

Die Algebra der Hecke-Operatoren

Daniel Heyen

22. November 2005

Seminar Funktionentheorie/ Analytische Zahlentheorie

Dozent: Dr. R. Busam

Wintersemester 2005/06

Quelle: Koecher/ Krieg: „Elliptische Funktionen und Modulformen“

Verwendete Notationen:

- (i) $V(\mathbb{H})$ ist der \mathbb{C} -Vektorraum der Funktionen aus $\{f \mid f : \mathbb{H} \rightarrow \mathbb{C}\}$ mit
- f ist auf \mathbb{H} meromorph
 - f hat die Periode 1
 - f hat bei ∞ höchstens einen Pol.
- (ii) $[\Gamma, k]$ ist der Vektorraum der ganzen Modulformen vom Gewicht k .
- (iii) $[\Gamma, k]_0$ ist der Vektorraum der Spitzenformen vom Gewicht k .
- (iv) Wir sagen ' a durchläuft ein Restesystem $(\text{mod } s)$ ', wenn für die Menge $\{b_\mu\} \subset \mathbb{Z}$ der *ganzen* Zahlen, die b annimmt, gilt

$$\{[b_\mu]_s\} = \{[0]_s, \dots, [s-1]_s\} ,$$

wenn also $b \pmod s$ alle Elemente aus $\mathbb{Z}/s\mathbb{Z}$ genau einmal annimmt. Natürlich ist es unpräzise, nur die Bezeichnung ' b ' zu verwenden, obwohl es mehrere Belegungen gibt, doch erspart dies verwirrende Indizes.

1 Die Multiplikativität der T_n

1.1 Satz. Für alle teilerfremden $m, n \in \mathbb{N}$ und alle $f \in V(\mathbb{H})$ gilt:

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

Dabei bedarf das zweite Gleichheitszeichen keines Beweises, da $mn = nm$ und somit $T_{mn}^{(k)} f = T_{nm}^{(k)} f$ gilt.

Für den Beweis des Satzes benötigen wir folgendes

1.2 Lemma. Sind $m, n \in \mathbb{N}$ teilerfremd, $m = a_1 d_1$, $n = a_2 d_2$ ($a_1, a_2, d_1, d_2 \in \mathbb{Z}$) und durchlaufe $b_1 \pmod{d_1}$, sowie $b_2 \pmod{d_2}$ je ein Restesystem, dann durchläuft

$$b_{12} := a_2 b_1 + b_2 d_1$$

ein Restesystem $(\text{mod } d_1 d_2)$.

Beweis. Die b_{12} sind paarweise inkongruent modulo $d_1 d_2$:

$$\begin{aligned} & a_2 \tilde{b}_1 + \tilde{b}_2 d_1 \equiv a_2 b_1 + b_2 d_1 \pmod{d_1 d_2} \quad | \cdot d_2 \\ \Rightarrow & a_2 \tilde{b}_1 d_2 \equiv a_2 b_1 d_2 \pmod{d_1 d_2} \\ \Rightarrow & a_2 \tilde{b}_1 \equiv a_2 b_1 \pmod{d_1} \\ \stackrel{\text{ggT}(a_2, d_1)=1}{\Rightarrow} & \tilde{b}_1 \equiv b_1 \pmod{d_1} \\ \Rightarrow & \tilde{b}_1 = b_1 \quad , \end{aligned}$$

da \tilde{b}_1 und b_1 nach Voraussetzung einem Restesystem $(\text{mod } d_1)$ angehören. Dies eingesetzt in die erste Gleichung ergibt

$$\begin{aligned} \tilde{b}_2 d_1 &\equiv b_2 d_1 \pmod{d_1 d_2} \\ \Rightarrow \tilde{b}_2 &\equiv b_2 \pmod{d_2} \\ \Rightarrow \tilde{b}_2 &= b_2 \quad , \end{aligned}$$

aus dem gleichen Grund wie oben.

Da es $d_1 \cdot d_2$ Kombinationen von b_1 mit b_2 gibt, durchläuft b_{12} wie behauptet ein Restesystem $(\text{mod } d_1 d_2)$.

□

Nun zum Beweis des Satzes:

$$\begin{aligned} (T_m^{(k)} (T_n^{(k)} f)) (\tau) &= m^{k-1} \sum_{a_1 d_1 = m} d_1^{-k} \sum_{b_1 (\text{mod } d_1)} T_n^{(k)} f \left(\frac{a_1 \tau + b_1}{d_1} \right) \\ &= m^{k-1} \sum_{a_1 d_1 = m} d_1^{-k} \sum_{b_1 (\text{mod } d_1)} n^{k-1} \sum_{a_2 d_2 = n} d_2^{-k} \sum_{b_2 (\text{mod } d_2)} f \left(\frac{a_2 \left(\frac{a_1 \tau + b_1}{d_1} \right) + b_2}{d_2} \right) \\ &= (mn)^{k-1} \sum_{\substack{a_1 d_1 = m \\ a_2 d_2 = n}} (d_1 d_2)^{-k} \sum_{\substack{b_1 (\text{mod } d_1) \\ b_2 (\text{mod } d_2)}} f \left(\frac{a_2 a_1 \tau + (a_2 b_1 + b_2 d_1)}{d_1 d_2} \right) \\ &\stackrel{(1)}{=} (mn)^{k-1} \sum_{ad=mn} d^{-k} \sum_{b_{12} (\text{mod } d)} f \left(\frac{a\tau + b_{12}}{d} \right) \\ &= (T_{mn}^{(k)} f) (\tau) \quad , \end{aligned}$$

wobei (1) einerseits gilt, da aufgrund der Teilerfremdheit von m und n $a_1 a_2$ (und damit auch $d_1 d_2$) genau einmal die Teiler von mn durchläuft, andererseits, weil $b_{12} := a_2 b_1 + b_2 d_1$ ein Restesystem $(\text{mod } d_1 d_2)$ durchläuft, wie in Lemma 1.2 gezeigt wurde.

□

Zur Illustration ein Beispiel für $T_m T_n \neq T_{mn}$ für $ggT(m, n) \neq 1$, welches allgemein im nächsten Kapitel behandelt wird.

