Produkte Abelscher Varietäten und Moduln über Ordnungen

Chad Schoen

Department of Mathematics
Duke University
Durham, NC 27706

USA

Max-Planck-Institut für Mathematik
Gottfried-Claren-Straße 26
D-5300 Bonn 3

Germany

MPI/91-49

Produkte Abelscher Varietäten und Moduln über Ordnungen

CHAD SCHOEN

Duke University

0. Einleitung. Eine komplexe Abelsche Varietät heißt einfach, wenn es keine Abelschen Untervarietäten positiver Dimension gibt. Sie heißt vollständig zerlegbar, wenn sie zu einem Produkt einfacher Abelscher Varietäten isomorph ist. Eine Isogenieklasse Abelscher Varietäten, $\mathcal{A}$, heißt vollständig zerlegbar, falls jedes Element aus $\mathcal{A}$ vollständig zerlegbar ist. Ziel dieser Arbeit ist folgende Klassifikation von vollständig zerlegbaren Isogenieklassen komplexer Abelscher Varietäten:

SATZ 0.1. *$\mathcal{A}$ ist genau dann vollständig zerlegbar, wenn*

(1) *$\mathcal{A}$ eine einfache Abelsche Varietät enthält oder*
(2) *$\mathcal{A}$ das mehrfache Selbstprodukt einer elliptischen Kurve mit komplexer Multiplikation enthält.*

Sei E eine elliptische Kurve mit komplexer Multiplikation. Die Tatsache, daß jede zu E^2 isogene Abelsche Fläche selber zu einem Produkt zweier elliptischer Kurven isomorph ist, wurde von Shioda und Mitani [**S-M**] erkannt und als Folgerung einer Untersuchung der Periodenabbildung für die zweite Kohomologie polarisierter Abelscher Flächen bewiesen. Ein elementarer Beweis findet sich bei Ruppert [**R**]. Daß die zu E^n gehörige Isogenieklasse vollständig zerlegbar ist, wurde von Lange [**L**] und Katsura [**K**], mittels nicht ganz einfacher Induktionsverfahren, auf den Satz von Shioda und Mitani zurückgeführt. Wir leiten diesen Satz als einfache Folgerung der Struktur der Kategorie der Moduln über Ordnungen in quadratischen Zahlkörpern her (siehe §2). Entscheidend ist die Tatsache, daß jeder endlich erzeugte, unzerlegbare Modul über einem solchen Ring den Rang 1 hat.

Die Modulstruktur quadratischer Ordnungen ist wesentlich einfacher als die Modulstruktur vieler Ordnungen in Divisionsalgebren von höherer $\mathbf{Q}$-Dimension. Gerade die Existenz unzerlegbarer Moduln höheren Ranges über diesen Ordnungen ermöglicht die Konstruktion von nicht vollständig zerlegbaren Abelschen Varietäten in den meisten von (1) und (2) verschiedenen Fällen.

Ich möchte U. Everling und F.-O. Schreyer für hilfreiche Hinweise danken.

Bezeichnungen.

Ringe sind stets assoziativ mit Einselement.

Ist R ein Ring, dessen Multiplikation mit $\cdot$ bezeichnet wird, so bezeichnet R° den Ring, der aus der Abelschen Gruppe R durch Hinzunehmen der Multiplikation $a * b = b \cdot a$ entsteht.

$I \in M_n(R)$ bezeichnet die Identität im Ring der $n \times n$-Matrizen über R.

R-Modul heißt endlich erzeugter R-Modul mit der Operation von links.

finanzielle Unterstützung der NSF (DMS 90-14954) und des MPI für Mathematik dankend anerkannt

Ein R-Modul heißt zerlegbar, falls er zu einer direkten Summe zweier von null verschiedener Untermoduln isomorph ist.

Eine Abelsche Varietät heißt zerlegbar, falls sie zu einer direkten Summe zweier von null verschiedener Abelscher Untervarietäten isomorph ist.

Ist $\mathfrak{r}$ ein Dedekindscher Ring, k sein Quotientenkörper, K eine einfache k-Algebra von endlichem Rang, so heißt ein Unterring $R \subset K$ mit $R \otimes_{\mathfrak{r}} k \simeq K$ eine K-Ordnung.

