Über das Reduktionsverhalten von Punkten auf abelschen Varietäten

Egon Rütsche

Diplomarbeit
23. 3. 2004

Betreuer: Prof. Dr. Richard Pink

Inhaltsverzeichnis

1 Einleitung

Sei A eine abelsche Varietät über einem Zahlkörper K, und sei Λ eine endlich erzeugte, torsionsfreie Untergruppe von $A(K)$ vom Rang $r > 0$. Sei v eine Stelle von K, an der A gute Reduktion hat. Durch Reduktion an der Stelle v erhält man somit eine abelsche Varietät A_v über dem endlichen Restklassenkörper k_v. Folglich ist die Reduktion jedes rationalen Punktes von A ein Torsionspunkt. Man möchte nun die Reduktion von Λ an der Stelle v untersuchen. Da es ziemlich schwierig ist, Aussagen über die volle Reduktion zu machen, beschreibt man den ℓ-Anteil der Reduktion, wobei ℓ eine Primzahl ist, für welche $v \nmid \ell$ gilt.

Ziel dieser Arbeit ist es, Aussagen über den ℓ-Anteil der Reduktion von Λ zu machen. Ausgangspunkt ist dabei Pinks Artikel [8]. Pink hat dort dieselben Fragestellungen für den ℓ-Anteil der Reduktion eines rationalen Punktes $a \in A(K)$ unendlicher Ordnung untersucht. Um die Methoden aus Pinks Artikel verwenden zu können, arbeitet man mit der abelschen Varietät

$$\tilde{A} := \mathrm{Hom}(\Lambda, A).$$

Die Identität auf Λ entspricht dann auf kanonische Weise einem rationalen Punkt $\tilde{a} \in \tilde{A}(K)$ unendlicher Ordnung.

Um den ℓ-Anteil der Reduktion von Λ zu untersuchen betrachtet man die Gruppe

$$\ell^{-\infty}(\Lambda) := \{x \in A(\bar{K}) \mid \exists n \geq 0 : \ell^n x \in \Lambda\}.$$

Dies ist eine Erweiterung von $\Lambda \otimes_{\mathbb{Z}_\ell} \mathbb{Z}[1/\ell]$ mit

$$A[\ell^\infty] := \{x \in A(\bar{K}) \mid \exists n \geq 0 : \ell^n x = 0\}.$$

Die Gruppe $A[\ell^\infty]$ kann mit Hilfe der Galois-Darstellung auf dem ℓ-adischen Tate-Modul $T_\ell(A)$ untersucht werden.

Im zweiten Kapitel wird zunächst ein Resultat über das Bild Γ_ℓ der Galois-Darstellung und dessen Zariski Abschluss G_ℓ erwähnt. Dann definiert man mit Hilfe von $\ell^{-\infty}(\Lambda)$ einen assoziierten Tate-Modul $T_\ell(A, \Lambda)$ und untersucht die Galois-Darstellung darauf. Das Bild dieser Darstellung wird mit $\tilde{\Gamma}_\ell$ und dessen Zariski Abschluss mit $\tilde{G}_\ell$ bezeichnet. Es wird auch noch kurz beschrieben, was man unter $\mathrm{Hom}(\Lambda, A)$ zu verstehen hat, und weshalb das wieder eine abelsche Varietät ist. Diese Konstruktion heisst Funktor von Punkten. Eine kurze Beschreibung dieser Konstruktion ist auch in [4] enthalten. Der Rest des zweiten Kapitels besteht aus Strukturaussagen über $\tilde{\Gamma}_\ell$ und $\tilde{G}_\ell$. Das Hauptziel des Kapitels ist es, das folgende Theorem zu beweisen.

Theorem. *Sei $\tilde{B}$ die Einskomponente des Zariski Abschlusses von $\mathbb{Z}\tilde{a}$ in $\tilde{A}$. Dann ist $\tilde{\Gamma}_\ell$ eine Erweiterung von Γ_ℓ mit einer offenen Untergruppe von $T_\ell(\tilde{B})$.*

Im dritten Kapitel wird dann der ℓ-Anteil der Reduktion untersucht. Dazu betrachtet man den Kompositionshomomorphismus

$$\kappa_v : \ell^{-\infty}(\Lambda) \subset A(\bar{K}) \longrightarrow A_v(\bar{k}_v) \longrightarrow A_v(\bar{k}_v)[\ell^\infty] \cong A[\ell^\infty].$$

Zunächst wird die Restriktion von κ_v auf Λ beschrieben. Es stellt sich heraus, dass diese durch das Bild des Frobeniuselementes Frob_v unter der Galois-Darstellung auf $T_\ell(A, \Lambda)$ bestimmt ist. Dann werden einige spezielle Fragestellungen behandelt. Es wird beschrieben, wann der ℓ-Anteil der Reduktion von A zyklisch ist, und wann der ℓ-Anteil der Reduktion von Λ zyklisch ist. Danach wird noch untersucht, wann der ℓ-Anteil der Reduktion von A durch den ℓ-Anteil der Reduktion von Λ erzeugt wird.

Im vierten Kapitel geht es um Dichtigkeitsaussagen. Dazu sei W eine Teilmenge von $\tilde{A}[\ell^\infty]$ und Σ die Menge aller Stellen von K, an denen A gute Reduktion hat und $v \nmid \ell$ gilt. Betrachte

$$S_{U_W} = \{v \in \Sigma \mid \kappa_v|_\Lambda \in W\}.$$

Im ersten Abschnitt des vierten Kapitels wird das folgende Theorem bewiesen.

Theorem. *Für jede Teilmenge W von $\tilde{A}[\ell^\infty]$ hat die Menge S_{U_W} eine Dirichlet Dichte.*

Diese Dichte wird dann auch in Termen des normierten Haar-Masses μ von $\tilde{\Gamma}_\ell$ beschrieben. Im zweiten Abschnitt wird dann untersucht, welche dieser Mengen S_{U_W} eine positive Dichte haben. Dabei erhält man das folgende Resultat.

Theorem. *Jede Abbildung, welche als Reduktionsabbildung von Λ auftritt, tritt mit positiver Dichte auf.*

Notation und Konvention. Mit K wird ein Zahlkörper bezeichnet, d.h., eine endliche Erweiterung von $\mathbb{Q}$. Mit A wird immer eine abelsche Varietät über K bezeichnet, d.h., eine vollständige, zusammenhängende algebraische Gruppe über K. Ein algebraischer Abschluss von K wird mit $\bar{K}$ bezeichnet und die dazugehörige Galois-Gruppe mit $\mathrm{Gal}(\bar{K}/K)$. Es wird vorausgesetzt, dass der Leser Grundkenntnisse in der algebraischen Geometrie, der Theorie der ℓ-adischen Zahlen und der Theorie der abelschen Varietäten besitzt. Die Theorie der abelschen Varietäten ist in [7] enthalten.

Danksagung. An dieser Stelle möchte ich mich bei all den Leuten bedanken, die mich während meiner Arbeit an diesem Text unterstützt haben. Besonderer Dank gebührt Prof. Dr. Richard Pink, ohne dessen Hilfe und Unterstützung dieser Text nie zu Stande gekommen wäre.

2 Die ℓ-adische Darstellung einer abelschen Varietät

In diesem Kapitel werden zunächst einige bekannte Resultate für Γ_ℓ wiederholt. Dann werden Aussagen aus Pinks Artikel [8] verallgemeinert. Die hier verwendeten Beweistechniken lehnen sich stark an die von Pink an.

2.1 Bekannte Resultate

Betrachte eine abelsche Varietät A der Dimension g über einem Zahlkörper K. Bezeichne mit $\bar{K}$ einen algebraischen Abschluss von K. Definiere

$$\begin{aligned} A[\ell^n] &:= \{x \in A(\bar{K}) \mid \ell^n x = 0\}, \\ A[\ell^\infty] &:= \{x \in A(\bar{K}) \mid \exists n \geq 0 : \ell^n x = 0\}. \end{aligned}$$

Die Gruppe $A[\ell^\infty]$ ist diskret und isomorph zu $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g}$. Die Galois-Gruppe $\mathrm{Gal}(\bar{K}/K)$ operiert stetig auf $A[\ell^\infty]$. Um diese Operation zu beschreiben, führt man den sogenannten ℓ-adischen Tate-Modul von A ein.

Definition. *Der ℓ-adische Tate-Modul von A* ist definiert durch

$$T_\ell(A) := \varprojlim_n A[\ell^n],$$

wobei die Übergangsabbildungen durch Multiplikation mit ℓ gegeben sind.

Der Tate-Modul ist ein freier $\mathbb{Z}_\ell$-Modul vom Rang $2g$ (siehe [7, Remark 8.4.]). Er ist zudem isomorph zu $\mathrm{Hom}(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A[\ell^\infty])$. Man hat also insgesamt

$$T_\ell(A) \cong \mathrm{Hom}\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, A[\ell^\infty]\big) \cong \mathbb{Z}_\ell^{2g}.$$

Die stetige Operation der Galois-Gruppe $\mathrm{Gal}(\bar{K}/K)$ auf $T_\ell(A)$ liefert einen Homomorphismus

$$\rho_\ell : \mathrm{Gal}(\bar{K}/K) \to \mathrm{Aut}_{\mathbb{Z}_\ell}\big(T_\ell(A)\big) \cong \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

Man interessiert sich hier für das Bild $\Gamma_\ell := \rho_\ell\big(\mathrm{Gal}(\bar{K}/K)\big)$. Diese Gruppe ist eine kompakte Untergruppe von $\mathrm{GL}_{2g}(\mathbb{Z}_\ell)$. Bezeichne mit G_ℓ den Zariski Abschluss von Γ_ℓ in $\mathrm{GL}_{2g,\mathbb{Q}_\ell}$. Dieser Abschluss ist eine lineare algebraische Gruppe über $\mathbb{Q}_\ell$, welche treu auf dem rationalen Tate-Modul

$$V_\ell(A) := T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell^{2g}$$

operiert. Die Abbildung ρ_ℓ liefert somit eine Darstellung

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

Dieser Homomorphismus heisst *die ℓ-adische Darstellung zu A.*

Für G_ℓ hat man das folgende Resultat.

Theorem 2.1.1. *(i) Die Operation von G_ℓ auf $V_\ell(A)$ ist halbeinfach und der natürliche Homomorphismus*

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_\ell \to End_{\mathbb{Q}_\ell, G_\ell}\big(V_\ell(A)\big)$$

ist ein Isomorphismus.

(ii) G_ℓ ist eine reduktive Gruppe.

(iii) Γ_ℓ ist eine offene Untergruppe von $G_\ell(\mathbb{Q}_\ell)$.

Beweis. Siehe [8, Theorem 1.1] □

2.2 Die ℓ-adische Galois-Gruppe einer abelschen Varietät

Betrachte eine endlich erzeugte, torsionsfreie Untergruppe Λ von $A(K)$ vom Rang $r > 0$. Definiere die diskrete Untergruppe

$$\ell^{-\infty}(\Lambda) := \{x \in A(\bar{K}) \mid \exists n \geq 0 : \ell^n x \in \Lambda\}.$$

Man hat eine natürliche Abbildung

$$\begin{array}{rcl} \ell^{-\infty}(\Lambda) & \to & \Lambda \otimes_{\mathbb{Z}_\ell} \mathbb{Z}[1/\ell] \cong \Lambda[1/\ell] \\ x & \mapsto & \ell^n x \otimes 1/\ell^n, \end{array}$$

wobei n so gewählt ist, dass $\ell^n x \in \Lambda$ gilt. Dies ist auf Grund der Eigenschaften des Tensorproduktes wohldefiniert. Mit dieser Abbildung erhält man eine natürliche kurze exakte Sequenz

$$0 \longrightarrow A[\ell^\infty] \longrightarrow \ell^{-\infty}(\Lambda) \longrightarrow \Lambda \otimes_{\mathbb{Z}_\ell} \mathbb{Z}[1/\ell] \longrightarrow 0. \tag{1}$$

Wähle eine Basis $a_1, \ldots, a_r$ von Λ. Indem man für jedes Element der Basis ein kompatibles System von ℓ-ten Wurzeln wählt, erhält man eine Spaltung

$$\begin{array}{rcl} \lambda : \Lambda \otimes_{\mathbb{Z}_\ell} \mathbb{Z}[1/\ell] & \to & \ell^{-\infty}(\Lambda), \\ a_i \otimes 1/\ell^n & \mapsto & (1/\ell^n)x \text{ für } n \in \mathbb{N} \text{ und } i = 1, \ldots, r. \end{array}$$

Eine solche Spaltung wird im folgenden *spezielle Spaltung* genannt.

