Comment. Math. Helvetici 39(51) 465-489 Birkhäuser Verlag, Basel

Die irreduziblen Darstellungen der Gruppen $SL_2(Z_p)$, insbesondere $SL_2(Z_2)$. I. Teil

ALEXANDRE NOBS[1]

Das Ziel dieser Arbeit ist eine vollständige Beschreibung der stetigen irreduziblen Darstellungen der Gruppen $\mathbf{SL}_2(\mathbf{Z}_p)$, wo $\mathbf{Z}_p$ der Ring der p-adischen ganzen Zahlen, und p eine beliebige Primzahl (insbesondere auch $p=2$) bezeichnen. Die Gruppen $\mathbf{SL}_2(\mathbf{Z}_p)$ sind kompakt und total unzusammenhängend. Jede stetige irreduzible Darstellung von $\mathbf{SL}_2(\mathbf{Z}_p)$ ist deshalb von endlichem Grad und lässt sich über $\mathbf{SL}_2(\mathbf{Z}/p^\lambda\mathbf{Z})$, für eine geeignete positive ganze Zahl λ, faktorisieren. Es genügt also, die irreduziblen Darstellungen der endlichen Gruppen $\mathbf{SL}_2(\mathbf{Z}/p^\lambda\mathbf{Z})$ für alle λ zu beschreiben. Eine Zusammenfassung dieser Arbeit findet man in [5] und [6] (für $p=2$).

Die Arbeiten von Kloosterman [2] und Tanaka [10], [11] ergeben zusammen eine vollständige Lösung unseres Problems im Fall $p\neq 2$; wir nehmen diesen Fall aber auch auf, da die hier verwendeten Methoden (siehe Teil I, §3 und Teil II, §1) den zweiten Teil der Arbeit von Kloosterman wesentlich vereinfachen (den ersten Teil haben J. Wolfart und ich in [4] vereinfacht und vervollständigt). Der Fall $p\neq 2$ ist neuerdings mit einer anderen Methode auch von Kutzko [3] vollständig gelöst worden.

Ueber den Fall $p=2$ ist in der bisherigen Literatur sehr viel weniger bekannt. Casselman [1] hat gewisse irreduzible Darstellungen der allgemeineren Gruppen $\mathbf{SL}_2(k)$ bzw. $\mathbf{SL}_2(\mathfrak{O}_k)$ konstruiert, wobei k ein nicht-archimedischer lokal kompakter Körper ist mit beliebiger Restklassenkörpercharakteristik, und $\mathfrak{O}_k$ der zugehörige Ring der ganzen Zahlen. Er erhält somit gewisse irreduzible Darstellungen der Gruppen $\mathbf{SL}_2(\mathbf{Z}/2^\lambda\mathbf{Z})$, nämlich diejenigen, die man mit primitiven Chakteren (s. Definition in Teil II, §1) aus der unverzweigten Weilschen Darstellung und aus den verzweigten Weilschen Darstellungen mit $\sigma=0$ oder 1 erhält (s. Teil II, Satz 2, Satz 3 und §9). Selbst wenn man die irreduziblen Darstellungen der zerlegten Reihe (principal series) und diejenigen, die man mit primitiven Charakteren aus den übrigen verzweigten Weilschen Darstellungen (also $\sigma>1$) erhält, hinzufügt, fehlen immer noch unendlich viele, nämlich diejenigen, die man nur mit nicht-primitiven Charakteren konstruieren kann (s. Teil II, §6 und §9), sowie die sogenannten Ausnahmedarstellungen (s. Teil II, §9).

[1] Unterstützt durch den Schweizerischen Nationalfonds (820.167.73).

In der vorliegenden Arbeit findet man für beliebige Primzahlen p und beliebige λ eine Klassifikation und Beschreibung aller irreduziblen Darstellungen von $\mathbf{SL}_2(\mathbf{Z}/p^\lambda\mathbf{Z})$. Wir geben auch jeweils den Grad und, für feste λ und p, die Anzahl der irreduziblen Darstellungen an. Im ersten Teil wird zuerst gezeigt, wie man, ausgehend von gewissen quadratischen Formen auf endlichen $\mathbf{Z}/p^\lambda\mathbf{Z}$-Moduln, mit der Methode von A. Weil [12] Darstellungen von $\mathbf{SL}_2(\mathbf{Z}/p^\lambda\mathbf{Z})$ konstruiert (§1, Satz 2). Die verwendeten quadratischen Formen werden vollständig klassifiziert (§2). Im dritten Paragraphen werden zwei Methoden beschrieben, mit denen man Unterdarstellungen der konstruierten Darstellungen finden kann. Die Anzahl der Konjugiertenklassen von $\mathbf{SL}_2(\mathbf{Z}/p^\lambda\mathbf{Z})$, d.h. die Anzahl der irreduziblen Darstellungen von $\mathbf{SL}_2(\mathbf{Z}/p^\lambda\mathbf{Z})$, wird im vierten Paragraphen berechnet. Entsprechende Betrachtungen sind für $p \neq 2$ von Kloosterman [2] durchgeführt worden. Im zweiten Teil (in Zusammenarbeit mit J. Wolfart), werden die Weilschen Darstellungen vollständig reduziert. Die Ausnahmedarstellungen, d.h. die irreduziblen Darstellungen, die nicht in den Weilschen Darstellungen vorkommen, werden durch Tensorprodukte konstruiert.

Ich möchte an dieser Stelle den Herren P. Cartier und J. Wolfart für Ihre wertvollen Hinweise und Bemerkungen, sowie dem "Institut des Hautes Etudes Scientifiques" in Bures-sur-Yvette für seine Gastfreundschaft herzlich danken.

1. Weilsche Darstellungen der Gruppen $\mathbf{SL}_2(A_\lambda)$.

Es sei p eine feste Primzahl und λ eine natürliche Zahl. Wir bezeichnen mit A_λ den Ring $\mathbf{Z}/p^\lambda\mathbf{Z}$. Die Methode von A. Weil (etwas vereinfacht), Darstellungen von $\mathbf{SL}_2(A_\lambda)$ zu konstruieren, beruht auf dem folgenden Struktursatz:

SATZ 1.[2] *Die Gruppe* $\mathbf{SL}_2(A_\lambda)$ *wird erzeugt von den Elementen*

$$u(b)=\begin{pmatrix}1 & b\\ 0 & 1\end{pmatrix}(b\in A_\lambda),\qquad h(a)=\begin{pmatrix}a & 0\\ 0 & a^{-1}\end{pmatrix}(a\in A_\lambda^\times)\quad \textit{und}\quad w=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}$$

und den Relationen:

$$\left.\begin{aligned}
&\text{a) } u(b_1)u(b_2)=u(b_1+b_2),\\
&\text{b) } h(a_1)h(a_2)=h(a_1a_2),\\
&\text{c) } h(a)u(b)=u(a^2b)h(a),\\
&\text{d) } h(a)w=wh(a^{-1}),\\
&\text{e) } w^2=h(-1),\\
&\text{f) } wu(a)w=u(-a^{-1})wu(-a)h(-a),
\end{aligned}\right\}\qquad (1)$$

für alle $b,\ b_1,\ b_2\in A_\lambda$ *und* $a,\ a_1,\ a_2\in A_\lambda^\times$.

[2] Siehe P. Cartier: Séminaire de théorie des groupes (1972/3), I.H.E.S. Bures-sur-Yvette.

Sei M eine additiv geschriebene abelsche Gruppe. Eine quadratische Form Q auf M ist eine Abbildung von M nach $\mathbf{Q}/\mathbf{Z}$, welche folgenden Bedingungen genügt:

a) $Q(-x) = Q(x)$ für alle $x \in M$,

b) $B(x, y) := Q(x+y) - Q(x) - Q(y)$ definiert eine $\mathbf{Z}$-bilineare Abbildung von $M \times M$ nach $\mathbf{Q}/\mathbf{Z}$.

B heisst *die zu Q gehörige Bilinearform.* Q heisst *nicht-entartet,* wenn B *nicht-entartet* ist, d.h. wenn für jedes $x \neq 0$ aus M ein $y \in M$ mit $B(x, y) \neq 0$ existiert.

Um Darstellungen von $\mathbf{SL}_2(A_\lambda)$ zu erhalten, betrachten wir endliche A_λ-Moduln M und quadratische Formen Q auf M mit Werten in $p^{-\lambda}\mathbf{Z}/\mathbf{Z} \subset \mathbf{Q}/\mathbf{Z}$. Die zugehörigen Bilinearformen B sind dann A_λ-bilinear: Es genügt, die Multiplikation $\bar{a} \cdot r$ für $\bar{a} \in A_\lambda$ und $r \in p^{-\lambda}\mathbf{Z}/\mathbf{Z}$ durch $a \cdot r$ in $\mathbf{Q}/\mathbf{Z}$ zu definieren, wo a ein Repräsentant von $\bar{a}$ in $\mathbf{Z}$ ist. Wir werden im folgenden, dort wo keine Verwechslungen möglich sind, die Klassen von A_λ und ihre Repräsentanten in $\mathbf{Z}$ nicht mehr unterscheiden.

