1.) Bezeichnungen

Sei p eine Primzahl, $p \geq 5$, $p \equiv 3 \bmod 4$;
Sei (H) die von den Reihen

$$\Theta_C = \frac{1}{2} + \sum_{\alpha \in C} q^{N(\alpha)}$$

aufgespannte $\mathbb{C}$-Vektorraum, wo C die Idealklassen von $\mathbb{Q}(\sqrt{-p})$ durchläuft, die Summe über alle ganzen Ideale $\alpha \in C$ zu nehmen ist, und wobei $N(\alpha) = |\mathcal{O}/\alpha|$, wenn $\mathcal{O}$ den Ring der ganzen Zahlen von $\mathbb{Q}(\sqrt{-p})$ bezeichnet.
Es ist $\Theta_C = \Theta_{C^{-1}}$.
Sei I die Idealklassengruppe von $\mathbb{Q}(\sqrt{-p})$; für $\chi \in \hat{I}$ (= Gruppe der Charaktere von I) sei

$$\Theta_\chi = \sum_{C \in I} \chi(C)\, \Theta_C .$$

Es ist $\Theta_\chi = \Theta_{\bar{\chi}^{-1}}$; bezeichnet χ_0 den Hauptcharakter von I, so ist

$$\Theta_{\chi_0} = \frac{h(-p)}{2} + \sum_{n \geq 1} \Big\{ \sum_{d \mid n} \left(\frac{d}{p}\right) \Big\} q^n,$$

wo $h(-p)$ für die Klassenzahl von $\mathbb{Q}(\sqrt{-p})$ steht.
Setzt man $q = e^{2\pi i z}$, so wird Θ_χ für $\chi \neq \chi_0$ eine normalisierte Hecke-Eigenform auf $\Gamma_0(p)$ vom Nebentypus $\left(\frac{\cdot}{p}\right)$.
Im folgenden bezeichne $H(I)$ ein System von Idealklassen von I, sodaß für jedes $C \in I$ gilt: $C \in H(I)$ oder $C^{-1} \in H(I)$, aber $C, C^{-1} \in H(I)$ nur für $C = 1$ erfüllt ist.
Entsprechend sei $H(\hat{I})$ ein System von Charakteren von I, sodaß für jedes $\chi \in \hat{I}$ gilt: $\chi \in H(\hat{I})$ oder $\bar{\chi}^{-1} \in H(\hat{I})$, aber $\chi, \bar{\chi}^{-1} \in H(\hat{I})$ nur für den Hauptcharakter erfüllt ist.
Als $\mathbb{C}$-Basis für (H) kann man dann nehmen:
die Reihen Θ_C mit $C \in H(I)$,
oder
die Reihen Θ_χ mit $\chi \in H(\hat{I})$.

Sei $R \subseteq \mathbb{C}$ ein Ring, $\mathfrak{a} \subseteq R$ ein Ideal, so bezeichne $\overline{\kappa}$ für $\kappa \in R$ stets die Restklasse von κ in $R/\mathfrak{a}$.

Für ein $f = \sum a(n) q^n \in R[[q]]$ sei $\overline{f} := \sum \overline{a(n)} q^n$, also $\overline{f} \in R/\mathfrak{a}[[q]]$.

Wir setzen

$$\mathfrak{H}(R) = \mathfrak{H} \cap R[[q]],$$

$$\mathfrak{H}(R) \bmod \mathfrak{a} = \{\overline{f} \mid f \in \mathfrak{H}(R)\}.$$

M_r bezeichne den $\mathbb{C}$-Vektorraum der ganzen Modulformen auf $SL_2\mathbb{Z}$ vom Gewicht r, S_r den Teilraum der Spitzenformen von M_r. Wir fassen die Fourierentwicklungen der Elemente von M_r, S_r wohlweise als formale Potenzreihen in q auf und setzen:

$$M_r(R) = M_r \cap R[[q]],$$

$$M_r(R) \bmod \mathfrak{a} = \{\overline{f} \mid f \in M_r(R)\}.$$

Sinngemäß definieren wir $S_r(R)$ und $S_r(R) \bmod \mathfrak{a}$.

2. Reduktion modulo $\mathfrak{P}$

Sei K ein algebraischer Zahlkörper, $\mathfrak{P}$ ein Primideal in K mit $\mathfrak{P}|p$, so bezeichne $\mathcal{O}_{\mathfrak{P}}$ den Ring der $\mathfrak{P}$-ganzen Zahlen in K; es sei $\mathcal{O}_p = \bigcap_{\mathfrak{P}|p} \mathcal{O}_{\mathfrak{P}}$, wo der Durchschnitt über alle Primideale $\mathfrak{P}$ aus K mit $\mathfrak{P}|p$ zu nehmen ist.

Proposition 1

$\mathfrak{H}(\mathcal{O}_p) \bmod p$ ist ein freier $\mathcal{O}_p/p\mathcal{O}_p$-Modul vom Rang $\frac{h(-p)+1}{2}$; genauer gilt:

a) $\overline{\Theta}_C$, $C \in H(I)$, ist eine Basis von $\mathfrak{H}(\mathcal{O}_p) \bmod p$,

b) Gilt $K \supseteq \bigcup_{\chi \in \hat{I}} \chi(I)$, so ist auch Θ_χ, $\chi \in H(\hat{I})$, eine Basis von $\mathfrak{H}(\mathcal{O}_p) \bmod p$.

Die Proposition gilt sinngemäß für $\mathfrak{H}(\mathcal{O}_{\mathfrak{P}}) \bmod \mathfrak{P}$ für jedes $\mathfrak{P}|p$.

