Die algebraische Struktur der Hecke-Operatoren I

Vortrag zum Seminar zur Höheren Funktionentheorie, 18.06.2008

Marc Ensenbach

Nachdem in den letzten beiden Vorträgen Hecke-Operatoren definiert und ihre Eigenschaften und Anwendungen diskutiert wurden, soll nun die algebraische Struktur hinter diesen Operatoren untersucht werden.

§1 Rechenregeln für Hecke-Operatoren

Als Vorbereitung für die algebraische Betrachtung der Hecke-Operatoren werden in diesem Abschnitt zwei wichtige Rechenregeln hergeleitet.

— *Multiplikativität* —

Die erste zu beweisende Rechenregel für Hecke-Operatoren trifft eine Aussage über $T_m T_n$ für teilerfremde $m, n \in \mathbb{N}$. Wesentliches Element des Beweises dieser Aussage ist ein Zusammenhang zwischen Vertretersystemen von Restklassenringen ganzer Zahlen.

(1.1) Lemma
Seien $m, n \in \mathbb{N}$ teilerfremd und $a_1, a_2, d_1, d_2 \in \mathbb{Z}$ mit $a_1 d_1 = m$ und $a_2 d_2 = n$. Ist dann B_1 ein Vertretersystem von $\mathbb{Z}/d_1\mathbb{Z}$ und B_2 ein Vertretersystem von $\mathbb{Z}/d_2\mathbb{Z}$, so ist $\{a_2 b_1 + b_2 d_1 \mid b_1 \in B_1 \text{ und } b_2 \in B_2\}$ ein Vertretersystem von $\mathbb{Z}/d_1 d_2\mathbb{Z}$. $\diamond$

Beweis
Da für jedes $i \in \{1, 2\}$ Vertretersysteme von $\mathbb{Z}/d_i\mathbb{Z}$ genau $|d_i|$ Elemente und Vertretersysteme von $\mathbb{Z}/d_1 d_2\mathbb{Z}$ genau $|d_1 d_2|$ Elemente beinhalten, genügt es zu zeigen, dass die $|d_1 d_2|$ Zahlen der Form $a_2 b_1 + b_2 d_1$ für $b_1 \in B_1$ und $b_2 \in B_2$ paarweise nicht kongruent modulo $d_1 d_2$ sind.

Seien nun $b_1, b_1' \in B_1$ und $b_2, b_2' \in B_2$ mit $a_2 b_1' + b_2' d_1 \equiv a_2 b_1 + b_2 d_1 \mod d_1 d_2$. Dann gilt erst recht $a_2 b_1' + b_2' d_1 \equiv a_2 b_1 + b_2 d_1 \mod d_1$ und somit $a_2 b_1' \equiv a_2 b_1 \mod d_1$. Da nach Voraussetzung m und n und damit erst recht a_2 und d_1 teilerfremd sind, gibt es nach dem erweiterten euklidischen Algorithmus $x, y \in \mathbb{Z}$ mit $a_2 x + d_1 y = 1$, also $a_2 x \equiv 1 \mod d_1$, so dass aus $a_2 b_1' \equiv a_2 b_1 \mod d_1$ zunächst $a_2 x b_1' \equiv a_2 x b_1 \mod d_1$ und damit $b_1' \equiv b_1 \mod d_1$ folgt. Da B_1 nach Voraussetzung aber keine zwei verschiedenen Zahlen, die zueinander kongruent modulo d_1 sind, enthält, muss bereits

$b_1' = b_1$ gelten. Aus der Ausgangskongruenz $a_2 b_1' + b_2' d_1 \equiv a_2 b_1 + b_2 d_1 \mod d_1 d_2$ erhält man mit $b_1' = b_1$ nun $b_2' d_1 \equiv b_2 d_1 \mod d_1 d_2$. Da d_1 wegen $a_1 d_1 = m \in \mathbb{N}$ nicht gleich 0 sein darf, kann man durch d_1 dividieren und erhält $b_2' \equiv b_2 \mod d_2$, und da B_2 ein Vertretersystem von $\mathbb{Z}/d_2\mathbb{Z}$ ist, erhält man daraus $b_2' = b_2$. Dies zeigt die Behauptung. $\square$

Mit dem gerade gezeigten Lemma stehen bereits alle nötigen Hilfsmittel zum Beweis der schon angekündigten Multiplikativitätsaussage zur Verfügung.

(1.2) Satz
Sind $m, n \in \mathbb{N}$ teilerfremde Zahlen und ist $f \in V(\mathbb{H})$, so gilt

$$T_m^{(k)} T_n^{(k)} f = T_{mn}^{(k)} f = T_{nm}^{(k)} f = T_n^{(k)} T_m^{(k)} f$$

für alle $k \in \mathbb{Z}$. $\diamond$

Beweis
Für alle $\tau \in \mathbb{H}$ gilt nach 1.1(6)

$$\begin{aligned}
&(T_m^{(k)} T_n^{(k)} f)(\tau) \\
&= m^{k-1} \sum_{\substack{a_1 d_1 = m \\ d_1 > 0}} d_1^{-k} \sum_{b_1 \bmod d_1} T_n^{(k)}(f)\left(\frac{a_1\tau + b_1}{d_1}\right) \\
&= m^{k-1} \sum_{\substack{a_1 d_1 = m \\ d_1 > 0}} d_1^{-k} \sum_{b_1 \bmod d_1} n^{k-1} \sum_{\substack{a_2 d_2 = n \\ d_2 > 0}} d_2^{-k} \sum_{b_2 \bmod d_2} f\left(\frac{a_2 \frac{a_1\tau + b_1}{d_1} + b_2}{d_2}\right) \\
&= (mn)^{k-1} \sum_{\substack{a_1 d_1 = m \\ d_1 > 0}} \sum_{\substack{a_2 d_2 = n \\ d_2 > 0}} (d_1 d_2)^{-k} \sum_{b_1 \bmod d_1} \sum_{b_2 \bmod d_2} f\left(\frac{a_1 a_2 \tau + a_2 b_1 + b_2 d_1}{d_1 d_2}\right) \\
&\overset{(1.1)}{=} (mn)^{k-1} \sum_{\substack{a_1 d_1 = m \\ d_1 > 0}} \sum_{\substack{a_2 d_2 = n \\ d_2 > 0}} (d_1 d_2)^{-k} \sum_{b \bmod d_1 d_2} f\left(\frac{a_1 a_2 \tau + b}{d_1 d_2}\right).
\end{aligned}$$

Da m und n teilerfremd sind, ist

$$\begin{aligned}
&\{(a_1, d_1, a_2, d_2) \in \mathbb{Z}^4 \mid a_1 d_1 = m,\ d_1 > 0,\ a_2 d_2 = m,\ d_2 > 0\} \\
&\quad \to \{(a, d) \in \mathbb{Z}^2 \mid ad = n,\ d > 0\}, \\
&(a_1, d_1, a_2, d_2) \mapsto (a_1 a_2, d_1 d_2)
\end{aligned}$$

eine Bijektion (denn für $x, y \in \mathbb{Z}$ mit $x \mid m$ und $y \mid n$ kann man dann stets x und y aus xy eindeutig bestimmen), also kann man weiter umformen

$$
\begin{aligned}
&(mn)^{k-1} \sum_{\substack{a_1 d_1 = m \\ d_1 > 0}} \sum_{\substack{a_2 d_2 = n \\ d_2 > 0}} (d_1 d_2)^{-k} \sum_{b \bmod d_1 d_2} f\left(\frac{a_1 a_2 \tau + b}{d_1 d_2}\right) \\
&= (mn)^{k-1} \sum_{\substack{ad = mn \\ d > 0}} d^{-k} \sum_{b \bmod d} f\left(\frac{a\tau + b}{d}\right) \\
&= (T_{mn}^{(k)} f)(\tau).
\end{aligned}
$$

