Zur Existenz einfacher abelscher Varietäten mit komplexer Multiplikation*)

Von *Norbert Schappacher* in Göttingen

Folgendes Resultat wird bewiesen:

Zu vorgegebenem CM-Körper F *gibt es genau dann keinen primitiven CM-Typ* $(\mathsf{F}, \mathfrak{T})$, *wenn* F *galoissch über* $\mathbb{Q}$ *und* $\mathrm{Gal}(\mathsf{F}/\mathbb{Q})$ *entweder die Kleinsche Vierergruppe oder die Diedergruppe der Ordnung acht ist.*

Dabei ist ein *CM-Körper* F eine total imaginäre, quadratische Erweiterung eines total reellen algebraischen Zahlkörpers K. (Vgl. [2], p. 125. — *CM* steht für *Complex Multiplication.*) Ist $\mathfrak{T}$ eine Menge von Isomorphismen $\mathsf{F} \to \mathbb{C}$, die zu jeder Einbettung $\varphi : \mathsf{K} \to \mathbb{R}$ genau eine der beiden Fortsetzungen von φ auf F enthält, so heißt $(\mathsf{F}, \mathfrak{T})$ ein *CM-Typ.* (Für den Zusammenhang mit abelschen Varietäten siehe [1], insbesondere pp. 43ff.) In Sprachmißbrauch nennen wir dann auch $\mathfrak{T}$ einen *CM-Typ für* F. Man nennt $(\mathsf{F}, \mathfrak{T})$ — bzw. $\mathfrak{T}$ — *primitiv*, falls die abelschen Varietäten vom Typ $(\mathsf{F}, \mathfrak{T})$ einfach sind. ([1], p. 68/69.)

Die Primitivität eines *CM*-Typs kann rein galois-theoretisch definiert werden. (Vgl. [1], pp. 66—74.) Dementsprechend ist der folgende Beweis des Resultats rein gruppentheoretischer Natur (wenn auch weitgehend körpertheoretisch formuliert).

1. Seien $\mathsf{F}, \mathsf{K}, \mathfrak{T}$ wie oben; $(\mathsf{F} : \mathbb{Q}) = 2 \cdot (\mathsf{K} : \mathbb{Q}) = 2n$. Es gibt offenbar genau 2^n verschiedene *CM*-Typen $\mathfrak{T}$ zu vorgegebenem F. Wir betrachten im folgenden alle Zahlkörper als Teilkörper von $\mathbb{C}$ und bezeichnen mit ϱ den Übergang zum komplex Konjugierten. Die *CM*-Körper sind unter den imaginären Zahlkörpern charakterisiert durch: $\mathsf{F}^{\varrho} \subset \mathsf{F}$ und $\varrho\varphi = \varphi\varrho$ für alle Isomorphismen $\varphi : \mathsf{F} \to \mathbb{C}$. ([2], Prop. 5. 5. 11, p. 125.) Jeder imaginäre Teilkörper eines *CM*-Körpers ist selbst ein *CM*-Körper.

Sei L die (über $\mathbb{Q}$) normale Hülle von F; $G = \mathrm{Gal}(\mathsf{L}/\mathbb{Q})$. Wir setzen:

$$\mathbf{S}(\mathfrak{T}) = \{\sigma \in G : \text{es gibt ein } \varphi \in \mathfrak{T} \text{ mit } \sigma|_{\mathsf{F}} = \varphi\}$$
$$H(\mathfrak{T}) = \{\sigma \in G : \sigma\mathbf{S}(\mathfrak{T}) = \mathbf{S}(\mathfrak{T})\}.$$

Der Fixkörper $\mathsf{F}(\mathfrak{T})$ von $H(\mathfrak{T})$ ist in F enthalten.

---

*) Dieser Artikel gibt einen Teil der 1975 in Göttingen eingereichten Diplomarbeit des Verfassers wieder. Die Arbeit wurde, betreut durch Herrn E. Maus, teils in Göttingen, teils während eines EAP-Studienaufenthaltes an der University of California in Berkeley angefertigt.

