Reduktion abelscher Varietäten

Diplomarbeit im
Departement für Mathematik
der ETH Zürich
Betreut von Prof. Dr. Richard Pink

Verfasst von Thomas Huber

Zürich, Oktober 2004

Inhaltsverzeichnis

Einführung

Sei A eine abelsche Varietät der Dimension g über einem Zahlkörper K. Für alle ausser endlich vielen Stellen $\mathfrak{p}$ in K ist die Reduktion $A_\mathfrak{p}$ von A bei $\mathfrak{p}$ wieder eine abelsche Varietät, definiert über dem endlichen Restklassenkörper $k_\mathfrak{p}$. Man sagt, A habe gute Reduktion bei $\mathfrak{p}$.

Diese Arbeit befasst sich mit zwei verschiedenen Eigenschaften der Reduktion $A_\mathfrak{p}$.

Sei $p = \mathrm{char}(k_\mathfrak{p})$. Die Gruppe $A_\mathfrak{p}[p^n](\overline{k}_\mathfrak{p})$ der p^n-Torsionspunkte ist als abstrakte Gruppe isomorph zu $(\mathbb{Z}/p^n\mathbb{Z})^h$ mit einem von n unabhängigen Exponenten $h \leq g$. Gilt $h = g$, nennt man $A_\mathfrak{p}$ gewöhnlich.

Vermutung 0.1 (über die gewöhnliche Reduktion). *Es gibt eine endliche Erweiterung K' von K und eine Menge V von Stellen der Dirichlet-Dichte 1 in K', sodass $A_{K'}$ gute Reduktion besitzt bei allen Stellen $v \in V$.*

Unter der Voraussetzung $\mathrm{End}(A_{\overline{K}}) = \mathbb{Z}$ konnte Pink diese Vermutung in vielen Fällen beweisen ([Pi1], Theorem 7.1).

Vermutung 0.2 (Pink, Rössler). *Es gibt eine endliche Erweiterung K' von K und eine Menge V von Stellen der Dirichlet-Dichte 1 in K', sodass gilt: Für alle $\mathfrak{p} \in V$ ist*

$$p \not| \ \mathrm{card}(A_\mathfrak{p}(k'_\mathfrak{p})),$$

wobei $p = \mathrm{char}(k'_\mathfrak{p})$.

Betrachte die ℓ-adische Galoisdarstellung

$$\rho_{ell} : \mathrm{Gal}(\overline{L}/L) \to \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell A) \cong \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$$

auf dem rationalen Tate-Modul von A. Sei $\mathfrak{p}$ eine Stelle von K, an der A gute Reduktion besitzt. Das charakteristische Polynom von $\rho_{ell}(\mathrm{Frob}_\mathfrak{p}$ besitzt ganze Koeffizienten. Daher sind die $2g$ Frobenius-Eigenwerte bei $\mathfrak{p}$ ganzalgebraische Zahlen. Sei λ eine Stelle in $\overline{\mathbb{Q}}$, die über $p = \mathrm{char}(k'_\mathfrak{p})$ liegt. Mindestens die Hälfte der

1 Grundlagen

1.1 Die Darstellung auf dem Tate-Modul

Sei K ein perfekter Körper und A eine abelsche Varietät der Dimension g, definiert über K. Wir wählen einen festen algebraischen Abschluss $\overline{K}$ von K. Für eine Primzahl ℓ sei

$$A[\ell^n] = \{x \in A(\overline{K}) \mid \ell^n \cdot x = 0\}$$

die Gruppe der ℓ^n-Torsionspunkte von A. Für $\ell \neq \mathrm{char}(K)$ gilt

$$A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}.$$

Im Fall $\mathrm{char}(K) = p > 0$ ist jedoch $A[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^h$ mit einem von n unabhängigen Exponenten $0 \leq h \leq g$. Gilt $h = g$, dann heisst A *gewöhnlich*. Im Folgenden sei ℓ stets verschieden von $\mathrm{char}(K)$. Die Multiplikation mit ℓ^{n-m} induziert einen Homomorphismus $A[\ell^n] \to A[\ell^m]$. Der inverse Limes der Gruppen $A[\ell^n]$ bezüglich dieser Homomorphismen ist der ℓ-adische *Tate-Modul* $T_\ell A$ von A. Es gilt

$$T_\ell A = \varprojlim A[\ell^n] \cong \mathbb{Z}_\ell^{2g}.$$

Der *rationale* Tate-Modul $V_\ell A = T_\ell A \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ ist somit ein $2g$-dimensionaler $\mathbb{Q}_\ell$-Vektorraum.

Die Galoisgruppe $\mathrm{Gal}(\overline{K}/K)$ operiert auf den diskreten Gruppen $A[\ell^n]$ und diese Operation ist verträglich mit den Abbildungen $A[\ell^n] \to A[\ell^m]$. Nach Übergang zum inversen Limes ergibt dies eine stetige Operation von $\mathrm{Gal}(\overline{K}/K)$ auf dem ℓ-adischen Tate-Modul und damit auch auf $V_\ell A$. Nach einer Basiswahl in $V_\ell A$ erhalten wir somit eine stetige ℓ-adische Darstellung

$$\rho_\ell : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{Aut}_{\mathbb{Q}_\ell}(V_\ell A) \cong \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

Von nun an sei K stets ein Zahlkörper. Wir setzen $\Gamma_\ell = \rho_\ell(\mathrm{Gal}(\overline{K}/K))$. Sei G_ℓ der Zariskiabschluss von Γ_ℓ in $\mathrm{GL}_{2g}(\mathbb{Q}_\ell)$. G_ℓ ist eine algebraische Gruppe. Γ_ℓ ist eine ℓ-adische Liegruppe, offen in G_ℓ. Wichtige Eigenschaften der Galoisdarstellung beschreibt folgendes Resultat von G. Faltings ([Fal])

Theorem 1.1. *Die Darstellung ρ_ℓ ist halbeinfach, und der natürliche Homomorphismus*

$$\mathrm{End}(A) \otimes \mathbb{Q}_\ell \to \mathrm{End}_{\mathbb{Q}_\ell[\mathrm{Gal}(\overline{K}/K)]}(V_\ell A)$$

ist ein Isomorphismus.

Korollar 1.2. *G_ℓ° ist reduktiv.*

Eine untere Schranke für die Grösse des Zentrums von G_ℓ gibt folgendes Resultat von Bogomolov ([Bog] Theorem 3).

Theorem 1.3. *G_ℓ enthält die Skalare $\mathbb{Q}_\ell \cdot \mathrm{id}$.*

Für jede natürliche Zahl n ist die Weil Paarung $e_{\ell^n} : A[\ell^n] \times A^\vee[\ell^n] \to \mu_{\ell^n}$ nicht ausgeartet, alternierend und $\mathrm{Gal}(\overline{K}/K)$-äquivariant. Nach Wahl einer Polarisierung und Übergang zum inversen Limes liefert dies eine Paarung

$$e_\ell : T_\ell A \times T_\ell A \to \varprojlim \mu_{\ell^n} \cong \mathbb{Z}_\ell(1) \tag{1}$$

mit denselben Eigenschaften, dabei operiert $\mathrm{Gal}(\overline{K}/K)$ auf $\mathbb{Z}_\ell(1)$ durch den zyklotomischen Charakter.

Daraus folgt, dass nach geeigneter Basiswahl in $V_\ell A$ das Bild Γ_ℓ von Galois in der Gruppe der symplektischen Ähnlichkeiten

$$\mathrm{CSp}_{2g}(\mathbb{Q}_\ell) = \{x \in \mathrm{GL}_{2g}(\mathbb{Q}_\ell) \mid x\,{}^tJm = \mu(x) \cdot J,\ \mu(x) \in \mathbb{Q}_\ell^*\},$$

liegt, wobei

$$J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

Der Multiplikator $\mu : \mathrm{CSp}_{2g}(\mathbb{Q}_\ell) \to \mathbb{Q}_\ell^*$ ist ein algebraischer Charakter dieser Gruppe.

1.2 Frobenius Eigenwerte

Sei K ein Zahlkörper. Wir betrachten eine endliche Stelle v von K und eine Stelle w von $\overline{K}$ über v. Für die Restklassenkörper k_v und $\overline{k}_w$, die Zerlegungsgruppe $\mathfrak{D}_w$ und die Trägheitsgruppe $\mathfrak{I}_w$ gilt die kurze exakte Sequenz

$$1 \to \mathfrak{I}_w \to \mathfrak{D}_w \to \mathrm{Gal}(\overline{k}_w/k_v) \to 1.$$

Die freie pro-endliche Gruppe $\mathfrak{D}_w/\mathfrak{I}_w \cong \mathrm{Gal}(\overline{k}_w/k_v)$ wird erzeugt durch den Frobeniusautomorphismus. Sei $\mathrm{Frob}_w \in \mathfrak{D}_w$ ein beliebiger Repräsentant dieses Erzeugers.

Sei ℓ eine Primzahl und v eine endliche Stelle von K. Die Darstellung ρ_ℓ heisst *unverzweigt* bei v, falls für alle Stellen w von $\overline{K}$ über v gilt $\rho_\ell(\mathfrak{I}_w) = \{\mathrm{id}\}$. Ist ρ_ℓ unverzweigt bei v, dann ist für alle w das Bild $\rho_\ell(\mathrm{Frob}_w)$ unabhängig von der Wahl des Repräsentanten in $\mathfrak{D}_w$. Die Gruppe $\mathrm{Gal}(\overline{K}/K)$

operiert transitiv auf der Menge aller Stellen über v. Sei w' eine weitere solche Stelle. Aus dem eben Gesagten folgt nun, dass $\rho_\ell(\mathrm{Frob}_w)$ und $\rho_\ell(\mathrm{Frob}_{w'})$ unter $\mathrm{im}(\rho_\ell)$ konjugiert sind, insbesondere besitzen sie dasselbe charakteristische Polynom als Automorphismen von $V_\ell A$. Dieses Polynom hängt also nur von der Stelle v ab, und wir bezeichnen es mit $P_{\ell,v}$.