Somit ist die erste der behaupteten Gleichheiten bewiesen. Die zweite Gleichheit erhält man wegen $mn = nm$, und die dritte Gleichheit ergibt sich dann wieder mit dem bereits bewiesenen Teil. □

— *Eine Rekursionsformel* —

Nachdem im letzten Teilabschnitt gezeigt wurde, dass $T_m T_n$ für $m, n \in \mathbb{N}$ teilerfremd selbst wieder ein Hecke-Operator ist, stellt sich nun die Frage, ob dies auch im Falle von nicht teilerfremden $m, n \in \mathbb{N}$ gilt. Es wird sich herausstellen, dass dies im Allgemeinen falsch ist. Es gilt jedoch eine schwächere Aussage, die es gestattet, $T_m T_n$ als Linearkombination von Hecke-Operatoren zu schreiben.

Wie im letzten Teilabschnitt werden auch hier Beziehungen zwischen Vertretersystemen von Restklassenringen ganzer Zahlen benötigt.

(1.3) Lemma
Sei p eine Primzahl und $v \in \mathbb{N}_0$. Ist dann B ein Vertretersystem von $\mathbb{Z}/p^v\mathbb{Z}$ und A ein Vertretersystem von $\mathbb{Z}/p\mathbb{Z}$, so ist $\{b + ap^v \mid b \in B \text{ und } a \in A\}$ ein Vertretersystem von $\mathbb{Z}/p^{v+1}\mathbb{Z}$. ◇

Beweis
Wie im Beweis von (1.1) genügt es zu zeigen, dass die Zahlen der Form $b + ap^v$ für $b \in B$ und $a \in A$ paarweise nicht kongruent modulo p^{v+1} sind. Seien nun $b, b' \in B$ und $a, a' \in A$ mit $b + ap^v \equiv b' + a'p^v \mod p^{v+1}$. Dann gilt erst recht die Kongruenz $b + ap^v \equiv b' + a'p^v \mod p^v$, also $b \equiv b' \mod p^v$. Da b und b' zu einem Vertretersystem von $\mathbb{Z}/p^v\mathbb{Z}$ gehören, folgt somit $b = b'$. Eingesetzt in die Ausgangskongruenz erhält man damit $b + ap^v \equiv b + a'p^v \mod p^{v+1}$ und folglich $ap^v \equiv a'p^v \mod p^{v+1}$, womit ein $k \in \mathbb{Z}$ mit $a'p^v = ap^v + kp^{v+1}$ existiert. Dividiert man nun beide Seiten durch p^v, so erhält man $a' = a + kp$, und da a und a' zu einem

Vertretersystem von $\mathbb{Z}/p\mathbb{Z}$ gehören, folgt somit $a = a'$. Damit ist die Behauptung bewiesen. $\square$

Eine Art »Umkehrung« von (1.3) wird ebenfalls benötigt.

(1.4) Lemma
Sei p eine Primzahl und $v \in \mathbb{N}_0$. Ist dann C ein Vertretersystem von $\mathbb{Z}/p^{v+1}\mathbb{Z}$, so gibt es paarweise disjunkte Mengen $B_1, \dots, B_p$ mit $B_1 \cup \dots \cup B_p = C$, so dass B_i für jedes $1 \leq i \leq p$ ein Vertretersystem von $\mathbb{Z}/p^v\mathbb{Z}$ ist. $\diamond$

Beweis
Sei $C = \{c_1, \dots, c_k\}$, wobei $k = p^{v+1}$ gelte. Weiter sei B ein Vertretersystem von $\mathbb{Z}/p^v\mathbb{Z}$ und $A = \{a_1, \dots, a_p\}$ ein Vertretersystem von $\mathbb{Z}/p\mathbb{Z}$. Nach (1.3) ist dann $C' := \{b + a_i p^v \mid b \in B \text{ und } 1 \leq i \leq p\}$ ein Vertretersystem von $\mathbb{Z}/p^{v+1}\mathbb{Z}$. Da auch C ein Vertretersystem von $\mathbb{Z}/p^{v+1}\mathbb{Z}$ ist, gibt es eine Bijektion $\varphi : C' \to C$, so dass $\varphi(c') \equiv c' \mod p^{v+1}$ für alle $c' \in C'$ gilt. Definiert man $B_i = \{\varphi(b + a_i p^v) \mid b \in B\}$ für alle $1 \leq i \leq p$, so liefert die Bijektivität von φ, dass $B_1, \dots, B_p$ paarweise disjunkt sind und $B_1 \cup \dots \cup B_p = C$ gilt, und weiter hat man für jedes $b \in B$ und $1 \leq i \leq p$ die Kongruenz $\varphi(b + a_i p^v) \equiv b + a_i p^v \mod p^{v+1}$ und damit $\varphi(b + a_i p^v) \equiv b \mod p^v$, womit folgt, dass jedes B_i für $1 \leq i \leq p$ ein Vertretersystem von $\mathbb{Z}/p^v\mathbb{Z}$ umfasst. Da B_i darüberhinaus nach Definition aufgrund der Bijektivität von φ genau p^v Elemente hat, folgt, dass B_i für jedes $1 \leq i \leq p$ ein Vertretersystem von $\mathbb{Z}/p^v\mathbb{Z}$ ist. Damit ist die Behauptung bewiesen. $\square$

Als Hauptresultat dieses Teilabschnitts wird eine Rekursionsformel zur Berechnung von $T_n f$ für den Fall, dass n eine Primzahlpotenz ist, bewiesen.

(1.5) Satz
Sei p eine Primzahl, $r \in \mathbb{N}$ und $k \in \mathbb{N}$ sowie $f \in V(\mathbb{H})$. Dann gilt

$$T^{(k)}_{p^{r+1}} f = T^{(k)}_{p^r} T^{(k)}_p f - p^{k-1} T^{(k)}_{p^{r-1}} f,$$

wobei man $T^{(k)}_{p^0} = T^{(k)}_1$ als identische Abbildung auffasst. $\diamond$

Beweis
Für alle $\tau \in \mathbb{H}$ gilt

$$
\begin{aligned}
(T_{p^r}^{(k)} T_p^{(k)} f)(\tau) &\overset{1.1(6)}{=} (p^r)^{k-1} \sum_{\substack{ad=p^r\\ d>0}} d^{-k} \sum_{b \bmod d} (T_p^{(k)} f)\left(\frac{a\tau+b}{d}\right) \\
&= p^{r(k-1)} \sum_{v=0}^{r} (p^v)^{-k} \sum_{b \bmod p^v} (T_p^{(k)} f)\left(\frac{p^{r-v}\tau+b}{p^v}\right) \\
&\overset{1.1(7)}{=} p^{r(k-1)} \sum_{v=0}^{r} p^{-vk} \sum_{b \bmod p^v} \left(p^{k-1} f\left(p\,\frac{p^{r-v}\tau+b}{p^v}\right)\right. \\
&\qquad \left. + p^{-1} \sum_{a \bmod p} f\left(\frac{\frac{p^{r-v}\tau+b}{p^v}+a}{p}\right)\right) \\
&= p^{r(k-1)} \sum_{v=1}^{r} p^{-vk} \sum_{b \bmod p^v} p^{k-1} f\left(\frac{p^{r-v}\tau+b}{p^{v-1}}\right) \\
&\qquad + p^{(r+1)(k-1)} f(p^{r+1}\tau) \\
&\qquad + p^{r(k-1)} \sum_{v=0}^{r} p^{-vk} \sum_{b \bmod p^v} p^{-1} \sum_{a \bmod p} f\left(\frac{p^{r-v}\tau+b+ap^v}{p^{v+1}}\right).
\end{aligned}
$$