1. Eine elementare Überlegung.

Die Äquivalenzrelation, E ist zu F isogen, wird mit $E \sim F$ bezeichnet.

LEMMA 1.1. *([Mu,§19].) Jede Abelsche Varietät ist zu einem Produkt $A = \prod_{1 \le i \le m} E_i^{a_i}$ isogen, wobei E_i einfach ist, und $Hom(E_i, E_j) = 0$ für $i \neq j$. Ist $A \sim \prod_{1 \le j \le m'} F_j^{b_j}$ mit F_j einfach und $Hom(F_j, F_k) \simeq 0$ für $j \neq k$, dann gilt $m = m'$ und nach eventuellem Vertauschen der Indizes $E_i \sim F_i$ und $a_i = b_i$.*

SATZ 1.2. *Jede vollständig zerlegbare Isogenieklasse Abelscher Varietäten enthält das Selbstprodukt einer einfachen Abelschen Varietät.*

BEWEIS: Sei $A = \prod_{1 \le i \le m} E_i^{a_i}$ wie oben und $\mathcal{A}$ die Isogenieklasse von A. Wir nehmen an, $\mathcal{A}$ sei vollständig zerlegbar und zeigen $m = 1$. Sei $A' = \prod_{1 \le j \le N} F_j$ ein in $\mathcal{A}$ enthaltenes Produkt einfacher Abelscher Varietäten. Definiere $B_i = \prod_{F_j \sim E_i} F_j$. Es gilt $A' = \prod_{1 \le i \le m} B_i$. Aus $Hom(E_i, B_j) = 0$ für $i \neq j$ folgt

$$Hom(A, A') = \prod_{1 \le i \le m} Hom(E_i^{a_i}, B_i).$$

Der Kern einer Isogenie $\rho \in Hom(A, A')$ hat nun die Gestalt $\prod_{1 \le i \le m} H_i$, wobei H_i eine endliche Untergruppe von $E_i^{a_i}$ ist. Ist nun $m > 1$, dann existiert eine Isogenie, $A \to A''$, deren Kern sich nicht in dieser Form schreiben läßt. Offenbar ist A'' nicht vollständig zerlegbar.

2. Selbstprodukte elliptischer Kurven mit komplexer Multiplikation.

In diesem Absatz benutzen wir einen Satz aus der kommutativen Algebra, um einen durchsichtigen Beweis des Satzes von Katsura, Lange, Mitani und Shioda zu geben.

Wir brauchen Information über die Struktur der Moduln über denjenigen Ringen, die als Endomorphismenringe einfacher Abelscher Varietäten auftreten. Der einfachste allgemeine Satz über Modulstruktur ist bekanntlich:

SATZ 2.1. *Sei R ein kommutativer Integritätsbereich. Dann sind folgende Aussagen äquivalent:*

(1) *Jeder torsionsfreie R-Modul ist isomorph zu R^n für geeignetes n.*
(2) *Jedes Ideal von R wird von einem einzigen Element erzeugt.*

Es liegt nahe, nach der Struktur der Kategorie der Moduln über kommutativen Integritätsbereichen, deren Ideale von höchstens zwei Elementen erzeugt werden, zu fragen. Hierauf hat Bass folgende Antwort gegeben:

SATZ 2.2. *([**Ba**,Thm. 1.7]) Sei R ein kommutativer Noetherscher Integritätsbereich. Setzen wir voraus, daß der ganze Abschluß $\tilde{R}$ von R in seinem Quotientenkörper ein endlich erzeugter R-Modul ist. Dann sind folgende Aussagen äquivalent:*

(1) *Jeder torsionsfreie R-Modul ist direkte Summe von Moduln vom Rang eins.*
(2) *Jedes R-Ideal kann von zwei Elementen erzeugt werden.*

Sind diese Bedingungen erfüllt, so ist ferner jeder torsionsfreie R-Modul vom Range eins ein projektiver S-Modul, wobei S ein eindeutig bestimmter Zwischenring $R \subset S \subset \tilde{R}$ ist.

Aus dem obigen Satz folgt unmittelbar folgender Satz von Borevich und Faddeev, der ursprünglich anders hergeleitet wurde [**BF1**] (siehe auch [**BF2-3**]).