$(\mathsf{F}, \mathfrak{T})$ *ist genau dann primitiv, wenn* $\mathsf{F} = \mathsf{F}(\mathfrak{T})$ *ist.* ([1], p. 69.)

Da $\mathbf{S}(\mathfrak{T})$ aus vollen Rechtsnebenklassen von $H(\mathfrak{T})$ besteht, erhält man zu $\mathfrak{T}$ einen CM-Typ $\mathfrak{T}_0$ von $\mathsf{F}(\mathfrak{T})$, mit $\mathfrak{T} = \mathfrak{T}_0$, falls $\mathfrak{T}$ primitiv ist. ($\mathsf{F}(\mathfrak{T})$ ist wieder CM-Körper!) Besteht allgemein $\mathfrak{T}$ aus allen möglichen Fortsetzungen auf F sämtlicher Elemente eines CM-Typs $\mathfrak{T}_0$ eines Teil-CM-Körpers F_0 von F, so sagen wir, $\mathfrak{T}$ sei *die Fortsetzung von* $\mathfrak{T}_0$ *auf* F. Man beweist leicht den

Hilfssatz. *Man erhält die nicht primitiven CM-Typen* $\mathfrak{T}$ *von* F *gerade als Fortsetzungen aller CM-Typen* $\mathfrak{T}_0$ *der maximalen echten Teil-CM-Körper* F_0 *von* F.

2. *Sei jetzt* F *galoissch.* Dann ist $\langle \varrho \rangle$ normale Untergruppe von $G = \mathrm{Gal}(\mathsf{F}/\mathbb{Q})$, und ein primitiver CM-Typ $\mathfrak{T}$ für F ist ein Repräsentantensystem von $G/\langle \varrho \rangle$, welches nur von $\mathbf{1} \in G$ unter Linksmultiplikation in sich überführt wird. Wir nennen $\mathfrak{T}$ auch einen (primitiven) *CM-Typ von G bzgl.* ϱ. Die Anzahl der primitiven CM-Typen von G bzgl. ϱ ist durch $2n$ teilbar. Ist $\mathsf{f} \in \mathrm{Aut}\, G$, so entsprechen die primitiven CM-Typen von G bzgl. ϱ vermöge f umkehrbar eindeutig denjenigen bzgl. $\mathsf{f}\varrho$.

Definition. Für jeden ungeraden Primteiler p von n setzen wir:

$d(p) = (\text{Anzahl der Elemente der Ordnung } p \text{ in } G) \cdot (p-1)^{-1}$

$d(2) = (\text{Anzahl der Elemente der Ordnung 2 in } G) - 1.$

Satz 1. *Ist* F *galoissch über* $\mathbb{Q}$, *so ist die Anzahl der nicht primitiven CM-Typen für* F *kleiner oder gleich*

$$\mathrm{B}(G) = \sum_{p \mid n} d(p) \cdot 2^{n/p},$$

wo p alle Primteiler von n durchläuft.

Beweis. Wir verwenden den Hilfssatz. Die maximalen echten Teil-CM-Körper von F entsprechen genau den Untergruppen von G, die von Elementen mit Primzahlordnung erzeugt werden — mit Ausnahme der von ϱ erzeugten Untergruppe. Da diese Untergruppen ϱ nicht enthalten, muß ihre Ordnung n teilen. Schließlich erzeugen je $p-1$ Elemente dieselbe Untergruppe der Ordnung p, und es gibt genau $2^{n/p}$ CM-Typen für einen CM-Körper des Grades $2\frac{n}{p}$ über $\mathbb{Q}$.

Bemerkung. Die Abschätzung aus Satz 1 ist im allgemeinen nicht optimal. (Für $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ z. B. ist sogar $\mathrm{B}(G) = 24 > 2^4$.) Das liegt daran, daß maximale Teil-CM-Körper sich in kleineren CM-Körpern schneiden können, deren CM-Typen dann mehrfach gezählt werden.