Theorem 1.4. *Sei S eine endliche Menge von Stellen in K, sodass A ausserhalb von S gute Reduktion besitzt. Nehme an, es gelte $v \notin S$ und $\ell \neq \mathrm{char}(k_v)$.*

(a) *ρ_ℓ ist unverzweigt bei v.*

(b) *Das charakteristische Polynom $P_{\ell,v}$ hat Koeffizienten in $\mathbb{Z}$ und hängt nicht von der Wahl von ℓ ab.*

Beweis. [S-T], Theorem 1 und Theorem 3. □

Dies bedeutet, dass (ρ_ℓ) ein strikt kompatibles System von ganzen, ℓ-adischen Galoisdarstellungen ist, vgl. [Se2], p. I-11. Insbesondere sind alle Frobenius-Eigenwerte (die Nullstellen von $P_{\ell,v}$) ganzalgebraisch und unabhängig von von $\ell \neq \mathrm{char}(k_v)$.

Sei $\overline{\mathbb{Q}}$ ein algebraischer Abschluss von $\mathbb{Q}$. Wir wählen eine feste Einbettung $\overline{\mathbb{Q}} \to \mathbb{C}$ und bezeichnen mit $|\ |_\infty$ den zugehörigen Absolutbetrag. Ebenso wählen wir für jede Primzahl q eine Einbettung von $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_q$ und bezeichnen mit ord_q die induzierte additive Bewertung, normiert durch $\mathrm{ord}_q(q) = 1$. Über die Bewertung der Frobeniuseigenwerte lässt sich folgendes sagen ([**?**, **?**, Pink1] Theorem 3.3):

Theorem 1.5. *Sei $a \in \overline{\mathbb{Q}}$ ein Frobeniuseigenwert an der Stelle $v \notin S$.*

(a) $|a|_\infty = \sqrt{\mathrm{card}(k_v)}$.

(b) $\mathrm{ord}_q(a) = 0$ *für jede Primzahl* $q \neq \mathrm{char}(k_v)$.

(c) $0 \leq \mathrm{ord}_p(a) \leq [k_v/\mathbb{F}_p]$ *für* $p = \mathrm{char}(k_v)$.

Zusätzlich zu der Aussage in (c) gilt

Satz 1.6. *Sei μ die Multiplikatorabbildung auf CSp_{2g} und v eine Stelle vom Grad 1 in K mit $p = \mathrm{char}(k_v) \neq \ell$.*

(a) $\mu(\rho_\ell(\mathrm{Frob}_v)) = p$.

(b) *Nach Umordnen gilt für die $2g$ Frobeniuseigenwerte $a_1, \ldots, a_g, b_1, \ldots, b_g$ an der Stelle v*

$$a_i \cdot b_i = p, \qquad i = 1, \ldots, g.$$

Beweis. (a) Wir müssen zeigen, dass Frob_v auf $\mathbb{Z}_\ell(1) = \varprojlim(\mu_{\ell^n}(\overline{\mathbb{Q}}))$ durch Multiplikation mit p operiert. Da v nicht über ℓ liegt, ist die Reduktionsabbildung $\mu_{\ell^n}(\overline{\mathbb{Q}}) \to \mu_{\ell^n}(\overline{\mathbb{F}}_p)$ ein Isomorphismus. Auf der rechten Seite operiert Frob_v aber durch $x \mapsto x^p$. Die Behauptung folgt nun, da die Reduktionsabbildung galoisäquivariant ist.

(b) Wir benötigen folgendes Lemma:

Lemma 1.7. *Sei F ein beliebiger Körper und V ein F-Vektorraum der Dimension $2g$. Sei E eine nichtausgeartete, alternierende Bilinearform auf V und $g \in \mathrm{GL}(V)$ ein halbeinfaches Element, für das ein $\lambda \neq 0$ existiert mit $E(gv, gw) = \lambda E(v, w)$ für alle $v, w \in V$. Dann haben die $2g$ Eigenwerte von g die Form $\alpha_1, \ldots, \alpha_g$, $\beta_1, \ldots, \beta_g$ mit $\alpha_i\beta_i = \lambda$.*

Beweis. Sei v ein Eigenvektor von g mit Eigenwert α. Das orthogonale Komplement $\langle v\rangle^\perp$ hat Kodimension 1 in V, da E nicht ausgeartet ist, und enthält Fv, da E alternierend ist. Folglich existiert ein Eigenvektor $w \in V \setminus \langle v\rangle^\perp$ mit Eigenwert β. Nun gilt

$$\lambda E(v, w) = E(gv, gw) = E(\alpha v, \beta w) = \alpha\beta E(v, w),$$

wegen $E(v, w) \neq 0$ also $\alpha\beta = \lambda$. V zerlegt sich in die direkte Summe

$$V = \langle v, w\rangle^\perp \oplus \langle v, w\rangle,$$

und E induziert eine nichtausgeartete, alternierende Bilinearform auf dem zweiten Summanden. Die Behauptung folgt nun induktiv. $\square$

Nach (a) genügt es zu zeigen, dass sich die Frobeniuseigenwerte bei v so paaren lassen, dass $a_ib_i = \mu(\mathrm{Frob}_v)$ gilt. Dazu können wir $\rho_\ell(\mathrm{Frob}_v)$ durch dessen halbeinfachen Anteil g ersetzen. Die Behauptung folgt nun aus dem Lemma mit $V = V_\ell A$ und der von (1) induzierten Bilinearform $E : V \times V \to \mathbb{Q}_\ell(1)$. $\square$

1.3 Dichten und der Satz von Cebotarev

Sei K ein Zahlkörper und S eine Menge von endlichen Stellen von K. Die Reihe

$$d(s) = \frac{\sum_{\mathfrak{p}\in S} N\mathfrak{p}^{-s}}{\sum_{\mathfrak{p}} N\mathfrak{p}^{-s}}$$

konvergiert absolut und lokal gleichmässig für $\mathrm{Re}\, s > 1$. Die Menge S hat die *Dirichlet Dichte* $\mathrm{dens}(S)$, falls der Limes $\mathrm{dens}(S) = \lim_{s\to 1+0} d(s)$ existiert. Zum Beispiel besitzt eine endliche Menge von Stellen die Dichte 0, die Menge aller Stellen von K die Dichte 1.

Theorem 1.8 (Cebotarev). *Sei L/K eine endliche Galois Erweiterung von Zahlkörpern mit Galoisgruppe G. Sei $X \subset G$ eine Menge, die invariant ist unter Konjugation. Die Menge der Stellen v in K, die unverzweigt sind in L, und deren Frobeniusklasse Frob_v in X enthalten ist, hat Dirichlet Dichte $\mathrm{card}(X)/\mathrm{card}(G)$.*

Beweis. [Neu] chap. VII, Theorem 13.4. □

Wir benötigen folgendes Resultat:

Theorem 1.9. *Sei K ein Zahlkörper, $G = \mathrm{Gal}(\overline{K}/K)$ und $\Gamma_\ell = \rho_\ell(G) \subset \mathrm{GL}_{2g}(\mathbb{Q}_\ell)$ das Bild von Galois. Sei $C \in \Gamma_\ell$ eine analytische ℓ-adische Untervarietät, die nirgends dicht liegt, und invariant ist unter Konjugation. Dann besitzt die Menge der Stellen v in K, sodass $\rho_\ell(\mathrm{Frob}_v) \in C$, die Dirichlet Dichte 0.*

2 Abelsche Varietäten

In diesem Abschnitt beschäftigen wir uns mit der Pink-Rössler-Vermutung. Wir betrachten eine abelsche Varietät A der Dimension g über einem Zahlkörper K. Sei $\mathfrak{p}$ eine endliche, unverzweigte Stelle von K, an der A gute Reduktion besitzt. Diese Reduktion bezeichnen wir mit $A_\mathfrak{p}$. Sei $k_\mathfrak{p}$ der Restklassenkörper bei $\mathfrak{p}$ und $p = \mathrm{char}(k_\mathfrak{p})$ deren Charakteristik. Über die Anzahl Punkte in der Reduktion $A_\mathfrak{p}$ gibt folgendes Resultat Auskunft:

Sei $v \notin S$ eine Stelle von K, und A_v die Reduktion bei v.

Theorem 2.1. *Seien $a_1, \ldots, a_{2g}$ die Frobeniuseigenwerte bei $\mathfrak{p}$, und sei $k_{\mathfrak{p},m}$ die eindeutig bestimmte Erweiterung des Restklassenkörpers $k_\mathfrak{p}$ vom Grad m. Dann gilt für $m \geq 1$*

$$\mathrm{card}(A_\mathfrak{p}(k_{\mathfrak{p},m})) = \prod_{i=1}^{2g}(1 - a_i^m)$$

Es gilt also genau dann $p \not| \mathrm{card}(A_\mathfrak{p}(k_\mathfrak{p}))$, wenn keiner der $2g$ Frobenius-Eigenwerte bei $\mathfrak{p}$ kongruent zu 1 ist an einer Stelle von $\overline{\mathbb{Q}}$ über p.

2.1 Elliptische Kurven

Theorem 2.2. *Die Vermutung 0.2 ist richtig für elliptische Kurven.*

Beweis. Wir wählen eine feste Primzahl ℓ und betrachten die Menge V_{gut} der endlichen Stellen $\mathfrak{p}$ in K mit folgenden Eigenschaften:

(i) $\mathrm{char}(k_{\mathfrak{p}}) = p \neq \ell$,

(ii) $\mathfrak{p}$ hat Grad 1,

(iii) E besitzt gute Reduktion bei $\mathfrak{p}$,

(iv) $p > 5$.

Die Menge V_{gut} hat Dirichlet Dichte 1. Es genügt zu zeigen, dass die Menge der Stellen $\mathfrak{p} \in V_{\mathrm{gut}}$, für die p ein Teiler ist von $\mathrm{card}(E_{\mathfrak{p}}(k_{\mathfrak{p}}))$, Dirichlet Dicht 0 besitzt. Sei $\mathfrak{p}$ im Folgenden so eine Stelle.