Betrachte den Fall $m = n = 2$ und beliebiges $f \in V(\mathbb{H})$ und $k \in \mathbb{Z}$. Dann ist

$$\begin{aligned}
\left((T_2^{(k)} \circ T_2^{(k)}) f \right) (\tau) &= 4^{k-1} \sum_{\substack{a_1 d_1 = 2 \\ a_2 d_2 = 2}} (d_1 d_2)^{-k} \sum_{\substack{b_1 \pmod{d_1} \\ b_2 \pmod{d_2}}} f \left(\frac{a_2 a_1 \tau + (a_2 b_1 + b_2 d_1)}{d_1 d_2} \right) \\
&= 4^{k-1} \cdot \left[4^{-k} \cdot \left(f \left(\frac{\tau}{4} \right) + f \left(\frac{\tau+1}{4} \right) + f \left(\frac{\tau+2}{4} \right) + f \left(\frac{\tau+3}{4} \right) \right) \right. \\
&\quad + 2^{-k} \cdot \left(f \left(\frac{2\tau}{2} \right) + f \left(\frac{2\tau+2}{2} \right) \right) \\
&\quad + 2^{-k} \cdot \left(f \left(\frac{2\tau}{2} \right) + f \left(\frac{2\tau+1}{2} \right) \right) \\
&\quad \left. + 1^{-k} \cdot f(4\tau) \right] ,
\end{aligned}$$

während

$$\begin{aligned}
\left(T_4^{(k)} f \right) (\tau) &= 4^{k-1} \sum_{ad=4} d^{-k} \sum_{b \pmod{d}} f \left(\frac{a\tau + b}{d} \right) \\
&= 4^{k-1} \cdot \left[4^{-k} \cdot \left(f \left(\frac{\tau}{4} \right) + f \left(\frac{\tau+1}{4} \right) + f \left(\frac{\tau+2}{4} \right) + f \left(\frac{\tau+3}{4} \right) \right) \right. \\
&\quad + 2^{-k} \cdot \left(f \left(\frac{2\tau}{2} \right) + f \left(\frac{2\tau+1}{2} \right) \right) \\
&\quad \left. + 1^{-k} \cdot f(4\tau) \right] .
\end{aligned}$$

Also ist

$$\begin{aligned}
\left((T_2^{(k)} \circ T_2^{(k)}) f \right) (\tau) &= \left(T_4^{(k)} f \right) (\tau) + 4^{k-1} \cdot 2^{-k} \cdot (f(\tau) + f(\tau+1)) \\
&= \left(T_4^{(k)} f \right) (\tau) + 2^{k-1} \cdot f(\tau) \quad , \text{ weil } f(\tau+1) = f(\tau) .
\end{aligned}$$

2 Eine Rekursionsformel für die Hecke-Operatoren von Primzahlpotenzen

2.1 Satz. Sei p prim, $r \in \mathbb{N}$, $k \in \mathbb{Z}$ und $f \in V(\mathbb{H})$. Dann gilt:

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

Hierbei ist $T_{p^0}^{(k)} = T_1^{(k)}$ die Identität.

Wiederum sind einfache Aussagen über Restesysteme notwendig, die in den beiden folgenden Lemmata bewiesen werden.

2.2 Lemma. Sei $\nu \in \mathbb{N}$. Falls b ein Restesystem (mod p^ν) und a eines (mod p) durchläuft, so durchläuft

$$c := b + a \cdot p^\nu$$

ein Restesystem (mod $p^{\nu+1}$).

Beweis. Wieder nehmen wir an, daß für zwei Kombinationen von a und b die resultierenden c 's kongruent sind und folgern, daß dann die a 's und b 's schon kongruent gewesen sein müssen.

$$\begin{aligned} \tilde{b} + \tilde{a} p^\nu &\equiv b + a p^\nu && \text{mod } p^{\nu+1} \quad | \cdot p \\ \Rightarrow p \tilde{b} + \tilde{a} p^{\nu+1} &\equiv p b + a p^{\nu+1} && \text{mod } p^{\nu+1} \\ \Rightarrow p \tilde{b} &\equiv p b && \text{mod } p^{\nu+1} \\ \Rightarrow \tilde{b} &\equiv b && \text{mod } p^\nu \\ \Rightarrow \tilde{b} &= b \quad , \end{aligned}$$

da \tilde{b} und b nach Voraussetzung einem Restesystem (mod p^ν) angehören. Dies eingesetzt in die erste Gleichung ergibt

$$\begin{aligned} \tilde{a} p^\nu &\equiv a p^\nu && \text{mod } p^{\nu+1} \\ \Rightarrow \tilde{a} &\equiv a && \text{mod } p \\ \Rightarrow \tilde{a} &= a \quad . \end{aligned}$$

Da es $p \cdot p^\nu = p^{\nu+1}$ Möglichkeiten für c gibt, ist das Lemma bewiesen. □

2.3 Lemma. Sei $\nu \in \mathbb{N}$ und durchlaufe b ein Restesystem (mod p^ν). Dann durchläuft $[b]_{p^{\nu-1}}$ (also die Reste von b modulo $p^{\nu-1}$) ein Restesystem (mod $p^{\nu-1}$) genau p -mal.

Beweis. Für das Standardrestesystem $\{0, \dots, p^\nu - 1\}$ ist die Aussage klar. Jedes Element des gegebenen Restesystems unterscheidet sich von genau einem Element des Standardrestesystems aber nur um ein Vielfaches von p^ν . Dieser Anteil wird

bei Restklassenbildung bzgl. $p^{\nu-1}$ aber auf die Null geschickt und daher durchlaufen auch die Reste eines beliebigen Restklassensystems $(\text{mod } p^\nu)$ in $\mathbb{Z}/p^{\nu-1}\mathbb{Z}$ ein Restesystem $(\text{mod } p^{\nu-1})$ genau p -mal.

□

Zum Beweis des Satzes:

$$\begin{aligned} \left(T_{p^r}^{(k)} T_p^{(k)} f\right)(\tau) &= p^{r(k-1)} \cdot \sum_{\nu=0}^r p^{-k\nu} \cdot \sum_{b(\text{mod } p^\nu)} T_p^{(k)} f\left(\frac{p^{r-\nu}\tau + b}{p^\nu}\right) \\ &= p^{r(k-1)} \cdot \sum_{\nu=0}^r p^{-k\nu} \cdot \sum_{b(\text{mod } p^\nu)} \left[p^{k-1} \cdot f\left(p \cdot \frac{p^{r-\nu}\tau + b}{p^\nu}\right) + \frac{1}{p} \cdot \sum_{a=1}^p f\left(\frac{\frac{p^{r-\nu}\tau + b}{p^\nu} + a}{p}\right) \right] \end{aligned}$$

Der Fall $\nu = 0$ wird getrennt von den anderen:

$$\begin{aligned} &= p^{r(k-1)} \cdot \left[p^{k-1} \cdot f(p^{r+1}\tau) + \frac{1}{p} \cdot \sum_{a=1}^p f\left(\frac{p^r\tau + a}{p}\right) \right] \\ &+ p^{r(k-1)} \cdot \sum_{\nu=1}^r p^{-k\nu} \cdot \\ &\quad \sum_{b(\text{mod } p^\nu)} \left[p^{k-1} \cdot f\left(\frac{p^{r-\nu}\tau + b}{p^{\nu-1}}\right) + \frac{1}{p} \cdot \sum_{a(\text{mod } p)} f\left(\frac{p^{r-\nu}\tau + (ap^\nu + b)}{p^{\nu+1}}\right) \right] \end{aligned}$$