Unter diesen Voraussetzungen sei V der Raum $\mathbf{C}^M$ der komplexwertigen Funktionen auf M. Wir nennen das Paar (M, Q) einen *quadratischen Modul.*

SATZ 2. *Die durch*

$$\left.\begin{aligned} &\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} f(x) = \mathbf{e}(bQ(x)) \cdot f(x), \quad \textit{für alle} \quad b \in A_\lambda, \\ &\begin{bmatrix} a & 0 \\ 0 & a^{-1} \end{bmatrix} f(x) = \Lambda(a) \cdot f(ax), \quad \textit{für alle} \quad a \in A_\lambda^\times, \\ &\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} f(x) = S_Q(-1)\,|M|^{-1/2} \sum_{y \in M} \mathbf{e}(B(x, y)) \cdot f(y), \end{aligned}\right\} \tag{2}$$

für alle $f \in V$ und alle $x \in M$ gegebene Operation der Erzeugenden von $\mathbf{SL}_2(A_\lambda)$ auf V mit

$$S_Q(a) = |M|^{-1/2} \sum_{x \in M} \mathbf{e}(-aQ(x)) \tag{3}$$

und

$$\Lambda(a) = S_Q(a) S_Q(1)^{-1} \tag{4}$$

definiert genau dann eine Darstellung von $\mathbf{SL}_2(A_\lambda)$, *wenn*

$$\Lambda(a_1a_2)=\Lambda(a_1)\Lambda(a_2) \quad \textit{für alle} \quad a_1, a_2\in A_\lambda^\times \tag{5}$$

gültig ist oder, was dazu äquivalent ist,

$$S_Q(a_1)S_Q(a_2)=S_Q(1)S_Q(a_1a_2) \quad \textit{für alle} \quad a_1, a_2\in A_\lambda^\times. \tag{5'}$$

(*Mit* $\mathbf{e}$ *bezeichnen wir den Homomorphismus von* $\mathbf{Q}/\mathbf{Z}$ *in* $\mathbf{C}^\times$, *der die Klasse* mod 1 *von* t *in* $\mathbf{e}^{2\pi it}$ *abbildet.*)

Zum Beweis von Satz 2 muss man zeigen, dass die Operatoren [ ] mit den Relationen (1) genau dann verträglich sind, wenn (5) bzw. (5') gilt. Für die erste Relation ist

$$\begin{bmatrix}1 & b_1\\ 0 & 1\end{bmatrix}\begin{bmatrix}1 & b_2\\ 0 & 1\end{bmatrix}=\begin{bmatrix}1 & b_1+b_2\\ 0 & 1\end{bmatrix} \quad \text{wegen} \quad \mathbf{e}(b_1Q(x))\cdot\mathbf{e}(b_2Q(x)) = \mathbf{e}((b_1+b_2)Q(x))$$

immer erfüllt. Die Relationen (1.b) gelten genau dann für die Operatoren [ ], wenn (5) richtig ist. Die Relationen (1.c) sind genau dann erfüllt, wenn für alle $b\in A_\lambda$ und $a\in A_\lambda^\times$ gilt:

$$\mathbf{e}(bQ(ax))=\mathbf{e}(a^2bQ(x));$$

dies folgt jedoch aus $Q(ax)=a^2Q(x)$ (Beweis durch Induktion über a).

Für den vierten Typ von Relationen erhalten wir

$$\begin{bmatrix}a & 0\\ 0 & a^{-1}\end{bmatrix}\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}f(x)=\Lambda(a)S_Q(-1)\,|M|^{-1/2}\sum_{y\in M}\mathbf{e}(B(ax,y))\cdot f(y),$$

$$\begin{bmatrix}0 & 1\\ -1 & 0\end{bmatrix}\begin{bmatrix}a^{-1} & 0\\ 0 & a\end{bmatrix}f(x)=\Lambda(a^{-1})S_Q(-1)\,|M|^{-1/2}\sum_{y'\in M}\mathbf{e}(B(x,y'))\cdot f(a^{-1}y'),$$

und die Substitution $y=a^{-1}y'$ in der zweiten Summe zeigt, dass hier $\Lambda(a)=\Lambda(a^{-1})$ für alle $a\in A_\lambda^\times$ nachzuweisen ist. Nach (4) und (3) ist dies jedoch klar, denn es ist

$$\sum_{x\in M}\mathbf{e}(-aQ(x))=\sum_{x\in M}\mathbf{e}(-a^{-1}Q(ax))=\sum_{y\in M}\mathbf{e}(-a^{-1}Q(y)).$$

Die fünfte Relation ist erfüllt, wenn

$$S_Q(-1)^2 |M|^{-1} \sum_{y,z \in M} \mathbf{e}(B(x+z, y)) \cdot f(z) = \Lambda(-1) \cdot f(-x) \tag{6}$$

ist. Da B nicht-entartet ist, hat man

$$\sum_{y \in M} \mathbf{e}(B(u, y)) = \begin{cases} |M|, & \text{wenn} \quad u = 0 \\ 0 & \text{andernfalls,} \end{cases}$$

was den Nachweis von (6) zurückführt auf.den Beweis von

$$S_Q(-1)^2 = \Lambda(-1) = S_Q(-1) S_Q(1)^{-1} \quad \text{oder} \quad S_Q(-1) \cdot S_Q(1) = 1,$$

und dies ist eine wohlbekannte Eigenschaft der Gausschen Summen.

Die Relationen (1.f) behandelt man folgendermassen:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} f(x)$$

$$= S_Q(-1)^2 |M|^{-1} \sum_{z \in M} \left\{ \sum_{y \in M} \mathbf{e}(B(x, y) + aQ(y) + B(y, z)) \right\} \cdot \hat{f}(z)$$

$$= S_Q(-1)^2 S_Q(-a) |M|^{-1/2} \sum_{z \in M} \mathbf{e}(-aQ(a^{-1}x + a^{-1}z)) \cdot f(z),$$

wenn man dabei benutzt, dass

$$B(x, y) + aQ(y) + B(y, z) = a\{Q(a^{-1}x + a^{-1}z + y) - Q(a^{-1}x + a^{-1}z)\}$$

gilt. Andererseits hat man

$$\begin{bmatrix} 1 & -a^{-1} \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & -a \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -a & 0 \\ 0 & -a^{-1} \end{bmatrix} f(x)$$

$$= S_Q(-1) \Lambda(-a) \mathbf{e}(-a^{-1} Q(x)) |M|^{-1/2} \sum_{y \in M} \mathbf{e}(B(x, y)) \cdot \mathbf{e}(-aQ(y)) \cdot f(-ay)$$

und durch die Substitution $z = -ay$ ergibt sich daraus

$$= S_Q(-1)\Lambda(-a)\,|M|^{-1/2} \sum_{z \in M} \mathbf{e}(-a^{-1}\{Q(x)+B(x,z)+Q(z)\}) \cdot f(z)$$

$$= S_Q(-1)\Lambda(-a)\,|M|^{-1/2} \sum_{z \in M} \mathbf{e}(-aQ(a^{-1}x+a^{-1}z)) \cdot f(z).$$

Nun zeigt (4), dass beide Ergebnisse gleich sind; damit ist Satz 2 bewiesen.

DEFINITION 1. Wenn (5) erfüllt ist, wollen wir mit $W(M, Q)$ die Darstellung bezeichnen, welche durch Satz 2 dem quadratischen Modul (M, Q) zugeordnet wird. Sie heisst die zu (M, Q) gehörige Weilsche Darstellung.

DEFINITION 2. Eine Darstellung von $\mathbf{SL}_2(\mathbf{Z}_p)$ heisst von der Stufe λ, wenn sie sich über $\mathbf{SL}_2(A_\lambda)$, aber nicht über $\mathbf{SL}_2(A_{\lambda-1})$ faktorisieren lässt. Analog heisst eine Darstellung von $\mathbf{SL}_2(A_\mu)$ von der Stufe λ, wenn sie sich über $\mathbf{SL}_2(A_\lambda)$, aber nicht über $\mathbf{SL}_2(A_{\lambda-1})$ faktorisieren lässt $(\mu \geq \lambda)$.

Um alle irreduziblen Darstellungen von $\mathbf{SL}_2(\mathbf{Z}_p)$ zu beschreiben, genügt es, für alle λ die irreduziblen Darstellungen der Stufe λ von $\mathbf{SL}_2(A_\lambda)$ zu beschreiben. Der Kern der Projektion von $\mathbf{SL}_2(A_\lambda)$ auf $\mathbf{SL}_2(A_{\lambda-1})$ ist die invariante Untergruppe von $\mathbf{SL}_2(A_\lambda)$, die von den Elementen $u(p^{\lambda-1}b)$, mit $b \in A_1$, erzeugt wird. Wenn die Werte von Q auf M in $p^{-\lambda+1}\mathbf{Z}/\mathbf{Z}$ liegen, dann ist der Operator $[u(p^{\lambda-1}b)]$ gleich der Identität für die Darstellung $W(M, Q)$ (siehe (2)), d.h. $W(M, Q)$ ist höchstens von der Stufe $\lambda - 1$. Deshalb setzen wir jetzt für ein fest gewähltes λ voraus, dass die Werte von Q auf M in $p^{-\lambda}\mathbf{Z}/\mathbf{Z}$ und nicht alle in $p^{-\lambda+1}\mathbf{Z}/\mathbf{Z}$ liegen. Die Darstellung $W(M, Q)$ ist dann von der Stufe λ.

Erfüllt der quadratische Modul (M_1, Q_1) die Bedingung (5), und ist (M_2, Q_2) zu (M_1, Q_1) äquivalent (d.h. gibt es einen Isomorphismus φ von M_1 auf M_2, sodass $Q_2 \circ \varphi = Q_1$), so erfüllt auch (M_2, Q_2) die Bedingung (5) und die Weilschen Darstellungen $W(M_1, Q_1)$ und $W(M_2, Q_2)$ sind isomorph.

2. Klassifikation Quadratischer Moduln und Weilscher Darstellungen.

Wir wollen in diesem Paragraphen die Klassen äquivalenter quadratischer Moduln klassifizieren. Die Resultate sind für $p \neq 2$ schon bekannt [11], werden aber vollständigkeitshalber wiederholt.

Wir beweisen zunächst folgendes

LEMMA 0. *Seien s und d feste Elemente aus* A_λ. *Die Menge*

$$S(s,d)=\{a\in A_\lambda^\times \mid \exists(\xi,\eta)\in A_\lambda\times A_\lambda \quad mit \quad \xi^2+s\xi\eta+d\eta^2=a\}$$

ist eine Untergruppe von $A_\lambda^\times$. *Die genaue Beschreibung von* $S(s,d)$ *entnimmt man aus der Tabelle* 1.

