Invent. math. 73, 349–366 (1983)

Inventiones mathematicae

Endlichkeitssätze für abelsche Varietäten über Zahlkörpern

G. Faltings

Fachbereich Mathematik, Bergische Universitäts-Gesamthochschule Wuppertal, Gaußstr. 20, D-5600 Wuppertal 1, Bundesrepublik Deutschland

§1. Einleitung

Sei K eine endliche Erweiterung von $\mathbb{Q}$, A eine über K definierte abelsche Varietät, $\pi=\mathrm{Gal}(\bar{K}/K)$ die absolute Galois-Gruppe von K, l eine Primzahl. Dann operiert π auf dem Tate-Modul

$$T_l(A)=\varprojlim A[l^n](\bar{K}).$$

Ziel der vorliegenden Arbeit ist der Beweis der folgenden Resultate:

a) Die Darstellung von π auf $T_l(A)\otimes_{\mathbb{Z}_l}\mathbb{Q}_l$ ist halbeinfach.

b) Die Abbildung

$$\mathrm{End}_K(A)\otimes_{\mathbb{Z}}\mathbb{Z}_l\to\mathrm{End}_\pi(T_l(A))$$

ist ein Isomorphismus.

c) Sei S eine endliche Menge von Stellen von K, $d>0$. Dann gibt es nur endlich viele Isomorphieklassen d-fach polarisierter abelscher Varietäten über K, welche gute Reduktion außerhalb S haben.

a) und b) sind bekannt unter dem Namen Tate-Vermutung, c) als Shafarevich-Vermutung. Weiter weiß man ([9]), daß aus c) die Mordell-Vermutung folgt. Die Tate-Vermutung ist von Tate selbst für abelsche Varietäten über endlichen Körpern gezeigt worden. Zarhin verallgemeinerte dies auf Funktionenkörper ([15, 16]) über solchen, und unser Beweis ist eine Übertragung seiner Methoden auf den Zahlkörper-Fall. Das zur Übersetzung notwendige Wörterbuch hat Arakelov geliefert ([2]), und seine Methoden sind vom Verfasser ausgebaut worden ([5]). Kurz gesagt handelt es sich darum, „alles“ mit hermiteschen Metriken zu versehen.

Der Beweis für c) erfolgt so, daß zunächst nur die Endlichkeit für Isogenie-Klassen gezeigt wird. Die grundlegende Idee dazu hat mir der Gutachter der „Inventiones“ anläßlich der Veröffentlichung meiner Arbeit [6] mitgeteilt, und ich mußte sie nur noch von der Hodge-Theorie in die étale Kohomologie über-setzen. Ich möchte daher dem mir persönlich unbekannten Gutachter an dieser Stelle für seine Anregung herzlich danken.

Der Rest des Beweises von c) benutzt eine Variante der bei a) und b) verwendeten Methoden.

Die Arbeit beginnt zunächst mit einigen technischen Details über Höhen. Die Komplikationen ergeben sich daraus, daß meines Wissens noch kein guter Modulraum semiabelscher Varietäten über $\mathbb{Z}$ existiert. (Mit ähnlichen Problemen hat sich auch L. Moret-Bailly zu kämpfen, der die Verhältnisse über Funktionenkörpern untersucht ([7]).) Danach werden die sehr schönen Ergebnisse von Tate ([13]) über p-divisible Gruppen benutzt. Der Schluß ist dann wieder etwas technischer.

Ich habe viel über das Thema von L. Szpiro gelernt, dem ich an dieser Stelle für seine Einführung in diesen Problemkreis danke. P. Deligne hat mich auf eine Unstimmigkeit in der ursprünglichen Fassung der Arbeit aufmerksam gemacht.

§2. Semiabelsche Varietäten

Definition. Sei S ein Schema (oder ein algebraic stack). Eine semiabelsche Varietät der relativen Dimension g über S ist eine glatte algebraische Gruppe p: $G \to S$, so daß die Fasern von p zusammenhängend von der Dimension g sind, und Erweiterungen einer abelschen Varietät durch einen Torus.

Beispiel. Sei q: $C \to S$ eine stabile Kurve vom Geschlecht g ([4]). Dann ist

$$J = \mathrm{Pic}^{\tau}(C/S) \to S$$

eine semiabelsche Varietät der relativen Dimension g.

Wir benötigen das folgende

Lemma 1. *Sei S normal, $U \subset S$ offen und dicht p_1: $A_1 \to S$ und p_2: $A_2 \to S$ zwei semiabelsche Varietäten, ϕ: $A_1/U \to A_2/U$ ein über U definierter Homomorphismus algebraischer Gruppen. Dann läßt sich ϕ eindeutig auf ganz S fortsetzen.*

Beweis. Dies ist wohlbekannt, falls S Spektrum eines kompletten diskreten Bewertungsringes ist. Im allgemeinen reduziert man sofort auf S noethersch und exzellent, und bezeichnet mit

$$X \subseteq A_1 \times_s A_2$$

den Abschluß des Graphen von ϕ.

Nach Basiswechsel mit geeigneten Bewertungsringen sieht man, daß die Projektion pr_1: $X \to A_1$ eigentlich ist, und daß ihre Fasern nur einen Punkt besitzen. Da A_1 normal ist, muß pr_1 ein Isomorphismus sein, und X der Graph der eindeutig bestimmten Fortsetzung von ϕ. (Eindeutigkeit folgt zum Beispiel durch Betrachtung von Torsionspunkten, oder auf tausend andere Arten.)

Definition. Sei p: $A \to S$ eine semiabelsche Varietät der relativen Dimension g, s: $S \to A$ der Nullschnitt.

Setze:

$$\omega_{A/S} = s^*(\Omega^g_{A/S}),$$

$\omega_{A/S}$ ist ein Geradenbündel auf S.

Bemerkungen. a) Wenn p eigentlich ist, so ist $\omega_{A/S} \cong p_*(\Omega^g_{A/S})$.

b) $\omega_{A/S}$ kommutiert mit Basiswechsel.

c) Wenn $A = \mathrm{Pic}^\tau(C/S)$ mit einer stabilen Kurve $q\colon C \to S$, so ist $\omega_{A/S} \cong \Lambda^g q_*(\omega_{C/S})$, wobei $\omega_{C/S}$ den relativen dualisierenden Modul bezeichnet.

d) Wenn $S = \mathrm{Spec}(\mathbb{C})$ und p eigentlich ist (d.h., $A/\mathbb{C}$ ist eine komplexe abelsche Varietät), so besitzt

$$\omega_{A/S} \cong \Gamma(A, \Omega^g_{A/\mathbb{C}})$$

ein kanonisches hermitesches Skalarprodukt:

Wenn α, β holomorphe Differentialformen auf A sind, so setze

$$\langle \alpha, \beta \rangle = \left(\frac{i}{2}\right)^g \int_A \alpha \wedge \bar{\beta}.$$

Wir benötigen einige Tatsachen über die Modulräume stabiler Kurven und abelscher Varietäten. Dazu scheint die Sprache der „algebraic stacks" am angemessensten zu sein. Falls dem Leser diese Notation zu abstrakt erscheint, so möge er die folgenden Überlegungen durchführen:

Es geht eigentlich um Endlichkeitsaussagen.

Wenn $\mathfrak{S}$ einer der demnächst einzuführenden algebraic stacks ist, und S den zugehörigen groben Modulraum bezeichnet, so gibt es stets eine offene Überdeckung

$$S = \bigcup_{i=1}^{r} U_i$$

und endlich surjektive Abbildungen $V_i \to U_i$, so daß über V_i das „universelle Objekt zu $\mathfrak{S}$" existiert. Man kann dann alle Rechnungen in den V_i durchführen.