Zwei spezielle Spaltungen von (1) unterscheiden sich um ein Element von

$$\mathrm{Hom}\big(\Lambda \otimes \mathbb{Z}[1/\ell]/\mathbb{Z}, A[\ell^\infty]\big) \cong \mathrm{Hom}\big(\Lambda \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell, A[\ell^\infty]\big) = \mathrm{Hom}\big(\Lambda, T_\ell(A)\big).$$

Zwei beliebige Spaltungen von (1) unterscheiden sich dagegen um ein Element von

$$\begin{aligned}
\operatorname{Hom}\big(\Lambda \otimes \mathbb{Z}[1/\ell], A[\ell^\infty]\big) &= \bigcup_{k\geq 0} \operatorname{Hom}\big(\Lambda \otimes \mathbb{Z}[1/\ell]/\ell^k\mathbb{Z}, A[\ell^\infty]\big) \\
&\cong \bigcup_{k\geq 0} \ell^{-k} \operatorname{Hom}\big(\Lambda \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell, A[\ell^\infty]\big) \\
&\cong \bigcup_{k\geq 0} \ell^{-k} \operatorname{Hom}\big(\Lambda, T_\ell(A)\big) = \operatorname{Hom}\big(\Lambda, V_\ell(A)\big).
\end{aligned}$$

Die Sequenz (1) ist äquivariant unter der Operation von $\operatorname{Gal}(\bar{K}/K)$, wobei die Operation auf $\mathbb{Z}[1/\ell]$ trivial ist. Um diese Operation zu beschreiben, führt man den assoziierten Tate-Modul ein

$$T_\ell(A, \Lambda) := \operatorname{Hom}\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \ell^{-\infty}(\Lambda)/\Lambda\big).$$

Die Gruppe $\ell^{-\infty}(\Lambda)/\Lambda$ ist isomorph zu $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{2g+r}$. Deshalb gilt für den assoziierten Tate-Modul

$$T_\ell(A, \Lambda) \cong \mathbb{Z}_\ell^{2g+r}.$$

Wenn man die Sequenz (1) modulo Λ betrachtet und die Isomorphie $\mathbb{Z}[1/\ell]/\mathbb{Z} \cong \mathbb{Q}_\ell/\mathbb{Z}_\ell$ benutzt, erhält man die kurze exakte Sequenz

$$0 \longrightarrow A[\ell^\infty] \longrightarrow \ell^{-\infty}(\Lambda)/\Lambda \longrightarrow \Lambda \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \longrightarrow 0.$$

Also liegt der assoziierte Tate-Modul in der folgenden kurzen exakten Sequenz

$$0 \longrightarrow T_\ell(A) \longrightarrow T_\ell(A, \Lambda) \longrightarrow \operatorname{Hom}\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \Lambda \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell\big) \longrightarrow 0.$$

Man hat einen natürlichen Isomorphismus

$$\Lambda \otimes \mathbb{Z}_\ell \xrightarrow{\sim} \operatorname{Hom}\big(\mathbb{Q}_\ell/\mathbb{Z}_\ell, \Lambda \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell\big) \cong \Lambda \otimes \operatorname{End}(\mathbb{Q}_\ell/\mathbb{Z}_\ell) \cong \Lambda \otimes \mathbb{Z}_\ell.$$

Alles in allem hat man also die kurze exakte Sequenz

$$0 \longrightarrow T_\ell(A) \longrightarrow T_\ell(A, \Lambda) \longrightarrow \Lambda \otimes \mathbb{Z}_\ell \longrightarrow 0. \tag{2}$$

Eine Spaltung dieser Sequenz liefert einen Isomorphismus

$$T_\ell(A, \Lambda) \cong T_\ell(A) \oplus \Lambda \otimes \mathbb{Z}_\ell.$$

Eine solche Zerlegung kann man nun in Vektorschreibweise darstellen. Dann kann die natürliche Galois-Darstellung auf $T_\ell(A,\Lambda)$ mit formalen Matrizen geschrieben werden und sieht folgendermassen aus

$$\begin{aligned}
\tilde{\rho}_\ell = \begin{pmatrix} \rho_\ell & * \\ 0 & 1 \end{pmatrix} : \mathrm{Gal}(\bar{K}/K) \quad &\rightarrow \quad \begin{pmatrix} \mathrm{Aut}_{\mathbb{Z}_\ell}\big(T_\ell(A)\big) & \mathrm{Hom}_{\mathbb{Z}_\ell}\big(\Lambda \otimes \mathbb{Z}_\ell, T_\ell(A)\big) \\ 0 & 1 \end{pmatrix} \\
&= \quad \begin{pmatrix} \mathrm{Aut}_{\mathbb{Z}_\ell}\big(T_\ell(A)\big) & \mathrm{Hom}\big(\Lambda, T_\ell(A)\big) \\ 0 & 1 \end{pmatrix} \\
&\cong \quad \begin{pmatrix} \mathrm{GL}_{2g}(\mathbb{Z}_\ell) & \mathrm{M}_{2g\times r}(\mathbb{Z}_\ell) \\ 0 & 1 \end{pmatrix}.
\end{aligned}$$

Auch hier interessiert man sich für das Bild

$$\tilde{\Gamma}_\ell := \tilde{\rho}_\ell\big(\,\mathrm{Gal}(\bar{K}/K)\big) \subset \begin{pmatrix} \Gamma_\ell & \mathrm{Hom}\big(\Lambda, T_\ell(A)\big) \\ 0 & 1 \end{pmatrix}.$$

Sei $N_\ell := \tilde{\Gamma}_\ell \cap \mathrm{Hom}\big(\Lambda, T_\ell(A)\big)$. Dann erhält man die natürliche kurze exakte Sequenz

$$0 \longrightarrow N_\ell \longrightarrow \tilde{\Gamma}_\ell \longrightarrow \Gamma_\ell \longrightarrow 1.$$

Wie im Fall von Γ_ℓ untersucht man die Gruppe $\tilde{\Gamma}_\ell$, indem man ihren Zariski Abschluss $\tilde{G}_\ell$ in $\mathrm{GL}_{2g,\mathbb{Q}_\ell} \ltimes M_{2g\times r,\mathbb{Q}_\ell}$ betrachtet. Dies ist eine lineare algebraische Gruppe über $\mathbb{Q}_\ell$ mit einer treuen Darstellung auf

$$V_\ell(A,\Lambda) := T_\ell(A,\Lambda) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \cong \mathbb{Q}_\ell^{2g+r}.$$

Dadurch erhält man eine natürliche kurze exakte Sequenz

$$0 \longrightarrow U_\ell \longrightarrow \tilde{G}_\ell \longrightarrow G_\ell \longrightarrow 1.$$

Die Gruppe U_ℓ ist eine algebraische Untergruppe von

$$\mathrm{Hom}\big(\Lambda, V_\ell(A)\big) = \mathrm{Hom}\big(\Lambda, T_\ell(A)\big) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell.$$

Nach Theorem 2.1.1 (ii) ist die Gruppe G_ℓ reduktiv. Deshalb ist U_ℓ genau das unipotente Radikal der linearen algebraischen Gruppe $\tilde{G}_\ell$.

Satz 2.2.1. *Die Gruppe $\tilde{\Gamma}_\ell$ ist offen in $\tilde{G}_\ell(\mathbb{Q}_\ell)$, und die Gruppe N_ℓ ist offen in $U_\ell(\mathbb{Q}_\ell)$.*

Beweis. Man hat die folgende Inklusion von kurzen exakten Sequenzen

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_\ell(\mathbb{Q}_\ell) & \longrightarrow & \tilde{G}_\ell(\mathbb{Q}_\ell) & \longrightarrow & G_\ell(\mathbb{Q}_\ell) & \longrightarrow & 1 \\
 & & \cup & & \cup & & \cup & & \\
0 & \longrightarrow & N_\ell & \longrightarrow & \tilde{\Gamma}_\ell & \longrightarrow & \Gamma_\ell & \longrightarrow & 1\,.
\end{array}$$

Man kann nun alle diese Gruppen als ℓ-adische Lie-Gruppen betrachten. Nach Konstruktion ist $\tilde{\Gamma}_\ell$ Zariski dicht in $\tilde{G}_\ell$. Ein Theorem von Chevalley [3, Chapter II, Corollary 7.9] impliziert

$$[\operatorname{Lie}\tilde{G}_\ell, \operatorname{Lie}\tilde{G}_\ell] \subset \operatorname{Lie}\tilde{\Gamma}_\ell.$$

Sei v eine Stelle von K, an der A gute Reduktion hat und $v \nmid \ell$ gilt. Bezeichne mit k_v den Restklassenkörper von K an der Stelle v. Sei Frob_v ein Element einer Zerlegunsgruppe an der Stelle v, welches auf $\mathrm{Gal}(\bar{K}/K)$ operiert, indem ein Element der Galois-Gruppe auf seine $|k_v|$-te Potenz abgebildet wird.

Man kann zeigen, dass alle Eigenwerte dieses sogenannten Frobeniuselementes komplexen Absolutbetrag > 1 haben. Deshalb kann $V_\ell(A)$ die triviale Darstellung von G_ℓ° nicht enthalten. Folglich enthält auch U_ℓ die triviale Darstellung von G_ℓ° nicht und somit auch von $\tilde{G}_\ell^\circ$ nicht. Für die unipotente Gruppe U_ℓ gilt $U_\ell \cong \operatorname{Lie} U_\ell$. Daraus folgt

$$\operatorname{Lie} U_\ell = [\operatorname{Lie}\tilde{G}_\ell, \operatorname{Lie} U_\ell] \subset [\operatorname{Lie}\tilde{G}_\ell, \operatorname{Lie}\tilde{G}_\ell] \subset \operatorname{Lie}\tilde{\Gamma}_\ell.$$

Nach Theorem 2.1.1 (iii) gilt $\operatorname{Lie}\Gamma_\ell = \operatorname{Lie} G_\ell$. Daraus folgt nun $\operatorname{Lie}\tilde{\Gamma}_\ell = \operatorname{Lie}\tilde{G}_\ell$. Also ist $\tilde{\Gamma}_\ell$ offen in $\tilde{G}_\ell(\mathbb{Q}_\ell)$ und somit auch N_ℓ in $U_\ell(\mathbb{Q}_\ell)$. □

Satz 2.2.2. *Nach Ersetzen von K durch eine geeignete endliche Erweiterung existiert eine Spaltung von (1), sodass*

$$\tilde{\Gamma}_\ell = \begin{pmatrix} \Gamma_\ell & N_\ell \\ 0 & 1 \end{pmatrix} \text{ gilt.}$$

Beweis. Wähle eine Levi-Zerlegung $\tilde{G}_\ell = G_\ell \ltimes U_\ell$ von $\tilde{G}_\ell$. Indem man die Sequenz (2) mit $\mathbb{Q}_\ell$ tensoriert erhält man

$$0 \longrightarrow V_\ell(A) \longrightarrow V_\ell(A, \Lambda) \longrightarrow \Lambda \otimes \mathbb{Q}_\ell \longrightarrow 0. \tag{3}$$

Die Gruppe G_ℓ ist reduktiv, operiert trivial auf $\Lambda \otimes \mathbb{Q}_\ell$ und nicht trivial auf jedem von Null verschiedenen Unterraum von $V_\ell(A)$. Folglich besitzt die Sequenz (3) eine eindeutige Spaltung, welche unter der Operation des Levi-Faktors G_ℓ invariant ist.

