Abelsche Varietäten

Wolfgang M. Ruppert

Sommersemester 1996

2. August 1996 [1]

[1] Im Sommersemester 1996 am Mathematischen Institut der Universität Erlangen-Nürnberg abgehaltene Vorlesung mit dem offiziellen Titel *Diophantische Geometrie II*

Einführung

Abelsche Varietäten sind projektive Varietäten, die eine mit der geometrischen Struktur verträgliche Gruppenstruktur tragen, d.h. sie lassen sich durch (polynomiale) Gleichungen beschreiben und die Addition und Inversenbildung durch (polynomiale) Formeln. Sie spielen eine große Rolle in der Algebraischen Geometrie und in der Zahlentheorie, neuerdings gibt es auch Anwendungen in der Kryptographie.
Für die Vorlesung wählen wir einen elementaren Zugang zu abelschen Varietäten über Thetafunktionen.

Literatur

1. S. Lang, Introduction to Algebraic and Abelian Functions, Springer 1982 [**LangAAF**]. (Hier wird ab Kapitel VI ein elementarer Zugang beschrieben, wie er für die Vorlesung gewählt wird.)
2. H. P. F. Swinnerton-Dyer, Analytic Theory of Abelian Varieties, Cambridge University Press 1974 [**SD**]. (Ähnlich wie Lang.)
3. H. Lange, Ch. Birkenhake, Complex Abelian Varieties, Springer-Verlag 1992 [**LB**]. (Dieses Buch vermittelt einen Eindruck von dem, was über $\mathbf{C}$ studiert wird.)
4. D. Mumford, Abelian Varieties, Oxford University Press 1974 [**Mumford**]. (Standardwerk, setzt Algebraische Geometrie voraus; leider gibt es keinen Fortsetzungsband.)
5. S. Lang, Abelian Varieties, Springer-Verlag 1983, Nachdruck von 1959 [**LangAV**]. (Obwohl eigentlich veraltet, findet man hier einiges, was bei Mumford fehlt.)
6. G. Cornell, J. H. Silverman (eds.), Arithmetic Geometry, Springer 1986 [**CS**]. (Hier sieht man, welche Bedeutung abelsche Varietäten bei dem Beweis der Mordell-Vermutung durch Faltings gespielt haben. Es gibt auch einführende Kapitel über abelsche Varietäten.)
7. S. Lang, Number Theory III — Diophantine Geometry, Springer-Verlag 1991 [**LangDG**]. (In diesem Buch kann man etwas davon sehen, welche Rolle abelsche Varietäten in der Zahlentheorie spielen.)
8. Abelsche Varietäten über endlichen Körpern und Kryptographie [**Koblitz**] [**Spallek**]

Inhaltsverzeichnis

KAPITEL 1

Thetafunktionen

1. Gitter

Im folgenden liegt stets ein komplexer Vektorraum V der Dimension n zugrunde. Also $V \simeq \mathbf{C}^n$. Wir werden auch oft $V = \mathbf{C}^n$ wählen. Den $\mathbf{C}$-Vektorraum V kann man auch als $\mathbf{R}$-Vektorraum auffassen, er hat dann Dimension $2n$; denn ist $e_1, \ldots, e_n$ eine $\mathbf{C}$-Basis von V, so ist $e_1, ie_1, \ldots, e_n, ie_n$ eine $\mathbf{R}$-Basis von V.

DEFINITION 1. *Ein Gitter Λ in einem n-dimensionalen $\mathbf{C}$-Vektorraum V ist ein $\mathbf{Z}$-Modul, so daß es eine $\mathbf{R}$-Basis $u_1, \ldots, u_{2n}$ von V gibt mit*

$$\Lambda = \mathbf{Z}u_1 + \cdots + \mathbf{Z}u_{2n}.$$

Beispiele:

1. Ist $e_1, \ldots, e_n$ eine $\mathbf{C}$-Basis von V, so ist
$$\Lambda = \mathbf{Z}e_1 + \mathbf{Z}ie_1 + \cdots + \mathbf{Z}e_n + \mathbf{Z}ie_n$$
ein Gitter in V.
2. Ist $\tau \in \mathbf{C}$ mit $Im(\tau) > 0$, so ist
$$\Lambda = \mathbf{Z} + \mathbf{Z}\tau$$
ein Gitter in $\mathbf{C}$.
3. Betrachtet man
$$\Lambda = \mathbf{Z} + \mathbf{Z}\sqrt{2} \subseteq \mathbf{C},$$
so gilt zwar als abelsche Gruppe $\Lambda \simeq \mathbf{Z}^2$, Λ ist aber kein Gitter, da der von Λ erzeugte $\mathbf{R}$-Vektorraum nicht ganz $\mathbf{C}$ ist.

DEFINITION 2. *Sei $\Lambda \subseteq \mathbf{C}^n$ ein Gitter und $u_1, \ldots, u_{2n}$ eine Gitterbasis. Dann heißt*

$$\Pi = (u_1 \ldots u_{2n})$$

(eine) Periodenmatrix von Λ.

Sei Λ ein Gitter in $\mathbf{C}^n$ mit Basis $u_1, \ldots, u_{2n}$.

- Λ ist eine Untergruppe der additiven Gruppe von $\mathbf{C}^n$, also erhält man eine Äquivalenzrelation auf $\mathbf{C}^n$ durch die Vorschrift
$$x \equiv y (\mathrm{mod} \Lambda) \quad \Longleftrightarrow \quad x - y \in \Lambda.$$
Die Menge der Äquivalenzklassen wird mit $\mathbf{C}^n/\Lambda$ bezeichnet.
- Jede reelle Zahl λ läßt sich eindeutig zerlegen als $\lambda = m + r$ mit $m \in \mathbf{Z}$ und $0 \leq r < 1$. Sei jetzt $x \in \mathbf{C}^n$. Wir schreiben $x = \lambda_1 u_1 + \cdots + \lambda_{2n} u_{2n}$ mit $\lambda_i \in \mathbf{R}$. Zerlegt man $\lambda_i = m_i + r_i$ mit $m_i \in \mathbf{Z}$ und $0 \leq r_i < 1$, so gilt
$$x \equiv r_1 u_1 + \cdots + r_{2n} u_{2n} \bmod \Lambda,$$
also bildet
$$\{r_1 u_1 + \cdots + r_{2n} u_{2n} : 0 \leq r_i < 1\}$$
ein Repräsentantensystem für die Äquivalenzrelation.
- Mit der Quotiententopologie versehen ist daher $\mathbf{C}^n/\Lambda$ kompakt.
- Wir können dies auch anders beschreiben:
$$\mathbf{C}^n/\Lambda = (\mathbf{R}u_1 + \cdots + \mathbf{R}u_{2n})/(\mathbf{Z}u_1 + \cdots + \mathbf{Z}u_{2n}) \simeq \mathbf{R}/\mathbf{Z} \oplus \cdots \oplus \mathbf{R}/\mathbf{Z}.$$

- Gruppentheoretisch gilt
$$\mathbf{C}^n/\Lambda \simeq S^1 \times \cdots \times S^1,$$
wo S^1 die Einheitskreislinie bezeichnet.

Mit diesen Vorbereitungen kann man definieren:

DEFINITION 3. *Ein komplexer Torus ist ein Quotient $\mathbf{C}^n/\Lambda$, wo Λ ein Gitter $\mathbf{C}^n$ ist.*

Unser Ziel ist die Konstruktion von analytischen bzw. meromorphen Funktionen auf komplexen Tori V/Λ. Dazu müssen wir einige Tatsachen und Grundbegriffe über analytische Funktionen auf $\mathbf{C}^n$ erwähnen.

2. Funktionentheorie mehrerer Veränderlicher

Viele Begriffe und Sätze übertragen sich von der Funktionentheorie einer Veränderlichen. Für Beweise siehe

- Grauert/Fritzsche, Einführung in die Funktionentheorie mehrerer Veränderlicher,
- Gunning/Rossi, Analytic Functions of Several Complex Variables.

Wir schreiben jetzt
$$\mathbf{C}^n = \{(z_1, \ldots, z_n) : z_j \in \mathbf{C}\}$$
und erhalten so komplexe Koordinaten $z_1, \ldots, z_n$ auf $\mathbf{C}^n$. Jedes $z \in \mathbf{C}$ hat eine eindeutige Zerlegung $z = x + iy$ in Realteil x und Imaginärteil y, also erhält man aus $z_j = x_j + iy_j$ reelle Koordinaten $x_1, y_1, \ldots, x_n, y_n$ auf $\mathbf{C}^n$. Typische offene Umgebungen eines Punktes $a \in \mathbf{C}^n$ bilden die Polyzylinder
$$\Delta(a, r) = \{(z_1, \ldots, z_n) \in \mathbf{C}^n : |z_1 - a_1| < r, \ldots, |z_n - a_n| < r\},$$
wobei r eine reelle Zahl > 0 ist.

DEFINITION 4. *Eine auf einer Umgebung eines Punktes $a \in \mathbf{C}^n$ definierte Funktion f heißt holomorph (oder analytisch) in a, falls sich f lokal um a in eine Potenzreihe entwicklen läßt:*
$$f = \sum_{j_1, \ldots, j_n} c_{j_1 \ldots j_n} (z_1 - a_1)^{j_1} \ldots (z_n - a_n)^{j_n}.$$
Eine auf einer offenen Menge U definierte Funktion $f : U \to \mathbf{C}$ heißt holomorph auf U (oder analytisch in U), falls f in jedem Punkt von U holomorph ist.

Natürlich sind holomorphe Funktionen insbesondere stetig.

SATZ 1 (Identitätssatz). *Sind f und g zwei auf einer zusammenhängenden offenen Menge U holomorphe Funktionen, die auf einer nichtleeren offenen Menge übereinstimmen, so gilt $f = g$.*

FOLGERUNG 1. *Sei U eine offene zusammenhängende Teilmenge von $\mathbf{C}^n$. Dann bilden die auf U holomorphen Funktionen einen Integritätsring $\mathcal{O}(U)$.*

Beweis: Daß $\mathcal{O}(U)$ ein kommutativer Ring mit Eins ist, ist klar. Wir müssen noch zeigen, daß $\mathcal{O}(U)$ nullteilerfrei ist: Seien also $f, g \in \mathcal{O}(U)$ mit $fg = 0$.
Ist $f = 0$, so sind wir fertig. Ist $f \neq 0$, so gibt es ein $a \in U$ mit $f(a) \neq 0$. Da f stetig ist, gibt es eine offene Menge U_a mit $a \in U_a \subseteq U$, so daß f in keinem Punkt von U_a Null wird. Also folgt $g|U_a = 0$. Nach dem Identitätssatz folgt $g = 0$, was wir zeigen wollten. ■

Die auf $\mathbf{C}^n$ holomorphen Funktionen bilden also einen Integritätsring. Die Elemente des Quotientenkörpers heißen meromorphe Funktionen, haben also die Form $\frac{f}{g}$.

SATZ 2 (Maximumprinzip). *Sei U eine nichtleere zusammenhängende offene Menge in $\mathbf{C}^n$ und f eine auf U holomorphe Funktion. Nimmt dann $|f|$ ein Maximum in einem Punkt von U an, so ist f schon konstant.*

SATZ 3. *Ist $f : \mathbf{C}^n \to \mathbf{C}$ holomorph mit $f(z) \neq 0$ für alle $z \in \mathbf{C}^n$, so gibt es eine holomorphe Funktion g mit*
$$r(z) = e^{g(z)}.$$

SATZ 4 (Hartogs). *Ist $U \subseteq \mathbf{C}^n$ eine offene Menge und $a \in U$, f eine auf $U \setminus \{a\}$ holomorphe Funktion, so läßt sich f auf ganz U fortsetzen.*

3. Thetafunktionen

Bemerkung: Ist $\Lambda \subseteq \mathbf{C}^n$ ein Gitter, so wollen wir Funktionen auf $\mathbf{C}^n/\Lambda$ konstruieren. Dies entspricht Funktionen $f : \mathbf{C}^n \to \mathbf{C}$ mit $f(x+u) = f(x)$ für alle $u \in \Lambda$. Ist eine solche Funktion holomorph, so wäre sie auch beschränkt, also gäbe es ein Maximum von $|f|$, nach dem Maximumprinzip ist dann f konstant. Daher werden wir die Periodizitätsforderung zunächst etwas abschwächen.

DEFINITION 5. *Eine holomorphe Funktion $f \neq 0$ auf $\mathbf{C}^n$ heißt eine Thetafunktion bzgl. eines Gitters Λ, wenn es Funktionen $L : \mathbf{C}^n \times \Lambda \to \mathbf{C}$ und $J : \Lambda \to \mathbf{C}$ gibt, so daß für jedes $u \in \Lambda$ die Funktion $x \mapsto L(x,u)$ $\mathbf{C}$-linear ist und gilt*

$$f(x+u) = f(x)e^{2\pi i[L(x,u)+J(u)]} \text{ für alle } x \in V \text{ und } u \in \Lambda.$$

Wir sagen, f hat Typ (L,J).

Bemerkungen:

1. Ist f eine Thetafunktion zu den Paaren (L,J) und (L',J'), so gilt $L = L'$ und $J(u) \equiv J'(u) \bmod \mathbf{Z}$. Außerdem kann man J immer additiv um eine Funktion $\tilde{J} : \Lambda \to \mathbf{Z}$ abändern.
2. Die Thetafunktionen vom Typ (L,J) bilden zusammen mit 0 einen $\mathbf{C}$-Vektorraum, den wir mit
$$Th(L,J)$$
bezeichnen.
3. Ist f eine Thetafunktion modulo einem Gitter Λ, so ist f keine Funktion auf $\mathbf{C}^n/\Lambda$, aber die Nullstellenmenge
$$\{\overline{x} \in \mathbf{C}^n/\Lambda : f(x) = 0\}$$
ist wohldefiniert.

Beispiel: Sei $g(x)$ ein quadratisches Polynom und $f(x) = e^{2\pi i g(x)}$. Wir wollen sehen, daß $f(x)$ eine Thetafunktion ist. Es gibt eine symmetrische komplexe Matrix A, eine Linearform $b(x)$ und $c \in \mathbf{C}$, so daß gilt

$$g(x) = \frac{1}{2}x^tAx + b(x) + c.$$

Nun gilt

$$\begin{aligned} f(x+u) &= e^{2\pi i[\frac{1}{2}(x+u)^tA(x+u)+b(x+u)+c]} = \\ &= f(x)e^{2\pi i[x^tAu+\frac{1}{2}u^tAu+b(u)]}, \end{aligned}$$

wählt man also

$$L(x,u) = x^tAu \quad \text{und} \quad J(u) = \frac{1}{2}u^tAu + b(u),$$

so ist f eine Thetafunktion. Thetafunktionen dieser Bauart heißen triviale Thetafunktionen.

SATZ 5. *Sei f eine Thetafunktion ohne Nullstelle. Dann ist f trivial.*

Beweis: Es gibt eine holomorphe Funktion g mit

$$f(x) = e^{2\pi i g(x)}.$$

Es gilt

$$e^{2\pi i[g(x+u)-g(x)]} = \frac{f(x+u)}{f(x)} = e^{2\pi i[L(x,u)+J(u)]},$$

also

$$g(x+u) - g(x) - L(x,u) - J(u) \in \mathbf{Z}.$$

Da wir J um ganze Zahlen abändern können, können wir o.E.

$$g(x+u) - g(x) = L(x,u) + J(u)$$

annehmen. Wir halten jetzt u fest. Dann ist $L(x,u)$ linear in x. Die zweiten partiellen Ableitungen sind also alle 0. Also gilt auch

$$\frac{\partial^2 g}{\partial x_i \partial x_j}(x+u) = \frac{\partial^2 g}{\partial x_i \partial x_j}(x).$$

Da dies wieder für alle u gilt, ist $\frac{\partial^2 g}{\partial x_i \partial x_j}(x)$ periodisch und damit konstant. Die dritten partiellen Ableitungen verschwinden also alle. Damit ist $g(x)$ ein Polynom vom Grad ≤ 2, wie behauptet. ■

LEMMA 1. *Sei f eine Thetafunktion vom Typ (L, J). Dann gilt:*

1. *$L : \mathbf{C}^n \times \Lambda \to \mathbf{C}$ setzt sich eindeutig zu einer Funktion $L : \mathbf{C}^n \times \mathbf{C}^n \to \mathbf{C}$ fort, so daß $L(x, y)$ bzgl. x $\mathbf{C}$-linear ist und bzgl. y $\mathbf{R}$-linear.*
2. *Für $u, v \in \Lambda$ ist*
$$L(u, v) \equiv L(v, u) \bmod \mathbf{Z},$$
d.h. $L(u, v) - L(v, u) \in \mathbf{Z}$.
3. *Für $u, v \in \Lambda$ gilt:*
$$J(u + v) \equiv J(u) + J(v) + L(u, v) \bmod \mathbf{Z}.$$

Beweis: Wir berechnen für $u, v \in \Lambda$:

$$\begin{aligned} f(x+u+v) &= f(x)e^{2\pi i[L(x,u+v)+J(u+v)]} = \\ &= f(x+u)e^{2\pi i[L(x+u,v)+J(v)]} = \\ &= f(x)e^{2\pi i[L(x,u)+J(u)+L(x+u,v)+J(v)]} = \\ &= f(x)e^{2\pi i[L(x,u)+L(x,v)+L(u,v)+J(u)+J(v)]}. \end{aligned}$$

Mit dem Identitätssatz folgt sofort

$$L(x, u + v) + J(u + v) \equiv L(x, u) + L(x, v) + L(u, v) + J(u) + J(v) \bmod \mathbf{Z}.$$

Da $L(x, u)$ linear in x, also stetig ist, gibt es $a_{uv} \in \mathbf{Z}$ mit

$$L(x, u + v) - L(x, u) - L(x, v) = L(u, v) + J(u) + J(v) - J(u + v) + a_{uv}.$$

Setzt man bei festen u, v $x = 0$ ein, so folgt, daß die rechte Seite 0 ist, also erhält man

$$L(x, u + v) = L(x, u) + L(v).$$

Ist jetzt $u_1, \ldots, u_{2n}$ eine Basis von Λ, so definieren wir für $x, y \in V$ mit $y = \lambda_1 u_1 + \cdots + \lambda_{2n} u_{2n}$ und $\lambda_i \in \mathbf{R}$:

$$L(x, y) = L(x, \lambda_1 u_1 + \cdots + \lambda_{2n} u_{2n}) = \lambda_1 L(x, u_1) + \cdots + \lambda_{2n} L(x, u_{2n}).$$

Dann ist klar, daß das neue L die Behauptung erfüllt.
Obige Gleichung wird jetzt zu

$$L(u, v) = J(u + v) - J(u) - J(v) - a_{uv}.$$

Damit ist

$$L(u, v) + a_{uv} = L(v, u) + a_{vu},$$

also

$$L(u, v) \equiv L(v, u) \bmod \mathbf{Z}.$$

Der Rest ist nun klar. ■

SATZ 6. *Definiert man*

$$E(x, y) = L(x, y) - L(y, x),$$

so erfüllt E die Eigenschaften:

1. *$E(x, y)$ ist $\mathbf{R}$-bilinear.*
2. *$E(x, y)$ ist alternierend, d.h. $E(x, y) = -E(y, x)$.*
3. *$E(x, y)$ ist reellwertig, d.h. $E(x, y) \in \mathbf{R}$.*
4. *$E(ix, iy) = E(x, y)$.*
5. *$E(ix, y) = E(iy, x)$, d.h. $(x, y) \mapsto E(ix, y)$ ist eine reelle symmetrische Bilinearform.*
6. *$E(u, v) \in \mathbf{Z}$ für alle $u, v \in \Lambda$, d.h. E nimmt ganzzahlige Werte auf dem Gitter an.*

Beweis:

1.: Dies folgt daraus, daß L in beiden Argumenten $\mathbf{R}$-linear ist.
2.: Dies folgt sofort aus der Definition.
6.: Folgt aus $L(u, v) - L(v, u) \in \mathbf{Z}$ für $u, v \in \Lambda$.

3.: Folgt aus 6., da E $\mathbf{R}$-bilinear ist und Λ den Vektorraum V über $\mathbf{R}$ erzeugt.
4. und 5.:

$$\begin{aligned} E(ix,iy)-E(x,y) &= [L(ix,iy)-L(iy,ix)]-[L(x,y)-L(y,x)] = \\ &= [iL(x,iy)-iL(y,ix)]-[-iL(ix,y)+iL(iy,x)] = \\ &= i[L(ix,y)-L(y,ix)]+i[L(x,iy)-L(iy,x)] = \\ &= i[E(ix,y)+E(x,iy)] \end{aligned}$$

Da E reellwertig ist, müssen beide Seiten identisch 0 sein, also folgt $E(ix,iy) = E(x,y)$ und $E(ix,y) = -E(x,iy) = E(iy,x)$. ■

SATZ 7. *Setzt man mit den Bezeichnungen von eben*

$$H(x,y) = E(ix,y) + iE(x,y),$$

so gilt:

1. *H ist hermitesch, d.h. H ist $\mathbf{R}$-bilinear und außerdem gilt*

$$H(ix,y) = iH(x,y), \quad H(y,x) = \overline{H(x,y)}, \quad H(x,iy) = -iH(x,y).$$

2. *$E(ix,y)$ ist der Realteil von H.*

Beweis: Die zweite Eigenschaft ist klar.

$$\begin{aligned} H(y,x) &= E(iy,x)+iE(y,x) = E(ix,y)-iE(x,y) = \overline{H(x,y)}, \\ H(ix,y) &= E(-x,y)+iE(ix,y) = i[E(ix,y)+iE(x,y)] = iH(x,y). \end{aligned}$$

Damit folgt die Behauptung. ■

4. Äquivalenz von Thetafunktionen

DEFINITION 6. *Zwei Thetafunktionen f und f' heißen äquivalent, wenn es eine symmetrische komplexe Matrix A, eine $\mathbf{C}$-Linearform b und $c \in \mathbf{C}$ gibt mit*

$$f' = fe^{2\pi i[\frac{1}{2}x^tAx+b(x)+c]},$$

d.h. wenn sich f' und f multiplikativ um eine triviale Thetafunktion unterscheiden.

Hat f Typ (L,J), f' Typ (L',J'), so gilt

$$L'(x,y) = L(x,y)+x^tAy, \quad J'(u) = J(u)+\frac{1}{2}u^tAu+b(u) \bmod \mathbf{Z}.$$

Insbesondere liefert die Multiplikation mit

$$g = e^{2\pi i[\frac{1}{2}x^tAx+b(x)+c}$$

einen Isomorphismus von $\mathbf{C}$-Vektorräumen

$$Th(L,J) \simeq Th(L',J').$$

Weiter gilt:

$$E'(x,y) = L'(x,y)-L'(y,x) = L(x,y)+x^tAy-L(y,x)-y^tAx = E(x,y),$$

da A symmetrisch ist. Also ist die alternierende Form E eine Invariante der Äquivalenzklasse.

Unser Ziel ist es jetzt, in jeder Äquivalenzklasse von Thetafunktionen eine *normalisierte* auszuzeichnen.

LEMMA 2. *Ist f eine Thetafunktion vom Typ (L,J), so gibt es eine dazu äquivalente vom Typ $(\frac{1}{2i}H,J')$.*

Beweis: Wegen

$$E(ix,y) = E(iy,x), \quad E(x,y) = -E(y,x), \quad H(x,y) = E(ix,y) + iE(x,y)$$

gilt

$$\frac{1}{2i}H(x,y) - \frac{1}{2i}H(y,x) = E(x,y).$$

Daher ist

$$\frac{1}{2i}H(x,y) - L(x,y)$$

symmetrisch, d.h. es gibt eine symmetrische komplexe Matrix A mit

$$\frac{1}{2i}H(x,y) - L(x,y) = x^t Ay.$$

Mit der trivialen Thetafunktion $g = e^{2\pi i[\frac{1}{2}x^t Ax]}$ erhält man dann die gewünschte Transformation. ■

Um J zu normalisieren, führen wir noch eine Größe ein:

LEMMA 3. *Definiert man $K : \Lambda \to \mathbf{C}$ durch*

$$J(u) = K(u) + \frac{1}{2}L(u,u),$$

so gilt

$$K(u+v) \equiv K(u) + K(v) + \frac{1}{2}E(u,v) \bmod \mathbf{Z}.$$

Beweis: Dies folgt sofort aus

$$K(u+v) + \frac{1}{2}L(u+v,u+v) \equiv K(u) + \frac{1}{2}L(u,u) + K(v) + \frac{1}{2}L(v,v) + L(u,v) \bmod \mathbf{Z}.$$■

LEMMA 4. *Ist f eine Thetafunktion vom Typ (L,J), so gibt es eine dazu äquivalente vom Typ $(L, \frac{1}{2}L(u,u)+K(u))$, so daß $K : \Lambda \to \mathbf{C}$ reellwertig ist.*

Beweis: Sei $K(u) = J(u) - \frac{1}{2}L(u,u)$. Sei $u_1, \ldots, u_{2n}$ eine Gitterbasis von Λ. Wir defineren eine $\mathbf{R}$-Linearform $g : \mathbf{C}^n \to \mathbf{R}$ durch

$$g(u_1) = ImK(u_1), \ldots, g(u_{2n}) = ImK(u_{2n}).$$

Wegen

$$K(u+v) \equiv K(u) + K(v) + \frac{1}{2}E(u,v) \bmod \mathbf{Z}$$

gilt

$$ImK(u+v) = ImK(u) + ImK(v)$$

und damit

$$g(u) = ImK(u)$$

Sei jetzt

$$b(x) = g(ix) + ig(x).$$

Dann ist b $\mathbf{R}$-linear und es gilt:

$$b(ix) = g(-x) + ig(ix) = i^2 g(x) + ig(ix) = ib(x),$$

also ist b sogar $\mathbf{C}$-linear. Ändern wir um die triviale Thetafunktion $e^{2\pi i[-b(x)]}$ ab, so gilt jetzt $ImK(u) = 0$ für alle $u \in \Lambda$. ■

Normalisieren wir zuerst L, dann J mit den entsprechenden Lemmatas, so erhalten wir den ersten Teil des folgendes Satzes:

SATZ 8. *Jede Thetafunktion ist äquivalent zu einer Thetafunktion vom Typ $(\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u)+K(u))$, wo K reellwertig ist. Solche Thetafunktion heißen normalisiert. Die Transformationformel hat die Gestalt*

$$f(x+u) = f(x)e^{2\pi i[\frac{1}{2i}H(x,u)+\frac{1}{4i}H(u,u)+K(u)]}.$$

Bis auf eine Konstante ist in jeder Äquivalenzklasse von Thetafunktionen genau eine normalisierte.

Beweis: Bis auf die Eindeutigkeit ist alles klar. Seien f und f' zwei äquivalente normalisierte Thetafunktionen vom Typ

$$(\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u)+K(u)) \quad \text{und} \quad (\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u)+K'(u)),$$

wo K und K' reellwertig sind. Sei

$$f' = fe^{2\pi i[\frac{1}{2}x^tAx+b(x)+c]}$$

mit einer komplexen symmetrischen Matrix A, einer $\mathbf{C}$-Linearform b und einer komplexen Zahl c. Dann gilt

$$\frac{1}{2i}H(x,y) = \frac{1}{2i}H(x,y) + x^tAy \text{ und } \frac{1}{4i}H(u,u)+K(u) \equiv \frac{1}{4i}H(u,u)+K'(u)+\frac{1}{2}u^tAu+b(u) \bmod \mathbf{Z}.$$

Zunächst folgt $A=0$ und dann $K(u) \equiv K'(u)+b(u) \bmod \mathbf{Z}$, d.h. $K(u)-K'(u)-b(u) \in \mathbf{Z}$. Da sowohl K als auch K' reellwertig ist, folgt $b(u) \in \Lambda$ für alle $u \in \Lambda$. Da aber Λ eine $\mathbf{C}$-Basis von $\mathbf{C}^n$ enthält und b $\mathbf{C}$-linear ist, folgt $u(x) \in \mathbf{R}$ für alle $x \in \mathbf{C}^n$. Zusammen mit $b(ix) = ib(x) \in \mathbf{R}$ liefert dies $b=0$, also bleibt von der trivialen Thetafunktion nur $e^{2\pi ic}$ übrig. Damit folgt die Behauptung. ■

Wir wollen dies gleich anwenden, um weitere Einschränkungen an E zu erhalten.

SATZ 9. *Sei f eine normalisierte Thetafunktion. Dann gilt:*

1. *Es gibt eine Zahl $C>0$, so daß für alle $x \in \mathbf{C}^n$ gilt:*
$$|f(x)| \le Ce^{\frac{\pi}{2}H(x,x)}.$$
2. *Die reelle symmetrische Form $E(ix,y)$ ist positiv semidefinit, d.h. $E(ix,x) \ge 0$ für alle $x \in \mathbf{C}^n$. Also ist auch die hermitesche Form $H(x,y)$ positiv semidefinit.*

Beweis:

1. Wir definieren
$$g(x) = f(x)e^{-\frac{\pi}{2}H(x,x)}$$
und erhalten bei Translation um $u \in \Lambda$:
$$\begin{aligned} g(x+u) &= f(x+u)e^{-\frac{\pi}{2}H(x+u,x+u)} = \\ &= f(x)e^{\pi H(x,u)+\frac{\pi}{2}H(u,u)+2\pi iK(u)-\frac{\pi}{2}[H(x,x)+H(x,u)+H(u,x)+H(u,u)]} = \\ &= g(x)e^{2\pi iK(u)}e^{\frac{\pi}{2}[2H(x,u)-H(x,u)-H(u,x)]} = \\ &= g(x)e^{2\pi iK(u)}e^{\frac{\pi}{2}[2iE(x,u)]} = \\ &= g(x)e^{2\pi i[K(u)+\frac{1}{2}E(x,u)]} \end{aligned}$$
Da sowohl E als auch K reellwertig ist, folgt
$$|g(x+u)| = |g(x)|,$$
also ist $|g|$ Λ-periodisch und damit nach oben beschränkt durch eine Konstante C. Da $H(x,x) \in \mathbf{R}$ gilt, folgt die erste Behauptung.
2. Angenommen, $E(ix_0,x_0) < 0$ für ein $x_0 \in \mathbf{C}^n$. Wir betrachten die holomorphe Funktion einer komplexen Veränderlichen
$$z \mapsto f(zx_0).$$
Für diese gilt die Abschätzung
$$|f(zx_0)| \le Ce^{\frac{\pi}{2}|z|^2H(x_0,x_0)} = Ce^{\frac{\pi}{2}|z|^2E(ix_0,x_0)}.$$
Die Funktion $z \mapsto f(zx_0)$ ist also beschränkt und damit konstant. Da sie für $z \to \infty$ gegen 0 konvergiert, ist sie 0, insbesondere $f(x_0)=0$. Nun ist $E(ix,x)<0$ eine offene Bedingung. Also gilt auf einer offenen Menge $f(x)=0$, also $f=0$, ein Widerspruch. ■

Die hergeleiteten Eigenschaften der einer Thetafunktion zugeordneten Form E fassen wir jetzt zusammen und definieren:

DEFINITION 7. *Eine Riemannsche Form E auf $\mathbf{C}^n$ bzgl. eines Gitters Λ ist eine Abbildung $\mathbf{R}$-Bilinearform $E : \mathbf{C}^n \times \mathbf{C}^n \to \mathbf{R}$, für die gilt:*

1. *E ist alternierend,*
2. *$E(u,v) \in \mathbf{Z}$ für alle $u, v \in \Lambda$,*
3. *$(x,y) \mapsto E(ix,y)$ ist symmetrisch und positiv semidefinit.*

Beispiel: Wir betrachten $\Lambda = \mathbf{Z} + \mathbf{Z}i \subseteq \mathbf{C}$. Wir bescheiben alles bzgl. der Gitterbasis $u_1 = 1, u_2 = i$, die auch $\mathbf{R}$-Basis von $\mathbf{C}$ ist. Wir wollen alle Riemannschen Formen bzgl. Λ bestimmen. Wir müssen ansetzen $E(x,y) = x^t \tilde{E} y$ mit

$$\tilde{E} = \begin{pmatrix} 0 & m \\ -m & 0 \end{pmatrix}$$

und $m \in \mathbf{Z}$. Wegen $iu_1 = u_2, iu_2 = -u_1$ wird die Multiplikation mit i durch die Matrix

$$I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

beschrieben. Wegen $E(ix,y) = E(Ix,y) = x^t I^t \tilde{E} y$ muß die Matrix $I^t \tilde{E}$ symmetrisch und positiv semidefinit sein. Nun ist

$$I^t \tilde{E} = \begin{pmatrix} -m & 0 \\ 0 & -m \end{pmatrix},$$

also haben wir genau für $m \leq 0$ eine Riemannsche Form.