SATZ 2.3. *Sei R eine Ordnung in einem quadratischen Erweiterungskörper von $\mathbf{Q}$. Dann ist jeder torsionsfreie R-Modul zu einer direkten Summe Moduln vom Rang eins isomorph.*

BEWEIS: Jedes R-Ideal ist schon als $\mathbf{Z}$-Modul, also erst recht als R-Modul, von zwei Elementen erzeugt.

SATZ 2.4. *Die Isogenieklasse eines Selbstprodukts einer elliptischen Kurve mit komplexer Multiplikation ist vollständig zerlegbar.*

BEWEIS: Wir bezeichnen mit R den Ring der ganzen Zahlen im (imaginär quadratischen) Körper K der komplexen Multiplikation und fixieren einen $\mathbf{R}$-Algebrenisomorphismus $R \otimes \mathbf{R} \simeq \mathbf{C}$. Dann ist $E := R \otimes \mathbf{R}/R$ eine elliptische Kurve mit $End(E) \simeq R$. Wir dürfen ohne Beschränkung der Allgemeinheit annehmen, daß unsere Isogenieklasse, nennen wir sie $\mathcal{A}$, das Element E^n enthält. Jedes Element $A \in \mathcal{A}$ läßt sich in der Form $A = (R \otimes \mathbf{R})^n/\Lambda$ schreiben, wobei $\Lambda \subset R^n$ eine Untergruppe von endlichem Index ist. Nun ist $S = \{s \in R : s\Lambda \subset \Lambda\}$ eine Ordnung in einem quadratischen Zahlkörper, und Λ ist torsionsfreier S-Modul vom Rang n. Nach (2.3) schreibt sich $\Lambda \simeq \Lambda_1 \oplus ... \oplus \Lambda_n$ als direkte Summe von S-Moduln vom Rang eins. Es ergibt sich ein Isomorphismus komplexer Vektorräume

$$\mathbf{C}^n \simeq (R \otimes \mathbf{R})^n \simeq \Lambda \otimes \mathbf{R} \simeq \Lambda_1 \otimes \mathbf{R} \ \oplus ... \oplus \ \Lambda_n \otimes \mathbf{R},$$

wobei die tautologische Operation von $S \otimes \mathbf{R} \simeq R \otimes \mathbf{R} \simeq \mathbf{C}$ auf $\Lambda_i \otimes \mathbf{R}$ die komplexe Struktur auf diesem Summanden liefert. Hieraus folgt der verlangte Isomorphismus

$$A \simeq \Lambda_1 \otimes \mathbf{R}/\Lambda_1 \ \times \ ... \ \times \ \Lambda_n \otimes \mathbf{R}/\Lambda_n \tag{2.5}$$

zu einem Produkt elliptischer Kurven.

BEMERKUNG 2.6: In der Zerlegung $\Lambda \simeq \Lambda_1 \oplus ... \oplus \Lambda_n$ sind die Isomorphieklassen der S-Moduln Λ_i nicht immer eindeutig bestimmt. Dies sieht man schon bei $R^2 \simeq \mathfrak{a} \oplus \bar{\mathfrak{a}}$, wobei $\mathfrak{a}$ ein Ideal von R und $\bar{\mathfrak{a}}$ das konjugierte Ideal ist. Schreiben wir $S_i = \{s \in K : s\Lambda_i \subset \Lambda_i\}$, dann kann man nach [**BF2**] die Zerlegung $\Lambda = \Lambda_1 \oplus ... \oplus \Lambda_n$ so wählen, daß S_i stets in S_{i+1} enthalten ist. Jeder S_i-Modul Λ_i ist zu einem Untermodul von K isomorph. Damit

ist $\prod_{1\leq i\leq n}\Lambda_i \in Pic(S_n)$ wohl definiert. Diese Klasse und die Sequenz der Ordnungen $S_1 \subset ... \subset S_n$ bestimmen Λ als S-Modul bis auf Isomorphie [**BF2**]. Man kann $\Lambda_i = S_i$ für $1 \leq i \leq n-1$ wählen, was Λ_n bis auf Isomorphie festlegt. Die Folgerungen für die Zerlegung von A als Summe elliptischer Kurven liegen auf der Hand. Die Mehrdeutigkeit der Zerlegung im Falle, daß A eine Abelsche fläche ist, wurde schon in [**S**] untersucht.