Sei $P_{\ell,\mathfrak{p}}$ das charakteristische Polynom von $\rho_\ell(\mathrm{Frob}_{\mathfrak{p}})$. Nach Theorem 1.4 besitzt dieses ganze Koeffizienten, die beiden Frobeniuseigenwerte α und β sind daher ganzalgebraisch. Sei L der Zerfällungskörper von $P_{\ell,\mathfrak{p}}$ über K und $\widetilde{\mathfrak{p}}$ eine Stelle von L über $\mathfrak{p}$.

Nach Theorem 2.1(a) und (ii) gilt

$$\mathrm{card}(E_{\mathfrak{p}}(k_{\mathfrak{p}})) = (1-\alpha)(1-\beta).$$

Nach Voraussetzung ist p ein Teiler der rechten Seite dieser Gleichung. Wegen Theorem 1.6 können wir ausserdem annehmen, dass $\beta \equiv 0 \pmod{\widetilde{\mathfrak{p}}}$ gilt. Folglich ist $\alpha \equiv 1 \pmod{\widetilde{\mathfrak{p}}}$. Die Zahl $\mathrm{tr} - 1 = \alpha + \beta - 1$ ist ganz und nach dem eben Gesagten gilt $\mathrm{ord}_{\widetilde{\mathfrak{p}}}(\mathrm{tr} - 1)$. Daher gilt sogar

$$p \mid \mathrm{tr} - 1. \tag{2}$$

Nach Theorem 1.5 (a) und (iv) haben wir ausserdem

$$|\,\mathrm{tr} - 1|_\infty \leq |\alpha|_\infty + |\beta|_\infty + 1 = 2\sqrt{p} + 1 < p.$$

Aus (1) und dieser Abschätzung folgt unmittelbar $\mathrm{tr} - 1 = 0$.

Wir zeigen nun, dass der Morphismus $f : \mathrm{GL}_2(\mathbb{Q}_\ell \to \mathbb{Q}_\ell$, $m \mapsto \mathrm{tr}(m) - 1$ auf keiner Zusammenhangskomponente von G_ℓ identisch verschwindet. Nach Theorem... enthält G_ℓ° die Skalare. Wir fixieren eine Zusammenhangskomponente von G_ℓ und ein Element m darin. Für jedes skalare Element σ liegen m und σm in derselben Komponente von G_ℓ und es gilt

$$f(\sigma m) = \mathrm{tr}(m)\sigma - 1.$$

Daher ist f surjektiv oder konstant 1 auf mG_ℓ°, verschwindet also nicht identisch.

Das Urbild $f^{-1}(0)$ ist eine abgeschlossene Untervarietät von G_ℓ, die keine Zusammenhangskomponente enthält. Daher ist $C = f^{-1}(0) \cap \Gamma_\ell$ eine analytische ℓ-adische Untervarietät von Γ_ℓ, die nirgends dicht liegt. Ausserdem ist C invariant unter Konjugation. Die Behauptung folgt nun aus dem Satz von Cebotarev, Theorem 1.9. $\square$

2.2 Der allgemeine Fall

Theorem 2.3. *Sei A/K eine abelsche Varietät der Dimension $g \geq 2$. Dann gibt es eine Menge V von endlichen Stellen von K der Dirichlet Dichte 1, sodass für alle $\mathfrak{p} \in V$ gilt: Seien $\alpha_1, \ldots, \alpha_{2g}$ die Eigenwerte von $\rho_\ell(\mathrm{Frob}_\mathfrak{p})$ und sei $\widetilde{\mathfrak{p}}$ eine Stelle über $\mathfrak{p}$ im Zerfällungskörper von $P_{\ell,v}$ über K; dann sind höchstens $g-2$ der Frobeniuseigenwerte kongruent zu $1 \pmod{\widetilde{\mathfrak{p}}}$.*

Beweis. Wir wählen eine feste Primzahl ℓ und betrachten die Menge V_{gut} der endlichen Stellen $\mathfrak{p}$ in K mit folgenden Eigenschaften:

(i) $p = \mathrm{char}(k_\mathfrak{p}) \neq \ell$,

(ii) $\mathfrak{p}$ hat Grad 1,

(iii) A besitzt gute Reduktion bei $\mathfrak{p}$,

(iv) $p \geq 4g^2$.

Die Menge V_{gut} hat Dirichlet Dichte 1. Es genügt daher zu zeigen, dass die Menge der Stellen $\mathfrak{p} \in V_{\mathrm{gut}}$, für die mindestens $g-1$ Frobeniuseigenwerte α_i kongruent zu $1 \pmod{\widetilde{\mathfrak{p}}}$ sind, Dirichlet Dichte 0 besitzt. Sei $\mathfrak{p}$ eine solche Stelle.

Wegen Theorem 1.6 können wir annehmen, dass gilt

$$\alpha_1 \equiv \ldots \equiv \alpha_g \equiv 0, \qquad \alpha_{g+1} \equiv \ldots \equiv \alpha_{2g-1} \equiv 1 \qquad \pmod{\widetilde{\mathfrak{p}}}$$

und setzen zur Abkürzung $\alpha = \alpha_{2g}$. Sei s_k das k-te elementarsymmetrische Polynom in den α_i (insbesondere ist $s_1 = -\mathrm{tr}$), nach Theorem 1.4 ist $s_k \in \mathbb{Z}$. Nach Voraussetzung gilt nun

$$s_1 \equiv g - 1 + \alpha \qquad \pmod{\widetilde{\mathfrak{p}}},$$

sowie

$$s_2 \equiv \prod_{g<i<j<2g} \alpha_i\alpha_j + \alpha \prod_{i=g+1}^{2g-1} \alpha_i \equiv \binom{g-1}{2} + (g-1)\alpha, \qquad \pmod{\widetilde{\mathfrak{p}}}.$$

Die ganze Zahl

$$f(\mathfrak{p}) = s_2 - (g-1)s_1 + g(g-1)/2$$

ist daher durch $\widetilde{\mathfrak{p}}$ und somit auch durch p teilbar. Mit Hilfe von Theorem 1.5(a) und (ii) lässt sich der Absolutbetrag von $f(\mathfrak{p})$ wie folgt abschätzen:

$$\begin{aligned} |f(\mathfrak{p})|_\infty &\leq |s_2|_\infty + (g-1)|s_1|_\infty + g(g-1)/2 \\ &\leq g(2g-1)p + 2g(g-1)\sqrt{p} + g(g-1)/2 \\ &< 2pg^2, \end{aligned}$$

dabei folgt die letzte Ungleichung aus (iv). Insgesamt gilt daher eine Gleichung der Form

$$f(\mathfrak{p}) = ap, \tag{3}$$

wobei a eine ganze Zahl ist mit $|a| < 2pg^2$.

Sei nun a eine ganze Zahl mit $|a| \leq 2g^2p$. Wir betrachten die endlich vielen Morphismen $f_a : \mathrm{CSp}_{2g}(\mathbb{Q}_\ell) \to \mathbb{Q}_\ell$, die definiert sind durch

$$f_a(m) = s_2(m) - (g-1)s_1(m) - a\mu(m) + g(g-1)/2,$$

wobei $\mu : \mathrm{CSp}_{2g}(\mathbb{Q}_\ell) \to \mathbb{Q}_\ell$ die Multiplikatorabbildung ist. Aus (2) folgt, dass $\rho_\ell(\mathrm{Frob}_\mathfrak{p})$ von einem dieser Morphismen auf 0 abgebildet wird, denn der Multiplikator dieses Elementes ist gleich p.

Wir zeigen nun, dass f_a auf keiner Zusammenhangskomponente von G_ℓ identisch verschwindet. Nach Theorem 1.3 können wir ein skalar operierendes Element $\sigma \in G_\ell^\circ$ unendlicher Ordnung wählen. Wir fixieren eine Zusammenhangskomponente von G_ℓ und ein Element m darin. Es gilt

$$f_a(\sigma^k m) = (s_2(m) - a\mu(m))(\sigma^k)^2 - (g-1)s_1(m)(\sigma^k) + g(g-1)/2.$$

Die rechte Seite ist ein quadratisches Polynom in σ^k, dessen konstanter Koeffizient nicht verschwindet. Da σ unendliche Ordnung hat, kann f_a auf der gewählten Komponente von G_ℓ nicht identisch verschwinden.

Das Urbild $f_a^{-1}(0)$ ist eine abgeschlossene Untervarietät von G_ℓ, die keine Zusammenhangskomponente enthält. Daher ist $C = f^{-1}(0) \cap \Gamma_\ell$ eine analytische ℓ-adische Untervarietät von Γ_ℓ, die nirgends dicht liegt. Ausserdem ist C invariant unter Konjugation. Die Behauptung folgt nun aus dem Satz von Cebotarev, Theorem 1.9. $\square$

Korollar 2.4. *Sei A eine abelsche Fläche über K. Die Vermutung 0.2 stimmt für A.*

2.3 Ein Beispiel in Dimension 4

Wir geben hier ein Beispiel, das zeigt, dass die verwendete Methode allgemein nicht zu einer stärkeren Aussage führt, als jener in Theorem 2.3.

Wir arbeiten im Folgenden über $\overline{\mathbb{Q}}_\ell$. Sei A/K eine abelsche Varietät der Dimension 4, sodass das Bild von Galois enthalten ist in der Gruppe

$$\mathbb{G}_m \cdot \mathrm{SL}_2 \cdot \mathrm{SL}_2 \cdot \mathrm{SL}_2 \subset \mathrm{GL}_8(\overline{\mathbb{Q}}_\ell).$$

Die tautologische Darstellung dieser Gruppe ist gegeben durch $\mathrm{std}_1 \otimes \mathrm{std}_2 \otimes \mathrm{std}_2 \otimes \mathrm{std}_2$. Die Elemente in Γ_ℓ operieren als

$$\lambda \cdot \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^{-1} \end{pmatrix} \otimes \begin{pmatrix} \beta & 0 \\ 0 & \beta^{-1} \end{pmatrix} \otimes \begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix},$$

wobei $\lambda, \alpha, \beta, \gamma \in \overline{\mathbb{Q}}_\ell$. Die Eigenwerte sind gegeben durch $\lambda \cdot \alpha^{\pm 1}\beta^{\pm 1}\gamma^{\pm 1}$ und die Wurzeln durch $\alpha^{\pm 2}, \beta^{\pm 2}, \gamma^{\pm 2}$.