Einfaches Ausmultiplizieren und Lemma 2.3 und 2.2 ergeben:

$$\begin{aligned} \left(T_{p^r}^{(k)} T_p^{(k)} f\right)(\tau) &= p^{(r+1)(k-1)} \cdot f(p^{r+1}\tau) + p^{r(k-1)-1} \cdot \sum_{a=1}^p f\left(\frac{p^r\tau + a}{p}\right) \\ &+ p^{r(k-1)} \cdot \sum_{\nu=1}^r p^{-k\nu} \cdot p \sum_{b(\text{mod } p^{\nu-1})} p^{k-1} \cdot f\left(\frac{p^{r-\nu}\tau + b}{p^{\nu-1}}\right) \\ &+ p^{r(k-1)} \cdot \sum_{\nu=1}^r p^{-k\nu} \sum_{c(\text{mod } p^{\nu+1})} \frac{1}{p} \cdot f\left(\frac{p^{r-\nu}\tau + c}{p^{\nu+1}}\right) \end{aligned}$$

Der zweite Term wird mit der Summe über $c \pmod{p^{\nu+1}}$ zusammengefasst:

$$\begin{aligned} \left(T_{p^r}^{(k)} T_p^{(k)} f\right)(\tau) &= p^{(r+1)(k-1)} \cdot f(p^{r+1}\tau) \\ &+ p^{r(k-1)} \cdot \sum_{\nu=1}^r p^{-(\nu-1)k} \sum_{b(\text{mod } p^{\nu-1})} f\left(\frac{p^{(r-1)-(\nu-1)}\tau + b}{p^{\nu-1}}\right) \\ &+ p^{r(k-1)} \cdot \sum_{\nu=0}^r p^{-\nu k-1} \sum_{c(\text{mod } p^{\nu+1})} f\left(\frac{p^{(r+1)-(\nu+1)}\tau + c}{p^{\nu+1}}\right) \end{aligned}$$

Nun muß nur noch die Definition der HECKE-Operatoren beachtet werden:

$$\begin{aligned}
\left(T_{p^r}^{(k)} T_p^{(k)} f\right)(\tau) &= p^{(r+1)(k-1)} \cdot f(p^{r+1}\tau) \\
&+ p^{r(k-1)-(r-1)(k-1)} \cdot T_{p^{r-1}}^{(k)} f(\tau) \\
&+ p^{(r+1)(k-1)} \cdot \sum_{\nu=0}^r p^{-(\nu+1)k} \sum_{c \pmod{p^{\nu+1}}} f\left(\frac{p^{(r+1)-(\nu+1)}\tau + c}{p^{\nu+1}}\right) \\
&= T_{p^{r+1}}^{(k)} f(\tau) + p^{k-1} \cdot T_{p^{r-1}}^{(k)} f(\tau) \quad .
\end{aligned}$$

□

2.4 Korollar. Für jedes $T_n^{(k)}$ ($n \in \mathbb{N}$) gibt es ein Polynom $P \in \mathbb{Q}[X_1, \dots, X_l]$, so daß

$$T_n^{(k)} = P(T_{p_1}, \dots, T_{p_l}) \quad ,$$

wobei $l \in \mathbb{N}$ die Anzahl der verschiedenen Primzahlen in der Primfaktorzerlegung von n ist.

Beweis. Sei $n = p_1^{r_1} \cdot \dots \cdot p_l^{r_l}$ (die p_i seien paarweise verschieden). Dann ist nach Satz 1.1

$$T_n^{(k)} = T_{p_1^{r_1}}^{(k)} \cdot \dots \cdot T_{p_l^{r_l}}^{(k)} \quad .$$

Nun ist es mit Satz 2.1 sehr leicht, durch Induktion über r_i zu zeigen, daß ein Polynom $P_i \in \mathbb{Q}[X]$ existiert mit

$$T_{p_i^{r_i}}^{(k)} = P_i(T_{p_i}^{(k)}) \quad ,$$

und dies zeigt die Behauptung.

□

2.5 Korollar. Sei p prim und $r, s \in \mathbb{N}_0$. Dann gilt

$$T_{p^r}^{(k)} T_{p^s}^{(k)} = \sum_{\nu=0}^{\min(r,s)} p^{\nu(k-1)} T_{p^{r+s-2\nu}}^{(k)}$$

Insbesondere kommutieren also $T_{p^r}^{(k)}$ und $T_{p^s}^{(k)}$.

Beweis. Durch Induktion nach s . Wir benötigen, wie im Beweis ersichtlich, zwei Verankerungen. Der Fall $s = 0$ ist trivial, und für $s = 1$ wurde die Behauptung in Satz 2.1 gezeigt.

Nun der Induktionsschritt, in dem ich der Einfachheit halber T_{p^r} statt $T_{p^r}^{(k)}$ schreibe.

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

Nun wenden wir Satz 2.1 an, müssen aber aufpassen, welche ν erlaubt sind, daß also nicht $r + s - 2\nu = 0$ ist, denn sonst fällt der zweite Summand einfach weg.

$$\begin{aligned}
T_{p^r} T_{p^{s+1}} &= \sum_{\nu=0}^{\min(r,s)} p^{\nu(k-1)} T_{p^{r+s-2\nu+1}} + \sum_{\substack{\nu=0 \\ 2\nu+1 \leq r+s}}^{\min(r,s)} p^{(\nu+1)(k-1)} T_{p^{r+s-2\nu-1}} \\
&- \sum_{\nu=0}^{\min(r,s-1)} p^{(\nu+1)(k-1)} T_{p^{r+s-2\nu-1}} \\
&= \sum_{\nu=0}^{\min(r,s)} p^{\nu(k-1)} T_{p^{r+s+1-2\nu}} + \sum_{\nu \in \Lambda} p^{(\nu+1)(k-1)} T_{p^{r+s-2\nu-1}} \quad ,
\end{aligned}$$

wobei

$$\Lambda = \{ \nu \in \mathbb{N}_0 \mid \min(r, s-1) < \nu \leq \min(r, s) \quad \text{und} \quad 2\nu + 1 \leq r + s \} .$$

Um Λ genauer zu bestimmen betrachten wir die verschiedenen Fälle: $r < s$ scheidet sofort aus, während $r = s$ an der Bedingung $2\nu + 1 \leq r + s$ scheitert. In diesen beiden Fällen ist also $\Lambda = \emptyset$ und somit unsere Behauptung schon bewiesen, denn dann ist $\min(r, s) = r = \min(r, s+1)$.