Nun zu den hier verwendeten algebraic stacks.

1. $\overline{\mathfrak{M}}_g$ klassifiziere die stabilen Kurven vom Geschlecht g ([4]). $\overline{\mathfrak{M}}_g$ ist eigentlich über $\mathrm{Spec}(\mathbb{Z})$, und der zugehörige grobe Modulraum heiße $\overline{M}_g$.

2. $\mathfrak{A}_g$ klassifiziere die prinzipal-polarisierten abelschen Varietäten der relativen Dimension g, und A_g sei der zugehörige Modulraum.

$\mathfrak{A}_g$ ist nicht eigentlich über $\mathrm{Spec}(\mathbb{Z})$, aber die folgenden Tatsachen sind bekannt:

a) Wenn

$$p\colon A \to \mathfrak{A}_g$$

die universelle abelsche Varietät über $\mathfrak{A}_g$ bezeichnet, so gibt es ein $r > 0$, für welches $(\omega_{A/\mathfrak{A}_g})^{\otimes r}$ ein sehr amples Geradenbündel auf $A_g/\mathbb{Q}$ definiert ([3]). Sei $\bar{A}_g/\mathbb{Q}$ der Zariski-Abschluß von $A_g/\mathbb{Q}$ in dem zugehörigen projektiven Raum $\mathbb{P}^N_{\mathbb{Q}}$, $\bar{A}_g/\mathbb{Z}$ der Zariski-Abschluß in $\mathbb{P}^N_{\mathbb{Z}}$, und $\mathcal{M}$ das Geradenbündel $\mathcal{O}(1)$ auf $\bar{A}_g/\mathbb{Z}$. ($\mathcal{M}$ setzt auf $\bar{A}_g/\mathbb{Q}$ $(\omega_{A/\mathfrak{A}_g})^{\otimes r}$ fort.)

b) Es gibt über $\mathbb{C}$ einen eigentlichen dominanten Morphismus

$$\phi\colon \mathfrak{N} \to \bar{A}_g/\mathbb{C},$$

so daß über $\mathfrak{N}$ eine semiabelsche Varietät existiert, welche die universelle abelsche Varietät über $\mathfrak{A}_g$ fortsetzt (siehe [8], §9). Außerdem ist bekannt, daß $\omega^{\otimes r}$ dieser semiabelschen Varietät isomorph zu $\phi^*(\mathscr{M})$ ist. (Hierzu muß man direkt rechnen, siehe meine Ausführungen dazu in [6], §2.)

Lemma 2. *Es gibt über* $\operatorname{Spec}(\mathbb{Z})$ *einen eigentlichen algebraic stack* $\mathfrak{Z}$, *eine offene Teilmenge* $\mathfrak{U} \subset \mathfrak{Z}$ *und einen eigentlichen Morphismus* $\psi\colon \mathfrak{U} \to \mathfrak{A}_g$, *welcher sich zu einem* $\bar{\psi}\colon \mathfrak{Z}/\mathbb{Q} \to \bar{A}_g/\mathbb{Q}$ *fortsetzt, so daß über* $\mathfrak{Z}$ *die folgenden Objekte existieren:*

a) *Eine stabile Kurve* $q\colon C \to \mathfrak{Z}$.

b) *Ein Untergeradenbündel* (*= lokal direkter Sumand*) $\mathscr{L} \subseteq \Lambda^g q_*(\omega_{C/\mathbb{Z}})$.

c) *Über* $\mathfrak{U}$ *ein Paar von Gruppenhomomorphismen*

$$\alpha\colon \operatorname{Pic}^\tau(C/\mathfrak{Z}) \to \psi^*(A),$$
$$\beta\colon \psi^*(A) \to \operatorname{Pic}^\tau(C/\mathfrak{Z})$$

mit

$$\alpha \circ \beta = \textit{Multiplikation mit einem } d \in \mathbb{N},\ d \neq 0.$$

(*Dabei sei A wieder die universelle abelsche Varietät über* $\mathfrak{A}_g$.)

d) *Auf* $\mathfrak{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ *existiert ein Isomorphismus* $\mathscr{L}^{\otimes r} = \bar{\psi}^*(\mathscr{M})$, *und* $\mathscr{L}$ *ist über* $\mathfrak{U}/\mathbb{Q}$ *das Bild von*

$$\alpha^*\colon \psi^*(\omega_{A/\mathfrak{A}_g}) \to \Lambda^g q_*(\omega_{C/Z}).$$

Der daraus resultierende Isomorphismus (*über* $\mathfrak{U}/\mathbb{Q}$)

$$\psi^*(\omega_{A/\mathfrak{A}_g})^{\otimes r} \cong \psi^*(\mathscr{M})$$

ist ψ^**-Pullback des bei der Konstruktion von* $\mathscr{M}$ *angegebenen Isomorphismus über* A_g.

Beweis. In dem generischen Punkte von $\mathfrak{A}_g$ ist die zugehörige abelsche Varietät Quotient einer Jacobischen. Die zugehörige Kurve entspricht einer rationalen Abbildung von $\mathfrak{A}_g$ in $\overline{\mathfrak{M}}_{\tilde{g}}$, für ein $\tilde{g}$.

Wenn man den Graphen dieser Abbildung betrachtet, so erhält man (mit Hilfe einiger trivialer Zusatzüberlegungen) einen ersten Kandidaten $\mathfrak{Z}$, so daß schon a) und (nach Lemma 1) c) erfüllt sind. $\mathscr{L}$ ist dann über $\mathfrak{U} \otimes_{\mathbb{Z}} \mathbb{Q}$ durch d) schon festgelegt, und liefert eine rationale Abbildung von $\mathfrak{U} \otimes_{\mathbb{Z}} \mathbb{Q}$ in ein geeignetes projektives Bündel über $\mathfrak{Z}$. Man ersetzt $\mathfrak{Z}$ durch die Normalisierung des Abschlusses des zugehörigen Graphen, und dann sind auch b) und der zweite Teil von d) erfüllt. Zum Rest von d) ist zu vermerken, daß man den gesuchten Isomorphismus schon über $\mathfrak{U} \otimes_{\mathbb{Z}} \mathbb{Q}$ konstruiert hat, und man muß nur noch die Fortsetzbarkeit auf $\mathfrak{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ zeigen. Dazu kann man den Grundkörper von $\mathbb{Q}$ auf $\mathbb{C}$ erweitern, und es reicht, die Fortsetzbarkeit für ein $\tilde{\mathfrak{Z}}/\mathbb{C}$ zu zeigen, welches dominant und eigentlich über $\mathfrak{Z}$ liegt.

Mit Hilfe des weiter oben eingeführten $\phi\colon \mathfrak{N} \to \bar{A}_g/\mathbb{C}$ konstruiert man ein normales $\tilde{\mathfrak{Z}}$, so daß $\psi^*(A)$ sich auf $\tilde{\mathfrak{Z}}$ zu einer semiabelschen Varietät fortsetzt. Nach Lemma 1 kann man auch α und β fortsetzen, und diese liefern den gewünschten Isomorphismus über $\tilde{\mathfrak{Z}}$.

Korollar. *Es gibt eine natürliche Zahl* $e > 0$ *mit der folgenden Eigenschaft:*

Sei K ein Zahlkörper, R der Ring der ganzen Zahlen in K,

$$p\colon A \to \operatorname{Spec}(R)$$

eine semiabelsche Varietät, so daß die generische Faser A/K eigentlich über K ist, und eine prinzipale Polarisation bestitzt. Dem entspricht eine Abbildung ρ: $\operatorname{Spec}(K) \to A_g/\mathbb{Q}$, welche sich zu einem ρ: $\operatorname{Spec}(R) \to \bar{A}_g/\mathbb{Z}$ fortsetzt.