Beispiel: Sei $\Lambda \subseteq \mathbf{C}^2$ gegeben durch die Periodenmatrix

$$\begin{pmatrix} 1 & i & 0 & \sqrt{2}i \\ 0 & 0 & 1 & \sqrt{3}+i \end{pmatrix},$$

wobei die 4 Spalten mit $u_1, \ldots, u_4$ bezeichnet werden. Wir berechnen alles bzgl. $u_1, \ldots, u_4$. E wird beschreiben durch eine Matrix

$$\tilde{E} = \begin{pmatrix} 0 & u & v & w \\ -u & 0 & x & y \\ -v & -x & 0 & z \\ -w & -y & -z & 0 \end{pmatrix}$$

mit $u, v, w, x, y, z \in \mathbf{Z}$. Wegen

$$\begin{aligned} iu_1 &= u_2, \\ iu_2 &= -u_1, \\ iu_3 &= -\sqrt{2}u_2 - \sqrt{3}u_3 + u_4, \\ iu_4 &= -\sqrt{2}u_1 - \sqrt{6}u_2 - 4u_3 + \sqrt{3}u_4 \end{aligned}$$

wird die Multiplikation mit i durch die Matrix

$$I = \begin{pmatrix} 0 & -1 & 0 & -\sqrt{2} \\ 1 & 0 & -\sqrt{2} & -\sqrt{6} \\ 0 & 0 & -\sqrt{3} & -4 \\ 0 & 0 & 1 & \sqrt{3} \end{pmatrix}$$

beschrieben. Nun ist

$$I^t \tilde{E} = \begin{pmatrix} -u & 0 & x & y \\ 0 & -u & -v & -w \\ \sqrt{2}u + \sqrt{3}v - w & \sqrt{3}x - y & -\sqrt{2}x - z & -\sqrt{2}y - \sqrt{3}z \\ \sqrt{6}u + 4v - \sqrt{3}w & -\sqrt{2}u + 4x - \sqrt{3}y & -\sqrt{2}v - \sqrt{6}x - \sqrt{3}z & -\sqrt{2}w - \sqrt{6}y - 4z \end{pmatrix}.$$

Die Symmetriebedingung liefert $u = v = w = x = y = 0$, übrig bleibt

$$t^t \tilde{E} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -z & \sqrt{3}z \\ 0 & 0 & -\sqrt{3}z & -4z \end{pmatrix},$$

also haben wir für $z \leq 0$ eine Riemannsche Form.

5. Alternierende Formen

Jeder Thetafunktion F ist eine alternierende Form E zugeordnet, die wir jetzt noch genauer untersuchen wollen.

SATZ 10. *Sei Λ ein freier endlich erzeugter $\mathbf{Z}$-Modul, d.h. $\Lambda \simeq \mathbf{Z}^r$, und $E : \Lambda \times \Lambda \to \mathbf{Z}$ eine alternierende Bilinearform. Dann gibt es eine Zerlegung*

$$\Lambda = \mathbf{Z}e_1 \oplus \mathbf{Z}f_1 \oplus \cdots \oplus \mathbf{Z}e_s \oplus \mathbf{Z}f_s \oplus \Lambda_0$$

und natürliche Zahlen $d_1, \ldots, d_s$ mit $d_1|d_2|\ldots|d_s$, so daß gilt:

$$E(e_i, e_j) = E(f_i, f_j) = 0, \quad E(e_i, f_j) = 0 \text{ für } i \neq j, \quad E(e_i, f_i) = d_i, \quad E(x, y) = 0 \text{ für } x \in \Lambda_0.$$

Weiter gilt

$$\Lambda_0 = \{x \in \Lambda : E(x, y) = 0 \text{ für alle } y \in \Lambda\}.$$

Wählt man noch eine Basis $g_1, \ldots, g_t$ von Λ_0, so hat E bzgl. $e_1, f_1, \ldots, e_s, f_s, g_1, \ldots, g_t$ die Matrixdarstellung

$$M = \begin{pmatrix} M_1 & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & \ldots & M_s & 0 \\ 0 & \ldots & 0 & 0 \end{pmatrix} \quad \text{mit} \quad M_i = \begin{pmatrix} 0 & d_i \\ -d_i & 0 \end{pmatrix}.$$

Eine solche Zerlegung nennen wir auch Frobeniuszerlegung von E. Das Produkt $d_1 \ldots d_s$ heißt die reduzierte Pfaffsche von E, im Fall $2s = r$ die Pfaffsche $pf(E)$ von E.

Beweis:

1. (a) Wir setzen $\Lambda_1 = \Lambda$ und konstruieren wie folgt induktiv freie $\mathbf{Z}$-Moduln Λ_i.
   (b) Verschwindet E auf Λ_i, so setzen wir $\Lambda_0 = \Lambda_i$ und hören auf.
   (c) Sei d_i die kleinste ganze Zahl > 0, die E auf Λ_i annimmt, und $e_i, f_i \in \Lambda_i$ mit $E(e_i, f_i) = d_i$.
   (d) Es gilt $E(e_i, \Lambda_i) \subseteq \mathbf{Z}d_i$ und $E(\Lambda_i, f_i) \subseteq \mathbf{Z}d_i$.
   (e) Wir definieren jetzt

   $$\Lambda_{i+1} = \{x \in \Lambda_i : E(x, e_i) = E(x, f_i) = 0\}.$$

   Es gilt

   $$(\mathbf{Z}e_i + \mathbf{Z}f_i) \cap \Lambda_{i+1} = 0.$$

   Sei $x \in \Lambda_i$. Wegen $d_i|E(x, e_i)$ und $d_i|E(x, f_i)$ sieht man schnell, daß

   $$x - \frac{E(x, f_i)}{d_i} e_i + \frac{E(x, e_i)}{d_i} f_i \in \Lambda_{i+1}$$

   gilt. Damit folgt

   $$\Lambda_i = \mathbf{Z}e_i \oplus \mathbf{Z}f_i \oplus \Lambda_{i+1}.$$

   (f) Jetzt geht man zurück zu (b).
2. Betrachtet man

   $$E(e_i + e_{i+1}, -af_i + f_{i+1}) = -ad_i + d_{i+1},$$

   so findet man $a \in \mathbf{Z}$ mit $0 \leq -ad_i + d_{i+1} \leq d_i - 1$. Da dies ein Wert ist, der von E auf Λ_i angenommen wird, folgt $d_{i+1} = ad_i$. Damit gilt $d_i|d_{i+1}$.
3. Wir erhalten also eine Zerlegung

   $$\Lambda = \mathbf{Z}e_1 \oplus \mathbf{Z}f_1 \oplus \ldots \mathbf{Z}e_s \oplus \mathbf{Z}f_s \oplus \Lambda_0,$$

   wobei $E(e_i, f_i) = d_i$ gilt, die anderen Produkte 0 sind. Außerdem verschwindet E auf Λ_0. Dazu gilt noch

   $$d_1|d_2|\ldots|d_s.$$

4. Es ist jetzt klar, daß man eine Matrizendarstellung wie angegeben erhält. Daraus folgt auch die Darstellung von Λ_0. ■

Bemerkungen:

1. Ist K ein Körper der Charakteristik $\neq 0$ und A eine schiefsymmetrische $n \times n$-Matrix, so ist
$$(x, y) \mapsto x^t A y$$
eine alternierende Form. Wie eben findet man eine Transformationsmatrix T, so daß gilt:
$$T^t A T = \begin{pmatrix} M & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots \\ 0 & \dots & M & 0 \\ 0 & \dots & 0 & 0 \end{pmatrix} \quad \text{mit} \quad M = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$
Man sieht daraus sofort: Ist n ungerade, so ist $\det A = 0$. Ist n gerade und $\det A \neq 0$, so ist $\det A = (\det T)^2$.
2. Sei jetzt n gerade und für $1 \leq i < j \leq n$ seien Unbestimmte x_{ij} gegeben und $x_{ji} = -x_{ij}$. Wir betrachten die Matrix $X = (x_{ij})$ (über $\mathbf{Z}$). Natürlich muß gelten $\det X \neq 0$. Über $K = \mathbf{Q}(x_{ij})$ kann man die schiefsymmetrische Matrix X wieder auf Normalform bringen, also gibt es $f, g \in \mathbf{Z}[x_{ij}]$ mit $\det X = (\frac{f}{g})^2$. Da $\mathbf{Z}[x_{ij}]$ faktoriell ist, ist $\det X$ selbst schon ein Quadrat eines Polynoms $\in \mathbf{Z}[x_{ij}]$. Wir schreiben
$$\det X = pf(X)^2,$$
wo $pf(X)$ so normiert ist, daß es auf obiger Normalform den Wert 1 annimmt. $pf(x_{ij})$ heißt Pfaffsches Polynom.

Ist E eine Riemannsche Form auf $\mathbf{C}^n$ bzgl. eines Gitters Λ, so definieren wir den Kern von E durch
$$Kern(E) = \{x \in \mathbf{C}^n : E(x, y) = 0 \text{ für alle } y \in \mathbf{C}^n\}.$$
Wählt man eine $\mathbf{R}$-Basis von $\mathbf{C}^n$, so wird E bzgl. dieser durch eine (schiefsymmetrische) reelle $2n \times 2n$-Matrix M beschrieben. Der Kern von E ist dann der Kern von M. Wir sagen E ist ausgeartet, falls $Kern(E) \neq 0$, sonst heißt E nichtausgeartet.

LEMMA 5. *Sei E eine Riemannsche Form auf $\mathbf{C}^n$ bzgl. eines Gitters Λ. Dann gilt:*
$$\begin{aligned} Kern(E) &= \{x \in \mathbf{C}^n : E(x, y) = 0 \textit{ für alle } y \in \mathbf{C}^n\} = \\ &= \{x \in \mathbf{C}^n : H(x, y) = 0 \textit{ für alle } y \in \mathbf{C}^n\} = \\ &= \{x \in \mathbf{C}^n : E(ix, x) = 0\} = \\ &= \{x \in \mathbf{C}^n : H(x, x) = 0\}. \end{aligned}$$
$Kern(E)$ ist ein $\mathbf{C}$-Untervektorraum.

Beweis: Wir bezeichnen die Mengen in den 4 Zeilen mit (1), (2), (3), (4).
(1) $\Rightarrow$ (3): klar. (3) $\iff$ (4): klar wegen $H(x, x) = E(ix, x)$.
(3) $\Rightarrow$ (1): Sei $E(ix, x) = 0$. Dann gilt für $y \in \mathbf{C}^n$ und $t \in \mathbf{R}$:
$$0 \leq E(i(y + tx), y + tx) = E(iy, y) - 2tE(x, iy).$$
Da $t \in \mathbf{R}$ beliebig gewählt werden kann, folgt $E(x, iy) = 0$. Da dies für alle $y \in \mathbf{C}^n$ gilt, folgt $x \in Kern(E)$.
(1) $\iff$ (2): Nun gilt für $x \in \mathbf{C}^n$:
$$\begin{aligned} x \in Kern(E) &\iff E(x, y) = 0 \text{ für alle } y \in \mathbf{C}^n \\ &\iff E(x, y) = -E(x, iy) = E(iy, x) = E(ix, y) = 0 \text{ für alle } y \in \mathbf{C}^n \\ &\iff H(x, y) = 0 \text{ für alle } y \in \mathbf{C}^n. \end{aligned}$$
Aus (2) folgt auch sofort, daß $Kern(E)$ ein $\mathbf{C}$-Vektorraum ist. Damit ist alles gezeigt. ■

Bemerkung: Man sieht jetzt sofort: Eine Riemannsche Form E ist genau dann nicht ausgeartet, wenn $(x, y) \mapsto E(ix, y)$ positiv definit ist, was gleichwertig damit ist, daß H positiv definit ist.

LEMMA 6. *Sei E eine Riemannsche Form bzgl. des Gitters $\Lambda \subseteq \mathbf{C}^n$ und*
$$\Lambda = \mathbf{Z}e_1 \oplus \mathbf{Z}f_1 \oplus \dots \oplus \mathbf{Z}e_m \oplus \mathbf{Z}f_m \oplus \Lambda_0$$
eine Frobeniuszerlegung. Dann gilt:

1. *Der von* Λ_0 *erzeugte* $\mathbf{R}$*-Vektorraum ist*
$$Kern(E) = \{x \in \mathbf{C}^n : E(x,y) = 0 \text{ für alle } y \in \mathbf{C}^n\},$$
also ein $\mathbf{C}$*-Vektorraum.*
2. *Wählt man eine* $\mathbf{C}$*-Basis* $e_{m+1}, \ldots, e_n$ *von* $Kern(E)$*, so ist* $e_1, \ldots, e_n$ *eine* $\mathbf{C}$*-Basis von* $\mathbf{C}^n$*.*

Beweis: 1. folgt sofort aus der Matrixdarstellung von E.
2. Angenommen, wir haben eine Relation
$$(a_1 + b_1 i)e_1 + \cdots + (a_n + ib_n) = 0$$
mit $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbf{R}$. Da mit $e_{m+1}, \ldots, e_n$ auch $ie_{m+1}, \ldots, ie_n$ in $Kern(E)$ liegen, gilt
$$\begin{aligned} E(i(b_1e_1 + \cdots + b_me_m), b_1e_1 + \cdots + b_me_m) &= E(i(b_1e_1 + \cdots + b_ne_n), b_1e_1 + \cdots + b_ne_n) \\ &= E(-(a_1e_1 + \cdots + a_ne_n), b_1e_1 + \cdots + b_ne_n) = 0, \end{aligned}$$
also $b_1e_1 + \cdots + b_me_m \in Kern(E)$. Da die Koeffizienten reell sind, folgt sofort $b_1 = \cdots = b_m = 0$. Dann folgt aber auch $a_1e_1 + \cdots + a_me_m \in Kern(E)$, was ebenso $a_1 = \cdots = a_m = 0$ liefert. Schließlich gibt dies $a_{m+1} + ib_{m+1} = \cdots = a_n + ib_n = 0$, d.h. $e_1, \ldots, e_n$ sind über $\mathbf{C}$ linear unabhängig. ■

6. Ausgeartete Thetafunktionen

Sei E eine ausgeartete Riemannsche Form auf $\mathbf{C}^n$ bzgl. eines Gitters Λ und
$$(\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u))$$
ein zugehöriger normalisierter Typ. Wir wählen eine Frobeniuszerlegung
$$\Lambda = \mathbf{Z}e_1 + \mathbf{Z}f_1 + \cdots + \mathbf{Z}e_m + \mathbf{Z}f_m + \Lambda_0 \quad \text{und } \Lambda_0 = \mathbf{Z}g_1 + \cdots + \mathbf{Z}g_{2n-2m}$$
und eine $\mathbf{C}$-Basis $e_{m+1}, \ldots, e_n$ von $Kern(E)$. Wir machen eine Koordinatenwechsel, so daß $e_1, \ldots, e_n$ die Einheitsvektoren sind. Sei $\phi : \mathbf{C}^n \to \mathbf{C}^m$ die Projektion auf die ersten m Koordinaten.

Behauptung: Ist $F \in Th(\frac{1}{2i}H, \frac{1}{4i}H(u,u) + K(u))$ eine normalisierte Thetafunktion, so gilt für alle $x_0 \in Kern(E)$ und alle $x \in \mathbf{C}^n$:
$$F(x) = F(x + x_0).$$

Beweis: Wir betrachten die holomorphe Funktion einer komplexen Veränderlichen
$$g(z) = F(x + zx_0).$$
Unsere Abschätzung liefert
$$|g(z)| \leq Ce^{\frac{\pi}{2}H(x+zx_0, x+zx_0)} = Ce^{\frac{\pi}{2}H(x,x)}.$$
Also ist $g(z)$ beschränkt, also konstant, also $g(0) = g(1)$, d.h.
$$F(x) = F(x + x_0). \quad ■$$

Damit wird durch
$$\tilde{F}(\phi(x)) = F(x) \text{ oder anders geschrieben } \tilde{F}(x_1, \ldots, x_m) = F(x_1, \ldots, x_n)$$
eine holomorphe Funktion auf $\mathbf{C}^m$ definiert. Wir wollen sehen, daß $\tilde{F}$ eine Thetafunktion ist.

Behauptung:
$$\tilde{\Lambda} = \mathbf{Z}\phi(e_1) + \mathbf{Z}\phi(f_1) + \cdots + \mathbf{Z}\phi(e_m) + \mathbf{Z}\phi(f_m)$$
ist ein Gitter in $\mathbf{C}^m$.

Beweis: Wir müssen zeigen, daß die obigen Vektoren linear unabhängig über $\mathbf{R}$ sind. Seien $r_1, s_1, \ldots, r_m, s_m \in \mathbf{R}$ mit
$$r_1\phi(e_1) + s_1\phi(f_1) + \cdots + r_m\phi(e_m) + s_m\phi(f_m) = 0,$$
also $r_1e_1 + s_1f_1 + \cdots + r_me_m + s_mf_m \in Kern(E)$. Dann gibt es $t_1, \ldots, t_{2n-2m} \in \mathbf{R}$ mit
$$r_1e_1 + s_1f_1 + \cdots + r_me_m + s_mf_m = t_1g_1 + \cdots + t_{2n-2m}g_{2n-2m},$$

was aber wegen der $\mathbf{R}$-linearen Unabhängigkeit von $e_1, f_1, \ldots, e_m, f_m, g_1, \ldots, g_{2n-2m}$ sofort $r_1 = s_1 = \cdots = r_m = s_m = 0$ liefert. ■

Behauptung: $\tilde{E}(\phi(x), \phi(y)) = E(x, y)$ definiert eine nichtausgeartete Riemannsche Form auf $\mathbf{C}^m$ bzgl. des Gitters $\tilde{\Lambda}$.

Beweis: $\tilde{E}$ ist wohldefiniert, nimmt auf $\tilde{\Lambda}$ ganzzahlige Werte an und ist natürlich nicht entartet. ■

Genauso definiert man die hermitesche Form $\tilde{H}$:

$$\tilde{H}(\phi(x), \phi(y)) = H(x, y).$$

Behauptung: Für $u \in \Lambda_0$ ist $K(u) \in \mathbf{Z}$ und für $u, v \in \Lambda$ mit $u \equiv v \bmod \Lambda_0$ gilt

$$K(u) \equiv K(v) \bmod \mathbf{Z}.$$

Indem wir $K(u)$ geeignet um ganze Zahlen abändern, können wir also eine Funktion $\tilde{K} : \tilde{\Lambda} \to \mathbf{R}$ finden mit

$$K(u) = \tilde{K}(\phi(u)).$$

Beweis: Sei $u \in \Lambda_0$. Dann liefert die Transformationsformel

$$F(x) = F(x + u) = F(x) e^{2\pi i [\frac{1}{2i} H(x,u) + \frac{1}{4i} H(u,u) + K(u)]} = F(x) e^{2\pi i K(u)},$$

also $K(u) \in \mathbf{Z}$. Ist jetzt $u \in \Lambda_0$ und $v \in \Lambda$, so gilt

$$K(u + v) \equiv K(u) + K(v) + \frac{1}{2} E(u, v) = K(v) \bmod \mathbf{Z}. \quad ■$$

Damit folgt jetzt aber sofort folgender Satz:

LEMMA 7. *Mit den Bezeichnungen von eben gilt:*

$$Th(\frac{1}{2i}\tilde{H}(x,u), \frac{1}{4i}\tilde{H}(u,u) + \tilde{K}(u)) \to Th(\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u)), \quad \tilde{F} \mapsto \tilde{F} \circ \phi$$

ist ein Isomorphismus von $\mathbf{C}$*-Vektorräumen und* $\tilde{E}$ *ist nicht ausgeartet.*

Wir können uns im folgenden also auf nichtausgeartete Riemannsche Formen beschränken.

7. Konstruktion von Thetafunktionen

Wir wollen jetzt (L, J) vorgeben und dazu Thetafunktionen konstruieren.

DEFINITION 8. *Sei* Λ *ein Gitter in* $\mathbf{C}^n$*. Ein Paar* (L, J) *heißt ein Typ bzgl. des Gitters* Λ*, wenn gilt:*

1. $L : \mathbf{C}^n \times \mathbf{C}^n \to \mathbf{C}, (x, y) \mapsto L(x, y)$ *ist* $\mathbf{C}$*-linear in* x *und* $\mathbf{R}$*-linear in* y*,*
2. $E(x, y) = L(x, y) - L(y, x)$ *ist eine Riemannsche Form bzgl.* Λ*,*
3. $J : \Lambda \to \mathbf{C}$ *erfüllt*

$$J(u + v) \equiv J(u) + J(v) + L(u, v) \bmod \mathbf{Z} \quad \textit{für alle } u, v \in \Lambda.$$

Ist E *nichtausgeartet, so nennen wir auch* (L, J) *nichtausgeartet.*

LEMMA 8. *Sei* (L, J) *ein Typ bzgl. eines Gitters* Λ*,* $u_1, \ldots, u_{2n}$ *eine Gitterbasis und* $F \neq 0$ *eine holomorphe Funktion mit*

$$F(x + u_j) = F(x) e^{2\pi i [L(x, u_j) + J(u_j)]} \textit{ für } j = 1, \ldots, 2n,$$

so ist F *eine Thetafunktion vom Typ* (L, J).

Beweis: Wir müssen für $u \in \Lambda$ die Funktionen $F(x+u)$ und $F(x)$ miteinander vergleichen. Wir machen dies zunächst für $u = -u_j$: Setzt man in

$$F(x+u_j) = F(x)e^{2\pi i[L(x,u_j)+J(u_j)]}$$

statt x den Wert $x-u_j$ ein, so erhält man

$$\begin{aligned} F(x-u_j) &= F(x)e^{2\pi i[-L(x-u_j,u_j)-J(u_j)]} = \\ &= F(x)e^{2\pi i[[L(x,-u_j)+J(-u_j)]+[-J(u_j)-J(-u_j)-L(-u_j,u_j)]]} = \\ &= F(x)e^{2\pi i[[L(x,-u_j)+J(-u_j)]-J(0)]} = \\ &= F(x)e^{2\pi i[L(x,-u_j)+J(-u_j)]}. \end{aligned}$$

Setzt man nämlich in die Bedingungsgleichung für J den Wert $v=0$ ein, so erhält man

$$J(u) \equiv J(u) + J(0) + L(u,0) \equiv J(u) + J(0) \bmod \mathbf{Z},$$

was $J(0) \equiv 0$ liefert.
Wir zeigen jetzt: Gilt die Transformationsformel für $u \in \Lambda$, so auch für $u+u_j$ und für $u-u_j$. Dann sind wir durch Induktion fertig.

$$\begin{aligned} F(x+u+u_j) &= F(x+u)e^{2\pi i[L(x+u,u_j)+J(u_j)]} = \\ &= F(x)e^{2\pi i[L(x,u)+J(u)+L(x+u,u_j)+J(u_j)]} = \\ &= F(x)e^{2\pi i[[L(x,u+u_j)+J(u+u_j)]+[-J(u+u_j)+J(u)+L(u,u_j)+J(u_j)]} = \\ &= F(x)e^{2\pi i[L(x,u+u_j)+J(u+u_j)]}. \end{aligned}$$

$$\begin{aligned} F(x+u-u_j) &= F(x+u)e^{2\pi i[L(x+u,-u_j)+J(-u_j)]} = \\ &= F(x)e^{2\pi i[L(x,u)+J(u)+L(x+u,-u_j)+J(-u_j)]} = \\ &= F(x)e^{2\pi i[[L(x,u-u_j)+J(u-u_j)]+[-J(u-u_j)+J(u)-L(u,u_j)+J(-u_j)]} = \\ &= F(x)e^{2\pi i[L(x,u-u_j)+J(u-u_j)]}. \end{aligned}$$

Damit folgt die Behauptung. ■

LEMMA 9. *Sei (L,J) ein nichtausgearteter Typ bzgl. des Gitters $\Lambda \subseteq \mathbf{C}^n$ und $e_1, f_1, \ldots, e_n, f_n$ eine Frobeniusbasis von Λ. Dann gilt:*

1. *$e_1, \ldots, e_n$ ist eine $\mathbf{C}$-Basis von $\mathbf{C}^n$, also können wir nach Koordinatenwechsel annehmen, daß $e_1, \ldots, e_n$ die Einheitsvektoren sind, d.h. jedes $x \in \mathbf{C}^n$ hat die Darstellung*
$$x = (x_1, \ldots, x_n)^t = x_1e_1 + \cdots + x_ne_n \text{ mit } x_i \in \mathbf{C}.$$
2. *Es einen äquivalenten Typ, für den gilt*
$$L(x,e_i) = 0 \text{ und } J(e_i) = 0 \text{ für } i = 1, \ldots, n.$$
Sei (L,J) jetzt so angenommen.
3. *Für $x = (x_1, \ldots, x_n)^t \in \mathbf{C}^n$ gilt:*
$$L(x,f_j) = d_jx_j = d_je_j^tx.$$
4. *Die Matrix*
$$M = (\frac{f_1}{d_1}, \ldots, \frac{f_n}{d_n})$$
ist symmetrisch, d.h. schreibt man $f_j = f_{1j}e_1 + \cdots + f_{nj}e_n$, so gilt
$$\frac{f_{jk}}{d_k} = \frac{f_{kj}}{d_j}.$$
5. *Die symmetrische reelle Matrix $Im(M)$ ist negativ definit.*

Beweis:

1. Wurde bereits bewiesen.

2. Wegen $E(x,y) = L(x,y) - L(y,x)$ und $E(e_i,e_j) = 0$ gilt $L(e_i,e_j) = L(e_j,e_i)$. Daher findet man eine symmetrische komplexe Matrix A mit $e_i^t A e_j = L(e_i,e_j)$. Daher gilt

$$L(e_i,e_j) - e_i^t A e_j = 0.$$

Da L $\mathbf{C}$-linear im ersten Eintrag ist, folgt

$$L(x,e_j) - x^t A e_j = 0 \text{ für alle } x \in \mathbf{C}^n.$$

Nach Translation um A können wir jetzt also

$$L(x,e_i) = 0 \text{ für alle } x \in \mathbf{C}^n$$

voraussetzen. Wir wählen jetzt eine $\mathbf{C}$-Linearform $b(x)$ mit $b(e_i) = J(e_i)$. Dann gilt $(J-b)(e_i) = 0$. Ersetzen wir J durch $J-b$, so erhalten wir $J(e_i) = 0$, was wir haben wollten.

3.
$$\begin{aligned} L(x,f_j) &= x_1 L(e_1,f_j) + \cdots + x_n L(e_n,f_j) = \\ &= x_1(E(e_1,f_j) + L(f_j,e_1)) + \cdots + x_n(E(e_n,f_j) + L(f_j,e_n)) = \\ &= x_1 E(e_1,f_j) + \cdots + x_n E(e_n,f_j) = x_j E(e_j,f_j) = d_j x_j = \\ &= d_j e_j^t x. \end{aligned}$$

4. Es gilt
$$d_k f_{kj} = L(f_j,f_k) = E(f_j,f_k) + L(f_k,f_j) = L(f_k,f_j) = d_j f_{jk},$$
woraus die Aussage folgt.

5. Sei $m = (m_1,\ldots,m_n)^t \in \mathbf{R}^n$ und $m \neq 0$. Dann gilt:
$$\begin{aligned} m^t M m &= \sum m_j m_k \frac{f_{kj}}{d_j} = \sum \frac{m_j m_k}{d_j d_k} d_k f_{kj} = \\ &= \sum \frac{m_j m_k}{d_j d_k} L(f_j,f_k) = \\ &= L(\sum \frac{m_j}{d_j} f_j, \sum \frac{m_k}{d_k} f_k) \end{aligned}$$

Sei jetzt
$$w = \sum \frac{m_j}{d_j} f_j = x + iy \text{ mit } x,y \in \mathbf{R}e_1 + \cdots + \mathbf{R}e_n.$$

Dann ist $y \neq 0$ und es gilt
$$\begin{aligned} L(w,w) &= L(x+iy,w) = L(x,w) + iL(y,w) = \\ &= [E(x,w) + L(w,x)] + iL(y,x+iy) = \\ &= E(x,w) + i[L(y,x) + L(y,iy)] = E(x,w) + iL(y,iy) = \\ &= E(x,w) + i[E(y,iy) + L(iy,y)] = E(x,w) - iE(iy,y). \end{aligned}$$

Damit folgt
$$\begin{aligned} Im(m^t A m) &= Im(L(w,w)) = \\ &= Im(E(x,w) - iE(iy,y)) = \\ &= -E(iy,y) < 0. \end{aligned}$$

Damit folgt die Behauptung. ■

SATZ 11 (Frobenius). *Sei (L,J) ein nichtausgearteter Typ bzgl. des Gitters $\Lambda \subseteq \mathbf{C}^n$ und E die zugehörige Riemannsche Form. Dann gilt:*

$$\dim_{\mathbf{C}} Th(L,J) = pf(E).$$

Genauer: Nimmt man die Bezeichnungen des letzten Lemmas, setzt man $b_j = -\frac{1}{2} f_{jj} + \frac{J(f_j)}{d_j}$ und $\Gamma = \mathbf{Z}d_1 e_1 + \cdots + \mathbf{Z}d_n e_n$, so bilden die Funktionen

$$F_{\tilde{m}} = \sum_{m \in \tilde{m} + \Gamma} e^{2\pi i[-\frac{1}{2} m^t M m + m^t(b+x)]}$$

eine Basis von $Th(L,J)$, wenn $\tilde{m}$ ein Repräsentatantensystem von $\mathbf{Z}^n/\Gamma$ durchläuft.