Der Fall $r > s$ ist hingegen möglich, es gilt dann $\Lambda = \{s\}$ und $\min(r, s+1) = s+1$. Es folgt in diesem Fall

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

womit das Korollar bewiesen ist.

□

3 Die Algebra der Hecke-Operatoren

Wir haben nun die zentralen Eigenschaften der HECKE-Operatoren bewiesen, die uns erlauben, mehr über ihre algebraische Struktur sagen zu können. Bisher wissen wir ja nur, daß jedes $T_n^{(k)}$ ein Endomorphismus auf $V(\mathbb{H})$ ist, der die Unterräume $[\Gamma, k]$ und $[\Gamma, k]_0$ wieder in sich abbildet. Ob wir aber eine "gute Struktur" auf der Menge der HECKE-Operatoren selber haben, ist bisher nicht klar.

Einige der hier aufgeführten Eigenschaften sind so einfach, daß wir sie bisher schon benutzt haben, ohne daß sie erwähnt werden mussten, so z.B. die Addition von zwei HECKE-Operatoren - wir definieren natürlich für beliebiges $f \in V(\mathbb{H})$

$$\left(T_n^{(k)} + T_m^{(k)}\right)f = T_n^{(k)}f + T_m^{(k)}f .$$

Ein neutrales Element der Addition ist der Nulloperator, der jedes $f \in V(\mathbb{H})$ auf die Nullfunktion abbildet.

Wichtig zu bemerken ist, daß etwa die obige Definition der Addition nicht schon beinhaltet, daß die Summe zweier HECKE-Operatoren wieder einer ist, dies wird i.A. falsch sein. Deshalb gehen wir den üblichen Weg, und definieren

$$\mathcal{H}_k := \left\{ \sum_{\lambda \in \Lambda} \alpha_\lambda \cdot T_\lambda^{(k)} \mid \alpha_\lambda \in \mathbb{C}, \Lambda \subset \mathbb{N}, \#\Lambda < \infty \right\}$$

Mit der oben definierten Addition und der naheliegenden Skalarmultiplikation wird \mathcal{H}_k ein \mathbb{C} -Vektorraum.

Zusätzlich nehmen wir als Multiplikation auf \mathcal{H}_k die Hintereinanderausführung von Operatoren, die natürlich assoziativ ist und die Distributivgesetze erfüllt. Es gilt der

3.1 Satz. \mathcal{H}_k ist eine kommutative \mathbb{C} -Algebra mit Eins, die von den T_p (p prim) erzeugt wird.

Für $m, n \in \mathbb{N}$ gilt:

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

Insbesondere ist jedes $T \in \mathcal{H}_k$ ein rationales Polynom in den $T_p^{(k)}$ (p prim).

Man nennt \mathcal{H}_k die HECKE-Algebra vom Gewicht k .

Beweis. (*) zeigt die Abgeschlossenheit von \mathcal{H}_k unter der Multiplikation, das Einselement ist $T_1^{(k)}$.

Die letzte Aussage folgt mit Korollar 2.4 sofort, wenn (*) gezeigt ist, ebenso wie die Kommutativität.

Um (*) zu beweisen führen wir eine Induktion über die Anzahl der Primteiler von $m \cdot n$ durch.

- *Verankerung.* Sei $m = p^r$, $n = p^s$ mit $r, s \in \mathbb{N}_0$. Dann gilt nach Korollar 2.5

$$\begin{aligned} T_{p^r} T_{p^s} &= \sum_{\nu=0}^{\min(r,s)} p^{\nu(k-1)} T_{p^{r+s-2\nu}} \\ &= \sum_{d \mid \text{ggT}(p^r, p^s) d^{k-1}} T_{\frac{p^r p^s}{d^2}} \quad , \end{aligned}$$

da sich jeder Teiler von $\text{ggT}(p^r, p^s)$ als p^ν schreiben läßt.

- *Schritt.* Sei $\text{ggT}(m, n) \neq 1$, denn sonst ist nach Satz 1.1 alles gezeigt. Es gibt dann eine Primzahl p mit $m = m' \cdot p^r$, $n = n' \cdot p^s$ ($r, s \geq 1$), so daß $\text{ggT}(m', p) = \text{ggT}(n', p) = 1$.

Nach Induktionsvoraussetzung gilt (*) für m' und n' :

$$\begin{aligned} T_m T_n &\stackrel{\text{Satz 1.1}}{=} T_{m'} T_{n'} T_{p^r} T_{p^s} \\ &= \sum_{t \mid \text{ggT}(m', n')} t^{k-1} T_{\frac{m' n'}{t^2}} \sum_{d \mid \text{ggT}(p^r, p^s)} d^{k-1} T_{\frac{p^r p^s}{d^2}} \\ &= \sum_{\substack{t \mid \text{ggT}(m', n') \\ d \mid \text{ggT}(p^r, p^s)}} (t \cdot d)^{k-1} T_{\frac{m n}{(td)^2}} \end{aligned}$$

Aber $t \cdot d$ durchläuft genau einmal alle Teiler von $\text{ggT}(m, n)$, da $\text{ggT}(m', p) = \text{ggT}(n', p) = 1$.

□

3.2 Korollar. Ist $f \in [\Gamma, k]$ nicht konstant, so sind folgende Eigenschaften äquivalent:

- (i) f ist simultane Eigenform bezüglich aller T_n .
- (ii) Zu jeder Primzahl p gibt es ein $\lambda_f(p) \in \mathbb{C}$, so daß
$$T_p f = \lambda_f(p) \cdot f \quad .$$
- (iii) Für jede Primzahl p und alle $m \in \mathbb{N}_0$ gilt für die FOURIER-Koeffizienten von f : $\alpha_f(1) \neq 0$ und

$$\alpha_f(p) \cdot \alpha_f(m) = \alpha_f(1) \cdot \left(\alpha_f(mp) + p^{k-1} \alpha_f\left(\frac{m}{p}\right) \right) \quad ,$$

wobei $\alpha_f\left(\frac{m}{p}\right) := 0$, falls $p \nmid m$.

Beweis.

(ii) \Rightarrow (i) Wir wissen, daß wir jedes T_n schreiben können als

$$T_n = \sum_{\substack{(\varepsilon_1, \dots, \varepsilon_l) \in \Lambda \\ \Lambda \subset \mathbb{N}^l, \#\Lambda < \infty}} \gamma_{\varepsilon_1, \dots, \varepsilon_l} \cdot T_{p_1}^{\varepsilon_1} \cdots T_{p_l}^{\varepsilon_l} \quad ,$$

weshalb

$$T_n f = \left[\sum \gamma_{\varepsilon_1, \dots, \varepsilon_l} \cdot \lambda(p_1)^{\varepsilon_1} \cdots \lambda(p_l)^{\varepsilon_l} \right] f \quad .$$

(i) \Rightarrow (iii) Wir wissen aus dem letzten Vortrag: Falls f simultane Eigenform ist, gilt: $\alpha_f(1) \neq 0$ und

$$\alpha_f(m) \cdot \alpha_f(n) = \alpha_f(1) + \sum_{d \mid \text{ggT}(m,n)} d^{k-1} \alpha_f\left(\frac{mn}{d^2}\right) \quad \text{für alle } m \in \mathbb{N}_0, n \in \mathbb{N},$$

und für $n = p$ ist das gerade (iii), denn $\text{ggT}(m, p)$ ist entweder 1 oder p , und es ergeben sich die behaupteten Terme.