Da f periodisch zur Periode 1 ist, gilt für $b \equiv b' \mod p^{v-1}$ stets

$$
f\left(\frac{p^{r-v}\tau+b'}{p^{v-1}}\right) = f\left(\frac{p^{r-v}\tau+b}{p^{v-1}}\right).
$$

Mit (1.4) erhält man daraus

$$
\begin{aligned}
\sum_{b \bmod p^v} p^{k-1} f\left(\frac{p^{r-v}\tau+b}{p^{v-1}}\right) &= p \sum_{b \bmod p^{v-1}} p^{k-1} f\left(\frac{p^{r-v}\tau+b}{p^{v-1}}\right) \\
&= p^k \sum_{b \bmod p^{v-1}} f\left(\frac{p^{r-v}\tau+b}{p^{v-1}}\right).
\end{aligned}
$$

Weiter hat man

$$
\sum_{b \bmod p^v} p^{-1} \sum_{a \bmod p} f\left(\frac{p^{r-v}\tau+b+ap^v}{p^{v+1}}\right) \overset{(1.3)}{=} p^{-1} \sum_{c \bmod p^{v+1}} f\left(\frac{p^{r-v}\tau+c}{p^{v+1}}\right).
$$

Mit diesen Gleichungen erhält man nun

$$
\begin{aligned}
& p^{r(k-1)} \sum_{v=1}^{r} p^{-vk} \sum_{b \bmod p^v} p^{k-1} f\left(\frac{p^{r-v}\tau + b}{p^{v-1}}\right) + p^{(r+1)(k-1)} f(p^{r+1}\tau) \\
& + p^{r(k-1)} \sum_{v=0}^{r} p^{-vk} \sum_{b \bmod p^v} p^{-1} \sum_{a \bmod p} f\left(\frac{p^{r-v}\tau + b + ap^v}{p^{v+1}}\right) \\
= \; & p^{r(k-1)} \sum_{v=1}^{r} p^{-(v-1)k} \sum_{b \bmod p^{v-1}} f\left(\frac{p^{r-v}\tau + b}{p^{v-1}}\right) + p^{(r+1)(k-1)} f(p^{r+1}\tau) \\
& + p^{r(k-1)} \sum_{v=0}^{r} p^{-vk-1} \sum_{c \bmod p^{v+1}} f\left(\frac{p^{r-v}\tau + c}{p^{v+1}}\right) \\
= \; & p^{r(k-1)} \sum_{v=0}^{r-1} p^{-vk} \sum_{b \bmod p^v} f\left(\frac{p^{r-v-1}\tau + b}{p^{v}}\right) + p^{(r+1)(k-1)} f(p^{r+1}\tau) \\
& + p^{(r+1)(k-1)} \sum_{v=1}^{r+1} p^{-vk} \sum_{c \bmod p^v} f\left(\frac{p^{r-v+1}\tau + c}{p^{v}}\right) \\
\overset{1.1(6)}{=} \; & p^{r(k-1)} p^{-(r-1)(k-1)} (T^{(k)}_{p^{r-1}} f)(\tau) \\
& + p^{(r+1)(k-1)} \sum_{v=0}^{r+1} p^{-vk} \sum_{c \bmod p^v} f\left(\frac{p^{r-v+1}\tau + c}{p^{v}}\right) \\
\overset{1.1(6)}{=} \; & p^{r(k-1)} p^{-(r-1)(k-1)} (T^{(k)}_{p^{r-1}} f)(\tau) \\
& + p^{(r+1)(k-1)} p^{-(r+1)(k-1)} (T^{(k)}_{p^{r+1}} f)(\tau) \\
= \; & p^{k-1} (T^{(k)}_{p^{r-1}} f)(\tau) + (T^{(k)}_{p^{r+1}} f)(\tau),
\end{aligned}
$$

also insgesamt

$$T^{(k)}_{p^r} T^{(k)}_{p} f = p^{k-1} T^{(k)}_{p^{r-1}} f + T^{(k)}_{p^{r+1}} f,$$

was die Behauptung beweist. □

Als Anwendung des gerade bewiesenen Satzes erhält man eine Formel, die $T_m T_n$ als Linearkombination von Hecke-Operatoren darstellt, wenn m und n Potenzen derselben Primzahl $p \in \mathbb{N}$ sind.

(1.6) Korollar
Sei p eine Primzahl und $k \in \mathbb{N}$. Weiter seien $r, s \in \mathbb{N}_0$. Dann gilt

$$T^{(k)}_{p^r} T^{(k)}_{p^s} = \sum_{v=0}^{\min\{r,s\}} p^{v(k-1)} T^{(k)}_{p^{r+s-2v}}.$$

Insbesondere gilt $T^{(k)}_{p^r} T^{(k)}_{p^s} = T^{(k)}_{p^s} T^{(k)}_{p^r}$. ◇

Beweis
Beweise die Behauptung durch Induktion nach s.

(IA) Die Behauptung für $s = 0$ ist trivial, für $s = 1$ ist sie äquivalent zu (1.5).

(IV) Sei nun $s \in \mathbb{N}$, und es gelte die Behauptung mit s' anstelle von s für alle $s' < s$.

(IS) Es gilt

$$\begin{aligned}
T^{(k)}_{p^r} T^{(k)}_{p^{s+1}} &\overset{(1.5)}{=} T^{(k)}_{p^r} \left(T^{(k)}_{p^s} T^{(k)}_p - p^{k-1} T^{(k)}_{p^{s-1}} \right) = T^{(k)}_{p^r} T^{(k)}_{p^s} T^{(k)}_p - p^{k-1} T^{(k)}_{p^r} T^{(k)}_{p^{s-1}} \\
&\overset{(IV)}{=} \sum_{v=0}^{\min\{r,s\}} p^{v(k-1)} T^{(k)}_{p^{r+s-2v}} T^{(k)}_p - p^{k-1} \sum_{v=0}^{\min\{r,s-1\}} p^{v(k-1)} T^{(k)}_{p^{r+s-1-2v}} \\
&= \sum_{\substack{0 \le v \le \min\{r,s\} \\ r+s-2v<1}} p^{v(k-1)} T^{(k)}_{p^{r+s-2v}} T^{(k)}_p + \sum_{\substack{0 \le v \le \min\{r,s\} \\ r+s-2v\ge 1}} p^{v(k-1)} T^{(k)}_{p^{r+s-2v}} T^{(k)}_p \\
&\quad - p^{k-1} \sum_{v=0}^{\min\{r,s-1\}} p^{v(k-1)} T^{(k)}_{p^{r+s-1-2v}} \\
&\overset{(1.5)}{=} \sum_{\substack{0 \le v \le \min\{r,s\} \\ r+s-2v<1}} p^{v(k-1)} T^{(k)}_{p^{r+s-2v}} T^{(k)}_p \\
&\quad + \sum_{\substack{0 \le v \le \min\{r,s\} \\ r+s-2v\ge 1}} p^{v(k-1)} \left(T^{(k)}_{p^{r+s-2v+1}} + p^{k-1} T^{(k)}_{p^{r+s-2v-1}} \right) \\
&\quad - p^{k-1} \sum_{v=0}^{\min\{r,s-1\}} p^{v(k-1)} T^{(k)}_{p^{r+s-1-2v}} \\
&= \sum_{\substack{0 \le v \le \min\{r,s\} \\ r+s-2v<1}} p^{v(k-1)} T^{(k)}_{p^{r+s-2v}} T^{(k)}_p + \sum_{\substack{0 \le v \le \min\{r,s\} \\ r+s-2v\ge 1}} p^{v(k-1)} T^{(k)}_{p^{r+s-2v+1}} \\
&\quad + \sum_{\substack{0 \le v \le \min\{r,s\} \\ r+s-2v\ge 1}} p^{(v+1)(k-1)} T^{(k)}_{p^{r+s-2v-1}} - \sum_{v=0}^{\min\{r,s-1\}} p^{(v+1)(k-1)} T^{(k)}_{p^{r+s-2v-1}}.
\end{aligned}$$