Ist allerdings etwa $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ oder $G = \mathfrak{D}_4$, so kann nichts dergleichen passieren, weil dann jede zu einem echten Teil-CM-Körper von F gehörige Untergruppe von G die Ordnung zwei hat. (Beachte, daß ϱ im Zentrum liegen muß, und daher im Falle $G = \mathfrak{D}_4 = \langle \sigma, \tau \rangle$ zwangsläufig $\varrho = \sigma^2$ ist!) In beiden Fällen gibt es also genau $\mathrm{B}(G)$ nicht primitive CM-Typen für F. Wegen $\mathrm{B}(\mathbb{Z}_2 \times \mathbb{Z}_2) = 4$ und $\mathrm{B}(\mathfrak{D}_4) = 16$ zeigt das, daß *es keine primitiven CM-Typen für* F *gibt, falls* F *galoissch mit Galoisgruppe* $\mathbb{Z}_2 \times \mathbb{Z}_2$ *oder* $\mathfrak{D}_4$ *ist.*

Ist p_0 der kleinste Primteiler von n, so gilt offenbar

$$\mathrm{B}(G) \leqq (2n-2) \cdot 2^{n/p_0} \cdot (p_0 - 1)^{-1}. \tag{1}$$

A fortiori also

$$B(G) \leqq (2n-2) \cdot 2^{n/2}. \tag{2}$$

Insbesondere „wächst" also im galoisschen Fall die Anzahl der primitiven CM-Typen „mit n".

Wir können jetzt den galoisschen Fall unseres Resultats beweisen:

Satz 2. *Sei G eine Gruppe der Ordnung $2n$, ϱ ein Element der Ordnung 2, welches im Zentrum von G liegt. G besitzt genau dann keinen primitiven CM-Typ bzgl. ϱ, wenn entweder $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ oder $G = \mathfrak{D}_4$ ist.*

Beweis. Es ist $(2n-2)\, 2^{n/2} < 2^n$ für alle $n \geqq 8$. Also folgt die Behauptung für $n \geqq 8$ aus Satz 1 mithilfe der Abschätzung (2). Für $n = 3, 5, 7$ folgt sie ebenso leicht mithilfe der Abschätzung (1). Die verbleibenden Fälle rechnet man einzeln nach:

n = 6

$$\left.\begin{array}{ll} G = \mathbb{Z}_{12} & B(G) = 4 \\ G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 & B(G) = 20 \\ G = \mathfrak{D}_6 & B(G) = 52 \\ G = \mathbb{Z}_3 \rtimes \mathbb{Z}_4 \ (\textit{semidir.}) & B(G) = 4 \end{array}\right\} < 2^6.$$

Da $G = \mathfrak{A}_4$ in unserer Theorie nicht auftritt, haben wir nach Satz 1 für $n = 6$ in jedem Falle die Existenz primitiver CM-Typen nachgewiesen.

n = 4

$G = \mathbb{Z}_8$ $\quad B(G) = 0$

G die Quaternionengruppe $\quad B(G) = 0$ } alle CM-Typen sind primitiv.

$G = \mathbb{Z}_2 \times \mathbb{Z}_4$ $\quad B(G) = 8 < 2^4$.

$G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: Da G genug Automorphismen hat, reicht es, bzgl. $\varrho = (0, 0, 1)$ einen primitiven CM-Typ anzugeben: $\{0, 0, 0), (1, 0, 0), (0, 1, 0), (1, 1, 1)\}$ ist z.B. offensichtlich primitiv.

$G = \mathfrak{D}_4$ wurde bereits als Ausnahme erkannt.

n = 2

Ist G zyklisch, so ist wieder $B(G) = 0$. Die Kleinsche Vierergruppe ist uns als Ausnahme schon bekannt.

Damit ist Satz 2 bewiesen.