Sei $\mathfrak{p}$ eine Stelle von K vom Grad 1, an der A gute Reduktion besitzt, und die nicht über ℓ liegt. Sei $p = \mathrm{char}(k_\mathfrak{p}$. Nach Theorem 1.5 gilt für die Bewertungen der Frobeniuseigenwerte $\lambda \cdot \alpha^{\pm 1}\beta^{\pm 1}\gamma^{\pm 1}$ bei $\mathfrak{p}$

(a) $|\lambda \cdot \alpha^{\pm 1}\beta^{\pm 1}\gamma^{\pm 1}|_\infty = \sqrt{p}$.

(b) $\mathrm{ord}_q(\lambda \cdot \alpha^{\pm 1}\beta^{\pm 1}\gamma^{\pm 1}) = 0$ für jede Primzahl $q \neq p$.

(c) $0 \leq \mathrm{ord}_p(\lambda \cdot \alpha^{\pm 1}\beta^{\pm 1}\gamma^{\pm 1}) \leq 1$.

Ausserdem ist λ^2 das Bild von $\mathrm{Frob}_\mathfrak{p}$ auf $\mathbb{Q}_\ell(1)$, also gleich p. Daraus folgt $\mathrm{ord}_p(\lambda) = 1/2$.

Aus (a) folgt sofort

$$|\lambda|_\infty = \sqrt{p}, \quad |\alpha|_\infty = |\beta|_\infty = |\gamma|_\infty = 1. \tag{4}$$

Mit (b) erhält man für alle $q \neq p$

$$\mathrm{ord}_q(\lambda) = \mathrm{ord}_q(\alpha) = \mathrm{ord}_q(\beta) = \mathrm{ord}_q(\gamma) = 0. \tag{5}$$

Mit (c) und $\mathrm{ord}_p(\lambda) = 1/2$ folgt $-1/2 \leq \mathrm{ord}_p(\alpha^{\pm 1}\beta^{\pm 1}\gamma^{\pm 1}) \leq 1/2$ und somit $\mathrm{ord}_p(\alpha^2) = \mathrm{ord}_p((\alpha\beta\gamma)/(\alpha^{-1}\beta\gamma)) \in [-1, 1]$. Nachdem man gegebenfalls α, β, γ umordnet oder durch die Inversen ersetzt, gilt also

$$0 \leq \mathrm{ord}_p(\alpha) \leq \mathrm{ord}_p(\beta) \leq \mathrm{ord}_p(\gamma) \leq 1/2. \tag{6}$$

Ausserdem ist $\mathrm{ord}_p(\alpha\beta\gamma) = \mathrm{ord}_p((\lambda\alpha\beta\gamma)/\gamma) \leq 1 - 1/2 = 1/2$. Wir nehmen nun zusätzlich an, dass A bei $\mathfrak{p}$ gewöhnliche Reduktion besitzt. Nach Übergang zu einer endlichen Erweiterung von K besitzt die Menge dieser Stellen Dirichlet Dichte 1, vgl. [Pi1] Theorem 7.1. Dann können wir (5) ersetzen durch

$$\mathrm{ord}_p(\alpha) = \mathrm{ord}_p(\beta) = 0, \quad \mathrm{ord}_p(\gamma) = 1/2. \tag{7}$$

Nach Theorem 2.3 sind höchstens 2 der Frobeniuseigenwerte kongruent zu 1 an der Stelle über $\mathfrak{p}$ für alle Stellen $\mathfrak{p}$ in einer Menge der Dirichlet Dichte 1. Wir wollen dieses Resultat nun zu verbessern versuchen. Dazu versuchen wir auszuschliessen, dass zwei Eigenwerte kongruent zu 1 sind.

Die Eigenwerte $\lambda\alpha^{\pm 1}\beta^{\pm 1}\gamma$ sind kongruent zu 0. Es gibt im Wesentlichen zwei Fälle:

1. $\lambda\alpha\beta\gamma^{-1} \equiv \lambda\alpha\beta^{-1}\gamma^{-1} \equiv 1$,

2. $\lambda\alpha\beta\gamma^{-1} \equiv \lambda\alpha^{-1}\beta^{-1}\gamma^{-1} \equiv 1$.

Wir betrachten nur den zweiten Fall. Es folgt, dass $\alpha^2\beta^2 \equiv \lambda^2\gamma^2 \equiv 1$ gilt. Wir versuchen nun auszuschliessen, dass $\mathrm{ord}_p(\alpha^2\beta^2 - 1) > 0$ ist. Dazu brauchen wir ein Polynom $P \in \mathbb{Q}[\alpha^{\pm 1}, \beta^{\pm 1}, \gamma^{\pm 1}, \lambda]$, welches folgende Bedingungen erfüllen soll:

(i) P ist symmetrisch in $\alpha^{\pm 1}, \beta^{\pm 1}, \gamma^{\pm 1}$,

(ii) Jedes Monom von P ist ein Produkt von Frobenius-Eigenwerten und $p = \lambda^2$ oder ihren Inversen,

(iii) $|M|_\infty \leq d \cdot p$ mit einer Konstanten d, für jedes Monom M,

(iv) $\mathrm{ord}_p(M) \geq 0$ für jedes Monom M,

(v) P ist durch das Polynom $(\alpha^2\beta^2 - 1)$ teilbar.

Sei $M = \lambda^n\alpha^a\beta^b\gamma^c$ ein Momom von P. Wegen (ii) gilt $n \equiv a \equiv b \equiv c \pmod 2$. Aus $\mathrm{ord}_p(M) = (n+c)/2$ und (iv) folgt $n+c \geq 0$, wegen der Symmetrie in (i) ist daher $|a|, |b|, |c| \leq n$. Aus $|M|_\infty = p^{n/2}$ und (iii) erhalten wir schliesslich $n \leq 2$. Aus diesen Bedingungen folgt, dass M eines der folgenden Monome ist:

$$\begin{gathered} 1, \quad \lambda\alpha^{\pm 1}\beta^{\pm 1}\gamma^{\pm 1}, \quad \lambda^2, \quad \lambda^2\alpha^{\pm 2}, \lambda^2\beta^{\pm 2}, \lambda^2\gamma^{\pm 2}, \\ \lambda^2\alpha^{\pm 2}\beta^{\pm 2}, \lambda^2\beta^{\pm 2}\gamma^{\pm 2}, \lambda^2\gamma^{\pm 2}\alpha^{\pm 2}, \\ \lambda^2\alpha^{\pm 2}\beta^{\pm 2}\gamma^{\pm 2}, \end{gathered}$$

dabei sind stets alle Vorzeichenkombinationen möglich.

Die Polynome $(\alpha^2\beta^2-1)$, $(\beta^2\gamma^2-1)$ und $(\gamma^2\alpha^2-1)$ sind teilerfremd. Da P durch das erste teilbar ist, muss P aus Symmetriegründen auch durch ihr Produkt teilbar sein. Ein Blick auf die Exponenten von α, β und γ in diesem Produkt zeigt, dass P keine $\mathbb{Q}$-linearkombination von Monomen aus obiger Liste sein kann.

3 Drinfeld Moduln

Wir betrachten nun die analoge Situation für Drinfeld Moduln. Sei $\mathbb{F}$ ein endlicher Körper der Charakteristik p und $K/\mathbb{F}$ eine endlich erzeugte Körpererweiterung von $\mathbb{F}$ mit Transzendenzgrad 1. Wir können annehmen, dass $\mathbb{F}$ der Konstantenkörper von K ist, also algebraisch abgeschlossen in K. Sei ∞ eine fest gewählte Stelle vom Grad d_∞ in K und A der Unterring der ausserhalb von ∞ regulären Funktionen. Wir betrachten eine endliche Körpererweiterung L von K und einen Drinfeld Modul

$$\varphi : A \to \mathrm{End}_k(\mathbb{G}_{a,L})$$

vom Rang n. Die Strukturabbildung $i : A \to L$ ist die Inklusion, also hat φ generische Charakteristik. Wir wählen einen algebraischen Abschluss $\overline{L}$ von L. Sei $L^{\mathrm{sep}} \subset \overline{L}$ der separable Abschluss von L. Für eine Stelle $\lambda \neq \infty$ von K bezeichnen K_λ und A_λ die Vervollständigungen von K und A bei λ.

Für ein Ideal $I \in A$ bezeichne $\varphi[I]$ die Menge der Elemente des A-Moduls $\overline{L}$, die von allen $x \in I$ annulliert werden. $\varphi[I]$ ist ein endlicher A/I-Modul (die I-Torsion in $\overline{L}$). Sei nun $\lambda \neq \infty$ eine Stelle von K und $\mathfrak{p}_\lambda$ das zugehörige maximale Ideal in A. Der projektive Limes bezüglich der kanonischen Abbildungen $\varphi[\mathfrak{p}_\lambda^{m+1}] \to \varphi[\mathfrak{p}_\lambda^m]$,

$$T_\lambda(\varphi) = \varprojlim \varphi[\mathfrak{p}_\lambda^m],$$

ist der λ-*adische Tate Modul* von φ. Der Tate Modul ist ein freier A_λ-Modul vom Rang n (φ hat generische Charakteristik). Ausserdem gibt die Operation von $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ auf den Moduln $\varphi[\mathfrak{p}_\lambda^m]$ Anlass zu einer stetigen Operation auf dem Tate Modul. Nach Wahl einer Basis in $T_\lambda(\varphi) \otimes_{A_\lambda} K_\lambda$ liefert dies eine stetige Darstellung

$$\rho_\lambda : \mathrm{Gal}(L^{\mathrm{sep}}/L) \longrightarrow \mathrm{GL}_n(K_\lambda).$$

Zentral ist die Grösse des Bildes von ρ_λ in $\mathrm{GL}_n(F_\lambda)$. Beachte, dass der Endomorphismenring $\mathrm{End}_L(\varphi)$ auf dem Tate Modul operiert, und dass diese Operation verträglich ist mit der Operation der Galoisgruppe $\mathrm{Gal}(L^{\mathrm{sep}}/L)$.