Nach Konstruktion besteht ein Isomorphismus

$$\rho^*(\mathscr{M}) \otimes_R K \cong (\omega_{A/R})^{\otimes r} \otimes_R K.$$

Unter Benutzung dieses Isomorphismus gilt:

$$e \cdot \rho^*(\mathscr{M}) \subseteq (\omega_{A/R})^{\otimes r} \subseteq e^{-1} \cdot \rho^*(\mathscr{M}) (\subseteq \rho^*(\mathscr{M}) \otimes_R K).$$

Beweis. Wir dürfen annehmen, daß $\bar{\psi}$: $\mathfrak{Z}/\mathbb{Q} \to \bar{A}_g/\mathbb{Q}$ sich fortsetzt zu einem eigentlichen $\bar{\psi}$: $\mathfrak{Z}/\mathbb{Z} \to \bar{A}_g/\mathbb{Z}$. Dann gibt es eine endliche Körpererweiterung $K' \supseteq K$ (mit ganzen Zahlen $R' \subseteq K'$), so daß sich ρ liften läßt zu

$$\tilde{\rho}\colon \operatorname{Spec}(R') \to \mathfrak{Z}.$$

Da über $\mathfrak{Z} \otimes_{\mathbb{Z}} \mathbb{Q}$ $\bar{\psi}^*(\mathscr{M})$ und $\mathscr{L}^{\otimes r}$ isomorph sind, gibt es ein $e_1 > 0$, *so daß über* $\mathfrak{Z}$

$$e_1 \cdot \mathscr{L}^{\otimes r} \subseteq \bar{\psi}^*(\mathscr{M}) \subseteq e_1^{-1} \cdot \mathscr{L}^{\otimes r}.$$

Es reicht, die Behauptung nach dem Basiswechsel zu R' zu zeigen, und wir müssen nur noch $\omega_{A/R'}$ und $\tilde{\rho}^*(\mathscr{L})$ vergleichen.

Durch Pullback erhält man eine stabile Kurve

$$q\colon C \to \operatorname{Spec}(R')$$

und

$$\alpha\colon \operatorname{Pic}^{\tau}(C/R') \to A/R', \qquad \beta\colon A/R' \to \operatorname{Pic}^{\tau}(C/R')$$

mit $\alpha \circ \beta = d \cdot \mathrm{id}$ (Benutze Lemma 1 über R'), so daß $\tilde{\rho}^*(\mathscr{L})$ das Unterbündel von $\Lambda^g q_*(\omega_{C/R'})$ ist, welches vom Bild von

$$\alpha^*\colon \omega_{A/R'} \to \Lambda^g q_*(\omega_{C/R'})$$

erzeugt wird. Daraus folgt unmittelbar, daß $d^g \cdot \tilde{\rho}^*(\mathscr{L}) \subseteq \omega_{A/R'} \subseteq \tilde{\rho}^*(\mathscr{L})$, und wir sind fertig.

§ 3. Höhen

Sei K wieder ein Zahlkörper, R der Ring der ganzen Zahlen in K. Analog zu [5] definieren wir ein metrisiertes Geradenbündel auf $\operatorname{Spec}(R)$ als einen projektiven R-Modul P vom Rang 1, zusammen mit Normen $\| \ \|_v$ auf $P \otimes_R K_v$ für alle unendlichen Stellen v von K. Dabei bezeichnet K_v die Komplettierung von K in v, und wir definieren ein $\varepsilon_v = 1$ oder 2, je nachdem ob $K_v \cong \mathbb{R}$ oder $K_v \cong \mathbb{C}$.

Der Grad des metrisierten Geradenbündels wird definiert als („#“ = Ordnung)

$$\mathrm{Grad}(P, \|\ \|) = \log(\#(P/R\cdot p)) - \sum_v \varepsilon_v \cdot \log \|p\|_v.$$

Dabei ist p ein von Null verschiedenes Element von P, die Summe geht über alle unendlichen Stellen von K, und die rechte Seite ist selbstverständlich unabhängig von p.

Bemerkung. Der Begriff des metrischen Geradenbündels stammt von Arakelov ([2]). Der Grad von P hängt natürlich auch mit dem Volumen von P zusammen.

Uns interessieren besonders die metrisierten Geradenbündel $\omega_{A/R}$, wobei

$$p\colon\ A \to \mathrm{Spec}(R)$$

eine semiabelsche Varietät ist, mit eigentlicher generischer Faser A/K. Die Metriken an den unendlichen Stellen kommen vom schon erwähnten Skalarprodukt:

$$\|\alpha\|_v^2 = \left(\frac{i}{2}\right)^g \cdot \int_{A(\bar{K}_v)} \alpha \wedge \bar{\alpha}.$$

Definition. Die modultheoretische Höhe $h(A)$ ist

$$h(A) = \frac{1}{[K:\mathbb{Q}]} \mathrm{Grad}(\omega_{A/R}).$$

Man sieht sofort, daß $h(A)$ invariant ist gegenüber Erweiterungen des Grundkörpers. Der Name „Höhe“ rechtfertigt sich wie folgt:

Im allgemeinen definiert man die Höhe eines Punktes $x \in \mathbb{P}^n(K)$, indem man x einen Morphismus $\rho\colon \mathrm{Spec}(R) \to \mathbb{P}^n_{\mathbb{Z}}$ zuordnet, das Bündel $\mathcal{O}(1)$ auf $\mathbb{P}^n_{\mathbb{C}}$ mit einer Metrik versieht, und dann als Höhe von x

$$\frac{1}{[K:\mathbb{Q}]} \cdot \mathrm{Grad}(\rho^* \mathcal{O}(1))$$

definiert.

Bei Veränderung der hermiteschen Metrik ändert sich die Höhenfunktion nur um einen beschränkten Betrag, und es ist bekannt, daß für jedes c nur endlich viele K-rationale Punkte des $\mathbb{P}^n$ Höhe $\leqq c$ haben. Entsprechende Überlegungen gelten für abgeschlossene Untervariatäten des $\mathbb{P}^n$. Angewandt auf unsere Situation bettet man wie bisher A_g mittels $\mathcal{M}$ in $\mathbb{P}^n_{\mathbb{Z}}$ ein. Außerdem hat man schon eine Metrik $\|\ \|$ auf dem von $\mathcal{M}$ auf $A_g(\mathbb{C})$ induzierten Bündel definiert. Wenn sich diese Metrik auf $\bar{A}_g(\mathbb{C})$ fortsetzen ließe, so könnte man sie zur Definition der Höhe verwenden, und aus dem Korollar zu Lemma 2 würde folgen, daß für eine semiabelsche Varietät A über R (wie oben), welche über K eine prinzipale Polarisation besitzt und damit ein $x \in A_g(K)$ definiert, $h(x)$ und $r \cdot h(A)$ sich nur um eine beschränkten Betrag unterscheiden.

Leider hat die Metrik $\|\ \|$ Singularitäten längs $\bar{A}_g(\mathbb{C}) - A_g(\mathbb{C})$, doch sind diese so mild, daß die fundamentale Endlichkeits-Eigenschaft der Höhe erhalten bleibt:

Definition. Sei $X/\mathbb{C}$ eine kompakte komplexe Varietät, $Y \subseteq X$ eine abgeschlossene Untervarietät, $\mathcal{M}$ eine Geradenbündel auf X, $\|\ \|$ eine hermitesche Metrik auf $\mathcal{M}|X-Y$. Die Metrik $\|\ \|$ hat logarithmische Singularitäten längs Y, wenn folgendes gilt: Es gibt eine eigentliche dominante Abbildung

$$\phi\colon \tilde{X} \to X,$$

so daß $\tilde{X}$ glatt und $\phi^{-1}(Y)$ ein Divisor mit normalen Überkreuzungen ist, und so daß für ein lokales Erzeugendes h von $\phi^*(\mathcal{M})$ und eine lokale Gleichung f von $\phi^{-1}(Y)$.

$$\operatorname{Sup}\{\|h\|, \|h\|^{-1}\} \leqq c_1 \cdot |(\log|f|)|^{c_2}$$

(mit Konstanten $c_1, c_2 > 0$) gilt.