Sei nun λ irgendeine Spaltung der Sequenz (1). Diese induziert eine Spaltung von (3), welche sich von der Levi-invarianten Spaltung um ein Element von $\operatorname{Hom}\big(\Lambda \otimes \mathbb{Q}_\ell, V_\ell(A)\big) = \operatorname{Hom}\big(\Lambda, V_\ell(A)\big)$ unterscheidet. Indem man λ durch dieses Element ersetzt, sieht man, dass die Levi-invariante Spaltung schon durch eine Spaltung von (1) induziert wird. Bezüglich dieser Spaltung ist die Zerlegung $\tilde{G}_\ell = G_\ell \ltimes U_\ell$ dieselbe wie die folgende Zerlegung in Matrixschreibweise

$$\tilde{G}_\ell = \begin{pmatrix} G_\ell & U_\ell \\ 0 & 1 \end{pmatrix}.$$

Nach Satz 2.2.1 ist $\big(G_\ell(\mathbb{Q}_\ell)\cap\tilde{\Gamma}_\ell\big) \ltimes \big(U_\ell(\mathbb{Q}_\ell)\cap\tilde{\Gamma}_\ell\big)$ eine offene Untergruppe von $\tilde{G}_\ell(\mathbb{Q}_\ell)$ und somit von $\tilde{\Gamma}_\ell$. Nach Galois-Theorie entsprechen die offenen Untergruppen von $\tilde{\Gamma}_\ell$ endlichen Körpererweiterungen von K in $\bar{K}$. Indem man also den Körper K durch die entsprechende endliche Erweiterung ersetzt, wird $\tilde{\Gamma}_\ell$ selbst ein semidirektes Produkt der obigen Form. □

Um die von Pink in [8] benutzten Argumente zum Beweis eines Resultates über N_ℓ und U_ℓ übernehmen zu können, muss man zunächst die abelsche Varietät $\mathrm{Hom}\big(\Lambda, A\big)$ definieren. Dazu benutzt man eine Konstruktion, die jedem Schema einen Funktor von der entgegengesetzten Kategorie der Schemata in die Kategorie der Mengen zuordnet. Diese Konstruktion wird in [4] Funktor von Punkten genannt.

Definition. Sei X ein Schema. *Der Funktor von Punkten von X* ist der Funktor

$$h_X : (Sch)^\circ \to Ens,$$

welcher jedem Schema Y die Menge $\mathrm{Mor}(Y, X)$ und jedem Morphismus $f : Y \to Z$ die Abbildung von Mengen $h_X(f) : h_X(Z) \to h_X(Y), g \mapsto g \circ f$ zuordnet.

Bemerkung. Wenn man mit Schemata, die über einem Basisschema S gegeben sind, arbeiten möchte, dann geht die Konstruktion genau gleich. Man betrachtet dann einfach nur die Morphismen über S, also $\mathrm{Mor}_S(Y, X)$, wobei X und Y natürlich S-Schemata sein müssen.

Dieser Funktor induziert einen Funktor

$$(Sch) \to \mathrm{Mor}\big((Sch)^\circ, Ens\big),$$

der jedem Schema X dessen Funktor von Punkten zuordnet. Man kann zeigen, dass dieser induzierte Funktor volltreu ist. Für K-Schemata X und X' hat man also einen Isomorphismus

$$\mathrm{Hom}\big(h_X, h_{X'}\big) \cong \mathrm{Mor}_K(X, X').$$

Dies erlaubt es, ein Schema über dessen Funktor von Punkten zu definieren. Auf diese Weise kann man das Schema $\mathrm{Hom}\big(\Lambda, A\big)$ definieren. Damit die folgende Definition Sinn macht, muss man sich zunächst überlegen, dass der Funktor $\mathrm{Hom}_{\mathbb{Z}}\big(\Lambda, h_A(.)\big)$ dem Funktor von Punkten eines Schemas entspricht. Dazu wählt man eine Basis von Λ. Dann sieht man, dass das Schema A^r diese Forderung erfüllt.

Definition. Das Schema $\mathrm{Hom}_{\mathbb{Z}}\big(\Lambda, A\big)$ ist definiert durch

$$h_{\mathrm{Hom}_{\mathbb{Z}}\left(\Lambda,A\right)}(.) := \mathrm{Hom}_{\mathbb{Z}}\big(\Lambda, h_A(.)\big).$$

Für ein K-Schema S hat man also

$$h_{\mathrm{Hom}_{\mathbb{Z}}\left(\Lambda,A\right)}(S) = \mathrm{Hom}_{\mathbb{Z}}\big(\Lambda, h_A(S)\big) = \mathrm{Hom}_{\mathbb{Z}}\big(\Lambda, \mathrm{Mor}_K\big(S, A\big)\big).$$

Bemerkung. Sobald man eine Basis von Λ wählt, hat man also

$$\mathrm{Hom}_{\mathbb{Z}}\big(\Lambda, A\big) \cong A^r.$$

Insbesondere ist $\mathrm{Hom}_{\mathbb{Z}}\big(\Lambda, A\big)$ eine abelsche Varietät, welche im folgenden mit $\tilde{A}$ bezeichnet wird.

Der Homomorphismus $\mathrm{id}\,|_\Lambda$ entspricht auf kanonische Weise einem Element $\tilde{a}$ aus $\tilde{A}$. Dieses Element wird also von Λ induziert und hat unendliche Ordnung.

Theorem 2.2.3. *Sei $\tilde{B}$ die Einskomponente des Zariski Abschlusses von $\mathbb{Z}\tilde{a}$ in $\tilde{A}$. Dann gelten die folgenden Aussagen:*

(i) *N_ℓ ist eine offene Untergruppe von $T_\ell(\tilde{B}) \subset T_\ell(\tilde{A})$*

(ii) $U_\ell = V_\ell(\tilde{B}) \subset V_\ell(\tilde{A})$.

Beweis. (i) Aus der Definition von $\tilde{A}$ ergeben sich die folgenden Gleichungen

$T_\ell(\tilde{A}) = \mathrm{Hom}_{\mathbb{Z}}\big(\Lambda, T_\ell(A)\big)$, $\tilde{A}[\ell^s] = \mathrm{Hom}_{\mathbb{Z}}\big(\Lambda, A[\ell^s]\big)$ für eine ganze Zahl $s \geq 0$.

Betrachte nun für ganze Zahlen $r \geq s \geq 0$ die folgenden Quotienten

$$\begin{array}{ccccc} \tilde{\Gamma}_\ell & \twoheadrightarrow & \tilde{\Gamma}_{\ell,r,s} & \subset & \mathrm{GL}_{2g}(\mathbb{Z}/\ell^r\mathbb{Z}) \ltimes T_\ell(\tilde{A})/\ell^s T_\ell(\tilde{A}) \\ \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow & & \downarrow\!\!\downarrow \\ \Gamma_\ell & \twoheadrightarrow & \Gamma_{\ell,r} & \subset & \mathrm{GL}_{2g}(\mathbb{Z}/\ell^r\mathbb{Z}) \end{array}$$

Man erhält die kurze exakte Sequenz

$$0 \longrightarrow N_{\ell,r,s} \longrightarrow \tilde{\Gamma}_{\ell,r,s} \longrightarrow \Gamma_{\ell,r} \longrightarrow 1$$

für eine Untergruppe $N_{\ell,r,s} \subset T_\ell(\tilde{A})/\ell^s T_\ell(\tilde{A}) \cong \tilde{A}[\ell^s]$. Hier kann man nun ein Theorem von Ribet [9] anwenden, das für den vorliegenden Fall von Bertrand [2] formuliert und von Hindry [6] in der hier benutzten Form aufgestellt worden ist.

Dazu muss $r \geq s + t$ gelten, wobei t der Exponent vom ℓ-Anteil von $[\overline{\mathbb{Z}\tilde{a}} : \tilde{B}]$ ist. Zudem muss $\tilde{a}$ ein indivisibler Punkt von $\tilde{A}(K)$ sein. Das kann man jedoch annehmen. Sonst ersetzt man $\tilde{a}$ durch ein indivisibles $\tilde{b}$ mit $\tilde{a} \in \mathbb{Z}\tilde{b}$. Dies erweitert die Gruppe $\ell^{-\infty}(\mathbb{Z}\tilde{a})$ um einen endlichen Index, welcher teilerfremd zu ℓ ist. Folglich ändert das die Gruppen $\tilde{\Gamma}_\ell$ und N_ℓ nicht.

Nach [6, §2, Proposition 1] ist $N_{\ell,r,s}$ eine Untergruppe von $T_\ell(\tilde{B})/\ell^s T_\ell(\tilde{B}) \cong \tilde{B}[\ell^s]$, deren Index unabhängig von r und s beschränkt ist. Die Gruppe N_ℓ ist der inverse Limes von den Gruppen $N_{\ell,r,s}$, wenn r und s gegen unendlich streben. Daraus folgt, dass N_ℓ eine offene Untergruppe von $T_\ell(\tilde{B})$ ist.

(ii) Aus Satz 2.2.1 folgt

$$U_\ell(\mathbb{Q}_\ell) = \mathbb{Q}_\ell N_\ell.$$

Zusammen mit Teil (i) folgt daraus $U_\ell = V_\ell(\tilde{B})$. □

Bemerkung. Nach Voraussetzung hat $\tilde{a}$ unendliche Ordnung. Aus Theorem 2.2.3 folgt daher, dass $N_\ell \neq 0$ gilt.

Korollar 2.2.4. *Die folgenden Aussagen sind äquivalent:*

(i) N_ℓ *ist offen in* $T_\ell(\tilde{A})$

(ii) $U_\ell = V_\ell(\tilde{A})$

(iii) $\mathbb{Z}\tilde{a}$ *ist Zariski dicht in* $\tilde{A}$.

Beweis. Folgt direkt aus Theorem 2.2.3 □

Jetzt kann man sich fragen, wie man die Aussagen des Korollars in Termen von A an Stelle von $\tilde{A}$ ausdrücken kann.

Satz 2.2.5. *Sei* $\mathbb{Z}\tilde{a}$ *Zariski dicht in* $\tilde{A}$. *Dann ist* $\mathbb{Z}a$ *Zariski dicht in* A *für jedes* $a \in \Lambda \setminus \{0\}$.

Beweis. Wähle eine Basis $a_1, \ldots, a_r$ von Λ. Die Bedingung, dass $\mathbb{Z}\tilde{a}$ Zariski dicht ist in $\tilde{A} \cong A^r$, bedeutet nun, dass $\mathbb{Z}(a_1, \ldots, a_r)$ dicht ist in A^r. Aus

$$\overline{\mathbb{Z}(a_1, \ldots, a_r)} \subseteq \overline{\mathbb{Z}a_1} \oplus \ldots \oplus \overline{\mathbb{Z}a_r}$$

und der Tatsache, dass die Projektion auf einen Faktor abgeschlossen ist, folgt $\overline{\mathbb{Z}a_i} = A$ für $i = 1, \ldots, r$.

Sei nun a ein von Null verschiedenes Element von Λ. Dann kann man ein Vielfaches von a zu einer Basis ergänzen und das obige Argument anwenden, um $\overline{\mathbb{Z}a} = A$ zu erhalten. □

Die Umkehrung des Satzes gilt nicht. Die Aussage $\tilde{B} \neq \tilde{A}$ ist äquivalent dazu, dass es einen nicht trivialen Quotienten $\tilde{A}/\tilde{B}$ und einen nicht trivialen Homomorphismus $\varphi : \tilde{A}/\tilde{B} \to A$ gibt. Dies wiederum ist äquivalent zur Tatsache, dass es $\varphi_1, \ldots, \varphi_r \in \operatorname{End}\big(A\big)$ gibt mit $\sum_i \varphi_i(a_i) = 0$.