(iii) \Rightarrow (ii) Wir wissen, daß sich der m -te FOURIER-Koeffizient von $T_n f$ schreibt als:

$$\alpha_{T_n f}(m) = \alpha_f(mp) + p^{k-1} \alpha_f\left(\frac{m}{p}\right).$$

Also ist

$$\alpha_{T_n f}(m) = \frac{\alpha_f(p)}{\alpha_f(1)} \cdot \alpha_f(m),$$

$\lambda_f(p) := \frac{\alpha_f(p)}{\alpha_f(1)}$ erfüllt also das Gewünschte.

□

4 Die Eisensteinreihen als simultane Eigenformen

Erinnert sei daran, daß wir die EISENSTEINreihe für alle geraden $k \geq 4$ schreiben können als

$$G_k(\tau) = 2\zeta(k) + 2 \frac{(2\pi i)^k}{(k-1)!} \cdot \sum_{m=1}^{\infty} \sigma_{k-1}(m) \cdot e^{2\pi i m \tau}, \quad \tau \in \mathbb{H}.$$

4.1 Satz. Für gerades $k \geq 4$ ist G_k eine simultane Eigenform, und zwar gilt:

$$T_n G_k = \sigma_{k-1}(n) \cdot G_k \quad \text{für alle } n \geq 1.$$

Beweis. Aus der bereits bewiesenen Formel

$$\alpha_{T_n f}(m) = \sum_{d|ggT(m,n)} d^{k-1} \cdot \alpha_f\left(\frac{mn}{d^2}\right),$$

die für ganze Modulformen für alle $m \in \mathbb{N}_0$ richtig ist, erhalten wir den Spezialfall

$$\alpha_{T_n f}(0) = \sigma_{k-1}(n) \cdot \alpha_f(0).$$

Das bedeutet, daß eine ganze Modulform vom Gewicht k , deren konstanter FOURIER-Koeffizient ungleich Null ist, höchstens die σ_{k-1} als Eigenwerte haben kann! Und in diesem Fall sind wir bei den EISENSTEINreihen, denn $\zeta(k)$ ist ungleich Null. Somit ist nach Korollar 3.2 der Satz bewiesen, wenn wir

$$\alpha(p) \cdot \alpha(m) = \alpha(mp) + p^{k-1} \alpha\left(\frac{m}{p}\right) \quad (\diamond)$$

für jede Primzahl p und jedes $m \in \mathbb{N}$ zeigen können, wobei $\alpha_m := \sigma_{k-1}(m)$ und $\alpha\left(\frac{m}{p}\right) = 0$, falls $p \nmid m$.

Betrachten wir zuerst den Fall, daß $m = p^r$ ist mit $r \in \mathbb{N}$.

$$\alpha_{p^r} = \sum_{d|p^r} d^{k-1} = \sum_{\nu=0}^r (p^{k-1})^\nu = \frac{q^{r+1} - 1}{q - 1}$$

nach der geometrischen Summenformel mit $q := p^{k-1}$.

(\diamond) ist also für $m = p^r$ äquivalent zu

$$\begin{aligned} \frac{q^2-1}{q-1} \cdot \frac{q^{r+1}-1}{q-1} &= \frac{q^{r+2}-1}{q-1} + q \cdot \frac{q^r-1}{q-1} \\ \Leftrightarrow (q^2-1) \cdot (q^{r+1}-1) &= (q^{r+2}-1) \cdot (q-1) + q \cdot (q-1) \cdot (q^r-1) \\ \Leftrightarrow q^{r+3} - q^2 - q^{r+1} + 1 &= q^{r+3} - q^{r+2} - q + 1 + q^{r+2} - q^2 - q^{r+1} + q \\ \Leftrightarrow 0 &= 0. \end{aligned}$$

Ist nun p kein Teiler von m , so hat (\diamond) die Gestalt

$$\alpha(p) \cdot \alpha(m) = \alpha(mp) ,$$

was aber richtig ist, da die σ_{k-1} multiplikativ sind, wie aus ihrer Definition sofort ersichtlich ist.

Sei also schließlich p ein Teiler von m , mit $m = m'p^r$ ($ggT(m',p) = 1$). Dann gilt aufgrund der Teilerfremdheit und des eben bewiesenen Resultats

$$\begin{aligned} \alpha(p) \cdot \alpha(m) &= \alpha(m') \cdot \left(\alpha(p) \cdot \alpha(p^r) \right) \\ &= \alpha(m') \cdot \left(\alpha(p^{r+1}) + p^{k-1} \alpha(p^{r-1}) \right) \\ &= \alpha(mp) + p^{k-1} \alpha\left(\frac{m}{p}\right) . \end{aligned}$$

□

Wir diskutierten schon eben, daß an eine Eigenform mit $\alpha_f(0) \neq 0$ starke Bedingungen gestellt sind - insofern überrascht der folgende Satz nicht.

4.2 Satz. Sei $k \geq 4$ gerade und $f \in [\Gamma, k]$ mit $\alpha_f(0) = 1$. Sei f eine Eigenform bezüglich T_n für irgendein $n > 1$, es existiere also ein $\lambda_f(n)$, so daß $T_n f = \lambda_f(n) \cdot f$.

$$\text{Dann ist } f = G_k^* .$$

Beweis. Aus der allgemeinen Bedingung für die FOURIER-Koeffizienten $\alpha_{T_n f}(0) = \sigma_{k-1}(n) \cdot \alpha_f(0)$ folgt

$$\lambda_f(n) = \sigma_{k-1}(n) .$$

Angenommen $f \neq G_k^*$. Dann ist

$$g := f - G_k^* \in [\Gamma, k]_0 , \quad \text{sowie } g \neq 0 .$$

Es ergibt sich

$$\begin{aligned} T_n g &= T_n f - T_n G_k^* \\ &\stackrel{\text{Satz 4.1}}{=} \lambda_f(n) \cdot f - \sigma_{k-1}(n) \cdot G_k^* \\ &= \sigma_{k-1}(n) \cdot g . \end{aligned}$$