Beispiel.

$$X = \bar{A}_g(\mathbb{C}), \qquad Y = \bar{A}_g(\mathbb{C}) - A_g(\mathbb{C}), \qquad \mathcal{M} \text{ und } \|\ \|$$

wie bisher.

Dies wurde zwar schon in [6] gezeigt (Ende von §2), doch folgt hier auf Wunsch der Referenten eine kurze Beweisskizze:

Allgemeiner gilt für ein glattes X, einen Divisor Y von X mit normalen Überkreuzungen und eine semiabelsche Varietät

$$p\colon A \to X,$$

so daß über $X - Y$ p eigentlich und A prinzipal polarisiert ist, daß die kanonische Metrik auf $\omega_{A/X}$ logarithmische Singularitäten längs Y hat.

Dazu betrachtet man statt $\omega_{A/X}$ $p_*(\Omega^1_{A/X})$ („logarithmische Singularitäten" läßt sich auch für Vektorbündel definieren), und mit den Methoden des §2 reduziert man das Problem auf den Fall, daß A Jacobische einer semi-stabilen Kurve $q\colon C \to X$ ist.

Wir behandeln kurz den Fall einer semi-stabilen Kurve über dem Einheitskreis $\mathbb{D}$. Der allgemeine Fall geht genauso. Wenn

$$q\colon C \to \mathbb{D} = \{t \mid |t| < 1\}$$

eine semi-stabile Kurve ist, mit guter Reduktion außerhalb 0, so besitzt C eine Überdeckung

$$C = \bigcup_{i=1}^{l} U_i,$$

so daß entweder

a) $U_i = \{(z,t) \mid |z| < 1,\ |t| < 1\}$, $q|U_i\colon U_i \to \mathbb{D}$ glatt, z liefert Koordinate auf allen Fasern

oder

b) $U_i = \{(z_1, z_2, t) \mid |z_1| < \varepsilon,\ |z_2| < \varepsilon,\ z_1 z_2 = t^m\}$, $q(z_1, z_2, t) = t$.

Wenn α ein lokaler Schnitt von $q_*(\omega_{C/\mathbb{D}})$ ist, so ist α auf den U_i von der Form

a) $\alpha = (\text{holomorph}) \cdot dz$ bzw.

b) $\alpha = (\text{holomorph}) \cdot \dfrac{dz_1}{z_1}$.

Eine explizite Rechnung ergibt, daß

$$\frac{i}{2}\int\limits_{U_i \cap q^{-1}(t)} \alpha \wedge \bar{\alpha}$$

für $t \to 0$ entweder beschränkt bleibt, oder höchstens wie $|\log|t||$ wächst. Außerdem sieht man sofort, daß

$$\| \ \| \geqq (\text{pos. Konst.}) \ \| \ \|_1,$$

wobei $\| \ \|_1$ eine auf ganz X erklärte hermitesche Metrik auf $q_*(\omega_{C/X})$ bezeichnet.

Lemma 3. *Sei $X \subseteq \mathbb{P}^n_{\mathbb{Z}}$ Zariski-abgeschlossen, $Y \subseteq X$ abgeschlossen, $\| \ \|$ eine hermitesche Metrik auf $\mathcal{O}(1)|(X(\mathbb{C}) - Y(\mathbb{C}))$, mit logarithmischen Singularitäten längs Y. Für einen Zahlkörper K und $x \in X(K) - Y(K)$ definiert man wie bisher $h(x)$. Dann gibt es für jedes c nur endlich viele $x \in X(K) - Y(K)$ mit $h(x) \leqq c$.*

Beweis. Sei $\| \ \|_1$ eine hermitesche Metrik für $\mathcal{O}(1)|X(\mathbb{C})$, h_1 die zugehörige Höhenfunktion, und man wähle ein $s > 0$ und

$$f_1, \ldots, f_t \in \Gamma(X/\mathbb{Z}, \mathcal{O}(s)),$$

deren gemeinsame Nullstellenmenge genau Y ist. Dann definiert $\| \ \|_1$ eine Metrik auf $\mathcal{O}(s)$ (welche auch $\| \ \|_1$ heiße), und aus den Voraussetzungen folgt sofort, daß Konstanten $c_1, c_2 > 0$ existieren

$$\text{mit } \log\left|\frac{\| \ \|}{\| \ \|_1}(z)\right| \leqq c_1 + c_2 \cdot \inf\{\log(|\log\|f_i(z)\|_1|)\}$$

für $z \in X(\mathbb{C})$.

Wenn $x \in X(K) - Y(K)$, entsprechend einem

$$\rho\colon \operatorname{Spec}(R) \to X,$$

so definieren die f_i Schnitte $\rho^*(f_i)$ von $\rho^*(\mathcal{O}(s))$, mit deren Hilfe man die Höhe $h_1(x)$ berechnen kann. Da $\|f_i(z)\|_1$ auf $X(\mathbb{C})$ nach oben beschränkt ist, erhält man sofort Konstanten $c_3, c_4 > 0$ mit

$$|h(x) - h_1(x)| \leqq c_3 + c_4 \cdot \log(h_1(x)).$$

Daraus folgt unmittelbar die Behauptung.

Wir können nun die Früchte unserer Bemühungen ernten. Das folgende Resultat ist schon fast bewiesen:

Satz 1. *Sei c gegeben. Dann gibt es nur endlich viele Isomorphieklassen von Paaren aus*

i) *einer semiabelschen Varietät der relativen Dimension g*

$$p\colon A \to \operatorname{Spec}(R)$$

mit eigentlicher generischer Faser A/K

ii) *einer prinzipalen Polarisation auf* A/K,
für welche

$$h(A) \leqq c$$

gilt.

Beweis. Nach dem Korollar zu Lemma 2 ist die Differenz zwischen $h(x)$ und $r \cdot h(A)$ beschränkt ($x \in A_g(K)$ gehört zu A). Nach Lemma 3 liefern die A mit $h(A) \leqq c$ somit nur endlich viele verschiedene $x \in A_g(K)$. Wir müssen uns nun noch überlegen, daß nur endlich viele K-Isomorphieklassen dieselbe Klasse über dem algebraischen Abschluß $\bar{K}$ induzieren können. Wir fixieren also eine solche Klasse über $\bar{K}$, und betrachten die entsprechenden A/K. Es ist bekannt, daß alle diese an denselben Stellen von K schlechte Reduktion haben. Aus dem Lemma 4 weiter unten folgt dann sofort die Existenz einer endlichen Erweiterung $K' \supseteq K$, welche für ein $n \geqq 3$ die Koordinaten der n-Teilungspunkte aller A/K enthält. Bekanntlich sind dann unsere A's schon über K' isomorph, und der Rest folgt aus allgemeinen Grundsätzen der Galois-Kohomologie.

Es bleibt nachzutragen das

Lemma 4. *Sei K ein Zahlkörper, S eine endliche Menge von Stellen von K. Dann gibt es nur endlich viele Körpererweiterungen $K' \supseteq K$ von vorgegebener Ordnung, welche außerhalb von S unverzweigt sind.*

Beweis. Bekannt (Hermite-Minkowski).