Beispiel. Sei A eine elliptische Kurve mit komplexer Multiplikation durch $\mathscr{O}_K = \mathbb{Z} \oplus \mathbb{Z}\omega$, und sei $a \in A(K)$ ein Punkt unendlicher Ordnung. Definiere $\Lambda := \mathscr{O}_K a$. Dann hat man einen Isomorphismus $\mathscr{O}_K \xrightarrow{\sim} \Lambda, x \mapsto xa$. Da a kein Torsionspunkt ist, muss $\mathbb{Z}b$ dicht sein in A für jedes von Null verschiedene $b \in \Lambda$. Für die $\mathbb{Z}$-Basis $a, \omega a$ von Λ existiert aber die nicht triviale Relation $1 \cdot (\omega a) - \omega \cdot (a) = 0$. Folglich sind $\tilde{B}$ und $\tilde{A}$ in diesem Fall nicht gleich.

Trotzdem kann man $\tilde{B}$ und U_ℓ noch etwas expliziter beschreiben. Definiere dazu $E := \operatorname{End}\big(A\big)$.

Satz 2.2.6. *(i)* $\tilde{B} = \operatorname{Hom}_E\big(E\Lambda, A\big)$.

(ii) $$U_\ell = V_\ell(\tilde{B}) \cong \left\{ \varphi \in \operatorname{Hom}_{\mathbb{Z}}\big(\Lambda, V_\ell(A)\big) \;\middle|\; \begin{array}{l} \sum_i e_i\varphi(a_i) = 0 \textit{ für jede} \\ \textit{endliche Folge von Elementen} \\ e_i \in E, a_i \in \Lambda \textit{ mit } \sum_i e_i a_i = 0 \end{array} \right\}.$$

Beweis. (i) Wähle eine Basis $a_1, \ldots, a_r$ von Λ. Dann hat die Gruppe $E\Lambda$ die Form $E\Lambda = Ea_1 + \ldots + Ea_r$. Diese Summe ist zwar nicht mehr direkt, besitzt aber eine endliche E-lineare Präsentation, d.h., man hat

$$E^m \xrightarrow{M} E^r \longrightarrow E\Lambda \longrightarrow 0,$$

wobei $E^r \to E\Lambda,\ \underline{x} = (x_1, \ldots, x_r) \mapsto \sum_i x_i a_i$. Indem man nun den Funktor $\operatorname{Hom}_E\big(., A\big)$ auf diese Präsentation anwendet, erhält man

$$0 \longrightarrow \operatorname{Hom}_E\big(E\Lambda, A\big) \longrightarrow \operatorname{Hom}_E\big(E^r, A\big) \xrightarrow{M^t} \operatorname{Hom}_E\big(E^m, A\big).$$

Dabei gilt $\operatorname{Hom}_E\big(E^r, A\big) = A^r \cong \tilde{A}$ und somit

$$\tilde{B} = \operatorname{Hom}_E\big(E\Lambda, A\big) \subset \operatorname{Hom}_{\mathbb{Z}}\big(\Lambda, A\big) = \tilde{A}.$$

(ii) Da sich $\tilde{B}$ und $\tilde{A}$ durch E-Relationen unterscheiden, wird auch $U_\ell = V_\ell(\tilde{B})$ durch $V_\ell(\tilde{A})$ durch solche Relationen gegeben. Es gilt somit

$$\begin{aligned} U_\ell = V_\ell(\tilde{B}) &\cong \operatorname{Hom}_E\big(E\Lambda, V_\ell(A)\big) \\ &= \left\{ \varphi \in \operatorname{Hom}_{\mathbb{Z}}\big(\Lambda, V_\ell(A)\big) \;\middle|\; \begin{array}{l} \sum_i e_i\varphi(a_i) = 0 \text{ für jede} \\ \text{endliche Folge von Elementen} \\ e_i \in E, a_i \in \Lambda \text{ mit } \sum_i e_i a_i = 0 \end{array} \right\}. \end{aligned}$$

□

Bemerkung. Es ist also $\tilde{B}$ der Kern von $A^r \xrightarrow{M^t} A^m$. Etwas in der Art hat man auch erwarten können, da sich nach dern obigen Ausführungen $\tilde{B}$ von $\tilde{A}$ durch E-Relationen unterscheidet, welche bei $\mathrm{Hom}_E\left(E\Lambda, A\right)$ rausdividiert werden. Wenn nun Λ die Bedingung $\Lambda = E\Lambda$ erfüllt, dann gilt die Umkehrung von Satz 2.2.5.

3 Der ℓ-Anteil der Reduktion

In diesem Kapitel wird der ℓ-Anteil der Reduktion genauer untersucht. Im ersten Abschnitt wird der ℓ-Anteil der Reduktion von Λ durch eine Abbildung beschrieben. In den darauffolgenden Abschnitten werden einige spezielle Fragestellungen behandelt.

3.1 Der ℓ-Anteil der Reduktion an der Stelle v

Sei Λ wie oben, und sei $v \nmid \ell$ eine Primstelle von K, an der A gute Reduktion hat. Dann induziert die Reduktionsabbildung einen Isomorphismus

$$A[\ell^\infty] \xrightarrow{\sim} A_v(\bar{k}_v)[\ell^\infty].$$

Betrachte den Kompositionshomomorphismus

$$\kappa_v : \ell^{-\infty}(\Lambda) \subset A(\bar{K}) \longrightarrow A_v(\bar{k}_v) \longrightarrow A_v(\bar{k}_v)[\ell^\infty] \cong A[\ell^\infty].$$

Nach Definition ist die Einschränkung von κ_v auf $A[\ell^\infty]$ die Identität. Folglich induziert κ_v eine Spaltung der Sequenz (1). Die Abbildung κ_v ist nach Konstruktion äquivariant unter der Operation von Frob_v .

Satz 3.1.1. *Sei $v \nmid \ell$ eine Primstelle von K, an der A gute Reduktion hat. Dann ist κ_v die einzige* Frob_v*-äquivariante Spaltung der Sequenz (1).*

Beweis. Jede andere Frob_v-äquivariante Spaltung unterscheidet sich von κ_v durch ein Element von

$$\mathrm{Hom}\big(\Lambda \otimes_{\mathbb{Z}} \mathbb{Z}[1/\ell], A[\ell^\infty]\big) \cong \mathrm{Hom}\big(\Lambda, V_\ell(A)\big) = V_\ell(\tilde{A}) \cong V_\ell(A)^r.$$

Alle Eigenwerte von Frob_v auf $V_\ell(A)$ haben komplexen Absolutbetrag > 1. Also ist der Unterraum der Frob_v-Invarianten in $V_\ell(A)^r$ null, und somit ist κ_v die einzige Frob_v-äquivariante Spaltung. □

Nun möchte man die Abbildung $\kappa_v|_\Lambda$ untersuchen. Diese beschreibt nach Konstruktion den ℓ-Anteil der Reduktion von Λ.

Dazu sei $a_1, \ldots, a_r$ eine Basis von Λ und λ eine spezielle Spaltung der Sequenz (1). Definiere

$$\tilde{\gamma}_v := \tilde{\rho}_\ell(\mathrm{Frob}_v) = \begin{pmatrix} \gamma_v & n_v \\ 0 & 1 \end{pmatrix},$$

wobei $\gamma_v = \rho_\ell(\mathrm{Frob}_v) \in \Gamma_\ell \subset \mathrm{GL}_{2g}(\mathbb{Z}_\ell), n_v \in \mathrm{Hom}\big(\Lambda, T_\ell(A)\big) \cong \mathrm{M}_{2g\times r}(\mathbb{Z}_\ell)$ gilt. Da γ_v keinen Eigenwert 1 hat, ist die Matrix $\gamma_v - \mathrm{id}$ über $\mathbb{Q}_\ell$ invertierbar. Definiere

$$m_v := (\gamma_v - \mathrm{id})^{-1} n_v \in \mathrm{Hom}\big(\Lambda, V_\ell(A)\big) \cong \mathrm{M}_{2g\times r}(\mathbb{Q}_\ell).$$

Sei π_ℓ der natürliche Kompositionshomomorphismus

$$\operatorname{Hom}\big(\Lambda, V_\ell(A)\big) \twoheadrightarrow \operatorname{Hom}\big(\Lambda, V_\ell(A)\big) / \operatorname{Hom}\big(\Lambda, T_\ell(A)\big) \cong \operatorname{Hom}\big(\Lambda, A[\ell^\infty]\big).$$

Satz 3.1.2. *Es gilt* $\kappa_v|_\Lambda = \pi_\ell(m_v) : \Lambda \to A[\ell^\infty]$.

Beweis. Die Spaltung λ induziert eine Zerlegung

$$V_\ell(A,\Lambda) = V_\ell(A) \oplus \big(\Lambda \otimes \mathbb{Q}_\ell\big),$$

und somit eine Zerlegung

$$\begin{aligned} \operatorname{Hom}\big(\Lambda, V_\ell(A,\Lambda)\big) &= \operatorname{Hom}\big(\Lambda, V_\ell(A)\big) \oplus \operatorname{Hom}\big(\Lambda, \Lambda \otimes \mathbb{Q}_\ell\big) \\ &\cong \mathrm{M}_{2g\times r}(\mathbb{Q}_\ell) \oplus \mathrm{M}_{r\times r}(\mathbb{Q}_\ell). \end{aligned}$$

Der Eigenraum von $\tilde{\gamma}_\ell$ in $\operatorname{Hom}\big(\Lambda, V_\ell(A,\Lambda)\big)$ zum Eigenwert 1 wird erzeugt durch

$$\begin{pmatrix} -m_v \\ \mathrm{id} \end{pmatrix} \in \mathrm{M}_{2g\times r}(\mathbb{Q}_\ell) \oplus \mathrm{M}_{r\times r}(\mathbb{Q}_\ell).$$

Es gilt $\Lambda \otimes \mathbb{Z}[1/\ell] \cong \Lambda[1/\ell]$. Die Abbildung

$$\begin{aligned} \operatorname{Hom}\big(\Lambda, \Lambda[1/\ell]\big) &\longrightarrow \operatorname{Hom}\big(\Lambda, \ell^{-\infty}(\Lambda)\big) = \operatorname{Hom}\big(\Lambda, A[\ell^\infty]\big) \oplus \operatorname{Hom}\big(\Lambda, \Lambda[1/\ell]\big), \\ x &\longmapsto \begin{pmatrix} -\pi_\ell(m_v x) \\ x \end{pmatrix} \end{aligned}$$

definiert eine $\tilde{\gamma}_v$-äquivariante Spaltung der Sequenz

$$0 \longrightarrow \operatorname{Hom}\big(\Lambda, A[\ell^\infty]\big) \longrightarrow \operatorname{Hom}\big(\Lambda, \ell^{-\infty}(\Lambda)\big) \longrightarrow \operatorname{Hom}\big(\Lambda, \Lambda[1/\ell]\big) \longrightarrow 0.$$

Dabei wird die Operation von $\tilde{\gamma}_v$ auf $\operatorname{Hom}\big(\Lambda, .\big)$ als Operation auf dem Bildraum verstanden. Also wird die Spaltung durch eine $\tilde{\gamma}_v$-äquivariante Spaltung

$$\Lambda[1/\ell] \longrightarrow \ell^{-\infty}(\Lambda)$$

induziert. Ebenso wird die $\tilde{\gamma}_v$-äquivariante Abbildung

$$\begin{aligned} \operatorname{Hom}\big(\Lambda, A[\ell^\infty]\big) \oplus \operatorname{Hom}\big(\Lambda, \Lambda[1/\ell]\big) = \operatorname{Hom}\big(\Lambda, \ell^{-\infty}(\Lambda)\big) &\longrightarrow \operatorname{Hom}\big(\Lambda, A[\ell^\infty]\big) \\ \begin{pmatrix} b \\ x \end{pmatrix} = \begin{pmatrix} b + \pi_\ell(m_v x) \\ 0 \end{pmatrix} + \begin{pmatrix} -\pi_\ell(m_v x) \\ x \end{pmatrix} &\longmapsto b + \pi_\ell(m_v x) \end{aligned}$$

durch eine $\tilde{\gamma}_v$-äquivariante Spaltung

$$\ell^{-\infty}(\Lambda) \longrightarrow A[\ell^\infty]$$

induziert. Nach Satz 3.1.1 kommt dafür nur κ_v in Frage.