Beweis

Sei $\overline{f} \in \textcircled{H}(\mathcal{O}_p) \bmod p$, $f = \sum a(n) q^n \in \textcircled{H}$, so gibt es zunächst Zahlen $\kappa_C \in \mathbb{C}$, sodaß

$$(*) \qquad f = \sum_{C \in H(I)} \kappa_C \, \Theta_C .$$

Sei nun $C_0 \in H(I)$, so gibt es ein Primideal $\mathfrak{l}$ in C_0, und aus (*) und der Definition der Θ_C folgt ~~mittels~~

$$(**) \qquad a(N(\mathfrak{l})) = \kappa_{C_0} \cdot \begin{cases} 1 \\ 2 \end{cases}$$

Da $f \in \textcircled{H}(\mathcal{O}_p)$ folgt somit $\kappa_{C_0} \in \mathcal{O}_p$, und wir haben

$$\overline{f} = \sum_{C \in H(I)} \overline{\kappa_C} \, \overline{\Theta_C} .$$

Sei $\overline{f} = 0$, also $\overline{a(n)} = 0$ für jede n, so folgt aus (**): $\overline{\kappa_{C_0}} = 0$.

Damit ist Teil a) bewiesen; insbesondere ist die Ordnung von $\textcircled{H}(\mathcal{O}_p) \bmod p$ gleich $\# H(I) = \dfrac{h(-p)+1}{2}$.

Da $\chi(C)$ für $\chi \in \hat{I}$, $C \in I$ stets eine ℓ-ein heits wurzel ist, haben wir unter der in Teil b) aus k gestellten Bedingung, daß $\chi(C) \in \mathcal{O}_p$; also ist $\Theta_\chi \in \textcircled{H}(\mathcal{O}_p)$ für jedes χ.

Für jede Idealklasse C ist nun

$$\sum_{\chi \in \hat{I}} \chi(C)^{-1} \Theta_\chi = \sum_{\chi \in I} \chi(C)^{-1} \sum_{D \in I} \chi(D) \, \Theta_D$$

$$= \sum_{D \in I} \Theta_D \sum_{\chi \in \hat{I}} \chi(C^{-1} D) = h(-p) \, \Theta_D .$$

Nun ist $h(-p)^{-1} \in \mathcal{O}_p$, und wir haben daher

$$\Theta_D = \frac{1}{h(-p)} \sum_{\chi \in \hat{I}} \overline{\chi(C)^{-1}} \; \overline{\Theta_\chi} .$$

Aus Teil a), aus $\Theta_\chi = \Theta_{\chi^{-1}}$ und aus $\# H(\hat{I}) = \dfrac{h(-p)+1}{2}$ folgt nun leicht die Aussage von Teil b). $\square$

Sei r eine natürliche Zahl mit

$$r \equiv \frac{p+1}{2} \bmod p-1$$

(sodaß r insbesondere gerade ist),

$$E_r = 1 - \frac{2r}{B_r} \sum_{n \geq 1} \sigma_{r-1}(n)\, q^n$$

(B_r ist die r-te Bernoullische Zahl: $\frac{q}{e^q - 1} = \sum \frac{B_n}{n!} q^n$).

Nach der Kummerschen Kongruenz für die Bernoullischen Zahlen ist B_r p-ganz ($p \geq 5$!) und

$$B_r \equiv B_{\frac{p+1}{2}} \bmod p;$$

es gilt ferner

$$-B_{\frac{p+1}{2}} \equiv \frac{h(-p)}{2} \bmod p, \quad \frac{h(-p)}{2} \not\equiv 0 \bmod p,$$

sodaß also $E_r \in M_r(\Gamma_p)$ und

$$E_r \equiv 1 + \frac{2}{h(-p)} \sum \Big(\sum_{d \mid n} d^{\frac{p-1}{2}} \Big) q^n$$

$$\equiv \frac{2}{h(-p)} \left\{ \frac{h(-p)}{2} + \sum \Big(\sum_{d \mid n} \Big(\frac{d}{p}\Big) \Big) q^n \right\}$$

$$\equiv \frac{2}{h(-p)}\, \Theta_{\chi_0} \bmod p,$$

wenn χ_0 den Hauptcharakter von I bezeichnet.

Es ist $M_r = \mathbb{C} E_r \oplus S_r$, und es gibt eine Basis $g_1, \dots, g_n$ von S_r, sodaß $g_i \in S_r(\mathbb{Z})$ und für $g_i = \sum a_i(n) q^n$ gilt:

$$a_i(n) = \begin{cases} 0 & \text{für } 1 \leq n \leq i \\ 1 & \text{für } n = i \end{cases}$$

(cf. Lang: Introduction to Mod. Forms, p. 158); es ist dann unmittelbar klar:

Proposition 2

$M_r(\mathcal{O}_p) \bmod p$ ist ein freier $\mathcal{O}_p / p\mathcal{O}_p$-Modul; als Basis kann $\overline{E}_r, \overline{g}_1, \dots, \overline{g}_n$ gewählt werden.

Diese Aussage gilt sinngemäß für $M_r(\mathcal{O}_{\mathfrak{P}}) \bmod \mathfrak{P}$ für jedes $\mathfrak{P} \mid p$.

Satz

Unter der Voraussetzung $r \equiv \frac{p+1}{2} \bmod p-1$ gilt:

$$\textcircled{H}(\mathcal{O}_p) \bmod p \subseteq M_r(\mathcal{O}_p) \bmod p$$

und für jedes Primideal $\mathfrak{P}$ mit $\mathfrak{P} \mid p$:

$$\textcircled{H}(\mathcal{O}_{\mathfrak{P}}) \bmod \mathfrak{P} \subseteq M_r(\mathcal{O}_{\mathfrak{P}}) \bmod \mathfrak{P}.$$

Beweis

Weiter unten in 4.) wird bewiesen, daß zu jeder Idealklasse C von $\mathbb{Q}(\sqrt{-p})$ eine $f \in M_{\frac{p+1}{2}}(\mathbb{Z})$ existiert, so daß $\Theta_C \equiv f \bmod p$.