Beweis:

1. Sei jetzt alles so gewählt wie im letzten Lemma. Ist $F \in Th(L,J), F \neq 0$, so gilt $F(x+e_j) = F(x)$, also besitzt F eine Fourierreihenentwicklung:
$$F(x) = \sum_{m_1,\ldots,m_n \in \mathbf{Z}} a(m_1,\ldots,m_n) e^{2\pi i[m_1x_1+\cdots+m_nx_n]} = \sum_{m\in\mathbf{Z}^n} a(m) e^{2\pi i m^t x}.$$
Wir wollen jetzt die Bedingung
$$F(x+f_j) = F(x) e^{2\pi i[L(x,f_j)+J(f_j)]}$$
untersuchen. Schreiben wir noch $c_j = J(f_j)$, so gilt einerseits
$$F(x+f_j) = \sum_m a(m) e^{2\pi i m^t(x+f_j)} = \sum_m a(m) e^{2\pi i m^t f_j} e^{2\pi i m^t x},$$
andererseits
$$\begin{aligned} F(x)e^{2\pi i[L(x,f_j)+J(f_j)]} &= \sum_m a(m) e^{2\pi i m^t x} e^{2\pi i[d_j e_j^t x + c_j)]} = \\ &= \sum_m a(m) e^{2\pi i[(m+d_j e_j)^t x + c_j]} = \\ &= \sum_m a(m-d_j e_j) e^{2\pi i c_j} e^{2\pi i m^t x}. \end{aligned}$$
Vergleich der Fourierkoeffizienten liefert die Bedingung
$$a(m-d_je_j)e^{2\pi i c_j} = a(m) e^{2\pi i m^t f_j}.$$
Sei jetzt
$$Z_\Gamma = \{\tilde{m}_1 e_1 + \cdots + \tilde{m}_n e_n : 0 \leq \tilde{m}_j \leq d_j - 1, \tilde{m}_j \in \mathbf{Z}\}.$$
Kennt man $a(\tilde{m})$ für alle $\tilde{m} \in Z_\Gamma$, so sind dadurch alle $a(m)$ bestimmt. Die Abbildung
$$Th(L,J) \to Abb(Z_\Gamma, \mathbf{C}), \quad F \mapsto (a(\tilde{m}))$$
ist also $\mathbf{C}$-linear und injektiv, also
$$\dim_{\mathbf{C}} Th(L,J) \leq d_1 \ldots d_n.$$

2. Wir wollen jetzt umgekehrt Thetafunktionen konstruieren. Man kann dazu den Ansatz
$$a(m) = e^{2\pi i g(m)}, \quad g(m) = m^t A m + b^t m$$
(mit einer symmetrischen Matrix A) machen und eine Lösung für
$$a(m) e^{2\pi i m^t f_j} = a(m-d_je_j) e^{2\pi i c_j}$$
suchen. Dies führt auf folgende Funktionen: Wir definieren
$$F_{\tilde{m}} = \sum_{m \in \tilde{m}+\Gamma} e^{2\pi i[-\frac{1}{2}m^t M m + m^t(b+x)]}$$
Wir verschieben zunächst den Konvergenzbeweis. Die Fourierkoeffizienten sind
$$a(m) = e^{2\pi i[-\frac{1}{2}m^t M m + m^t b]} \text{ für } m \equiv \tilde{m} \bmod \Gamma, \quad a(m) = 0 \text{ sonst.}$$
Nun gilt für $m \equiv \tilde{m} \bmod \Gamma$:
$$\begin{aligned} \frac{a(m-d_je_j)e^{2\pi i c_j}}{a(m)e^{2\pi i m^t f_j}} &= e^{2\pi i[-\frac{1}{2}(m-d_je_j)^t M(m-d_je_j) + (m-d_je_j)^t b + c_j + \frac{1}{2}m^t M m - m^t b - m^t f_j]} = \\ &= e^{2\pi i[d_j m^t M m - \frac{1}{2}d_j^2 e_j T 6 M e_j - d_j e_j^t b + c_j - m^t f_j]} = \\ &= e^{2\pi i[m^t f_j - \frac{1}{2}d_j f_{jj} - d_j b_j + c_j - m^t f_j]} = \\ &= e^{2\pi i[-\frac{1}{2}d_j f_{jj} + c_j - d_j[-\frac{1}{2}f_{jj} + \frac{c_j}{d_j}]]} = \\ &= 1. \end{aligned}$$
Ist also die Konvergenz gezeigt, so ist $F_{\tilde{m}}$ eine Thetafunktion. Außerdem sind man an den Fourierkoeffizienten, daß
$$\{F_{\tilde{m}} : \tilde{m} \in Z_\Gamma\}$$

eine Menge von $d_1 \dots d_n$ $\mathbf{C}$-linear unabhängigen Thetafunktionen ist, womit schließlich $\dim_{\mathbf{C}} Th(L,J) = pf(E)$ folgt.

3. Wir wollen jetzt zeigen, daß die Reihe für $F_{\tilde{m}}$ lokal gleichmäßig und absolut konvergiert. Dann ist $F_{\tilde{m}}$ eine Thetafunktion.
Die Matrix $Im(M)$ ist negativ definiert, d.h. für alle $m \in \mathbf{R}^n \setminus \{0\}$ ist
$$\frac{m^t Im(M) m}{\sum m_j^2} < 0.$$
Da diese Funktion homogen in m vom Grad 0 ist, nimmt sie alle Werte schon auf der kompakten Sphere $\sum m_j^2 = 1$ an, also gibt es ein $c_1 > 0$ mit
$$\pi \frac{m^t Im(M) m}{\sum m_j^2} \leq -c_1.$$
Damit gilt
$$\pi m^t Im(M) m \leq -c_1 \sum m_j^2$$
und
$$e^{\pi Im(m^t M m)} \leq e^{-c_1 \sum m_j^2}$$
für alle $m \in \mathbf{Z}^n$.
Nun ergibt sich
$$a(m) e^{2\pi i m^t x} = e^{2\pi i [-\frac{1}{2} m^t M m + b^t m + x^t m]}$$
und damit
$$\begin{aligned} |a(m) e^{2\pi i m^t x}| &= e^{Re(2\pi i [-\frac{1}{2} m^t M n + b^t m + x^t m])} = \\ &= e^{\pi Im(m^t M m) - 2\pi m^t (Im(b) + Im(x))} \leq \\ &\leq e^{-c_1 \sum m_j^2 + 2\pi \max(|Im(b_j)| + |Im(x_j)|) \sum |m_j|}. \end{aligned}$$
Sei jetzt U eine beliebige (offene) beschränkte Teilmenge in $\mathbf{C}^n$. Dann gibt es ein $R > 0$ mit
$$2\pi(|Im(b_j)| + |Im(x_j)|) \leq R \text{ für } x \in U,$$
was die Abschätzung
$$|a(m) e^{2\pi i m^t M m}| \leq e^{-c_1 \sum m_j^2 + R \sum |m_j|}$$
ergibt. Dann gilt für jede endliche Menge $S \subseteq \mathbf{Z}^n$ und alle $x \in U$:
$$\begin{aligned} \sum_{m \in S} |a(m) e^{2\pi i m^t M m}| &\leq \sum_{m \in S} e^{-c_1 \sum m_j^2 + R \sum |m_j|} \leq \\ &\leq \sum_{m \in \mathbf{Z}^n} e^{-c_1 \sum m_j^2 + R \sum |m_j|} = \\ &= (\sum_{m \in \mathbf{Z}} e^{-c_1 m^2 + R|m|})^n = \\ &= (1 + 2 \sum_{m \geq 1} e^{-c_1 m^2 + Rm})^n < \infty. \end{aligned}$$
Also konvergiert $\sum_{m \in \mathbf{Z}^n} a(m) e^{2\pi i m^t M m}$ lokal gleichmäßig und absolut. Also ist $F_{\tilde{m}}$ eine holomorphe Funktion wie behauptet. ■

FOLGERUNG 2. *Ist (L,J) Typ bzgl. eines Gitters $\Lambda \subseteq \mathbf{C}^n$ und die zugehörige Riemannsche Form E ausgeartet, so hat $Th(L,J)$ die Dimension $pf_{red}(E)$.*

Beweis: Die wesentliche Arbeit wurde bereits im letzten Abschnitt geleistet. Wir hatten gesehen $Th(L,J) \simeq Th(\tilde{L}, \tilde{J})$, so daß $\tilde{E}$ nicht ausgeartet ist. Nach Konstruktion war $pf_{red}(E) = pf(\tilde{E})$. ■

Für spätere Anwendung brauchen wir noch einen Satz:

SATZ 12. *Sei (L,J) ein nichtausgearteter Typ bzgl. eines Gitters $\Lambda \subseteq \mathbf{C}^n$. Dann gibt es eine endliche Vereinigung V von echten Teilräumen von $Th(L,J)$, so daß gilt: Ist $F \in Th(L,J)$ auch Thetafunktion bzgl. eines Gitters $\Lambda' \supset \Lambda$, so ist $F \in V$.*

1. $F \in Th(L,J)$ sei auch Thetafunktion bzgl. eines Gitters $\Lambda' \supset \Lambda$ und habe bzgl. Λ' den Typ (L',J'). Da L und L' im zweiten Argument $\mathbf{R}$-linear ist, folgt sofort $L' = L$. Damit ist auch $E' = E$.
2. Es gibt eine Basis $u'_1, \ldots, u'_{2n}$ von Λ' und natürliche Zahlen $c_1, \ldots, c_{2n}$ mit $c_1 | \ldots | c_{2n}$, so daß $u_1 = c_1 u'_1, \ldots, u_{2n} = c_{2n} u'_{2n}$ eine Basis von Λ ist. Außerdem ist $c_{2n} > 1$. Man sieht weiter $c_{2n}\Lambda' \subseteq \Lambda$.
3. Wegen $E(u_j, u_k) = c_j c_k E(u'_j, u'_k)$ folgt für die Pfaffschen sofort
$$pf_\Lambda(E) = c_1 \ldots c_{2n} pf_{\Lambda'}(E).$$
Da alles natürliche Zahlen sind, folgt
$$c_{2n} | pf_\Lambda(E)$$
und damit $pf_\Lambda(E)\Lambda' \subseteq \Lambda$, also
$$\Lambda \subset \Lambda' \subseteq \frac{1}{pf_\Lambda(E)}\Lambda.$$
Es kommen also nur endliche viele Gitter Λ' in Frage.
4. Wegen $J'|\Lambda \equiv J \bmod \mathbf{Z}$ und der Funktionalgleichung gibt es auch nur endlich viele Möglichkeiten, J nach Λ' fortzusetzen. Also ist
$$F \in \cup \text{ endlich viele } {}_{\Lambda'} \text{ und } {}_{(L,J')} Th_{\Lambda'}(L,J') =: V.$$
5. Schließlich gilt noch
$$\dim_{\mathbf{C}} Th(L,J') = pf_{\Lambda'}(E) = \frac{pf_\Lambda(E)}{c_1 \ldots c_{2n}} < pf_\Lambda(E) = \dim_{\mathbf{C}} Th(L,J),$$
woraus die Behauptung folgt. ■

KAPITEL 2

Divisoren

Im folgenden bezeichnet Λ ein Gitter in $\mathbf{C}^n$ und $T = \mathbf{C}^n/\Lambda$ den zugehörigen Torus.
Sind F_1 und F_2 zwei Thetafunktionen vom Typ (L_1, J_1) und (L_2, J_2), so ist $\theta = \frac{F_1}{F_2}$ eine meromorphe Funktion, die sich wie

$$\theta(x+u) = \theta(x)e^{2\pi i[L(x,u)+J(u)]}$$

transformiert, wo

$$L = L_1 - L_2 \quad \text{und} \quad J = J_1 - J_2$$

ist. Wir nennen dies eine meromorphe Thetafunktion vom Typ (L, J). Das Paar (L, J) hat die üblichen Eigenschaften.
Ist θ eine meromorphe Thetafunktion vom Typ (L, J), so ist $E(x, y) = L(x, y) - L(y, x)$ eine reellwertige alternierende Form mit $E(\Lambda, \Lambda) \subseteq \mathbf{Z}$ und $E(ix, y) = E(iy, x)$.
Zwei meromorphe Thetafunktionen θ_1 und θ_2 heißen äquivalent, wenn sie sich um eine triviale Thetafunktion unterscheiden. Genauso wie früher sieht man, daß in jeder Äquivalenzklasse eine normalisierte Thetafunktion liegt.
Die meromorphen Thetafunktionen bilden eine Gruppe bzgl. der Multiplikation, die Äquivalenzrelation ist damit verträglich.

DEFINITION 9. *Eine Äquivalenzklasse von (meromorphen) Thetafunktionen heißt ein Divisor X bzgl. Λ oder auf $\mathbf{C}^n/\Lambda$. Der Divisor, der die meromorphe Thetafunktion θ enthält, wird mit (θ) bezeichnet. Die Menge aller Divisoren schreiben wir $Div(T) = Div(\mathbf{C}^n/\Lambda)$.*

Nach dem zuvor Gesagten ist $Div(T)$ eine abelsche Gruppe; wir schreiben sie additiv, d.h. $(\theta_1) + (\theta_2) = (\theta_1\theta_2)$. Das neutrale Element ist die Äquivalenzklasse der trivialen Thetafunktionen.
Wir wissen auch, daß sich jeder Divisor durch genau eine normalisierte meromorphe Thetafunktion repräsentieren läßt. Wir führen eine Ordnungsrelation auf $Div(T)$ ein:

DEFINITION 10. *Ein Divisor X heißt effektiv oder positiv, $X \geq 0$, falls $X = (\theta)$ mit einer holomorphen Thetafunktion gilt. Weiter setzt man für Divisoren X und Y:*

$$X \geq Y \quad \Longleftrightarrow \quad X - Y \geq 0.$$

Bemerkungen:

1. Jeder Divisor ist Differenz effektiver Divisoren.
2. Sind X und Y effektive Divisoren, so ist auch $X + Y$ effektiv.
3. Ist X ein effektiver Divisor und $X = (\theta)$, so ist

$$\{x \in T : \theta(x) = 0\}$$

unabhängig von θ definiert. Man kann sich daher X als Hyperfläche in T vorstellen.

Ist X ein Divisor und $X = (\theta)$, θ vom Typ (L, J) und $E(x, y) = L(x, y) - L(y, x)$ die zugehörige alternierende Form, so ist E unabhängig von der Wahl von θ und wir schreiben $E = E_X$. Ein effektiver Divisor heißt nichtausgeartet, falls E_X eine nichtausgeartete Riemannsche Form ist.

DEFINITION 11. *Eine abelsche Funktion f bzgl. Λ (oder auf $\mathbf{C}^n/\Lambda$) ist eine meromorphe Thetafunktion vom Typ $(0, 0)$.*

Eine abelsche Funktion ist also Λ-periodisch, kann also als Funktion auf T aufgefaßt werden. Die abelschen Funktionen zusammen mit 0 bilden einen Körper, den Funktionenkörper $\mathbf{C}(T)$.

DEFINITION 12. *Zwei Divisoren X und Y heißen linear äquivalent, $X \sim Y$, wenn es eine abelsche Funktion $f \neq 0$ gibt mit $Y = (f) + X$.*

Man kann dies auch anders ausdrücken: Ein Divisor einer abelschen Funktion heißt Hauptdivisor. Die Hauptdivisoren bilden eine Untergruppe $H(T)$ von $Div(T)$. Die Faktorgruppe $Div(T)/H(T)$ heißt die Picardgruppe $Pic(T)$ oder auch Klassengruppe von T. Die Klasse eines Divisors X schreiben wir als $cl(X)$. Es gilt dann also

$$X \sim Y \quad \Longleftrightarrow \quad cl(X) = cl(Y).$$

DEFINITION 13. *Für einen Divisor X definieren wir*

$$\mathcal{L}(X) = \{f \text{ abelsche Funktion mit } (f) + X \geq 0\} \cup \{0\}.$$

Sei $X = (\theta)$ effektiv, d.h. θ holomorph. Sei (L, J) der Typ von θ. Ist f abelsche Funktion mit $(f) + X \geq 0$, so ist $(f\theta) \geq 0$, d.h. $f\theta$ ist holomorph und natürlich vom Typ (L, J), also $f\theta \in Th(L, J)$. Ist umgekehrt $\theta' \in Th(L, J)$, so ist $f = \frac{\theta'}{\theta}$ eine abelsche Funktion und $(f) + X \geq 0$. Also haben wir eine Bijektion

$$Th(L, J) \to \mathcal{L}(X), \quad \theta' \mapsto \frac{\theta'}{\theta}.$$

Insbesondere ergibt sich damit sofort der folgende Satz:

SATZ 13. *Ist X ein effektiver Divisor, so ist $\mathcal{L}(X)$ ein $\mathbf{C}$-Vektorraum der Dimension*

$$\ell(X) = \dim_{\mathbf{C}}(\mathcal{L}(X)) = pf_{red}(E_X).$$

Genauer: Ist $X = (\theta)$, so ist

$$\mathcal{L}(X) = \{\frac{\theta'}{\theta} : \theta' \in Th(L, J)\}.$$

Sei X ein beliebiger Divisor. Ist $\mathcal{L}(X) = \{0\}$, so ist $\mathcal{L}(X)$ ein $\mathbf{C}$-Vektorraum. Sei jetzt $\mathcal{L}(X) \neq \{0\}$ und $f \in \mathcal{L}(X)$, $f \neq 0$. Dann ist $Y = (f) + X$ ein effektiver Divisor. Es gilt:

$$g \in \mathcal{L}(X) \iff (g) + X \geq 0 \iff (\frac{g}{f}) + (f) + X \geq 0 \iff g \in f\mathcal{L}(Y),$$

also

$$\mathcal{L}(X) = f\mathcal{L}(Y).$$

Damit ist auch $\mathcal{L}(X)$ ein $\mathbf{C}$-Vektorraum. Wir haben auch noch gesehen:

LEMMA 10. *Gilt $X \sim Y$, dann sind $\mathcal{L}(X)$ und $\mathcal{L}(Y)$ isomorph als $\mathbf{C}$-Vektorräume, insbesondere*

$$\ell(X) = \ell(Y),$$

d.h. $\ell(X) = \ell(cl(X))$.

SATZ 14 (Riemann-Roch). *Seien $X_0, \ldots, X_m$ effektive Divisoren und X_0 sei nicht ausgeartet. Dann gibt es Polynom P in $m+1$ Variablen, so daß für alle ganzen Zahlen $r_0, \ldots, r_m \geq 0$ mit $r_0 \geq 1$ gilt:*

$$\ell(r_0X_0 + \cdots + r_mX_m) = P(r_0, \ldots, r_m).$$

Ist X ein nichtausgearteter effektiver Divisor mit Riemannscher Form E, so gilt für alle natürlichen Zahlen $r \geq 1$:

$$\ell(rX) = r^n pf(E).$$

Beweis: Es gilt nach obigem Lemma

$$\ell(r_0X_0 + \cdots + r_mX_m) = pf_{red}(r_0E_{X_0} + \cdots + r_mE_{X_m}).$$

Nun ist aber $r_0E_{X_0} + \cdots + r_mE_{X_m}$ nichtausgeartet, da für $x \in \mathbf{C}^n, x \neq 0$ gilt

$$r_0E_{X_0}(ix, x) + \cdots + r_mE_{X_m}(ix, x) \geq r_0E_{X_0}(ix, x) > 0.$$

Also können wir oben pf_{red} durch pf ersetzen, was das Polynom $P(r_0, \ldots, r_m)$ liefert.
Ist X nichtausgearteter effektiver Divisor, so gilt für $r \geq 1$:

$$\ell(rX) = pf_{red}(rE) = pf(rE) = r^n pf(E). \quad \blacksquare$$

Wir wollen jetzt sehen, daß wir uns auf einen bestimmten Fall zurückziehen können.

Überlegungen:

1. Sind E_1 und E_2 zwei Riemannsche Formen auf $\mathbf{C}^n$ bzgl. eines Gitters Λ, so auch $E_1 + E_2$ und
$$Kern(E_1 + E_2) = Kern(E_1) \cap Kern(E_2).$$
Beweis: Daß E_j eine Riemannsche Form ist, bedeutet: E_j ist reellwertig, $\mathbf{R}$-bilinear, alternierend, nimmt auf Λ ganzzahlige Werte an, $(x, y) \mapsto E_j(ix, y)$ ist ist symmetrisch und positiv semidefinit. Damit ist auch klar, daß $E_1 + E_2$ eine Riemannsche Form ist. Für $x \in \mathbf{C}^n$ gilt
$$\begin{aligned} x \in Kern(E_1 + E_2) &\iff 0 = (E_1 + E_2)(ix, x) = E_1(ix, x) + E_2(ix, x) \\ &\iff E_1(ix, x) = E_2(ix, x) = 0 \\ &\iff x \in Kern(E_1) \cap Kern(E_2), \end{aligned}$$
da $E_j(ix, x) \geq 0$ gilt.
2. Daraus ergibt sich sofort die Aussage: Es gibt eine Riemannsche Form E_0 mit
$$\cap\{Kern(E) : E \text{ Riemannsche Form bzgl. } \Lambda\} = Kern(E_0).$$
3. Sei $\Lambda \subseteq \mathbf{C}^n$ ein Gitter, so daß alle Riemannschen Formen bzgl. Λ ausgeartet seien. Dann ist der Durchschnitt über alle Kerne ein komplexer Vektorraum $U \neq 0$.
4. Wie früher findet man eine Projektion $\phi : \mathbf{C}^n \to \mathbf{C}^m$ mit Kern U, so daß $\tilde{\Lambda} = \phi(\Lambda)$ ein Gitter in $\mathbf{C}^m$ ist, alle normalisierten Thetafunktionen bzgl. Λ von normalisierten Thetafunkionen bzgl. $\tilde{\Lambda}$ herkommen und auf $\mathbf{C}^m$ eine nichtausgeartete Riemannsche Form bzgl. $\tilde{\Lambda}$ existiert.
5. Insbesondere gilt für die Funktionenkörper
$$\mathbf{C}(\mathbf{C}^n/\Lambda) \simeq \mathbf{C}(\mathbf{C}^m/\tilde{\Lambda}).$$
6. Daher kann man sich auf den Fall zurückziehen, daß es eine nichtausgeartete Riemannsche Form bzgl. Λ gibt.

Jetzt können wir einen fundamentalen Begriff erwähnen:

DEFINITION 14. *Ein Torus $\mathbf{C}^n/\Lambda$ heißt abelsche Varietät, wenn es eine nichtausgeartete Riemannsche Form auf $\mathbf{C}^n$ bzgl. Λ gibt.*

SATZ 15. *Der Funktionenkörper $\mathbf{C}(T) = \mathbf{C}(\mathbf{C}^n/\Lambda)$ hat höchstens Transzendenzgrad n.*

Beweis: Wir können o.E. annehmen, daß es eine nichtausgeartete Riemannsche Form bzgl. Λ gibt. Seien $f_1, \ldots, f_m \in \mathbf{C}(T)$ algebraisch unabhängig über $\mathbf{C}$. Wir müssen $m \leq n$ zeigen. Die f_i's sind Quotienten von holomorphen Thetafunktionen. Indem wir alle Nenner zusammenmultiplizieren, können wir $f_i = \frac{\theta_i}{\theta}$ schreiben mit einer Thetafunktion θ vom Typ (L, J). Indem wir noch mit einer Thetafunktion erweitern, können wir annehmen, daß die zu θ gehörige Riemannsche Form E nichtausgeartet ist.
Sei $N \in \mathbf{N}$. Da die f_i's algebraisch unabhängig sind, sind die Thetafunktionen
$$\theta^N f_1^{n_1} \ldots f_m^{n_m} = \theta^{N-n_1-\cdots-n_m} \theta_1^{n_1} \ldots \theta_m^{n_m} \quad \text{mit } n_1 + \cdots + n_m \leq N$$
linear unabhängig über $\mathbf{C}$. Alle diese Funktionen liegen in $Th(NL, NJ)$, also gilt
$$\binom{N+m}{m} \leq \dim Th(NL, NJ) = pf(NE) = N^n pf(E).$$
Da N beliebig groß werden kann, links ein Polynom vom Grad m in N, rechts eines vom Grad n steht, folgt $m \leq n$. ■

Hat $\mathbf{C}(\mathbf{C}^n/\Lambda)$ Transzendenzgrad n, so gibt es insbesondere eine nichtausgeartete Riemannsche Form auf Λ.

SATZ 16. *Hat $\mathbf{C}(T) = \mathbf{C}(\mathbf{C}^n/\Lambda)$ Transzendenzgrad n über $\mathbf{C}$ und sind $f_1, \ldots, f_n \in \mathbf{C}(T)$ algebraisch unabhängig, so ist $\mathbf{C}(T)$ eine endliche Körpererweiterung von $\mathbf{C}(f_1, \ldots, f_n)$.*

Beweis:

1. Nach den Vorüberlegungen können wir schreiben $f_i = \frac{\theta_i}{\theta}$, wo θ eine nichtausgeartete holomorphe Thetafunktion vom Typ (L, J) mit Riemannscher Form E ist und $\theta_i \in Th(L, J)$. Außerdem sei $X = (\theta) \geq 0$.

2. Sei $g \in \mathbf{C}(T)$ beliebig. Wir schreiben $g = \frac{\psi'}{\psi}$ mit holomorphen Thetafunktionen ψ und ψ'. Sei $Y = (\psi) \geq 0$. Für natürliche Zahlen r und s betrachten wir alle Funktionen
$$f_1^{r_1} \dots f_n^{r_n} g^{s_0} \quad \text{mit } r_1 + \dots + r_n \leq r \text{ und } 0 \leq s_0 \leq s.$$
Ihre Anzahl ist
$$(s+1)\binom{r+n}{n},$$
was für große r bei festem s wächst wie
$$\frac{s+1}{n!} r^n + \dots .$$
Diese Funktionen liegen alle in $\mathcal{L}(rX + sY)$. Für große r bei festem s gilt
$$\dim \mathcal{L}(rX + sY) = \ell(rX + sY) = pf(rE_X + sE_Y) = r^n pf(E_X) + \dots .$$
Wählt man nun s so, daß
$$\frac{s+1}{n!} > pf(E_X),$$
also z.B. $s = n! pf(E)$, so können obige Funktionen für großes r nicht linear unabhängig über $\mathbf{C}$ sein, d.h. $1, g, g^2, \dots, g^s$ sind linear abhängig über $\mathbf{C}(f_1, \dots, f_n)$, d.h.
$$[\mathbf{C}(f_1, \dots, f_n, g) : \mathbf{C}(f_1, \dots, f_n)] \leq s.$$
3. Da die letzte Aussage für jedes $g \in \mathbf{C}(T)$ gilt, folgt
$$[\mathbf{C}(T) : \mathbf{C}(f_1, \dots, f_n)] \leq s,$$
woraus die Behauptung folgt. ■

Bemerkung: Jedem Divisor X haben wir eine alternierende Form E_X zugeordnet. Für zwei Divisoren X und Y gilt $E_{X+Y} = E_X + E_Y$, für den Divisor einer abelschen Funktion f natürlich $E_{(f)} = 0$. Also ist die Zuordnung $X \mapsto E_X$ ein Gruppenhomomorphismus, wo die Hauptdivisoren auf 0 gehen. Wir nennen einen Divisor X oder eine Divisorklasse $cl(X)$ positiv definit oder nichtausgeartet, wenn E_X eine positiv definite Riemannsche Form ist.

Damit gilt:

LEMMA 11. *Ist E eine positiv definite Riemannsche Form und X ein Divisor mit $E_X = E$, so gilt*
$$\ell(X) = pf(E).$$
Insbesondere ist X zu einem effektiven Divisor linear äquivalent.

Beweis: Wir wissen dies schon im Fall, daß X effektiv ist. Sei $X = (\theta)$ und (L, J) der Typ von θ. Da die zugehörige Riemannsche Form E positiv definit ist, folgt nach dem Satz von Frobenius $\dim Th(L, J) = pf(E)$. Sei $\theta_0 \in Th(L, J)$. Dann ist $\frac{\theta_0}{\theta}$ eine abelsche Funktion und
$$X = (\theta) \sim (\theta_0),$$
also
$$\ell(X) = \ell((\theta_0)) = pf(E),$$
nach dem, was wir bereits wissen. ■

DEFINITION 15. *Die Menge*
$$\{E : \mathbf{C}^n \times \mathbf{C}^n \to \mathbf{R} : E \ \mathbf{R}\text{-bilinear, alternierend und } E(\Lambda, \Lambda) \subseteq \mathbf{Z}, E(ix, y) = E(iy, x)\}$$
wird durch Addition eine abelsche Gruppe und heißt die Néron-Severi-Gruppe $NS(T)$ von $T = \mathbf{C}^n/\Lambda$.

Ist $u_1, \dots, u_{2n}$ eine $\mathbf{Z}$-Basis von Λ, so ist
$$NS(T) \to M(2n \times 2n, \mathbf{Z}), \quad E \mapsto (E(u_j, u_k)_{j,k})$$
ein injektiver Gruppenhomomorphismus. Also ist $NS(T)$ eine freie abelsche Gruppe vom Rang $\leq 4n^2$. Es gilt sogar:

SATZ 17. *$NS(T)$ ist eine freie abelsche Gruppe vom Rang $\leq n^2$.*

Beweis: Sei H_n der $\mathbf{R}$-Vektorraum der hermiteschen Formen auf $\mathbf{C}^n$. Er hat Dimension n^2. Wir definieren

$$\psi : NS(T) \to H_n, \quad E(x,y) \mapsto E(ix,y) + iE(x,y).$$

Wir zeigen, daß $\psi(NS(T))$ diskret ist. Sei $u_1, \ldots, u_{2n}$ eine Gitterbasis von Λ. Sei $\psi(E)$ klein, z.B. $|\psi(E)(u_j, u_k)| < 1$ für alle j, k. Dann folgt $|E(u_j, u_k)| < 1$ und wegen $E(u_j, u_k) \in \mathbf{Z}$ natürlich $E = 0$. Daraus folgt die Behauptung. ■

SATZ 18. *Hat T eine nichtausgeartete Riemannsche Form, so ist die Abbildung $Div \to NS$ mit $X \mapsto E_X$ ein surjektiver Homomorphismus und induziert*

$$Pic(T) \to NS(T) \to 0.$$

Beweis: Nur die Surjektivität ist noch zu zeigen. Sei E_0 eine nichtausgeartete Riemannsche Form auf T und $E \in NS(T)$ beliebig. Für großes $m \in \mathbf{N}$ ist dann auch die symmetrische Form $E(ix,y) + mE_0(ix,y)$ positiv definit. Nach dem Satz von Frobenius findet man effektive Divisoren X und X_0 mit

$$E_{X_0} = E_0 \quad \text{und} \quad E_X = E + mE_0,$$

also

$$E_{X - mX_0} = E,$$

was zu zeigen war. ■

Beispiel: Seien $a, b \in \mathbf{R}$ mit $a, b > 0$. Wir betrachten in $\mathbf{C}^2$ das durch folgende Periodenmatrix gegebene Gitter Λ:

$$\Pi = \begin{pmatrix} 1 & ai & 0 & 0 \\ 0 & 0 & 1 & bi \end{pmatrix}.$$

Bzgl. der dadurch gegebenen Gitterbasis wird die Multiplikation mit i durch folgende Matrix gegeben

$$I = \begin{pmatrix} 0 & -a & 0 & 0 \\ \frac{1}{a} & 0 & 0 & 0 \\ 0 & 0 & 0 & -b \\ 0 & 0 & \frac{1}{b} & 0 \end{pmatrix}.$$

Wir setzen nun $E \in NS$ an als

$$E = \begin{pmatrix} 0 & -n_1 & -n_2 & -n_3 \\ n_1 & 0 & -n_4 & -n_5 \\ n_2 & n_4 & 0 & -n_6 \\ n_3 & n_5 & n_6 & 0 \end{pmatrix}.$$

Folgende Matrix muß symmetrisch sein:

$$I^t E = \begin{pmatrix} \frac{n_1}{a} & 0 & -\frac{n_4}{a} & -\frac{n_5}{a} \\ 0 & an_1 & an_2 & an_3 \\ \frac{n_3}{b} & \frac{n_5}{b} & \frac{n_6}{b} & 0 \\ -bn_2 & -bn_4 & 0 & bn_6 \end{pmatrix}.$$

Setzt man $n_2 = n_3 = n_4 = n_5 = 0, n_1 = n_6 = 1$, so erhält man eine nichtausgeartete Riemannsche Form, d.h. $T = \mathbf{C}^2/\Lambda$ ist eine abelsche Varietät. Die Symmetriebedingungen lauten

$$an_3 + bn_4 = 0 \quad \text{und} \quad abn_2 - n_5 = 0.$$

Daraus ergibt sich schnell folgende Formel:

$$Rang(NS(\mathbf{C}^2/\Lambda) = 6 - \dim_{\mathbf{Q}}(\mathbf{Q}a + \mathbf{Q}b) - \dim_{\mathbf{Q}}(\mathbf{Q} + \mathbf{Q}ab).$$

So können wir Néron-Severi-Gruppen der Ränge 2,3 und 4 konstruieren.