Im Falle $r \geq s+1$ gilt für $0 \leq v \leq \min\{r,s\} = s$ stets $r+s-2v \geq r-v \geq 1$ und $\min\{r,s-1\} = s-1$, also vereinfacht sich obige Gleichung dann zu

$$\begin{aligned} T_{p^r}^{(k)} T_{p^{s+1}}^{(k)} &= \sum_{v=0}^{s} p^{v(k-1)} T_{p^{r+s-2v+1}}^{(k)} + \sum_{v=0}^{s} p^{(v+1)(k-1)} T_{p^{r+s-2v-1}}^{(k)} - \sum_{v=0}^{s-1} p^{(v+1)(k-1)} T_{p^{r+s-2v-1}}^{(k)} \\ &= \sum_{v=0}^{s} p^{v(k-1)} T_{p^{r+s-2v+1}}^{(k)} + p^{(s+1)(k-1)} T_{p^{r+s-2s-1}}^{(k)} \\ &= \sum_{v=0}^{s+1} p^{v(k-1)} T_{p^{r+s-2v+1}}^{(k)} = \sum_{v=0}^{\min\{r,s+1\}} p^{v(k-1)} T_{p^{r+s-2v+1}}^{(k)}, \end{aligned}$$

was die Behauptung für $s+1$ anstelle von s ist. Im Falle $r = s$ gilt $r+s-2v = 0$ für $v = s$ und $r+s-2v \geq 1$ für alle $0 \leq v < s$ sowie $\min\{r,s-1\} = s-1$, also vereinfacht sich obige Gleichung zu

$$\begin{aligned} T_{p^r}^{(k)} T_{p^{s+1}}^{(k)} &= p^{s(k-1)} T_1^{(k)} T_p^{(k)} + \sum_{v=0}^{s-1} p^{v(k-1)} T_{p^{2s-2v+1}}^{(k)} \\ &\quad + \sum_{v=0}^{s-1} p^{(v+1)(k-1)} T_{p^{2s-2v-1}}^{(k)} - \sum_{v=0}^{s-1} p^{(v+1)(k-1)} T_{p^{2s-2v-1}}^{(k)} \\ &= p^{s(k-1)} T_1^{(k)} T_p^{(k)} + \sum_{v=0}^{s-1} p^{v(k-1)} T_{p^{2s-2v+1}}^{(k)} = \sum_{v=0}^{s} p^{v(k-1)} T_{p^{2s-2v+1}}^{(k)} \\ &\overset{r=s}{=} \sum_{v=0}^{\min\{r,s+1\}} p^{v(k-1)} T_{p^{r+s-2v+1}}^{(k)}, \end{aligned}$$

was die Behauptung für $s+1$ anstelle von s ist. Im Falle $r < s$ schließlich gilt für $0 \leq v \leq \min\{r,s\} = r$ stets $r+s-2v \geq s-v \geq 1$ und $\min\{r,s-1\} = r$, also vereinfacht sich obige Gleichung dann zu

$$\begin{aligned} T_{p^r}^{(k)} T_{p^{s+1}}^{(k)} &= \sum_{v=0}^{r} p^{v(k-1)} T_{p^{r+s-2v+1}}^{(k)} + \sum_{v=0}^{r} p^{(v+1)(k-1)} T_{p^{r+s-2v-1}}^{(k)} - \sum_{v=0}^{r} p^{(v+1)(k-1)} T_{p^{r+s-2v-1}}^{(k)} \\ &= \sum_{v=0}^{r} p^{v(k-1)} T_{p^{r+s-2v+1}}^{(k)} = \sum_{v=0}^{\min\{r,s+1\}} p^{v(k-1)} T_{p^{r+s-2v+1}}^{(k)}, \end{aligned}$$

was ebenfalls die Behauptung für $s+1$ anstelle von s ist. Somit ist der Induktionsschluss vollständig. □

§2 Die Algebra der Hecke-Operatoren

In diesem Abschnitt wird aus den Hecke-Operatoren eine $\mathbb{C}$-Algebra von Endomorphismen von $\mathbb{M}_k$ konstruiert. Zunächst wird dazu eine Bezeichnung für den zugrundeliegenden $\mathbb{C}$-Vektorraum eingeführt.

(2.1) Bezeichnung
Für jedes $k \in \mathbb{N}_0$ führt man die Bezeichnung

$$\mathcal{H}_k = \left\{ \sum_{n \in N} \alpha_n T_n^{(k)} \;\middle|\; N \subseteq \mathbb{N} \text{ endlich und } \alpha_n \in \mathbb{C} \text{ für alle } n \in N \right\}$$

ein. ◇

Nun wird der $\mathbb{C}$-Vektorraum $\mathcal{H}_k$ zusammen mit einer weiteren Verknüpfung zu einer Algebra gemacht.

(2.2) Satz
Sei $k \in \mathbb{N}_0$. Der $\mathbb{C}$-Vektorraum $\mathcal{H}_k$ wird zusammen mit der Hintereinanderausführung von Operatoren zu einer kommutativen $\mathbb{C}$-Algebra mit Eins, die Unteralgebra von $\operatorname{End} \mathbb{M}_k$ ist, wobei $\operatorname{End} \mathbb{M}_k$ die $\mathbb{C}$-Algebra aller Endomorphismen auf $\mathbb{M}_k$ bezeichnet. Als $\mathbb{C}$-Algebra wird $\mathcal{H}_k$ von den $T_p^{(k)}$ für Primzahlen $p \in \mathbb{N}$ erzeugt. Sind $m, n \in \mathbb{N}$, so gilt

$$T_m^{(k)} T_n^{(k)} = \sum_{\substack{d \mid (m,n) \\ d > 0}} d^{k-1} T_{\frac{mn}{d^2}}^{(k)}.$$

Insbesondere gibt es zu jedem $n \in \mathbb{N}$ eine endliche Menge $\{p_1, \ldots, p_l\}$ von Primzahlen, so dass $T_n^{(k)} \in \mathbb{Q}[T_{p_1}^{(k)}, \ldots, T_{p_l}^{(k)}]$ gilt. ◇

Beweis
(1) Das Einselement von $\mathcal{H}_k$ ist die identische Abbildung T_1, und dass $\mathcal{H}_k \subseteq \operatorname{End} \mathbb{M}_k$ gilt, folgt nach Definition von $\mathcal{H}_k$ bereits aus der Tatsache, dass T_n für jedes $n \in \mathbb{N}$ nach Korollar 1.3 ein Endomorphismus von $\mathbb{M}_k$ ist.