~~hat $r = \frac{p+1}{2} + t(p-1)$,~~

Nach der Von-Staudtschen Kongruenz für die Bernoullischen Zahlen ist $E_{p-1} \equiv 1 \bmod p$,

Daher haben wir - mit $r = \frac{p+1}{2} + t(p-1)$ für eine geeignete Zahl t - :

$$\Theta_C \equiv f E_{p-1}^t \bmod p \text{ und } f E_{p-1}^t \in M_r(\mathbb{Z}).$$

Der Satz folgt nun unmittelbar aus Proposition 1. $\square$

Mit den üblichen Schlußweisen der linearen Algebra sieht man leicht, daß

$$M_r(\mathcal{O}_p) \bmod p = \textcircled{H}(\mathcal{O}_p) \bmod p \oplus \bigoplus_{n=1}^{\dim S_r - \frac{h(-p)-1}{2}} \mathcal{O}_p/p\mathcal{O}_p \; \overline{g_{i_n}}$$

für geeignete Zahlen i_n, wo $g_1, g_2, \ldots$ die oben erwähnte $\mathbb{Z}$-Basis von $\Delta_r(\mathbb{Z})$ bedeutet; wir können $g_i = \Delta^i E_4^a E_6^b$ für geeignete Zahlen a, b und mit $\Delta = q \prod_{n=1}^{\infty}(1-q^n)^{12}$ wählen.

So erhält man beispielsweise für $p \leq 163$:

$$M_{\frac{p+1}{2}}(\mathcal{O}_p) \bmod p = \textcircled{H}(\mathcal{O}_p) \bmod p \quad \text{für } p = 7, 11, 19, 23, 31, 47, 71$$

$$\textcircled{H}(\mathcal{O}_p) \bmod p = \mathcal{O}_p/p\mathcal{O}_p \; E_{\frac{p+1}{2}} \quad \text{für } p = 7, 11, 19, 43, 67, 103, 163$$

und für die übrigen p:

p	Basis von $M_{\frac{p+1}{2}}(\mathcal{O}_p)$ mod p	
	Basis von $\Theta(\mathcal{O}_p)$ mod p	$g_{i_1}, g_{i_2}, \ldots$
59	$[1,1,15]$, $[3,1,5]$	$\Delta^2 E_6$
79	$[1,1,20]$, $[2,1,10]$, $[4,1,5]$	$\Delta^3 E_4$
83	$[1,1,21]$, $[3,1,7]$	$\Delta^2 E_6^3$, $\Delta^3 E_6$
103	$[1,1,26]$, $[2,1,13]$, $[4,3,7]$	$\Delta^3 E_6^2 E_4$, $\Delta^4 E_4$
107	$[1,1,27]$, $[3,1,9]$	$\Delta^2 E_6^5$, $\Delta^3 E_6^3$, $\Delta^4 E_6$
127	$[1,1,32]$, $[2,1,16]$, $[4,1,8]$	$\Delta^3 E_6^4 E_4$, $\Delta^4 E_6^2 E_4$, $\Delta^5 E_4$
131	$[1,1,33]$, $[3,1,11]$, $[5,3,7]$	$\Delta^3 E_6^5$, $\Delta^4 E_6^3$, $\Delta^5 E_6$
139	$[1,1,35]$, $[5,1,7]$	$\Delta^2 E_6^7 E_4$, $\Delta^3 E_6^5 E_4$, $\Delta^4 E_6^3 E_4$, $\Delta^5 E_6 E_4$
151	$[1,1,38]$, $[2,1,19]$, $[4,3,10]$, $[5,3,8]$	$\Delta^3 E_6^6 E_4$, $\Delta^5 E_6^2 E_4$, $\Delta^6 E_4$

Dabei steht $[a,b,c]$ als Abkürzung für $\sum_{x,y \in \mathbb{Z}} q^{ax^2+bxy+cy^2}$;

3.) Kongruenzen zwischen Hecke-Eigenformen

Sei $r \equiv \frac{p+1}{2} \bmod (p-1)$, seien $f_1, \dots, f_n$ die normalisierten Hecke-Eigenformen von S_r,

$$f_i = \sum a_i(n)\, q^n .$$

Die $a_i(n)$ sind ganz algebraische Zahlen, und es ist möglich den Zahlkörper K aus 2.) so zu wählen, daß K die Fourierkoeffizienten der f_i und $\mathcal{O}_K$ umfaßt.

Sei $\mathcal{H}$ der Ring der Hecke-Operatoren auf S_r, d.h. $\mathcal{H} \subseteq \mathrm{End}_{\mathbb{C}} S_r$ ist der von den Operatoren $T(l)$ (l durchläuft die Menge der Primzahlen) erzeugte Ring, wo für $f = \sum a(n)\, q^n \in S_r$!

$$(*) \qquad f|T(l) = \sum \{a(ln) + l^{r-1} a(\tfrac{n}{l})\}\, q^n$$

($a(\frac{n}{l}) := 0$ für $l \nmid n$).

Es ist stets

$$(**) \qquad \prod_{i=1}^{n} (T(l) - a_i(l)) = 0 .$$

Wegen (*) gibt es einen ~~Hom~~ Ringhomomorphismus

$$\mathcal{O}_p \mathcal{H} \longrightarrow \mathrm{End}\left(S_r(\mathcal{O}_p) \bmod p\right) \quad (\text{bzw. } \mathrm{End}((S_r(\mathcal{O}_{\mathfrak{P}}) \bmod \mathfrak{P}))$$
$$\Lambda \longrightarrow \bar{\Lambda}$$

wo $\bar{\Lambda}$ sich erklären läßt durch $\bar{f}|\bar{\Lambda} = \overline{f|\Lambda}$ für $f \in S_r \mathcal{O}_p$ (bzw. $f \in S_r \mathcal{O}_{\mathfrak{P}}$).