Beispiel: $\Lambda \subseteq \mathbf{C}^2$ sei durch folgende Periodenmatrix gegeben

$$\Pi = \begin{pmatrix} 1 & 0 & i & -i\sqrt{2} \\ 0 & 1 & i\sqrt{2} & i \end{pmatrix}.$$

Man kann nachrechnen, daß bzgl. Λ keine positiv semidefinite Riemannsche Form gibt, also $Pic(T) = 0$, daß aber $NS(T) \simeq \mathbf{Z}$ gilt.

Man nennt Divisoren X und Y algebraisch äquivalent, $X \equiv Y$, wenn $E_X = E_Y$ gilt. Und analog für Divisorklassen. Der Kern der Abbildung $Pic(T) \to NS(T)$ heißt $Pic_0(T)$ und besteht aus den zu 0 algebraisch äquivalenten Divisorenklassen.

Wir wollen jetzt ein weiteres wichtiges Hilfsmittel zur Konstruktion neuer Divisoren kennenlernen. Ist θ eine Thetafunktion, so definieren wir für $a \in \mathbf{C}^n$

$$\theta_a(x) = \theta(x - a).$$

LEMMA 12. *Ist θ eine Thetafunktion vom Typ (L, J), so ist θ_a eine Thetafunktion vom Typ $(L, J(u) - L(a, u))$.*

Beweis: Für $u \in \Lambda$ gilt:

$$\theta_a(x + u) = \theta(x - a + u) = \theta(x - a)e^{2\pi i[L(x-a,u)+J(u)]} = \theta_a(x)e^{2\pi i[L(x,a)+J(u)-L(a,u)]}. \quad \blacksquare$$

Bemerkungen:

1. Ist $X = (\theta)$, so schreiben wir $X_a = (\theta_a)$. Ist X effektiv und betrachten wir X als Nullstellenmenge von θ, so gilt

   $$x \in X_a \iff \theta_a(x) = 0 \iff \theta(x - a) = 0 \iff x - a \in X \iff x \in X + a,$$

   also $X_a = X + a$, d.h. geometrisch ist X_a die Translation von X um a auf dem Torus T. So wird auch die Vorzeichenwahl deutlich.
2. Ist $a \in \Lambda$ und θ eine Thetafunktion vom Typ (L, J), so ist

   $$\theta_a(x) = \theta(x - a) = \theta(x)e^{2\pi i[-L(x,a)+J(-a)]},$$

   also sind θ und θ_a äquivalente Thetafunktionen, d.h. $(\theta) = (\theta_a)$. Insbesondere liefert dies für einen Divisor X und $a, b \in \mathbf{C}^n$:

   $$X_a = X_b \quad \text{falls } a \equiv b \bmod \Lambda.$$
3. Aus dem Lemma folgt auch sofort für die zugehörigen Formen

   $$E_{X_a} = E_X.$$

   Ist $f \neq 0$ eine abelsche Funktion, so gilt für den Divisor $Y = (f) + X_a$ auch $E_X = E_Y$. Um die Umkehrung dieser Aussage zu behandeln, brauchen wir folgendes Lemma:

LEMMA 13. *Ist θ eine normalisierte Thetafunktion vom Typ $(\frac{1}{2i}H(x, u), \frac{1}{4i}H(u, u) + K(u))$ mit (alternierender) Form E, so ist*

$$\theta(x - a)e^{2\pi i[\frac{1}{2i}H(x,a)]}$$

die zu θ_a äquivalente normalisierte Thetafunktion vom Typ

$$(\frac{1}{2i}H(x, u), \frac{1}{4i}H(u, u) + K(u) + E(u, a)).$$

Beweis: θ hat Typ (L, J) mit

$$L = \frac{1}{2i}H(x, u) \quad \text{und} \quad J = \frac{1}{4i}H(u, u) + K(u)),$$

wo $K(u)$ reellwertig ist. Dann hat $\theta(x - a)e^{2\pi i[\frac{1}{2i}H(x,a)]}$ Typ (L, J') mit

$$\begin{aligned} J'(u) &= J(u) - L(a, u) + \frac{1}{2i}H(u, a) = \\ &= \frac{1}{4i}H(u, u) + K(u) - \frac{1}{2i}H(a, u) + \frac{1}{2i}H(u, a) = \\ &= \frac{1}{4i}H(u, u) + K(u) + E(u, a), \end{aligned}$$

woraus wegen der Reellwertigkeit von $K(u) + E(u, a)$ die Behauptung folgt. $\blacksquare$

Damit können wir jetzt folgenden Satz beweisen:

SATZ 19. *Seien X und Y Divisoren mit $E_X = E_Y$. Ist dann E_X positiv definit oder sind X und Y effektiv, so gibt es $a \in \mathbf{C}^n$ und eine abelsche Funktion f mit*

$$Y = X_a + (f),$$

d.h. $Y \sim X_a$ bzw. $cl(Y) = cl(X_a)$.

Beweis: Ist E_X positiv definit, so können wir nach Abänderung um einen Hauptdivisor annehmen, daß X effektiv ist. Dann können wir allgemein nach Reduktion annehmen, daß E_X nichtausgeartet ist. Sei $X = (\theta_1)$ und $Y = (\theta_2)$ mit normalisierten Thetafunktionen θ_1, θ_2. Sei $a \in \mathbf{C}^n$. Der Divisor $Y - X_a$ enthält die normalisierte Thetafunktion

$$\frac{\theta_2(x)}{\theta_1(x-a)e^{2\pi i[\frac{1}{2i}H(x,a)]}},$$

die den Typ

$$(0, K_2(u) - K_1(u) - E(a,u))$$

hat. Wegen $K_i(u+v) \equiv K_i(u) + K_i(v) + \frac{1}{2}E(u,v) \bmod \mathbf{Z}$, gibt es eine lineare Abbildung $K : \Lambda \to \mathbf{R}$ mit $K(u) \equiv K_2(u) - K_1(u) \bmod \mathbf{Z}$. Dann gibt es ein $a \in \mathbf{C}^n$ mit $K(u) = E(a,u)$ für alle $u \in \Lambda$. Also hat obige Thetafunktion Typ $(0,0)$, ist also eine abelsche Funktion f, woraus sofort die Behauptung folgt. ■

LEMMA 14. *Für einen Divisor X ist $cl(X) \in Pic_0(T)$ genau dann, wenn es einen effektiven Divisor Y und $a \in \mathbf{C}^n$ gibt mit*

$$X \sim Y_a - Y.$$

Beweis: Die eine Richtung kennen wir bereits. Sei $E_X = 0$. Wir schreiben $X = Z - Y$ mit effektiven Divisoren Y und Z. Dann ist $E_Y = E_Z$, also gibt es eine abelsche Funktion f und $a \in \mathbf{C}^n$ mit $Z = (f) + Y_a$ und damit

$$X = ((f) + Y_a) - Y \sim Y_a - Y,$$

wie behauptet. ■

LEMMA 15. *Sei X ein Divisor. Dann ist die Abbildung*

$$\mathbf{C}^n \to Pic_0(T), \quad a \mapsto cl(X_a - X)$$

ein Homomorphismus. Anders ausgedrückt:

$$X_{a+b} + X \sim X_a + X_b.$$

Natürlich induziert dies einen Homomorphismus

$$\phi_X : \mathbf{C}^n/\Lambda \to Pic_0(T), \quad a \mapsto cl(X_a - X).$$

Beweis: Seien $a, b \in \mathbf{C}^n$ und $X = (\theta)$. Die zu θ äquivalente normalisierte Thetafunktion $\tilde{\theta}$ hat dann Typ

$$Typ(\tilde{\theta}) = (\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u)),$$

für die zu $\theta_a, \theta_b, \theta_{a+b}$ äquivalenten normalisierten Thetafunktionen gilt

$$\begin{aligned} Typ(\tilde{\theta_a}) &= (\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u) + E(u,a)), \\ Typ(\tilde{\theta_b}) &= (\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u) + E(u,b)), \\ Typ(\tilde{\theta_{a+b}}) &= (\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u) + E(u,a+b)), \end{aligned}$$

also hat $\frac{\theta_{a+b}\theta}{\theta_a\theta_b}$ Typ $(0,0)$, ist also eine abelsche Funktion, woraus die Behauptung folgt. ■

SATZ 20. *Sei X ein effektiver nichtausgearteter Divisor. Dann ist*

$$\phi_X : \mathbf{C}^n/\Lambda \to Pic_0(T)$$

surjektiv mit endlichem Kern der Ordnung

$$pf(E_X)^2.$$

Hat E_X Typ $(d_1, \ldots, d_n)$, so ist

$$Kern(\phi_X) \simeq (\mathbf{Z}/d_1 \times \cdots \times \mathbf{Z}/d_n)^2.$$

Beweis: Wir zeigen die Surjektivität: Sei $cl(Y) \in Pic_0(T)$ und $Z = X + Y$. Dann gilt $E_X = E_Z$. Da E_X nichtausgeartet ist, gibt es $a \in \mathbf{C}^n$ mit $Z \sim X_a$, also $Y \sim X_a - X$.
Sei $X = (\theta)$ und θ normalisiert vom Typ

$$(\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u)).$$

Für $a \in \mathbf{C}^n$ hat die zu θ_a äquivalente normalisierte Thetafunktion $\tilde{\theta_a}$ Typ

$$(\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u) + E(u,a)).$$

Also hat $\frac{\theta_a}{\theta}$ Typ $(0, E(u,a))$. Damit gilt

$$\begin{aligned} \phi_X(a) = 0 \quad &\iff \quad X_a \sim X \iff \frac{\tilde{\theta_a}}{\theta} \text{ ist abelsche Funktion} \\ &\iff \quad E(u,a) \in \mathbf{Z} \text{ für alle } u \in \Lambda. \end{aligned}$$

Sei $e_1, \ldots, e_n, f_1, \ldots, f_n$ eine Frobeniusbasis von $\mathbf{C}^n$ bzgl. E und $E(e_j, f_j) = d_j$. Sei

$$a = x_1 e_1 + \cdots + x_n e_n + y_1 f_1 + \cdots + y_n f_n \text{ mit } x_j, y_j \in \mathbf{R}.$$

Dann gilt

$$E(e_j, a) = y_j d_j \text{ und } E(f_j, a) = -x_j d_j,$$

woraus sofort folgt

$$a \in Kern(\phi_X) \iff a \in \frac{1}{d_1}\mathbf{Z}e_1 + \cdots + \frac{1}{d_n}\mathbf{Z}e_n + \frac{1}{d_1}\mathbf{Z}f_1 + \cdots + \frac{1}{d_n}\mathbf{Z}f_n$$

und damit, wenn wir den Kern als Untergruppe von T auffassen

$$Kern(\phi_X) \simeq (\mathbf{Z}/d_1 \times \cdots \times \mathbf{Z}/d_n)^2,$$

woraus die Behauptung folgt. ■

Aus dem Beweis sieht man auch direkt:

FOLGERUNG 3. *$Pic_0(T)$ ist ein komplexer Torus der Dimension n.*

Später werden wir sehen, daß $Pic_0(T)$ auch eine abelsche Varietät ist.

LEMMA 16. *Sei X nichtausgearteter Divisor mit Riemannscher Form E vom Typ $(d_1, \ldots, d_n)$. Dann gibt es einen (effektiven nichtausgearteten) Divisor Y mit*

$$X \sim d_1 Y.$$

Beweis: Auch $\tilde{E} = \frac{1}{d_1}E$ ist eine nichtausgeartete Riemannsche Form bzgl. Λ. Also gibt es nach dem Satz von Frobenius einen Divisor Z mit $E_Z = \tilde{E}$ und damit $E_{d_1 Z} = E = E_X$. Da E nichtausgeartet ist, gibt es $a \in \mathbf{C}^n$ mit

$$X \sim (Z + \cdots + Z)_a = d_1 Z_a.$$

Wählt man $Y = Z_a$, folgt die Behauptung. ■

KAPITEL 3

Projektive Einbettungen

Sei $\Lambda \subseteq \mathbf{C}^n$ ein Gitter und $T = \mathbf{C}^n/\Lambda$. Wir wollen versuchen, eine Einbettung $T \hookrightarrow \mathbf{P}^m$ zu konstruieren. Grundlegend ist folgende Konstruktion:

Konstruktion: Sei X ein effektiver Divisor. Dann gibt es eine holomorphe Thetafunktion θ mit $X = (\theta)$. Sei (L, J) der Typ von θ. Wir wählen eine $\mathbf{C}$-Basis $\theta_0, \ldots, \theta_m$ von $Th(L, J)$ und betrachten die Abbildung

$$F(x) = (\theta_0(x) : \cdots : \theta_m(x)),$$

die offensichtlich auf der offenen nichtleeren Menge

$$U = \mathbf{C}^n \setminus \{x \in \mathbf{C}^n : \theta_0(x) = \cdots = \theta_m(x) = 0\}$$

definiert ist. Für $x \in U_0$ und $u \in \Lambda$ gilt

$$\begin{aligned} F(x+u) &= (\theta_0(x+u) : \cdots : \theta_m(x+u)) = \\ &= (\theta_0(x)e^{2\pi i[L(x,u)+J(u)} : \cdots : \theta_m(x)e^{2\pi i[L(x,u)+J(u)}) = \\ &= (\theta_0(x) : \cdots : \theta_m(x)) = \\ &= F(x). \end{aligned}$$

Insbesondere ist $x + u \in U$ und $F(x + u) = F(x)$. Also ist

$$U_0 = \{\overline{x} \in T : x \in U\}$$

offene nichtleere Teilmenge von T und F induziert eine Abbildung

$$\varphi_X : U_0 \to \mathbf{P}^m, \quad \overline{x} \mapsto (\theta_0(x) : \cdots : \theta_m(x)).$$

Bemerkungen:

1. Ist $\theta'_0, \ldots, \theta'_m$ eine andere $\mathbf{C}$-Basis von $Th(L, J)$, so gibt es eine Matrix $A = (a_{jk}) \in GL_n(\mathbf{C})$ mit
$$\begin{pmatrix} \theta'_0(x) \\ \vdots \\ \theta'_m(x) \end{pmatrix} = A \begin{pmatrix} \theta_0(x) \\ \vdots \\ \theta_m(x) \end{pmatrix},$$
also geht die Abbildung $F'(x) = (\theta'_0(x) : \cdots : \theta'_m(x))$ aus $F(x) = (\theta_0(x) : \cdots : \theta_m(x))$ durch einen projektiven Koordinatenwechsel hervor. Bis auf Koordinatenwechsel in $\mathbf{P}^m$ ist also φ_X durch $Th(L, J)$ eindeutig bestimmt.
2. Ist θ' eine andere holomorphe Thetafunktion mit $X = (\theta')$, so sind θ und θ' äquivalent, also gibt es eine triviale Thetafunktion g mit $\theta'(x) = \theta(x)g(x)$ und auch $Th(L', J') = gTh(L, J)$, wenn (L', J') der Typ von θ' ist. Damit ist die zu $Th(L', J')$ gehörige Abbildung
$$(\theta_0(x)g(x) : \cdots : \theta_m(x)g(x)) = (\theta_0(x) : \cdots : \theta_m(x)),$$
da g nirgends verschwindet; wir erhalten also unsere alte Abbildung.
3. Damit folgt, daß die Abbildung φ_X durch X bis auf projektiven Koordinatenwechsel eindeutig definiert ist.
4. Die Dimension des projektiven Raums $\mathbf{P}^m$ ist
$$m = \dim Th(L, J) - 1 = pf_{red}(E_X).$$

LEMMA 17. *Seien X und Y effektive linear äquivalente Divisoren. Dann gilt $\varphi_X = \varphi_Y$, genauer: die Abbildungen unterscheiden sich nur um einen projektiven Koordinatenwechsel.*

Beweis: Sei $X = (\theta)$, θ holomorph vom Typ (L, J) und $Y = (f) + X$ mit einer abelschen Funktion f. Dann ist $Y = (f\theta)$, $f\theta$ also holomorphe Thetafunktion vom Typ (L, J). Da also φ_X und φ_Y mittels einer Basis von $Th(L, J)$ definiert werden, folgt die Behauptung. ■

Wir können also $\varphi_X = \varphi_{cl(X)}$ schreiben.

Bemerkung: Sei X ein ausgearteter effektiver Divisor und θ eine normalisierte Thetafunktion mit $X = (\theta)$. Sei $(L, J) = (\frac{1}{2i}H(x, u), \frac{1}{4i}H(u, u) + K(u))$ der Typ von θ. Sei $\theta_0, \ldots, \theta_m$ eine Basis von $Th(L, J)$. Da sie normalisiert sind, gilt für alle $x \in \mathbf{C}^n$ und alle $x_0 \in Kern(E)$: $\theta_j(x + x_0) = \theta_j(x)$ und damit

$$\varphi_X(x + x_0) = \varphi_X(x)$$

für alle $x_0 \in Kern(E)$ und alle x im Definitionsbereich. Damit kann φ_X nie injektiv sein. Wir werden uns daher im folgenden auf nichtausgeartete effektive Divisoren beschränken.

Bemerkung: Sei $c \in Pic(T)$ eine nichtausgeartete Klasse, d.h. E_c ist eine nichtausgeartete Riemannsche Form bzgl. Λ. Sei Y ein Divisor mit $cl(Y) = c$. Dann ist

$$\ell(Y) = pf(E_Y) = pf(E_c) > 0,$$

also gibt es eine abelsche Funktion $f \in \mathcal{L}(Y)$, also ist $X = (f) + Y$ effektiv. Nach unseren Überlegungen ist also

$$\varphi_c = \varphi_X$$

bis auf projektiven Koordinatenwechsel eindeutig definiert.

LEMMA 18. *Ist θ eine holomorphe Thetafunktion vom Typ (L, J), sind $a_1, \ldots, a_{d-1} \in \mathbf{C}$, $(d \geq 2)$, so ist*

$$\theta(x - a_1) \ldots \theta(x - a_{d-1})\theta(x + a_1 + \cdots + a_{d-1})$$

eine holomorphe Thetafunktion vom Typ (dL, dJ), d.h. vom gleichen Typ wie θ^d.

Beweis: Dies folgt sofort aus der Tatsache, daß $\theta_a(x) = \theta(x - a)$ Typ $(L, J(u) - L(a, u))$ hat. ■

SATZ 21. *Ist X ein effektiver Divisor und $d \geq 2$, so ist φ_{dX} auf ganz T definiert.*

Beweis: Sei $X = (\theta)$ mit einer holomorphen Thetafunktion θ vom Typ (L, J). Sei $\theta_0, \ldots, \theta_m$ eine Basis von $Th(dL, dJ)$. Dann ist

$$\varphi_{dX}(x) = (\theta_0(x) : \cdots : \theta_m(x)).$$

Sei $x_0 \in \mathbf{C}^n$. Wir wollen zeigen, daß φ_{dX} in x_0 definiert ist. Da θ nicht identisch 0 ist, gibt es ein $a \in \mathbf{C}^n$ mit $\theta(x_0 - a) \neq 0$. Da die holomorphen Funktionen auf $\mathbf{C}^n$ einen Integritätsring bilden, ist auch die holomorphe Funktion

$$x \mapsto (\theta(x_0 - a))^{d-2}\theta(x_0 - x)\theta(x_0 + (d - 2)a + x)$$

nicht identisch 0, also gibt es $b \in \mathbf{C}^n$ mit

$$(\theta(x_0 - a))^{d-2}\theta(x_0 - b)\theta(x_0 + (d - 2)a + b) \neq 0.$$

Nun ist

$$\psi(x) = (\theta(x - a))^{d-2}\theta(x - b)\theta(x + (d - 2)a + b) \in Th(dL, dJ),$$

also gibt es $c_0, \ldots, c_m \in \mathbf{C}$ mit

$$\psi(x) = c_0\theta_0(x) + \cdots + c_m\theta_m(x).$$

Wegen $\psi(x_0) \neq 0$ gibt es einen Index j mit $\theta_j(x_0) \neq 0$ und somit ist $\varphi_{dX}(x_0)$ definiert, was wir zeigen wollten. ■

FOLGERUNG 4. *Ist X nichtausgearteter effektiver Divisor mit Riemannscher Form E vom Typ $(d_1, \ldots, d_n)$ und $d_1 \geq 2$, so ist φ_X auf ganz T definiert.*

Beweis: Nach einem früheren Lemma finden wir einen nichtausgearteten effektiven Divisor Y mit $X \sim d_1 Y$ und somit

$$\varphi_X = \varphi_{d_1 Y},$$

was die Aussage liefert. ■

LEMMA 19. *Ist X nichtausgearteter effektiver Divisor, so ist φ_{3X} injektiv.*

Beweis:

1. Sei $X = (\theta')$ mit einer holomorphen Thetafunktion θ' vom Typ (L, J). Sei $\theta_0, \ldots, \theta_m$ eine Basis von $Th(3L, 3J)$. Dann gilt
$$\varphi_{3X} = (\theta_0(x) : \cdots : \theta_m(x)).$$
2. Wir nehmen jetzt an, daß $\varphi_{3X}(a) = \varphi_{3X}(b)$ gilt. Dann gibt es $\lambda \in \mathbf{C}, \lambda \neq 0$ mit
$$\theta_j(a) = \lambda\theta_j(b) \text{ für } j = 0, \ldots, m.$$
3. In $Th(L, J)$ gibt es eine Thetafunktion θ, die nicht bzgl. eines größeren Gitters Thetafunktion ist. Für $z, z' \in \mathbf{C}^n$ ist $\theta(x - z)\theta(x - z')\theta(x + z + z')$ in $Th(3L, 3J)$, also eine Linearkombination von $\theta_0, \ldots, \theta_m$. Also gilt
$$\theta(a - z)\theta(a - z')\theta(a + z + z') = \lambda\theta(b - z)\theta(b - z')\theta(b + z + z')$$
für alle z, z'. Wir setzen jetzt
$$z = a - x, \quad z' = a - y, \quad b = a + v,$$
womit sich ergibt
$$\theta(x)\theta(y)\theta(3a - x - y) = \lambda\theta(x + v)\theta(y + v)\theta(v + 3a - x - y).$$
Wir bilden die logarithmische Ableitung nach x_j und erhalten mit $\psi_j(x) = \frac{1}{\theta(x)}\frac{\partial\theta}{\partial x_j}$ die Beziehung
$$\psi_j(x) - \psi_j(3a - x - y) = \psi_j(x + v) - \psi_j(v + 3a - x - y).$$
Daher ist $\psi_j(x) - \psi_j(x + v)$ konstant, d.h.
$$\frac{\partial}{\partial x_j} \ln \frac{\theta(x + v)}{\theta(x)} = c_j.$$
Dies liefert
$$\theta(x + v) = \theta(x) \cdot Ae^{c_1x_1 + \cdots + c_nx_n} = \theta(x)e^{2\pi i[\ell(x) + c]}.$$
4. Sei jetzt $u \in \Lambda$. Dann ist einerseits
$$\begin{aligned} \theta(x + u + v) &= \theta(x + v)e^{2\pi i[L(x+v,u) + J(u)]} = \\ &= \theta(x) \cdot e^{2\pi i[\ell(x) + c + L(x+v,u) + J(u)]} \end{aligned}$$
und andererseits
$$\begin{aligned} \theta(x + u + v) &= \theta(x + u) \cdot e^{2\pi i[\ell(x+u) + c]} = \\ &= \theta(x) \cdot e^{2\pi i[\ell(x+u) + c + L(x,u) + J(u)]}, \end{aligned}$$
woraus sich ergibt
$$\ell(u) \equiv L(v, u) \bmod \mathbf{Z}.$$
Also gibt es ganze Zahlen n_u mit
$$\ell(u) = L(v, u) + n_u = L(u, v) + E(v, u) + n_u.$$
Dies ergibt
$$\ell(u) - L(u, v) = E(v, u) + n_u.$$
Die linke Seite ist $\mathbf{C}$-linear, die rechte Seite immer reell, also ist $\ell(u) = L(u, v)$ und damit $E(v, u) \in \mathbf{Z}$ für alle $u \in \Lambda$. Damit ist $\ell(x) = L(x, v)$, so daß wir haben
$$\theta(x + v) = \theta(x)e^{2\pi i[L(x,v) + c]}.$$
5. Nun ist
$$\Lambda_0 = \{x \in \mathbf{C}^n : E(x, \Lambda) \subseteq \mathbf{Z}\}$$
ein Gitter in $\mathbf{C}^n$, das Λ und v enthält. Also ist auch $\Lambda + \mathbf{Z}v$ ein Gitter.
6. Obige Relation liefert, daß θ auch Thetafunktion bzgl. $\Lambda + \mathbf{Z}v$ ist. Nach unserer Voraussetzung folgt $v \in \Lambda$ und damit $a \equiv b \bmod \Lambda$, was wir zeigen wollten. ■

Ist X nichtausgearteter Divisor, so ist also φ_{3X} definiert und injektiv. Da T kompakt ist, ist auch $\varphi_{3X}(T) \subseteq \mathbf{P}^m$ kompakt, also abgeschlossen. Wir wollen sehen, daß φ_{3X} sogar eine Einbettung ist. Dazu müssen wir φ_{3X} noch lokal untersuchen.

SATZ 22 (Lefschetz). *Ist X ein nichtausgearteter Divisor, so ist φ_{3X} eine Einbettung.*

Beweis:

1. O.E. ist X effektiv, $X = (\theta)$, θ holomorph vom Typ (L, J) und $\theta_0, \ldots, \theta_m$ eine Basis von $Th(3L, 3J)$. Dann ist
$$\varphi_{3X} = (\theta_0(x) : \cdots : \theta_m(x)).$$
Sei $a \in T$. Wir müssen zeigen, daß φ_{3X} lokal in a einen biholomorphen Isomorphismus aus Bild liefert. Da φ_{3X} überall definiert ist, können wir o.E. $\theta_0(a) \neq 0$ annehmen. Damit ist $U = \{x \in T : \theta_0(x) \neq 0\}$ eine offene Umgebung von a. Für $x \in U$ gilt:
$$\varphi_{3X}(x) = (1 : \frac{\theta_1(x)}{\theta_0(x)} : \cdots : \frac{\theta_m(x)}{\theta_0(x)}).$$
Schreiben wir $f_j(x) = \frac{\theta_j(x)}{\theta_0(x)}$, so erhalten wir also eingeschränkt auf U eine Abbildung $U \to \mathbf{C}^n$ mit
$$x \mapsto (f_1(x), \ldots, f_m(x)).$$
Dies ist ein lokaler Isomorphismus aufs Bild, falls die Jacobimatrix
$$(\frac{\partial f_j}{\partial x_k}(a))_{j,k}$$
maximalen Rang, also Rang n hat.
2. Wir nehmen jetzt an, die Jacobimatrix hat Rang $< n$. Dann gibt es komplexe Zahlen $b_1, \ldots, b_n$, nicht alle 0, mit
$$b_1 \frac{\partial f_j}{\partial x_1}(a) + \cdots + b_n \frac{\partial f_j}{\partial x_n}(a) = 0$$
für $j = 0, \ldots, m$. Ist
$$x_j = \sum b_{jk} y_k$$
ein linearer Koordinatenwechsel in $\mathbf{C}^n$, so ist
$$\frac{\partial f}{\partial y_1} = \sum_j \frac{\partial f}{\partial x_j} \frac{\partial x_j}{\partial y_1} = \sum_j \frac{\partial f}{\partial x_j} b_{j1},$$
nach Koordinatenwechsel können wir also o.E.
$$\frac{\partial f_j}{\partial x_1}(a) = 0 \text{ für } j = 0, \ldots, m$$
annehmen. Setzen wir $f_j = \frac{\theta_j}{\theta_0}$ ein, so folgt
$$\theta_0(a) \frac{\partial \theta_j}{\partial x_1}(a) = \theta_j(a) \frac{\partial \theta_0}{\partial x_1}(a).$$
also gibt es eine komplexe Zahl $\lambda \neq 0$ mit
$$\lambda \theta_j(a) = \frac{\partial \theta_j}{\partial x_1}(a).$$
Da die θ_j eine Basis von $Th(L, J)$ bilden, folgt für alle $\tilde{\theta} \in Th(L, J)$ die Gleichung
$$\lambda \tilde{\theta}(a) = \frac{\partial \tilde{\theta}}{\partial x_1}(a)$$
bzw.
$$\lambda = \frac{\partial}{\partial x_1} \ln \tilde{\theta}(a),$$
sofern definiert.