Die Gruppe Λ induziert auf eindeutige Weise ein Element in $\mathrm{Hom}\big(\Lambda, \ell^{-\infty}(\Lambda)\big)$. Weil λ eine spezielle Spaltung der Sequenz (1) war, entspricht dieses Element dem Element

$$\begin{pmatrix} 0 \\ \mathrm{id} \end{pmatrix} \in \mathrm{Hom}\left(\Lambda, A[\ell^\infty]\right) \oplus \mathrm{Hom}\left(\Lambda, \Lambda[1/\ell]\right).$$

Also folgt $\kappa_v|_\Lambda = \pi_\ell(m_v \,\mathrm{id}) = \pi_\ell(m_v)$. □

3.2 Eigenschaften von $A_v(k_v)[\ell^\infty]$

In diesem Abschnitt soll untersucht werden, wann der ℓ-Anteil der Reduktion von A zyklisch ist.

Sei $v \nmid \ell$ eine Primstelle, an der A gute Reduktion hat. Definiere

$$\gamma_v := \rho_\ell(\mathrm{Frob}_v) \in \Gamma_\ell \subset \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

Satz 3.2.1. $A_v(k_v)[\ell^\infty] \cong A(\bar{K})[\ell^\infty]^{\mathrm{Frob}_v} \cong T_\ell(A)/(\gamma_v - \mathrm{id})T_\ell(A)$.

Beweis. Man hat die folgenden Gleichungen

$$\begin{aligned} A_v(k_v)[\ell^\infty] &= A_v(\bar{k}_v)[\ell^\infty]^{\mathrm{Frob}_v} \cong A(\bar{K})[\ell^\infty]^{\mathrm{Frob}_v} \\ &= \big(T_\ell(A) \otimes (\mathbb{Q}_\ell/\mathbb{Z}_\ell)\big)^{\gamma_v}. \end{aligned}$$

Der Tate-Modul liegt in der folgenden kurzen exakten Sequenz

$$0 \longrightarrow T_\ell(A) \longrightarrow V_\ell(A) \longrightarrow A(\bar{K})[\ell^\infty] \longrightarrow 0.$$

Betrachte die Gruppe $\langle \mathrm{Frob}_v \rangle$. Zu dieser Gruppe und zur obigen Sequenz gehört eine lange exakte Kohomologiesequenz. Betrachte daraus den folgenden Teil

$$\begin{aligned} V_\ell(A)^{\mathrm{Frob}_v} &\longrightarrow A(\bar{K})[\ell^\infty]^{\mathrm{Frob}_v} \longrightarrow \mathrm{H}^1\left(\langle \mathrm{Frob}_v \rangle, T_\ell(A)\right) \\ &\longrightarrow \mathrm{H}^1\left(\langle \mathrm{Frob}_v \rangle, V_\ell(A)\right). \end{aligned}$$

Die Matrix γ_v hat keinen Eigenwert 1 auf $V_\ell(A)$. Deshalb gilt $\big(V_\ell(A)\big)^{\gamma_v} = 0$. Da die Gruppe $\langle \mathrm{Frob}_v \rangle$ zyklisch ist, folgt

$$\begin{aligned} \mathrm{H}^1\left(\langle \mathrm{Frob}_v \rangle, T_\ell(A)\right) &= T_\ell(A)_{\gamma_v} = T_\ell(A)/(\gamma_v - \mathrm{id})T_\ell(A), \text{ und} \\ \mathrm{H}^1\left(\langle \mathrm{Frob}_v \rangle, V_\ell(A)\right) &= V_\ell(A)_{\gamma_v} = V_\ell(A)/(\gamma_v - \mathrm{id})V_\ell(A). \end{aligned}$$

Die Matrix $\gamma_v - \mathrm{id}$ ist über $\mathbb{Q}_\ell$ invertierbar. Daraus folgt $V_\ell(A)_{\gamma_v} = 0$. Alles in allem hat man also

$$A(\bar{K})[\ell^\infty]^{\mathrm{Frob}_v} \cong T_\ell(A)/(\gamma_v - \mathrm{id})T_\ell(A),$$

und damit auch

$$A_v(k_v)[\ell^\infty] \cong T_\ell(A)/(\gamma_v - \mathrm{id})T_\ell(A).$$

□

Definiere

$$D := \gamma_v - \mathrm{id} \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell).$$

Dann hat man das folgende Resultat.

Korollar 3.2.2. *Die folgenden Aussagen sind äquivalent*

(i) Der ℓ-Anteil der Reduktion von A an der Stelle v ist zyklisch.

(ii) $\mathrm{Rang}(D \mod \ell) \geq 2g - 1$.

Beweis. Nach Konstruktion gilt $D = \gamma_v - \mathrm{id}$. Nach Satz 3.2.1 gilt

$$A_v(k_v)[\ell^\infty] \cong T_\ell(A)/DT_\ell(A).$$

Die Gruppe $T_\ell(A)/DT_\ell(A)$ ist genau dann zyklisch, wenn $\big(T_\ell(A)/DT_\ell(A)\big) \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell$ zyklisch ist. Das wiederum ist äquivalent zur Bedingung $\mathrm{Rang}(D \mod \ell) \geq 2g - 1$. □

3.3 Vergleich von Untergruppen

Sei Λ eine endlich erzeugte torsionsfreie Untergruppe von $A(K)$, und sei Σ eine endlich erzeugte Untergruppe von Λ. Nun kann man sich fragen, wann die ℓ-Anteile der Reduktion von Λ und Σ übereinstimmen.

Nehme dazu an, dass der Quotient von Λ und Σ keine ℓ-Torsion hat. Da eine von ℓ verschiedene Torsion für den ℓ-Anteil keine Rolle spielt, kann man dann annehmen, dass $\Lambda = \Sigma \oplus \Sigma'$ gilt. Betrachte die formale Matrix

$$\tilde{\gamma}_v := \tilde{\rho}_\ell(\mathrm{Frob}_v) = \begin{pmatrix} \gamma_v & n_v \\ 0 & 1 \end{pmatrix}.$$

Dabei gilt $n_v \in \mathrm{Hom}\big(\Lambda, T_\ell(A)\big)$. Diese Element n_v lässt sich nun schreiben als $n_v = \begin{pmatrix} s_v & s'_v \end{pmatrix}$ mit $s_v \in \mathrm{Hom}\big(\Sigma, T_\ell(A)\big), s'_v \in \mathrm{Hom}\big(\Sigma', T_\ell(A)\big)$. Damit kann man $\tilde{\gamma}_v$ als 3×3-Blockmatrix auffassen

$$\tilde{\gamma}_v = \begin{pmatrix} \gamma_v & s_v & s'_v \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Satz 3.3.1. *Die folgenden Aussagen sind äquivalent*

(i) Die ℓ-Anteile der Reduktion von Λ und Σ stimmen überein.

(ii) $s'_v = s_v U + (\gamma_v - \mathrm{id})V$ für ein $U : \Sigma' \to \Sigma$ und ein $V : \Sigma' \to T_\ell(A)$.

Beweis. Die Aussage, dass die ℓ-Anteile der Reduktion von Λ und Σ übereinstimmen ist äquivalent zu

$$\kappa_v(\Lambda) = \kappa_v(\Sigma).$$

Nach Konstruktion hat man

$$\kappa_v(\Lambda) = (\gamma_v - \mathrm{id})^{-1} n_v(\Lambda) + T_\ell(A).$$

Mit der oben beschriebenen Zerlegung erhält man

$$\begin{aligned}(\gamma_v - \mathrm{id})^{-1} n_v(\Lambda) + T_\ell(A) &= (\gamma_v - \mathrm{id})^{-1} \begin{pmatrix} s_v & s'_v \end{pmatrix} (\Lambda) + T_\ell(A) \\ &= (\gamma_v - \mathrm{id})^{-1} (s_v\Sigma + s'_v\Sigma') + T_\ell(A) \\ &= (\gamma_v - \mathrm{id})^{-1} s_v\Sigma + (\gamma_v - \mathrm{id})^{-1} s'_v\Sigma' + T_\ell(A).\end{aligned}$$

Die Bedingung $\kappa_v(\Lambda) = \kappa_v(\Sigma)$ bedeutet genau, dass der ℓ-Anteil der Reduktion von Σ' schon im ℓ-Anteil der Reduktion von Σ liegt. Das wiederum ist gleichbedeutend mit

$$(\gamma_v - \mathrm{id})^{-1} s'_v\Sigma' \subset (\gamma_v - \mathrm{id})^{-1} s_v\Sigma + T_\ell(A).$$

Nach Multiplizieren mit $(\gamma_v - \mathrm{id})$ erhält man

$$s'_v\Sigma' \subset s_v\Sigma + (\gamma_v - \mathrm{id})T_\ell(A).$$

Das bedeutet aber genau, dass es ein $U : \Sigma' \to \Sigma$ und ein $V : \Sigma' \to T_\ell(A)$ gibt mit $s'_v = s_v U + (\gamma_v - \mathrm{id})V$. □

Als Spezialfall betrachte man nun die Situation, wenn der Rang von Σ gleich $n-1$ ist. In diesem Fall gilt $\Sigma' = \mathbb{Z}a$ für ein $a \in A(K)$. Wegen $\mathbb{Z}a \cong \mathbb{Z}$ kann man s'_v als Element von $T_\ell(A)$ auffassen. Damit erhält man das folgende Resultat.

Korollar 3.3.2. *Die folgenden Aussagen sind äquivalent*

(i) Der ℓ-Anteil der Reduktion von a liegt im ℓ-Anteil der Reduktion von Σ.

(ii) $s'_v = s_v U + (\gamma_v - \mathrm{id})V$ für ein $U \in \Sigma$ und ein $V \in T_\ell(A)$.

Betrachte nun zwei Punkte $a, b \in A(K)$ unendlicher Ordnung. Setze $\Lambda = \mathbb{Z}a \oplus \mathbb{Z}b$ und $\Sigma = \mathbb{Z}b$. In diesem Fall kann man s_v und s'_v als Elemente von $T_\ell(A)$ auffassen. Damit erhält man das folgende Resultat.

Korollar 3.3.3. *Seien a und b zwei Punkte unendlicher Ordnung von $A(K)$. Dann sind die folgenden Aussagen äquivalent*

(i) Der ℓ-Anteil der Reduktion von a ist ein Vielfaches des ℓ-Anteils der Reduktion von b.

(ii) $s'_v = ms_v + (\gamma_v - \mathrm{id})V$ für ein $m \in \mathbb{Z}_\ell^*$ und ein $V \in T_\ell(A)$.

Korollar 3.3.4. *Seien a und b zwei Punkte unendlicher Ordnung von $A(K)$. Dann sind die folgenden Aussagen äquivalent*

(i) Die ℓ-Anteile der Reduktion von a und b erzeugen dieselbe Untergruppe von $A_v(k_v)[\ell^\infty]$.

(ii) Es gibt ein $m \in \mathbb{Z}_\ell^*$ und ein $V \in T_\ell(A)$, sodass gilt $s'_v = ms_v + (\gamma_v - \mathrm{id})V$.

3.4 Zyklizität

In diesem Abschnitt soll nun untersucht werden, wann der ℓ-Anteil der Reduktion von Λ zyklisch ist. Bezeichne dazu mit $x_1, \ldots, x_{2g}$ die Spalten von m_v.

Satz 3.4.1. *Die folgenden Aussagen sind äquivalent*

(i) Der ℓ-Anteil der Reduktion von Λ ist zyklisch.

(ii) Es gibt eine Spalte x_i von m_v, sodass jede andere Spalte von m_v ein $\mathbb{Z}_\ell$-Vielfaches von x_i ist.