3. Ein Unzerlegbarkeitskriterium.

Sei $E = \mathbf{C}^g/\Gamma$ eine einfache Abelsche Varietät, $R = End(E)$ und $K = R \otimes \mathbf{Q}$. Dann gilt $End(E^n) \simeq M_n(R)$. Γ^n ist auf kanonische Weise ein $M_n(R)$-Modul. Sei $\Lambda \subset \Gamma^n$ eine Untergruppe von endlichem Index. Definiere $L = End_{M_n(K)}(\Gamma^n \otimes \mathbf{Q})$ und $\tilde{S} = \{s \in L : s\Lambda \subset \Lambda\}$.

SATZ 3.1. *Ist Λ unzerlegbar als $\tilde{S}$-Modul, dann enthält die zu E^n gehörige Isogenieklasse eine unzerlegbare Abelsche Varietät.*

BEWEIS: $A = \mathbf{C}^{gn}/\Lambda$ ist zu $(\mathbf{C}^g/\Gamma)^n \simeq E^n$ isogen. $End(A) = \{t \in M_n(K) : t\Lambda \subset \Lambda\}$ ist eine $M_n(K)$-Ordnung. Wäre A zerlegbar, so existierten nichttriviale orthogonale Idempotente $P_1, P_2 \in End(A)$, so daß $\Lambda = P_1\Lambda \oplus P_2\Lambda$ eine direkte Summe nichttrivialer Untergruppen wäre. P_1 und P_2 sind jedoch $\tilde{S}$-linear, was der Annahme, Λ sei unzerlegbar, widerspricht.

Die einfachen Abelschen Varietäten lassen sich in drei Klassen einteilen:

(1) K ist kommutativ und $dim_K\Gamma \otimes \mathbf{Q} = 1$. In diesem Fall sagt man, E habe komplexe Multiplikation.
(2) K ist nicht kommutativ und $dim_K\Gamma \otimes \mathbf{Q} = 1$.
(3) $dim_K\Gamma \otimes \mathbf{Q} = b > 1$.

4. Abelsche Varietäten mit komplexer Multiplikation.

SATZ 4.1. *Sei $E = \mathbf{C}^g/\Gamma$ eine einfache Abelsche Varietät der Dimension $g > 1$. Wenn E komplexe Multiplikation hat, enthält die Isogenieklasse von E^n eine unzerlegbare Abelsche Varietät.*

BEWEIS: Aus $dim_K\Gamma \otimes \mathbf{Q} = 1$, folgt $L = End_{M_n(K)}(K^n) =$ Zentrum $(M_n(K)) \simeq K$. Wir können o.B.d.A. annehmen $\Gamma = R$. Dann ist $\Gamma^n = R^n$, und die Operation des Unterrings $R \subset L$ auf R^n ist die übliche. Wir wählen eine rationale Primzahl p die in R völlig zerfällt [**N**,V6.5], und definieren die K-Ordnung $S = \mathbf{Z} + pR$. Ein Spezialfall einer Konstruktion von Dade [**C-R**,Thm 33.8] liefert einen unzerlegbaren S-Untermodul $\Lambda \subset R^n$ von endlichem Index. Da $S \subset \tilde{S}$, ist nach (3.1) die zu E^n isogene Abelsche Varietät $A = \mathbf{C}^{gn}/\Lambda$ unzerlegbar.

Der Vollständigkeit halber führen wir die Konstruktion von Dade in dem von uns benötigten Fall durch. Da p völlig zerfällt, induziert Reduktion modulo p einen surjektiven Ringhomomorphismus $\pi : R[x]/x^n \to (\mathbf{F}_p[x]/x^n)^{2g}$. Definiere

$$W = \text{ Bild } ((\mathbf{F}_p[x]/x^n)^2 \to (\mathbf{F}_p[x]/x^n)^{2g}), \qquad (a,b) \to (a, b, a+b, a+bx, a, ..., a)$$

und $\Lambda = \pi^{-1}(W)$. (Hier wird die Voraussetzung $g > 1$ verwendet.) Nun ist Λ ein S-Untermodul von $R[x]/x^n \simeq R^n$ und genügt $R \otimes_S \Lambda \simeq R[x]/x^n$. Um die Unzerlegbarkeit

von Λ zu zeigen, weisen wir nach, daß 0 und 1 die einzigen idempotenten Elemente von $End_S(\Lambda)$ sind.