3. Wir wählen jetzt
$$\tilde{\theta} = \theta(x-b)\theta(x-a)\theta(x+a+b),$$
setzen
$$\psi = \frac{1}{\theta(x)}\frac{\partial\theta}{\partial x_1}$$
und erhalten damit
$$\lambda = \psi(a-b) + \psi(a-c) + \psi(a+b+c).$$
Wir schreiben jetzt x statt b:
$$\lambda = \psi(a-x) + \psi(a-c) + \psi(a+x+c)$$
und differenzieren nach x_j:
$$0 = -\frac{\partial\psi}{\partial x_j}(a-x) + \frac{\partial\psi}{\partial x_j}(a+x+c)$$
Da dies für alle x und alle c aus einer offenen Menge gilt, ist $\frac{\partial\psi}{\partial x_j}$ konstant. Damit folgt
$$\frac{1}{\theta(x)}\frac{\partial\theta}{\partial x_1} = g(x) = a_1x_1 + \cdots + a_nx_n + b$$
auf einer offenen Menge mit komplexen Zahlen $a_1, \ldots, a_n, b$.
4. Wir setzen jetzt
$$q(x) = \frac{1}{2}a_1x_1^2 + a_2x_1x_2 + \cdots + a_nx_1x_n + bx_1.$$
Dann folgt für $\theta'(x) = \theta(x)e^{-q(x)}$:
$$\frac{\partial\theta'}{\partial x_1} = \frac{\partial\theta}{\partial x_1}e^{-q(x)} + \theta e^{-q(x)}(-1)[a_1x_1 + a_2x_2 + \cdots + a_nx_n + b] = 0.$$
Also hängt θ' nicht von x_1 ab, ist also ausgeartet. Damit ist auch E_X ausgeartet, ein Widerspruch zur Voraussetzung. ■

Aus dem Beweis werden wir folgenden Satz folgern:

FOLGERUNG 5. *Der Funktionenkörper $\mathbf{C}(T)$ hat Transzendenzgrad n über $\mathbf{C}$.*

Beweis: Wir wissen bereits, daß der Transzendenzgrad höchstens n ist. Wir betrachten $f_j(x) = \frac{\theta_j(x)}{\theta_0(x)}$ wie im Beweis. Nach eventueller Umindizierung können wir annehmen, daß die Jacobimatrix
$$(\frac{\partial f_j}{\partial x_k})_{j,k=1,\ldots,n}$$
auf einer nichtleeren offenen Menge U Rang n hat. Angenommen, $f_1, \ldots, f_n$ sind algebraisch abhängig über $\mathbf{C}$. Dann gibt es ein Polynom $F \in \mathbf{C}[y_1, \ldots, y_n]$, das nicht 0 ist, mit $F(f_1, \ldots, f_n) = 0$. Wir können annehmen, daß F minimalen Grad mit dieser Eigenschaft hat. Differenzieren ergibt:
$$0 = \sum_j \frac{\partial F}{\partial y_j}(f_1, \ldots, f_n)\frac{\partial f_j}{\partial x_k}$$
für alle $x \in U$. Dies liefert aber
$$\frac{\partial F}{\partial y_j}(f_1, \ldots, f_n) = 0$$
und nach dem Identitätssatz demnach in $\mathbf{C}(T)$. Auf Grund der Minimalität von F folgt $\frac{\partial F}{\partial y_j} = 0$, also F konstant, also $F = 0$: ein Widerspruch. Demnach sind $f_1, \ldots, f_n$ algebraisch unabhängig über $\mathbf{C}$, woraus dann mit den Vorüberlegungen die Behauptung folgt. ■

Der Satz von Chow sagt nun, daß eine analytische Untervarietät von $\mathbf{P}^m$ auch eine algebraische Varietät ist. Damit erhalten wir:

FOLGERUNG 6. *Ist X ein nichtausgearteter Divisor, so ist $\varphi_{3X}(T)$ eine nichtsinguläre algebraische Varietät in $\mathbf{P}^m$. Damit erhält T die Struktur einer nichtsingulären projektiven algebraischen Varietät.*

Damit ist auch der Begriff abelsche Varietät für komplexe Tori mit einer nichtausgearteten Riemannschen Form gerechtfertigt.
Der Satz von Lefschetz läßt sich wie folgt verallgemeinern:

SATZ 23. *Ist X nicht ausgeartet und E_X vom Typ $d_1, \ldots, d_n$ mit $d_1 \geq 3$, so ist φ_X eine Einbettung*

$$T \hookrightarrow \mathbf{P}^{d_1 \ldots d_n - 1}.$$

($\varphi_X(T)$ hat Grad $n! d_1 \ldots d_n$.)

KAPITEL 4

Elliptische Kurven

Sei $\Lambda \subseteq \mathbf{C}$ ein Gitter und $T = \mathbf{C}/\Lambda$.

1. Die Néron-Severi-Gruppe $NS(T)$

Nach Koordinatenwechsel können wir schreiben

$$\Lambda = \mathbf{Z} + \mathbf{Z}\tau \text{ mit } \tau = \beta + i\gamma, \quad \beta, \gamma \in \mathbf{R}, \gamma > 0.$$

Ist $E \in NS(T)$, so ist

$$H(x,y) = E(ix,y) + iE(x,y)$$

eine hermitesche Form auf $\mathbf{C}$, also von der Form

$$H(x,y) = \alpha x\overline{y} \text{ mit } \alpha \in \mathbf{R}, x, y \in \mathbf{C}.$$

Seien A und B die Matrizen der reellen Bilinearformen $E(ix,y)$ und $E(x,y)$ bzgl. der Gitterbasis $1, \tau$. Aus

$$\begin{aligned} H(1,1) &= \alpha, \\ H(1,\tau) &= \alpha\overline{\tau} = \alpha(\beta - i\gamma) = \alpha\beta - i\alpha\gamma, \\ H(\tau,1) &= \alpha\tau = \alpha\beta + i\alpha\gamma, \\ H(\tau,\tau) &= \alpha|\tau|^2 \end{aligned}$$

folgt

$$A = \begin{pmatrix} \alpha & \alpha\beta \\ \alpha\beta & \alpha|\tau|^2 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & -\alpha\gamma \\ \alpha\gamma & 0 \end{pmatrix}.$$

B muß eine ganzzahlige Matrix sein, d.h. es gibt $d \in \mathbf{Z}$ mit $\alpha\gamma = d$, d.h. $\alpha = d\frac{1}{\gamma}$. Dann ist

$$A = \frac{d}{\gamma}\begin{pmatrix} 1 & \beta \\ \beta & |\tau|^2 \end{pmatrix}.$$

A ist genau dann positiv definit, wenn $d > 0$ gilt. Dann ist

$$E(x,y) = \frac{1}{2i}[H(x,y) - H(y,x)] = \frac{d}{2i\gamma}(x\overline{y} - \overline{x}y).$$

Wir formulieren dies als Satz:

Satz 24. *Ist $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$ mit $\tau = \beta + i\gamma$ mit $\gamma > 0$, so ist*

$$NS(T) = \mathbf{Z} \cdot E$$

mit

$$E(x,y) = \frac{x\overline{y} - \overline{x}y}{2i\gamma}.$$

E ist eine nichtausgeartete Riemannsche Form.

Jede elliptische Kurve hat also ganz natürlich eine Riemannsche Form. Daher spielen die Riemannschen Formen bei den elliptischen Kurven auch keine explizite Rolle.

2. Die Weierstraßsche σ-Funktion

In der Funktionentheorie lernt man manchmal folgende Funktion kennen:

$$\sigma(z) = z \prod_{\omega \in \Lambda \setminus \{0\}} (1 - \frac{z}{\omega}) e^{\frac{z}{\omega} + \frac{z^2}{2\omega^2}}.$$

Sie heißt Weierstraßsche σ-Funktion und ist nach dem Weierstraßschen Produktsatz so gemacht, daß sie konvergiert, holomorph ist und einfache Nullstellen in den Gitterpunkten hat.
Die logarithmische Ableitung heißt die Weierstraßsche Zetafunktion:

$$\zeta(z) = \frac{\sigma'(z)}{\sigma(z)} = \frac{d}{dz} \ln \sigma(z) = \frac{1}{z} + \sum_{\omega \in \Lambda \setminus \{0\}} (\frac{1}{z - \omega} + \frac{1}{\omega} + \frac{z}{\omega^2}).$$

Durch Differenzieren von $-\zeta(z)$ erhält man die Weierstraßsche $\wp$-Funktion:

$$\wp(z) = -\zeta'(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \frac{1}{(z - \omega)^2}.$$

Da $\wp$ periodisch ist, gibt es für jedes $\omega \in \Lambda$ ein $\eta(\omega) \in \mathbf{C}$ mit

$$\zeta(z + \omega) = \zeta(z) + \eta(\omega).$$

LEMMA 20. *Es gilt*

$$\eta(\omega + \omega') = \eta(\omega) + \eta(\omega')$$

und für $\Lambda = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$*:*

$$\omega_1 \eta(\omega_2) - \omega_2 \eta(\omega_1) = 2\pi i.$$

Beweis: Aus

$$\zeta(z) + \eta(\omega + \omega') = \zeta(z + \omega + \omega') = \zeta(z + \omega) + \eta(\omega') = \zeta(z) + \eta(\omega) + \eta(\omega')$$

folgt, daß $\eta : \Lambda \to \mathbf{C}$ additiv ist. Die zweite Behauptung folgt durch Integration mit dem Residuensatz. ■

LEMMA 21. *σ ist eine Thetafunktion vom Typ $(L, *)$ mit*

$$L(z, \omega) = \frac{1}{2\pi i} z \eta(\omega).$$

Die zugehörige Riemannsche Form hat Typ 1, erzeugt also $NS(T)$. Außerdem ist σ ungerade, d.h. $\sigma(-z) = -\sigma(z)$.

Beweis: Aus

$$\frac{d}{dz} \ln \frac{\sigma(z + \omega)}{\sigma(z)} = \eta(\omega)$$

ergibt sich durch Integrieren und Exponenzieren:

$$\sigma(z + \omega) = \sigma(z) e^{\eta(\omega) z + 2\pi i J(\omega)}$$

mit geeigneter Zahl $J(\omega) \in \mathbf{C}$. Folglich ist σ eine Thetafunktion mit

$$L(z, \omega) = \frac{1}{2\pi i} z \eta(\omega).$$

Ist ω_1, ω_2 eine Gitterbasis, so gilt dür die zugehörige Riemannsche Form E:

$$E(\omega_1, \omega_2) = L(\omega_1, \omega_2) - L(\omega_2, \omega_1) = \frac{1}{2\pi i} [\omega_1 \eta(\omega_2) - \omega_2 \eta(\omega_1)] = 1.$$

Also erzeugt E die Néron-Severi-Gruppe $NS(\mathbf{C}/\Lambda)$. ■

Wir betrachten die Transformationsformel noch etwas genauer. Es ist üblich, sie in der Form

$$\sigma(z + \omega) = \psi(\omega) e^{\eta(\omega)(z + \frac{\omega}{2})} \sigma(z)$$

zu schreiben. Dann gilt:

LEMMA 22.

$$\psi(\omega) = \begin{cases} 1 & \frac{\omega}{2} \in \Lambda \\ -1 & \frac{\omega}{2} \notin \Lambda \end{cases}$$

Beweis: Benutzt man $\sigma(-z) = -\sigma(z)$, so ergibt sich, wenn man $z = -\frac{\omega}{2}$ einsetzt:

$$\sigma(\frac{\omega}{2}) = \psi(\omega)\sigma(-\frac{\omega}{2}) = -\psi(\omega)\sigma(\frac{\omega}{2}).$$

Ist $\frac{\omega}{2} \notin \Lambda$, so ist $\sigma(\frac{\omega}{2}) \neq 0$, so daß $\eta(\omega) = -1$ folgt. Berechnet man jetzt $\sigma(z + 2\omega)$ direkt und dann über $\sigma((z + \omega) + \omega)$, so erhält man

$$\psi(2\omega) = \psi(\omega)^2,$$

woraus die Behauptung folgt. ■

3. Projektive Einbettungen

Sei X der Divisor (σ). Dann liefert φ_{3X} eine Einbettung von T. Die Riemannsche Form E_{3X} hat Typ 3, also ist $\varphi_{3X}(T) \subseteq \mathbf{P}^2$ eine (nichtsinguläre) Kurve vom Grad 3, d.h. es gibt ein homogenes kubisches Polynom

$$f = a_0x_0^3 + a_1x_0^2x_1 + a_2x_0^2x_2 + \cdots + a_9x_2^3$$

mit

$$\varphi_{3X}(T) = \{f = 0\}.$$

Um überhaupt Aussagen über f machen zu können, versuchen wir, φ_{3X} möglichst symmetrisch zu schreiben. Wir halten uns dabei an [**Hulek**]. Wir definieren für $m \in \mathbf{Z}$:

$$\theta_m(z) = e^{\pi i m - \frac{1}{3}\eta_2\omega_1 m - \frac{1}{6}\eta_1\omega_1 m^2 + m\eta_1 z}\sigma(z - \frac{m\omega_1}{3})\sigma(z - \frac{m\omega_1 + \omega_2}{3})\sigma(z - \frac{m\omega_1 + 2\omega_2}{3}).$$

LEMMA 23. *Es gibt nirgends verschwindende Funktionen $A(z), B(z), C(z)$, so daß für alle $m \in \mathbf{Z}$ gilt:*

$$\begin{aligned} \theta_{m+3}(z) &= \theta_m(z), \\ \theta_m(-z) &= A(z)\theta_{-m}(z), \\ \theta_m(z - \frac{\omega_1}{3}) &= B(z)\theta_{m+1}(z), \\ \theta_m(z + \frac{\omega_2}{3}) &= C(z)\zeta_3^m\theta_m(z). \end{aligned}$$

$\theta_0, \theta_1, \theta_2$ sind linear unabhängig über $\mathbf{C}$.

Beweis: [**Hulek**]. ■

Wir betrachten jetzt die Abbildung

$$\varphi_{3X} : \quad z \mapsto (\theta_0(z) : \theta_1(z) : \theta_2(z)).$$

Das Bild ist die Nullstellenmenge eines kubischen Polynoms $f = a_0x_0^3 + \cdots + a_9x_2^3$:

$$\{(\theta_0(z) : \theta_1(z) : \theta_2(z)) \in \mathbf{P}^2 : z \in \mathbf{C}\} = \{(y_0 : y_1 : y_2) \in \mathbf{P}^2 : f(y_0, y_1, y_2) = 0\}.$$

LEMMA 24. *Es gibt $b, c, d \in \mathbf{C}$ mit*

$$\begin{aligned} f(x_1, x_2, x_0) &= bf(x_0, x_1, x_2), \\ f(x_0, x_2, x_1) &= cf(x_0, x_1, x_2), \\ f(x_0, \zeta_3x_1, \zeta_3^2x_2) &= df(x_0, x_1, x_2). \end{aligned}$$

Beweis: Wir beweisen die erste Aussage, die anderen gehen ganz genauso. Sei $(y_0 : y_1 : y_2) \in C$. Dann gibt es $z \in \mathbf{C}$ mit

$$(y_0 : y_1 : y_2) = (\theta_0(z) : \theta_1(z) : \theta_2(z)).$$

Nun gilt

$$\begin{aligned} (y_0 : y_2 : y_1) &= (\theta_0(z) : \theta_2(z) : \theta_1(z)) = \\ &= (A(z)\theta_{-0}(z) : A(z)\theta_{-1}(z) : A(z)\theta_{-2}(z)) = \\ &= (\theta_0(-z) : \theta_1(-z) : \theta_2(-z)) \in C \end{aligned}$$

und damit $f(y_0, y_2, y_1) = 0$, was sofort

$$\{f(x_0, x_1, x_2) = 0\} \subseteq \{f(x_0, x_2, x_1) = 0\}$$

ergibt. Daraus folgt die Behauptung. ■

Setzt man f wie oben an, so erhält man durch Koeffizientenvergleich ein lineares Gleichungssystem. Diskutiert man dies, so kommt man auf die Gestalt

$$f = \lambda(x_0^3 + x_1^3 + x_2^3) - \mu x_0 x_1 x_2.$$

$\lambda = 0$ ist nicht möglich, da f sonst reduzibel wäre, also kann man o.E. schreiben

$$f = x_0^3 + x_1^3 + x_2^3 - \mu x_0 x_1 x_2.$$

Wir erhalten also:

SATZ 25. *Mit den oben definierten Größen gilt:*

$$\varphi_{3X}(T) = \{x_0^3 + x_1^3 + x_2^3 - \mu x_0 x_1 x_2 = 0\}.$$

KAPITEL 5

Holomorphe Abbildungen zwischen komplexen Tori und abelschen Varietäten

Ganz natürlich ergeben sich folgende holomorphen Abbildungen zwischen komplexen Tori:

1. Sind $T_i = \mathbf{C}^{n_i}/\Lambda_i$, $i = 1, 2$ komplexe Tori, ist $F : \mathbf{C}^{n_1} \to \mathbf{C}^{n_2}$ eine lineare Abbildung mit
$$F(\Lambda_1) \subseteq \Lambda_2,$$
so induziert F eine holomorphe Abbildung
$$T_1 \to T_2, \quad x + \Lambda_1 \mapsto Fx + \Lambda_2.$$
Sie bildet außerdem 0 auf 0 ab.
2. Ist $T = \mathbf{C}^n/\Lambda$ ein komplexer Torus und $a \in T$, so ist
$$t_a : T \to T, \quad x \mapsto x + a$$
eine holomorphe Abbildung, die Translation um a.
Ist $\alpha : T_1 \to T_2$ eine Abbildung zwischen komplexen Tori mit $\alpha(0) = a$, so ist $t_{-a} \circ \alpha$ eine Abbildung $T_1 \to T_2$, die 0 auf 0 abbildet. So kann man sich leicht auf diesen Fall zurückziehen.

Das folgende Lemma zeigt, daß man so schon alle holomorphen Abbildungen zwischen komplexen Tori erhält:

LEMMA 25. *Ist $\alpha : T_1 \to T_2$ eine holomorphe Abbildung zwischen komplexen Tori $T_i = \mathbf{C}^{n_i}/\Lambda_i$ mit $\alpha(0) = 0$, so gibt es eine $\mathbf{C}$-lineare Abbildung $F : \mathbf{C}^{n_1} \to \mathbf{C}^{n_2}$ mit*
$$F(\Lambda_1) \subseteq \Lambda_2 \quad \textit{und} \quad \alpha(x + \Lambda_1) = F(x) + \Lambda_2.$$
F ist eindeutig bestimmt und wird mit $\rho_a(\alpha)$ bezeichnet.

Beweis: Wir betrachten die zusammengesetzte Abbildung $\mathbf{C}^{n_1} \to T_1 \to T_2$. Da $\mathbf{C}^{n_2}$ die universelle Überlagerung von T_2 ist, gibt es eine holomorphe Abbildung $F : \mathbf{C}^{n_1} \to \mathbf{C}^{n_2}$, die α induziert. Sei $u \in \Lambda_1$. Dann ist für alle x auch $F(x + u) - F(x) \in \Lambda_2$, also
$$F(x + u) - F(x) = b_u.$$
Differenzieren ergibt
$$\frac{\partial F}{\partial x_j}(x + u) = \frac{\partial F}{\partial x_j}(x).$$
Da dies für alle $u \in \Lambda_1$ gilt, ist $F(x)$ beschränkt und damit konstant. Damit folgt
$$F(x) = x_1 a_1 + \cdots + x_n a_n + b$$
mit $a_1, \ldots, a_n, b \in \mathbf{C}^{n_2}$. Wegen $\alpha(0) = 0$ ist $b \in \Lambda_2$ und wir können o.E. $b = 0$ annehmen. Dann ist also F linear. Daß F eindeutig bestimmt ist, ist dann klar. ■

FOLGERUNG 7. *Ist $\alpha : T_1 \to T_2$ holomorph mit $\alpha(0) = 0$, so ist α ein Gruppenhomomorphismus.*

Wir definieren jetzt
$$Hom(T_1, T_2) = \{\alpha : T_1 \to T_2, \alpha(0) = 0\}$$
und bezeichnen die Elemente als Homomorphismen. $Hom(T_1, T_2)$ ist eine abelsche Gruppe. Wir haben bereits die sogenannte analytische Darstellung definiert:
$$\rho_a : Hom(T_1, T_2) \to Hom_{\mathbf{C}}(\mathbf{C}^{n_1}, \mathbf{C}^{n_2}), \quad \alpha \mapsto \rho_a(\alpha).$$

(Dies ist natürlich ein Gruppenhomomorphismus.) Ist $\alpha \in Hom(T_1, T_2)$, so gilt für $F = \rho_a(\alpha)$: $F(\Lambda_1) \subseteq \Lambda_2$, wir erhalten also auch ein Element von $Hom_{\mathbf{Z}}(\Lambda_1, \Lambda_2)$, das wir mit $\rho_r(\alpha)$ bezeichnen:

$$\rho_r : Hom(T_1, T_2) \to Hom_{\mathbf{Z}}(\Lambda_1, \Lambda_2).$$

ρ_r wird rationale Darstellung genannt. Sowohl ρ_a als auch ρ_r sind injektiv. Aus

$$Hom(T_1, T_2) \hookrightarrow Hom_{\mathbf{Z}}(\Lambda_1, \Lambda_2) \simeq Hom_{\mathbf{Z}}(\mathbf{Z}^{2n_1}, \mathbf{Z}^{2n_2}) \simeq M(2n_2 \times 2n_1, \mathbf{Z}) \simeq \mathbf{Z}^{4n_1 n_2}$$

folgt sofort der Satz:

SATZ 26. *$Hom(T_1, T_2)$ eine freie abelsche Gruppe vom Rang $\leq 4n_1 n_2$.*

Im Fall $T = T_1 = T_2 = \mathbf{C}^n/\Lambda$ ist $Hom(T, T)$ sogar ein Ring, der sogenannte Endomorphismenring $End(T)$ von T. Für jedes $m \in \mathbf{Z}$ ist

$$m : T \to T, \quad x \mapsto mx$$

ein Endomorphismus, die sogenannte Multiplikation mit m. Wir erhalten so

$$\mathbf{Z} \hookrightarrow End(E).$$

Untertori: Ist $T = \mathbf{C}^n/\Lambda$ ein Torus und $W \subseteq \mathbf{C}^n$ ein $\mathbf{C}$-Untervektorraum, so ist $\Lambda \cap W$ ein freier $\mathbf{Z}$-Modul in W, der diskret ist, vom Rang $\leq n$. I.a. ist aber $\Lambda \cap W$ kein Gitter in W.
Ist $\Lambda \cap W$ ein Gitter in W, so ist die induzierte Abbildung

$$W/(\Lambda \cap W) \to \mathbf{C}^n/\Lambda$$

injektiv, man betrachtet $W/(\Lambda \cap W)$ als Untertorus von T.

LEMMA 26. *Ist T eine abelsche Varietät und T_0 ein Untertorus von T, so ist auch T_0 eine abelsche Varietät.*

Beweis: Sei $T = \mathbf{C}^n/\Lambda$ und E eine nichtausgeartete Riemannsche Form bzgl. Λ. Ist $T_0 = W/(W \cap \Lambda)$, so erhält man durch Einschränkung auf W eine nichtausgeartete Riemannsche Form bzgl. $W \cap \Lambda$, woraus die Behauptung folgt. ■

LEMMA 27. *Ist $\alpha : T_1 \to T_2$ ein Homomorphismus komplexer Tori, so ist $\alpha(T_1)$ ein Untertorus von T_2 und es gibt eine endliche Untergruppe G, einen Untertorus S von T_1 mit*

$$Kern(\alpha) = G \oplus S.$$

Außerdem gilt

$$\dim T_1 = \dim \alpha(T_1) + \dim S.$$

Beweis:

1. Sei $T_i = \mathbf{C}^{n_i}/\Lambda_i$ und $F = \rho_a(\alpha) : \mathbf{C}^{n_1} \to \mathbf{C}^{n_2}$ die zu α gehörige lineare Abbildung. Dann sind
$$U = Kern(F) \quad \text{und} \quad V = Bild(F)$$
$\mathbf{C}$-Untervektorräume von $\mathbf{C}^{n_1}$ bzw. $\mathbf{C}^{n_2}$.
2. Wegen $F(\Lambda_1) \subseteq \Lambda_2$ erhalten wir eine Abbildung $\Lambda_1 \to \Lambda_2$. Wir machen jetzt Basiswechsel in Λ_1 und Λ_2: Es gibt eine Basis
$$u_1, \ldots, u_{2n_1} \text{ von } \Lambda_1 \text{ und } v_1, \ldots, v_{2n_2} \text{ von } \Lambda_2,$$
natürliche Zahlen $d_1 | d_2 | \ldots | d_m$, so daß gilt
$$F(u_1) = d_1 v_1, \ldots, F(u_m) = d_m v_m, F(u_{m+1}) = 0, \ldots, F(u_{2n_1}) = 0.$$
3. Damit ist
$$V = Bild(F) = \mathbf{R}v_1 + \cdots + \mathbf{R}v_m, \quad V \cap \Lambda_2 = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_m,$$
also ist
$$\alpha(T_1) = V/(V \cap \Lambda_2)$$
ein Untertorus von T_2 der Dimension $\frac{m}{2}$.

4. Der Kern von α ist $F^{-1}(\Lambda_2)/\Lambda_1$. Aus unserer Darstellung sieht man aber sofort
$$F^{-1}(\Lambda_2) = \frac{1}{d_1}\mathbf{Z}u_1 + \cdots + \frac{1}{d_m}\mathbf{Z}u_m + \mathbf{R}u_{m+1} + \cdots + \mathbf{R}u_{2n_1}.$$
Nun ist
$$U/(U \cap \Lambda_1) = (\mathbf{R}u_{m+1} + \cdots + \mathbf{R}u_{2n_1})/(\mathbf{Z}u_{m+1} + \cdots + \mathbf{Z}u_{2n_1})$$
ein Untertorus S von T_1 und
$$G = (\frac{1}{d_1}\mathbf{Z}u_1 + \cdots + \frac{1}{d_m}\mathbf{Z}u_m)/(\mathbf{Z}u_1 + \cdots + \mathbf{Z}u_m)$$
eine endliche Gruppe. Also
$$F^{-1}(\Lambda_2)/\Lambda_1 = G \oplus S.$$
Mit
$$\dim S = n_1 - \frac{m}{2}$$
folgt dann die Behauptung. ■

LEMMA 28. *Sei $T = \mathbf{C}^n/\Lambda$ ein komplexer Torus.*

1. *Ist G eine endliche Untergruppe von T, so ist auch T/G ein komplexer Torus.*
2. *Ist S ein Untertorus von T, so ist auch T/S ein komplexer Torus.*

Beweis:

1. Wir schreiben
$$G = \Lambda'/\Lambda.$$
Dann ist auch Λ' ein Gitter in $\mathbf{C}^n$, also $T' = \mathbf{C}^n/\Lambda'$ ein komplexer Torus. Der natürliche Homomorphismus
$$\mathbf{C}^n/\Lambda \to \mathbf{C}^n\Lambda'$$
hat als Kern $\Lambda'/\Lambda = G$, woraus die Behauptung folgt.
2. Sei $S = V/(V \cap \Lambda)$ und $\dim V = m$.
   (a) $V \cap \Lambda$ ist Gitter in V, ist also ein freier $\mathbf{Z}$-Modul vom Rang $2m$. Es gibt eine Basis $u_1, \ldots, u_{2m}$ von Λ, natürliche Zahlen $d_1|d_2|\ldots|d_{2m}$, so daß
   $$d_1u_1, \ldots, d_{2m}u_{2m}$$
   eine Basis von $V \cap \Lambda$ ist.
   (b) Wir zerlegen $\mathbf{C}^n = V \oplus W$ mit einem komplexen Vektorraum W der Dimension $n - m$. Sei $\pi : \mathbf{C}^n \to W$ die Projektion.
   (c)
   $$\pi(\Lambda) = \mathbf{Z}\pi(u_{2m+1}) + \cdots + \mathbf{Z}\pi(u_{2n})$$
   erzeugt W als $\mathbf{R}$-Vektorraum, ist also ein Gitter in W.
   (d) Wir betrachten die natürliche Abbildung
   $$\alpha : \mathbf{C}^n/\Lambda \to W/\pi(\Lambda),$$
   die surjektiv ist. Was ist der Kern? Sei $x = r_1u_1 + \cdots + r_{2n}u_{2n}$ mit $r_1, \ldots, r_{2n} \in \mathbf{R}$. Dann gilt:
   $$\begin{aligned} \overline{x} \in Kern(\alpha) &\iff \pi(x) \in \pi(\Lambda) \\ &\iff r_{2m+1}, \ldots, r_{2n} \in \mathbf{Z} \\ &\iff x \in V + \Lambda \\ &\iff \overline{x} \in (V + \Lambda)/\Lambda \simeq V/(V \cap \Lambda) \end{aligned}$$
   Also
   $$Kern(\alpha) = V/(V \cap \Lambda),$$
   was wir zeigen wollten. ■

Wir wollen jetzt sehen, wie sich Thetafunktionen und Divisoren mit Homomorphismen vertragen.

LEMMA 29. *Sei $\alpha : T_1 \to T_2$ ein Homomorphismus komplexer Tori, $T_i = \mathbf{C}^{n_i}/\Lambda_i$ und $F = \rho_a(\alpha)$. Ist dann θ eine Thetafunktion auf $\mathbf{C}^{n_2}$ bzgl. Λ_2 vom Typ (L, H) mit Riemannscher Form E, so ist $F^*\theta = \theta \circ F$ eine Thetafunktion auf $\mathbf{C}^{n_1}$ bzgl. Λ_1 vom Typ $(L(F(x), F(u)), J(F(u))$ mit Riemannscher Form $E(F(x), F(y))$.*

Beweis: Es gilt

$$\theta(F(x+u)) = \theta(F(x)+F(u)) = \theta(F(x))e^{2\pi i[L(F(x),F(u))+J(F(u))]},$$

woraus alles folgt. ■

Sei $\alpha : T_1 \to T_2$ ein Homomorphismus und $F = \rho_a(\alpha)$. Ist θ triviale Thetafunktion bzgl. T_2, so ist $\theta \circ F$ trivial bzgl. T_1, also ist folgende Abbildung wohldefiniert:

$$\alpha^* : Div(T_2) \to Div(T_1), \quad (\theta) \mapsto (\theta \circ F).$$

Da Hauptdivisoren bei dieser Abbildung in Hauptdivisoren übergehen, erhalten wir eine induzierte Abbildung

$$\alpha^* : Pic(T_2) \to Pic(T_1).$$

Außerdem gilt für $X \in Div(T_2)$:

$$E_{\alpha^* X} = F^*(E_X),$$

also induzierte Abbildungen

$$\alpha^* Pic_0(T_2) \to Pic_0(T_1) \quad \text{und} \quad \alpha^* NS(T_2) \to NS(T_1).$$

DEFINITION 16. *Ein Homomorphismus $\alpha : T_1 \to T_2$ heißt Isogenie, wenn $\rho_a(\alpha)$ ein Isomorphismus ist. (Insbesondere ist α surjektiv mit endlichem Kern.) $\#Kern(\alpha)$ heißt Grad der Isogenie.*

Bemerkung: Sei $\alpha : T_1 \to T_2$ eine Isogenie mit $F = \rho_a(\alpha)$. Nach $\mathbf{C}$-Basiswechsel links und rechts können wir $F = id$ annehmen. Dann ist also

$$T_1 = \mathbf{C}^n/\Lambda_1, \quad T_2 = \mathbf{C}/\Lambda_2 \quad \text{mit } \Lambda_1 \subseteq \Lambda_2.$$

Der Kern der Isogenie ist Λ_2/Λ_1.

Beispiel: Ist $T = \mathbf{C}^n/\Lambda$ ein komplexer Torus und $m \in \mathbf{Z}, m > 0$, so ist die Multiplikation mit m:

$$T \to T, \quad x \mapsto mx$$

surjektiv mit Kern

$$\frac{1}{m}\Lambda/\Lambda \simeq (\mathbf{Z}/m)^{2n},$$

also eine Isogenie vom Grad m^{2n}. Manchmal wird dafür auch m_T oder $[m]$ geschrieben.