3. *Sei* F *nicht mehr notwendig galoissch.*

Definition. Seien $\mathfrak{T}$ und $\mathfrak{T}'$ CM-Typen für F. $\mathfrak{T}'$ heißt *Nachbar* von $\mathfrak{T}$, falls $\mathfrak{T}$ und $\mathfrak{T}'$ in genau $n-1$ ihrer n Elemente übereinstimmen.

Satz 3. *Sei* F *ein CM-Körper vom Grade* $(\mathsf{F} : \mathbb{Q}) = 2n$.

(a) *Ist n ungerade, so hat jeder CM-Typ von* F *mindestens einen primitiven Nachbarn.*

(b) *Ist n gerade und* F *nicht galoissch über $\mathbb{Q}$, so gibt es primitive CM-Typen für* F.

Vorüberlegung zum Beweis. Sei $\mathfrak{T}$ ein CM-Typ von F. Wir legen eine feste Numerierung der Elemente von $\mathfrak{T}$ zugrunde, so daß wir vom *i-ten Nachbarn* $\mathfrak{T}^i$ von $\mathfrak{T}$ reden können (für $i=1,\ldots,n$):

$$\mathfrak{T}=\{\varphi_1,\ldots,\varphi_n\},\quad \mathfrak{T}^i=\{\varphi_1,\ldots,\varrho\varphi_i,\ldots,\varphi_n\}.$$

Wir denken uns alle φ_i auf eine bestimmte Weise auf L fortgesetzt, d. h. $\varphi_i\in G=\mathrm{Gal}(\mathsf{L}/\mathbb{Q})$. (Bezeichnungen wie im Abschnitt 1!) Schreibe

$$K_0=H(\mathfrak{T});\quad K_i=H(\mathfrak{T}^i)\quad\text{für}\quad i=1,\ldots,n.$$

Sei H die F entsprechende Untergruppe von G. Setze $k_i=(K_i:H)$ für $i=0,\ldots,n$.

Man hat stets:

$$K_0\cap K_i=H\quad\text{für}\quad i\neq 0. \tag{3}$$

Denn aus $\sigma\in K_0\cap K_i$ folgt $\sigma\bigcup_{j\neq i}H\varphi_j=\bigcup_{j\neq i}H\varphi_j$, also $\sigma H\varphi_i=H\varphi_i$, d. h. $\sigma\in H$.

$$(K_i\cap K_j:H)\leqq 2\quad\text{für}\quad i\neq j. \tag{4}$$

Ist nämlich $\sigma\in K_i\cap K_j-H$, so gilt

$$\sigma(H\varphi_i\varrho\cup H\varphi_j)=H\varphi_i\varrho\cup H\varphi_j,$$

mithin insbesondere $\sigma\in H\varphi_j\varphi_i^{-1}\varrho$.

Beweis von (a). Da n ungerade ist, folgt aus (3) und (4), daß $K_i\cap K_j=H$ ist für alle $i\neq j$; denn die K_i enthalten ϱ nicht, so daß stets $k_i|n$ gilt. Ist nun m die Ordnung von H, so folgt also:

$$m(2n-1)=\#(G-H)>\#\bigcup_{i=0}^{n}K_i-H=m\sum_{0}^{n}(k_i-1).$$

Da aus $k_i\neq 1$ sogar $k_i\geqq 3$ folgt, müssen mindestens zwei der k_i gleich 1 sein. Das beweist (a).

Beweis von (b). Sei N der Normalisator von H in $G=\mathrm{Gal}(\mathsf{L}/\mathbb{Q})$; $r=(G:N)$. Es ist also $r\geqq 2$ vorausgesetzt. Sei $2k=(N:H)$ (es ist $\varrho\in N$!), d. h. $r=n/k$.