Beweis. Nach Satz 3.1.2 gilt

$$\kappa_v|_\Lambda = \pi_\ell(m_v).$$

Also ist der ℓ-Anteil der Reduktion von Λ genau dann zyklisch, wenn

$$\mathrm{Rang}(\pi_\ell(m_v) \mod \ell) \leq 1.$$

Nach Konstruktion gilt

$$\pi_\ell : V_\ell(\tilde{A}) \to V_\ell(\tilde{A})/T_\ell(\tilde{A}).$$

Also ist die obige Bedingung äquivalent dazu, dass es eine Spalte x_i von m_v gibt, sodass jede andere Spalte von m_v ein $\mathbb{Z}_\ell$-Vielfaches von x_i ist. □

3.5 Surjektivität von $\kappa_v|_\Lambda$

In diesem Abschnitt wird nun untersucht, wann der ℓ-Anteil der Reduktion von A an der Stelle v vom ℓ-Anteil der Reduktion von Λ erzeugt wird. Nach Konstruktion der Abbildung κ_v ist dies gleichbedeutend mit der Bedingung, dass $\kappa_v|_\Lambda$ surjektiv ist.

Satz 3.5.1. *Die folgenden Aussagen sind äquivalent*

(i) *Der ℓ-Anteil der Reduktion von A wird durch den ℓ-Anteil der Reduktion von Λ erzeugt.*

(ii) $\mathrm{Rang}\big((\tilde{\gamma}_v - \mathrm{id}) \mod \ell\big) = 2g.$

Beweis. Nach Konstruktion gilt

$$\kappa_v|_\Lambda \in \mathrm{Hom}\big(\Lambda, A[\ell^\infty]\big).$$

Nach Satz 3.2.1 gilt

$$A_v(k_v)[\ell^\infty] \cong A[\ell^\infty]^{\mathrm{Frob}_v}.$$

Also hat man

$$\kappa_v|_\Lambda \colon \Lambda \longrightarrow A[\ell^\infty]^{\mathrm{Frob}_v} \cong \big(V_\ell(A)/T_\ell(A)\big)^{\gamma_v}.$$

Die Elemente aus $\big(V_\ell(A)/T_\ell(A)\big)^{\gamma_v}$ entsprechen genau den $w \in V_\ell(A)$ mit $\gamma_v(w) \equiv w \mod 1$. Diese Bedingung ist gleichbedeutend mit

$$w \in (\gamma_v - \mathrm{id})^{-1}\big(T_\ell(A)\big).$$

Also ist $\kappa_v|_\Lambda$ genau dann surjektiv, wenn es für alle w wie oben ein $\lambda \in \Lambda$ gibt mit

$$m_v(\lambda) \equiv w \mod 1.$$

Das ist aber äquivalent zu

$$m_v(\Lambda) + T_\ell(A) = (\gamma_v - \mathrm{id})^{-1}\big(T_\ell(A)\big).$$

Dies wiederum ist gleichbedeutend mit

$$n_v(\Lambda) + (\gamma_v - \mathrm{id})\big(T_\ell(A)\big) = T_\ell(A).$$

Diese Bedingung ist genau dann erfüllt, wenn

$$\mathrm{Rang}\big((\gamma_v - \mathrm{id}, n_v) \mod \ell\big) = 2g. \tag{4}$$

Nach Definition gilt

$$\tilde{\gamma}_v = \begin{pmatrix} \gamma_v & n_v \\ 0 & 1 \end{pmatrix}.$$

Also ist (4) äquivalent zu $\mathrm{Rang}\big((\tilde{\gamma}_v - \mathrm{id}) \mod \ell\big) = 2g.$ $\square$

4 Dichtigkeitsaussagen

In diesem Kapitel geht es zunächst darum zu zeigen, dass bestimmte Mengen eine Dirichlet Dichte haben. Im zweiten Abschnitt wird dann untersucht, unter welchen Bedingungen diese Dichte positiv ist. Dabei bezeichnet μ das normierte Haar-Mass der Gruppe $\tilde{\Gamma}_\ell$ mit Gesamtvolumen 1.

4.1 Existenz von Dichten

Sei W eine Teilmenge von $\mathrm{Hom}\big(\Lambda, A[\ell^\infty]\big) = \tilde{A}[\ell^\infty]$. Die Elemente von $\tilde{\Gamma}_\ell$ haben die Form $\begin{pmatrix} \gamma & n \\ 0 & 1 \end{pmatrix}$ und werden der Einfachheit halber mit $\tilde{\gamma}$ bezeichnet. Definiere

$$U_W := \left\{ \tilde{\gamma} \in \tilde{\Gamma}_\ell \;\middle|\; \begin{array}{l} \det(\gamma - \mathrm{id}) \neq 0 \text{ und} \\ \pi_\ell\big((\gamma - \mathrm{id})^{-1} n\big) \in W \end{array} \right\}.$$

Definiere

$$S_{U_W} := \{v \in \Sigma \mid \rho_\ell(\mathrm{Frob}_v) \in U_W\}.$$

Nach Konstruktion gilt

$$S_{U_W} = \{v \in \Sigma \mid \kappa_v|_\Lambda \in W\}.$$

Theorem 4.1.1. *Für jede Teilmenge W von $\tilde{A}[\ell^\infty]$ hat die Menge S_{U_W} die Dirichlet Dichte $\mu(U_W)$.*

Beweis. Definiere

$$V_n := \left\{ \gamma \in \Gamma_\ell \;\middle|\; \begin{array}{l} \det(\gamma - \mathrm{id}) \neq 0 \text{ und} \\ (\gamma - \mathrm{id})^{-1} \equiv 0 \mod \ell^{-n} \end{array} \right\}.$$

Bezeichne mit μ' das normierte Haar-Mass auf Γ_ℓ mit Gesamtvolumen 1. Definiere

$$Z := \{\gamma \in \Gamma_\ell \mid \det(\gamma - \mathrm{id}) = 0\}.$$

Dies ist eine konjugationsinvariante, analytische Untervarietät kleinerer Dimension. Somit gilt nach Serre [11]

$$\mu'(Z) = 0.$$

Nun kann man $\Gamma_\ell \setminus Z$ durch die Mengen V_n ausschöpfen

$$\Gamma_\ell \setminus Z = \bigcup_{n \geq 0} V_n.$$

Definiere $U_{W,n} := U_W \cap \big(\tilde{\Gamma}_\ell \cap V_n \ltimes T_\ell(\tilde{A})\big)$. Dann kann man U_W ausschöpfen

$$U_W = \bigcup_{n \geq 0} U_{W,n}.$$

Lemma 4.1.2. *Die Menge* $\mathrm{Stab}_{\tilde{\Gamma}_\ell}(U_{W,n})$ *ist offen.*

Beweis. Sei $\gamma \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ mit

$$\det(\gamma - \mathrm{id}) \neq 0 \text{ und } (\gamma - \mathrm{id})^{-1} \equiv 0 \mod \ell^{-n},$$

und sei $\delta \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ mit $\delta \equiv \mathrm{id} \mod \ell^{2n}$. Dann folgt

$$\gamma\delta - \mathrm{id} \equiv \gamma - \mathrm{id} \mod \ell^{2n},$$

und somit

$$\begin{aligned} \ell^n(\gamma - \mathrm{id})^{-1}(\gamma\delta - \mathrm{id}) &\equiv \ell^n(\gamma - \mathrm{id})^{-1}(\gamma - \mathrm{id}) \mod \ell^{2n} \\ &\equiv \ell^n \,\mathrm{id} \mod \ell^{2n}. \end{aligned}$$

Also gibt es ein $u \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell)$ mit $u \equiv \mathrm{id} \mod \ell^n$ und

$$\ell^n(\gamma - \mathrm{id})^{-1}(\gamma\delta - \mathrm{id}) = \ell^n u.$$

Daraus folgt $\det(\delta\gamma - \mathrm{id}) \neq 0$.

Aus der Eigenschaft $u \equiv \mathrm{id} \mod \ell^n$ folgt $u^{-1} \equiv \mathrm{id} \mod \ell^n$. Nach Voraussetzung erfüllt γ die Bedingung $(\gamma - \mathrm{id})^{-1} \equiv 0 \mod \ell^{-n}$. Alles in allem hat man also

$$\begin{aligned} (\gamma\delta - \mathrm{id})^{-1} &= u^{-1}(\gamma - \mathrm{id})^{-1} \\ &\equiv (\gamma - \mathrm{id})^{-1} \mod 1. \end{aligned}$$

Es gilt also

$$\tilde{\Gamma}_\ell \cap \{\delta \in \mathrm{GL}_{2g}(\mathbb{Z}_\ell) \mid \delta \equiv \mathrm{id} \mod \ell^{2n}\} \ltimes \ell^n T_\ell(\tilde{A}) \subset \mathrm{Stab}_{\tilde{\Gamma}_\ell}(U_{W,n}).$$

Somit ist $\mathrm{Stab}_{\tilde{\Gamma}_\ell}(U_{W,n})$ offen. □

Nehme nun eine offene normale Untergruppe Δ von $\tilde{\Gamma}$, die in $\mathrm{Stab}_{\tilde{\Gamma}_\ell}(U_{W,n})$ liegt. Nach Galois-Theorie ist der Quotient $\tilde{\Gamma}_\ell/\Delta$ die Galois-Gruppe einer endlichen Erweiterung L von K in $\bar{K}$. Betrachte die Quotientenabbildung $\pi : \tilde{\Gamma}_\ell \twoheadrightarrow \mathrm{Gal}(L/K)$. Dann gilt

$$U_{W,n} = \pi^{-1}(\pi(U_{W,n})).$$

Somit hängt die Eigenschaft $\rho_\ell(\mathrm{Frob}_v) \in U_{W,n}$ nur von $\pi(\rho_\ell(\mathrm{Frob}_v))$ ab. Auf die endliche Körpererweiterung L/K kann man nun den Cebotarevschen Dichtigkeitssatz anwenden und erhält, dass die Menge $S_{U_{W,n}}$ die Dirichlet Dichte $\mu(U_{W,n})$ hat.

Die Menge $\{\tilde{\gamma} \in \tilde{\Gamma}_\ell \mid \det(\gamma - \mathrm{id}) = 0\}$ ist eine konjugationsinvariante, analytische Untervarietät kleinerer Dimension. Daraus folgt nach Serre [11]

$$\mu\big(\{\tilde{\gamma} \in \tilde{\Gamma}_\ell \mid \det(\gamma - \mathrm{id}) = 0\}\big) = 0. \tag{5}$$

Nach Konstruktion hat man U_W ausgeschöpft durch $U_W = \bigcup_{n \geq 0} U_{W,n}$. Deshalb gilt

$$\mu(U_W) = \lim_{n \to \infty} \mu(U_{W,n}). \tag{6}$$

Bezeichne mit $\overline{W}$ das Komplement von W in $\tilde{A}[\ell^\infty]$. Aus (5) folgt

$$\mu(U_W) + \mu(U_{\overline{W}}) = \mu(U_W \amalg U_{\overline{W}}) = \mu(U_{W \amalg \overline{W}}) = 1. \tag{7}$$

Bezeichne die untere Dirichlet Dichte mit $\underline{\delta}$, die obere Dirichlet Dichte mit $\overline{\delta}$ und die Dirichlet Dichte mit δ. Für alle $n \geq 0$ hat man $\underline{\delta}(S_{U_W}) \geq \underline{\delta}(S_{U_{W,n}}) = \mu(U_{W,n})$. Daraus folgt mit (6)

$$\underline{\delta}(S_{U_W}) \geq \mu(U_W).$$

Analog gilt $\underline{\delta}(S_{U_{\overline{W}}}) \geq \mu(U_{\overline{W}})$. Diese Aussage ist wegen (7) äquivalent zu

$$\overline{\delta}(S_{U_W}) \leq \mu(U_W).$$

Daraus folgt nun $\delta(S_{U_W}) = \mu(U_W)$. □

Man kann also die Dirichlet Dichte mit dem Haar-Mass ausdrücken. Damit kann man auch die Eigenschaften des Haar-Masses benutzen und erhält das folgende Resultat.

Korollar 4.1.3. *Die Dirichlet Dichte von S_{U_W} ist σ-additiv in W.*

Bemerkung. Es ist klar, dass die Dirichlet Dichte additiv ist in W für eine endliche disjunkte Vereinigung. Es ist aber a priori überhaupt nicht offensichtlich, dass sie sogar σ-additiv ist.