Folglich liegt das Bild von ρ_λ im Zentralisator $\mathrm{Cent}_{\mathrm{GL}_n(K_\lambda)}(\mathrm{End}_L(\varphi))$. Nach Übergang zu einer endlichen Erweiterung von L können wir annehmen, dass $\mathrm{End}_{\overline{L}}(\varphi) = \mathrm{End}_L(\varphi)$. Es gilt nun

Theorem 3.1. *Nehme an, es gelte* $\mathrm{End}_{\overline{L}}(\varphi) = \mathrm{End}_L(\varphi)$. *Dann hat die Abbildung*

$$\mathrm{Gal}(L^{\mathrm{sep}}/L) \longrightarrow \mathrm{Cent}_{\mathrm{GL}_n(K_\lambda)}(\mathrm{End}_L(\varphi))$$

offenes Bild.

Für einen Beweis siehe [Pi2], Theorem 0.2. Sei G_λ der Zariskiabschluss von $\rho_\lambda(\mathrm{Gal}(L^{\mathrm{sep}}/L))$. In der Situation des Theorems enthält G_λ ein skalar operierendes Element m unendlicher Ordnung. Dies gilt nun aber auch ohne Übergang zu einer endlichen Erweiterung von L, denn ein solcher Übergang verkleinert das Bild von Galois. Ausserdem können wir annehmen, dass m in der Einskomponente G_λ° liegt (ersetze m gegebenenfalls durch eine geeignete Potenz).

Für jede Stelle v von L wählen wir eine feste Fortsetzung $\overline{v}$ auf $\overline{L}$. Zwei solche Fortsetzungen unterscheiden sich nur um einen Automorphismus von $\overline{L}$ über L. Sei $G = \mathrm{Gal}(L^{\mathrm{sep}}/L)$ und $\mathfrak{I}_{\overline{v}}$ die Trägheitsgruppe von G bei $\overline{v}$. Wir erinnern daran, dass eine Darstellung von G *unverzweigt* ist bei v, wenn $\mathfrak{I}_{\overline{v}}$ im Kern dieser Darstellung liegt. Diese Eigenschaft ist unabhängig von der gewählten Erweiterung $\overline{v}$, da die Trägheitsgruppen zu verschiedenen Erweiterungen konjugiert sind in G. Über die Verzweigtheit der Darstellung ρ_λ gibt folgendes Resultat Auskunft.

Satz 3.2. *φ hat genau dann gute Reduktion bei v, wenn die Darstellung ρ_λ unverzweigt ist bei v.*

Sei v eine Stelle von L, an der φ gute Reduktion besitzt, und $\overline{v}$ sei wieder eine Fortsetzung auf $\overline{L}$. Sei $\mathfrak{I}_{\overline{v}}$ die Trägheitsgruppe und $\mathfrak{D}_{\overline{v}}$ die Zerlegungsgruppe bei $\overline{v}$. Wir fixieren ein erzeugendes Element Frob_v von $\mathfrak{D}_{\overline{v}}/\mathfrak{I}_{\overline{v}}$, einen *Frobeniusautomorphismus* zu v. Nach Wahl von v ist das Bild $\rho_\lambda(\mathrm{Frob}_v)$ wohldefiniert. Ausserdem führt eine andere Wahl der Fortsetzung $\overline{v}$ zu einem Frobeniusautomorphismus, der in derselben Konjugationsklasse von G liegt. Daher ist das charakteristische Polynom von $\rho_\lambda(\mathrm{Frob}_v)$ unabhängig von allen getroffenen Wahlen. Wir bezeichnen die Stelle von K unter v mit λ_v.

Theorem 3.3. *Das charakteristische Polynom von $\rho_\lambda(\mathrm{Frob}_v)$ hat Koeffizienten in A und ist unabhängig von λ, solange $\lambda \neq \lambda_v, \infty$.*

Sei $\overline{K}$ ein algebraischer Abschluss von K und seien $\alpha_1, \ldots, \alpha_n \in \overline{K}$ die Eigenwerte von $\rho_\lambda(\mathrm{Frob}_v)$. Betrachte eine Stelle λ_1 von K und eine Fortsetzung

$\overline{\lambda}_1$ auf $\overline{K}$. Die Bewertung $\mathrm{ord}_{\overline{\lambda}_1}$ sei so normiert, dass ein Uniformisierendes von λ_1 in K Bewertung 1 hat. Sei ℓ_v der Restklassenkörper von L bei v. Über die Bewertungen der α_i ist folgendes bekannt.

Theorem 3.4. (a) *Es gilt* $\mathrm{ord}_{\overline{\lambda}_1}(\alpha_i) = 0$ *für alle* $1 \leq i \leq n$ *und alle* $\lambda_1 \neq \lambda_v, \infty$.

(b) *Für* $1 \leq i \leq n$ *gilt* $\mathrm{ord}_{\overline{\infty}}(\alpha_i) = -[\ell_v : \mathbb{F}]/(n \cdot d_\infty)$.

(c) *Für* $1 \leq i \leq n$ *gilt* $\mathrm{ord}_{\overline{\lambda}_v}(\alpha_i) \geq 0$.

Schliesslich benötigen wir noch ein Analogon der Aussage, dass die Menge der Primstellen vom Grad 1 in einem Zahlkörper Dirichlet Dichte 1 hat.

Theorem 3.5. *(Siehe [Pi2], prop. B8) Es gibt eine Menge von Stellen v in L der Dirichlet Dichte 1, für die gilt*

$$[\ell_v : k_{\lambda_v}] = 1.$$

Nach diesen Vorbereitungen können wir das Hauptresultat dieses Abschnittes beweisen.

Theorem 3.6. *Für eine Menge von Stellen v von L der Dirichlet Dichte 1 ist keiner der n Frobeniuseigenwerte kongruent zu 1 modulo der Stelle über λ_v von $\overline{K}$.*

Beweis. Für das folgende sei $\lambda \neq \infty$ eine fest gewählte Stelle von K. Sei V_{gut} die Menge der Stellen v von L mit folgenden Eigenschaften:

(i) v liegt nicht über λ oder ∞,

(ii) φ besitzt gute Reduktion bei v,

(iii) $[\ell_v : k_{\lambda_v}] = 1$.

Nach Theorem 3.5 hat V_{gut} Dirichlet Dichte 1. Für $v \in V$ ist das charakteristische Polynom $\mathrm{chp}_v(x) = \det(x - \rho_\lambda(\mathrm{Frob}_v))$ von Frob_v wohldefiniert und hat Koeffizienten in A. Es genügt zu zeigen, dass die Menge der Stellen $v \in V_{\mathrm{gut}}$, für welche mindestens eine der Nullstellen $\alpha_1, \ldots, \alpha_n$ von chp_v kongruent zu 1 ist an der Stelle über λ_v, Dichte 0 hat. Sei nun v eine solche Stelle.

Das Produkt $P = \alpha_1 \cdots \alpha_n$ liegt in A und hat nach Theorem 3.4 die Bewertungen $\mathrm{ord}_{\lambda_1}(P) = 0$ für $\lambda_1 \neq \lambda_v, \infty$, $\mathrm{ord}_\infty(P) = -[\ell_v : \mathbb{F}]/d_\infty$ und $\mathrm{ord}_{\lambda_v}(P) \geq 0$. Die Produktformel liefert nun $\mathrm{ord}_{\lambda_v}(P) = [\ell_v : k_{\lambda_v}] = 1$.

Setze $S = \prod_{i=1}^{n}(1-\alpha_i) = \mathrm{chp}_v(1) \in A$. Es gilt $\mathrm{ord}_{\lambda_1}(S) \geq 0$ für $\lambda_1 \neq \lambda_v, \infty$, sowie $\mathrm{ord}_\infty(S) = -[\ell_v : \mathbb{F}]/d_\infty$ nach Theorem 3.4. Nach Voraussetzung an v ist ausserdem $\mathrm{ord}_{\lambda_v}(S) \geq 1$. Die Produktformel für S liefert nun

$$0 = \sum_{\lambda_1 \neq \lambda_v, \infty} \mathrm{ord}_{\lambda_1}(S) \cdot [k_{\lambda_1} : \mathbb{F}] + \mathrm{ord}_{\lambda_v}(S) \cdot [k_{\lambda_v} : \mathbb{F}] - [\ell_v : \mathbb{F}].$$

Wegen $[\ell_v : k_{\lambda_v}] = 1$ folgt daraus

$$\sum_{\lambda_1 \neq \lambda_v, \infty} \mathrm{ord}_{\lambda_1}(S) \cdot [k_{\lambda_1} : \mathbb{F}] = [\ell_v : \mathbb{F}](1 - \mathrm{ord}_{\lambda_v}(S)).$$

Die linke Seite dieser Gleichung ist ≥ 0, die rechte nach Voraussetzung aber ≤ 0. Daraus folgt, dass S und P dieselben Bewertungen haben an allen Stellen von K. Somit gilt $S = aP$ für eine konstante Funktion $a \in \mathbb{F}^*$.