Nach der im vorigen Vortrag bewiesenen, für unsere Voraussetzungen gültigen Abschätzung ist

$$|\lambda_f(n)| \leq n^{\frac{k}{2}} \sigma_{-1}(n) ,$$

und daher

$$\sigma_{k-1}(n) - n^{\frac{k}{2}} \cdot \sigma_{-1}(n) \leq 0 . \quad (\spadesuit)$$

Es ist aber

$$\begin{aligned}
2\sigma_{k-1}(n) - 2n^{\frac{k}{2}}\sigma_{-1}(n) &= \sum_{d|n} \left[d^{k-1} + \left(\frac{n}{d}\right)^{k-1} - n^{\frac{k}{2}} \left(\frac{1}{d} + \frac{d}{n}\right) \right], \\
&\quad \text{weil mit } d \text{ auch } \frac{n}{d} \text{ alle Teiler von } n \text{ durchläuft.} \\
&= \sum_{d|n} \frac{n^{\frac{k}{2}}}{d} \cdot \left(\frac{d^k}{n^{\frac{k}{2}}} + \frac{n^{\frac{k}{2}-1}}{d^{k-2}} - \left(1 + \frac{d^2}{n}\right) \right) \\
&= \sum_{d|n} \frac{n^{\frac{k}{2}}}{d} \cdot \left(1 - \left(\frac{\sqrt{n}}{d}\right)^{k-2} \right) \cdot \left(\left(\frac{d}{\sqrt{n}}\right)^k - 1 \right) \\
&> 0,
\end{aligned}$$

denn:

- Kein Summand ist negativ: Ist $\frac{\sqrt{n}}{d} > 1$, dann ist $\frac{d}{\sqrt{n}} < 1$.
- Es gibt positive Terme: Null wird ein Summand, falls $d = \sqrt{n}$. Da wir $n > 1$ vorausgesetzt haben, gibt es Terme mit $\frac{\sqrt{n}}{d} \neq 1$.

Wir erhalten einen Widerspruch zu (\spadesuit), also muß $f = G_k^*$ sein.

□

Nebenbei bemerkt ist die Einschränkung $n > 1$ natürlich nicht wesentlich, da ja T_1 die Identität ist, also jedes $f \in [\Gamma, k]$ Eigenform bezüglich T_1 ist.

Für manche Anwendungen kann es noch nützlich sein zu wissen, daß auch die *bedingt konvergente EISENSTEINREIHE*

$$G_2(\tau) := \sum_{n \neq 0} n^{-2} + \sum_{m \neq 0} \left(\sum_{n \in \mathbb{Z}} (m\tau + n)^{-2} \right),$$

welche sich schreiben läßt als

$$G_2(\tau) = \frac{\pi^2}{3} \cdot \left(1 - 24 \cdot \sum_{n=1}^{\infty} \sigma_1(n) \cdot e^{2\pi i n \tau} \right),$$

eine simultane Eigenform ist.

Zwar ist G_2 keine Modulform (denn es gilt $G_2\left(-\frac{1}{\tau}\right) = \tau^2 G_2(\tau) - 2\pi i \tau$), aber die geforderten Beziehungen zwischen den FOURIER-Koeffizienten, damit eine Funktion auf der oberen Halbebene eine Eigenform ist, wurden nur an ein $f \in V(\mathbb{H})$ gestellt.

G_2 ist aber aus $V(\mathbb{H})$, und die FOURIER-Koeffizienten erfüllen die geforderten Bedingungen, so daß

$$T_n G_2 = \sigma_1(n) G_2.$$

5 Eine ganzzahlige Darstellung der Hecke-Operatoren

5.1 Ganze Modulformen mit ganzen Fourierkoeffizienten

Zahlentheoretische Bedeutung bekommen die Modulformen in dem Fall, daß wir es mit ganzen FOURIER-Koeffizienten zu tun haben, z.B. bei der Diskriminante, deren FOURIER-Koeffizienten die $\tau(m)$ sind.

Wir definieren

$$[\Gamma, k]^{\mathbb{Z}} := \{f \in [\Gamma, k] \mid \alpha_f(m) \in \mathbb{Z} \text{ für alle } m \in \mathbb{N}_0\} .$$

$[\Gamma, k]^{\mathbb{Z}}$ ist offensichtlich ein \mathbb{Z} -Modul, und es gilt

$$[\Gamma, k]^{\mathbb{Z}} \cdot [\Gamma, l]^{\mathbb{Z}} \subset [\Gamma, k+l]^{\mathbb{Z}} \quad \text{für } k, l \in \mathbb{N}_0 .$$

Wir nennen $f \in [\Gamma, k]^{\mathbb{Z}}$ *normiert*, falls $\alpha_f(0) = 1$ ist.

Die EISENSTEINREIHEN sind wichtige Beispiele von Modulformen aus $[\Gamma, k]^{\mathbb{Z}}$, es gilt

$$G_4^{*r} \cdot G_6^{*s} \in [\Gamma, k]^{\mathbb{Z}} \quad \text{für } 4r + 6s = k ,$$

und diese Produkte sind alle normiert.

Ohne Beweis der folgende

5.1.1 Satz. $[\Gamma, k]^{\mathbb{Z}}$ ist ein freier \mathbb{Z} -Modul, dessen Rang gleich der Dimension von $[\Gamma, k]$ ist. Basen von $[\Gamma, k]^{\mathbb{Z}}$ über \mathbb{Z} erhält man in der Form

$$g_\nu \cdot \Delta^{*\nu} \quad 0 \leq \nu \leq \left\lfloor \frac{k}{12} \right\rfloor \quad \text{bzw. } 0 \leq \nu < \left\lfloor \frac{k}{12} \right\rfloor , \quad \text{falls } k \equiv 2 \pmod{12} .$$

wobei $g_\nu \in [\Gamma, k - 12\nu]^{\mathbb{Z}}$ normiert ist.

Dies ist gleichzeitig eine \mathbb{C} -Basis von $[\Gamma, k]$ - solch eine Basis nennen wir *Ganzheitsbasis*.

Analog definiert man

$$[\Gamma, k]_0^{\mathbb{Z}} := [\Gamma, k]^{\mathbb{Z}} \cap [\Gamma, k]_0 ,$$

und man kann zeigen, daß

$$[\Gamma, k]_0^{\mathbb{Z}} = \Delta^* \cdot [\Gamma, k - 12\nu]^{\mathbb{Z}} .$$

5.2 Matrixdarstellung

Aus der bereits häufiger verwendeten Gleichung für die FOURIER-Koeffizienten

$$\alpha_{T_n f}(m) = \sum_{d|ggT(m,n)} d^{k-1} \cdot \alpha_f\left(\frac{mn}{d^2}\right)$$

erkennt man sofort, daß für $k > 0$

$$f \in [\Gamma, k]^{\mathbb{Z}} \implies T_n f \in [\Gamma, k]^{\mathbb{Z}}$$

und

$$f \in [\Gamma, k]_0^{\mathbb{Z}} \implies T_n f \in [\Gamma, k]_0^{\mathbb{Z}}$$

gilt.