Dass die Menge $S(s,d)$ eine Untergruppe von $A_\lambda^\times$ ist, folgt sofort aus der Tatsache, dass

$$\xi^2+s\xi\eta+d\eta^2=\det\left(\xi E+\eta\begin{pmatrix}s & d\\ -1 & 0\end{pmatrix}\right).$$

Sei zunächst $p\neq 2$. Es ist leicht zu zeigen, dass

$$A_\lambda^\times\supset S(s,d)\supset (A_\lambda^\times)^2\supset 1+pA_\lambda.$$

Auf der anderen Seite nimmt die quadratische Form $\xi^2+s\xi\eta+d\eta^2$ jeden Wert aus $A_\lambda^\times$ an, ausser wenn ihre Diskriminante $\Delta=s^2-4d$ kongruent null ist mod p. In diesem Fall stellt sie nur Quadrate dar (siehe etwa H. Hasse: Vorlesung über Zahlentheorie, 2. Auf., Springer-Verlag, §10.4). Damit ist die Richtigkeit der Tabelle 1 für $p\neq 2$ bewiesen.

Tabelle 1

	Bedingungen für s, d		λ	$S(s,d)$	$[A_\lambda^\times:S(s,d)]$
$p\neq 2$	$\Delta=s^2-4d\equiv 0 \bmod p$		$\lambda\geq 1$	$\left\{a\in A_\lambda^\times \mid \left(\frac{a}{p}\right)=1\right\}$	2
	$\Delta=s^2-4d\not\equiv 0 \bmod p$			$A_\lambda^\times$	1
$p=2$	$s\equiv 1 \bmod 2$		$\lambda\geq 1$	$A_\lambda^\times$	1
	$s=2s'$	$s'^2-d\equiv 0 \mod 8$	$\lambda\geq 3$	$\{a\in A_\lambda^\times \mid a\equiv 1 \mod 8\}$	4
		$s'^2-d\equiv 3,4,7 \mod 8$		$\{a\in A_\lambda^\times \mid a\equiv 1,5 \mod 8\}$	2
		$s'^2-d\equiv 2 \mod 8$		$\{a\in A_\lambda^\times \mid a\equiv 1,7 \mod 8\}$	2
		$s'^2-d\equiv 6 \mod 8$		$\{a\in A_\lambda^\times \mid a\equiv 1,3 \mod 8\}$	2
		$s'^2-d\equiv 1,5 \mod 8$		$\{a\in A_\lambda^\times \mid a\equiv 1,3,5,7 \mod 8\}$	1
		$s'^2-d\equiv 0,3 \mod 4$	$\lambda=2$	$\{a\in A_\lambda^\times \mid a\equiv 1 \mod 4\}$	2
		$s'^2-d\equiv 1,2 \mod 4$		$\{a\in A_\lambda^\times \mid a\equiv 1,3 \mod 4\}$	1
		$s'=0$	$\lambda=1$	$A_\lambda^\times$	1

Sei jetzt $p=2$ und $\lambda \geq 3$. Es gilt

$$A_\lambda^\times \supset S(s,d) \supset (A_\lambda^\times)^2 = 1+8A_\lambda.$$

Um $S(s,d)$ vollständig zu beschreiben, genügt es, die ungeraden Zahlen mod 8, die von $\xi^2+s\xi\eta+d\eta^2$ dargestellt werden, anzugeben. Wir unterscheiden zwei Fälle:

1. Sei $s \equiv 1 \bmod 2$, dann stellt $\xi^2+s\xi\eta+d\eta^2$ alle ungeraden Zahlen mod 8 dar. Um dies einzusehen, genügt es, die Paare

$$(\xi,\eta) = \begin{cases} (1,1),(3,1),(5,1),(7,1) & \text{falls} \quad d \equiv 1 \bmod 2 \\ (1,0),(1,2),(1,4),(3,2) & \text{falls} \quad d \equiv 0 \bmod 2, \end{cases}$$

zu betrachten.

2. Sei $s=2s'$, dann gilt

$$\xi^2+s\xi\eta+d\eta^2 = (\xi+s'\eta)^2-(s'^2-d)\eta^2,$$

und es ist eine leichte Aufgabe, die ungeraden Zahlen mod 8, die durch diese quadratische Form dargestellt werden, in Abhängigkeit von (s'^2-d) zu bestimmen.

Die Fälle $\lambda=2$ und $\lambda=1$ lassen sich ohne Schwierigkeit von den Resultaten für $\lambda \geq 3$ ableiten. Damit ist Lemma 0 bewiesen.

Wir nehmen zuerst an, dass M von einem einzigen Element erzeugt wird. Die einzigen quadratischen A_λ-Moduln (M,Q), welche für die Erzeugung von Darstellungen der Stufe λ von $\mathbf{SL}_2(A_\lambda)$ in Frage kommen, sind dann

$$\left.\begin{array}{llll} M=A_\lambda, & Q(x)=p^{-\lambda}rx^2, & r \not\equiv 0 \bmod p, \text{ falls } p \neq 2, & \lambda \geq 1, \\ M=A_{\lambda-1}, & Q(x)=2^{-\lambda}rx^2, & r \equiv 1 \bmod 2, \text{ falls } p=2, & \lambda \geq 2. \end{array}\right\} \tag{7}$$

Für $p \neq 2$ hat man zwei Klassen, gegeben durch die Werte des Legendre-Symbols $\left(\frac{r}{p}\right)$. Für $p=2$ und $\lambda \geq 3$ hat man vier Klassen, gegeben durch $r \equiv 1$, 3, 5 und 7 mod 8.

LEMMA 1. *Sei $p \neq 2$. Die quadratischen Moduln (M,Q) von (7) erfüllen die Bedingung (5) von Satz 2, erzeugen also Weilsche Darstellungen von $\mathbf{SL}_2(A_\lambda)$. Die Faktoren $\Lambda(a)$ und $S_Q(-1)$ lauten:*

$$\Lambda(a) = \left(\frac{a}{p}\right)^\lambda, \qquad S_Q(-1) = \begin{cases} 1 & \text{falls } \lambda \text{ gerade,} \\ \left(\frac{r}{p}\right)\varepsilon(p) & \text{falls } \lambda \text{ ungerade,} \end{cases}$$

wobei $\varepsilon(d)=1$ oder i ist, je nachdem ob $d \equiv 1$ oder $3 \bmod 4$ ist.

Zum Beweis verwendet man die Formeln in [7] (IV, §3).

LEMMA 2. *Sei* $p=2$. *Die quadratischen Moduln* (M, Q) *von* (7) *erfüllen die Bedingung* (5) *von Satz* 2 *nicht, erzeugen also keine Weilschen Darstellungen von* $\mathbf{SL}_2(A_\lambda)$.

Die Berechnung von $\Lambda(a)=S_Q(a)S_Q(1)^{-1}$ erfolgt durch

$$S_Q(a)=|A_{\lambda-1}|^{-1/2}\sum_{x\in A_{\lambda-1}}\mathbf{e}(-aQ(x))=2^{-(\lambda-1)/2}2^{-1}\sum_{x\in A_\lambda}\mathbf{e}(-2^{-\lambda}rax^2),$$

und folglich

$$S_Q(a)=-\frac{(1+i)}{\sqrt{2}}\left(\frac{-2^\lambda}{ar}\right)\varepsilon(-ar) \tag{8}$$

(s. [7], IV, §3), das Minuszeichen kommt daher, dass dabei $\left(\frac{m}{-n}\right)=(\text{sign m})\left(\frac{m}{n}\right)$ gesetzt wird. Der Quotient $S_Q(a)/S_Q(1)$ wird nun

$$\Lambda(a)=\left(\frac{-2^\lambda}{a}\right)\frac{\varepsilon(-ar)}{\varepsilon(-r)}=\left(\frac{-2^\lambda}{a}\right)i^{-r(\bar{a}^2-1)/8}$$

wo $\bar{a}$ der kleinste natürliche Rest von a mod 4 ist. Weiter ist

$$\frac{1}{2}\left[\frac{\bar{a}_1^2-1}{8}+\frac{\bar{a}_2^2-1}{8}-\frac{\overline{(a_1a_2)}^2-1}{8}\right]\equiv\frac{a_1-1}{2}\cdot\frac{a_2-1}{2}\bmod 2$$

für alle $a_1,\ a_2\in A_\lambda^\times$. Andererseits hat man für das Hilbertsymbol

$$(a_1, a_2)_2=(-1)^{[(a_1-1)/2][(a_2-1)/2]}\quad\text{(siehe [9], S. 39).}$$

Alles zusammen gibt uns die Beziehung

$$\Lambda(a_1a_2)=\Lambda(a_1)\Lambda(a_2)(a_1, a_2)_2,$$

und damit ist Lemma 2 bewiesen.

Sei jetzt M von genau zwei Elementen erzeugt (d.h. M/pM ist zweidimensional über $\mathbf{Z}/p\mathbf{Z}$), und Q eine quadratische Form auf M. Wir sagen dann, dass (M, Q) ein *binärer quadratischer Modul* ist.

SATZ 3. *Sei* $p \neq 2$. *Die folgenden quadratischen Moduln bilden ein Repräsentantensystem der Klassen der binären nicht-entarteten quadratischen Moduln mit Werten in* $p^{-\lambda}\mathbf{Z}/\mathbf{Z}$, *aber nicht nur in* $p^{-\lambda+1}\mathbf{Z}/\mathbf{Z}$:

$$\left.\begin{array}{lll} \text{a) } M = A_\lambda \oplus A_\lambda, & Q(x) = p^{-\lambda} x_1 x_2 & (\lambda \geq 1), \\ \text{b) } M = A_\lambda \oplus A_\lambda, & Q(x) = p^{-\lambda}(x_1^2 - u x_2^2)^{(3)} & (\lambda \geq 1), \\ \text{c) } M = A_\lambda \oplus A_{\lambda-\sigma}, & Q(x) = p^{-\lambda} r(x_1^2 + p^\sigma t x_2^2) & (\lambda \geq 2), \end{array}\right\} \tag{10}$$

wobei σ *die Menge* $\{1, 2, \ldots, \lambda - 1\}$ *durchläuft und* r, t *die Menge* $\{1, u\}$, *mit* $\left(\frac{u}{p}\right) = -1$.