4.2 Positive Dichten

In diesem Abschnitt soll nun untersucht werden, welche S_{U_W} eine positive Dichte haben. Dazu seien $\tilde{a}$, $\tilde{A}$ und $\tilde{B}$ wie oben. Bezeichne mit S die endliche Menge von Stellen, an denen A schlechte Reduktion hat oder $v|\ell$ gilt. Für Dichtigkeitsaussagen kann man S vernachlässigen.

Sei $b \in \tilde{B}[\ell^\infty]$. Nehme eine spezielle Spaltung von (1) und definiere

$$U := \{\tilde{\gamma} \in \tilde{\Gamma}_\ell | \det(\gamma - \mathrm{id}) \neq 0\}.$$

Diese Menge ist offen in $\tilde{\Gamma}_\ell$. Die Abbildung

$$U \to \tilde{A}[\ell^\infty],\ \tilde{\gamma} \mapsto \pi_\ell\big((\gamma - \mathrm{id})^{-1} n\big)$$

ist stetig und somit lokal konstant. Also ist die Menge

$$U_b := \left\{ \tilde{\gamma} \in \tilde{\Gamma}_\ell \;\middle|\; \begin{array}{l} \det(\gamma - \mathrm{id}) \neq 0 \text{ und} \\ \pi_\ell\big((\gamma - \mathrm{id})^{-1} n\big) = b \end{array} \right\}$$

offen in $\tilde{\Gamma}_\ell$.

Lemma 4.2.1. *Die Menge U_b ist nicht leer.*

Beweis. Es gilt

$$\tilde{A}[\ell^\infty] \cong V_\ell(\tilde{A})/T_\ell(\tilde{A}).$$

Nach Definition ist π_ℓ die Abbildung $V_\ell(\tilde{A}) \to V_\ell(\tilde{A})/T_\ell(\tilde{A})$. Also genügt es zu zeigen, dass das Bild der Abbildung

$$U \to V_\ell(\tilde{A}),\ \begin{pmatrix} \gamma & n \\ 0 & 1 \end{pmatrix} \mapsto (\gamma - \mathrm{id})^{-1} n$$

die Menge $V_\ell(\tilde{B})$ umfasst. Es genügt, diese Aussage nach Ersetzen von K durch eine endliche Erweiterung zu zeigen. Mit Satz 2.2.2 kann man also annehmen, dass

$$\tilde{\Gamma}_\ell = \begin{pmatrix} \Gamma_\ell & N_\ell \\ 0 & 1 \end{pmatrix}$$

gilt. Dann genügt es zu zeigen, dass

$$V_\ell(\tilde{B}) = \bigcup_{\substack{\gamma \in \Gamma_\ell \\ \det(\gamma - \mathrm{id}) \neq 0}} (\gamma - \mathrm{id})^{-1} N_\ell$$

gilt. Nach Theorem 2.2.1 ist N_ℓ offen in $T_\ell(\tilde{B})$. Somit gibt es ein $k \in \mathbb{Z}$ mit

$$\ell^k T_\ell(\tilde{B}) \subset N_\ell.$$

Sei $v \notin S$, und sei $s \in \mathbb{N}$. Für jedes hinreichend divisible m erfüllt dann $\gamma := \rho_\ell(\mathrm{Frob}_v)^m$ die Bedingung $\gamma \equiv \mathrm{id} \mod \ell^s$.

Für dieses γ gilt dann

$$(\gamma - \mathrm{id}) T_\ell(\tilde{B}) \subset \ell^s T_\ell(\tilde{B}) \subset \ell^{s-rk} N_\ell.$$

Daraus folgt

$$\ell^{k-s} T_\ell(\tilde{B}) \subset (\gamma - \mathrm{id})^{-1} N_\ell.$$

Jetzt lässt man s gegen unendlich gehen. $\square$

Theorem 4.2.2. *Sei $b \in \tilde{B}[\ell^\infty]$. Dann hat die Menge S_{U_b} die Dirichlet Dichte $\mu(U_b)$, und diese Dichte ist positiv.*

Beweis. Nach Theorem 4.1.1 hat die Menge S_{U_b} die Dirichlet Dichte $\mu(U_b)$. Aus Lemma 4.2.1 folgt nun, dass $\mu(U_b) > 0$. $\square$

Bemerkung. In Theorem 4.2.2 wird eine Aussage über die Dichte von S_{U_b} für $b \in \tilde{B}[\ell^\infty]$ gemacht. Es ist klar, dass nur solche b als Reduktionsabbildungen auftreten können. Für $a \in \tilde{A}[\ell^\infty] \setminus \tilde{B}[\ell^\infty]$ gilt $S_{U_a} = \varnothing$.

Korollar 4.2.3. *Sei $k \geq 0$ eine ganze Zahl. Dann hat die Menge der Primstellen $v \notin S$, an denen der ℓ-Anteil der Reduktion von Λ Exponent ℓ^k hat, eine positive Dirichlet Dichte.*

Beweis. Nehme in Theorem 4.2.2 ein Element b der Ordnung ℓ^k. Dann hat die Menge aller Primstellen v mit $\kappa_v|_\Lambda = b$ eine positive Dirichlet Dichte. Für diese Stellen gilt somit $\ell^k \kappa_v|_\Lambda = 0$. $\square$

Man kann sich jetzt natürlich fragen, welche Dichtigkeitsaussagen im Zusammenhang mit der Zyklizität des ℓ-Anteiles der Reduktion von Λ gelten.

Beispiel. Sei A' eine abelsche Varietät über einem Zahlkörper K, und sei $a' \in A'(K)$ ein Punkt unendlicher Ordnung. Definiere

$$A := A' \times A', \text{ und } \Lambda := \mathbb{Z}a' \times \mathbb{Z}a'.$$

Dann ist das Reduktionsverhalten in beiden Faktoren dasselbe. Also ist der ℓ-Anteil der Reduktion von Λ genau dann zyklisch, wenn er trivial ist. Zudem ist die Ordnung des ℓ-Anteiles der Reduktion von Λ immer eine Quadratzahl.

Dieses Beispiel zeigt, dass man im allgemeinen nicht sagen kann, dass der ℓ-Anteil der Reduktion von Λ mit positiver Dichte zyklisch von einer gegebenen Ordnung ist. Ebenso kann man nicht sagen, dass die Ordnung des ℓ-Anteiles mit positiver Dichte eine bestimmte Zahl ist, da nicht immer alle Zahlen auftreten können.

4.3 Quantitatives Verhalten

In diesem Abschnitt geht es um das quantitative Verhalten der Dichten einiger bestimmter Mengen. Betrachte die Kompositionsabbildung

$$\begin{array}{rcl} \tilde{\Gamma}_\ell \setminus \{\tilde{\gamma} \in \tilde{\Gamma}_\ell \mid \det(\gamma - \mathrm{id}) = 0\} & \xrightarrow{\alpha} & V_\ell(\tilde{A}) \twoheadrightarrow V_\ell(\tilde{A})/T_\ell(\tilde{A}) \\ \tilde{\gamma} = (\gamma,\ n) & \mapsto & (\gamma - \mathrm{id})^{-1} n. \end{array}$$

Sei X eine Teilmenge von $V_\ell(\tilde{A})/T_\ell(\tilde{A})$. Dann ist X das Bild einer Menge $\tilde{X} \subset V_\ell(\tilde{A})$ mit

$$\tilde{X} + T_\ell(\tilde{A}) = \tilde{X}.$$

Nun möchte man $\mathrm{vol}\big(\alpha^{-1}(\tilde{X})\big)$ bestimmen. Definiere für $m \in \mathbb{Z}$

$$\Gamma_{\ell,m} := \{\gamma \in \Gamma_\ell \mid \gamma \equiv \mathrm{id} \mod \ell^m\}.$$

Die Gruppe $\tilde{\Gamma}_\ell$ ist offen in $\Gamma_\ell \ltimes T_\ell(\tilde{B})$. Deshalb gibt es ein $m \in \mathbb{Z}$ mit

$$\tilde{\Gamma}_{\ell,m} := \Gamma_{\ell,m} \ltimes \ell^m T_\ell(\tilde{B}) \subset \tilde{\Gamma}_\ell.$$

Die Gruppe $\tilde{\Gamma}_{\ell,m}$ hat endlichen Index in $\tilde{\Gamma}_\ell$. Also gibt es ein $s \in \mathbb{Z}$ und Elemente $\tilde{\gamma}_1 = (\gamma_1,\ n_1), \ldots, \tilde{\gamma}_s = (\gamma_s,\ n_s) \in \tilde{\Gamma}_\ell$ mit

$$\tilde{\Gamma}_\ell = \coprod_{i=1}^{s} \tilde{\gamma}_i \tilde{\Gamma}_{\ell,m}.$$

Man hat also

$$\mathrm{vol}\left(\alpha^{-1}(\tilde{X})\right) = \sum_i \mathrm{vol}\left(\alpha^{-1}(\tilde{X}) \cap \tilde{\gamma}_i \tilde{\Gamma}_{\ell,m}\right).$$

Für ein festes $i \in \{1, \ldots, s\}$ hat man

$$\begin{aligned}
\mathrm{vol}\left(\alpha^{-1}(\tilde{X}) \cap \tilde{\gamma}_i \tilde{\Gamma}_{\ell,m}\right) &= \int_{\gamma \in \Gamma_{\ell,m}} \int_{\substack{n \in \ell^m T_\ell(\tilde{B}) \\ (\gamma_i\gamma - \mathrm{id})^{-1}(\gamma_i n + n_i) \in \tilde{X}}} dn\, d\gamma \\
&= \int_{\gamma \in \Gamma_{\ell,m}} \int_{\substack{n \in \ell^m T_\ell(\tilde{B}) \\ \gamma_i n + n_i \in (\gamma_i\gamma - \mathrm{id})(\tilde{X})}} dn\, d\gamma \\
&= \int_{\gamma \in \Gamma_{\ell,m}} \int_{\substack{n \in \ell^m T_\ell(\tilde{B}) \\ n \in (\gamma - \gamma_i^{-1})(\tilde{X}) - \gamma_i^{-1} n_i}} dn\, d\gamma \\
&= \int_{\gamma \in \Gamma_{\ell,m}} \mathrm{vol}\left(\ell^m T_\ell(\tilde{B}) \cap \left((\gamma - \gamma_i^{-1})(\tilde{X}) - \gamma_i^{-1} n_i\right)\right) d\gamma.
\end{aligned}$$

Nun kann man versuchen, für bestimme Mengen $\tilde{X}$ diese Integrale zu bestimmen. Dazu sei $k \in \mathbb{Z}$. Definiere

$$\tilde{X} := \ell^{-k} T_\ell(\tilde{A}).$$

Wenn $\gamma_i^{-1} n_i \notin \ell^m T_\ell(\tilde{B}) + (\gamma - \gamma_i^{-1})\ell^{-k} T_\ell(\tilde{A})$ gilt, hat man

$$\mathrm{vol}\Big(\ell^m T_\ell(\tilde{B}) \cap \big((\gamma - \gamma_i^{-1})\ell^{-k} T_\ell(\tilde{A}) - \gamma_i^{-1} n_i\big)\Big) = 0.$$

Wenn $\gamma_i^{-1} n_i \in \ell^m T_\ell(\tilde{B}) + (\gamma - \gamma_i^{-1})\ell^{-k} T_\ell(\tilde{A})$ gilt, hat man

$$\mathrm{vol}\Big(\ell^m T_\ell(\tilde{B}) \cap \big((\gamma - \gamma_i^{-1})\ell^{-k} T_\ell(\tilde{A}) - \gamma_i^{-1} n_i\big)\Big) = \mathrm{vol}\Big(\ell^m T_\ell(\tilde{B}) \cap (\gamma - \gamma_i^{-1})\ell^{-k} T_\ell(\tilde{A})\Big).$$