LEMMA 30. *Sei T ein komplexer Torus und $X \in Div(T)$. Dann gilt für jede ganze Zahl m*

$$m^*X \sim \frac{m^2+m}{2}X + \frac{m^2-m}{2}(-1)^*X.$$

Beweis: Wir beweisen die Formel nur für $m \geq 0$. Der Rest folgt dann sofort, indem man die Formel auf $|m|^*((-1)^*X)$ anwendet. Sei $X = (\theta)$ mit einer Thetafunktion vom Typ (L, J). Dann ist

$$\frac{m^2+m}{2}X + \frac{m^2-m}{2}(-1)^*X - m^*X = (\tilde{\theta}),$$

wo

$$\tilde{\theta}(x) = \frac{\theta(x)^{\frac{m^2+m}{2}}\theta(-x)^{\frac{m^2-m}{2}}}{\theta(mx)}.$$

$\tilde{\theta}$ ist eine Thetafunktion vom Typ $(\tilde{L}, \tilde{J})$ mit

$$\begin{aligned}\tilde{L}(x,u) &= \frac{m^2+m}{2}L(x,u) + \frac{m^2-m}{2}L(-x,-u) - L(mx,mu) = 0,\\ \tilde{J}(u) &= \frac{m^2+m}{2}J(u) + \frac{m^2-m}{2}J(-u) - J(mu).\end{aligned}$$

Wir wissen

$$J(u+v) \equiv J(u) + J(v) + L(u,v) \text{ und } J(0) = 0.$$

Aus

$$0 = J(0) = J(u + (-u)) \equiv J(u) + J(-u) + L(u, -u)$$

folgt dann

$$J(-u) \equiv -J(u) + L(u, u).$$

Behauptung:

$$J(mu) \equiv mJ(u) + \frac{m^2 - m}{2} L(u, u).$$

Dies gilt für $m = 1$ und dann durch Induktion aus

$$\begin{aligned} J((m+1)u) &\equiv J(mu) + J(u) + L(mu, u) \equiv (m+1)J(u) + (\frac{m^2 - m}{2} + m)L(u, u) = \\ &= (m+1)J(u) + \frac{m(m+1)}{2} L(u, u). \end{aligned}$$

Damit gilt dann

$$\begin{aligned} \tilde{J}(u) &= \frac{m^2 + m}{2} J(u) + \frac{m^2 - m}{2} J(-u) - J(mu) = \\ &\equiv \frac{m^2 + m}{2} J(u) + \frac{m^2 - m}{2} [-J(u) + L(u, u)] - [mJ(u) + \frac{m^2 - m}{2} L(u, u)] \equiv 0. \end{aligned}$$

Also ist $\tilde{\theta}$ eine Thetafunktion vom Typ $(0, 0)$, d.h. eine abelsche Funktion, was zu beweisen war. ■

LEMMA 31. *Sind $\alpha : T_1 \to T_2$ und $\beta : T_2 \to T_3$ Isogenien, so auch $\beta \circ \alpha$ und*

$$\deg(\beta \circ \alpha) = \deg(\beta) \deg(\alpha).$$

Beweis: Klar. ■

LEMMA 32. *Ist $\alpha : T_1 \to T_2$ eine Isogenie vom Grad m, so gibt es eine Isogenie $\beta : T_2 \to T_1$ mit*

$$\alpha \circ \beta = m, \quad \beta \circ \alpha = m.$$

Beweis: Sei $F = \rho_a(\alpha)$. Nach komplexem Basiswechsel können wir $F = id$ annehmen. Dann ist $\Lambda_1 \subseteq \Lambda_2$ und

$$Kern(\alpha) = \Lambda_2 / \Lambda_1.$$

Wegen $\#\Lambda_2/\Lambda_1 = m$ gilt

$$m\Lambda_2 \subseteq \Lambda_1.$$

Setzen wir $G(x) = mx$, so induziert dies einen Homomorphismus $\beta : T_2 \to T_1$ mit Kern

$$\frac{1}{m}\Lambda_1/\Lambda_2 \simeq \Lambda_1/m\Lambda_2.$$

Die Behauptungen $\alpha \circ \beta = m$ und $\beta \circ \alpha = m$ sind dann klar. ■

Damit sieht man, daß Isogenie eine Äquivalenzrelation ist. Wir nennen komplexe Tori T_1 und T_2 isogen, wenn es eine Isogenie $T_1 \to T_2$ zwischen ihnen gibt.

LEMMA 33. *Sind T_1 und T_2 isogene komplexe Tori, ist T_1 abelsche Varietät, so auch T_2.*

Beweis: O.E. $T_1 = \mathbf{C}^n/\Lambda_1$, $T_2 = \mathbf{C}^n/\Lambda_2$ und $\Lambda_2 \subseteq \Lambda_1$. Ist E eine nichtausgeartete Riemannsche Form bzgl. Λ_1, so auch bzgl. Λ_2, was alles zeigt. ■

Produkte komplexer Tori: Sind $T_1 = \mathbf{C}^{n_1}/\Lambda$ und $T_2 = \mathbf{C}^{n_2}/\Lambda_2$ komplexe Tori, so ist auch

$$T_1 \times T_2 = (\mathbf{C}^{n_1} \times \mathbf{C}^{n_2})/(\Lambda_1 \times \Lambda_2)$$

ein komplexer Torus. Sind T_1 und T_2 abelsche Varietäten, so offensichtlich auch $T_1 \times T_2$. Natürlich sind auch die Projektionen $T_1 \times T_2 \to T_i$, sowie die Einbettungen $T_1 \to T_1 \times T_2, x \mapsto (x, 0)$ und $T_2 \to T_1 \times T_2, y \mapsto (0, y)$ holomorph.

LEMMA 34. *Für komplexe Tori T_1 und T_2 gilt:*

$$End(T_1 \times T_2) = \begin{pmatrix} End(T_1) & Hom(T_2,T_1) \\ Hom(T_1,T_2) & End(T_2) \end{pmatrix} = \left\{ \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} : \alpha_{ij} \in Hom(T_j,T_i) \right\}$$

und für eine natürliche Zahl m und einen komplexen Torus T:

$$End(T^m) = M_m(End(T)),$$

wo $M_m(R)$ den Matrizenring der $m \times m$ Matrizen mit Koeffizienten aus R bezeichnet.

Beweis: Sei $\alpha \in End(T_1 \times T_2)$. Dann sind die induzierten Abbildungen $T_j \to T_1 \times T_2 \to T_i$ Homomorphismen $\alpha_{ij} \in Hom(T_j,T_i)$. Für $x \in T_1, y \in T_2$ gilt:

$$\begin{aligned} \alpha \begin{pmatrix} x \\ y \end{pmatrix} &= \begin{pmatrix} \alpha_1(x,y) \\ \alpha_2(x,y) \end{pmatrix} = \\ &= \begin{pmatrix} \alpha_1((x,0)+\alpha_1((0,y)) \\ \alpha_2((x,0))+\alpha_2((0,y)) \end{pmatrix} = \\ &= \begin{pmatrix} \alpha_{11}(x)+\alpha_{12}(y) \\ \alpha_{21}(x)+\alpha_{22}(y) \end{pmatrix} = \\ &= \begin{pmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}. \end{aligned}$$

Umgekehrt ist natürlich auch jede Abbildung dieser Bauart ein Homomorphismus. Die Aussage für T^m ergibt sich analog. ■

Ein fundamentaler Satz für abelschen Varietäten ist folgender:

SATZ 27 (Poincarés cher Reduzibilitätssatz). *Ist T eine abelsche Varietät und T_1 ein nichttrivialer komplexer Untertorus, so gibt es einen komplexen Untertorus T_2, so daß*

$$T_1 \times T_2 \to T, \quad (x,y) \mapsto x+y$$

eine Isogenie ist.

Beweis:

1. Sei $T = \mathbf{C}^n/\Lambda$ und $T_1 = V_1/(V_1 \cap \Lambda)$ mit einem Untervektorraum $V_1 \subseteq \mathbf{C}^n$. Dann ist $\Lambda_1 = V_1 \cap \Lambda$ ein Gitter in V_1. Sei E eine nichtausgeartete Riemannsche Form auf $\mathbf{C}^n$ bzgl. Λ.
2. Sei
$$V_2 = \{x \in \mathbf{C}^n : E(x,V_1) = 0\}.$$
V_2 ist ein $\mathbf{C}$-Vektorraum, denn ist $x \in V_2$ und $y \in V_1$, so ist $iy \in V_1$ und damit
$$E(ix,y) = E(iy,x) = 0.$$
Da E nichtausgeartet ist, erhalten wir
$$\mathbf{C}^n = V_1 \oplus V_2.$$
3. Sei
$$\Lambda_2 = \{x \in \Lambda : E(x,\Lambda_1) = 0\}.$$
Λ_2 ist ein freier $\mathbf{Z}$-Modul vom Rang $\geq 2n - 2n_1$. Außerdem ist Λ_2 diskret. Natürlich gilt $\Lambda_2 \subseteq V_2$ und daher ist Λ_2 ein Gitter in V_2. Wegen $\Lambda_2 = V_2 \cap \Lambda$ ist V_2/Λ_2 ein komplexer Untertorus von T.
4. Wir definieren
$$T_1 \times T_2 \to T, \quad (x,y) \mapsto x+y.$$
Dies ist surjektiv, also eine Isogenie. ■

Das folgende Beispiel zeigt, daß die Aussage des Poincaréschen Satzes nicht mehr gültig sein muß, wenn T keine abelsche Varietät ist.

Beispiel: Sei $T = \mathbf{C}^2/\Lambda$ mit

$$\Lambda = \begin{pmatrix} i & 1 & 0 & \sqrt{2} \\ 0 & 0 & 1 & i \end{pmatrix} \mathbf{Z}^4 = \{ \begin{pmatrix} xi+y+t\sqrt{2} \\ z+ti \end{pmatrix} : x,y,z,t \in \mathbf{Z} \}.$$

Wir wollen alle echten Untertori $U/(U\cap\Lambda)$ von T bestimmen. U ist also 1-dimensional über $\mathbf{C}$. $U\cap\Lambda$ ist ein Gitter in U, also gibt es Gittervektoren u_1, u_2 mit $U\cap\Lambda = \mathbf{Z}u_1 + \mathbf{Z}u_2$. Natürlich sind u_1, u_2 linear abhängig über $\mathbf{C}$, d.h. $u_2 = (a+bi)u_1$ mit $a, b \in \mathbf{R}, b \neq 0$. Wir machen den Ansatz

$$\begin{pmatrix} x_2 i + y_2 + t_2\sqrt{2} \\ z_2 + t_2 i \end{pmatrix} = (a+bi)\begin{pmatrix} x_1 i + y_1 + t_1\sqrt{2} \\ z_1 + t_1 i \end{pmatrix}.$$

1. Fall: $z_1 + t_1 i \neq 0$*:* Die zweite Komponente liefert durch Vergleich von Real- und Imaginärteil:

$$z_2 = az_1 - bt_1, \quad t_2 = at_1 + bz_1,$$

woraus sich ergibt

$$a = \frac{z_1 z_2 + t_1 t_2}{z_1^2 + t_1^2}, \quad b = \frac{z_1 t_2 - z_2 t_1}{z_1^2 + t_1^2},$$

insbesondere sind $a, b \in \mathbf{Q}$. Die erste Komponente liefert

$$y_2 + t_2\sqrt{2} + x_2 i = (ay_1 - bx_1) + at_1\sqrt{2} + (ax_1 + by_1)i + bt_1\sqrt{2}i.$$

Nun sind $1, \sqrt{2}, i, \sqrt{2}i$ linear unabhängig über $\mathbf{Q}$, also folgt durch Koeffizientenvergleich

$$\begin{aligned} x_2 &= ax_1 + by_1 \\ y_2 &= ay_1 - bx_1 \\ t_2 &= at_1 \\ 0 &= bt_1 \end{aligned}$$

Wegen $b \neq 0$ folgt $t_1 = 0$ und damit $t_2 = 0$. Aus einer früheren Gleichung ergibt sich aber dann $z_1 = 0$, ein Widerspruch zur Voraussetzung.
2. Fall: $z_1 + t_1 i = 0$*:* Dann ist alles richtig wegen

$$U = \{\begin{pmatrix} z \\ 0 \end{pmatrix} : z \in \mathbf{C}\}, \quad U\cap\Lambda = \mathbf{Z}\begin{pmatrix} 1 \\ 0 \end{pmatrix} + \mathbf{Z}\begin{pmatrix} i \\ 0 \end{pmatrix}.$$

Es gibt also nur einen komplexen Untertorus, damit kann der Satz von Poincare nicht gültig sein.

DEFINITION 17. *Eine abelsche Varietät A heißt einfach, wenn sie keine nichttrivialen abelschen Untervarietäten besitzt.*

FOLGERUNG 8. *Jede abelsche Varietät A ist isogen zu einem Produkt*

$$A_1^{e_1} \times \cdots \times A_r^{e_r}$$

mit $e_1, \ldots, e_r \geq 1$, wobei die A_i einfache abelsche Varietäten sind, die paarweise nicht isogen sind. (Die A_i's sind dabei bis auf Isogenie eindeutig bestimmt.)

LEMMA 35. *Sind A_1 und A_2 einfache abelsche Varietäten, $\alpha : A_1 \to A_2$ ein Homomorphismus, so ist entweder $\alpha = 0$ oder α ist eine Isogenie.*

Beweis: Wir wissen:

$$Kern(\alpha) = G \oplus S,$$

wo G eine endliche Untergruppe und S ein Untertorus von A_1 ist. Da S trivial sein muß, bleiben nur zwei Fälle:
1. Fall: $S = 0$*:* Dann ist $\dim \alpha(A_1) = \dim S > 0$, das Bild ist also ein Untertorus $\neq 0$ von A_2, also $\alpha(A_1) = A_2$: damit ist α eine Isogenie.
2. Fall: $S = A_1$*:* Dann ist $\alpha = 0$. ■

Sind also A_1 und A_2 nichtisogene einfache abelsche Varietäten, so ist $Hom(A_1, A_2) = 0$.

Wir wissen, daß für einen n-dimensionalen Torus T der Endomorphismenring $End(T)$ ein freier $\mathbf{Z}$-Modul vom Rang $\leq 4n^2$ ist. Wir betrachten jetzt den davon erzeugten $\mathbf{Q}$-Vektorraum:

$$End_{\mathbf{Q}}(T) = End(T) \otimes_{\mathbf{Z}} \mathbf{Q} = \mathbf{Q} \cdot End(T) = \{\frac{\alpha}{n} : \alpha \in End(T), n \in \mathbf{N}\}.$$

Wir können $End(T) \subseteq End_{\mathbf{Q}}(T)$ annehmen. Analog kann man für komplexe Tori $Hom_{\mathbf{Q}}(T_1, T_2) = Hom(T_1, T_2) \otimes_{\mathbf{Z}} \mathbf{Q}$ betrachten und hat dann

$$Hom(T_1, T_2) \hookrightarrow Hom_{\mathbf{Q}}(T_1, T_2).$$

SATZ 28. *Sind die komplexen Tori T_1 und T_2 isogen, so sind $End_{\mathbf{Q}}(T_1)$ und $End_{\mathbf{Q}}(T_2)$ isomorph (als $\mathbf{Q}$-Algebren).*

Beweis: Es gibt Isogenien $\lambda : T_1 \to T_2$ und $\mu : T_2 \to T_1$ mit

$$\lambda \circ \mu = m, \quad \mu \circ \lambda = m.$$

Wir definieren

$$f : End_{\mathbf{Q}}(T_1) \to End_{\mathbf{Q}}(T_2), \quad \alpha \mapsto \frac{1}{m}\lambda\alpha\mu \quad \text{und} \quad g : End_{\mathbf{Q}}(T_2) \to End_{\mathbf{Q}}(T_1), \quad \beta \mapsto \frac{1}{m}\mu\beta\lambda.$$

Dann sind f und g Ringhomomorphismen, die $\mathbf{Q}$ festlassen und weiter gilt

$$fg = 1 \text{ und } gf = 1,$$

also folgt

$$End_{\mathbf{Q}}(T_1) \simeq End_{\mathbf{Q}}(T_2). \quad \blacksquare$$

Die Umkehrung gilt im allgemeinen nicht.

FOLGERUNG 9. *Ist A eine abelsche Varietät und isogen zu $A_1^{n_1} \times \cdots \times A_r^{n_r}$, wo $A_1, \ldots, A_r$ paarweise nichtisogene abelsche Varietäten sind, so gilt*

$$End_{\mathbf{Q}}(A) \simeq M_{n_1}(End_{\mathbf{Q}}(A_1)) \oplus \cdots \oplus M_{n_r}(End_{\mathbf{Q}}(A_r)).$$

SATZ 29. *Eine abelsche Varietät A ist genau dann einfach, wenn $End(A)_{\mathbf{Q}}$ ein Schiefkörper ist.*

Statt Schiefkörper ist auch der Name Divisionsalgebra gebräuchlich.

Beweis: Sei A einfach und $\frac{1}{m}\alpha \in End_{\mathbf{Q}}(A)$, $\frac{1}{m}\alpha \neq 0$ mit $\alpha \in End(A)$. Dann ist α eine Isogenie, also gibt es ein $\beta \in End(A)$, ein $n \in \mathbf{N}$ mit $\alpha\beta = n, \beta\alpha = n$. Dann ist aber $\frac{1}{m}\alpha$ Einheit wegen

$$\frac{1}{m}\alpha \cdot \frac{m}{n}\beta = 1 \text{ und } \frac{m}{n}\beta \cdot \frac{1}{m}\alpha = 1$$

und damit $End_{\mathbf{Q}}(A)$ ein Schiefkörper. Ist A nicht einfach, so ist nach obigem Zerlegungssatz $End_{\mathbf{Q}}(A)$ sicher kein Schiefkörper. $\blacksquare$

Beispiel: Wir betrachten die elliptischen Kurven

$$E_f = \mathbf{C}/\Lambda_f \text{ mit } \Lambda_f = \mathbf{Z} + \mathbf{Z}fi \text{ für } f \in \mathbf{N}.$$

Λ_f ist nicht nur ein Gitter, sondern sogar ein Ring:

$$\Lambda_f = \mathbf{Z} + \mathbf{Z}fi = \mathbf{Z}[fi].$$

Isogenie: Sind $f_1, f_2 \in \mathbf{N}$, so gilt $f_2\Lambda_{f_1} \subseteq \Lambda_{f_2}$, d.h. die Multiplikation mit f_2 liefert eine Isogenie $E_{f_1} \to E_{f_2}$. Alle betrachteten Kurven E_f sind also isogen.
Endomorphismenringe: Die Endomorphismen von E_f werden durch Multiplikation mit komplexen Zahlen α beschrieben, genauer:

$$End(E_f) = \{\alpha : \alpha\Lambda_f \subseteq \Lambda_f\}.$$

Ist $\alpha \in End(E_f)$, so ist wegen $1 \in \Lambda_f$ natürlich $\alpha \in \Lambda_f = \mathbf{Z}[fi]$; umgekehrt gilt natürlich $\mathbf{Z}[fi]\Lambda_f \subseteq \Lambda_f$, also hat man

$$End(E_f) = \mathbf{Z}[fi].$$

Isomorphie: Die Ringe $\mathbf{Z}[fi]$ sind paarweise nichtisomorph; f ist nämlich in $\mathbf{Z}[fi]$ dadurch charakterisiert, daß es die kleinste natürlich Zahl n ist, für die die Gleichung $x^2 + n = 0$ eine Lösung besitzt. Also sind auch die Kurven E_f paarweise nichtisomorph.
Weiter gilt

$$End_{\mathbf{Q}}(E_f) = \mathbf{Q} \times_{\mathbf{Z}} \mathbf{Z}[fi] = \mathbf{Q}(i).$$

KAPITEL 6

Die duale abelsche Varietät

Sei $T = \mathbf{C}^n/\Lambda$ eine abelsche Varietät. Wir hatten die exakte Sequenz

$$0 \to Pic_0(T) \to Pic(T) \to NS(T) \to 0.$$

Ist X ein nichtausgearteter Divisor, so wissen wir, daß

$$\phi_X : T \to Pic_0(T), \quad a \mapsto cl(X_a - X)$$

surjektiv ist mit Kern der Ordnung $Pf(E_X)^2$. Insbesondere ist auch $Pic_0(T)$ ein komplexer Torus. Wir wollen dies nochmals unabhängig von X machen.

Sei $X \in Div(T)$. Dann gibt es genau eine normalisierte Thetafunktion θ mit $X = (\theta)$. θ hat Typ

$$(\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u))$$

mit $K(u) \in \mathbf{R}$ und

$$K(u+v) \equiv K(u) + K(v) + \frac{1}{2}E(u,v) \bmod \mathbf{Z}.$$

Ist $cl(X) \in Pic_0(T)$, so ist $E_X = 0$, also bleibt die Bedingung, daß $K : \Lambda \to \mathbf{R}/\mathbf{Z}$ additiv ist. Geht man zu einem linear äquivalenten Divisor über, so bleibt der Typ gleich, also ist

$$\tau : Pic_0(T) \to \{K : \Lambda \to \mathbf{R}/\mathbf{Z} \text{ additiv } \}$$

wohldefiniert.

LEMMA 36. *τ ist ein Isomorphismus, d.h.*

$$Pic_0(T) \simeq \{K : \Lambda \to \mathbf{R}/\mathbf{Z} \textit{ additiv } \}.$$

Beweis: Injektivität: Sei $cl(X) \in Kern(\tau)$ mit $X = (\theta)$, θ normalisiert. Dann ist θ abelsche Funktion, also $cl(X) = 0$.
Surjektivität: Sei $K : \Lambda \to \mathbf{R}/\mathbf{Z}$ additiv. Sei (L, J) nichtausgearteter Typ. Dann ist auch $(L, J+K)$ nichtausgeartet. Nach dem Satz von Frobenius gibt es (holomorphe) Thetafunktionen θ und θ' vom Typ (L, J) bzw. $(L, J+K)$. Die Funktion $\frac{\theta'}{\theta}$ hat dann Typ $(0, K)$, K ist also Bild von $cl((\frac{\theta'}{\theta}))$. ■

Um eine komplexe Struktur auf $Pic_0(T)$ einzuführen, brauchen wir noch folgendes Lemma:

LEMMA 37. *Die Abbildung*

$$\mathbf{C}^n \times \mathbf{C}^n \to \mathbf{R}, \quad (x,y) \mapsto Im(x^t\overline{y})$$

ist $\mathbf{R}$-bilinear und nichtausgeartet. (D.h. beschreibt man die Abbildung durch eine reelle $2n \times 2n$-Matrix, so ist die Determinante $\neq 0$.)

Beweis: Die $\mathbf{R}$-Bilinearität ist klar. Jedes $x \in \mathbf{C}^n$ hat eine Zerlegung $x = a + ib$, wo a, b nur reelle Einträge haben. Sei $x \neq 0$. Dann gilt:

$$Im((-b+ia)^t\overline{(a+ib)}) = a^ta + b^tb > 0,$$

also ist die Form nichtausgeartet. ■

Es gilt auch noch

$$Im(x^t\overline{y}) = Im(\overline{y}^t x) = -Im(\overline{\overline{y}^t x}) = -Im(y^t\overline{x}).$$

Wir definieren jetzt

$$\sigma : \mathbf{C}^n \to \{K : \Lambda \to \mathbf{R}/\mathbf{Z} \text{ additiv } \} \simeq Pic_0(T), \quad x \mapsto (u \mapsto Im(x^t\overline{u}) \bmod \mathbf{Z}).$$

LEMMA 38. *σ ist surjektiv.*

Beweis: Wir können uns ein Element von $Pic_0(T)$ durch ein Element von $K : \Lambda \to \mathbf{R}/\mathbf{Z}$ gegeben denken. Dann gibt es eine additive Abbildung $\tilde{K} : \Lambda \to \mathbf{R}$ mit $\tilde{K} \equiv K \bmod \mathbf{Z}$. $\tilde{K}$ setzt sich eindeutig zu einer $\mathbf{R}$-linearen Form $\mathbf{C}^n \to \mathbf{R}$ fort, also gibt es ein $x \in \mathbf{C}^n$ mit $K(u) = Im(x^t\overline{u})$, woraus die Behauptung folgt. ■

LEMMA 39. *$Kern(\sigma)$ ist ein Gitter $\hat{\Lambda}$ in $\mathbf{C}^n$.*

Beweis: Sei $u_1, \ldots, u_{2n}$ eine Gitterbasis von Λ. Sei $v_1, \ldots, v_{2n}$ die ($\mathbf{R}$-)duale Basis zu $u_1, \ldots, u_{2n}$, d.h.

$$Im(v_i^t\overline{u_j}) = \delta_{ij}.$$

Daraus folgt sofort

$$\{x \in \mathbf{C}^n : Im(x^t\overline{u}) \in \mathbf{Z}\} = \mathbf{Z}v_1 + \cdots + \mathbf{Z}v_{2n}.$$

Dies ist ein Gitter $\hat{\Lambda}$ in $\mathbf{C}^n$. Nun gilt für $x \in \mathbf{C}^n$:

$$x \in Kern(\sigma) \iff Im(x^t\overline{u}) \in \mathbf{Z} \text{ für } u \in \Lambda \iff x \in \hat{\Lambda},$$

die Behauptung. ■

DEFINITION 18. *$\hat{T} = \mathbf{C}^n/\hat{\Lambda}$ heißt der zu T duale komplexe Torus, wobei*

$$\hat{\Lambda} = \{x \in \mathbf{C}^n : Im(x^t\overline{u}) \in \mathbf{Z} \textit{ für alle } u \in \Lambda\}.$$

Nach Konstruktion gilt:

SATZ 30. *Die Abbildung $\tau^{-1}\sigma$ induziert einen Isomorphismus*

$$\hat{T} \simeq Pic_0(T).$$

LEMMA 40. *$\hat{\hat{\Lambda}} = \Lambda$ und damit $\hat{\hat{T}} = T$.*

Beweis: folgt sofort durch Wahl von Basen wie oben. ■

Ist $\alpha : T_1 \to T_2$ ein Homomorphismus abelscher Varietäten, so hatten wir die natürliche Abbildung

$$\alpha^* : Pic_0(T_2) \to Pic_0(T_1).$$

Wir wollen die induzierte Abbildung

$$\hat{T_2} \simeq Pic_0(T_2) \to Pic_0(T_1) \simeq \hat{T_1}$$

betrachten. Sei $T_i = \mathbf{C}^{n_i}/\Lambda_i$, $F = \rho_a(\alpha)$. Wir denken uns F als komplexe $n_2 \times n_1$-Matrix. Sei $x \in \mathbf{C}^{n_2}$ Repräsentant eines Elements aus $\hat{T_2}$. Dies liefert in $Pic_0(T_2)$ das Element $K : \Lambda_2 \to \mathbf{R}/\mathbf{Z}$ mit

$$K(u) = Im(x^t\overline{u}), u \in \Lambda_2.$$

Die Anwendung von $\alpha^* : Pic_0(T_2) \to Pic_0(T_1)$ ergibt

$$\tilde{K}(v) = K(F(v)) = Im(x^t\overline{Fv}) = Im((\overline{F}^t x)^t\overline{v}) \quad \text{für } v \in \Lambda_1,$$

was dem Element $\overline{F}^t x \in \mathbf{C}^{n_1}$ entspricht.
Behauptung: $\overline{F}^t\hat{\Lambda_2} \subseteq \hat{\Lambda}_1$.
Beweis: Sei $x \in \hat{\Lambda}_2$. Sei $u \in \Lambda_1$ beliebig. Dann ist

$$Im((\overline{F}^t x)^t\overline{u}) = Im(x^t\overline{Fu}) = 0,$$

also folgt die Behauptung. ■

Die Matrix $\overline{F}^t$ induziert also einen Homomorphismus $\hat{\alpha} : \hat{T_2} \to \hat{T_1}$. Damit haben wir:

SATZ 31. *Ist $\alpha : T_1 \to T_2$ ein Homomorphismus, $F = \rho_a(\alpha)$ die zugehörige Matrix, so definiert $\overline{F}^t$ einen Homomorphismus $\hat{\alpha} : \hat{T_2} \to \hat{T_1}$, der mit $\alpha^* : Pic_0(T_2) \to Pic_0(T_1)$ übereinstimmt. Nochmals:*

$$\rho_a(\alpha) = F, \quad \rho_a(\hat{\alpha}) = \overline{F}^t.$$

LEMMA 41.

$$\hat{id} = id, \quad \hat{\alpha\beta} = \hat{\beta}\hat{\alpha} \text{ und } \hat{\hat{\alpha}} = \alpha.$$

Beweis: Dies rechnet man mit der analytischen Darstellung sofort nach. ■

LEMMA 42. *Ist $\alpha : T_1 \to T_2$ eine Isogenie, so auch $\hat{\alpha}$ und $Kern(\alpha) \simeq Kern(\hat{\alpha})$, insbesondere*

$$\deg \alpha = \deg \hat{\alpha}.$$

Beweis: Ist $F = \rho_a(\alpha)$, so ist $\overline{F}^t = \rho_a(\hat{\alpha})$. Da F bijektiv ist, ist es auch $\overline{F}^t$, also ist $\hat{\alpha}$ eine Isogenie. Außerdem gilt

$$Kern(\alpha) = F^{-1}(\Lambda_2)/\Lambda_1 \text{ und } Kern(\hat{\alpha}) = \overline{F}^{t-1}(\hat{\Lambda_1})/\hat{\Lambda_2}.$$

Sei $u_1, \ldots, u_{2n}$ eine Gitterbasis von $F^{-1}(\Lambda_2)$, so daß $d_1u_1, \ldots, d_{2n}u_{2n}$ eine Gitterbasis von Λ_1 ist mit $d_i \in \mathbf{N}$. Dann ist $F(u_1), \ldots, F(u_{2n})$ Basis von Λ_2. Sei $v_1, \ldots, v_{2n}$ duale Basis, d.h.

$$Im(v_i^t \overline{Fu_j}) = \delta_{ij}.$$

Dann ist $v_1, \ldots, v_{2n}$ Basis von $\hat{\Lambda_2}$. Nun gilt

$$\delta_{ij} = Im((\overline{F}^t v_i)^t \overline{u_j}) = Im((\frac{1}{d_i}\overline{F}^t v_i)^t \overline{d_j u_j}),$$

also ist

$$\frac{1}{d_1}\overline{F}^t v_1, \ldots, \frac{1}{d_{2n}}\overline{F}^t v_{2n}$$

Basis von $\hat{\Lambda_1}$ und damit

$$\frac{1}{d_1}v_1, \ldots, \frac{1}{d_{2n}}v_{2n}$$

Basis von $\overline{F}^{t-1}(\hat{\Lambda_1})$ und damit

$$\begin{aligned} \overline{F}^{t-1}(\hat{\Lambda_1})/\hat{\Lambda_2} &= (\mathbf{Z}\frac{1}{d_1}v_1 + \ldots \mathbf{Z}\frac{1}{d_{2n}}v_{2n})/(\mathbf{Z}v_1 + \ldots \mathbf{Z}v_{2n}) \simeq \\ &\simeq (\mathbf{Z}v_1 + \ldots \mathbf{Z}v_{2n})/(\mathbf{Z}d_1v_1 + \ldots \mathbf{Z}d_{2n}v_{2n}) = \\ &= F^{-1}(\Lambda_2)/\Lambda_1, \end{aligned}$$

was die Behauptung war. ■

SATZ 32. *Ist X ein Divisor auf T, so ist*

$$\phi_X : T \to \hat{T} \simeq Pic_0(T), \quad a \mapsto cl(X_a - X)$$

ein Homomorphismus mit

$$\rho_a(\phi_X)(a) = (-H^t)a,$$

wo H die Matrix ist, die die zu X gehörige hermitesche Form beschreibt.