Diese binären quadratischen Moduln erfüllen alle die Bedingung (5) *von Satz* 2. *Die Faktoren* $\Lambda(a)$ *und* $S_Q(-1)$ *lauten:*

$$\left.\begin{array}{ll} \text{a) } \Lambda(a) = 1, & S_Q(-1) = 1, \\ \text{b) } \Lambda(a) = 1, & S_Q(-1) = (-1)^\lambda, \\ \text{c) } \Lambda(a) = \left(\frac{a}{p}\right)^\sigma, & S_Q(-1) = \begin{cases} \left(\frac{r}{p}\right)\left(\frac{t}{p}\right)^{\lambda+1} \varepsilon(p) & \text{falls } \sigma \text{ ungerade,} \\ \left(\frac{-t}{p}\right)^\lambda & \text{falls } \sigma \text{ gerade.} \end{cases} \end{array}\right\} \tag{11}$$

Den Beweis von (10) kann man wie für $p = 2$ (siehe unten) vornehmen. Man verwendet dabei Lemma 0. Die Resultate stehen aber schon bei Tanaka [11].

Die (M, Q) in (10) lassen sich alle als direkte Summe $(M_1 \oplus M_2, Q_1 \oplus Q_2)$ schreiben, mit (M_i, Q_i) von der Form (7), daraus folgt sofort (11).

SATZ 4. *Sei* $p = 2$. *Die folgenden quadratischen Moduln bilden ein Repräsentantensystem der Klassen der binären nicht-entarteten quadratischen Moduln mit Werten in* $2^{-\lambda}\mathbf{Z}/\mathbf{Z}$, *aber nicht nur in* $2^{-\lambda+1}\mathbf{Z}/\mathbf{Z}$:

$$\left.\begin{array}{lll} \text{a) } M = A_\lambda \oplus A_\lambda, & Q(x) = 2^{-\lambda} x_1 x_2 & (\lambda \geqslant 1), \\ \text{b) } M = A_\lambda \oplus A_\lambda, & Q(x) = 2^{-\lambda}(x_1^2 + x_1 x_2 + x_2^2) & (\lambda \geqslant 1), \\ \text{c) } M = A_{\lambda-1} \oplus A_{\lambda-\sigma-1}, & Q(x) = 2^{-\lambda} r(x_1^2 + 2^\sigma t x_2^2) & (r, t \text{ ungerade}, \lambda \geqslant 2) \end{array}\right\} \tag{12}$$

wobei σ *die Menge* $\{0, 1, 2, \ldots, \lambda - 2\}$ *durchläuft, und die Paare* (r, t) *ein*

[3] Ist Ist äquivalent zu $Q(x) = p^{-\lambda}(x_1^2 + x_1 x_2 + [(1+t)/4]x_2^2)$, $t \equiv 3 \bmod 4$, $\left(\frac{-t}{p}\right) = -1$.

Repräsentantensystem der Klassen durchlaufen, die wie folgt definiert werden:

$$(r_1, t_1) \sim (r_2, t_2) \Leftrightarrow t_2 \equiv t_1 \bmod \operatorname{Min}(2^3, 2^{\lambda-\sigma})$$

und

$$\begin{cases} r_2 \equiv r_1 \quad \textit{oder} \quad r_1 t_1 \bmod 4, & \textit{falls} \quad \sigma = 0, \\ r_2 \equiv r_1 \quad \textit{oder} \quad r_1 + 2 r_1 t_1 \bmod 8, & \textit{falls} \quad \sigma = 1, \\ r_2 \equiv r_1 \bmod 4, & \textit{falls} \quad \sigma = 2, \\ r_2 \equiv r_1 \bmod 8, & \textit{falls} \quad \sigma \geq 3. \end{cases}$$

Diese binären quadratischen Moduln erfüllen alle die Bedingung (5) *von Satz* 2. *Die Faktoren* $\Lambda(d)$ *und* $S_Q(a)$ *lauten:*

$$\left.\begin{array}{ll} \text{a)}\ \Lambda(a) = 1, & S_Q(a) = 1, \\ \text{b)}\ \Lambda(a) = 1, & S_Q(a) = (-1)^{\lambda}, \\ \text{c)}\ \Lambda(a) = \left(\dfrac{2}{a}\right)^{\sigma} \left(\dfrac{-1}{a}\right)^{(t+1)/2}, & S_Q(a) = i \left(\dfrac{-1}{t}\right) \left(\dfrac{2}{t}\right)^{\lambda-\sigma} \left(\dfrac{2}{r}\right)^{\sigma} \left(\dfrac{2}{a}\right)^{\sigma} \varepsilon(-ar)\varepsilon(-art). \end{array}\right\} \tag{13}$$

Wir wollen den Beweis von Satz 4 in mehreren Etappen durchführen. Die allgemeinste Gestalt eines binären quadratischen A_λ-Moduls (M', Q') mit Werten in $2^{-\lambda}\mathbf{Z}/\mathbf{Z}$, aber nicht nur in $2^{-\lambda+1}\mathbf{Z}/\mathbf{Z}$, ist (bei Einführung von Koordinaten in M'):

$$M' = A_{\mu_1} \oplus A_{\mu_2}, \qquad Q'(x) = 2^{-\lambda}(r x_1^2 + s x_1 x_2 + t x_2^2) \quad \text{für} \quad x = (x_1, x_2) \in M'. \tag{14}$$

Die Koeffizienten r, s, t dürfen nicht alle gerade sein. Wir haben μ_1, μ_2 so zu wählen, dass (M', Q') ein nicht-entarteter quadratischer A_λ-Modul ist. Diese Wahl ist eindeutig und hängt von r, s, t ab. Wir müssen dann zeigen, dass (14) zu (12) a), b) oder c) äquivalent ist.

A. Sei $s \equiv 1 \bmod 2$. Es ist leicht zu sehen, dass für $\mu_1 = \mu_2 = \lambda$ die quadratische Form Q' auf M' nicht-entartet ist. Sei o.B.d.A. (ohne Beschränkung der Allgemeinheit) $r \equiv 1 \bmod 2$: Wenn nämlich $2 \mid r$, aber $2 \nmid t$ ist, vertausche man x_1 und x_2; wenn r und t beide gerade sind, ersetze man x_2 durch $x_1 + x_2$, um eine äquivalente quadratische Form der gewünschten Eigenschaft zu erhalten. Mit der Annahme $r \equiv 1 \bmod 2$ werden wir nun zeigen, dass Q' zu Q aus (12) a) bzw. aus (12) b) äquivalent ist, wenn $t \equiv 0$ bzw. $t \equiv 1 \bmod 2$ gilt.

Sei zunächst $r \equiv 1$, $s \equiv 1$, $t \equiv 0 \bmod 2$. Dann existiert ein isotroper Vektor $u \not\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \bmod 2$ in M'. Multipliziert man nämlich die Kongruenz

$$rx_1^2 + sx_1x_2 + tx_2^2 \equiv 0 \bmod 2^\lambda$$

mit $4r^{-1}$, so erhält man

$$(2x_1 + r^{-1}sx_2)^2 \equiv [(r^{-1}s)^2 - 4r^{-1}t]x_2^2 \bmod 2^{\lambda+2}.$$

Die rechte Seite ist kongruent 1 mod 8 für $x_2 = 1$, also existiert eine Lösung von $Q'(u) = 0$ (in $\mathbf{Q}/\mathbf{Z}$) mit $2^{\lambda-1}u \not\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Dazu gibt es ein $v \in M'$ mit $2^\lambda B'(u, v) \in A_\lambda^\times$ (B' ist die zu Q' gehörige Bilinearform), denn andernfalls würde $B'(2^{\lambda-1}u, y)$ für alle $y \in M'$ in $\mathbf{Q}/\mathbf{Z}$ verschwinden; das ist unmöglich, da $2^{\lambda-1}u \not\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ und B' nicht-entartet ist. O.B.d.A. darf man sogar $2^\lambda B'(u, v) = 1$ annehmen (Normierung von v). Die Elemente u und v bilden eine Basis von M': wäre nämlich $v \equiv \mu u \bmod 2$, so wäre auch

$$1 \equiv 2^\lambda B'(u, v) \equiv \mu 2^\lambda B'(u, u) \equiv 0 \bmod 2,$$

was unmöglich ist. Wenn $Q'(v) = 0$, dann hat man $Q'(\xi_1 u + \xi_2 v) = 2^{-\lambda}\xi_1\xi_2$, also ist Q' zu Q aus (12)a) äquivalent; andernfalls ersetze man v durch $v' = v - Q'(v)u$.