Sei $\mathcal{H}_p$ (bzw. $\mathcal{H}_{\mathfrak{P}}$) das Bild dieses Homomorphismus; $\mathcal{H}_p$ (bzw. $\mathcal{H}_{\mathfrak{P}}$) ist eine $\mathcal{O}_p/p\mathcal{O}_p$- (bzw. $\mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{\mathfrak{P}}$-) Algebra, und wir haben n Algebren-Homomorphismen $S_1, \dots, S_n : \mathcal{H}_p \longrightarrow \mathcal{O}_p/p\mathcal{O}_p$

(bzw. $S_1 \to S_n : \mathcal{H}_{\mathfrak{P}} \to \mathcal{O}_{\mathfrak{P}}/\mathfrak{P}\mathcal{O}_{\mathfrak{P}}$), die definiert sind durch:

$$\overline{f_i}\,|_\lambda = S(\lambda)\,\overline{f_i} \qquad (\lambda \in \mathcal{H}_p \text{ (bzw. } \lambda \in \mathcal{H}_{\mathfrak{P}})).$$

Aus (**) folgt leicht

$$(***) \qquad \prod_{i=1}^{n} (\lambda - S_i(\lambda)) = 0 \quad \text{für alle } \lambda \in \mathcal{H}_p \text{ (bzw. } \in \mathcal{H}_{\mathfrak{P}}).$$

Proposition 3

Ist $\chi \in \hat{I}$, $\chi \neq 1$, so gibt es eine Darstellung

$$\varphi : \mathcal{H}_p \to \mathcal{O}_p/p\mathcal{O}_p,$$

sodass $\overline{\Theta}_\chi\,|_\lambda = \varphi(\lambda)\,\overline{\Theta}_\chi$ für $\lambda \in \mathcal{H}_p$.

Eine ähnliche Aussage gilt für jedes in $\mathfrak{P}$ aufgehende Primideal.

Beweis

Zunächst ist ~~klar, dass~~ nach dem bisher Gezeigten klar, dass $\overline{\Theta}_\chi \in S_r(\mathcal{O}_p)$ mod p.

Da die Operatoren $\overline{T(l)}$ $\mathcal{H}_p$ erzeugen, genügt es nachzuweisen, dass $\overline{\Theta}_\chi$ Eigenvektor der $\overline{T(l)}$ ist; nun ist aber Θ_χ als Modulform auf $\Gamma_0(p)$ vom Nebentypus $(1, (\frac{-}{p}))$ eine normalisierte Hecke-Eigenform, d.h. für jede Primzahl l gilt:

$$a(ln) + \left(\frac{l}{p}\right) a\left(\frac{n}{l}\right) = a(l)\,a(n) \qquad \left(\left(\frac{p}{p}\right) := 0\right)$$

falls $\Theta_\chi = \sum a(n)\,q^n$; da $\left(\frac{l}{p}\right) \equiv l^{\frac{r-1}{2}} \bmod p$, folgt die Behauptung nun mit (**). □

Es folgt i.A. nicht:

$$\Theta_\chi \equiv f_i \bmod p \quad \text{für eine der } f_i.$$

Gegenbeispiel:

Für $p = 47$ ist $h(-p) = 5$; ist daher $\zeta = e^{2\pi i/5}$, bezeichnet $C \neq 1$ eine Idealklasse von $\mathbb{Q}(\sqrt{-47})$, so sind die beiden normalisierten Hecke-Eigen- und Spitzenformen von (1) gegeben durch:

$$\Theta_1 = \Theta_{C^0} + (\zeta + \zeta^4)\,\Theta_C + (\zeta^2 + \zeta^3)\,\Theta_{C^2}$$

$$\Theta_2 = \Theta_{C^0} + (\zeta^2 + \zeta^3)\,\Theta_C + (\zeta^1 + \zeta^4)\,\Theta_{C^2}.$$

Nun ist $\zeta + \zeta^4 = \frac{-1+\sqrt{5}}{2}$, $(\zeta^2 + \zeta^3) = \frac{-1-\sqrt{5}}{2}$; der von den Fourierkoeffizienten von Θ_1, Θ_2 erzeugte Körper ist $\mathbb{Q}(\sqrt{5})$.

Auf der anderen Seite ist $\dim S_{22} = 2$, und der von den beiden normalisierten Hecke-Eigenformen $f_1, f_2 \in S_{22}$ erzeugte Körper ist $\mathbb{Q}(\sqrt{144\,169})$.

Für k kann also $\mathbb{Q}(\sqrt{144\,169}, \sqrt{5})$ genommen werden.

Wäre etwa

$$\Theta_1 \equiv f_1 \bmod p,$$

so sei $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$ der Automorphismus mit

$\sqrt{5} \longrightarrow -\sqrt{5}$, $\sqrt{144\,169} \longrightarrow \sqrt{144\,169}$, sodaß

$$\Theta_2 = \Theta_1^\sigma \equiv f_1^\sigma = f_1 \bmod p$$

gilt (für $f = \sum a(n) q^n \in k[[q]]$ sei $f^\sigma := \sum a(n)^\sigma q^n$),

daher $\Theta_1 \equiv \Theta_2 \bmod p$, was unmöglich ist (vgl. Proposition 1).

Es gilt aber

Satz

Sei $\mathfrak{p}$ ein Primideal in k mit $\mathfrak{p} \mid p$; dann gibt es zu jedem Θ_χ eine normalisierte Hecke-Eigenform $f \in S_\tau$, sodaß

$$\Theta_\chi \equiv f \bmod \mathfrak{p}.$$

Beweis

Sei $F = \mathcal{O}_{\mathfrak{p}} / \mathfrak{p}\mathcal{O}_{\mathfrak{p}}$, dann ist F ein Körper.

Wir definieren eine Abbildung

$$\underline{\Psi} : \mathcal{H}_{\mathfrak{p}} \longrightarrow \underbrace{F \oplus \dots \oplus F}_{n\text{-mal}}$$

$$\Lambda \longmapsto (g_1(\Lambda), \dots, g_n(\Lambda))$$

(wobei wie oben $n = \dim S_r$, $\overline{f_i}|_\Lambda = g_i(\Lambda)\,\overline{f_i}$, wenn $f_1, \dots, f_n$ die normalisierten Hecke-Eigenformen von S_r sind.

Sei $\varphi : \mathcal{H}_{\mathfrak{p}} \to F$ gemäß Proposition 3 definiert durch $\overline{\Theta_\chi}|_\Lambda = \varphi(\Lambda)\,\overline{\Theta_\chi}$; es genügt zu zeigen, daß $\varphi = g_i$ für ein i.

Sei $A = \mathcal{H}_{\mathfrak{p}} / \ker \underline{\Psi}$, so ist A eine F-Algebra; nun ist $F \oplus \dots \oplus F$ halbeinfach, daher ist auch $\Psi(\mathcal{H}_{\mathfrak{p}})$ halbeinfach, wegen $A \cong \Psi(\mathcal{H}_{\mathfrak{p}})$ ist somit A halbeinfach.