(2) Für jedes $r \in \mathbb{N}_0$ und jede Primzahl $p \in \mathbb{N}$ ist $T_{p^r}^{(k)}$ ein Polynom in $T_p^{(k)}$ mit Koeffizienten in $\mathbb{Q}$: Für $r \in \{0, 1\}$ ist diese Aussage klar. Ist $r \geq 1$ und ist $T_{p^s}^{(k)}$ für alle $s \leq r$ ein Polynom in $T_p^{(k)}$ mit Koeffizienten in $\mathbb{Q}$, so ist auch

$$T_{p^{r+1}}^{(k)} \overset{(1.5)}{=} T_{p^r}^{(k)} T_p^{(k)} - p^{k-1} T_{p^{r-1}}^{(k)}$$

als Produkt von Polynomen selbst wieder ein Polynom in $T_p^{(k)}$ mit Koeffizienten in $\mathbb{Q}$. Induktiv folgt nun die Behauptung.

(3) Die Hecke-Algebra $\mathcal{H}_k$ ist kommutativ: Führe zunächst die Bezeichnung $v_p(n)$ für alle $n \in \mathbb{N}$ und Primzahlen $p \in \mathbb{N}$ für die Vielfachheit von p in der Primfaktorzerlegung von n ein, so dass stets

$$n = \prod_{p \text{ Primzahl}} p^{v_p(n)}$$

gilt. Sind nun $R, S \in \mathcal{H}_k$ mit

$$R = \sum_{m \in M} \alpha_m T_m^{(k)} \quad \text{und} \quad S = \sum_{n \in N} \beta_n T_n^{(k)}$$

für endliche Mengen $M, N \subseteq \mathbb{N}$, so folgt

$$\begin{aligned} RS &= \left(\sum_{m \in M} \alpha_m T_m^{(k)} \right) \left(\sum_{n \in N} \beta_n T_n^{(k)} \right) = \sum_{\substack{m \in M \\ n \in N}} \alpha_m \beta_n T_m^{(k)} T_n^{(k)} \\ &\overset{(1.2)}{=} \sum_{\substack{m \in M \\ n \in N}} \alpha_m \beta_n \left(\prod_{p \text{ Primzahl}} T_{p^{v_p(m)}}^{(k)} \right) \left(\prod_{p \text{ Primzahl}} T_{p^{v_p(n)}}^{(k)} \right) \\ &= \sum_{\substack{m \in M \\ n \in N}} \alpha_m \beta_n \prod_{p \text{ Primzahl}} T_{p^{v_p(m)}}^{(k)} T_{p^{v_p(n)}}^{(k)}. \end{aligned}$$

Zu jeder Primzahl $p \in \mathbb{N}$ existiert nach (2) für jedes $m \in M$ ein Polynom $F_{m,p} \in \mathbb{Q}[X]$ und für jedes $n \in N$ ein Polynom $G_{n,p} \in \mathbb{Q}[X]$ mit

$$T_{p^{v_p(m)}}^{(k)} = F_{m,p}(T_p^{(k)}) \quad \text{und} \quad T_{p^{v_p(n)}}^{(k)} = G_{n,p}(T_p^{(k)}).$$

Für $r, s \in \mathbb{N}_0$ gilt stets

$$(T_p^{(k)})^r (T_p^{(k)})^s = (T_p^{(k)})^{r+s} = (T_p^{(k)})^{s+r} = (T_p^{(k)})^s (T_p^{(k)})^r,$$

also folgt

$$\begin{aligned}
\sum_{\substack{m\in M\\ n\in N}} \alpha_m\beta_n \prod_{p \text{ Primzahl}} T^{(k)}_{p^{v_p(m)}} T^{(k)}_{p^{v_p(n)}} &= \sum_{\substack{m\in M\\ n\in N}} \alpha_m\beta_n \prod_{p \text{ Primzahl}} F_{m,p}(T^{(k)}_p) G_{n,p}(T^{(k)}_p) \\
&= \sum_{\substack{m\in M\\ n\in N}} \beta_n\alpha_m \prod_{p \text{ Primzahl}} G_{n,p}(T^{(k)}_p) F_{m,p}(T^{(k)}_p) \\
&= \sum_{\substack{m\in M\\ n\in N}} \beta_n\alpha_m \prod_{p \text{ Primzahl}} T^{(k)}_{p^{v_p(n)}} T^{(k)}_{p^{v_p(m)}} \\
&= \sum_{\substack{m\in M\\ n\in N}} \beta_n\alpha_m \left(\prod_{p \text{ Primzahl}} T^{(k)}_{p^{v_p(n)}}\right)\left(\prod_{p \text{ Primzahl}} T^{(k)}_{p^{v_p(m)}}\right) \\
&\overset{(1.2)}{=} \sum_{\substack{m\in M\\ n\in N}} \beta_n\alpha_m T^{(k)}_n T^{(k)}_m \\
&= \left(\sum_{n\in N} \beta_n T^{(k)}_n\right)\left(\sum_{m\in M} \alpha_m T^{(k)}_m\right) = SR.
\end{aligned}$$

(4) Zeige nun die Formel für das Produkt zweier Hecke-Operatoren durch Induktion nach der Anzahl w der verschiedenen Primteiler von mn. Ist $w = 1$, so existieren $r, s \in \mathbb{N}_0$ und eine Primzahl $p \in \mathbb{N}$ mit $m = p^r$ sowie $n = p^s$. Dann hat man

$$T^{(k)}_m T^{(k)}_n = T^{(k)}_{p^r} T^{(k)}_{p^s} \overset{(1.6)}{=} \sum_{v=0}^{\min\{r,s\}} p^{v(k-1)} T^{(k)}_{p^{r+s-2v}} = \sum_{\substack{d\mid(p^r,p^s)\\ d>0}} d^{k-1} T^{(k)}_{\frac{p^r p^s}{d^2}}.$$

Sei nun $w \geq 2$, und es sei die behauptete Produktformel bereits für $m', n' \in \mathbb{N}$ anstelle von m beziehungsweise n bewiesen, wenn $m'n'$ genau $w-1$ verschiedene Primteiler hat. Betrachte zunächst den Fall, dass m und n teilerfremd sind. Dann gilt

$$T^{(k)}_m T^{(k)}_n \overset{(1.2)}{=} T^{(k)}_{mn} = 1^{k-1} T^{(k)}_{\frac{mn}{1}} = \sum_{\substack{d\mid(m,n)\\ d>0}} d^{k-1} T^{(k)}_{\frac{mn}{d^2}}.$$