Ist nämlich $f \in End_S(\Lambda)$ idempotent, dann ist $1 \otimes f \in End_R(R \otimes_S \Lambda) = End_R(R[x]/x^n)$ auch idempotent. Durch Reduktion modulo p erhalten wir ein idempotentes Element $\bar{f} \in End_{\mathbf{F}_p^{2g}}((\mathbf{F}_p[x]/x^n)^{2g})$, mit $\bar{f}(W) \subset W$. Ist f von 0 und 1 verschieden, so hat nach dem Lemma von Nakayama $\bar{f}$ die gleiche Eigenschaft. Weil $\bar{f}$ bezüglich $\mathbf{F}_p^{2g}$ linear ist, gilt $\bar{f} = \oplus_{1 \le i \le 2g} \bar{f}_i$ mit $\bar{f}_i \in End_{\mathbf{F}_p}(\mathbf{F}_p[x]/x^n)$. Aus $\bar{f}(W) \subset W$ folgt

$$\bar{f}(a, 0, a, ..., a) = (\bar{f}_1 a, 0, \bar{f}_3 a, ..., \bar{f}_{2g} a), \qquad \text{also} \qquad \bar{f}_1 = \bar{f}_3 = ... = \bar{f}_{2g}$$
$$\text{und } \bar{f}(0, b, b, bx, 0, ..., 0) = (0, \bar{f}_2 b, \bar{f}_3 b, x\bar{f}_3 b, 0, ..., 0), \quad \text{also} \quad \bar{f}_2 = \bar{f}_3, \bar{f}_4(bx) = x\bar{f}_3(b).$$

Offenbar sind alle $\bar{f}_i$ gleich und darüber hinaus $\mathbf{F}_p[x]/x^n$-linear. Deshalb gilt $\bar{f} = (h, ..., h)$, wobei h durch Multiplikation mit einem idempotenten Element aus $\mathbf{F}_p[x]/x^n$ gegeben wird. Die einzigen idempotenten Elemente im lokalen Ring $\mathbf{F}_p[x]/x^n$ sind 0 und 1.

5. Einfache Abelsche Varietäten von den Typen 2 und 3.

Unzerlegbare Abelsche Varietäten werden mit Hilfe folgenden Satzes aus der ganzzahligen Darstellungstheorie konstruiert.

SATZ 5.1. *Für $b > 1$ und $n > 0$ existiert ein unzerlegbarer $\mathbf{Z}_p I + pM_b(\mathbf{Z}_p)$-Modul Λ'_p mit $Rang_{\mathbf{Z}_p} \Lambda'_p = bn$.*

SATZ 5.2. *Sei E eine einfache Abelsche Varietät vom Typ 2 oder 3. Ist $n > 0$, dann enthält die Isogenieklasse von E^n eine unzerlegbare Abelsche Varietät.*

BEWEIS: Wir behandeln zunächst den Fall, daß E vom Typ 3 ist. Indem E durch eine isogene Abelsche Varietät ersetzt wird, können wir annehmen $\Gamma \simeq R \otimes \mathbf{Z}^b$. Hieraus ergibt sich eine Einbettung $M_b(\mathbf{Z}) \subset End_{M_n(R)}(\Gamma^n)$. Nach (5.1) existiert ein unzerlegbarer $\mathbf{Z}_p I + pM_b(\mathbf{Z}_p)$-Modul, Λ'_p, mit $Rang_{\mathbf{Z}_p}(\Lambda'_p) = bmRang_{\mathbf{Z}} R$. Wir dürfen o.B.d.A. annehmen, Λ'_p sei ein $\mathbf{Z}_p I + pM_b(\mathbf{Z}_p)$-Untermodul von $R^n \otimes \mathbf{Z}_p^b$ von endlichem Index. Definiere $\Lambda = R^n \otimes \mathbf{Z}^b \cap \Lambda'_p \subset R^n \otimes \mathbf{Z}_p^b$. Dann ist Λ ein $S = \mathbf{Z}I + pM_n(\mathbf{Z})$-Untermodul von Γ^n von endlichem Index. Ferner gilt $\Lambda \otimes \mathbf{Z}_p \simeq \Lambda'_p$. Infolgedessen ist Λ unzerlegbar als S-Modul. S wird mit einem Unterring von $\tilde{S}$ identifiziert, was die $\tilde{S}$-Unzerlegbarkeit von Λ impliziert. Offensichtlich ist $A = \mathbf{C}^{gn}/\Lambda$ zu $E^n = (\mathbf{C}^g/\Gamma)^n$ isogen. Die Unzerlegbarkeit von A folgt aus (3.1).