Beweis: Ist $X = (\theta)$ mit einer normalisierten Thetafunktion θ vom Typ $(\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u))$, ist $\tilde{\theta_a}$ die zu θ_a äquivalente normalisierte Thetafunktion, so hat $\tilde{\theta_a}$ Typ $(\frac{1}{2i}H(x,u), \frac{1}{4i}H(u,u) + K(u) + E(u,a))$, also hat $\frac{\tilde{\theta_a}}{\theta}$ Typ $(0, E(u,a))$. Das Bild $\phi_X(a)$ in $\{K : \Lambda \to \mathbf{R}/\mathbf{Z}\}$ wird also durch $u \mapsto E(u,a)$ gegeben. Nun gilt

$$E(u,a) = -E(a,u) = -ImH(a,u) = -Im(a^t H\overline{u}) = Im((-H^t a)^t \overline{u}),$$

also

$$\phi_X(a) = (-H^t)a \bmod \hat{\Lambda}.$$

Man sieht auch sofort, daß für $a \in \Lambda$ gilt $(-H^t)a \in \hat{\Lambda}$. ■

FOLGERUNG 10. *Ist X ein nichtausgearteter Divisor auf T, so ist ϕ_X eine Isogenie, insbesondere $\hat{T}$ auch eine abelsche Varietät.*

FOLGERUNG 11. *Für eine abelsche Varietät T gilt:*

1. *Für Divisoren X und Y gilt:*

$$\phi_X = \phi_Y \quad \Longleftrightarrow \quad E_X = E_Y \quad \Longleftrightarrow \quad X \text{ und } Y \text{ haben das gleiche Bild in } NS(T).$$

2. *Die durch 1. induzierte Abbildung*

$$NS(T) \to Hom(T, \hat{T}), \quad X \mapsto \phi_X$$

ist ein injektiver Gruppenhomomorphismus. Wir schreiben auch ϕ_E statt ϕ_X.

3. *Mit der Identifikation $\hat{\hat{T}} = T$ gilt*

$$\hat{\phi_X} = \phi_X.$$

Beweis: 1. Dies folgt sofort aus $\rho_a(\phi_X) = -H^t$.
2. Dies folgt aus 1. mit der analytischen Darstellung.
3. Dies ergibt sich aus

$$\rho_a(\hat{\phi_X}) = \overline{\rho_a(\phi_X)}^t = \overline{-H^t}^t = -H^t = \rho_a(\phi_X). \quad \blacksquare$$

Bemerkung: Ist E eine nichtausgeartete Riemannsche Form vom Typ $(d_1, \ldots, d_n)$, so sagt man, E definiert eine Polarisierung vom Typ $(d_1, \ldots, d_n)$. Hat E Typ $(1, \ldots, 1)$, so sagt man, E definiert eine Prinzipalpolarisierung. Für eine prinzipalpolarisierte abelsche Varietät T gilt also $T \simeq \hat{T}$.

KAPITEL 7

Endomorphismenringe abelscher Varietäten

Sei im folgenden $T = \mathbf{C}^n/\Lambda$ eine abelsche Varietät. Wir haben die analytische und rationale Darstellung

$$\rho_a : End(T) \hookrightarrow M_n(\mathbf{C}), \quad \rho_r : End(T) \hookrightarrow M_{2n}(\mathbf{Z})$$

und damit

$$\rho_a : End_{\mathbf{Q}}(T) \hookrightarrow M_n(\mathbf{C}), \quad \rho_r : End_{\mathbf{Q}}(T) \hookrightarrow M_{2n}(\mathbf{Q}).$$

Insbesondere ist $End_{\mathbf{Q}}(T)$ ein $\mathbf{Q}$-Vektorraum der Dimension $\leq 4n^2$.

1. Die Rosati-Involution

Sei E eine nichtausgeartete Riemannsche Form bzgl. der abelschen Varietät $T = \mathbf{C}^n/\Lambda$. Dann ist

$$\phi_E : T \to \hat{T}$$

eine Isogenie, d.h. es gibt eine Isogenie $\psi : \hat{T} \to T$, eine natürliche Zahl m mit

$$\phi_E \psi = m, \quad \psi \phi_E = m.$$

(Man kann $m = pf(E)^2$ wählen.) Wir setzen

$$\phi_E^{-1} = \frac{1}{m}\psi \in Hom_{\mathbf{Q}}(\hat{T}, T).$$

DEFINITION 19. *Definiert man für $\alpha \in End(T)$*

$$\alpha' = \phi_X^{-1} \hat{\alpha} \phi_X \in End_{\mathbf{Q}}(T),$$

so induziert dies eine Abbildung

$$' : End_{\mathbf{Q}}(T) \to End_{\mathbf{Q}}(T),$$

die als Rosati-Involution bezeichnet wird. (Sie hängt von E ab.)

Durch einfaches Einsetzen ergibt sich:

LEMMA 43. *Für die Rosati-Involution gilt:*

$$(\alpha + \beta)' = \alpha' + \beta', \quad (\alpha\beta)' = \beta'\alpha', \quad \alpha'' = \alpha, \quad (r\alpha)' = r\alpha', r \in \mathbf{Q}.$$

LEMMA 44. *Schreibt man $H(x, y) = x^t H y$ mit einer hermiteschen Matrix H, und ist $A = \rho_a(\alpha)$, so gilt*

$$\rho_a(\alpha') = H^{t-1}\overline{A}^t H^t.$$

Beweis: Dies folgt sofort aus

$$\rho_a(\alpha') = \rho_a(\phi_E^{-1}\hat{\alpha}\phi_E) = (-H^t)^{-1}\overline{A}^t(-H^t). \quad \blacksquare$$

Beispiel: Ist $\tilde{E} = \mathbf{C}/\Lambda$ mit $\Lambda = \mathbf{Z} + \mathbf{Z}\tau$, so war

$$H(x, y) = \frac{1}{Im(\tau)} x\overline{y}$$

die hermitesche Form einer Riemannschen Form für $\tilde{E}$. H wird also durch die komplexe Zahl $\frac{1}{Im(\tau)}$ beschreiben. Denken wir uns $End_{\mathbf{Q}}(\tilde{E}) \subseteq \mathbf{C}$ über die analytische Darstellung, so folgt, daß die Rosati-Involution die komplexe Konjugation ist.

Beispiel: Seien $E_i = \mathbf{C}/\Lambda_i$ mit $\Lambda_i = \mathbf{Z} + \mathbf{Z}\tau_i$ elliptische Kurven. Wir betrachten $E_1 \times E_2$ als $\mathbf{C}^2/\Lambda$ mit der Periodenmatrix

$$\begin{pmatrix} 1 & \tau_1 & 0 & 0 \\ 0 & 0 & 1 & \tau_2 \end{pmatrix}.$$

Die natürliche hermitesche Form, die von der Produktstruktur kommt, ist

$$H(x,y) = x^t \begin{pmatrix} \frac{1}{Im(\tau_1)} & 0 \\ 0 & \frac{1}{Im(\tau_2)} \end{pmatrix} \overline{y}.$$

Wir unterscheiden zwei Fälle:
E_1 **und** E_2 **sind nicht isogen:** Dann ist $Hom(E_1, E_2) = Hom(E_2, E_1) = 0$, die Endomorphismen von $E_1 \times E_2$ sind also in der analytischen Darstellung

$$End(E_1 \times E_2) = \left\{ \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} : \alpha_i \in End(E_i) \right\},$$

so daß

$$End_{\mathbf{Q}}(E_1 \times E_2) = End_{\mathbf{Q}}(E_1) \oplus End_{\mathbf{Q}}(E_2)$$

und die Rosati-Involution operiert auf den einzelnen Teilen wieder durch komplexe Konjugation.
E_1 **und** E_2 **sind isogen:** O.E. nehmen wir $E_1 = E_2 = E$ an, da uns nur $End_{\mathbf{Q}}(E_1 \times E_2)$ interessiert. Dann ist

$$H(x,y) = \frac{1}{Im(\tau)} x^t I \overline{y},$$

wo I die Einheitsmatrix bezeichnet. Ist $K = End_{\mathbf{Q}}(E)$, so ist

$$End_{\mathbf{Q}}(E) = M_2(K) \subseteq M_2(\mathbf{C}).$$

Die Rosati-Involution ist durch

$$A \mapsto \overline{A}^t$$

gegeben.

LEMMA 45. *Für $A = \rho_a(\alpha)$ und $A' = \rho_a(\alpha')$ gilt:*

$$H(Ax, y) = H(x, A'y).$$

Beweis: Wir schreiben $H(x,y) = x^t H \overline{y}$ mit H als hermitescher Matrix, d.h. $H^t = \overline{H}$. Einerseits gilt

$$\begin{aligned} H(Ax,y) &= (Ax)^t H \overline{y} = x^t A^t H \overline{y}, \\ H(x,A'y) &= x^t H \overline{A'} \overline{y} = x^t H \cdot \overline{H}^{t-1} A^t \overline{H}^t \overline{y} = \\ &= x^t H H^{-1} A^t H \overline{y} = x^t A^t H \overline{y}. \quad \blacksquare \end{aligned}$$

FOLGERUNG 12. *Für $\alpha \in End_{\mathbf{Q}}(T)$ mit $\alpha \neq 0$ gilt:*

$$Sp(\rho_a(\alpha\alpha')) > 0.$$

Also insbesondere $Sp(\rho_a(\alpha\alpha')) \in \mathbf{R}$.

Beweis: Wir schreiben wieder $A = \rho_a(\alpha)$ und $A' = \rho_a(\alpha')$. Ist $A \neq 0$, so auch $A' \neq 0$, also gibt es $e_1 \in \mathbf{C}^n$ mit $A'e_1 \neq 0$. Wir können (nach Strecken von e_1) ein Orthonormalbasis $e_1, \ldots, e_n$ konstruieren, d.h. $H(e_i, e_j) = \delta_{ij}$. Sei

$$AA'e_i = \sum_j a_{ij} e_j.$$

Dann ist

$$a_{ii} = H(AA'e_i, e_i) = H(A'e_i, A'e_i) \geq 0 \text{ und } a_{11} > 0.$$

Daher ist

$$Sp(AA') = a_{11} + \cdots + a_{nn} > 0,$$

insbesondere eine reelle Zahl. $\blacksquare$

LEMMA 46. *Für $\alpha \in End_{\mathbf{Q}}(T)$ gilt:*

$$Sp(\rho_r(\alpha)) = 2 \cdot Re(Sp(\rho_a(\alpha))).$$

Beweis: Sei $e_1, \ldots, e_n \in \mathbf{C}^n$ eine $\mathbf{C}$-Basis von $\mathbf{C}^n$ und $u_1, \ldots, u_{2n}$ eine Gitterbasis von Λ. Gilt

$$\alpha e_j = \sum_k a_{jk} e_k, a_{jk} \in \mathbf{C} \text{ und } \alpha u_j = \sum_k d_{jk} u_k, d_{jk} \in \mathbf{Q},$$

so ist

$$Sp(\rho_a(\alpha)) = a_{11} + \cdots + a_{nn} \text{ und } Sp(\rho_r(\alpha)) = d_{11} + \cdots + d_{nn}.$$

Nun ist $u_1, \ldots, u_{2n}$ eine $\mathbf{R}$-Basis von $\mathbf{C}^n$. Wir können also $Sp(\rho_r(\alpha))$ auch nach $\mathbf{R}$-Basiswechsel berechnen. Wir wählen als neue $\mathbf{R}$-Basis $e_1, \ldots, e_n, ie_1, \ldots, ie_n$. Zerlegt man $a_{jk} = b_{jk} + ic_{jk}$ mit $b_{jk}, c_{jk} \in \mathbf{R}$, so gilt

$$\begin{aligned} \alpha e_j &= \sum_k b_{jk} e_k + \sum_k c_{jk} ie_k, \\ \alpha ie_j &= \sum_k b_{jk} ie_k - \sum_k c_{jk} e_k, \end{aligned}$$

so daß gilt

$$Sp(\rho_r(\alpha)) = \sum_j (b_{jj} + b_{jj}) = 2 \cdot Re(Sp(\rho_a(\alpha))). \quad \blacksquare$$

Daher folgt sogleich:

FOLGERUNG 13. *Für $\alpha \in End_{\mathbf{Q}}(T)$ mit $\alpha \neq 0$ gilt:*

$$Sp(\rho_r(\alpha\alpha')) > 0.$$

Die Spur ist hier jedenfalls eine rationale Zahl.

Wir definieren weiter, wobei E wie zuvor fest gegeben ist:

$$\varphi : NS(T) \to End_{\mathbf{Q}}(T), \quad \tilde{E} \mapsto \phi_E^{-1} \phi_{\tilde{E}}.$$

Es gilt

$$\rho_a(\varphi(\tilde{E})) = (-H^t)^{-1}(-\tilde{H}^t) = H^{t-1}\tilde{H}^t.$$

Dies setzt sich natürlich zu einer Abbildung $\varphi : NS_{\mathbf{Q}}(T) \to End_{\mathbf{Q}}(T)$ fort. Die analytische Darstellung zeigt: φ ist injektiver $\mathbf{Q}$-Vektorraumhomomorphismus. Nun gilt:

$$\begin{aligned} \rho_a(\varphi(\tilde{E})') &= H^{t-1}\overline{(\tilde{H}H^{-1})}H^t = H^{t-1}\tilde{H}^t H^{t-1} H^t = \\ &= H^{t-1}\tilde{H}^t = \rho_a(\varphi(\tilde{E})), \end{aligned}$$

d.h.

$$\varphi(\tilde{E})' = \varphi(\tilde{E}),$$

die Bilder unter φ sind also symmetrisch bzgl. der Rosati-Involution. Wir setzen

$$End^s_{\mathbf{Q}}(T) = \{\alpha \in End_{\mathbf{Q}}(T) : \alpha' = \alpha\}.$$

Wir wollen jetzt eine Abbildung $\psi : End^s_{\mathbf{Q}}(T) \to NS_{\mathbf{Q}}(T)$ definieren. Sei $\alpha \in End^s_{\mathbf{Q}}(T)$ und zunächst $\alpha \in End(T)$. Dann gilt für $A = \rho_a(\alpha)$

$$H(Ax, y) = H(x, Ay)$$

und damit für den Imaginärteil:

$$E(Ax, y) = E(x, Ay).$$

Sei

$$\tilde{E}(x, y) = E(Ax, y).$$

Wir zeigen, daß $\tilde{E} \in NS(T)$ ist:

- Wegen $A\Lambda \subseteq \Lambda$ nimmt auch $\tilde{E}$ auf Λ ganzzahlige Werte an.
- Natürlich ist $\tilde{E}$ $\mathbf{R}$-bilinear. Außerdem gilt:

  $$\tilde{E}(y, x) = E(Ay, x) = E(y, Ax) = -E(Ax, y) = -\tilde{E}(x, y),$$

  d.h. $\tilde{E}$ ist alternierend.

- $$\tilde{E}(ix,y) = E(Aix,y) = E(iAx,y) = E(iy,Ax) = E(Aiy,x) = \tilde{E}(iy,x),$$
  woraus schließlich die Behauptung folgt.

Wir definieren

$$\psi : End^s_{\mathbf{Q}}(T) \to NS_{\mathbf{Q}}(T), \quad \alpha \mapsto E(\rho_r(\alpha)x,y),$$

wie eben.

SATZ 33. *φ und ψ sind invers zueinander, d.h.*

$$NS_{\mathbf{Q}}(T) \simeq End^s_{\mathbf{Q}}(T).$$

Beweis: $\psi\varphi$: Wir gehen aus von $\tilde{E}$ bzw. $\tilde{H}$ mit $\tilde{E} = Im(\tilde{H})$ und berechnen das Bild unter $\psi\varphi$: Es ist

$$\rho_a(\phi_E^{-1}\phi_{\bar{E}}) = H^{t-1}\tilde{H}^t,$$

also ist

$$\begin{aligned} \psi\varphi(\tilde{E})(x,y) &= E(H^{t-1}\tilde{H}^t x,y) = ImH(H^{t-1}\tilde{H}^t x,y) = \\ &= Im(H^{t-1}\tilde{H}^t x)^t H\overline{y} = Im(x^t\tilde{H}H^{-1}H\overline{y}) = Im\tilde{H}(x,y) = \tilde{E}(x,y), \end{aligned}$$

also folgt $\psi\varphi = id$.
$\varphi\psi$: Sei $\alpha = \alpha'$ und $A = \rho_a(\alpha)$. Dann ist $\psi(\alpha) = \tilde{E}$ mit

$$\tilde{E}(x,y) = E(Ax,y).$$

Die zugehörige hermitesche Form ist

$$\tilde{H}(x,y) = \tilde{E}(ix,y) + i\tilde{E}(x,y) = E(iAx,y) + iE(Ax,y) = H(Ax,y) = (Ax)^t H\overline{y} = x^t A^t H\overline{y},$$

damit ist

$$\rho_a(\varphi(\tilde{E})) = H^{t-1}\tilde{H}^t = H^{t-1}H^t A = A,$$

woraus sofort $\varphi\psi = id$ folgt. ■

Wir geben noch eine Anwendung obiger Abbildung $\psi : End^s_{\mathbf{Q}}(T) \to NS_{\mathbf{Q}}(T)$ an:

LEMMA 47. *Sei T einfache abelsche Varietät. Ist $\alpha \in End_{\mathbf{Q}}(T)$ mit $\alpha' = \alpha$, so genügt α einem Polynom mit rationalen Koeffizienten vom Grad $\leq n$.*

Beweis: Sei $u_1, \ldots, u_{2n}$ eine Gitterbasis von Λ. Wir betrachten jetzt alle Matrizen bzgl. dieser Basis. Sei $E(x,y) = x^t Ey$ mit E als alternierender $2n \times 2n$-Matrix. Sei $A = \rho_r(\alpha)$. Dann ist

$$E(Ax,y) = (Ax)^t Ey = x^t A^t Ey$$

alternierend, also $A^t E$ eine alternierende $2n \times 2n$-Matrix. Die Matrix $(tI - A)^t E$ ist also auch alternierend mit Koeffizienten in $\mathbf{Q}[t]$. Die Determinante ist ein Quadrat, d.h. es gibt ein $f \in \mathbf{Q}[t]$ mit

$$\det((tI - A)^t E) = f(t)^2.$$

Mit $\det(E) = c^2$, $c \in \mathbf{Q}$ folgt

$$\det(tI - A) = (\frac{1}{c}f(t))^2.$$

Da α sein charakteristisches Polynom erfüllt, folgt

$$f(\alpha)f(\alpha) = 0$$

und da T einfach, also $End_{\mathbf{Q}}(T)$ Schiefkörper ist: $f(\alpha) = 0$, was behauptet war. ■

Damit erhalten wir nochmals einen Satz, den wir schon kennen:

SATZ 34. *Für eine elliptische Kurve E ist $End_{\mathbf{Q}}(E)$ ein imaginärquadratischer Zahlkörper $\mathbf{Q}(\sqrt{-d})$, $d \in \mathbf{N}$ quadratfrei, oder der Körper der rationalen Zahlen $\mathbf{Q}$. Ist $End_{\mathbf{Q}}(E) \neq \mathbf{Q}$, so sagen wir, E hat komplexe Multiplikation.*

Beweis: Sei $K = End_{\mathbf{Q}}(E)$. Über die analytische Darstellung ist $K \subseteq \mathbf{C}$. Der Fixkörper der Rosati-Involution ist nach dem letzten Lemma $\mathbf{Q}$. Die Rosati-Involution hat Ordnung 1 oder 2, also ist $K = \mathbf{Q}$ oder $[K : \mathbf{Q}] = 2$. Ist $[K : \mathbf{Q}] = 2$, so operiert die Rosati-Involution nichttrivial und durch komplexe Konjugation, also folgt die Behauptung. ■

Wir wenden jetzt obige Sätze an:

SATZ 35. *Für elliptische Kurven E_1, E_2 gilt für $NS(E_1 \times E_2)$:*

$$Rang(NS(E_1 \times E_2)) = \begin{cases} 2, \text{ falls } E_1 \text{ und } E_2 \text{ nicht isogen sind,} \\ 3, \text{ falls } E_1 \text{ und } E_2 \text{ isogen sind, aber ohne komplexe Multiplikation,} \\ 4, \text{ falls } E_1 \text{ und } E_2 \text{ isogen sind, aber mit komplexer Multiplikation.} \end{cases}$$

Beweis: Wir benutzen den Satz

$$NS_{\mathbf{Q}}(E_1 \times E_2) \simeq End^s_{\mathbf{Q}}(E_1 \times E_2).$$

Sind E_1, E_2 nicht isogen, so ist $End_{\mathbf{Q}}(E_1 \times E_2) = End_{\mathbf{Q}}(E_1) \oplus End_{\mathbf{Q}}(E_2)$, die Rosati-Involution operiert durch komplexe Konjugation, so daß ein 2-dimensionaler $\mathbf{Q}$-Vektorraum bleibt. Sind E_1 und E_2 isogen, $K = End_{\mathbf{Q}}(E_i)$, so ist

$$End_{\mathbf{Q}}(E_1 \times E_2) = M_2(K) \subseteq M_2(\mathbf{C}).$$

Die Rosati-Involution operiert als $A \mapsto \overline{A}^t$. Ist $K = \mathbf{Q}$, so sind die symmetrischen Matrizen Rosati-invariant; sie bilden einen 3-dimensionalen Vektorraum. Ist K imaginärquadratisch, so sind die hermitischen Matrizen in $M_2(K)$ Rosati-invariant; sie bilden einen $\mathbf{Q}$-Vektorraum der Dimension 4. ■Wir wollen

im folgenden $End_{\mathbf{Q}}(T)$ für $\dim T = 1, 2$ betrachten.

2. Elliptische Kurven

Ist E eine elliptische Kurve, so ist also $End_{\mathbf{Q}}(E)$ ein imaginärquadratischer Zahlkörper oder $\mathbf{Q}$, wie wir eben gesehen haben. Im letzten Semester haben wir die Endomorphismenringe ausgerechnet sogar explizit bestimmt. Wir zitieren das Ergebnis:

SATZ 36. *Ist E eine elliptische Kurve, so ist $End(E) = \mathbf{Z}$ oder es gibt eine quadratfreie natürliche Zahl d, eine natürliche Zahl f mit*

$$End(E) = \left\{ \begin{array}{cc} \mathbf{Z}[f\sqrt{-d}] & \text{für } d \equiv 1, 2 \bmod 4, \\ \mathbf{Z}[f\frac{1+\sqrt{-d}}{2}] & \text{für } d \equiv 3 \bmod 4. \end{array} \right\}$$

Obige Ringe $\neq \mathbf{Z}$ werden umgekehrt endlich oft als Endomorphismenringe elliptischer Kurven realisiert.

3. Abelsche Flächen

Ist $A = \mathbf{C}^2/\Lambda$ eine nichteinfache abelsche Fläche, so ist A isogen zu einem Produkt elliptischer Kurven $E_1 \times E_2$. In diesem Fall kennen wir bereits $End_{\mathbf{Q}}(E_1 \times E_2)$ und $Rang(NS(E_1 \times E_2))$. Wir können also im folgenden annehmen, daß A einfach ist und damit $End_{\mathbf{Q}}(A)$ ein Schiefkörper.

LEMMA 48. *Ist A eine einfache abelsche Fläche, so gilt für $D = End_{\mathbf{Q}}(A)$:*

$$\dim_{\mathbf{Q}}(D) \in \{1, 2, 4\}.$$

Beweis: $End(A)$ operiert auf Λ, d.h. Λ ist ein $End(A)$-Modul. Also ist $\mathbf{Q} \otimes \Lambda$ ein $D = End_{\mathbf{Q}}(A)$-Vektorraum. Damit gilt

$$4 = \dim_{\mathbf{Q}} \mathbf{Q} \otimes \Lambda = \dim_D \mathbf{Q} \otimes \Lambda \cdot \dim_{\mathbf{Q}} D,$$

woraus sofort die Behauptung folgt. ■

Wir unterscheiden jetzt zunächst, ob $End_{\mathbf{Q}}(A)$ kommutativ ist oder nicht.

4. Quaternionenmultiplikation

Sei D ein Schiefkörper mit $\mathbf{Q} \subseteq D$. Ist $\dim_{\mathbf{Q}}(D) = 1$, so ist $D = \mathbf{Q}$. Ist $\dim_{\mathbf{Q}}(D) = 2$ und $\alpha \in D \setminus \mathbf{Q}$, so ist $D = \mathbf{Q}(\alpha) = \mathbf{Q} + \mathbf{Q}\alpha$ und damit D kommutativ. Soll also $End_{\mathbf{Q}}(A)$ nichtkommutativ sein, A einfach, so muß $\dim_{\mathbf{Q}} End_{\mathbf{Q}}(A) = 4$ gelten.

Überlegungen: Sei A einfache abelsche Fläche und $D = End_{\mathbf{Q}}(A)$ ein nichtkommutativer Schiefkörper. Dann ist $\mathbf{Q} \subseteq D$ und $\dim_{\mathbf{Q}}(D) = 4$. Weiter hat man (nach Wahl einer nichtausgearteten Riemannschen Form) eine Rosati-Involution. Außerdem benutzen wir die analytische Darstellung $\rho_a : D \hookrightarrow M_2(\mathbf{C})$.

1. Ist $\alpha \in D \setminus \mathbf{Q}$, so ist
$$K = \mathbf{Q}(\alpha) = \mathbf{Q} + \mathbf{Q}\alpha + \mathbf{Q}\alpha^2 + \mathbf{Q}\alpha^3 \subseteq D$$
ein (kommutativer) Körper, also folgt $[K : \mathbf{Q}] = 2$, d.h. α ist quadratisch über $\mathbf{Q}$. Dann gibt es $\tilde{\alpha}$ mit
$$K = \mathbf{Q}(\alpha) = \mathbf{Q}(\tilde{\alpha})$$
und
$$\tilde{\alpha}^2 = a \in \mathbf{Q}^\times \setminus \mathbf{Q}^{\times 2}.$$
2. Sei jetzt $K = \mathbf{Q}(\alpha)$ ein quadratischer Teilkörper von D mit $\alpha^2 = a \in \mathbf{Q}$. Da K über $\mathbf{Q}$ galoissch ist, liefert die Rosati-Involution einen Automorphismus von K über $\mathbf{Q}$. Es gibt jetzt zwei Fälle:
Fall $'|K = id_K$: Dann ist
$$2a = Sp(\rho_a(a)) = Sp(\rho_a(\alpha^2)) = Sp(\rho_a(\alpha\alpha')) > 0,$$
also $a > 0$ und damit K reellquadratisch.
Fall $'|K \neq id_K$: Dann ist $\alpha' = -\alpha$ und damit
$$-2a = Sp(\rho_a(-a)) = Sp(\rho_a(-\alpha^2)) = Sp(\rho_a(\alpha\alpha')) > 0,$$
also $a < 0$ und damit K imaginärquadratisch.
3. Wir wählen jetzt ein $\alpha \in D \setminus \mathbf{Q}$ mit $\alpha^2 = a \in \mathbf{Q}$. Dann ist $\mathbf{Q}(\alpha) \neq D$. Wir wählen ein $\tilde{\beta} \in D \setminus \mathbf{Q}(\alpha)$. Dann ist $\mathbf{Q}(\tilde{\beta})$ quadratisch über $\mathbf{Q}$ und $\mathbf{Q}(\alpha) \cap \mathbf{Q}(\tilde{\beta}) = \mathbf{Q}$. Wie zuvor finden wir $\beta \in D$ mit $\mathbf{Q}(\tilde{\beta}) = \mathbf{Q}(\beta)$ und $\beta^2 = b \in \mathbf{Q}$.
4. Wir zeigen zunächst:
$$D = \mathbf{Q} + \mathbf{Q}\alpha + \mathbf{Q}\beta + \mathbf{Q}\alpha\beta,$$
wobei die Summe aus Dimenionsgründen direkt ist.
Beweis: Wir zeigen, daß $1, \alpha, \beta, \alpha\beta$ linear unabhängig über $\mathbf{Q}$ sind: Seien $x, y, z, t \in \mathbf{Q}$ mit
$$x + y\alpha + z\beta + t\alpha\beta = 0.$$
Dann ist
$$\beta(z + t\alpha) = -x - y\alpha.$$
Wäre $z + t\alpha \neq 0$, so wäre $\beta \in \mathbf{Q}(\alpha)$, was nicht geht, also ist $z + t\alpha = 0$ und damit $z = t = 0$ und damit auch $x = y = 0$. ■

5. Die Abbildung
$$\sigma : D \to D, \quad \lambda \mapsto \alpha^{-1}\lambda\alpha$$
ist ein Körperautomorphismus von D. Da $\mathbf{Q}(\beta)$ galoissch ist über $\mathbf{Q}$, ist $\sigma|_{\mathbf{Q}(\beta)}$ ein Körperautomorphismus von $\mathbf{Q}(\beta)$. Es gibt jetzt zwei Möglichkeiten:
Angenommen $\sigma|_{\mathbf{Q}(\beta)} = id_{\mathbf{Q}(\beta)}$: Dann ist
$$\beta = \alpha^{-1}\beta\alpha,$$
also $\alpha\beta = \beta\alpha$ und damit wegen $D = \mathbf{Q} + \mathbf{Q}\alpha + \mathbf{Q}\beta + \mathbf{Q}\alpha\beta$ der Schiefkörper D kommutativ, ein Widerspruch zur Voraussetzung. Dieser Fall kann also nicht auftreten. Es muß also gelten $\sigma|_{\mathbf{Q}(\beta)} \neq id_{\mathbf{Q}(\beta)}$ und damit
$$\alpha^{-1}\beta\alpha = -\beta,$$
was
$$\beta\alpha = -\alpha\beta$$

liefert. Damit folgt auch

$$(\alpha\beta)^2 = \alpha\beta\alpha\beta = -\alpha^2\beta^2 = -ab.$$

6. Die obigen Aussagen über die Rosati-Involution lassen sich so formulieren:

$$\alpha' = sgn(a)\alpha, \quad \beta' = sgn(b)\beta.$$

Damit folgt

$$(\alpha\beta)' = \beta'\alpha' = sgn(ab)\beta\alpha = -sgn(ab)\alpha\beta,$$

so daß sich insgesamt ergibt:

$$(t + x\alpha + y\beta + z\alpha\beta)' = t + x \cdot sgn(a)\alpha + y \cdot sgn(b)\beta - z \cdot sgn(ab)\alpha\beta.$$

Damit läßt sich leicht $End^s_{\mathbf{Q}}(A)$ und somit $NS_{\mathbf{Q}}(A)$ ausrechnen. Wir erhalten folgende Tabelle:

	$End^s_{\mathbf{Q}}(A)$	$Rang(NS(A))$
$a > 0, b > 0$	$\{t + x\alpha + y\beta : t, x, y \in \mathbf{Q}\}$	3
$a > 0, b < 0$	$\{t + x\alpha + z\alpha\beta : t, x, z \in \mathbf{Q}\}$	3
$a < 0, b > 0$	$\{t + y\beta + z\alpha\beta : t, y, z \in \mathbf{Q}\}$	3
$a < 0, b < 0$	$\{t : t \in \mathbf{Q}\}$	1

DEFINITION 20. *Für $a, b \in \mathbf{Q}^\times$ definiert man eine 4-dimensionale $\mathbf{Q}$-Algebra $Q_{a,b}$ durch die Vorschriften*

$$Q_{a,b} = \mathbf{Q} + \mathbf{Q}\alpha + \mathbf{Q}\beta + \mathbf{Q}\alpha\beta$$

mit

$$\alpha^2 = a, \quad \beta^2 = b \quad \beta\alpha = -\alpha\beta.$$

(Dann ist $(\alpha\beta)^2 = -ab$.) Man nennt $Q_{a,b}$ eine Quaternionenalgebra.