Sei nun $r \equiv 1$, $s \equiv 1$, $t \equiv 1 \bmod 2$. Hier existieren keine isotropen Vektoren v mit $v \not\equiv \begin{pmatrix} 0 \\ 0 \end{pmatrix} \bmod 2$, da $rx_1^2 + sx_1x_2 + tx_2^2$ stets ungerade ist, wenn x_1 und x_2 nicht beide gerade sind. Es existiert aber ein $u \in M'$ mit $2^\lambda Q'(u) \equiv 1 \bmod 2^\lambda$. Um dies einzusehen, multipliziert man

$$ru_1^2 + su_1u_2 + tu_2^2 \equiv 1 \bmod 2^\lambda$$

mit $4r^{-1}$ und erhält

$$(2u_1 + r^{-1}su_2)^2 \equiv 4r^{-1} + [(r^{-1}s)^2 - 4r^{-1}t]u_2^2 \bmod 2^{\lambda+2}.$$

Für $u_2 = 1$ gibt es eine Lösung u_1, denn die rechte Seite ist dann kongruent 1 mod 8. Zu diesem $u = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}$ existiert ausserdem ein $v = \begin{pmatrix} v_1 \\ v_2 \end{pmatrix} \in M'$ mit $2^\lambda Q'(v) \equiv 1$ und $2^\lambda B'(u, v) \equiv 1 \bmod 2^\lambda$. Mit anderen Worten: Es gibt eine Lösung der beiden

Kongruenzen

$$rv_1^2+sv_1v_2+tv_2^2\equiv 1 \bmod 2^\lambda,$$

$$2ru_1v_1+su_1v_2+su_2v_1+2tu_2v_2\equiv 1 \bmod 2^\lambda.$$

Dabei ist die zweite Kongruenz von der Form

$$av_1+bv_2\equiv 1 \bmod 2^\lambda,$$

wobei mindestens einer der Koeffizienten a, b invertierbar ist, denn u_1 und u_2 sind nicht beide gerade. O.B.d.A. sei $b\in A_\lambda^\times$ (andernfalls vertauscht man die Variablen); wenn man nun $v_2\equiv b^{-1}-b^{-1}av_1 \bmod 2^\lambda$ in die erste Kongruenz einsetzt, findet man

$$[r-b^{-1}as+(b^{-1}a)^2t]v_1^2+[sb^{-1}-2ab^{-2}t]v_1+tb^{-2}-1\equiv 0 \bmod 2^\lambda.$$

Die Koeffizienten von v_1^2 und v_1 sind ungerade, während das konstante Glied gerade ist. Die Lösbarkeit dieser Kongruenz zeigt man wie oben durch Multiplikation mit $4[r-b^{-1}as+(b^{-1}a)^2t]^{-1}$. Die Elemente u und v bilden eine Basis von M'. Man erhält also

$$Q'(\xi_1u+\xi_2v)=2^{-\lambda}(\xi_1^2+\xi_1\xi_2+\xi_2^2),$$

was die Aequivalenz von Q' und Q aus (12)b) beweist. (Man kann den zweiten Fall auch behandeln, indem man zeigt, dass sich Q' mittels der Norm der eindeutig bestimmten unverzweigten quadratischen Erweiterung von $\mathbf{Q}_2$ realisieren lässt; [7], S. 49, Prop. 9.)

B. Sei $s\equiv 0 \bmod 2$. Man darf dann o.B.d.A. $r\equiv 1 \bmod 2$ annehmen (andernfalls wäre $t\equiv 1 \bmod 2$ und man könnte die Variablen vertauschen). Die Transformation

$$x_1\to x_1-s'r^{-1}x_2, \qquad x_2\to x_2, \quad \text{mit} \quad s=2s',$$

zeigt, dass die quadratische Form Q' aus (14) in diesem Fall auf $M'=A_{\lambda-1}\oplus A_{\lambda-\sigma-1}$ nicht-entartet ist, und dass (M', Q') zu einem quadratischen Modul (M, Q) aus (12) c) äquivalent ist.

Die Automorphismen φ von $M=A_{\lambda-1}\oplus A_{\lambda-\sigma-1}$ lassen sich alle als

$$\left.\begin{aligned}&\varphi(x)=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}\begin{pmatrix}x_1\\ x_2\end{pmatrix} \quad \text{für alle} \quad x=\begin{pmatrix}x_1\\ x_2\end{pmatrix},\\ &\text{mit} \quad \alpha\in A_{\lambda-1},\ \beta\in 2^\sigma A_{\lambda-1},\ \gamma,\delta\in A_{\lambda-\sigma-1} \quad \text{und} \quad d=\alpha\delta-\beta\gamma\in A_{\lambda-\sigma-1}^\times,\end{aligned}\right\} \tag{15}$$

darstellen. Die quadratischen Formen

$$Q_1(x)=2^{-\lambda}r_1(x_1^2+2^{\sigma}t_1x_2^2), \qquad Q_2(x)=2^{-\lambda}r_2(x_1^2+2^{\sigma}t_2x_2^2)$$

sind genau dann äquivalent, wenn es einen Automorphismus φ von $M=A_{\lambda-1}\oplus A_{\lambda-\sigma-1}$ gibt mit $Q_1\circ\varphi=Q_2$, d.h. wenn es eine Matrix $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ von der Form (15) gibt mit

$$\left.\begin{aligned}
&\text{a) } r_1(\alpha^2+2^{\sigma}t_1\gamma^2)\equiv r_2 \bmod 2^{\lambda},\\
&\text{b) } \alpha\beta+2^{\sigma}t_1\gamma\delta\equiv 0 \bmod 2^{\lambda-1},\\
&\text{c) } r_1(\beta^2+2^{\sigma}t_1\delta^2)\equiv 2^{\sigma}r_2t_2 \bmod 2^{\lambda},\\
&\text{d) } \alpha\delta-\beta\gamma\equiv d \bmod 2^{\lambda-\sigma-1}.
\end{aligned}\right\} \tag{16}$$

Dieses Kongruenzensystem für α, β, γ, δ und d ist äquivalent zu:

$$\left.\begin{aligned}
&\text{a) } r_1(\alpha^2+2^{\sigma}t_1\gamma^2)\equiv r_2 \bmod 2^{\lambda},\\
&\text{b) } r_1^2t_1d^2\equiv r_2^2t_2 \bmod 2^{\lambda-\sigma},\\
&\text{c) } r_2\beta\equiv -2^{\sigma}t_1r_1\gamma d \bmod 2^{\lambda-1},\\
&\text{d) } r_2\delta\equiv r_1\alpha d \bmod 2^{\lambda-\sigma-1}.
\end{aligned}\right\} \tag{17}$$

Dass (16) aus (17) folgt, lässt sich ohne Schwierigkeiten nachrechnen. Umgekehrt, quadriert man (16.b) und multipliziert man (16.a) mit (16.c), so erhält man mit (16.d) die Kongruenz (17.b). Multipliziert man (16.a) mit β (bzw. (16.c) mit α) und (16.b) mit α (bzw. β), so erhält man (17.c) (bzw. (17.d)).

Aus (17) sieht man jetzt, dass Q_1 und Q_2 genau dann äquivalent sind, wenn

$$\left.\begin{aligned}
&\text{a) } t_1\equiv t_2 \bmod \operatorname{Min}(2^3, 2^{\lambda-\sigma}),\\
&\text{b) } \exists\alpha\in A_{\lambda-1}, \qquad \gamma\in A_{\lambda-\sigma-1} \quad \text{mit} \quad \alpha^2+2^{\sigma}t_1\gamma^2\equiv r_2r_1^{-1} \bmod 2^{\lambda}.
\end{aligned}\right\} \tag{18}$$

Sind nämlich (18.a) und (18.b) erfüllt, so lassen sich β und δ aus (17.c) und (17.d) berechnen und es gilt (16.d).

Die Lösbarkeit von (18.b) entnimmt man aus Lemma 0, bzw. Tabelle 1.

Es bleiben die Faktoren $\Lambda(a)$ und $S_Q(a)$ zu bestimmen. Für (12)a) erhält man

$$S_Q(a)=|M|^{-1/2}\sum_{x_1,x_2\in A_{\lambda}}\mathbf{e}(-2^{-\lambda}ax_1x_2)=2^{-\lambda}\sum_{x_1\in A_{\lambda}}\delta_0(x_1)2^{\lambda}=1.$$

Mit den Bezeichnungen $F=\begin{pmatrix}2 & 1\\ 1 & 2\end{pmatrix}$, $q=\Delta=3$, folgt aus [4] (§2, (5)), für (12)b):

$$S_Q(a)=2^{-\lambda}G_F(-a,2^\lambda)=\left(\tfrac{2}{3}\right)^\lambda=(-1)^\lambda.$$

In diesen beiden Fällen ist damit $\Lambda(a)=1$; die Bedingung (5) von Satz 2 ist demnach erfüllt.

In (12)c) ist $Q(x)=2^{-\lambda}r(x_1^2+2^\sigma t x_2^2)$ die direkte Summe der quadratischen Formen $Q_1(x_1)=2^{-\lambda}rx_1^2$ und $Q_2(x_2)=2^{-\lambda+\sigma}rtx_2^2$. Man findet deshalb mit Hilfe von (8)

$$S_Q(a)=S_{Q_1}(a)S_{Q_2}(a)=i\left(\frac{-1}{t}\right)\left(\frac{2}{t}\right)^{\lambda-\sigma}\left(\frac{2}{r}\right)^\sigma\left(\frac{2}{a}\right)^\sigma\varepsilon(-ar)\varepsilon(-art).$$

Für den Faktor $\Lambda(a)$ erhält man

$$\Lambda(a)=S_Q(a)S_Q(1)^{-1}=\left(\frac{2}{a}\right)^\sigma\frac{\varepsilon(-ar)\xi(-art)}{\varepsilon(-r)\varepsilon(-rt)}.$$

Für alle ungeraden u, v gilt:

$$\varepsilon(u)\varepsilon(uv)=\varepsilon(v)(-1)^{[(u-1)/2]\cdot[(v-1)/2]}\quad\text{und}\quad\left(\frac{-1}{u}\right)=(-1)^{(u-1)/2}.$$

Folglich ist

$$\Lambda(a)=\left(\frac{2}{a}\right)^\sigma\left(\frac{-1}{a}\right)^{(t+1)/2}$$

ein Charakter von $A_\lambda^\times$ und erfüllt die Bedingung (5) von Satz 2.

Auf eine Untersuchung quadratischer Moduln, die von mehr als zwei Elementen erzeugt werden, kann man hier verzichten, denn die Darstellungen, die zu den quadratischen Moduln (7) und (10) bzw. (12) gehören, reichen für unsere Ziele im wesentlichen aus. Es ist aber zu bemerken, dass im Fall $p\neq 2$ jeder hier betrachtete quadratische Modul zu einer direkten Summe quadratischer Moduln, die von einem einzigen Element erzeugt werden, äquivalent ist. Im Fall $p=2$ ist jeder quadratische Modul zu einer direkten Summe quadratischer Moduln, die von einem oder zwei Elementen erzeugt werden, äquivalent (man verwendet ein Resultat von Minkowski über ganzzahlige quadratische Formen mod n, $n\in N$).