Sei nun $E = \mathbf{C}^g/\Gamma$ eine einfache Abelsche Varietät vom Typ 2. Wir können o.B.d.A. annehmen, Γ sei ein freier R-Modul vom Rang 1. R operiert diagonal vom rechts auf R^n und liefert dadurch eine Einbettung $R^\circ \subset End_{M_n(R)}(\Gamma^n)$. $R^\circ \otimes \mathbf{Q} = K^\circ$ ist eine Divisionsalgebra mit einem Zahlkörper C als Zentrum. Es gibt eine feste Zahl $b > 1$ mit der Eigenschaft, daß für fast alle Stellen ν von C gilt $K^\circ_\nu \simeq M_b(C_\nu)$ [**W**,XI Thm.1]. Für unendliche viele Stellen ν existiert nach dem Satz von Tschebotarev [**N**,V6.5] eine rationale Primzahl p, so daß $C_\nu \simeq \mathbf{Q}_p$. Da R° fast überall lokal mit der maximalen Ordnung übereinstimmt, können wir eine Stelle ν so wählen, daß $R^\circ_\nu \simeq M_b(\mathbf{Z}_p)$. Nach (5.1) gibt es einen unzerlegbaren $\mathbf{Z}_p I + pM_b(\mathbf{Z}_p)$-Modul Λ'_p mit $Rang_{\mathbf{Z}_p} \Lambda'_p = b^2 n$. Jeder

solche Modul läßt sich als $\mathbf{Z}_p I + pM_b(\mathbf{Z}_p)$-Untermodul von endlichem Index in $M_b(\mathbf{Z}_p)^n$ auffassen. Mit Hilfe der Identifizierung $R_\nu^\circ \simeq M_b(\mathbf{Z}_p)$ definieren wir

$$S = R^\circ \cap (\mathbf{Z}_p + pR_\nu^\circ) \subset R_\nu^\circ \qquad \text{und} \qquad \Lambda = \Lambda_p' \cap (R^\circ)^n \subset (R_\nu^\circ)^n.$$

Offenbar ist $\Lambda \subset R^n \simeq \Gamma^n$ ein S-Modul von endlichem Index. Wegen $S_\nu \simeq \mathbf{Z}_p I + pM_b(\mathbf{Z}_p)$ und $\Lambda_\nu \simeq \Lambda_p'$ ist Λ unzerlegbar. $A = \mathbf{C}^{gn}/\Lambda$ ist zu $E^n = (\mathbf{C}^g/\Gamma)^n$ isogen. Nach (3.1) ist A unzerlegbar.

Der Vollständigkeit halber geben wir einen Bewies von (5.1). (Siehe [**C-R**,§34D]).

BEWEIS VON 5.1: Wir schreiben $\tilde{T} = M_b(\mathbf{Z}_p)$, $T = \mathbf{Z}_p I + pM_b(\mathbf{Z}_p)$ und $L = \mathbf{Z}_p^b$ für den tautologischen $\tilde{T}$-Modul. Ein $\mathbf{Z}_p$- freier $\tilde{T}$- (bzw. T)-Modul heißt $\tilde{T}$- (bzw. T)-Gitter. Ein T-Gitter, M, liefert eine exakte Sequenz von T-Moduln

$$0 \to p\tilde{T}M \xrightarrow{i} M \xrightarrow{\pi} M/p\tilde{T}M \to 0, \tag{5.3}$$

wobei $p\tilde{T}M$ sogar ein $\tilde{T}$-Gitter und $M/p\tilde{T}M$ ein $T/p\tilde{T} \simeq \mathsf{F}_p$-Vektorraum ist. Jedes $\tilde{T}$-Gitter ist zu L^r für geeignetes r isomorph [**C-R**, 26.28(iv)]. Damit ist M eine Modulerweiterung von F_p^s durch L^r. Es gilt, die Erweiterungsklasse in $Ext_T^1(\mathsf{F}_p^s, L^r)$ so zu wählen, daß M unzerlegbar ist.