Ist $\Lambda \in \ker \underline{\Psi}$, so ist $\Lambda^n = 0$ (nach (***)), daher $\varphi(\Lambda)^n = 0$, d.h. $\varphi(\Lambda) = 0$; also ist $\ker \underline{\Psi} \subseteq \ker \varphi$, also induzieren φ und (wegen $\ker \underline{\Psi} \subseteq \ker g_i$) die g_i F-Algebren Homomorphismen $\underline{\varphi}, \underline{g_i} : A \to F$.

Da A halbeinfach ist, gibt es ein Ideal $\mathcal{U} \subseteq A$, sodaß

$$A = \ker \underline{\varphi} \oplus \mathcal{U};$$

$\mathcal{U}$ ist ein Körper, denn $\varphi|_{\mathcal{U}} : \mathcal{U} \to F$ ist ein Isomorphismus.

$A \to F \oplus \dots \oplus F$, $a \mapsto (\underline{g_1}(a), \dots, \underline{g_n}(a))$ ist eine Injektion, sodaß daher für ein i $g_i(\mathcal{U}) \neq 0$, d.h. $\ker \underline{g_i} \cap \mathcal{U} \neq \mathcal{U}$ gelten muß; da $\mathcal{U}$ ein Körper ist, erhalten wir für solch ein i: $\ker \underline{g_i} \cap \mathcal{U} = 0$, also $\ker \underline{g_i} \subseteq \ker \underline{\varphi}$; da $\ker \underline{g_i}$ ein maximales Ideal in A ist ($A / \ker \underline{g_i} \cong F$!), folgt $\ker \underline{g_i} = \ker \varphi$, daher auch $\ker g_i = \ker \varphi$.

Also haben wir für $\kappa \in F$, $\lambda \in \mathcal{H}_{\mathfrak{p}}$:

$$S_i(\lambda - \kappa) = 0 \iff \varphi(\lambda - \kappa) = 0,$$

daher $S_i = \varphi$. □

Anmerkung

Sei $\mathcal{H}_Q$ der Ring der Hecke-Operatoren auf $S_r(Q)$, sei k Galoiserweiterung von Q, sodaß k die ~~ganzen~~ Koeffizienten der normalisierten Hecke-Eigenformen von $f_1, \dots, f_n$ von S_r umfaßt; ~~Gal(k/Q)~~

Es ist $\mathcal{H}_Q$ aufgefaßt als $\mathcal{H}_Q$-Modul genau dann irreduzibel, wenn $\mathrm{Gal}(k/Q)$ transitiv auf $\{f_1, \dots, f_n\}$ operiert ($f_i^\sigma = \sum a_{i(n)}^\sigma q^n$ sei $f_i = \sum a_{i(n)} q^n$ sei $\sigma \in \mathrm{Gal}(k/Q)$); operiert nun $\mathrm{Gal}(k/Q)$ transitiv auf $\{f_1, \dots, f_n\}$, so erhalten wir mit dem eben bewiesenen Satz zu jedem f_i ein Primideal $\mathfrak{P}/\mathfrak{p}$ und ein Θ_α, sodaß $f_i \equiv \Theta_\alpha \bmod \mathfrak{P}$.

Beispiele

Sei $T_r(X)$ das charakteristische Polynom von $T(2)$ auf S_r. Die $T_r(X)$ für $2 \le r \le 120$ sind irreduzibel über Q, daher ist auch $S_r(Q)$ irreduzibler $\mathcal{H}_Q$-Modul; ~~daher für jede normierte Hecke-Eigenform~~ ~~gilt~~

ist D_r die Diskriminante von $T_r(X)$, so gilt für alle $p \equiv 3 \bmod 4$ und $5 \le p \le 167$: $p \mid D_r$ genau für $p = 131$; ~~es~~ sind daher für $5 \le p \le 167$, $p \neq 131$ die normalisierten Hecke-Eigenformen von $S_{\frac{p+1}{2}}$ für jedes $\mathfrak{P}/\mathfrak{p}$ paarweise ein anderer Kongruenz $\bmod \mathfrak{P}$.

(Diese Informationen entstammen einer Tabelle von Y. Maeda)

Sind $f_1, \dots f_n$ die normalisierten Hecke-Eigenformen von $S_{\frac{p+1}{2}}$, $\mathfrak{R}/p$, $\tilde{h} = \frac{h(-p)-1}{2}$ und $\Theta_1, \dots \Theta_{\tilde{h}}$ die normalisierten Hecke-Eigen- und Spitzenformen von (H), schließlich $B_{\mathfrak{R}}(\Theta_i) = \{ f_j \mid f_j \equiv \Theta_i \bmod \mathfrak{R} \}$, $B_{\mathfrak{R}} = \{ f_j \mid$ für kein Θ_i gilt: $f_j \equiv \Theta_i \bmod \mathfrak{R} \}$, so ist

$$\{ f_1, \dots, f_n \} = B_{\mathfrak{R}} + B_{\mathfrak{R}}(\Theta_1) + \dots + B_{\mathfrak{R}}(\Theta_{\tilde{h}}) \quad \text{(disjunkte Vereinigung)}.$$

Die Anzahlen $\# B_{\mathfrak{R}}$ und $\# B_{\mathfrak{R}}(\Theta_i)$ sind unabhängig von der Wahl von $\mathfrak{R}$.

Für die p mit $5 \le p \le 167$ und $p \neq 131$ hat man nach obigen Gesagten: $\# B_{\mathfrak{R}}(\Theta_1) = \dots = \# B_{\mathfrak{R}}(\Theta_{\tilde{h}}) = 1$, $\# B_{\mathfrak{R}} = n - \tilde{h}$.