Anhand von Satz 2 sieht man leicht, dass für quadratische Moduln (M, Q), die von mehr als zwei Elementen erzeugt werden, die Darstellung $W(M, Q)$, falls sie existiert, zum Tensorprodukt der Weilschen Darstellungen, welche von den Summanden von (M, Q) erzeugt werden, äquivalent ist.

DEFINITION 3. Die Darstellungen von $\mathbf{SL}_2(A_\lambda)$, die zu den binären quadratischen Moduln (10) bzw. (12) gehören, heissen:

—die *zerlegte Weilsche Darstellung* D_λ im Fall a);
—die *unverzweigte Weilsche Darstellung* N_λ im Fall b);
—die *verzweigten Weilschen Darstellungen* $R_\lambda^\sigma(r, t)$ im Fall c).

Die Darstellungen von $\mathbf{SL}_2(A_\lambda)$, die im Fall $p \neq 2$ zu den quadratischen Moduln (7) gehören, heissen $R_\lambda(r)$.

3. Zwei Zerlegungsmethoden.

In diesem Paragraphen beschreiben wir zwei Methoden, um Unterdarstellungen der Weilschen Darstellungen zu konstruieren.

Die erste Methode stammt von Kloosterman [2]. Sei (M, Q) ein quadratischer Modul, der eine Weilsche Darstellung von $\mathbf{SL}_2(A_\lambda)$ erzeugt, und sei $\mathrm{Aut}(M, Q)$ die Gruppe der unter Q invarianten Automorphismen von M, d.h. für alle $\varphi \in \mathrm{Aut}(M, Q)$ gilt $Q(\varphi(x)) = Q(x)$ für alle $x \in M$. Sei $\mathfrak{U}$ eine abelsche Untergruppe von $\mathrm{Aut}(M, Q)$ und χ ein Charakter von $\mathfrak{U}$, dann ist

$$V(\chi) := \{f \in \mathbf{C}^M \mid f(\varepsilon x) = \chi(\varepsilon) f(x)\ \forall \varepsilon \in \mathfrak{U}, \forall x \in M\}$$

ein unter $\mathbf{SL}_2(A_\lambda)$ invarianter Unterraum von $V = \mathbf{C}^M$. Schreibt man $W(M, Q, \chi)$ für die Unterdarstellung von $W(M, Q)$ im Raum $V(\chi)$, so gilt

$$W(M, Q) = \bigoplus_\chi W(M, Q, \chi)$$

wobei χ alle Charaktere von $\mathfrak{U}$ durchläuft.

Die zweite Methode beruht auf einem Lemma von P. Cartier.

LEMMA 3. *Sei (M, Q) ein quadratischer Modul, der eine Weilsche Darstellung $W(M, Q)$ von $\mathbf{SL}_2(A_\lambda)$ erzeugt. Sei H ein Untermodul von M, sodass Q auf H verschwindet, und sei*

$$H^\perp = \{x \in M \mid B(x, y) = 0\ \forall y \in H\},$$

wobei B die zu Q gehörige Bilinearform ist. Es gilt $H^\perp \supset H$. Setzt man

$$M_1 := H^\perp/H \quad \text{und} \quad Q_1(x+H) := Q(x) \quad \text{für alle} \quad x \in H^\perp,$$

so erfüllt (M_1, Q_1) die Bedingung (5) von Satz 2, und $W(M_1, Q_1)$ ist zu einer Unterdarstellung von $W(M, Q)$ isomorph.

Q_1 ist nicht-entartet, denn $(H^\perp)^\perp = H$. Nun hat man

$$\sum_{h\in H} \mathbf{e}(Q(y+h)) = \sum_{h\in H} \mathbf{e}(B(y,h)+Q(y)) = \begin{cases} 0 & \text{für} \quad y \notin H^\perp, \\ |H|\,\mathbf{e}(Q(y)) & \text{für} \quad y \in H^\perp. \end{cases}$$

Diese Formel bleibt richtig, wenn man Q durch aQ und B durch aB ersetzt für beliebige $a \in A_\lambda^\times$. Daraus folgt

$$S_Q(a) = |M|^{-1/2} \sum_{x\in M} \mathbf{e}(-aQ(x)) = |M|^{-1/2} \sum_{x\in M/H^\perp} \sum_{y\in H^\perp/H} \sum_{h\in H} \mathbf{e}(-aQ(x+y+h))$$

$$= |M|^{-1/2} \sum_{y\in H^\perp/H} |H|\,\mathbf{e}(-aQ(y))$$

$$S_Q(a) = |M|^{-1/2}\,|H|\,|M_1|^{+1/2}\,S_{Q_1}(a) = S_{Q_1}(a).^{(4)} \tag{20}$$

Die Bedingung (5′) ist also für Q_1 genau dann erfüllt, wenn sie für Q erfüllt ist. Um zu zeigen, dass $W(M_1, Q_1)$ eine Unterdarstellung von $W(M, Q)$ ist, betrachten wir den Unterraum E von $\mathbf{C}^M$, der die Funktionen $f \in \mathbf{C}^M$ enthält, welche

1) $f(x) = o$ für alle $x \notin H^\perp$,

2) $f(x) = f(x')$ für alle $x, x' \in H^\perp$ mit $x - x' \in H$,

erfüllen. E ist wegen (19) ein invarianter Unterraum von $\mathbf{C}^M$ und ist zu $\mathbf{C}^{M_1}$ isomorph. Mit Hilfe von (20) ist leicht einzusehen, dass $W(M_1, Q_1)$ gerade die zu E gehörige Unterdarstellung von $W(M, Q)$ ist.

4. Die Konjugiertenklassen von $\mathbf{SL}_2(A_\lambda)$.[5]

Um die Klassen konjugierter Elemente in den Gruppen $\mathbf{SL}_2(A_\lambda)$ zu untersuchen, erweist es sich als zweckmässig, eine Partition von $\mathbf{SL}_2(A_\lambda)$ in zwei

[4] Um $|M| = |H|^2\,|M_1|$ zu beweisen, bemerkt man, dass durch die Zuordnung $x \to B(x, ?)$ eine eineindeutige Abbildung von M auf $\mathrm{Car}^+(M)$ (additive Charaktere) gegeben ist. Man verwendet dann die allgemeinen Sätze über Charaktere (Siehe etwa H. Hasse, Vorlesungen über Zahlentheorie, 2. Aufl., §13.4).

[5] Dieser Paragraph entstand unabhängig von "The automorphisms and conjugacy classes of $\mathbf{LF}(2, 2^n) = \mathbf{PSL}_2(\mathbf{Z}/2^n\mathbf{Z})$" von J. B. Dennin, Illinois J. of Math. 19, 542–552, 1976.

konjugationsinvariante Teilmengen

$$M_1^\lambda := \{U \in \mathbf{SL}_2(A_\lambda) \mid \text{für alle } a \in A_1 \text{ ist } U \not\equiv aE \bmod p\}$$

und

$$M_2^\lambda := \{U \in \mathbf{SL}_2(A_\lambda) \mid \exists a \in A_1 \text{ mit } U \equiv aE \bmod p\}$$

$\left(\text{mit } E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right)$ vorzunehmen. (Wir werden in diesem Paragraphen meistens in $A_\lambda = \mathbf{Z}/p^\lambda\mathbf{Z}$ rechnen, und nur dort Kongruenzen benutzen, wo es zweckmässiger ist. Wir werden aber für eine Klasse aus $\mathbf{Z}/p^\lambda\mathbf{Z}$ und deren Repräsentanten stets den gleichen Buchstaben verwenden.)

Wir beweisen zuerst zwei Lemmata, die auch noch richtig sind, wenn man A_λ durch einen lokalen Ring ersetzt.

LEMMA 4. *Sei* $U = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ *aus* $M_2(A_\lambda)$ (*Menge der* (2, 2)-*Matrizen mit Koeffizienten aus* A_λ) *mit* $U \not\equiv aE \bmod p$ *für alle* a *aus* A_1, *dann existiert* X *aus* $\mathbf{SL}_2(A_\lambda)$, *sodass* $XUX^{-1} = \begin{pmatrix} * & * \\ \gamma_1 & * \end{pmatrix}$ *mit* $\gamma_1 \in A_\lambda^\times$ *gilt.*

Wenn $\gamma \equiv 0 \not\equiv \beta \bmod p$ ist, so konjugiert man U mit $X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Wenn $\gamma \equiv \beta \equiv 0 \not\equiv \alpha - \delta \bmod p$ ist, so konjugiert man U mit $X = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Der Fall $\gamma \equiv \beta \equiv \alpha - \delta \equiv 0 \bmod p$ ist nach Voraussetzung ausgeschlossen.

LEMMA 5. *Seien* $U_i = \begin{pmatrix} \alpha_i & \beta_i \\ \gamma_i & \delta_i \end{pmatrix} (i = 1, 2)$ *aus* $\mathbf{M}_2(A_\lambda)$ *mit* $\gamma_i \in A_\lambda^\times$. *Es existiert genau dann ein* X *aus* $\mathbf{SL}_2(A_\lambda)$ *mit* $XU_2X^{-1} = U_1$, *wenn*

1) $\operatorname{Sp} U_1 = \operatorname{Sp} U_2 = s$ (*Spur*),
2) $\det U_1 = \det U_2 = d$ (*Determinante*),
3) *die Gleichung*

$$\xi^2 + s\xi\eta + d\eta^2 = \gamma_1\gamma_2^{-1} \tag{21}$$

mindestens eine Lösung (ξ, η) *aus* $A_\lambda \times A_\lambda$ *besitzt.*

Die Notwendigkeit der Bedingungen 1) und 2) ist klar. Existiert $X = \begin{pmatrix} * & * \\ x & y \end{pmatrix}$ aus $\mathbf{SL}_2(A_\lambda)$ mit $XU_2X^{-1} = U_1$, so gilt

$$\gamma_2 y^2 + (\alpha_2 - \delta_2)xy - \beta_2 x^2 = \gamma_1. \tag{22}$$

Das Paar (ξ, η) mit

$$\xi = y - \delta_2 \gamma_2^{-1} x \quad \text{und} \quad \eta = \gamma_2^{-1} x \tag{23}$$

ist eine Lösung von (21).