§ 4. Isogenien

Wir untersuchen das Verhalten von $h(A)$ unter Isogenien. Wie immer ist K ein Zahlkörper, $R \subset K$ der Ring der ganzen Zahlen.

Seien

$$p_1 \colon A_1 \to \mathrm{Spec}(R)$$

und

$$p_2 \colon A_2 \to \mathrm{Spec}(R)$$

semiabelsche Varietäten mit eigentlicher generischer Faser,

$$s \colon \mathrm{Spec}(R) \to A_1$$

der Nullschnitt, und $\phi \colon A_1 \to A_2$ eine Isogenie. (Nach Lemma 1 reicht es natürlich, wenn man ϕ über K definiert.)

Wir setzen $G = \mathrm{Ker}(\phi) \subseteq A_1$. Da ϕ automatisch flach ist, ist G ein quasiendliches flaches Gruppenschema über $\mathrm{Spec}(R)$.

ϕ induziert eine Injektion

$$\phi^* \colon \omega_{A_2/R} \to \omega_{A_1/R},$$

und man sieht sofort, daß

$$\#(\omega_{A_1/R}/\phi^*(\omega_{A_2/R})) = \# s^*(\Omega^1_{A_1/A_2}) = \# s^*(\Omega^1_{G/R}).$$

Da außerdem ϕ^* die Normen an den unendlichen Stellen um $(\mathrm{Grad}(\phi))^{1/2}$ verändert, folgt unmittelbar

Lemma 5.

$$h(A_2)=h(A_1)+\tfrac{1}{2}\log(\mathrm{Grad}(\phi))-\frac{1}{[K:\mathbb{Q}]}\cdot\log(\#s^*(\Omega^1_{G/R})).$$

Bemerkung. Wenn G von einer Zahl $n\in\mathbb{N}$ annulliert wird, so annulliert n auch $\Omega^1_{G/R}$. Daraus folgt, daß

$$\exp(2[K:\mathbb{Q}]\cdot(h(A_2)-h(A_1)))$$

eine rationale Zahl ist, in deren Zähler und Nenner nur Primteiler von $\mathrm{Grad}(\phi)$ auftauchen. Die Exponenten dieser Primteiler darin können durch ihre Exponenten in $\mathrm{Grad}(\phi)$ beschränkt werden.

Wir untersuchen nun das Verhalten der $h(A_n)$, falls $A_n=A/G_n$, wobei die G_n die Stufen einer l-divisiblen Gruppe $G\subseteq A[l^\infty]$ durchlaufen.

Satz 2. *Sei p: $A\to\mathrm{Spec}(R)$ eine semiabelsche Varietät mit eigentlicher generischer Faser, l eine Primzahl, und $G/K\subseteq A[l^\infty]/K$ eine l-divisible Untergruppe.*

Weiter sei G_n der Kern von l^n auf G, und A_n die semiabelsche Varietät $A_n=A/G_n$. Dann ist

$$h(A_n)=h(A).$$

Beweis. Seien $v_1,\dots,v_r$ die über l liegenden Stellen von k, $K_i=K_{v_i}$ die entsprechenden lokalen Körper, $R_i\subseteq K_i$ die Bewertungsringe, $m_i=[K_i:\mathbb{Q}_l]$, so daß

$$m=[K:\mathbb{Q}]=\sum_{i=1}^{r} m_i.$$

Wir wählen ein festes i, und betrachten das formale Gruppenschema $\hat{A}$ über $Spf(R_i)$, die Komplettierung von A/R_i längs der Faser A_s über dem abgeschlossenen Punkt s von $\mathrm{Spec}(R_i)$.

A_s ist eine Erweiterung $0\to T_s\to A_s\to B_s\to 0$ mit T_s Torus, B_s eine abelsche Varietät.

Nach allgemeinen Grundsätzen kann man T_s liften zu einem Torus T über $\mathrm{Spec}(R_i)$, und $\hat{T}$ ist abgeschlossenes formales Unterschema von $\hat{A}$. (Morphismen von T_s in glatte Gruppenschemata können geliftet werden.)

Sei

$$\hat{H}_i=\hat{A}[l^\infty]$$

die assoziierte l-divisible Gruppe. $\hat{H}_i$ ist formale Komplettierung einer l-divisiblen Gruppe H_i über R_i, und H_i/K_i ist eine l-divisible Untergruppe von $A[l^\infty]/K_i$. Dasselbe gilt für $T[l^\infty]$, und zu diesen Untergruppen gehören $\mathbb{Z}_l$-Untergitter

$$T_l(T)\subseteq T_l(H_i)\subseteq T_l(A).$$

Lemma 6. *Sei $D_i=\mathrm{Gal}(\bar{K}_i/K_i)$ die absolute Galois-Gruppe von K_i, $I_i\subseteq D_i$ die Verzweigungsgruppe.*

Dann operiert I_i trivial auf $T_l(A)/T_l(H_i)$, und die induzierte Operation von $D_i/I_i\cong\hat{\mathbb{Z}}$ erfolgt über einen endlichen Quotienten von $\hat{\mathbb{Z}}$.

Beweis. Sei

$$\langle\ ,\ \rangle:\ T_l(A)\times T_l(A)\to\mathbb{Z}_l(1)=T_l(\mathbb{G}_m)$$

die von einer Polarisation von A/K induzierte symplektische Form. $\langle\,,\rangle$ ist nicht ausgeartet, und bekanntlich (SGA VII, Exp. IX, § 7) ist

$$\langle T_l(T), T_l(H_i)\rangle = 0.$$

Aus Dimensionsgründen ist $T_l(H_i) = T_l(T)^{\perp}$, und wir erhalten eine Injektion

$$T_l(A)/T_l(H_i) \hookrightarrow \mathrm{Hom}_{\mathbb{Z}_l}(T_l(T), \mathbb{Z}_l(1)).$$

Diese Injektion ist D_i-linear, und D_i operiert in der verlangten Art und Weise auf $\mathrm{Hom}_{\mathbb{Z}_l}(T_l(T), \mathbb{Z}_l(1))$.

Nunmehr zurück zu unserem $G/K \subseteq A[l^\infty]/K$. Nach Basiserweiterung $K \subseteq K_i$ können wir den Durchschnitt $G_i = G \cap H_i$ bilden. Dies ist die maximale l-divisible Untergruppe von G_i/K_i, welche sich über R_i ausdehnen läßt, und es ist

$$\#(s^* \Omega^1_{A/A_n} \otimes_R R_i) = \# s^*(\Omega^1_{(G_i)_n/R_i}).$$

Nach [13], Proposition 2 kann man dies sofort ausrechnen: Sei d_i die Dimension der maximalen formalen Untergruppe von G_i. Dann ist

$$\# s^*(\Omega^1_{(G_i)_n/R_i}) = l^{n \cdot m_i \cdot d_i}.$$

Wenn C_i die Komplettierung des algebraischen Abschlusses von K_i bezeichnet, so ist weiter bekannt ([13], Theorem 3, Corollary 2), daß

$$T_l(G_i) \otimes_{\mathbb{Z}_l} C_i \cong C_i^{h_i - d_i} \oplus C_i^{d_i}(+1),$$

$$(h_i = \text{Höhe}(G_i),\ „(+1)“ = \text{Tate-Twist}) \text{ als } D_i\text{-Moduln.}$$

Zusammen mit Lemma 6 ergibt sich daraus, daß D_i auf

$$\Lambda^h T_l(G) \otimes_{\mathbb{Z}_l} C_i \subseteq \Lambda^h T_l(A) \otimes_{\mathbb{Z}_l} C_i$$
$$(h = \text{Höhe}(G))$$

wie auf

$$C_i(\chi_0^{d_i}) = C_i(d_i)$$

operiert (χ_0 = zyklotomischer Charakter).