Für $p = 23, 31, \dots, 71$ ergibt das Satz aus 3.):

(1) $\Delta \equiv \frac{1}{2}(\Theta_{[1,1,6]} - \Theta_{[2,1,3]})$ $\quad (\Theta_{[a,b,c]} := \sum_{x,y \in \mathbb{Z}} q^{ax^2+bxy+cy^2})$

$\equiv \frac{3}{4}(\Theta_{[1,1,6]} - E_{12}) \bmod 23$

(2) $\Delta E_4 \equiv \frac{1}{2}(\Theta_{[1,1,8]} - \Theta_{[2,1,4]})$

$\equiv \frac{3}{4}(\Theta_{[1,1,8]} - E_{16}) \bmod 31$

(3) $2 \sum Tr_{24} T(n)\, q^n \equiv 2\,\Theta_{[1,1,12]} - (\Theta_{[2,1,6]} + \Theta_{[3,1,4]})$

$\equiv \frac{5}{2}(\Theta_{[1,1,12]} - E_{24}) \bmod 47$

($Tr_{\frac{p+1}{2}} T(n)$ = Spur von $T(n)$ auf $S_{\frac{p+1}{2}}$),

(4) $2 \sum Tr_{36} T(n)\, q^n \equiv 3\,\Theta_{[1,1,18]} - (\Theta_{[2,1,9]} + \Theta_{[3,1,6]} + \Theta_{[4,3,5]})$

$\equiv \frac{7}{2}(\Theta_{[1,1,18]} - E_{36}) \bmod 71$

(5) Für $p = 59$ ist $h^{\frac{(-p)-1}{2}} = 1$;

die Hecke-Eigen-Spitzenform von ⑭ ist

$$\frac{1}{2}\left(\Theta_{[1,1,15]} - \Theta_{[3,1,5]}\right) = q - q^3 + \dots .$$

Das charakteristische Polynom von $T(2)$ auf S_{30} ist

$$X^2 - 8640\,X - 454 \cdot 569 \cdot 984,$$

die Diskriminante ist $2^{12} \cdot 3^2 \cdot 51\,349$;

die beiden Eigenwerte $g_\pm$ von $T(2)$ sind also

$$g_\pm = 96\,(45 \pm \sqrt{d}), \quad d = 51\,349.$$

Für die beiden normalisierten Hecke-Eigenformen $f_\pm$ von S_{30} haben wir also:

$$f_\pm \equiv \frac{1}{2}\left(\Theta_{[1,1,15]} - \Theta_{[3,1,5]}\right) + g_\pm\, \Delta^2 E_6 \bmod 59.$$

In $\mathbb{Q}(\sqrt{51\,349})$ haben wir die Primidealzerlegung

$$59 = (59,\ 45 + \sqrt{d}) \cdot (59,\ 45 - \sqrt{d}).$$

4.) Sei V ein endlich-dimensionaler $\mathbb{Q}$-Vektorraum mit einem positiv-definiten Skalarprodukt $(\lambda, \mu) \longmapsto \lambda \cdot \mu \in \mathbb{Q}$.

Sei $\Lambda \subseteq V$ ein vollständiges, ganzes und gerades Gitter (d.h. $\operatorname{rang}(\Lambda) = \dim V$; $\lambda \cdot \mu \in \mathbb{Z}$, $\lambda^2 \in 2\mathbb{Z}$ für alle $\lambda, \mu \in \Lambda$).

Λ^* bezeichne das zu Λ duale Gitter, $d = \det(\Lambda) = |\Lambda^*/\Lambda|$, s = Stufe von Λ (die kleinste positive natürliche Zahl, sodaß für alle $\lambda, \mu \in \Lambda^*$: $s\lambda \cdot \mu \in \mathbb{Z}$, $s\lambda^2 \in 2\mathbb{Z}$); für $\xi \in \Lambda^*$ bezeichne $\overline{\xi}$ die Nebenklasse $\xi + \Lambda$.

Für $M \subseteq \Lambda^*$ sei $\Theta_M = \sum_{\lambda \in M} q^{\lambda^2/2}$ $(q = e^{2\pi i z}, \operatorname{Im} z > 0)$, für $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2\mathbb{Z}$ sei $\Theta_M|_A$ die Funktion

$$\Theta_M|_A(z) = \frac{\Theta_M(Az)}{\sqrt{cz+d}^{\operatorname{rang}(\Lambda)}},$$

wobei die Wurzel so gewählt sei, daß $-\pi/2 < \arg(\sqrt{cz+d}) \leq +\pi/2$.

Es gilt die

Satz 0

Es gibt eine Abbildung $D : SL_2\mathbb{Z} \longrightarrow GL_d R$ – wobei $R = \mathbb{Z}\left[\frac{1}{\det\Lambda}, e^{\pi i s/4}\right]$ ($d = \det\Lambda$, s = Stufe von Λ) –, sodaß D einen Homomorphismus

$$SL_2\mathbb{Z} \longrightarrow GL_d R/\{\pm 1\} \quad \text{– falls } r \equiv 1 \text{ mod } 2$$

bzw. $$SL_2\mathbb{Z} \longrightarrow GL_d R \quad \text{– falls } r \equiv 0 \text{ mod } 2$$

induziert,

und sodaß mit $D(A) = \left(D(A)|_{\bar{\lambda},\bar{\mu}}\right)_{\bar{\lambda},\bar{\mu} \in \Lambda^*/\Lambda}$ gilt:

$$\Theta_{\bar{\lambda}}|_A = \sum_{\bar{\mu} \in \Lambda^*/\Lambda} D(A)|_{\bar{\lambda},\bar{\mu}}\, \Theta_{\bar{\mu}}.$$

Dabei ist

$$D\left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right)\Big|_{\bar{z},\bar{\tau}} = \frac{e^{-\pi i \frac{\operatorname{sig} \Lambda}{4}}}{\sqrt{\det(\Lambda)}} \; e^{-2\pi i z \cdot \mu},$$

$$D\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right)\Big|_{\bar{z},\bar{\tau}} = e^{\pi i \lambda^2} \quad \text{für } \bar{z} = \bar{\mu} \text{ und } = 0 \text{ sonst},$$

und für $A \in \Gamma_0(S)$, $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$:

$$D(A)\Big|_{z,\bar{\tau}} = \text{8-te Einheitswurzel falls } \bar{\mu} = a\bar{z} \text{ und } = 0 \text{ sonst.}$$

Da g ein Endomorphismus des $\mathbb{Q}$-Vektorraums V mit $g\Lambda \subseteq \Lambda$ und $g\Lambda^* \subseteq \Lambda^*$, so induziert g einen Endomorphismus des $\mathbb{Z}$-Moduls Λ^*/Λ; ist insbesondere g ein Automorphismus des Gitters Λ, d.h. ist g ein Element der orthogonalen Gruppe von V und $g\Lambda = \Lambda$, so folgt $g\Lambda^* = \Lambda^*$ und g induziert einen Automorphismus von Λ^*/Λ.