Andernfalls wähle eine Primzahl $p \in \mathbb{N}$ mit $p \mid (m, n)$. Dann gibt es $m', n' \in \mathbb{N}$ und $r, s \in \mathbb{N}$ mit $m = p^r m'$ und $n = p^s n'$ sowie $p \nmid m'$ und $p \nmid n'$. Dann folgt auch $p \nmid m'n'$, aber es gilt $q \mid m'n'$ für Primzahlen $q \neq p$ genau dann, wenn $q \mid mn$ gilt. Somit hat $m'n'$ genau $w-1$ verschiedene Primteiler. Gemäß Induktionsvoraussetzung gilt nun

$$T^{(k)}_{m'} T^{(k)}_{n'} = \sum_{\substack{d\mid(m',n')\\ d>0}} d^{k-1} T^{(k)}_{\frac{m'n'}{d^2}}.$$

Damit erhält man

$$\begin{aligned}
T_m^{(k)} T_n^{(k)} &= T_{p^r m'}^{(k)} T_{p^s n'}^{(k)} \overset{(1.2)}{=} T_{p^r}^{(k)} T_{m'}^{(k)} T_{p^s}^{(k)} T_{n'}^{(k)} \overset{(3)}{=} (T_{p^r}^{(k)} T_{p^s}^{(k)})(T_{m'}^{(k)} T_{n'}^{(k)}) \\
&= \left(\sum_{t|(p^r,p^s),\, t>0} t^{k-1} T^{(k)}_{\frac{p^r p^s}{t^2}} \right) \left(\sum_{d|(m',n'),\, d>0} d^{k-1} T^{(k)}_{\frac{m'n'}{d^2}} \right) \\
&= \sum_{\substack{t|(p^r,p^s),\, t>0 \\ d|(m,n),\, d>0}} (td)^{k-1} T^{(k)}_{\frac{p^r p^s}{t^2}} T^{(k)}_{\frac{m'n'}{d^2}} \\
&\overset{(1.2)}{=} \sum_{\substack{t|(p^r,p^s),\, t>0 \\ d|(m,n),\, d>0}} (td)^{k-1} T^{(k)}_{\frac{p^r p^s m'n'}{t^2 d^2}} \\
&= \sum_{u|(p^r m',p^s n'),\, u>0} u^{k-1} T^{(k)}_{\frac{p^r p^s m'n'}{u^2}} = \sum_{u|(m,n),\, u>0} u^{k-1} T^{(k)}_{\frac{mn}{u^2}}.
\end{aligned}$$

(5) Für jedes $n \in \mathbb{N}$ gilt

$$T_n = \prod_{p \text{ Primzahl}} T^{(k)}_{p^{v_p(n)}} = \prod_{p \text{ Primzahl}} G_{n,p}(T_p^{(k)})$$

mit den Bezeichnungen aus (3). Da $v_p(n) = 0$ nur für endlich viele Primzahlen $p \in \mathbb{N}$ gilt, kann auch $G_{n,p}$ nur für endlich viele Primzahlen $p \in \mathbb{N}$ von 1 verschieden sein. Bezeichnet man diese Primzahlen mit $p_1, \ldots, p_l$, so gilt

$$\prod_{p \text{ Primzahl}} G_{n,p}(T_p^{(k)}) = \prod_{i=1}^{l} G_{n,p_i}(T_{p_i}^{(k)}) \in \mathbb{Q}[T_{p_1}^{(k)}, \ldots, T_{p_l}^{(k)}].$$

□

Die gerade bewiesenen Eigenschaften von $\mathcal{H}_k$ geben Anlass zu der folgenden Definition.

(2.3) Definition (Hecke-Algebra)
Sei $k \in \mathbb{N}_0$. Der $\mathbb{C}$-Vektorraum $\mathcal{H}_k$ zusammen mit der Hintereinanderausführung von Operatoren heißt *Hecke-Algebra* vom Gewicht k. Kurz wird auch von der Hecke-Algebra $\mathcal{H}_k$ gesprochen. ◇

§ 3 Die Eisenstein-Reihen als simultane Eigenformen

Die Ergebnisse des letzten Abschnitts werden nun für die Untersuchung simultaner Eigenformen verwendet.

(3.1) Korollar
Sei $k \in \mathbb{N}$ und $f \in \mathbb{M}_k$ nicht konstant mit $\alpha_f(1) \neq 0$. Dann sind äquivalent:

(i) Die Funktion f ist simultane Eigenform bezüglich aller Hecke-Operatoren.

(ii) Zu jeder Primzahl p gibt es ein $\lambda_f(p) \in \mathbb{C}$ mit $T_p^{(k)} f = \lambda_f(p) f$.

(iii) Für jede Primzahl p und alle $m \in \mathbb{N}_0$ gilt

$$\alpha_f(p)\alpha_f(m) = \alpha_f(1)(\alpha_f(mp) + p^{k-1}\alpha_f(\tfrac{m}{p})),$$

wobei im Fall $p \nmid m$ noch $\alpha_f(\frac{m}{p}) = 0$ gesetzt sei.

Ist eine der Bedingung (i), (ii), (iii) erfüllt, so gilt

$$T_n^{(k)} f = \frac{\alpha_f(n)}{\alpha_f(1)} f \quad \text{für alle } n \in \mathbb{N}.$$

◇

Beweis
(i) $\Rightarrow$ (ii): trivial

(ii) $\Rightarrow$ (i): Sei $n \in \mathbb{N}$. Gemäß (2.2) existieren Primzahlen $p_1, \dots, p_l \in \mathbb{N}$, eine endliche Menge $I \subseteq \mathbb{N}^l$ und $c_i \in \mathbb{Q}$ für alle $i \in I$ mit

$$T_n^{(k)} = \sum_{i=(i_1,\dots,i_l)\in I} c_i (T_{p_1}^{(k)})^{i_1} \cdots (T_{p_l}^{(k)})^{i_l},$$

also

$$\begin{aligned} T_n^{(k)} f &= \sum_{i=(i_1,\dots,i_l)\in I} c_i (T_{p_1}^{(k)})^{i_1} \cdots (T_{p_l}^{(k)})^{i_l} f \\ &= \sum_{i=(i_1,\dots,i_l)\in I} c_i (T_{p_1}^{(k)})^{i_1} \cdots (T_{p_{l-1}}^{(k)})^{i_{l-1}} \lambda_f(p_l)^{i_l} f \\ &= \sum_{i=(i_1,\dots,i_l)\in I} c_i \lambda_f(p_l)^{i_l} (T_{p_1}^{(k)})^{i_1} \cdots (T_{p_{l-1}}^{(k)})^{i_{l-1}} f \\ &= \cdots = \sum_{i=(i_1,\dots,i_l)\in I} c_i \lambda_f(p_1)^{i_1} \cdots \lambda_f(p_l)^{i_l} f, \end{aligned}$$

also ist f eine Eigenform von T_n. Da $n \in \mathbb{N}$ beliebig war, folgt (i).