Die Gruppe der Erweiterungsklassen wird dadurch berechnet, daß $Hom_T(\ , L^r)$ auf die exakte Sequenz

$$0 \to \tilde{T}^s \xrightarrow{p} T^s \to \mathsf{F}_p^s \to 0$$

angewandt wird. Ein Isomorphismus

$$Hom_T(\tilde{T}^s, L^r)/pHom_T(T^s, L^r) \xrightarrow{\sim} Ext_T^1(\mathsf{F}_p^s, L^r) \tag{5.4}$$

entsteht, der wie folgt zu interpretieren ist: Einem Homomorphismus $F \in Hom_T(\tilde{T}^s, L^r)$ ordnet man den T-Modul $M = L^r \oplus T^s/(F \oplus (-p))(\tilde{T}^s)$ und die Modulerweiterung in der unteren Zeile des kommutativen Diagrams,

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \tilde{T}^s & \xrightarrow{p} & T^s & \longrightarrow & \mathsf{F}_p^s & \longrightarrow & 0 \\ & & {\scriptstyle F}\downarrow & & \downarrow & & \| & & \\ 0 & \longrightarrow & L^r & \longrightarrow & M & \longrightarrow & \mathsf{F}_p^s & \longrightarrow & 0 \end{array} \tag{5.5}$$

zu. Wenn $L^r = p\tilde{T}M$ gilt, kann die untere Zeile mit (5.3) identifiziert werden. Dies kommt vor, wenn F surjektiv ist, wie man aus

$$p\tilde{T}M = pL^r \oplus p\tilde{T}^s/((F \oplus (-p))(\tilde{T}^s) \cap pL^r \oplus p\tilde{T}^s) \to L^r, \qquad (x, y) \to x + F(y/p),$$

entnimmt.

Wenn M zerfällt, so zerfällt die ganze Sequenz (5.3) als

$$0 \longrightarrow p\tilde{T}M_1 \oplus p\tilde{T}M_2 \longrightarrow M_1 \oplus M_2 \longrightarrow M_1/p\tilde{T}M_1 \oplus M_2/p\tilde{T}M_2 \longrightarrow 0. \tag{5.6}$$

Um alles nun explizit durch Matrizen ausdrücken zu können, wird der Isomorphismus

$$Hom_T(\tilde{T}^s, L^r)/pHom_T(T^s, L^r) \xrightarrow{\alpha} Hom_{\mathbf{F}_p}(\mathbf{F}_p^s, L^r/p) \simeq Hom_{\mathbf{F}_p}(\mathbf{F}_p^s, \mathbf{F}_p^r) \otimes_{\mathbf{Z}} L,$$

$$\alpha(F)\begin{pmatrix} \bar{a}_1 \\ \vdots \\ \bar{a}_s \end{pmatrix} = F\begin{pmatrix} a_1 I \\ \vdots \\ a_s I \end{pmatrix} \mod p \tag{5.7}$$

eingeführt. Identifiziere $p\tilde{T}M_i \simeq L^{r_i}$, $M_i/p\tilde{T}M_i \simeq \mathbf{F}_p^{s_i}$ und schreibe $\gamma : L^r \simeq L^{r_1} \oplus L^{r_2}$ und $\mu : \mathbf{F}_p^s \simeq \mathbf{F}_p^{s_1} \oplus \mathbf{F}_p^{s_2}$ für die durch den Isomorphismus von (5.3) nach (5.6) induzierten Abbildungen. Da γ T-linear ist, existiert $\bar{\gamma} \in Gl(\mathbf{F}_p^r)$ mit $\bar{\gamma} \circ \alpha(F) = \alpha(\gamma \circ F)$.