Es gilt das folgende

Lemma

Sei g ein Automorphismus des Gitters Λ, so gilt für jedes $A \in SL_2\mathbb{Z}$:

$$D(A)\Big|_{\overline{gz},\overline{g\mu}} = D(A)\Big|_{z,\bar{\tau}}.$$

Beweis

Aus Satz C folgt unmittelbar die Richtigkeit der Behauptung für $S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ und $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$; sodaß die allgemeine Behauptung durch Induktion über die Länge eines „Wortes" in S und T folgt. □

Satz

Sei g ein Automorphismus des Gitters Λ, sodaß

(i) Ordnung von $g = p$ für eine Primzahl p

(ii) $(p-1 \mid [Sl_2\mathbb{Z} : \Gamma_0(s)]) = 1$ (s = Stufe von Λ),

(iii) $g - 1$ einen Automorphismus von $\Lambda^\vee/\Lambda$ induziert;

dann gilt:

1.) $\operatorname{rang}(\Lambda) \equiv \sigma \bmod 4$,

$\Theta_\Lambda|_A = \Theta_\Lambda$ für $A \in B_0(s)$;

ist R ein Repräsentantensystem für $\Gamma_0(s) \backslash Sl_2\mathbb{Z}$, so ist

$$\tilde{\Theta}_\Lambda := \frac{1}{[Sl_2\mathbb{Z} : \Gamma_0(s)]} \sum_{A \in R} \Theta_\Lambda|_A$$

von der Wahl von R unabhängig und eine Modulform der Stufe 1 mit Fourierkoeffizienten in $\mathbb{Z}_p[e^{\pi i s/4}]$ – wo $\mathbb{Z}_p$ für den nach p lokalisierten Ring $\mathbb{Z}$ steht –,

und

2.) $$\Theta_\Lambda \equiv \tilde{\Theta}_\Lambda \bmod p.$$

Zusatz

Sei $\Gamma = \{z \in \Lambda \mid gz = z\}$, dann gilt

3.) $\Theta_\Gamma \equiv \Theta_\Lambda \bmod p$

4.) Aus (i) und $(p, \det\Lambda) = (\det\Gamma, \det\Lambda) = 1$ folgt (iii).

Beweis

Ist G die von g erzeugte zyklische Gruppe, so operiert G auf Λ^*/Λ und Λ^*/Λ zerfällt unter dieser Operation in Bahnen; wegen i) und iii) enthält die Bahn eines jeden von 0 verschiedenen Elements von Λ^*/Λ genau p Elemente, d.h. es existiert eine Zerlegung der Gestalt:

$$\textcircled{1} \quad \Lambda^*/\Lambda = \{0\} + \sum_{\bar{z} \in \mathfrak{L}} G\bar{z}, \quad |G\bar{z}| = p \text{ für } \bar{z} \neq 0.$$

Wir haben ferner zunächst

$$\textcircled{2} \quad \det \Lambda \equiv 1 \bmod p,$$

und mit Satz 2 folgt, daß $D(A) \in GL_d R$.

Aus ①, Satz 6 und dem Lemma folgt weiter für $A, B \in SL_2\mathbb{Z}$:

$$D(AB)|_{0,0} \equiv \pm \sum_{\bar{z} \in \Lambda^*/\Lambda} D(A)|_{0,\bar{z}}\, D(B)|_{\bar{z},0}$$

$$\equiv \pm D(A)|_{0,0}\, D(B)|_{0,0} \bmod p,$$

d.h.

$$\textcircled{3} \quad A \longmapsto D(A)|_{0,0} \text{ induziert einen Homomorphismus}$$

$$\chi : SL_2\mathbb{Z} \longrightarrow (R/pR)^*/\{\pm 1\},$$

wo $(R/pR)^*$ für die Gruppe der Einheiten von R/pR steht. Es ist aber $\chi\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) = 1$, und die $SL_2\mathbb{Z}/K(SL_2\mathbb{Z})$ — wo $K(SL_2\mathbb{Z})$ für die Kommutatorgruppe von $SL_2\mathbb{Z}$ steht — von $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} K(SL_2\mathbb{Z})$ erzeugt wird, folgt $\chi(A) = 1$ für alle $A \in \mathbb{Z}$, d.h.

$$D(A)|_{0,0} \equiv \pm 1 \bmod p \text{ für } A \in SL_2\mathbb{Z}.$$

Im besonderen ist daher

$$1 \equiv D\left(\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\right)^2_{0,0} \equiv e^{-\pi i \frac{\operatorname{rang} \Lambda}{2}} \bmod p$$

wovon

④ $\quad \operatorname{rang} \Lambda \equiv 0 \mod 4$

folgt.

Daher kann man in ③ $(R/pR)^*/\{\pm 1\}$ durch $(R/pR)^*$ ersetzen, und mit der gleichen Argumentation wie eben folgt

⑤ $\quad D(A)|_{0,0} \equiv +1 \mod p$ für $A \in Sl_2 \mathbb{Z}$,

ins besondere mit Satz 6 noch

⑥ $\quad D(A)|_{0,0} = +1$ für $A \in \Gamma_0(5)$.

Damit ist Teil 1.) des Satzes evident.