(ii) $\Leftrightarrow$ (iii): Nach Korollar 1.1 gilt

$$\alpha_{T_p^{(k)} f}(m) = \begin{cases} \alpha_f(mp), & \text{falls } p \nmid m, \\ \alpha_f(mp) + p^{k-1}\alpha_f(\frac{m}{p}), & \text{falls } p \mid m, \end{cases}$$

also mit der Konvention aus (iii) stets $\alpha_{T_p^{(k)}f}(m) = \alpha_f(mp) + p^{k-1}\alpha_f(\frac{m}{p})$. Somit gilt

$$\begin{aligned}
&T_p^{(k)}f = \lambda_f(p)f && \Leftrightarrow\\
&\forall m \in \mathbb{N}_0 : \ \alpha_{T_p^{(k)}f}(m) = \lambda_f(p)\alpha_f(m) && \Leftrightarrow\\
&\forall m \in \mathbb{N}_0 : \ \alpha_f(mp) + p^{k-1}\alpha_f(\tfrac{m}{p}) = \lambda_f(p)\alpha_f(m).
\end{aligned}$$

Ist diese Bedingung erfüllt, so folgt für $m = 1$ insbesondere $\alpha_f(p) = \lambda_f(p)\alpha_f(1)$, also hat man

$$\begin{aligned}
&\forall m \in \mathbb{N}_0 : \ \alpha_f(mp) + p^{k-1}\alpha_f(\tfrac{m}{p}) = \lambda_f(p)\alpha_f(m) && \Rightarrow\\
&\forall m \in \mathbb{N}_0 : \ \alpha_f(1)(\alpha_f(mp) + p^{k-1}\alpha_f(\tfrac{m}{p})) = \alpha_f(1)\lambda_f(p)\alpha_f(m) = \alpha_f(p)\alpha_f(m),
\end{aligned}$$

was die Bedingung aus (iii) ist. Damit ist (ii) $\Rightarrow$ (iii) bewiesen. Nun sei umgekehrt die Bedingung aus (iii) erfüllt. Wegen $\alpha_f(1) \neq 0$ ist $\lambda_f(p) := \alpha_f(1)^{-1}\alpha_f(p)$ wohldefiniert. Nun gilt

$$\begin{aligned}
&\forall m \in \mathbb{N}_0 : \ \alpha_f(p)\alpha_f(m) = \alpha_f(1)(\alpha_f(mp) + p^{k-1}\alpha_f(\tfrac{m}{p})) && \overset{\alpha_f(1)\neq 0}{\Rightarrow}\\
&\forall m \in \mathbb{N}_0 : \ \alpha_f(1)^{-1}\alpha_f(p)\alpha_f(m) = (\alpha_f(mp) + p^{k-1}\alpha_f(\tfrac{m}{p})) && \Rightarrow\\
&\forall m \in \mathbb{N}_0 : \ \lambda_f(p)\alpha_f(m) = (\alpha_f(mp) + p^{k-1}\alpha_f(\tfrac{m}{p})),
\end{aligned}$$

was nach obiger Äquivalenzumformung gleichbedeutend mit der Bedingung aus (ii) ist. □

Mit diesem Korollar kann gezeigt werden, dass die Eisensteinreihen simultane Eigenformen sind. Das folgende Lemma dient als Vorbereitung des Beweises.

(3.2) Lemma
Sei $k \in \mathbb{N}$ und $\alpha(m) = \sigma_{k-1}(m)$ für alle $m \in \mathbb{N}$. Für jede Primzahl p gilt dann

$$\alpha(p)\alpha(m) = \alpha(mp) + p^{k-1}\alpha(\tfrac{m}{p}),$$

wenn man $\alpha(\frac{m}{p}) = 0$ für im Falle $p \nmid m$ setzt. ◇

Beweis
Sei $p \in \mathbb{N}$ eine Primzahl. Für jedes $r \in \mathbb{N}$ gilt

$$\alpha(p^r) = \sigma_{k-1}(p^r) = \sum_{\substack{d|p^r\\ d>0}} d^{k-1} = \sum_{v=0}^{r}(p^v)^{k-1} = \sum_{v=0}^{r}(p^{k-1})^v = \frac{(p^{k-1})^{r+1}-1}{p^{k-1}-1},$$

also hat man

$$\begin{aligned}\alpha(p)\alpha(p^r) &= \frac{(p^{k-1})^2-1}{p^{k-1}-1}\cdot\frac{(p^{k-1})^{r+1}-1}{p^{k-1}-1} = (p^{k-1}+1)\frac{(p^{k-1})^{r+1}-1}{p^{k-1}-1}\\ &= \frac{(p^{k-1})^{r+2}+(p^{k-1})^{r+1}-p^{k-1}-1}{p^{k-1}-1}\\ &= \frac{((p^{k-1})^{r+2}-1)+p^{k-1}((p^{k-1})^{r}-1)}{p^{k-1}-1}\\ &= \frac{(p^{k-1})^{r+2}-1}{p^{k-1}-1}+p^{k-1}\frac{(p^{k-1})^{r}-1}{p^{k-1}-1} = \alpha(p^{r+1})+p^{k-1}\alpha(p^{r-1})\end{aligned}$$

für alle $r\in\mathbb{N}$.

Ist p kein Teiler von m, so gilt $\alpha(p)\alpha(m)=\alpha(mp)$ aufgrund der Multiplikativität von σ_{k-1}, was die Behauptung in diesem Fall beweist. Sei nun p ein Teiler von m. Dann gibt es ein $r\in\mathbb{N}$ und ein $m'\in\mathbb{N}$ mit $p\nmid m'$ und $m=p^rm'$. Mit der oben bewiesenen Formel für $\alpha(p)\alpha(p^r)$ und der Multiplikativität der σ_{k-1} erhält man

$$\begin{aligned}\alpha(p)\alpha(m) &= \alpha(p)\alpha(p^rm') = \alpha(p)\alpha(p^r)\alpha(m') = (\alpha(p^{r+1})+p^{k-1}\alpha(p^{r-1}))\alpha(m')\\ &= \alpha(p^{r+1})\alpha(m')+p^{k-1}\alpha(p^{r-1})\alpha(m') = \alpha(p^{r+1}m')+p^{k-1}\alpha(p^{r-1}m')\\ &= \alpha(pp^rm')+p^{k-1}\alpha(p^{-1}p^rm') = \alpha(pm)+p^{k-1}\alpha(\tfrac{m}{p}),\end{aligned}$$

was den Beweis der Behauptung abschließt. □

Mit diesem Hilfsresultat kann nun die schon angekündigte Aussage, dass Eisenstein-Reihen simultane Eigenformen sind, bewiesen werden.

(3.3) Korollar
Die Eisenstein-Reihe G_k ist für jedes gerade $k\in\mathbb{N}$ mit $k\geq 4$ eine simultane Eigenform, genauer gilt

$$T_n^{(k)}G_k = \sigma_{k-1}(n)G_k \quad \text{für alle } n\in\mathbb{N}.$$ ◇

Beweis
Nach Satz I.4.2 gilt

$$G_k(\tau) = 2\zeta(k)+2\frac{(2\pi i)^k}{(k-1)!}\sum_{m=1}^{\infty}\sigma_{k-1}(m)e^{2\pi i m\tau}$$

für alle $\tau \in \mathbb{H}$, also hat man $\alpha_{G_k}(0) = 2\zeta(k)$ und

$$\alpha_{G_k}(m) = 2\frac{(2\pi i)^k}{(k-1)!}\alpha(m)$$

für alle $m \in \mathbb{N}$, insbesondere $\alpha_{G_k}(1) = 2\frac{(2\pi i)^k}{(k-1)!}$ wegen $\alpha(1) = \sigma_{k-1}(1) = 1$, also $\alpha_{G_k}(1) \neq 0$. Ist $m \in \mathbb{N}$ und $p \in \mathbb{N}$ eine Primzahl, so gilt dann

$$\begin{aligned}
\alpha_{G_k}(p)\alpha_{G_k}(m) &= \left(2\frac{(2\pi i)^k}{(k-1)!}\right)^2 \alpha(p)\alpha(m) \overset{(3.2)}{=} \left(2\frac{(2\pi i)^k}{(k-1)!}\right)^2 (\alpha(mp) + p^{k-1}\alpha(\tfrac{m}{p})) \\
&= 2\frac{(2\pi i)^k}{(k-1)!}\left(2\frac{(2\pi i)^k}{(k-1)!}\alpha(mp) + p^{k-1}2\frac{(2\pi i)^k}{(k-1)!}\alpha(\tfrac{m}{p})\right) \\
&= \alpha_{G_k}(1)(\alpha_{G_k}(mp) + p^{k-1}\alpha_{G_k}(\tfrac{m}{p})).
\end{aligned}$$