Erster Fall: $N/H\neq\mathbb{Z}_2\times\mathbb{Z}_2$ *und* $N/H\neq\mathfrak{D}_4$. Sei $\mathfrak{T}'$ gemäß Satz 2 ein primitiver CM-Typ für N/H bzgl. ϱH: $\mathfrak{T}'=\{\psi_1,\ldots,\psi_k\}$. Sei $\{\sigma_1,\ldots,\sigma_r\}$ ein volles System von Repräsentanten der Rechtsnebenklassen von N in G. Sei $\mathfrak{T}$ der CM-Typ von F mit

$$\mathbf{S}(\mathfrak{T})=\bigcup_{j=1}^{r}(\psi_1\sigma_j\cup\cdots\cup\psi_k\sigma_j).$$

Für $\mathfrak{T}$ ist dann (mit den Bezeichnungen der Vorüberlegung) $K_0-H\subset G-N$. Nach Wahl von $\mathfrak{T}$ ist aber auch $K_i-H\subset G-N$ für $i\geqq 1$, weil $\mathbf{S}(\mathfrak{T}^i)$ wegen $r\geqq 2$ stets mindestens eine unveränderte Teilmenge der Form $\psi_1\sigma_j\cup\cdots\cup\psi_k\sigma_j$ enthält.

Mit (3) und (4) folgt jetzt $K_i\cap K_j=H$ für $i\neq j$, sowie daß $k_i\neq 1$ sofort $k_i\geqq 3$ zur Folge hat. Also können wir wie unter (a) weiterschließen und finden unter den Nachbarn von $\mathfrak{T}$ mindestens einen primitiven CM-Typ.

Zweiter Fall: $N/H = \mathbb{Z}_2 \times \mathbb{Z}_2$ *oder* $N/H = \mathfrak{D}_4$. Sei $\mathfrak{T}'$ irgendein CM-Typ von N/H bzgl. ϱH. Für seinen Stabilisator $H(\mathfrak{T}')$ unter Linksmultiplikation mit Elementen aus N/H gilt dann $H(\mathfrak{T}') = \{H, H\alpha\}$ für ein $\alpha \notin H$. (Für $\mathbb{Z}_2 \times \mathbb{Z}_2$ ist das klar; in $\mathfrak{D}_4$ enthält jede Untergruppe der Ordnung 4 schon $\varrho = \sigma^2$.) Wir konstruieren wie oben aus $\mathfrak{T}'$ einen CM-Typ $\mathfrak{T}$ von F. Bezüglich $\mathfrak{T}$ gilt dann analog:

$$K_i \cap N - H \subset H\alpha .$$

Es ist aber $H\alpha \subset K_0$, so daß aus (3) folgt:

$$H\alpha \cap K_i = \emptyset \quad \text{für} \quad i \geqq 1 .$$

Das besagt wegen (4) wiederum $K_i \cap K_j = H$ für alle $i \neq j$, und daß für $i \geqq 1$ aus $k_i \neq 1$ sogar $k_i \geqq 3$ folgt. Ein Schubfachschluß wie im Beweis von (a) ergibt jetzt ohne weiteres die Existenz eines primitiven Nachbarn von $\mathfrak{T}$. Damit ist Satz 3 vollständig bewiesen.

Bemerkung. Die Existenz *primitiver Nachbarn* zu vorgegebenem CM-Körper, die in Satz 3, (a) in einem Spezialfall bewiesen (und in der dieser Veröffentlichung zugrunde liegenden Diplomarbeit vollständig behandelt) wird, kann zum Studium der Idealgruppe benutzt werden, die man durch Schneiden aller Gruppen H_0 (im Sinne von [1], Main Theorem 1, p. 128) für festes K^* und variierenden *primitiven* CM-Typ $\{\varphi_i\}$ von K^* erhält.

Literatur

[1] *G. Shimura* and *Y. Taniyama*, Complex Multiplication of Abelian Varieties and its Applications to Number Theory, Publ. Math. Soc. Japan **6** (1961).

[2] *G. Shimura*, Introduction to the Arithmetic Theory of Automorphic Functions, Publ. Math. Soc. Japan **11** (1971).

Mathematisches Institut der Universität, Bunsenstr. 3—5, D-3400 Göttingen

Eingegangen 1. Juni 1976