Wir übertragen dies nun wieder auf den globalen Fall:

Es ist

$$\# s^*(\Omega^1_{A/A_n}) = l^{n \sum_{i=1}^{r} m_i d_i}, \qquad (l^n \cdot \Omega^1_{A/A_n} = 0)$$

und

$$h(A_n) - h(A) = n \cdot \log(l) \cdot \left(\frac{h}{2} - \sum_{i=1}^{r} \frac{m_i}{m} \cdot d_i\right).$$

Wir müssen also zeigen, daß $\sum_{i=1}^{r} m_i d_i = \frac{1}{2} m h$. Dazu betrachten wir die absolute Galois-Gruppe $\tilde{\pi} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, und den $\tilde{\pi}$-Modul

$$\tilde{V} = \mathrm{Ind}_{\pi}^{\tilde{\pi}}(T_l(A)) \qquad (\pi = \mathrm{Gal}(\overline{K}/K)).$$

Dieser enthält den Untermodul

$$\tilde{W} = \mathrm{Ind}_{\pi}^{\tilde{\pi}}(T_l(G))$$

vom Rang $m h$, und $\tilde{\pi}$ operiert auf der Geraden

$$L = \Lambda^{mh}(\tilde{W}) \subseteq \Lambda^{mh}(\tilde{V})$$

via einen Charakter $\chi \colon \tilde{\pi} \to \mathbb{Z}_l^*$.

Aus der Klassenkörpertheorie folgt, daß χ von der Form $\chi = $($l$-adische Potenz von χ_0)$\cdot$(Charakter endlicher Ordnung) ist.

Die darin auftretende l-adische Potenz von χ_0 bestimmt sich wie folgt: Sei C die Komplettierung des algebraischen Abschlusses von $\mathbb{Q}_l$,

$$D \cong \mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l) \subseteq \tilde{\pi}$$

die Zerlegungs-Gruppe von l. Dann gilt als D-Modul

$$L \otimes_{\mathbb{Z}_l} C \cong C\left(+\sum_{i=1}^{r} m_i d_i\right)$$

(dies folgt aus unseren vorherigen Berechnungen), und somit ist nach [13], Theorem 2

$$\chi \cdot \chi_0^{-\sum_{i=1}^{r} m_i d_i}$$

ein Charakter endlicher Ordnung auf D und auch auf $\tilde{\pi}$. Schließlich folgt aus dem schon von Weil bewiesenen Teil der Weil-Vermutungen mit einigen lokalen Überlegungen, daß $\chi(F_p)$ ($p =$ Primzahl, $F_p =$ Frobenius) für fast alle p eine algebraische Zahl ist, all deren Konjugierte Betrag $p^{\frac{mh}{2}}$ haben. Da $\chi_0(F_p) = p$, ist wie verlangt

$$\sum_{i=1}^{r} m_i d_i = \frac{mh}{2}.$$

§ 5. Endomorphismen

Sei K Zahlkörper, A/K eine abelsche Varietät der Dimension g, l eine Primzahl, $T_l = T_l(A)$ der Tate-Modul, auf dem $\pi = \mathrm{Gal}(\overline{K}/K)$ operiert.

Satz 3. *Die Operation von π auf $T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ ist halbeinfach.*

Satz 4. *Die Abbildung*

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{End}_{\pi}(T_l)$$

ist ein Isomorphismus.

Beweis. Die beiden Sätze werden zusammen bewiesen. Es reicht bekanntlich, statt Satz 4 die etwas schwächere Aussage zu beweisen, daß die Abbildung

$$\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_l \to \mathrm{End}_{\pi}(T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l)$$

bijektiv ist.

Man darf dann zum Beweis den Grundkörper erweitern, oder A durch eine isogene abelsche Varietät ersetzen. Wir können also annehmen, daß A/K prinzipal polarisiert ist, und daß A sich zu einer semiabelschen Varietät über $\mathrm{Spec}(R)$ fortsetzt. Dann besitzt T_l eine nichtausgeartete schiefsymmetrische Bilinearform. Sei

$$W \subseteq T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$$

ein π-invarianter maximal isotroper Teilraum. Dem entspricht eine l-divisible Untergruppe $G \subseteq A[l^\infty]$, und die semiabelschen Varietäten $A_n = A/G_n$ tragen wieder prinzipale Polarisationen.

Nach Satz 2 ist $h(A_n) = h(A)$, und nach Satz 1 sind unendlich viele A_n's isomorph.

Wie in [16] folgt daraus, daß W Bild eines Idempotents aus $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Q}_l$ ist. Der Rest des Beweises geht genauso wie in [16], und sei daher nur skizziert:

Wähle $a, b, c, d \in \mathbb{Q}_l$ mit $a^2+b^2+c^2+d^2=-1$. Setze

$$v = \begin{pmatrix} a & -b & -c & -d \\ b & a & d & -c \\ c & -d & a & b \\ d & c & -b & a \end{pmatrix}$$

(entsprechend dem Quaternion $a+bi+cj+dk$), so daß $v \cdot {}^t v = -1$. Wenn W ein beliebiger π-invarianter Teilraum von $T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ ist, so wendet man obige Überlegungen an auf den maximal isotropen Teilraum

$$W_1 = \{(x, vx) \mid x \in W^4\} \oplus \{(y, -vy) \mid y \in (W^\perp)^4\} \subseteq T_l(A)^8 \otimes_{\mathbb{Z}_l} \mathbb{Q}_l.$$

Korollar 1. *Seien A_1 und A_2 abelsche Varietäten über K. Dann ist*

$$\mathrm{Hom}_K(A_1, A_2) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{Hom}_\pi(T_l(A_1), T_l(A_2))$$

ein Isomorphismus.

Beweis. Satz 4 für $A_1 \times A_2$.

Die L-Reihe eines A's ist bekanntlich definiert als

$$L(A,s) = \prod_v \frac{1}{\det(1-(N_v)^{-s} \cdot F_v \mid T_l(A))} = \prod_v L_v(A,s),$$

wobei das Produkt über fast alle Stellen von K zu erstrecken ist. Die lokalen L-Faktoren $L_v(A,s)$ sind unabhängig von l.

Korollar 2. *Seien A_1, A_2 wie im Korollar 1. Es sind äquivalent*

i) *A_1 und A_2 sind isogen.*
ii) *$T_l(A_1) \otimes_{\mathbb{Z}} \mathbb{Q}_l \cong T_l(A_2) \otimes_{\mathbb{Z}} \mathbb{Q}_l$ als π-Modul.*
iii) *$L_v(s, A_1) = L_v(s, A_2)$ für fast alle Stellen v von K.*
iv) *$L_v(s, A_1) = L_v(s, A_2)$ für alle v.*

Beweis. Die Äquivalenz von i) und ii) folgt aus Satz 4, die von ii) und iii) aus Satz 3 (+Čebotarev), und aus ii) folgt iv) folgt iii) ist trivial.