Wir zeigen nun, dass die Gleichung $S = aP$ auf keiner Zusammenhangskomponente von G_λ identisch erfüllt sein kann. Sei $g \in \mathrm{GL}_n(K_\lambda)$ beliebig. Das charakteristische Polynom von g ist von der Form

$$x^n + c_1(g)x^{n-1} + c_2(g)x^{n-2} + \ldots + c_n g,$$

wobei c_i ein Polynom in den Matrixeinträgen von g ist, genauer: c_i ist bis auf das Vorzeichen das i-te Elementarsymmetrische Polynom in den Eigenwerten von g. Für jede der endlich vielen Konstanten $a \in \mathbb{F}^*$ definieren wir einen Morphismus

$$f_a : \mathrm{GL}_n(K_\lambda) \to \mathbb{A}^1, \qquad g \mapsto \det(1-g) - a\det(g).$$

Betrachte eine Zusammenhangskomponente gG_λ° von G_λ und wähle ein skalares Element $m = \mu \cdot 1$ unendlicher Ordnung in G_λ° (siehe Bemerkung nach Theorem 3.1). Die Elemente $m^j g$ liegen alle in gG_λ° und es gilt

$$f_a(m^j g) = 1 + \sum_{i=1}^{n-1} c_i(g) \cdot (\mu^j)^i + (1-a)c_n(g) \cdot (\mu^j)^n.$$

Die rechte Seite ist ein nichtkonstantes Polynom in μ^j und nimmt daher unendlich viele Werte an. Folglich ist f_a auf keiner Zusammenhangskomponente von G_λ konstant.

Das Urbild $f_a^{-1}(0) \cap \mathrm{im}\,\rho_\ell$ ist daher eine nirgends dichte analytische Untervarietät von $\mathrm{im}\,\rho_\ell$ und ausserdem invariant unter Konjugation. Die Behauptung folgt nun wieder aus dem Satz von Cebotarev. $\square$

4 Varietäten mit imaginärquadratischer komplexer Multiplikation

4.1 Stellen gewöhnlicher Reduktion

Sei K ein imaginärquadratischer Zahlkörper und L eine endliche Erweiterung. In diesem Abschnitt betrachten wir eine abelsche Varietät A über L mit $\operatorname{End} A = \mathcal{O}_K$. Wir wählen eine feste Primzahl ℓ, die träge ist in K, und setzen $K_\ell = K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Dies ist ein ℓ-adischer Zahlkörper vom Grad 2. Sei $x \mapsto \overline{x}$ der nichttriviale Galoisautomorphismus von K_ℓ.

Das Bild der ℓ-adischen Darstellung

$$\rho_\ell : \operatorname{Gal}(\overline{L}/L) \longrightarrow \operatorname{GL}_{2g}(\mathbb{Q}_\ell)$$

bezeichnen wir mit Γ_ℓ und den Zariskiabschluss in $\operatorname{GL}_{2g}(\mathbb{Q}_\ell)$ mit G_ℓ. Nach Theorem 1.1 gilt

$$K_\ell \cong \operatorname{End} A \otimes \mathbb{Q}_\ell \cong \operatorname{End}_{\mathbb{Q}_\ell[\operatorname{Gal}(\overline{L}/L)]} V_\ell A. \tag{8}$$

Die Operation von $\mathcal{O}_K$ auf dem rationalen Tate-Modul $V_\ell A$ vertauscht mit der Operation von $\operatorname{Gal}(\overline{L}/L)$, daher trägt $V_\ell A$ die Struktur eines K_ℓ-Vektorraums. Die alternierende Bilinearform auf V_ℓ, die von der Weil-Paarung stammt, induziert eine Hermitesche Form H auf diesem Raum. Man kann zeigen, dass G_ℓ in der Gruppe der unitären Ähnlichkeiten $\operatorname{CU}(H)$ dieser Form liegt. H habe die Signatur (n, m). Nach geeigneter Basiswahl in $V_\ell A$ liegt G_ℓ daher in

$$\operatorname{CU}(n,m) = \{x \in \operatorname{GL}_{n+m}(K_\ell) \mid \overline{x}^{\,t} J x = \lambda \cdot J,\ \lambda \in K_\ell^*\},$$

wobei

$$J = \begin{pmatrix} I_n & 0 \\ 0 & -I_m \end{pmatrix}.$$

$\operatorname{CU}(m,n)$ ist eine algebraische Gruppe über $\mathbb{Q}_\ell$. Wir sagen in dieser Situation, dass die Galoisdarstellung von A *vom Typ* (m,n) ist.

Im Folgenden nehmen wir stets an, dass die Darstellung ρ_ℓ vom Typ $(n,1)$ ist. Sei $\mathfrak{q}$ eine Stelle in L vom Grad 1. Die Stellen unter $\mathfrak{q}$ in K und $\mathbb{Q}$ seien $\mathfrak{p}$ und p. $\mathfrak{p}$ hat ebenfalls Grad 1, und wir bezeichnen die andere Stelle in K über p mit $\mathfrak{p}'$. Das charakteristische Polynom von $\rho_\ell(\operatorname{Frob}_\mathfrak{q})$ über K_ℓ hat Koeffizienten in K. Die Eigenwerte von $\rho_\ell(\operatorname{Frob}_\mathfrak{q})$ über K_ℓ bezeichnen wir mit $\alpha_1, \ldots, \alpha_{n+1}$. Die Eigenwerte über $\mathbb{Q}_\ell$ sind dann gegeben durch

$$\alpha_1, \ldots, \alpha_{n+1}, \beta_1 = \overline{\alpha_1}, \ldots, \beta_{n+1} = \overline{\alpha_{n+1}},$$

und es gilt $\alpha_i\beta_i = p$ für $i = 1, \ldots, n+1$ (Satz 1.6). Zusätzlich zu den Aussagen in Theorem 1.5 ist ausserdem bekannt, dass das Newtonpolygon des charakteristischen Polynoms von $\rho_\ell(\mathrm{Frob}_\mathfrak{q})$ bezüglich der Bewertung bei $\mathfrak{p}$ über dem Hodgepolynom liegt. Letzteres besteht eus einem horizontalen Segment der x-Länge n und einem Segment der x-Länge 1 mit Steigung 1.

Wir wählen eine Elliptische Kurve E über L mit $\operatorname{End} E = \mathcal{O}_K$, sodass die ℓ-adische Galoisdarstellung

$$\tau_\ell : \mathrm{Gal}(\overline{L}/L) \to V_\ell E \cong K_\ell$$

vom Typ $\mathrm{CU}(1,0)$ ist. Wir betrachten nun die Darstellung

$$\delta : \mathrm{Gal}(\overline{L}/L) \to V_\ell A \times V_\ell E.$$

Den Zariskiabschluss von $\operatorname{im} \delta$ bezeichnen wir mit G. Nach Konstruktion ist $G \subset \mathrm{CU}(n,1) \times \mathrm{CU}(1,0)$.

Wir rekapitulieren kurz den Zusammenhang zwischen diagonalisierbaren Gruppen und ihren Charaktergruppen. Dabei beschränken wir uns auf Gruppen, die über $\mathbb{Q}$ definiert sind.
Eine über $\mathbb{Q}$ definierte algebraische Gruppe G heisst diagonalisierbar, falls $G_{\overline{\mathbb{Q}}}$ über $\overline{\mathbb{Q}}$ isomorph ist zu einer Untergruppe von $D(k, \overline{\mathbb{Q}})$ für ein geeignetes k. Bekanntlich gilt dann $G_{\overline{\mathbb{Q}}} \cong \mathbb{G}^r_{m,\overline{\mathbb{Q}}} \times H$ mit einer endlichen Gruppe H. Ist G ein Torus, dann ist $H = 1$. Die Charaktergruppe $X^*(G)$ ist die Gruppe aller Homomorphismen $\chi : G_{\overline{\mathbb{Q}}} \to \mathbb{G}_{m,\overline{\mathbb{Q}}}$, die über $\overline{\mathbb{Q}}$ definiert sind. Wir schreiben $X^*(G)$ stets additiv. $X^*(G)$ ist endlich erzeugt und abelsch. Für $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ und $\chi \in X^*(G)$ definieren wir $\chi^\sigma \in X^*(G)$ durch $\chi^\sigma(x) = \sigma(\chi(\sigma^{-1}x))$. Dies ergibt eine stetige Operation der Galoisgruppe. Der kontravariante Funktor $G \mapsto X^*(G)$ von der Kategorie der diagonalisierbaren Gruppen über $\mathbb{Q}$ in die Kategorie der endlich erzeugten $\mathbb{Z}[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-Moduln ist in der Tat eine Äquivalenz von Kategorien. Dabei entsprechen die Tori genau den torsionsfreien Moduln.

Sei T ein Torus über $\mathbb{Q}$ und T' eine algebraische Untergruppe. Wir fixieren ein Element $t \in T(\mathbb{Q})$ und definieren T' als den Zariskiabschluss der von t erzeugten Untergruppe in T. Für jede Stelle λ in $\overline{\mathbb{Q}}$ definieren wir einen Homomorphismus

$$w_\lambda : X^*(T) \to \mathbb{R}, \quad \chi \mapsto \log |\chi(t)|_\lambda.$$

Lemma 4.1. *Charakter $\chi \in X^*(T)$ liegt genau dann in $\bigcap_\lambda \ker w_\lambda$, wenn ein Vielfaches davon trivial ist auf T'.*

Proof. Nehme an, $\chi \in \bigcap_\lambda \ker w_\lambda$. Dann ist $\chi(t)$ eine Einheit an allen Stellen in $\overline{\mathbb{Q}}$, also eine Einheitswurzel. Wähle ein k, sodass $\chi(t)^k = 1$. Der Charakter $k \cdot \chi$ ist trivial auf der von t erzeugten Untergruppe $\langle t \rangle$ und somit auch auf T'. Sei umgekehrt $\chi \in X^*(T)$ ein Charakter, sodass $k \cdot \chi$ trivial ist auf T', dann ist $\chi(t)$ eine Einheitswurzel und damit eine Einheit an allen Stellen von $\overline{\mathbb{Q}}$. Daher gilt $\chi \in \bigcap_\lambda \ker w_\lambda$. □

Wegen dem Lemma ist $G_\ell = Z \cdot G_\ell^{\mathrm{der}}$, dabei ist $Z = Z(G)^\circ$ die Einskomponente des Zentrums. Nach Faltings gilt

$$K_\ell \cong \operatorname{End} A^\circ \otimes \mathbb{Q}_\ell \cong \operatorname{End}_{\mathbb{Q}_\ell[\operatorname{Gal}(\overline{L}/L)]} V_\ell A.$$

Daraus folgt unmittelbar

$$Z \subset K_\ell^*$$

Proposition 4.2. *Nehme an, es gilt $n \geq 2$.*

(a) $Z(G_\ell)^\circ = K_\ell^*$.