Seien umgekehrt 1) und 2) erfüllt und sei $(\xi, \eta) \in A_\lambda \times A_\lambda$ eine Lösung von (21). Aus (23) lässt sich ein Paar (x, y) berechnen, das (22) erfüllt. Die Elemente x und y können, wegen der Voraussetzung über γ_i, nicht beide in $A_\lambda - A_\lambda^\times$ liegen. Man kann also das Paar (x, y) zu einer Matrix $X_1 = \begin{pmatrix} * & * \\ x & y \end{pmatrix}$ aus $\mathbf{SL}_2(A_\lambda)$ ergänzen und U_2 ist zu einer Matrix $U_3 = X_1 U_2 X_1^{-1} = \begin{pmatrix} \alpha_3 & \beta_3 \\ \gamma_3 & \delta_3 \end{pmatrix}$ mit $\gamma_3 = \gamma_1$ konjugiert. Die Spuren und Determinanten von U_1 und U_3 stimmen überein, wegen 1) und 2). Wählt man

$$X_2 = \begin{pmatrix} 1 & \gamma_1^{-1}(\alpha_1 - \alpha_3) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \gamma_1^{-1}(\delta_3 - \delta_1) \\ 0 & 1 \end{pmatrix},$$

so gilt

$$X_2 U_3 X_2^{-1} = X_2 X_1 U_2 (X_2 X_1)^{-1} = U_1$$

mit $X_2 X_1$ aus $\mathbf{SL}_2(A_\lambda)$. Damit ist Lemma 5 bewiesen.

Lemma 4 und Lemma 5 lassen sich auf M_1^λ anwenden.

LEMMA 6. *Die Anzahl der Konjugiertenklassen in* M_1^λ *ist* $(p+2)p^{\lambda-1}$, *falls* $p \neq 2$ *und* $\lambda \geq 1$ *oder* $p = 2$ *und* $\lambda \geq 3$ (*sie ist* 6 *falls* $p = 2$ *und* $\lambda = 2$, 2 *falls* $p = 2$ *und* $\lambda = 1$).

Die Elemente aus M_1^λ erfüllen die Bedingung von Lemma 4. Aus Lemma 5

$(d=1)$ folgt, dass die Matrizen $\begin{pmatrix} s & -\gamma^{-1} \\ \gamma & 0 \end{pmatrix}$ ein Repräsentantensystem der Konjugiertenklassen in M_1^λ bilden, wobei s ganz A_λ und γ ein Repräsentantensystem von $A_\lambda^\times \bmod S(s,1)$ (siehe §2) durchlaufen. Die Anzahl der verschiedenen γ ist für ein festes s gleich $[A_\lambda^\times : S(s,1)]$ (siehe Tabelle 1), damit lässt sich die Anzahl der Konjugiertenklassen in M_1^λ sofort berechnen.

Die Tabelle 2 gibt vollständige Angaben über M_1^λ. Um die Mächtigkeit der Klassen zu berechnen, geht man wie folgt vor. Sei $U = \begin{pmatrix} s & -\gamma^{-1} \\ \gamma & 0 \end{pmatrix}$. Die Matrizen aus $\mathbf{SL}_2(A_\lambda)$, die mit U kommutieren, sind alle von der Form $\xi E + \eta U$ mit $(\xi, \eta) \in A_\lambda \times A_\lambda$ und

$$\det(\xi E + \eta U) = \xi^2 + s\xi\eta + \eta^2 = 1.$$

Die Mächtigkeit $m(U)$ der Klasse von U ist also gleich der Ordnung von $\mathbf{SL}_2(A_\lambda)$ dividiert durch die Anzahl $N(s)$ der Lösungen (ξ, η) in $A_\lambda \times A_\lambda$ von

$$\xi^2 + s\xi\eta + \eta^2 = 1.$$

Sei $n_\lambda(s, d)$ die Anzahl der Lösungen (ξ, η) in $A_\lambda \times A_\lambda$ von

$$\xi^2 + s\xi\eta + d\eta^2 \not\equiv 0 \bmod p,$$

Tabelle 2

Die Matrizen $\begin{pmatrix} s & -t^{-1} \\ t & 0 \end{pmatrix}$, wobei s und t folgende Werte durchlaufen, bilden ein Repräsentantensystem der Konjugiertenklassen von M_1^λ.

p	λ	$s \in A_\lambda$ mit	$t=$	Anzahl der Klassen	Mächtigkeit der Klassen
$p \neq 2$	$\lambda \geq 1$	$s \equiv \pm 2 \bmod p$	$1, u; \left(\frac{u}{p}\right) = -1$	$4p^{\lambda-1}$	$\frac{1}{2}(p^2-1)p^{2\lambda-2}$
		$s \not\equiv \pm 2 \bmod p, \left(\frac{s^2-4}{p}\right) = +1$	1	$\frac{1}{2}(p-3)p^{\lambda-1}$	$(p+1)p^{2\lambda-1}$
		$s \not\equiv \pm 2 \bmod p, \left(\frac{s^2-4}{p}\right) = -1$	1	$\frac{1}{2}(p-1)p^{\lambda-1}$	$(p-1)p^{2\lambda-1}$
$p=2$	$\lambda \geq 3$	$s \equiv 2 \bmod 4$	1, 3, 5, 7	2^λ	$3 \cdot 2^{2\lambda-4}$
		$s \equiv 0 \bmod 4$	1, 3	$2^{\lambda-1}$	$3 \cdot 2^{2\lambda-3}$
		$s \equiv 1 \bmod 2$	1	$2^{\lambda-1}$	$2^{2\lambda-1}$
	$\lambda = 2$	$s \equiv 0 \bmod 2$	1, 3	4	6
		$s \equiv 1 \bmod 2$	1	2	8
	$\lambda = 1$	$s = 0$	1	1	3
		$s = 1$	1	1	2

dann ist $N(s)$ gleich $n_\lambda(s,1)$ dividiert durch die Ordnung von $S(s,1)$ (Lemma 0). Man erhält also

$$m(U)=\frac{|\mathbf{SL}_2(A_\lambda)|\,|S(s,1)|}{n_\lambda(s,1)}=\frac{|\mathbf{SL}_2(A_\lambda)|\,|A_\lambda^\times|}{n_\lambda(s,1)[A_\lambda^\times:S(s,1)]}$$

Eine leichte Rechnung zeigt, dass für $\lambda\geq 1$

$$|\mathbf{SL}_2(A_\lambda)|=(p^2-1)p^{3\lambda-2}$$

$$n_\lambda(s,d)=\left\{\begin{array}{lll}(p-1)\left(p-\left(\frac{\Delta}{p}\right)\right)p^{2\lambda-2} & \text{falls} & p\neq 2 \quad (\Delta=s^2-4d),\\ 2^{2\lambda-1} & \text{falls} & s\equiv 0 \bmod 2\\ 2^{2\lambda-2} & \text{falls} & d\equiv 0\\ 3\cdot 2^{2\lambda-2} & \text{falls} & d\equiv 1\end{array}\right\}\ \text{und}\ s\equiv 1 \bmod 2\ \Big\}\ \text{und}\ p=2;\Big\} \tag{24}$$

damit lässt sich jetzt $m(U)$ explizit berechnen.

LEMMA 7. *Jedes Element U aus M_2^λ besitzt, eventuell nach Konjugation mit einem geeigneten X aus $\mathbf{SL}_2(A_\lambda)$, die Gestalt*

$$U=\varepsilon E+p^h\begin{pmatrix}s & -dt^{-1}\\ t & 0\end{pmatrix} \tag{25}$$

mit $1\leq h\leq\lambda$, $\varepsilon<p^h$, $\varepsilon^2\equiv 1 \bmod p^h$, $s,d\in A_{\lambda-h}$, $t\in A_{\lambda-h}^\times$, *und* s *lässt sich* $\bmod p^{\lambda-h}$ *eindeutig in Abhängigkeit von* ε, h, d *durch die Kongruenz*

$$\varepsilon^2+p^hs\varepsilon+p^{2h}d\equiv 1 \bmod p^\lambda \tag{26}$$

berechnen ($A_{\lambda-h}=A_{\lambda-h}^\times=\{0\}$ *falls* $h=\lambda$).

Wenn $U=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$ in M_2^λ liegt, so gibt es einen Exponenten $h\geq 1$ mit $p^h=\mathrm{g.g.}T.(\alpha-\delta,\beta,\gamma)$, und eine Zahl $a\in A_\lambda^\times$, sodass

$$U\equiv aE \bmod p^h \quad \text{und für alle} \quad a'\in A_\lambda \qquad U\not\equiv a'E \bmod p^{h+1}.$$

Es gibt also ein $\varepsilon<p^h$ mit $\varepsilon\equiv a \bmod p^h$ und ein $V\in\mathbf{M}_2(A_{\lambda-h})$, sodass

$$U=\varepsilon E+p^hV.$$

Die Matrix V erfüllt die Bedingung von Lemma 4, d.h. sie lässt sich durch Konjugation auf die Form $\begin{pmatrix} s & -dt^{-1} \\ t & 0 \end{pmatrix}$ mit $t \in A_{\lambda-h}^{\times}$ bringen (Anwendung von Lemma 5). Berechnet man die Determinante von U, so erhält man die Relation (26). Daraus folgt insbesondere, dass $\varepsilon^2 \equiv 1 \bmod p^h$ gelten muss, d.h. $1 \bmod p^h$ ist

$$\varepsilon \equiv \begin{cases} \pm 1 & \text{falls } h \geq 1 \text{ und } p \neq 2, \\ \left.\begin{array}{ll} 1 & \text{falls } h = 1 \\ \pm 1 & \text{falls } h = 2 \\ \pm 1, \pm(1+2^{h-1}) & \text{falls } h \geq 3 \end{array}\right\} & \text{und } p = 2. \end{cases}$$

LEMMA 8. *Zwei Matrizen* $U_i = \varepsilon_i E + p^{h_i}\begin{pmatrix} s_i & -dt_i^{-1} \\ t_i & 0 \end{pmatrix}$ $(i = 1, 2)$ *aus* M_2^{λ} *sind genau dann konjugiert, wenn*

$$\varepsilon_1 = \varepsilon_2, \qquad h_1 = h_2 = h, \qquad s_1 = s_2 = s, \qquad d_1 = d_2 = d$$

und die Gleichung (im Ring $A_{\lambda-h}$*)*

$$\xi^2 + s\xi\eta + d\eta^2 = t_1 t_2^{-1}$$

mindestens eine Lösung (ξ, η) *aus* $A_{\lambda-h} \times A_{\lambda-h}$ *besitzt.*

Das ist eine unmittelbare Folgerung aus Lemma 5.