Korollar 3. *Sei A/K eine abelsche Varietät, $d>0$. Dann gibt es nur endlich viele Isomorphieklassen d-fach polarisierter abelscher Varietäten B/K, so daß für alle l $T_l(A)\cong T_l(B)$.*

Beweis. Die Voraussetzung besagt, daß zu jedem l eine Isogenie vom Grad prim zu l zwischen A und B existiert. Wir dürfen weiter den Grundkörper K zum Beweis erweitern, und dann annehmen, daß A und alle B's sich zu semi-abelschen Varietäten über $\operatorname{Spec}(R)$ fortsetzen, und daß es für alle B's eine Isogenie vom Grad $\sqrt{d}$ mit einer prinzipal polarisierten abelschen Varietät gibt. Man kommt dann leicht auf folgende Voraussetzungen:

a) alle B's haben semistabile Reduktion,

b) alle B/K sind prinzipal polarisiert,

c) es gibt ein N, so daß für jede Primzahl l und alle B's Isogenien $\phi\colon A\to B$ existieren, für die die größte l-Potenz in $\operatorname{Grad}(\varphi)$ N teilt.

Die Bemerkung nach Lemma 5 zeigt dann, daß $\exp(2[K:\mathbb{Q}](h(B)-h(A))$ eine rationale Zahl ist, deren Zähler und Nenner durch eine geeignete Potenz von N abgeschätzt werden kann.

Also sind die $h(B)$ beschränkt, und man kann Satz 1 anwenden.

§ 6. Endlichkeitssätze

Satz 5. *Sei S eine endliche Menge von Stellen von K. Dann gibt es nur endlich viele Isogenie-Klassen abelscher Varietäten vorgegebener Dimension über K, welche gute Reduktion außerhalb S haben.*

Beweis. Sei A eine solche abelsche Varietät. Nach den Weil-Vermutungen gibt es für $v\notin S$ nur endlich viele Möglichkeiten für den lokalen L-Faktor $L_v(A,s)$. Wir werden endlich viele Stellen $v_1,\dots,v_r$ konstruieren, so daß zwei A's schon isogen sind, wenn sie an diesen Stellen denselben lokalen L-Faktor haben. Dazu wähle man eine Primzahl l. Nach Lemma 4 existiert eine endliche Galois-Erweiterung $K'\supseteq K$, welche alle außerhalb l und S unverzweigten Körpererweiterungen von K vom Grad $\leqq l^{8g^2}$ umfaßt ($g=\dim(A)$).

Sei $G=\operatorname{Gal}(K'/K)$; und man wähle $v_1,\dots,v_r$ so daß jede Konjugationsklasse in G das Bild eines Frobenius F_v für $v\in\{v_1,\dots,v_r\}$ enthält (Čebotarev). Dann erfüllen $v_1,\dots,v_r$ unsere Forderungen: Seien A_1, A_2 zwei abelsche Varietäten über K, welche denselben lokalen L-Faktor an $v_1,\dots,v_r$ haben.

Sei

$$M\subseteq \operatorname{End}_{\mathbb{Z}_l}(T_l(A_1))\times \operatorname{End}_{\mathbb{Z}_l}(T_l(A_2))$$

die $\mathbb{Z}_l$-Unteralgebra, die vom Bild von π erzeugt wird.

Dann ist M freier $\mathbb{Z}_l$-Modul vom Rang $\leqq 8g^2$, und M besitzt Darstellungen auf $T_l(A_1)$ und $T_l(A_2)$.

Wir müssen zeigen, daß für jedes $m\in M$

$$\operatorname{Spur}(m\,|\,T_l(A_1))=\operatorname{Spur}(m\,|\,T_l(A_2)).$$

Es reicht natürlich, dies für m aus einer $\mathbb{Z}_l$-Modulbasis von M zu zeigen, und nach Voraussetzung gilt die Gleichheit schon, wenn m Bild eines Elements aus der Konjugationsklasse von F_v ist, für $v \in \{v_1, \dots, v_r\}$. Wir zeigen, daß diese Bilder M über $\mathbb{Z}_l$ erzeugen. Nach Nakayama reicht es, wenn sie M/lM erzeugen. Dies gilt aber aus folgendem Grund:

Wir haben eine Darstellung

$$\rho\colon \pi \to (M/lM)^* = \text{Einheiten von } M/lM,$$

deren Bild M/lM erzeugt.

Da

$$\#(M/lM)^* \leqq l^{8g^2},$$

faktorisiert ρ über G, und $\rho(\pi)$ ist die Vereinigung der Bilder der Konjugationsklassen der F_v, $v \in \{v_1, \dots, v_r\}$.

Satz 6 (Shafarevich-Vermutung). *Sei S eine endliche Menge von Stellen von K, $d>0$. Dann gibt es nur endlich viele Isomorphie-Klassen d-fach polarisierter abelscher Varietäten über K von vorgegebener Dimension, welche außerhalb S gute Reduktion haben.*

Beweis. Nach Satz 5 nehmen wir an, daß die betrachteten abelschen Varietäten B/K alle isogen zu einem festen A/K sind. Wie im Beweis des Korollar 3 zu Satz 4 dürfen wir weiter voraussetzen, daß sich alle B's zu semiabelschen Varietäten über $\operatorname{Spec}(R)$ fortsetzen, und daß $d=1$ ist. Wir wissen schon, daß

$$\exp(2[K:\mathbb{Q}](h(B)-h(A)))$$

eine rationale Zahl ist. Wir werden ein N konstruieren, so daß Zähler und Nenner dieser rationalen Zahl keine Primfaktoren $l>N$ besitzen, und daß die auftretenden l-Potenzen für Primzahlen $l \leqq N$ beschränkt sind.

Das letztere ist ganz einfach:

Wenn für zwei abelsche Varietäten B_1/K und B_2/K $T_l(B_1)$ und $T_l(B_2)$ als π-Moduln isomorph sind, so existiert nach Satz 4 eine Isogenie vom Grad prim zu l zwischen B_1 und B_2, und l tritt nicht in

$$\exp(2[K:\mathbb{Q}](h(B_1)-h(B_2)))$$

auf.

Es reicht also, wenn es nur endlich viele Isomorphie-Klassen π-invarianter Gitter in $T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ gibt. Dazu sei M_l die von π erzeugte $\mathbb{Z}_l$-Unteralgebra von $\operatorname{End}_{\mathbb{Z}_l}(T_l(A))$. Es folgt dann alles aus der Tatsache, daß $M_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ halbeinfach ist (Satz 3).

Wir kommen nun zur Wahl von N. Dazu sei n das Produkt der Primzahlen l, für welche entweder die Erweiterung $K \supseteq \mathbb{Q}$ in l verzweigt, oder A nicht gute Reduktion an allen Stellen der Charakteristik l hat.

Wähle eine Primzahl p, welche n nicht teilt. Sei wieder

$$\tilde{\pi} = \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \supseteq \pi = \operatorname{Gal}(\overline{K}/K),$$

und, für $0 \leqq h \leqq 2gm$ ($g = \dim(A)$, $m = [K:\mathbb{Q}]$), sei

$$P_h(T) = \det[T - F_p \mid \Lambda^h(\operatorname{Ind}_{\pi}^{\tilde{\pi}}(T_l(A)))].$$

Dabei ist l eine zu pn prime Primzahl, und F_p bezeichnet den Frobenius an der Stelle p.

Die $P_h(T)$ sind unabhängig von l, haben Koeffizienten in $\mathbb{Z}$, und ihre Nullstellen haben absoluten Betrag $p^{+\frac{h}{2}}$ (Weil-Vermutung oder besser -Satz).

Wir wählen nun $N \geqq 2$ so groß, daß keine Primzahl $l > N$ $P_h(\pm p^j)$ teilt, falls

$$0 \leqq h \leqq 2gm$$
$$0 \leqq j \leqq gm$$
$$j \neq \tfrac{1}{2}h.$$

Außerdem sei $N \geqq np$.