Ein Element aus $Ext_T^1(\mathbf{F}_p^s, L^r)$ schreibt sich wegen (5.4) und (5.6) bezüglich einer Basis $\{e_1, ..., e_b\}$ von L in der Form $\sum_{1 \le i \le b} F_i \otimes e_i \in Hom_{\mathbf{F}_p}(\mathbf{F}_p^s, \mathbf{F}_p^r) \otimes L$. Setze

$$r = s, \qquad F_1 = I, \qquad F_2 = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix} \qquad \text{und} \qquad F_i = 0 (i \ge 3).$$

Aus $F_1 = I$ folgt, daß F surjektiv ist. Nach (5.5) ist der zu dieser Erweiterungsklasse assozierte T-Modul M ein Gitter. Zerfiele M, dann existierten Matrizen $\bar{\gamma}, \mu \in GL(\mathbf{F}_p^r)$, so daß

$$\bar{\gamma} F_i \mu \in Hom(\mathbf{F}_p^{r_1}, \mathbf{F}_p^{s_1}) \oplus Hom(\mathbf{F}_p^{r_2}, \mathbf{F}_p^{s_2}) \subset End_{\mathbf{F}_p}(\mathbf{F}_p^r)$$

für geeignete positive Zahlen $r_1 + r_2 = r, s_1 + s_2 = r$ und alle $i \in \{1, ..., b\}$. Bei der obigen Wahl von F_1 und F_2 ist dies jedoch nicht möglich, wie wir nun zeigen.

Die Invertierbarkeit von $\bar{\gamma} F_1 \mu = \bar{\gamma}\mu$ impliziert $r_1 = s_1$, $r_2 = s_2$ und $\bar{\gamma}\mu \in End(\mathbf{F}_p^{r_1})^* \times End(\mathbf{F}_p^{r_2})^*$. Der charakteristische Polynom von F_2 ist x^r. Deshalb gilt $\bar{\gamma} F_2 \bar{\gamma}^{-1} \notin End(\mathbf{F}_p^{r_1}) \times End(\mathbf{F}_p^{r_2})$, woraus $\bar{\gamma} F_2 \mu = \bar{\gamma} F_2 \bar{\gamma}^{-1} \bar{\gamma}\mu \notin End(\mathbf{F}_p^{r_1}) \times End(\mathbf{F}_p^{r_2})$ folgt.

Literatur.

[Ba] Bass, H., Torsion free and projective modules, Trans. Amer. Math. Soc. 102, 319-327 (1962)

[BF1] Borevich, Z. I. and Faddeev, D. K., Integral representations of quadratic rings (in Russian), Vestnik Leningrad. Univ. 15, no. 19, 52-64 (1960)

[BF2] Borevich, Z. I. and Faddeev, D. K., Representations of orders with cyclic index, Trudy. Mat. Inst. Steklov. 80, 51-65 (1965)

[BF3] Borevich, Z. I. and Faddeev, D. K., Remarks on orders with cyclic index, Soviet math. Dokl. 6, 1273-1274 (1965)

[C-R] Curtis, C. and Reiner, I., Methods of Representation Theory, vol. I, John Wiley and Sons, New York (1981)

[K] Katsura, T., On the structure of singular abelian varieties, Proc. Japan Acad. 51, 224-228 (1975)

[L] Lange, H., Produkte elliptischer Kurven, Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl. II, 95-108 (1975)

[Mu] Mumford, D., Abelian Varieties, Oxford University Press (1970)

[N] Neukirch, J., Class Field Theory, Springer-Verlag (1986)

[R] Ruppert, W., When is an abelian surface isomorphic or isogenous to a product of elliptic curves?, Math. Z. 203, 293-299 (1990)

[S] Shioda, T., Some remarks on abelian varieties, J. Fac. Sci. Univ. Tokyo Sect. 1A Math. 24, 11-21 (1977)

[S-M] Shioda, T. and Mitani, N., Singular abelian surfaces and binary quadratic forms, in Classification of algebraic varieties and compact complex manifolds, ed. H. Popp, Springer Lect. Notes in Math. 412, 259-287 (1974)

[W] Weil, A., Basic Number Theory, Springer-Verlag (1973)

Department of Mathematics, Duke University, Durham, NC 27706 USA