Für jede Primzahl $p \in \mathbb{N}$ gilt weiter

$$\begin{aligned}
\alpha_{G_k}(p)\alpha_{G_k}(0) &= 2\frac{(2\pi i)^k}{(k-1)!}\alpha(p)\cdot 2\zeta(k) = 2\frac{(2\pi i)^k}{(k-1)!}\sigma_{k-1}(p)\cdot 2\zeta(k) \\
&= 2\frac{(2\pi i)^k}{(k-1)!}(1+p^{k-1})\cdot 2\zeta(k) = \alpha_{G_k}(1)(1+p^{k-1})\alpha_{G_k}(0) \\
&= \alpha_{G_k}(1)(\alpha_{G_k}(0\cdot p) + p^{k-1}\alpha_{G_k}(\tfrac{0}{p})).
\end{aligned}$$

Insgesamt ist somit die Bedingung (iii) aus (3.1) erfüllt, was beweist, dass G_k eine simultane Eigenform ist. Weiter erhält man aus diesem Korollar

$$T_n^{(k)}G_k = \frac{\alpha_{G_k}(n)}{\alpha_{G_k}(1)}G_k = \frac{2\frac{(2\pi i)^k}{(k-1)!}\alpha(n)}{2\frac{(2\pi i)^k}{(k-1)!}\alpha(1)} = \frac{\alpha(n)}{\alpha(1)} = \frac{\sigma_{k-1}(n)}{\sigma_{k-1}(1)} = \sigma_{k-1}(n)$$

für alle $n \in \mathbb{N}$, was den Beweis der Behauptung vervollständigt. □

Der folgende Satz beinhaltet eine Umkehrung von (3.3).

(3.4) Satz
Sei $k \in \mathbb{N}$ gerade mit $k \geq 4$ und $f \in \mathbb{M}_k$ mit $\alpha_f(0) = 1$. Gibt es ein $n \in \mathbb{N}$ mit $n \geq 2$, so dass f eine Eigenform bezüglich $T_n^{(k)}$ ist, so gilt bereits $f = G_k^*$. ◇

Beweis
Ist $T_n^{(k)}f = \lambda_f(n)f$, so gilt

$$\sigma_{k-1}(n) = \sigma_{k-1}(n)\alpha_f(0) \overset{\text{Lemma 1.1}}{=} \alpha_{T_n^{(k)}f}(0) = \lambda_f(n)\alpha_f(0) = \lambda_f(n),$$

also $T_n^{(k)} f = \sigma_{k-1}(n)$. Setze $g = f - G_k^*$. Dann gilt $g \in \mathbb{S}_k$, da f und G_k^* jeweils den nullten Fourierkoeffizienten 1 haben. Weiter gilt

$$\begin{aligned} T_n^{(k)} g &= T_n^{(k)} f - T_n^{(k)} G_k^* = \sigma_{k-1}(n) f - T_n^{(k)} G_k^* \overset{(3.3)}{=} \sigma_{k-1}(n) f - \sigma_{k-1}(n) G_k^* \\ &= \sigma_{k-1}(n)(f - G_k^*) = \sigma_{k-1}(n) g. \end{aligned}$$

Annahme: $g \neq 0$. Dann folgt mit Proposition 1.4

$$\sigma_{k-1}(n) = |\lambda_g(n)| \leq n^{\frac{k}{2}} \sigma_{-1}(n).$$

Andererseits hat man

$$\begin{aligned} 2\sigma_{k-1}(n) - 2n^{\frac{k}{2}}\sigma_{-1}(n) &= \sum_{d|n} d^{k-1} + \sum_{d|n} d^{k-1} - n^{\frac{k}{2}} \sum_{d|n} \frac{1}{d} - n^{\frac{k}{2}} \sum_{d|n} \frac{1}{d} \\ &= \sum_{d|n} d^{k-1} + \sum_{d|n} \left(\frac{n}{d}\right)^{k-1} - n^{\frac{k}{2}} \sum_{d|n} \frac{1}{d} - n^{\frac{k}{2}} \sum_{d|n} \frac{1}{\frac{n}{d}} \\ &= \sum_{d|n} \left(d^{k-1} + \left(\frac{n}{d}\right)^{k-1} - n^{\frac{k}{2}} \left(\frac{1}{d} + \frac{d}{n} \right) \right) \\ &= \sum_{d|n} \frac{n^{\frac{k}{2}}}{d} \left(\frac{d^k}{n^{\frac{k}{2}}} + \frac{n^{\frac{k}{2}-1}}{d^{k-2}} - 1 - \frac{d^2}{n} \right) \\ &= \sum_{d|n} \frac{n^{\frac{k}{2}}}{d} \left(\left(\frac{d}{\sqrt{n}}\right)^k + \left(\frac{\sqrt{n}}{d}\right)^{k-2} - 1 - \left(\frac{d}{\sqrt{n}}\right)^2 \right) \\ &= \sum_{d|n} \frac{n^{\frac{k}{2}}}{d} \left(1 - \left(\frac{\sqrt{n}}{d}\right)^{k-2} \right) \left(\left(\frac{d}{\sqrt{n}}\right)^k - 1 \right) \\ &= n^{\frac{k}{2}} \overbrace{(1 - (\sqrt{n})^{k-2})}^{<0,\text{ da } n\geq 2} \overbrace{((\sqrt{n})^{-k} - 1)}^{<0,\text{ da } n\geq 2} \\ &\quad + \sum_{\substack{d|n \\ d>1}} \frac{n^{\frac{k}{2}}}{d} \left(1 - \left(\frac{\sqrt{n}}{d}\right)^{k-2} \right) \left(\left(\frac{d}{\sqrt{n}}\right)^k - 1 \right) \\ &> \sum_{\substack{d|n \\ d>1}} \frac{n^{\frac{k}{2}}}{d} \left(1 - \left(\frac{\sqrt{n}}{d}\right)^{k-2} \right) \left(\left(\frac{d}{\sqrt{n}}\right)^k - 1 \right) \geq 0, \end{aligned}$$

da für $d < \sqrt{n}$ sowohl $1 - (\sqrt{n}/d)^{k-2}$ als auch $(d/\sqrt{n})^k - 1$ negativ sind, für $d > \sqrt{n}$ diese beiden Faktoren positiv sind und für $d = \sqrt{n}$ beide Faktoren den Wert 0 haben.

Dies stellt einen Widerspruch zur Ungleichung $\sigma_{k-1}(n) \leq n^{\frac{k}{2}}\sigma_{-1}(n)$ dar, die oben gezeigt wurde. Deshalb muss die Annahme $g \neq 0$ falsch sein. Es gilt also $g = 0$, was äquivalent zu $f = G_k^*$ ist. Dies beweist die Behauptung. $\square$