Wir werden zeigen, daß für jede Isogenie

$$\phi\colon B_1 \to B_2$$

von zu A isogenen abelschen Varietäten, deren Grad eine l-Potenz mit einer Primzahl $l > N$ ist, $h(B_1)$ und $h(B_2)$ übereinstimmen. Dies geht ähnlich wie beim Beweis des Satzes 2: Wir dürfen annehmen, daß l den Kern G von ϕ annulliert. Sei

$$V_l = T_l(B_1)/l \cdot T_l(B_1) \cong B_1[l](\bar{K}),$$
$$\tilde{V}_l = \operatorname{Ind}_\pi^{\tilde{\pi}}(V),$$
$$W_l = G(\bar{K}) \subseteq V_l$$
$$\tilde{W}_l = \operatorname{Ind}_\pi^{\tilde{\pi}}(W_l) \subseteq \tilde{V}_l.$$

Wenn ϕ die Ordnung l^h hat, so operiert $\tilde{\pi}$ auf

$$L = \Lambda^{mh}(\tilde{W}_l) \subseteq \Lambda^{mh}(\tilde{V}_l)$$

via einen Charakter $\chi\colon \tilde{\pi} \to (\mathbb{Z}/l\mathbb{Z})^*$.

Wenn $\varepsilon\colon \tilde{\pi} \to \{\pm 1\}$ den Charakter bezeichnet, mit dem $\tilde{\pi}$ auf $\Lambda^m \operatorname{Ind}_\pi^{\tilde{\pi}}(\mathbb{Z})$ operiert, so ist $\chi \cdot \varepsilon^h$ unverzweigt außerhalb l, denn die Trägheitsgruppen der Stellen v von K, welche l nicht teilen, operieren unipotent auf V_l (semistabile Reduktion). Nach der Klassenkörpertheorie ist $\chi \cdot \varepsilon^h$ eine Potenz des zyklotomischen Charakters χ_0. Diese Potenz läßt sich mit Hilfe von [10], Théorème 4.11 (statt der Tateschen Theorie [13]) wie folgt bestimmen:

Sei

$$l^d = \# s^*(\Omega^1_{G/R}),$$
$$0 \leqq d \leqq gm.$$

Dann ist (nach Raynaud) $\chi \cdot \varepsilon^h = \chi_0^{+d}$. Also ist

$$\chi_0^d(F_p) = \pm p^d$$

eine Nullstelle von $P_{mh}(T)$ modulo l, und nach Wahl von N muß $d = \frac{hm}{2}$ gelten.

Da wieder

$$h(B_2) - h(B_1) = \log(l)\left(\frac{h}{2} - \frac{d}{m}\right),$$

folgt unsere Behauptung, und es ergibt sich, daß die $h(B)$'s der betrachteten B's beschränkt sind. Damit folgt Satz 6 aus Satz 1.

Korollar 1. *Es gibt nur endlich viele Isomorphie-Klassen glatter Kurven X/K vom Geschlecht $g \geqq 2$, welche außerhalb S gute Reduktion haben.*

Beweis. Torelli.

Satz 7 (Mordell-Vermutung). *Sei X/K eine glatte Kurve vom Geschlecht $g \geqq 2$. Dann ist $X(K)$ endlich.*

Beweis. Dies steht in [9]: Nach eventueller Erweiterung des Grundkörpers gibt es eine unverzweigte Überlagerung vom Grad $m > 2$:

$$\phi: X_1 \to X.$$

Lemma 4 liefert einen endlichen Oberkörper $K_1 \supseteq K$, so daß für jedes $x \in X(K)$ $\phi^{-1}(x)$ aus m verschiedenen K_1-rationalen Punkten besteht. Man wähle einen davon aus, etwa $y \in p^{-1}(x)$.

Sei $D = \phi^{-1}(x) - \{y\}$, und A/K_1 die verallgemeinerte Jacobische zu dem Paar (X_1, D). Mit Hilfe von y konstruiert man eine Abbildung von $X_1 - D$ nach A.

Die Multiplikation mit 2 auf A induziert dann eine genaue über D verzweigte Überlagerung $Y(x) \to X_1$, wobei die Kurve $Y(x)$ nur an solchen Stellen v von K_1 schlechte Reduktion haben kann, für die eine der drei folgenden Bedingungen gilt:

a) v teilt 2.

b) X_1 hat schlechte Reduktion in v.

c) ϕ verzweigt in der Faser mod v.

Dies sind nur endlich viele Stellen, und es gibt somit nur endlich viele Möglichkeiten für $Y(x)$.

Dasselbe gilt für die Abbildung $Y(x) \to X_1 \to X$, welche genau über x verzweigt. Es folgt die Behauptung.

Bemerkungen. 1. Man erhält auf diesem Wege auch einen Beweis des Siegelschen Satzes (über ganze Punkte), welcher ohne diophantische Approximation auskommt.

2. Mit Hilfe der Methode aus [16] kann man aus Satz 6 folgern, daß für fast alle Primzahlen l die von π erzeugte Unteralgebra M_l von $\mathrm{End}_{\mathbb{Z}_l}(T_l(A))$ der volle Kommutator von $\mathrm{End}_K(A) \otimes_{\mathbb{Z}} \mathbb{Z}_l$ ist.

Literatur

1. Arakelov, S.: Families of curves with fixed degeneracies. Math. USSR Izvestija **5**, 1277–1302 (1971)
2. Arakelov, S.: An Intersection theory for divisors on an arithmetic surface. Math. USSR Izvestija **8**, 1167–1180 (1974)
3. Baily, W.L., Borel, A.: Compactification of arithmetic quotients of bounded symmetric domains. Ann. of Math. **84**, 442–528 (1966)

4. Deligne, P., Mumford, D.: The irreducibility of the space of curves of a given genus. Publ. math. I.H.E.S. **36**, 75–110 (1969)
5. Faltings, G.: Calculus on arithmetic surfaces. Eingereicht bei Ann. of Math.
6. Faltings, G.: Arakelov's theorem for abelian varieties. Invent. math. **73**, 337–347 (1983)
7. Moret-Bailly, L.: Variétés abéliennes polarisées sur les corps de fonctions. C.R. Acad. Sc. Paris **296**, 267–270 (1983)
8. Namikawa, Y.: Toroidal compactification of Siegel spaces. Lecture Notes in Mathematics, vol. 812. Berlin-Heidelberg-New York: Springer 1980
9. Parshin, A.N.: Algebraic curves over function fields I. Math. USSR Izvestija **2**, 1145–1170 (1968)
10. Raynaud, M.: Schémas en groupes de type $(p,\dots,p)$. Bull. Soc. Math. France **102**, 241–280 (1974)
11. Szpiro, L.: Sur le théorème de rigidité de Parsin et Arakelov. Astérisque **64**, 169–202 (1979)
12. Szpiro, L.: Séminaire sur les pinceaux de courbes de genre au moins deux. Astérisque **86** (1981)
13. Tate, J.: p-divisible groups. Proceedings of a conference on local fields, Driebergen 1966, pp. 158–183. Berlin-Heidelberg-New York: Springer 1967
14. Tate, J.: Endomorphisms of abelian varieties over finite fields. Invent. math. **2**, 134–144 (1966)
15. Zarhin, J.G.: Isogenies of abelian varieties over fields of finite characteristics. Math. USSR Sbornik **24**, 451–461 (1974)
16. Zarhin, J.G.: A remark on endomorphisms of abelian varieties over function fields of finite characteristics. Math. USSR Izvestija **8**, 477–480 (1974)

Oblatum 8-VI & 10-VII-1983

Zusatz bei der Korrektur

Herr O. Gabber hat mir mitgeteilt, daß der Beweis von Satz 2 nicht ganz korrekt ist. Man erhält nur, daß die Folge $h(A_n)$ stationär wird. Dies reicht für unsere Zwecke.