned}$$

Erfüllt andererseits α_f^* die angegebene Bedingung, so folgt für $r = p_1^{s_1} \cdot \dots \cdot p_l^{s_l}$, $p_i \in \mathbb{P}$, $s_i \in \mathbb{N}$, sukzessiv

$$\begin{aligned}\alpha_f^*(r, N) &= \sum_{\nu_1=0}^{s_1} p_1^{\nu_1(k-1)} \alpha_f^*(p_2^{s_2} \cdot \dots \cdot p_l^{s_l}, p_1^{2(s_1-\nu_1)} N) \\ &= \sum_{\nu_1=0}^{s_1} \dots \sum_{\nu_l=0}^{s_l} p_1^{\nu_1(k-1)} \cdot \dots \cdot p_l^{\nu_l(k-1)} \alpha_f^*(1, p_1^{2(s_1-\nu_1)} \cdot \dots \cdot p_l^{2(s_l-\nu_l)} N) \\ &= \sum_{d|r} d^{k-1} \alpha_f^*(1, r^2 N/d^2),\end{aligned}$$

also (*). □

Wir setzen α_f^* durch 0 zu einer Funktion $\mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{C}$ fort.

(5.21) Satz. *Der Maaß-Raum $\mathcal{M}_k^*$ ist unter allen Hecke-Operatoren $T_2(p)$, $p \in \mathbb{P}$ ungerade, invariant.*

Beweis. Sei $f \in \mathcal{M}_k^*$ und $g := f \mid_k T_2(p) \in \mathcal{M}_k(\Gamma_2)$. Nach (5.1) gilt

$$\alpha_g(T) = \sum_{\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} : \Gamma_2 \backslash T_2(p)} (\det D)^{-k} \alpha_f \left(\frac{1}{p} T[D^{tr}] \right) e^{\pi i \operatorname{Sp}(TB^{tr}D)/p}$$

für alle $T \in \Lambda_2$, $T \geq 0$. Nach (4.6) hat man zu summieren über

$$\begin{aligned}D &= pE, & B &\in \operatorname{Sym}(2; \mathbb{Z}) \bmod p, \\ D &= E, & B &= 0, \\ D &= \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, & B &= \begin{pmatrix} b & 0 \\ 0 & 0 \end{pmatrix}, & b &\in \mathbb{Z} \bmod p, \\ D &= \begin{pmatrix} 1 & d \\ 0 & p \end{pmatrix}, & B &= \begin{pmatrix} 0 & 0 \\ 0 & b \end{pmatrix}, & b, d &\in \mathbb{Z} \bmod p.\end{aligned}$$

Mit der bereits verwendeten Konvention $\alpha_f(T) = 0$ für $T \notin \Lambda_2$ folgt dann

$$\begin{aligned} \alpha_g(T) &= p^{3-2k} \alpha_f(pT) + \alpha_f\left(\frac{1}{p}T\right) \\ &\quad + p^{1-k} \left[\alpha_f\left(\frac{1}{p}T \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}\right) + \sum_{d \bmod p} \alpha_f\left(\frac{1}{p}T \begin{bmatrix} 1 & 0 \\ d & p \end{bmatrix}\right) \right]. \end{aligned}$$

Sei nun

$$T = p^s r \begin{pmatrix} 2n & t \\ t & 2m \end{pmatrix} \geq 0, \quad T \neq 0, \quad \text{ggT}(n, m, t) = 1, \quad p \nmid r, \quad N = 4nm - t^2.$$

Für

$$T' = \frac{1}{p}T \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix} = p^{s-1}r \begin{pmatrix} 2np^2 & pt \\ pt & 2m \end{pmatrix}$$

bzw.

$$T' = \frac{1}{p}T \begin{bmatrix} 1 & 0 \\ d & p \end{bmatrix} = p^{s-1}r \begin{pmatrix} 2(n+td+md^2) & p(t+md) \\ p(t+md) & 2p^2m \end{pmatrix}$$

gilt

$$\varepsilon(T') = p^{s-1}r\mu, \quad \mu \in \{1, p, p^2\}.$$

Um beide Fälle zusammenzufassen betrachten wir

$$\nu := \frac{1}{p-1} \# \{(x, y) \in \mathbb{Z} \times \mathbb{Z}; (x, y) \not\equiv (0, 0) \bmod p, nx^2 + txy + my^2 \equiv 0 \bmod p\},$$

wobei wir obige Lösungen durch $x = 0, y = 1$ oder $x = 1, y = d$ realisieren. Gilt $p \nmid n$, so suchen wir

$$4n(nx^2 + txy + my^2) = (2nx + ty)^2 + Ny^2 \equiv 0 \bmod p.$$

Es gilt mit dem Legendre-Symbol

$$\nu = 1 + \left(\frac{-N}{p}\right) = \begin{cases} 2 & \text{falls } \left(\frac{-N}{p}\right) = 1, \\ 0 & \text{falls } \left(\frac{-N}{p}\right) = -1, \\ 1 & \text{falls } \left(\frac{-N}{p}\right) = 0. \end{cases}$$

Man beachte, dass im Fall $p \mid N$ und $p^2 \nmid N$ stets

$$p^2 \nmid (nx^2 + txy + my^2)$$

gilt und dass im Fall $p^2 \mid N$ die gesuchte Lösung auch

$$p^2 \mid (nx^2 + txy + my^2)$$

erfüllt. Nun verifiziert man, dass dies auch für $p \nmid m$ und den wegen $\text{ggT}(m, n, p) = 1$ verbleibenden Fall $p \mid m, p \mid n, p \nmid t$ gilt. Damit verifiziert man

$$\mu = \begin{cases} 1, & \text{falls } nx^2 + txy + my^2 \not\equiv 0 \pmod{p}, \\ p, & \text{falls } nx^2 + txy + my^2 \equiv 0 \pmod{p}, p^2 \nmid N, \\ p^2, & \text{falls } nx^2 + txy + my^2 \equiv 0 \pmod{p}, p^2 \mid N. \end{cases}$$