(b) *Der Morphismus*

$$\varphi : \mathrm{CU}(1,n) \times T_\ell \to T_\ell, \quad (x,y) \mapsto \det(x)/(\overline{y} \cdot y^n).$$

ist definiert über $\mathbb{Q}_\ell$ und es gilt $Z(G)^* = (\ker \varphi \cap K_\ell^\circ \times K_\ell^*)^\circ$.

Beweis. Betrachte die Determinantenabbildung über K_ℓ,

$$\det : G_\ell \longrightarrow K_\ell^*.$$

Wegen $\det(G_\ell^{\mathrm{der}}) = 1$ genügt es zu zeigen, dass diese Abbildung surjektiv ist. Wir wählen eine Stelle $\mathfrak{q}$ in L, die über $\mathfrak{p}$ liegt, und setzen

$$\gamma = \det(\rho_\ell(\mathrm{Frob}_\mathfrak{q})).$$

Nach Satz... ist $\gamma \in K^*$.

K^* ist die Gruppe der $\mathbb{Q}$-rationalen Punkte eines zweidimensionalen Torus T über $\mathbb{Q}$. Wegen $T_{\overline{\mathbb{Q}}} \cong \overline{\mathbb{Q}}\sigma_1 \times \overline{\mathbb{Q}}\sigma_2$ gilt

$$X^*(T) = \mathbb{Z}\sigma_1 \oplus \mathbb{Z}\sigma_2,$$

als $\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-Modul, wobei $\sigma_{1,2} : K \to \overline{\mathbb{Q}}$ die beiden Einbettungen von K in den algebraischen Abschluss sind. Sei $T' \subset T$ der Zariskiabschluss der von γ erzeugten Untergruppe $\langle \gamma \rangle$.

Nach Satz.... gilt $|\gamma|_{\lambda_1} = p^{(n+1)/2}$ für jede Stelle $\lambda_1 \mid \infty$ in $\overline{\mathbb{Q}}$. Wir fixieren eine solche Stelle. Damit findet man leicht

$$\begin{aligned} w_{\lambda_1}(\sigma_1) &= \log|\gamma|_{\lambda_1} = (n+1)/2 \log p, \\ w_{\lambda_1}(\sigma_2) &= \log|\overline{\gamma}|_{\lambda_1} = (n+1)/2 \log p. \end{aligned}$$

Somit gilt $\ker w_{\lambda_1} = \{x(\sigma_1 - \sigma_2) \mid x \in \mathbb{Z}\} \subset X^*(T)$. Sei nun λ_2 eine Stelle von $\overline{\mathbb{Q}}$, die über $\mathfrak{p}$ liegt.

$$\begin{aligned} w_{\lambda_2}(\sigma_1) &= \log|\gamma|_{\lambda_2} = \log|p|_{\lambda_2} = c, \\ w_{\lambda_2}(\sigma_2) &= \log|\overline{\gamma}|_{\lambda_2} = \log|\gamma|_{\overline{\lambda}_2} = \log(|p|_{\overline{\lambda}_2})^n = n \cdot c. \end{aligned}$$

Daraus folgt $\ker w_{\lambda_2} = \{x(n\sigma_1 - \sigma_2) \mid x \in \mathbb{Z}\}$. Wir wenden nun Lemma 4.1 an. Es gilt

$$\bigcap_\lambda \ker w_\lambda \subseteq \ker w_{\lambda_1} \cap \ker w_{\lambda_2} = 0,$$

wegen $n \geq 2$. Daher ist $X^*(T/T')$ eine endliche Torsionsgruppe und T und T' haben dieselbe Dimension. Da T zusammenhängend ist, gilt $T = T'$.

Nach Theorem... enthält G_ℓ die Skalare $\mathbb{Q}_\ell \cdot \mathrm{id}$. Zusammen mit der Gleichheit $T = T'$ folgt nun, dass $\det : G_\ell \to K_\ell^*$ surjektiv ist, also gilt $Z = K_\ell^*$. □

Proposition 4.3. *Die Abbildung* $f : \mathrm{CU}(1,n)(K_\ell) \times K_\ell^* \to K_\ell^*$,

$$f(x,y) = \mathrm{tr}(x^{-1}) \cdot y,$$

ist nicht konstant auf G.

Proof. Sei $\mathfrak{q}$ eine Stelle in L vom Grad 1, die über der Stelle $\mathfrak{p}$ von K liegt. Dann ist $\delta(\mathrm{Frob}_\mathfrak{q}) = (\rho_\ell(\mathrm{Frob}_\mathfrak{q}), \tau_\ell(\mathrm{Frob}_\mathfrak{q})) = (u_\mathfrak{q}, v_\mathfrak{q})$. Nach Theorem.. liegen $\det(u_\mathfrak{q})$ und $\overline{v}_\mathfrak{q} \cdot v_\mathfrak{q}^n$ beide in K und haben dieselben Bewertungen an allen Stellen von K. Ihr Quotient ist daher eine Einheitswurzel $\zeta \in K^*$.

Betrachte den über $\mathbb{Q}_\ell$ definierten Morphismus

$$\varphi : \mathrm{CU}(1,n)(K_\ell) \times K_\ell^* \to K_\ell^*, \quad (x,y) \mapsto \frac{\det(x)}{\overline{y} \cdot y^n}.$$

Aus dem Gesagten folgt, dass $\varphi(\delta(\mathrm{Frob}_\mathfrak{q}))$ eine Einheitswurzel ist. Da die Menge der Frobenius-Automorphismen dicht liegt in $\mathrm{Gal}(\overline{L}/L)$ und G zusammenhängend ist, liegt G in der Untergruppe $H = \ker \varphi$. Die Einskomponente des Zentrums von H,

$$Z(H)^\circ = (K_\ell^* \times K_\ell^* \cap \ker \varphi)^\circ$$

ist ein zweidimensionaler Torus, der $Z(G)^\circ$ enthält.

G ist reduktiv und die Abbildung $\det \circ \mathrm{pr}_1 : G \to K_\ell^*$ ist surjektiv (Beweis wie in prop...). Daher hat $Z(G)^\circ$ ebenfalls Dimension 2 und somit gilt

$$Z(G)^\circ = (K_\ell^* \times K_\ell^* \cap \ker \varphi)^\circ.$$

Sei $\mathrm{Nm} : K_\ell^* \to \mathbb{Q}_\ell^*$ die Normabbildung und $T_1 = \ker \mathrm{Nm}$ der Norm-1-Torus in K_ℓ^*. Für jedes $a \in T_1$ liegt $(a^{n-1} \cdot \mathrm{id}, a^{n+1})$ in G wegen

$$\frac{\det(a^{n-1} \cdot \mathrm{id})}{\overline{a}^{n+1} \cdot (a^{n+1})^n} = \frac{a^{n^2-1}}{a^{-n-1} \cdot a^{n^2+n}} = 1.$$

Die zusammengesetzte Abbildung $T_1 \to K_\ell^*$,

$$a \longmapsto (a^{n-1} \cdot \mathrm{id}, a^{n+1}) \overset{f}{\longmapsto} (n+1)a^2,$$

ist nicht konstant. Folglich ist f auf G ebenfalls nicht konstant. □

Wir haben nun genügend Informationen zusammengetragen, um die Vermutung über die gewöhnliche Reduktion zu beweisen.

Theorem 4.4. *Sei K ein imaginär quadratischer Zahlkörper und L/K eine endliche Erweiterung. Sei A/L eine abelsche Varietät mit $\mathrm{End}_{\overline{L}} A^\circ \cong K$ vom Typ $\mathrm{CU}(1,n)$, $n \geq 2$. Dann existiert eine endliche Erweiterung L' von L und eine Menge V von Stellen der Dirichlet Dichte 1 in L', sodass $A_{L'}$ gewöhnliche Reduktion besitzt an allen Stellen aus V.*

Beweis. Wir wählen eine elliptische Kurve E/L mit $\mathrm{End}\, E^\circ = K$. $\mathrm{Gal}(\overline{L}/L)$ operiert nun auf dem rationalen Tate Modul $V_\ell A$ von A, wie auch auf dem Tate-Modul $V_\ell E \cong K_\ell^*$ von E. Dabei wählen wir die Operation auf $V_\ell E$ so, dass sie vom Typ $\mathrm{CU}(1,0)(K_\ell)$ ist. Diese beiden Operationen liefern eine Darstellung

$$\delta : \mathrm{Gal}(\overline{L}/L) \longrightarrow \mathrm{CU}(1,n)(K_\ell) \times K_\ell^*.$$

Sei G der Zariskiabschluss von $\delta(\mathrm{Gal}(\overline{L}/L))$. Indem wir L durch eine endliche Erweiterung ersetzen, können wir annehmen, dass G zusammenhängend ist.

Sei V_{gut} die Menge aller Stellen $\mathfrak{q}$ in L mit folgenden Eigenschaften:

(i) $\mathfrak{q}$ liegt nicht über ℓ,

(ii) $\mathfrak{q}$ hat Grad 1,

(iii) A besitzt gute Reduktion bei $\mathfrak{q}$, Es genügt zu zeigen, dass die Menge der Stellen $\mathfrak{q} \in V_{\text{gut}}$, bei denen die Reduktion $A_{\mathfrak{q}}$ nicht gewöhnlich ist, Dirichlet-Dichte 0 besitzt.