LEMMA 9. *Die Anzahl der Konjugiertenklassen in* M_2^{λ} *ist*

$$\begin{array}{lll} 4\dfrac{p^{\lambda}-1}{p-1} - 2p^{\lambda-1} & \textit{falls } \lambda \geq 1 & \textit{und } p \neq 2, \\ \left.\begin{array}{ll} 15 \cdot 2^{\lambda-2} - 16 & \textit{falls } \lambda \geq 3 \\ 4 & \textit{falls } \lambda = 2 \\ 1 & \textit{falls } \lambda = 1 \end{array}\right\} & \textit{und } p = 2. \end{array}$$

Aus den Lemmata 7 und 8 folgt, dass die Konjugiertenklassen in M_2^{λ} durch

1) h (durchläuft alle ganzen Zahlen von 1 bis λ),
2) ε (durchläuft die Lösungen von $\varepsilon^2 \equiv 1 \bmod p^h$, mit $\varepsilon < p^h$),
3) d (durchläuft ganz $A_{\lambda-h}$),
4) t (durchläuft, für gegebene h, ε, d, ein Repräsentantensystem von $A_{\lambda-h}^{\times} \bmod S(s, d)$, wobei s (26) erfüllt)

eineinduetig charakterisiert werden. Mit Hilfe von Tabelle 1 lässt sich nun die Anzahl der Konjugiertenklassen in M_2^λ sofort berechnen.
Die Tabelle 3 enthält vollständige Angaben über M_2^λ. Sei

$$U = \varepsilon E + p^h V, \quad \text{mit} \quad V = \begin{pmatrix} s & -dt^{-1} \\ t & 0 \end{pmatrix} \in \mathbf{M}_2(A_{\lambda-h}),$$

Tabelle 3

Die Matrizen $\varepsilon E + p^h \begin{pmatrix} s & -dt^{-1} \\ t & 0 \end{pmatrix}$, wobei ε, h, d und t folgende Werte durchlaufen und s die Kongruenz (26) erfüllt, bilden ein Repräsentantensystem der Konjugiertenklassen von M_2^λ.

λ, h	ε	$d \in A_{\lambda-h}\cdot d \equiv$	$t =$	Anzahl der Klassen	Mächtigkeit der Klassen
$p \neq 2$					
		$d \equiv 0 \bmod p$	$1, u$	$4p^{\lambda-h-1}$	$\frac{1}{2}(p^2-1)p^{2\lambda-2h-2}$
$\lambda \geq 1$ $1 \leq h < \lambda$	± 1	$\left(\frac{-d}{p}\right) = +1$	1	$(p-1)p^{\lambda-h-1}$	$(p+1)p^{2\lambda-2h-1}$
		$\left(\frac{-d}{p}\right) = -1$	1	$(p-1)p^{\lambda-h-1}$	$(p-1)p^{2\lambda-2h-1}$
$1 \leq h = \lambda$	± 1	0	0	2	1
$p = 2$					
$\lambda \geq 4$ $h = 1$	1	0, 1 mod 8	1, 3, 5, 7	$2^{\lambda-1}$	$3 \cdot 2^{2\lambda-6}$
		4, 5 mod 8	1, 3	$2^{\lambda-2}$	$3 \cdot 2^{2\lambda-5}$
		2, 3, 6, 7 mod 8	1, 5	$2^{\lambda-1}$	$3 \cdot 2^{2\lambda-5}$
$\lambda = 3, h = 1$	1	0, 1 mod 4	1, 3	4	6
		2, 3 mod 4	1	2	12
$\lambda = 2, h = 1$	1	0, 1 mod 2	1	2	3
$\lambda \geq 5$ $2 \leq h \leq \lambda - 3$	± 1	0 mod 8	1, 3, 5, 7	$2^{\lambda-h}$	$3 \cdot 2^{2\lambda-2h-4}$
		1, 4, 5 mod 8	1, 3	$3 \cdot 2^{\lambda-h-1}$	$3 \cdot 2^{2\lambda-2h-3}$
		2, 6 mod 8	1, 5	$2^{\lambda-h}$	$3 \cdot 2^{2\lambda-2h-3}$
		3, 7 mod 8	1	$2^{\lambda-h-1}$	$3 \cdot 2^{2\lambda-2h-2}$
$\lambda \geq 4$ $3 \leq h < \lambda$	$\pm(1+2^{h-1})$	1 mod 2	1	$2^{\lambda-h}$	$2^{2\lambda-2h-1}$
		0 mod 2	1	$2^{\lambda-h}$	$3 \cdot 2^{2\lambda-2h-1}$
$\lambda \geq 4$ $h = \lambda - 2$	± 1	0, 1 mod 4	1, 3	8	6
		2, 3 mod 4	1	4	12
$\lambda \geq 3$ $h = \lambda - 1$	± 1	0, 1 mod 2	1	4	3
$\lambda = h = 3$	± 1	0	0	4	1
	$\pm(1+2^{h-1})$				
$\lambda = h = 2$	± 1	0	0	2	1
$\lambda = h = 1$	1	0	0	1	1

wie in (25). Eine Matrix X aus $\mathbf{SL}_2(A_\lambda)$ kommutiert genau dann mit U, wenn

$$XV \equiv VX \bmod p^{\lambda-h}.$$

Die Mächtigkeit $m(U)$ der Klasse von U ist demnach gleich der Ordnung von $\mathbf{SL}_2(A_{\lambda-h})$ dividiert durch die Anzahl der X aus $\mathbf{SL}_2(A_{\lambda-h})$, die mit V kommutieren. Man wiederholt jetzt fast wörtlich die Rechnung, die für U aus M_1^λ gemacht wurde, und erhält

$$m(U) = \frac{|\mathbf{SL}_2(A_{\lambda-h})|\,|A_{\lambda-h}^\times|}{n_\lambda(s,d)[A_{\lambda-h}^\times : S(s,d)]}$$

(wobei $S(s,d)$ hier eine Untergruppe von $A_{\lambda-h}^\times$ ist, d.h. λ muss in Tabelle 1 durch $\lambda - h$ ersetzt werden).

SATZ 5. *Die Anzahl der Konjugiertenklassen in* $\mathbf{SL}_2(A_\lambda)$ *(mit* $A_\lambda = \mathbf{Z}/p^\lambda\mathbf{Z}$*) ist gleich*

$$\begin{aligned} &p^\lambda + 4(p^\lambda - 1)/(p-1) \quad \textit{falls} \quad p \neq 2, \qquad \lambda \geq 1, \\ &\left.\begin{aligned} 23 \cdot 2^{\lambda-2} - 16 \quad &\textit{falls} \quad \lambda \geq 3 \\ 10 \quad &\textit{falls} \quad \lambda = 2 \\ 3 \quad &\textit{falls} \quad \lambda = 1 \end{aligned}\right\} \quad \textit{und} \quad p = 2. \end{aligned}$$

Das folgt aus den Lemmata 6 und 9. Damit ist nun auch die Anzahl der irreduziblen Darstellungen von $\mathbf{SL}_2(A_\lambda)$ bekannt.

LITERATUR

[1] CASSELMAN, W.: *On the representations of* $\mathbf{SL}_2(k)$ *related to binary quadratic forms.* Am. J. Math. *94* (1972) 810–834.

[2] KLOOSTERMAN, H. D.: *The behaviour of general theta functions under the modular group and the characters of the binary modular congruence groups I, II.* Ann. of Math., II. Ser., *47* (1946) 317–447.

[3] KUTZKO, P. C.: *The characters of the binary modular congruence groups.* Ph.D. thesis, University of Wisconsin-Madison (1972).

[4] NOBS, A. and WOLFART, J.: *Darstellungen von* $\mathbf{SL}(2, \mathbf{Z}/p^\lambda\mathbf{Z})$ *und Thetafunktionen I.* Math. Z. *138* (1974) 239–254.

[5] —— und ——: *Les représentations de Weil du groupe* $\mathbf{SL}_2(\mathbf{Z}_2)$. C.R. Acad. Sc. Paris, *281*, Série A (1975) 137–140.

[6] —— und ——: *Les représentations irréductibles du groupe* $\mathbf{SL}_2(\mathbf{Z}_2)$. C. R. Acad. Sc. Paris, *281*, Série A (1975) 261–264.

[7] LANG S.: *Algebraic number theory.* Addison-Wesley, Reading (Mass.) (1970).
[8] ROHRBACH, H.: *Die Charaktere der binären Kongruenzgruppen* mod p^2. Schr. d. math. Sem. Univ. Berlin, *1* (1932) 33–94.
[9] SERRE, J. P.: *Cours d'arithmétique,* Presses univ. de France, Paris (1970).
[10] TANAKA, S.: *On irreducible unitary representations of some special linear groups of the second order II.* Osaka J. Math., Ser. *2,* 3 (1966) 229–242.
[11] ——: *Irreducible representations of the binary modular congruence groups* mod p^λ. J. Math. Kyoto Univ., 7 (1967) 123–132.
[12] WEIL, A.: *Sur certains groupes d'opérateurs unitaires.* Acta Math., *111* (1964) 143–211.

Institute for Advanced Study
Princeton, N.J. 08540
USA

Received May, 1976