Daraus ergibt sich mit (5.19) im Fall $p^2 \nmid N$

$$\begin{aligned} \alpha_g(T) &= p^{3-2k} \alpha_f^*(p^{s+1}r, N) + \alpha_f^*(p^{s-1}r, N) \\ &\quad + p^{1-k} \left[\left(1 + \left(\frac{-N}{p} \right) \right) \alpha_f^*(p^s r, N) + \left(p - \left(\frac{-N}{p} \right) \right) \alpha_f^*(p^{s-1}r, p^2 N) \right] \end{aligned}$$

bzw. für $p^2 \mid N$

$$\begin{aligned} \alpha_g(T) &= p^{3-2k} \alpha_f^*(p^{s+1}r, N) + \alpha_f^*(p^{s-1}r, N) \\ &\quad + p^{1-k} [\alpha_f^*(p^{s+1}r, p^{-2}N) + p \alpha_f^*(p^{s-1}r, p^2 N)]. \end{aligned}$$

Daraus ergibt sich sofort

$$\alpha_g(T) = \alpha_g^*(p^r s, N)$$

mit einer Funktion α_g^* , die man direkt aus den obigen Formeln ablesen kann. Die Identität (ii) in (5.20) ergibt sich für $q \neq p$ direkt aus derjenigen für α_f^* . Sei also $q = p, p \nmid r$. Dann hat man mit (5.19)

$$\begin{aligned} \alpha_g^*(p^s r, N) &= p^{3-2k} \alpha_f^*(p^{s+1}r, N) + \alpha_f^*(p^{s-1}r, N) \\ &\quad + p^{1-k} \alpha_f^*(p^{s+1}r, p^{-2}N) + p^{2-k} \alpha_f^*(p^{s-1}r, p^2 N) \\ &= \sum_{\nu=0}^{s+1} p \cdot p^{(\nu-2)(k-1)} \alpha_f^*(r, p^{2(s+1-\nu)} N) \\ &\quad + \sum_{\nu=0}^{s-1} p^{\nu(k-1)} \alpha_f^*(r, p^{2(s-1-\nu)} N) \\ &\quad + \sum_{\nu=0}^{s+1} p^{(\nu-1)(k-1)} \alpha_f^*(r, p^{2(s-\nu)} N) \\ &\quad + \sum_{\nu=0}^{s-1} p \cdot p^{(\nu-1)(k-1)} \alpha_f^*(r, p^{2(s-\nu)} N) \\ &= \sum_{\nu=-2}^s \beta_\nu p^{\nu(k-1)} \alpha_f^*(r, p^{2(s-1-\nu)} N) \end{aligned}$$

mit $\beta_{-2} = p, \beta_{-1} = 2p + 1, \beta_\nu = 2p + 2$ für $0 \leq \nu \leq s - 2, \beta_{s-1} = p + 2, \alpha_s = 1$.

Andererseits gilt wiederum mit (5.19)

$$\begin{aligned}
& \sum_{\nu=0}^s p^{\nu(k-1)} \alpha_g^*(r, p^{2(s-\nu)} N) \\
&= \sum_{\nu=0}^s p^{\nu(k-1)} \left[p^{3-2k} \alpha_f^*(pr, p^{2(s-\nu)} N) + p^{1-k} \alpha_f^*(pr, p^{2(s-\nu)} N) \right] \\
&= \sum_{\nu=0}^s \left[p \cdot p^{(\nu-2)(k-1)} \alpha_f^*(r, p^{2(s+1-\nu)} N) + p \cdot p^{(\nu-1)(k-1)} \alpha_f^*(r, p^{2(s-\nu)} N) \right. \\
&\quad \left. + p^{(\nu-1)(k-1)} \alpha_f^*(r, p^{2(s+1-\nu)} N) + p^{\nu(k-1)} \alpha_f^*(r, p^{2(s-\nu)} N) \right] \\
&= \alpha_g^*(p^r s, N).
\end{aligned}$$

Für $p^2 \nmid N$ führt eine völlig analoge Rechnung zum Ziel. Nach (5.19) gehört g zu $\mathcal{M}_k^*$. $\square$

Mit völlig analogen Rechnungen zeigt man die gleiche Behauptung für $p = 2$ und für $T_2(p)^2 - T_2(p^2)$. Das Ergebnis ist die

(5.22) Bemerkung. Der Maaß-Raum $\mathcal{M}_k^*$ ist unter allen Hecke-Operatoren invariant.

Als Anwendung erhalten wir den

(5.23) Satz. Für gerades $k > 3$ gilt

$$E_k^{(2)} \in \mathcal{M}_k^*.$$

Beweis. Nach V(2.5) und V(1.10) enthält $\mathcal{M}_k^*$ für gerades $k > 4$ eine Modulform f mit $\alpha_f(0) \neq 0$. Da $\mathcal{M}_k^*$ nach (5.20) unter $T_2(p)$, $p \in \mathbb{P}$ ungerade, invariant ist, folgern wir aus (5.1) und (5.2), dass ein $f \in \mathcal{M}_k^*$ existiert und

$$f \mid_k T_2(p) = \lambda f \quad \text{und} \quad \alpha_f(0) = 1.$$

Nun schließen wir $f = E_k^{(2)}$ aus (5.6). $\square$