Man wählt sich nun eine Ganzheitsbasis

$$g_1, \dots, g_t \quad t = \dim_{\mathbb{C}}[\Gamma, k] = \text{rang}_{\mathbb{Z}}[\Gamma, k]^{\mathbb{Z}}$$

von $[\Gamma, k]$ und $[\Gamma, k]^{\mathbb{Z}}$ und definiert

$$g := \begin{pmatrix} g_1 \\ \dots \\ \dots \\ \dots \\ g_t \end{pmatrix} \in \left([\Gamma, k]^{\mathbb{Z}}\right)^t ,$$

sowie

$$T_n g := T_n \begin{pmatrix} g_1 \\ \dots \\ \dots \\ \dots \\ g_t \end{pmatrix} := \begin{pmatrix} T_n g_1 \\ \dots \\ \dots \\ \dots \\ T_n g_t \end{pmatrix} .$$

Dieser Vektor drückt also aus, wie T_n auf einer Basis operiert. Interessanterweise können wir die Wirkung der T_n durch ganzzahlige Matrizen ausdrücken, die sich auf bekannte Art und Weise multiplizieren und sich aus den Matrizen zu Primzahlen berechnen lassen:

5.2.1 Satz. Für $k > 0$ gilt :

(i) Zu jedem $n \in \mathbb{N}$ gibt es eine eindeutig bestimmte Matrix $A(n) \in M(t \times t; \mathbb{Z})$ mit

$$T_n g = A(n) g$$

(ii) Die Matrizen $A(n)$ ($n \in \mathbb{N}$) sind paarweise vertauschbar und es gilt

$$A(m) \cdot A(n) = \sum_{d|ggT(m,n)} d^{k-1} \cdot A\left(\frac{mn}{d^2}\right) \quad \text{für alle } m, n \in \mathbb{N} .$$

(iii) Der von den Matrizen $A(n)$ ($n \in \mathbb{N}$) erzeugte Unterring $\mathcal{H}_k^{\mathbb{Z}}$ von $M(t \times t; \mathbb{Z})$ wird schon von den $A(p)$ (p prim) und der Einheitsmatrix erzeugt.

Beweis.

(i) Da $T_n g_\nu \in [\Gamma, k]^{\mathbb{Z}}$ und $\{g_\nu\}$ eine Basis dieses Moduls ist, gibt es eindeutig bestimmte $a_{\nu\mu}(n) \in \mathbb{Z}$ mit

$$T_n g_\nu = \sum_{\mu=1}^t a_{\nu\mu}(n) \cdot g_\mu \quad \text{für alle } \nu \in \{1, \dots, t\} .$$

$$A(n) := \left(a_{\nu\mu}(n) \right)_{\nu, \mu} \quad (\text{und nur diese}) \text{ erfüllt } T_n g = A(n) g .$$

(ii),(iii) sind damit sofort bewiesen, weil die entsprechenden Eigenschaften für die T_n gelten. □

5.2.2 Korollar. Die Eigenwerte der Matrizen $A(n)$ ($n \in \mathbb{N}$) sind algebraisch über \mathbb{Z} mit Grad $\leq t$.

Beweis. Die Eigenwerte sind die Nullstellen von $\det(X \cdot E - A(n))$, dies ist ein Polynom in $\mathbb{Z}[X]$ vom Grad t . □

Wenn wir von Eigenwerten von $A(n)$ reden, meinen wir natürlich die Eigenwerte der linearen Abbildung

$$A(n) : \mathbb{C}^t \longrightarrow \mathbb{C}^t .$$

Um die Wirkung der HECKE-Operatoren zu beschreiben verwenden wir aber die lineare Abbildung

$$\tilde{A}(n) : \prod_{i=1}^t \langle g_i \rangle \longrightarrow \prod_{i=1}^t \langle g_i \rangle ,$$

wobei wir das kartesische Produkt als \mathbb{C} -Vektorraum sofort mit $[\Gamma, k]$ identifizieren können, weil die g_i ja eine Basis bilden.

Der Isomorphismus

$$\Phi : \mathbb{C}^t \rightarrow [\Gamma, k] \quad e_i \mapsto g_i ,$$

wobei e_i der i -te Standardbasisvektor von \mathbb{C}^t ist, zeigt uns, daß die Eigenwerte von $A(n)$ genau die Eigenwerte von T_n sind, was ich nun etwas umständlich zeige.

Es sieht komplizierter aus als es ist, wenn man festhält, daß

$$\Phi(A(n) \cdot v) = \tilde{A}(n) \cdot \Phi(v) \quad \text{für alle } v \in \mathbb{C}^t$$

gilt.

Für $v \in \mathbb{C}^t$ und $f = \Phi(v) \in [\Gamma, k]$ ist damit

$$\begin{aligned} A(n) \cdot v = \lambda(n) \cdot v &\Leftrightarrow \Phi(A(n) \cdot v) = \Phi(\lambda(n) \cdot v) \\ &\Leftrightarrow \tilde{A}(n) \cdot \Phi(v) = \lambda(n) \cdot \Phi(v) \\ &\Leftrightarrow T_n f = \lambda(n) \cdot f . \end{aligned}$$

Hat man sich dies überlegt ist unmittelbar klar, daß wir aus Korollar 5.2.2 sofort folgern können, daß auch

5.2.3 Korollar. *Die Eigenwerte von T_n ($n \in \mathbb{N}$) sind algebraisch über \mathbb{Z} mit Grad $\leq t$.*

richtig ist.

□

Ebenso einfach wird damit das

5.2.4 Korollar *Sei $f \in [\Gamma, k]$ eine simultane Eigenform mit $\alpha_f(1) = 1$. Dann sind alle FOURIER-Koeffizienten von f algebraisch über \mathbb{Z} mit Grad $\leq t$.*

Beweis. Für eine simultane Eigenform wurde gezeigt, daß

$$\lambda_f(m) = \frac{\alpha_f(m)}{\alpha_f(1)} \quad \text{für alle } m \in \mathbb{N}$$

gilt.

□

6 Der erste neue Fall

In diesem Kapitel wird ein Beispiel zu Kapitel 5 durchgerechnet, wodurch wir eine explizite Darstellung der $A(p)$ (p prim) sowie genauere Kenntnis über ihre Eigenwerte gewinnen.

Wir betrachten hierbei nicht den Vektorraum aller ganzen Modulformen $[\Gamma, k]$, sondern nur die Spitzenformen $[\Gamma, k]_0$, da diese für die nicht-ganzen, und damit interessanten Eigenwerte verantwortlich sind. Alle Aussagen in Kapitel 5 sind auch für $[\Gamma, k]_0$ gültig.