Zum Beweis von Teil 2) ~~schreibe~~ hat man nach einander mit ①, dem Lemma und ⑥:

$$\begin{aligned}
\Theta_\Lambda|_A &= \sum_{\bar{z} \in \Lambda^*/\Lambda} D(A)|_{0,\bar{z}} \; \Theta_{\bar{z}} \\
&= D(A)|_{0,0} \; \Theta_\Lambda + \sum_{\bar{z} \in \mathcal{L}} \sum_{h \in G} D(A)|_{0,h\bar{z}} \; \Theta_{h\bar{z}} \\
&= D(A)|_{0,0} \; \Theta_\Lambda + p \sum_{\bar{z} \in \mathcal{L}} D(A)|_{0,\bar{z}} \; \Theta_{\bar{z}} \\
&\equiv \Theta_\Lambda \mod p .
\end{aligned}$$

Der Zusatz 3.) folgt aus der Tatsache, daß G auf $\Lambda_n = \{z \in \Lambda \mid n = z^2/2\}$ für jede Zahl n operiert; aus der Zerlegung in Bahnen folgt unmittelbar die Behauptung.

Zum Beweis von 4.) sei $\Gamma' = \{z \in \Lambda^* \mid gz = z\}$; wir zeigen zunächst $\Gamma = \Gamma'$:

Ist $V_1 \subseteq V$ der von Γ erzeugte $\mathbb{Q}$-Vektorraum, so bilde man $\Gamma^* \subseteq V_1$; ist nun $z \in \Gamma'$, d.h. $gz = z$, so ist auch $gsz = sz$ und $sz \in \Lambda$, also $sz \in \Gamma$, also $z \in V_1$, also $z \in \Gamma^*$; also $\Gamma' \subseteq \Gamma^*$.

Da aber ist $|\Gamma'/\Gamma|$ ein Teiler von $\det\Gamma$, ~~$= 1$ oder $= p$, der zweite Fall ist aber unmöglich~~ und ν die kanonische Abbildung $\Gamma'/\Gamma \to \Lambda^\vee/\Lambda$ eine Injektion ist, und $(\det\Gamma, \det\Lambda) = 1$ gilt; folgt $|\Gamma'/\Gamma| = 1$.

Ist nun $g\xi \equiv \xi \bmod \Lambda$ für ein $\xi \in \Lambda^\vee$, so ist $\sum_{i=1}^{p} g^i\xi \equiv p\xi \bmod \Lambda$; aber $\sum_{i=1}^{p} g^i\xi \in \Gamma' = \Gamma$, daher $p\xi \in \Lambda$; da $(p, \det\Lambda) = 1$ zieht $p\xi \in \Lambda$ aber $\xi \in \Lambda$ nach sich. □

Anwendung

Sei $[a, b, c]$ eine positiv-definite quadratische Form der Diskriminante $-p$, $(a, p) = 1$.

Sei

$$\Lambda = \left\{ \frac{1}{\sqrt{2a}} (x_1, \dots, x_{p+1}) \in \frac{1}{\sqrt{2a}} \mathbb{Z}^{p+1} \;\middle|\; \frac{x_1}{i} \equiv x_2 \equiv \dots \equiv x_{p+1} \bmod 2a \right\} \subset \mathbb{Q}^{p+1},$$

wo $\mathbb{Q}^{p+1}$ mit dem „üblichen" Skalarprodukt versehen sei.

Es ist dann

$$\Lambda^\vee = \left\{ \frac{1}{\sqrt{2a}} (x_1, \dots, x_{p+1}) \in \frac{1}{\sqrt{2a}} \mathbb{Z}^{p+1} \;\middle|\; b x_1 + x_2 + \dots + x_{p+1} \equiv 0 \bmod 2a \right\},$$

$\det\Lambda = (2a)^{p-1}$, Stufe von $\Lambda = 2a$.

Sei $g \in \mathcal{O}(\mathbb{Q}^{p+1})$ folgendermaßen definiert:

$$g(x_1, \dots, x_{p+1}) = (x_1, x_{p+1}, x_2, x_3, \dots, x_p);$$

dann ist g ein Automorphismus von Λ mit

(i) Ordnung von $g = p$,

und

(ii) $$[SL_2\mathbb{Z} : \Gamma_0(2a)] = 2a \prod_{\substack{\ell \mid 2a \\ \ell \text{ Primz}}} \left(1 + \frac{1}{\ell}\right) \not\equiv 0 \bmod p \text{ falls } p > 3;$$

wäre nun $\ell \mid 2a$ für eine Primzahl $\ell \mid 2a$: $\ell \equiv -1 \bmod p$, so ist wegen $p > 3$ ℓ ungerade, und so:

$$-1 = \left(\frac{-1}{p}\right) = \left(\frac{\ell}{p}\right) = (-1)^{\frac{\ell-1}{2}}\left(\frac{p}{\ell}\right) = \left(\frac{-p}{\ell}\right) = +1,$$

was ein Widerspruch ist. ($-p = b^2 - 4ac$, d.h. $-p$ quadratischer Rest mod ℓ !)

Schließlich ist

$$\Gamma := \{\gamma \in \Lambda \mid g\gamma = \gamma\} = \left\{\frac{1}{\sqrt{2a}}(x, y, \dots, y) \in \frac{1}{\sqrt{2a}}\mathbb{Z}^{p+1} \;\middle|\; x \equiv by \bmod 2a\right\},$$

durch

$$\det \Gamma = \begin{vmatrix} 2a & b \\ b & 2c \end{vmatrix} = p;$$

mit dem Zusatz b) folgt durch

(ccc) $\quad g - 1$ induziert einen Automorphismus von $\Lambda^\vee/\Lambda$.

Nach dem Satz existiert dann eine Modulform f zur $Sl_2\mathbb{Z}$ vom Gewicht $\frac{p+1}{2}$ mit p-ganzen Koeffizienten, sodaß

$$\Theta_{[a,b,c]} \equiv f \bmod p.$$

Da der Vektorraum der Modulformen von $Sl_2\mathbb{Z}$ vom Gewicht $\frac{p+1}{2}$ eine Basis von Funktionen mit Fourierkoeffizienten in $\mathbb{Z}$ besitzt, folgt leicht, daß f eine Modulform mit ~~Fourier~~ ganz-rationalen Fourierkoeffizienten gewählt werden kann.