Sei $\mathfrak{q} \in V_{\text{gut}}$ eine Stelle, sodass $A_{\mathfrak{q}}$ nicht gewöhnlich ist. Seien $\mathfrak{p}$ und p die Stellen in K und $\mathbb{Q}$ unter $\mathfrak{q}$. Es gelte $p\mathcal{O}_K = \mathfrak{p} \cdot \mathfrak{p}'$. Nach Voraussetzung liegt das Newtonpolygon des charakteristischen Polynoms von $\rho_\ell(\mathrm{Frob}_{\mathfrak{q}})$ bezüglich der zu $\mathfrak{p}$ gehörenden Bewertung strikt über dem entsprechenden Hodgepolynom. Für die Frobenius-Eigenwerte $\alpha_1, \ldots, \alpha_{n+1}$ gilt daher

$$0 \leq \mathrm{ord}_{\mathfrak{p}}(\alpha_i) < 1, \qquad i = 1, \ldots, n+1.$$

Wir setzen

$$f_{\mathfrak{q}} = \left(\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \ldots + \frac{1}{\alpha_{n+1}}\right) \cdot t_{\mathfrak{q}} \in K.$$

$f_{\mathfrak{q}}$ ist ganz an allen Stellen von K, die nicht über p oder ∞ liegen. Ausserdem gilt

- $\mathrm{ord}_{\mathfrak{p}} f_{\mathfrak{q}} = \mathrm{ord}_{\mathfrak{p}} \left(\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \ldots + \frac{1}{\alpha_{n+1}}\right) + \mathrm{ord}_{\mathfrak{p}} t_{\mathfrak{q}} > -1 + 0 = -1,$
- $\mathrm{ord}_{\mathfrak{p}'} f_{\mathfrak{q}} = \mathrm{ord}_{\mathfrak{p}'} \left(\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \ldots + \frac{1}{\alpha_{n+1}}\right) + \mathrm{ord}_{\mathfrak{p}'} t_{\mathfrak{q}} \geq -1 + 1 = 0,$
- $|f_{\mathfrak{q}}|_\infty \leq \frac{n+1}{\sqrt{p}} \cdot \sqrt{p} = n+1.$

Da $\mathrm{ord}_{\mathfrak{p}} : K \to \mathbb{Z}$ nur ganze Werte annimmt, ist $f_{\mathfrak{q}}$ ganz bei $\mathfrak{p}$. Folglich ist $a_{\mathfrak{p}}$ ein Element aus $\mathcal{O}_K$ von beschränktem Absolutbetrag. Da K imaginärquadratisch ist, gibt es nur endlich viele solche Elemente.

Sei T die algebraische Gruppe K_ℓ^* über $\mathbb{Q}_\ell$. Nach Proposition 4.3 ist der Morphismus

$$f : \mathrm{CU}(n,1) \times T \to T, \qquad (x,y) \mapsto \mathrm{tr}(x^{-1}) \cdot y$$

nicht konstant auf G. Wegen $f_{\mathfrak{q}} = f(\delta(\mathrm{Frob}_{\mathfrak{q}}))$ bedeutet dies, dass die Menge der Stellen $\mathfrak{q}$, bei denen die Reduktion $A_{\mathfrak{q}}$ nicht gewöhnlich ist...

□

4.2 Die Mumford-Tate Vermutung

Sei A wieder eine abelsche Varietät über L, sodass $\mathrm{End}^\circ A = K$ gilt. Die Galoisdarstellung auf dem Tate-Modul sei vom Typ $\mathrm{CU}(n,1)$.

Die erste Homologiegruppe $V = H_1(A(\mathbb{C}), \mathbb{Q})$ ist ein $2g$-dimensionaler $\mathbb{Q}$-Vektorraum. Er trägt eine natürliche Hodgestruktur vom Typ $\{(1,0),(0,1)\}$, das heisst, es gibt eine Zerlegung $V \otimes_{\mathbb{Q}} \mathbb{C} = V^{1,0} \oplus V^{0,1}$ von $\mathbb{C}$-Vektorräumen, sodass $V^{0,1} = \overline{V^{1,0}}$. Wir wählen einen festen Isomorphismus $V \cong \mathbb{Q}^{2g}$. Sei $\mu_\infty : \mathbb{G}_{m,\mathbb{C}} \to \mathrm{GL}_{2g,\mathbb{C}}$ der Cocharakter, durch den jedes $z \in \mathbb{C}^*$ durch Multiplikation mit z auf $V^{1,0}$ und trivial auf $V^{0,1}$ operiert. Die kleinste über $\mathbb{Q}$ definierte algebraische Untergruppe $G_\infty \subset \mathrm{GL}_{2g,\mathbb{Q}}$, sodass das Bild von μ_∞ in $G_\infty \times_{\mathbb{Q}} \mathbb{Q}$ enthalten ist, heisst *Mumford-Tate-Gruppe* von A.

Jede Polarisierung auf A induziert eine nichtausgeartete, alternierende $\mathbb{Q}$-Bilinearform

$$E : V \times V \to \mathbb{Q}(1),$$

und es ist bekannt, dass das Bild von μ_∞ in $\mathrm{CSp}_{2g,\mathbb{Q}}$ liegt. Folglich gilt

$$G_\infty \subset \mathrm{CSp}_{2g,\mathbb{Q}}\,. \tag{9}$$

Der Raum $H_1(A(\mathbb{C}), \mathbb{Q})$ trägt eine natürliche Operation von $\mathrm{End}(A(\mathbb{C}))$, die mit der Operation von G_∞ kommutiert. Da alle Endomorphismen von $A(\mathbb{C})$ algebraisch sind über $\overline{K}$, folgt daraus

$$G_\infty \subset \mathrm{Aut}_K(V). \tag{10}$$

Proposition 4.5. *$G_\infty \subset \mathrm{CU}(n, 1)$.*

Beweis. Es ist bekannt, dass für die Form E in dieser Situation gilt:

$$E(xv, w) = E(v, \overline{x}w), \qquad \forall x \in K.$$

Wegen (10) besitzt V eine natürliche K-Vektorraumstruktur. Wir wählen ein festes $x \in K$ mit $\overline{x} = -x$ und definieren $H : V \times V \to K$ durch

$$H(v, w) = E(xv, w) + xE(v, w).$$

Man rechnet nun leicht nach, dass H eine hermitsche Form auf V ist. Ausserdem besitzt H dieselbe Signatur wie die $\mathrm{Gal}(\overline{L}/L)$-äquivariante, hermitsche Form auf dem Tate-Modul von A. Wegen (9) liegt G_∞ in $\mathrm{CU}(H)$, dies beweist die Behauptung. □

Die enge Verbindung zwischen der Mumford-Tate-Gruppe und der Gruppe G_ℓ wird unterstrichen durch folgendes Resultat (vgl. [Pi1], Theorem 5.6):

Theorem 4.6. *Für jede Primzahl ℓ gilt*

$$G_\ell^\circ \subset G_\infty \times_{\mathbb{Q}} \mathbb{Q}_\ell.$$

Dies liefert eine obere Grenze für G_ℓ. Allgemein wird vermutet, dass obige Inklusion sogar eine Gleichheit ist:

Vermutung 4.7 (Mumford-Tate). *Für jede Primzahl ℓ gilt*

$$G_\ell^\circ = G_\infty \times_{\mathbb{Q}} \mathbb{Q}_\ell.$$

Sei A wieder eine abelsche Varietät über L, sodass $\operatorname{End}^\circ A = K$ gilt. Die Galoisdarstellung auf dem Tate-Modul sei vom Typ $\mathrm{CU}(n,1)$.

Es gilt daher $G_\ell \subset \mathrm{CU}(n,1)$, wobei $\mathrm{CU}(n,1)$ über $\mathbb{Q}_\ell$ definiert ist. Sei $V = V_\ell A$ der rationale Tate-Modul von A. Es gilt

$$\mathrm{CU}(n,1) = \{g \in \mathrm{GL}_{K_\ell}(V) \mid H(gu, gv) = \lambda H(u,v); \lambda \in K_\ell^*\},$$

mit einer hermitschen Form H mit Signatur $(n,1)$.

Sei σ die Konjugation auf K_ℓ. Ein Element $g \in \mathrm{CU}(n,1)_{\overline{\mathbb{Q}}_\ell}$ operiert auf

$$V \otimes_{\mathbb{Q}_\ell} \overline{\mathbb{Q}}_\ell = (V \otimes_{K_\ell} \overline{\mathbb{Q}}_\ell) \oplus (V \otimes_{K_\ell, \sigma} \overline{\mathbb{Q}}_\ell)$$

durch ein Paar $g = (g_1, g_2)$, wobei $g_2 = \lambda \cdot ({g_1}^t)^{-1}$. Die Projektion auf die erste Komponente $\mathrm{pr}_1 : g \mapsto g_1$ ist ein Morphismus

$$\mathrm{CU}(n,1)_{\overline{\mathbb{Q}}_\ell} \xrightarrow{\mathrm{pr}_1} \mathrm{GL}_{n+1, \overline{\mathbb{Q}}_\ell},$$

der einen Isomorphismus

$$\mathrm{SU}(n,1)_{\overline{\mathbb{Q}}_\ell} \xrightarrow{\cong} \mathrm{SL}_{n+1, \overline{\mathbb{Q}}_\ell}$$

induziert.

Literatur

[Bog] F. A. Bogomolov, *Points of Finite Order on an Abelian Variety,*

[Fal] G. Faltings, *Finiteness Theorems for Abelian Varieties over Number Fields*, Arithmetic Geometry, G. Cornell, J. H. Silverman (Hrsg.), Springer-Verlag, New York etc., 1986

[Gos] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, 1996

[Neu] J. Neukirch, *Algebraic Number Theory*, Springer-Verlag, 1999

[Ros] M. Rosen, *Number Theory in Function Fields*, Springer-Verlag, 2002

[Se1] J-P. Serre, *Complex Semisimple Lie Algebras*, Springer-Verlag, 2001

[Se2] J-P. Serre, *Abelian ℓ-adic Representations and Elliptic Curves*, W.A. Benjamin, New York 1968

[S-T] J-P. Serre, J. Tate, *Good Reduction of Abelian Varieties*, Annals of Math. **88** (1968), 492-517

[Si1] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, 1999

[Pi1] R. Pink, *ℓ-adic algebraic monodromy groups, cocharacters, and the Mumford-Tate conjecture*, J. reine angew. Math. **108** (1998), 187-237

[Pi2] R. Pink, *The Mumford-Tate Conjecture for Drinfeld-Modules*, RIMS, Kyoto University **33** (1997), 393-425