Im Fall $k = 24$ hat $[\Gamma, k]_0$ zum ersten Mal die Dimension 2. Als Ganzheitsbasis wählen wir nach Satz 5.1.1

$$g_1 := G_6^* \cdot \Delta^* , \quad g_2 := \Delta^{*2} .$$

Wir kürzen wieder $q := e^{2\pi i \tau}$ ab. Aus den FOURIER-Darstellungen der normierten Diskriminante und EISENSTEINreihe errechnet man

$$\begin{aligned} \Delta^*(q) &= q - 2^3 \cdot 3 \cdot q^2 + 2^2 \cdot 3^2 \cdot 7 \cdot q^3 - 2^6 \cdot 23 \cdot q^4 + \dots \\ G_6^*(q) &= 1 - 2^3 \cdot 3^2 \cdot 7 \cdot q - 2^3 \cdot 3^3 \cdot 7 \cdot 11 \cdot q^2 - 2^5 \cdot 3^2 \cdot 7 \cdot 61 \cdot q^3 - \dots , \end{aligned}$$

und daraus

$$\begin{aligned} g_1(q) &= q - 2^3 \cdot 3 \cdot 43 \cdot q^2 + 2^2 \cdot 3^2 \cdot 7^2 \cdot 139 \cdot q^3 + 2^6 \cdot 31 \cdot 5527 \cdot q^4 + \dots \\ g_2(q) &= q^2 - 2^4 \cdot 3 \cdot q^3 + 2^3 \cdot 3^3 \cdot 5 \cdot q^4 + \dots . \end{aligned}$$

Da T_2 ein Endomorphismus auf $[\Gamma, k]_0$ ist, muß sich $T_2 g_1$ wieder als Linearkombination von g_1 und g_2 schreiben lassen.

Es ist

$$\alpha_{T_p f}(m) = \alpha_f(pm) + p^{23} \cdot \alpha_f\left(\frac{m}{p}\right) ,$$

wobei der letzte Summand nur dann $\neq 0$ ist, wenn $p \mid m$.

Also ist

$$\alpha_{T_2 g_1}(1) = \alpha_{g_1}(2) = -2^3 \cdot 3 \cdot 43 .$$

Nun ist glücklicherweise $\alpha_{g_2}(1) = 0$, weshalb wir schon folgern können, daß

$$T_2 g_1 = -2^3 \cdot 3 \cdot 43 \cdot g_1 + \beta \cdot g_2$$

mit noch zu bestimmendem β ist. Aus

$$\alpha_{T_2 g_1}(2) = \alpha_{g_1}(4) + 2^{23} \cdot \alpha_{g_1}(1) = 2^6 \cdot 31 \cdot 5527 + 2^{23}$$

folgt $\beta = 2^9 \cdot 3^6 \cdot 7^2$, also

$$T_2 g_1 = -2^3 \cdot 3 \cdot 43 \cdot g_1 + 2^9 \cdot 3^6 \cdot 7^2 \cdot g_2 .$$

Analog zeigt man

$$T_2 g_2 = g_1 + 2^6 \cdot 3 \cdot 11 \cdot g_2 .$$

In Matrixform:

$$A(2) = -2^3 \cdot 3 \cdot 43 \cdot E + A \quad \text{mit } A = \begin{pmatrix} 0 & 2^9 \cdot 3^6 \cdot 7^2 \\ 1 & 2^3 \cdot 3 \cdot 131 \end{pmatrix} .$$

Diese Vorgehensweise funktioniert aber nicht nur für 2, sondern auch für andere Primzahlen. Vereinfacht wird dies dadurch, daß $p \nmid 2$ für $p > 2$. Mit den Abkürzungen

$$\begin{aligned}\xi(p) &:= \alpha_{g_1}(2p) + 2^3 \cdot 3 \cdot 43 \cdot \alpha_{g_1}(p) \\ \eta(p) &:= \alpha_{g_1}(2p) + 2^3 \cdot 3 \cdot 43 \cdot \alpha_{g_1}(p)\end{aligned}$$

gilt:

$$A(p) = \begin{pmatrix} \alpha_{g_1}(p) & \xi(p) \\ \alpha_{g_2}(p) & \eta(p) \end{pmatrix} = \alpha_{g_1}(p) \cdot E + \begin{pmatrix} 0 & \xi(p) \\ \alpha_{g_2}(p) & \eta(p) - \alpha_{g_1}(p) \end{pmatrix} .$$

Für sich genommen ist das natürlich noch kein brauchbares Resultat. Aber wir wissen ja, daß $A(2) \cdot A(p) = A(p) \cdot A(2)$ ist, woraus wir sofort

$$\xi(p) = 2^9 \cdot 3^6 \cdot 7^2 \cdot \alpha_{g_2}(p) \quad \text{und} \quad \eta(p) - \alpha_{g_1}(p) = 2^3 \cdot 3 \cdot 131 \cdot \alpha_{g_2}(p)$$

folgern können. Daraus ergibt sich der folgende

6.1 Satz. *Für jede Primzahl p gilt:*

$$A(p) = \alpha_{g_1}(p) \cdot E + \alpha_{g_2}(p) \cdot A \quad \text{mit} \quad A = \begin{pmatrix} 0 & 2^9 \cdot 3^6 \cdot 7^2 \\ 1 & 2^3 \cdot 3 \cdot 131 \end{pmatrix} .$$

□

Zum Abschluß können wir Satz 6.1 benutzen, um eine Aussage über die Eigenwerte der $A(p)$ zu machen.

6.2 Korollar. *Die Eigenwerte aller Matrizen $A(p)$ (p prim) liegen im Körper $\mathbb{Q}[\sqrt{144169}]$.*

Beweis. Das charakteristische Polynom einer 2×2 -Matrix A ist

$$\chi(X) = X^2 - \text{spur}(A) \cdot X + \det(A) .$$

Damit wir einen Körper haben, in dem alle Nullstellen dieses Polynoms - und damit alle Eigenwerte - enthalten sind, müssen wir zu \mathbb{Q}

$$\sqrt{(\text{spur}(A))^2 - 4 \cdot \det(A)}$$

adjungieren.

Eine einfache Rechnung zeigt:

$$(\text{spur}(A))^2 - 4 \cdot \det(A) = (\alpha_{g_2}(p))^2 \cdot 2^6 \cdot 3^2 \cdot 144169 .$$

Für jedes p ist $\alpha_{g_2}(p) \in \mathbb{Z}$, und deshalb hat $(\alpha_{g_2}(p))^2 \cdot 2^6 \cdot 3^2$ insbesondere eine Wurzel in \mathbb{Q} .

□