Definiere

$$t := \mathrm{Rang}\,\big(T_\ell(\tilde{A})\big).$$

Damit erhält man im zweiten Fall

$$\begin{aligned} \mathrm{vol}\Big(\ell^m T_\ell(\tilde{B}) \cap (\gamma - \gamma_i^{-1})\ell^{-k} T_\ell(\tilde{A})\Big) &= \ell^{kt}\,\mathrm{vol}\Big(\ell^{k+m} T_\ell(\tilde{B}) \cap (\gamma - \gamma_i^{-1}) T_\ell(\tilde{A})\Big) \\ &= \frac{\ell^{kt}}{\big[T_\ell(\tilde{A}) \;:\; \ell^{k+m} T_\ell(\tilde{B}) \cap (\gamma - \gamma_i^{-1}) T_\ell(\tilde{A})\big]}\,. \end{aligned}$$

Das Bestimmen der obigen Integrale führt zu ziemlich komplizierten Berechnungen, die den Rahmen dieser Arbeit sprengen würden. Als Beispiel wird hier noch der einfachste Fall einer semiabelschen Varietät, also der Fall der multiplikativen Gruppe, untersucht. Dann gilt $t = 1$ und

$$\tilde{\Gamma}_\ell \subset \mathbb{Z}_\ell^* \ltimes \mathbb{Z}_\ell.$$

Die Bedingung

$$\gamma_i^{-1} n_i \notin \ell^m \mathbb{Z}_\ell + (\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell$$

ist dann äquivalent zu

$$n_i \notin \ell^m \mathbb{Z}_\ell + (\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell.$$

In diesem Fall gilt wieder

$$\mathrm{vol}\Big(\ell^m \mathbb{Z}_\ell \cap \big((\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell - \gamma_i^{-1} n_i\big)\Big) = 0.$$

Wenn $n_i \in \ell^m \mathbb{Z}_\ell + (\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell$ gilt, hat man

$$\begin{aligned} \mathrm{vol}\Big(\ell^m \mathbb{Z}_\ell \cap \big((\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell - \gamma_i^{-1} n_i\big)\Big) &= \mathrm{vol}\Big(\ell^m \mathbb{Z}_\ell \cap (\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell\Big) \\ &= \ell^k\,\mathrm{vol}\Big(\ell^{k+m}\mathbb{Z}_\ell \cap (\gamma - \gamma_i^{-1})\mathbb{Z}_\ell\Big). \end{aligned}$$

Der Vorteil in diesem Beispiel ist nun, dass von den beiden Moduln $\ell^{k+m}\mathbb{Z}_\ell$ und $(\gamma - \gamma_i^{-1})\mathbb{Z}_\ell$ immer einer in dem anderen enthalten ist. Deshalb gilt

$$\operatorname{vol}\Big(\ell^m\mathbb{Z}_\ell \cap \big((\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell - \gamma_i^{-1}n_i\big)\Big) = \ell^k \min\{\ell^{-k-m},\ \left|\gamma - \gamma_i^{-1}\right|_\ell\}.$$

Alles in allem hat man also für die $i \in \{1, \ldots, s\}$ mit $n_i \in \ell^m\mathbb{Z}_\ell + (\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell$ die folgenden Gleichungen

$$\int_{\gamma\in\Gamma_{\ell,m}} \operatorname{vol}\Big(\ell^m\mathbb{Z}_\ell \cap \big((\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell - \gamma_i^{-1}n_i\big)\Big)\, d\gamma = \int_{\gamma\in\Gamma_{\ell,m}} \min\{\ell^{-m},\ \ell^k\left|\gamma - \gamma_i^{-1}\right|_\ell\}\, d\gamma.$$

Im Fall der multiplikativen Gruppe gilt

$$\Gamma_{\ell,m} = 1 + \ell^m\mathbb{Z}_\ell.$$

Indem man nun vom normierten Haar-Mass auf $\Gamma_{\ell,m}$ zum normierten additiven Haar-Mass auf $\mathbb{Z}_\ell$ übergeht, ändern sich die Ausdrücke um eine von ℓ unabhängige Konstante a. Die Bedingung $n_i \in \ell^m\mathbb{Z}_\ell + (\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell$ wird dann zu $n_i \in \ell^m\mathbb{Z}_\ell + (1 + \ell^m x - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell$. Also hat man

$$\int_{\gamma\in\Gamma_{\ell,m}} \operatorname{vol}\ \ \ell^m\mathbb{Z}_\ell \cap\ \ (\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell - \gamma_i^{-1}n_i \quad d\gamma = a\int_{x\in\mathbb{Z}_\ell} \min\{\ell^{-m},\ \ell^k\ \ 1 + \ell^m x - \gamma_i^{-1}\ \ {}_\ell\}\, dx.$$

Jetzt muss man zwei Fälle unterscheiden. Zunächst betrachtet man die $i \in \{1, \ldots, s\}$ mit $\gamma_i \not\equiv 1 \mod \ell^m$. Für diese γ_i gilt

$$1 - \gamma_i^{-1} \not\equiv 0 \mod \ell^m.$$

Also ist die Bedingung $n_i \in \ell^m\mathbb{Z}_\ell + (1 + \ell^m x - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell$ äquivalent zu

$$n_i \in \ell^m\mathbb{Z}_\ell + (1 - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell,$$

und somit unabhängig von x. Dies ist gleichbedeutend mit

$$\ell^k n_i \in \ell^{k+m}\mathbb{Z}_\ell + (1 - \gamma_i^{-1})\mathbb{Z}_\ell.$$

Da nun $1 - \gamma_i^{-1} \not\equiv 0 \mod \ell^m$ gilt, hat man

$$\ell^{m-1}\mathbb{Z}_\ell \subset (1 - \gamma_i^{-1})\mathbb{Z}_\ell.$$

Also ist die obige Bedingung für $k \geq m - 1$ erfüllt. Für k hinreichend gross gilt natürlich

$$\min\{\ell^{-m},\ \ell^k\left|1 - \gamma_i^{-1}\right|_\ell\} = \ell^{-m}.$$

Alles in allem gilt also für die $i \in \{1, \ldots, s\}$ mit $\gamma_i \not\equiv 1 \mod \ell^m$ und für k hinreichend gross

$$\int_{\gamma \in \Gamma_{\ell,m}} \mathrm{vol}\left(\ell^m \mathbb{Z}_\ell \cap \left((\gamma - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell - \gamma_i^{-1} n_i\right)\right) d\gamma = c_i' \ell^{-m} \tag{8}$$

für Konstanten c_i'.

Als nächstes betrachtet man die $i \in \{1, \ldots, s\}$ mit $\gamma_i \equiv 1 \mod \ell^m$. Für diese γ_i kann man ohne Beschränkung der Allgemeinheit annehmen, dass $\gamma_i = 1$ gilt. Die Bedingung $n_i \in \ell^m \mathbb{Z}_\ell + (1 + \ell^m x - \gamma_i^{-1})\ell^{-k}\mathbb{Z}_\ell$ ist dann äquivalent zu

$$n_i \in \ell^m \mathbb{Z}_\ell + \ell^{m-k}\mathbb{Z}_\ell,$$

was für $k \geq m$ erfüllt ist. Also hat man für k hinreichend gross

$$\begin{aligned}
a \int_{x \in \mathbb{Z}_\ell} \min\{\ell^{-m},\ \ell^k \left|1 + \ell^m x - \gamma_i^{-1}\right|_\ell\} &= a \int_{x \in \mathbb{Z}_\ell} \min\{\ell^{-m},\ \ell^k \left|\ell^m x\right|_\ell\}\, dx \\
&= a\ell^{-m} \int_{x \in \mathbb{Z}_\ell} \min\{1,\ \ell^k \left|x\right|_\ell\}\, dx \\
&= a\ell^{-m} \sum_{j=0}^{\infty} \frac{\ell^{-j}}{1 - \ell^{-1}} \min\{1,\ \ell^{k-j}\} \\
&= a \frac{\ell^{-m}}{1 - \ell^{-1}} \left(\sum_{j=0}^{k-1} \ell^{-j} + \sum_{j=k}^{\infty} \ell^{2k-2j}\right) \\
&= a \frac{\ell^{-m}}{1 - \ell^{-1}} \left(\frac{1 - \ell^{-k}}{1 - \ell^{-1}} + \frac{\ell^{-k}}{1 - \ell^{-2}}\right) \\
&= b_i + c_i' \ell^{-k},
\end{aligned}$$

für eine Konstante c_i'.

Jetzt muss man noch über die i summieren. Mit (8) folgt dann, dass es Konstanten b und c' gibt, sodass für k hinreichend gross gilt

$$\mathrm{vol}\left(\alpha^{-1}(\ell^{-k}\mathbb{Z}_\ell)\right) = b + c'\ell^{-k}.$$

Da hier mit dem normierten Haar-Mass gerechnet wurde, gilt

$$\lim_{k \to \infty} \mathrm{vol}\left(\alpha^{-1}(\ell^{-k}\mathbb{Z}_\ell)\right) = 1.$$

Also muss

$$b = 1, \text{ und } c' \leq 0$$

gelten. Definiere $c := -c'$. Damit erhält man für die multiplikative Gruppe das folgende Resultat.

Satz 4.3.1. *Es gibt eine Konstante c, sodass für k hinreichend gross gilt* $\mathrm{vol}\Big(\alpha^{-1}(\ell^{-k}\mathbb{Z}_\ell)\Big) = 1 - c\ell^{-k}$.

Beweis. Die Behauptung folgt aus den obigen Ausführungen. □

Bemerkung. Die Tatsache, dass von den beiden Moduln $\ell^{k+m}\mathbb{Z}_\ell$ und $(\gamma - \gamma_i^{-1})\mathbb{Z}_\ell$ immer einer in dem anderen enthalten ist, erlaubt es, die Berechnungen im Fall der multiplikativen Gruppe ziemlich direkt durchzuführen. Im allgemeinen Fall muss man aber mit den Moduln $\ell^m T_\ell(\tilde{A})$ und $(\gamma - \gamma_i^{-1})\ell^{-k}T_\ell(\tilde{A})$ arbeiten. Für diese Moduln gilt aber nicht mehr, dass immer einer in dem anderen enthalten ist. Dadurch wird es ziemlich kompliziert, den Ausdruck $\mathrm{vol}\Big(\ell^m T_\ell(\tilde{A}) \cap (\gamma - \gamma_i^{-1})\ell^{-k}T_\ell(\tilde{A})\Big)$ zu bestimmen.

Literatur

[1] M. Bashmakov: *The cohomology of abelian varieties over a number field*, Russian Mathematical Surveys 27 (6), 1977, 25-70

[2] D. Bertrand: *Galois representations and transcendental numbers*, New advances in transcendence theory (Durham, 1986), Cambridge University Press, 1988, 37-55

[3] A. Borel: *Linear Algebraic Groups*, Springer-Verlag, New York etc., 1991

[4] D. Eisenbud, J. Harris: *The Geometry of Schemes*, Springer-Verlag, New York etc., 2000

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

[6] M. Hindry: *Autour d'une conjecture der Serge Lang*, Inventiones mathematicae 94, 1988, 575-603

[7] J. S. Milne: *Abelian Varieties*, Arithmetic Geometry, G. Cornell, J. H. Silverman(Hrsg.), Springer-Verlag, New York etc., 1986

[8] R. Pink: *On the Order of the Reduction of a Point on an Abelian Variety*, Preprint(15 p.), 28. 6. 2003

[9] K. A. Ribet: *Kummer theory on extensions of abelian varieties by tori*, Duke Mathematical Journal 46 No. 4, 1979, 745-761

[10] J.-P. Serre: *Lettre à Ken Ribet du 1. 1. 1981*, Oeuvres vol. IV, Springer-Verlag, Berlin etc., 2000, 1-17

[11] J.-P. Serre: *Quelques applications du théorème de densité de Chebotarev*, Publications mathématiques de l'I.H.É.S., tome 54 (1981), 123-201

[12] J.-P. Serre: *Résumé des cours de 1985-1986*, Annuaire du Collège de France (1986), 05-99 = Oeuvres vol. IV, Spriger-Verlag, Berlin etc., 2000, 33-37