LEMMA 49. *In $Q_{a,b}$ gilt mit $x, y, z, t \in \mathbf{Q}$:*

$$\begin{aligned}(x\alpha + y\beta + z\alpha\beta)^2 &= ax^2 + by^2 - abz^2,\\ (t + x\alpha + y\beta + z\alpha\beta)^2 &= t^2 + ax^2 + by^2 - abz^2 + 2t(x\alpha + y\beta + z\alpha\beta),\\ (t + x\alpha + y\beta + z\alpha\beta)(t - x\alpha - y\beta - z\alpha\beta) &= t^2 - ax^2 - by^2 + abz^2.\end{aligned}$$

Beweis: durch einfaches Ausrechnen. ■

SATZ 37. *Die Quaternionenalgebra $Q_{a,b}$ ist genau dann ein Schiefkörper, wenn die quadratische Gleichung*

$$t^2 - ax^2 - by^2 + abz^2 = 0$$

nur trivial über $\mathbf{Q}$ lösbar ist. Ist $Q_{a,b}$ kein Schiefkörper, so gilt $Q_{a,b} \simeq M_2(\mathbf{Q})$.

Beweis: Gibt es $x, y, z, t \in \mathbf{Q}$ nicht alle 0 mit $t^2 - ax^2 - by^2 + abz^2 = 0$, so hat nach der dritten Formel $Q_{a,b}$ Nullteiler, kann also kein Schiefkörper sein. Sei jetzt umgekehrt $t^2 - ax^2 - by^2 + abz^2 = 0$ nur trivial lösbar. Sind $x, y, z, t \in \mathbf{Q}$ nicht alle 0, so ist

$$(t + x\alpha + y\beta + z\alpha\beta)^{-1} = \frac{1}{t^2 - ax^2 - by^2 + abz^2}(t - x\alpha - y\beta - z\alpha\beta),$$

also $Q_{a,b}$ ein Schiefkörper. Wir nehmen jetzt an, daß $Q_{a,b}$ kein Schiefkörper ist. Dann gibt es $t, x, y, z \in \mathbf{Q}$ nicht alle 0 mit $t^2 - ax^2 - by^2 + abz^2 = 0$. Ist a kein Quadrat in $\mathbf{Q}$ ist, so gibt es $u, v \in \mathbf{Q}$ mit

$$b = \frac{t^2 - ax^2}{y^2 - az^2} = u^2 - av^2,$$

da die Norm von $\mathbf{Q}(\sqrt{a})$ nach $\mathbf{Q}$ multiplikativ ist. Ist a Quadrat in $\mathbf{Q}$, so gibt es ebenso $u, v \in \mathbf{Q}$ mit $b = u^2 - av^2$. Wir definieren jetzt

$$A = \begin{pmatrix} 0 & 1 \\ a & 0 \end{pmatrix}, B = \begin{pmatrix} u & v \\ -av & -u \end{pmatrix} \in M_2(\mathbf{Q}).$$

Dann gilt

$$A^2 = a, \quad B^2 = u^2 - av^2 = b, \quad AB = -BA.$$

Damit folgt $Q_{a,b} \simeq M_2(\mathbf{Q})$. ■

Beispiele:

1. Wir betrachten $Q_{5,7}$: Angenommen $f = t^2 - 5x^2 - 7y^2 + 35z^2 = 0$ hat eine nichttriviale Lösung in $\mathbf{Q}^4$. Dann können wir o.E. $t, x, y, z \in \mathbf{Z}$ mit $ggT(t,x,y,z) = 1$ annehmen. Es ist
$$0 \equiv t^2 - 5x^2 \bmod 7,$$
da aber 5 kein Quadrat mod7 ist, folgt $t \equiv x \equiv 0 \bmod 7$. Also $t = 7t_1$, $x = 7x_1$ und damit
$$0 = 7t_1^2 - 35x_1^2 - y^2 + 5z^2,$$
was
$$0 \equiv -y^2 + 5z^2 \bmod 7,$$
also wieder $y \equiv z \equiv 0 \bmod 7$ ergibt. Dies widerspricht $ggT(t,x,y,z) = 1$. Daher ist $Q_{5,7}$ ein Schiefkörper.
2. Was ist mit $Q_{-5,-7}$? Die quadratische Form $f = t^2 + 5x^2 + 7y^2 + 35z^2 = 0$ hat offensichtlich schon über $\mathbf{R}$ nur die triviale Nullstelle, daher auch über $\mathbf{Q}$. Also ist $Q_{-5,-7}$ ein Schiefkörper.
3. Wir betrachten $Q_{5,11}$: Wir müssen $f = t^2 - 5x^2 - 11y^2 + 55z^2$ untersuchen. Durch Probieren findet man $f(7,1,2,0) = 0$, also ist $Q_{5,11}$ kein Schiefkörper.

Die Lösbarkeit obiger Gleichung läßt sich systematisch behandeln. Man erhält den Satz:

SATZ 38. *Die Gleichung $f = t^2 - ax^2 - by^2 + abz^2 = 0$ besitzt genau dann nichttriviale Lösungen über $\mathbf{Q}$, wenn für die Hilbertsymbole gilt*
$$(a,b)_p = 1 \quad \textit{für alle Primzahlen } p \textit{ und } p = \infty.$$

Beweis: Dies beweist man mit der Theorie der quadratischen Formen über $\mathbf{Q}$ [**Serre**]. ■

Wir betrachten jetzt noch die quadratischen Teilkörper von $Q_{a,b}$:

SATZ 39. *Ist $Q_{a,b}$ ein Schiefkörper, so sind die quadratischen Teilkörper von $Q_{a,b}$ die Körper*
$$\mathbf{Q}(\sqrt{ax^2 + by^2 - abz^2}) \quad \textit{für } (x,y,z) \in \mathbf{Q}^3 \setminus \{0\}.$$

Beweis: Ist K ein quadratischer Teilkörper von $Q_{a,b}$, so gibt es ein $\lambda \in K$ mit $\lambda^2 = c$, $c \in \mathbf{Q}^\times \setminus \mathbf{Q}^{\times 2}$. Wir setzen an $\lambda = t + x\alpha + y\beta + z\alpha\beta$. Mit obiger Formel folgt $t = 0$ und $c = ax^2 + by^2 - abz^2$, wie behauptet. Umgekehrt ist $ax^2 + by^2 - abz^2$ nie ein Quadrat $\neq 0$. ■

Auch dies kann man lokal charakterisieren:

SATZ 40. *Sei $Q_{a,b}$ ein Schiefkörper. Für $m \in \mathbf{Z} \setminus \{0\}$ gilt dann*
$$\mathbf{Q}(\sqrt{m}) \subseteq Q_{a,b} \iff m \notin \mathbf{Q}_p^{\times 2} \textit{ für alle Primzahlen } p \textit{ und } p = \infty \textit{ mit } (a,b)_p = -1.$$

Beweis: Dies ergibt sich durch Anwendung entsprechender Sätze aus der Theorie der quadratischen Formen. [**Serre**] ■

Beispiele:

1. Wir betrachten den Schiefkörper $Q_{5,7}$. Die Stellen p mit $(5,7)_p = -1$ sind 5 und 7. Sei nun $m \in \mathbf{Z} \setminus \{0\}$ quadratfrei. Dann ist $m \notin \mathbf{Q}_5 \times 2$ genau dann, wenn $5|m$ oder wenn $(\frac{m}{5}) = -1$, d.h. wenn $m \equiv 0, 2, 3 \bmod 5$. Analog ist $m \notin \mathbf{Q}_7^{\times 2}$ genau dann, wenn $7|m$ oder wenn $(\frac{m}{7}) = -1$, d.h. wenn $m \equiv 0, 3, 5, 6 \bmod 7$. Damit erhält man für quadratfreies $m \in \mathbf{Z} \setminus \{0\}$:
$$\sqrt{m} \in Q_{a,b} \iff m \equiv 0, 3, 5, 7, 10, 12, 13, 17, 20, 27, 28, 33 \bmod 35.$$
Im Bereich $-50 \leq m \leq 50$ sind dies die Zahlen
$$-43, -42, -37, -35, -30, -23, -22, -15, -7, -2, 3, 5, 7, 10, 13, 17, 33, 35, 38, 42, 47.$$
2. Wir betrachten den Schiefkörper $Q_{-5,-7}$. Die Stellen p mit $(-5,-7)_p = -1$ sind $p = 5$ und $p = \infty$. Sei jetzt $m \in \mathbf{Z}$ quadratfrei. Dann ist $m \notin \mathbf{Q}_5^{\times 2}$ genau dann, wenn $m \equiv 0, 2, 3 \bmod 5$. Es ist $m \notin \mathbf{Q}_\infty^{\times 2} = \mathbf{R}^{\times 2}$ genau dann, wenn $m < 0$ gilt. Also gilt
$$\sqrt{m} \in Q_{-5,-7} \iff m < 0 \text{ und } m \equiv 0, 2, 3 \bmod 5.$$
Im Bereich $-50 \leq m \leq -1$ sind dies die Zahlen
$$-2, -3, -5, -7, -10, -13, -15, -17, -22, -23, -30, -33, -35, -37, -38, -42, -43, -47.$$

Bemerkungen:

1. Ist $a,b<0$, so ist $f=t^2-ax^2-by^2+abz^2$ positiv definit, besitzt also keine nichttrivialen Nullstellen über $\mathbf{R}$ und $\mathbf{Q}$, also ist $Q_{a,b}$ ein Schiefkörper. $Q_{a,b}$ heißt definite Quaternionenalgebra. $Q_{a,b}$ enthält nur imaginärquadratische Teilkörper. Außerdem ist $NS(A)\simeq\mathbf{Z}$. $\mathbf{R}\otimes_{\mathbf{Q}}Q_{a,b}$ ist dann die Algebra der Hamiltonschen Quaternionen $\mathbf{H}$.
2. Sei $a>0$ oder $b>0$ und $Q_{a,b}$ Schiefkörper. Die Form $f=t^2-ax^2-by^2+abz^2$ ist indefinit, $Q_{a,b}$ heißt indefinite Quaternionenalgebra. $Q_{a,b}$ enthält reell- und imaginärquadratische Teilkörper. Dann ist $NS(A)\simeq\mathbf{Z}^3$. Es ist $\mathbf{R}\otimes_{\mathbf{Q}}Q_{a,b}\simeq M_2(\mathbf{R})$. Mit obigem Beweis findet man Matrizen $A,B\in M_2(\mathbf{R})$ mit $A^2=a,B^2=b,AB=-BA$, so daß man eine Darstellung
$$\rho: Q_{a,b}\hookrightarrow M_2(\mathbf{R})$$
erhält.

Nun gelten die Sätze:

SATZ 41. *Eine definite Quaternionenalgebra $Q_{a,b}$ kann nicht als $End_{\mathbf{Q}}(A)$ einer abelschen Fläche realisiert werden.*

Beweis: [**Shimura**], [**LB**] ■

Aufgabe: Beweise dies elementar.

SATZ 42. *Sei $Q_{a,b}$ eine indefinite Quaternionenalgebra (und Schiefkörper) und*
$$\rho: Q_{a,b}\hookrightarrow M_2(\mathbf{R})$$
eine reelle Darstellung. Ist dann $\mathfrak{a}$ ein Gitter in $Q_{a,b}$, $u=(u_1u_2)^t\in\mathbf{C}^2$ mit $u_1u_2\neq 0$ und $Im(\frac{u_1}{u_2})\neq 0$, so ist
$$\Lambda=\rho(\mathfrak{a})u$$
ein Gitter in $\mathbf{C}^2$ und $A=\mathbf{C}^2/\Lambda$ eine abelsche Fläche mit
$$End_{\mathbf{Q}}(A)=Q_{a,b}.$$
(Insbesondere ist $NS(A)\simeq\mathbf{Z}^3$.) Umgekehrt entsteht jede abelsche Fläche mit Quaternionenmultiplikation auf diese Weise.

Beweis: [**LangAAF**]. ■

5. Komplexe Multiplikation

Sei A eine einfache abelsche Fläche und $K=End_{\mathbf{Q}}(A)$ ein Körper mit $[K:\mathbf{Q}]=4$. Die Rosati-Involution ist ein Automorphismus von K der Ordnung 1 oder 2. Für den Fixkörper $K_0=\{\alpha\in K:\alpha'=\alpha\}$ gilt also $[K:K_0]\in\{1,2\}$. Andererseits wissen wir, daß alle Elemente von K_0 Grad ≤ 2 über $\mathbf{Q}$ haben. Aus $4=[K:\mathbf{Q}]=[K:K_0][K_0:\mathbf{Q}]\leq 2\cdot 2$ folgt dann sofort
$$[K:K]=2\quad\text{ und }\quad[K_0:\mathbf{Q}]=2.$$
Nun ist $K_0=\mathbf{Q}(\delta)$ mit $\delta^2=d$ und $d\in\mathbf{Z}$ quadratfrei $\neq 0,1$. Wegen $2d=Sp(\rho_a(d))=Sp(\rho_a(\delta^2))=Sp(\rho_a(\delta\delta'))>0$ folgt $d>0$, d.h. $K_0=\mathbf{Q}(\sqrt{d})$ ist reellquadratisch.

Sei $\alpha\in K$ mit $K=\mathbf{Q}(\alpha)$. Ist $f=x^4-a_1x^3+a_2x^2-a_3x+a_4$ das Minimalpolynom von α mit $a_1,\ldots,a_4\in\mathbf{Q}$ und
$$f=(x-\alpha_1)\ldots(x-\alpha_4),$$
so erhält man durch
$$\sigma_i: K\hookrightarrow\mathbf{C},\quad\alpha\mapsto\alpha_i$$
die komplexen Einbettungen von K. Das charakteristische Polynom von $\rho_r(\alpha)$ hat ebenfalls Grad 4 und α als Nullstelle, also ist es f. Sei nun $g(x)$ das charakteristische Polynom von $\rho_a(\alpha)$. Dann gilt die wichtige Aussage
$$f(x)=g(x)\overline{g(x)}$$

(Beweis als Übung). Nach Umnumerieren der α_i folgt also

$$g(x) = (x - \alpha_1)(x - \alpha_2) \text{ und } \alpha_3 = \overline{\alpha_1}, \alpha_4 = \overline{\alpha_2}.$$

Da $f(x)$ separabel ist, sind alle Zahlen

$$\alpha_1, \overline{\alpha_1}, \alpha_2, \overline{\alpha_2}$$

paarweise verschieden, insbesondere ist K total komplex, d.h. kein α_i ist reell.

Da $g(x)$ separabel ist, erhält man nach Basiswechsel in $\mathbf{C}^2$:

$$\rho_a(\alpha) = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix}.$$

Da α den Körper K über $\mathbf{Q}$ erzeugt, folgt

$$\rho_a(x) = \begin{pmatrix} \sigma_1(x) & 0 \\ 0 & \sigma_2(x) \end{pmatrix} \text{ für alle } x \in K.$$

Wir haben also $K = \mathbf{Q}(\alpha, \delta)$ mit $\alpha^2 = a + b\sqrt{d}$. Daher gilt

$$a + b\sqrt{d} < 0, \quad a - b\sqrt{d} < 0.$$

Für die Rosati-Involution gilt $\alpha' = -\alpha$, für die komplexe Konjugation ebenso $\overline{\alpha} = -\alpha$, also ist die Rosati-Involution ist die komplexe Konjugation. Damit haben wir insbesondere bewiesen:

SATZ 43. *Ist A eine einfache abelsche Fläche und $K = End_{\mathbf{Q}}(A)$ ein Körper mit $[K : \mathbf{Q}] = 4$, so ist K total imaginär und quadratisch über einem reellquadratischen Zahlkörper, d.h. es gibt $\alpha, \delta \in K$ und $a, b, d \in \mathbf{Z}$ mit*

$$K = \mathbf{Q}(\alpha, \delta), \quad \delta^2 = d, \quad \alpha^2 = a + b\delta$$

und $d > 1$ quadratfrei,

$$a + b\sqrt{d} < 0, \quad a - b\sqrt{d} < 0.$$

Weiter ist $NS(A) \simeq \mathbf{Z}^2$. Man sagt, daß A eine abelsche Fläche mit komplexer Multiplikation ist.

Die Aussage über die Néron-Severigruppe ergibt sich aus der Darstellung

$$K = \mathbf{Q} + \mathbf{Q}\delta + \mathbf{Q}\alpha + \mathbf{Q}\alpha\delta \text{ und } \delta' = \delta, \alpha' = -\alpha.$$

Sei umgekehrt ein total komplexer Zahlkörper K vom Grad 4 über $\mathbf{Q}$ vorgegeben, der einen reellquadratischen Teilkörper enthält. Seien σ_1, σ_2 komplexe Einbettungen von K, die nicht konjugiert komplex sind. Ist dann $\mathfrak{a}$ ein Gitter in K, so ist

$$\Lambda = \{\begin{pmatrix} \sigma_1(x) \\ \sigma_2(x) \end{pmatrix} : x \in \mathfrak{a}\}$$

ein Gitter in $\mathbf{C}^2$ und $A = \mathbf{C}^2/\Lambda$ eine abelsche Fläche mit $End_{\mathbf{Q}}(A) = K$. Dann ist $NS(A) \simeq \mathbf{Z}^2$.

Verallgemeinerung: Ist $A = \mathbf{C}^n/\Lambda$ eine einfache abelsche Varietät der Dimension n und $K = End_{\mathbf{Q}}(A)$ ein (kommutativer) Körper, so ist $\mathbf{Q}\Lambda$ ein K-Vektorraum, also folgt $[K : \mathbf{Q}] | 2n$. Ist K_0 der Fixkörper der Rosati-Involution, so hat man

$$[K : K_0] \leq 2 \quad \text{und } [K_0 : \mathbf{Q}] \leq n.$$

Gilt nun $[K : \mathbf{Q}] = 2n$, so ist K quadratisch über K_0, K total komplex und K_0 total reell. Man sagt dann, A hat komplexe Multiplikation.

Bemerkung: Abelsche Varietäten mit komplexer Multiplikation spielen eine gewisse Rolle in der Zahlentheorie, vgl. [**ST**], [**LangCM**].

6. Reelle Multiplikation

Sei A eine einfache abelsche Fläche, so daß $K = End_{\mathbf{Q}}(A)$ ein quadratischer Zahlkörper ist, d.h. $K = \mathbf{Q}(\delta)$ mit $\delta^2 = d$, $d \in \mathbf{Z} \setminus \{0, 1\}$ quadratfrei. Die Rosati-Involution ist ein Automorphismus von K. Wie früher sieht man $\delta' = sgn(d)\delta$. Es gibt also zwei Möglichkeiten:
Fall $d > 0$: Dann ist K reellquadratisch und $'$ die Identität. $NS(A) \simeq \mathbf{Z}^2$.
Fall $d < 0$: Dann ist K imaginärquadratisch und $'$ die komplexe Konjugation. $NS(A) \simeq \mathbf{Z}$.

SATZ 44. *Es gibt keine abelsche Fläche A, so daß $End_{\mathbf{Q}}(A)$ imaginärquadratischer Zahlkörper ist.*

Beweis: [**Shimura**] ■

Aufgabe: Gib einen elementaren Beweis dieser Tatsache.

Bemerkung: Sei K ein imaginärquadratischer Zahlkörper. Dann gibt es indefinite Quaternionenschiefkörper $Q_{a,b}$ mit $K \subseteq Q_{a,b}$. Ist jetzt A eine abelsche Fläche mit $End_{\mathbf{Q}}(A) = Q_{a,b}$, so gilt natürlich

$$K \subseteq End_{\mathbf{Q}}(A),$$

d.h. $K \subseteq End_{\mathbf{Q}}(A)$ ist möglich, nicht aber $K = End_{\mathbf{Q}}(A)$.

Wir wollen jetzt umgekehrt skizzieren, wie man abelsche Flächen mit reeller Multiplikation konstruiert:

Sei $d \geq 2$ eine quadratfreie natürliche Zahl, $\tau_1, \tau_2 \in \mathbf{C}$ mit $Im(\tau_1), Im(\tau_2) > 0$ und

$$\Lambda = \begin{pmatrix} 1 & \sqrt{d} & \tau_1 & \sqrt{d}\tau_1 \\ 1 & -\sqrt{d} & \tau_2 & -\sqrt{d}\tau_2 \end{pmatrix} \cdot \mathbf{Z}^4.$$

Dann gilt:

- Λ ist ein Gitter in $\mathbf{C}^2$.
- Definiert man
$$R = \{ \begin{pmatrix} a + b\sqrt{d} & 0 \\ 0 & a - b\sqrt{d} \end{pmatrix} : a, b \in \mathbf{Z} \} \simeq \mathbf{Z}[\sqrt{d}],$$
so gilt
$$R \subseteq End(\mathbf{C}^2/\Lambda).$$
- Definiert man
$$H(x, y) = x^t \begin{pmatrix} \frac{1}{Im(\tau_1)} & 0 \\ 0 & \frac{1}{Im(\tau_2)} \end{pmatrix} \overline{y},$$
so ist $E(x, y) = ImH(x, y)$ eine nichtausgeartete Riemannsche Form bzgl. Λ.
- Gilt jetzt $End_{\mathbf{Q}}(A) = \mathbf{Q}(\sqrt{d})$?

Zusammenfassung: Für eine abelsche Fläche A gibt es folgende Möglichkeiten:

- A nicht einfach, d.h. $A \sim E_1 \times E_2$ mit elliptischen Kurven E_1 und E_2:
  - $E_1 \sim E_2$ mit komplexer Multiplikation: $End_{\mathbf{Q}}(A) = M_2(\mathbf{Q}(\sqrt{-d}))$, $NS(A) \simeq \mathbf{Z}^4$.
  - $E_1 \sim E_2$ ohne komplexe Multiplikation: $End_{\mathbf{Q}}(A) = M_2(\mathbf{Q})$ und $NS(A) \simeq \mathbf{Z}^3$.
  - $E_1 \not\sim E_2$: $End_{\mathbf{Q}}(A) = End_{\mathbf{Q}}(E_1) \oplus End_{\mathbf{Q}}(E_2)$, also $\mathbf{Q} \oplus \mathbf{Q}$ oder $\mathbf{Q} \oplus \mathbf{Q}(\sqrt{-d})$ oder $\mathbf{Q}(\sqrt{-d_1}) \oplus \mathbf{Q}(\sqrt{-d_2})$. In jedem Fall $NS(A) \simeq \mathbf{Z}^2$.
- A einfach
  - $End_{\mathbf{Q}}(A) = Q_{a,b}$ ein indefiniter Quaternionenschiefkörper, $NS(A) \simeq \mathbf{Z}^3$.
  - $End_{\mathbf{Q}}(A) = \mathbf{Q}(\sqrt{d}, \sqrt{a + b\sqrt{d}})$ eine rein komplexe Erweiterung eines reellquadratischen Zahlkörpers, $NS(A) \simeq \mathbf{Z}^2$.
  - $End_{\mathbf{Q}}(A) = \mathbf{Q}(\sqrt{d})$ reellquadratischer Zahlkörper und $NS(A) \simeq \mathbf{Z}^2$.
  - $End_{\mathbf{Q}}(A) = \mathbf{Q}$ und $NS(A) \simeq \mathbf{Z}$.

KAPITEL 8

Public-Key-Kryptosysteme

Sowohl in der Codierungstheorie als auch in der Kryptographie geht es um Nachrichtenübertragung:

In der Codierungstheorie geht es darum, einen Text so zu verschlüsseln, daß er gut rekonstruiert werden kann, wenn es auch Störungen bei der Übertragung gibt. Beispiele: Signale eines Satelliten, CD-Spieler, Computernetze, gesprochene Sprache.

In der Kryptographie geht es darum, den Inhalt einer Nachricht vor Unbefugten zu schützen.

Anwendungsbeispiele der Kryptographie:

- Militärische Informationen sollen vor dem Feind geheim gehalten werden.
- Abhörsicherheit bei Mobiltelefonen oder bei Satellitenübertragung von Telefongesprächen.
- Pay-TV: Nur wer zahlt, darf fernsehen.
- Elektronische Bankgeschäfte.
- Computernetze.
- Chipkarten, z.B. Telefonkarten.

Die Situation in der Kryptographie ist also folgende: A will einen Text T an B senden. A hat eine Verschlüsselungsfunktion bzw. -vorschrift f und macht aus T den Text $C = f(T)$. Dieser wird an B übermittelt. B wendet die Entschlüsselungsfunktion bzw. -vorschrift f^{-1} an auf C und erhält $T = f^{-1}(C)$, den ursprünglichen Text. Wichtig: f und f^{-1} werden geheimgehalten.

Beispiel: Auf Gaius Julius Caesar (100–44 v.Chr.) soll folgendes Verfahren zurückgehen:

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Also ist $f(a) = D$, ... $f^{-1}(A) = x$, ... Aus dem Text *heute ist donnerstag* wird dann *KHXWH LVW GRQQHUVWDJ*.
Nummeriert man die Buchstaben durch von 0 bis 25, so wird die Verschlüsselungsfunktion

$$f(x) = x + 3 \bmod 25$$

und damit die Entschlüsselungsfunktion

$$f^{-1}(x) = x - 3 \bmod 25.$$

Natürlich kann man auf diese Weise viele Verschlüsselungsverfahren konstruieren.

Public-Key-Kryptosysteme: (Die Idee geht auf Diffie und Hellman (1976) zurück.) Man benutzt Verschlüsselungsfunktionen f, so daß man aus der Kenntnis von f die Entschlüsselungsfunktion f^{-1} praktisch nicht berechnen kann. Man hat ein System mit vielen Teilnehmern A. Jeder Teilnehmer A hat eine Verschlüsselungsfunktion f_A und die zugehörige Entschlüsselungsfunktion f_A^{-1}. In einer Liste (Telefonbuch) findet man die Daten (A, f_A). Die Verschlüsselungsfunktion ist also allgemein bekannt. Allerdings ist f_A^{-1} nur A selbst bekannt. Was kann man damit machen?

- Will A einen Text T an B senden, so sendet er $f_B(T)$. Mit $f_B^{-1}(f_B(T)) = T$ erfährt B den ursprünglichen Text. Da andere Teilnehmer C die Funktion f_C^{-1} nicht kennen, können sie T nicht berechnen.

- Wie kann B sicher sein, daß die Nachricht T von A stammt? (Authentifikation, wichtig z.B. bei Bankgeschäften) A nimmt ein Wort P und schreibt an den Schluß seines Textes $f_B(f_A^{-1}(P))$. B erhält dann am Schluß nach Entschlüsselung den unverständlichen Text $f_A^{-1}(P)$. B wendet jetzt f_A an und erhält P, was verständlich ist. Da f_A^{-1} nur A bekannt ist, kann der Text nur von A kommen.
- Ein solches System kann viele Teilnehmer haben, auch neue können unproblematisch dazu kommen.

Frage: Gibt es Verschlüsselungsfunktionen f, so daß f^{-1} sich nicht aus f praktisch erschließen läßt?

Das RSA-Kryptosystem (nach Rivest, Adleman, Shamir 1977): Wähle große Primzahlen p und q, berechne $N = pq$ und wähle eine natürliche Zahl k geeignet. Der Text wird übersetzt in Zahlen $0 \leq T \leq N-1$ (oder ähnlich). Die Verschlüsselungsvorschrift lautet dann

$$f(T) \equiv T^k \bmod N.$$

Beispiel: Wir wählen $N = 10000109503$ und $k = 101$. Die Buchstaben des Textes verwandeln wir in zweistellige Zahlen wie folgt:

	A	B	C	D	E	F	G	H	I
00	01	02	03	04	05	06	07	08	09
J	K	L	M	N	O	P	Q	R	S
10	11	12	13	14	15	16	17	18	19
T	U	V	W	X	Y	Z	a	b	c
20	21	22	23	24	25	26	27	28	29
d	e	f	g	h	i	j	k	l	m
30	31	32	33	34	35	36	37	38	39
n	o	p	q	r	s	t	u	v	w
40	41	42	43	44	45	46	47	48	49
x	y	z	0	1	2	3	4	5	6
50	51	52	53	54	55	56	57	58	59
7	8	9	.	,	;	:	!	?	-
60	61	62	63	64	65	66	67	68	69

usw.

Einen Text codiert man mit dieser Tabelle und gruppert jeweils 10 Ziffern zusammen zu einer Zahl T_i. Man erhält also eine Folge von 10-stelligen Zahlen $T_1, T_2, T_3, \ldots$. Diese transformiert man in $C_i = f(T_i)$ und erhält eine Folge von 11-stelligen Zahlen $C_1, C_2, C_3, \ldots$. Diese kann man dann verschicken. Wir nehmen den Text

Heute findet der Institutsausflug statt.

Man erhält dann

i	T_i	$C_i = f(T_i)$
1	0831474631	01691823167
2	0032354030	06940953091
3	3146003031	02001124503
4	4400094045	08743235231
5	4635464746	04190592492
6	4527474532	08877559908
7	3847330045	07217268008
8	4627464663	06710036419

Bemerkung: Potenzieren geht schnell: Wir wollen für x den Wert $x^k \bmod N$ berechnen. Wir nehmen die Binärzerlegung von k:

$$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \cdots + k_r \cdot 2^r,$$

dann ist

$$x^k = \prod_{i=0}^{r} (x^{2^i})^{k_i} \bmod N.$$

Wir definieren rekursiv Folgen x_i, y_i durch $x_0 = x$, $y_0 = x^{k_0}$ und

$$x_{i+1} = x_i^2, \quad y_{i+1} = y_i x_{i+1}^{k_{i+1}}.$$

Dann gilt $y_r \equiv x^k \bmod N$. Dies läßt sich einfach programmieren und braucht $O(\log k)$ Schritte.

Frage: Was ist f^{-1}? Wir haben $N = pq$ mit verschiedenen Primzahlen p und q. Natürlich sollte die Abbildung $x \mapsto x^k$ auf $\mathbf{Z}/N$ bijektiv sein, insbesondere auch auf $(\mathbf{Z}/N)^\times$. Wann ist dies der Fall? Es gilt

$$(\mathbf{Z}/N)^\times \simeq \mathbf{Z}_{p-1} \times \mathbf{Z}_{q-1},$$

also sollte die Multiplikation mit k auf $\mathbf{Z}_{p-1} \times \mathbf{Z}_{q-1}$ bijektiv sein, also $ggT(k, p-1) = ggT(k, q-1) = 1$. Damit ist auch

$$ggT(k, kgV(p-1, q-1)) = 1.$$

Sei

$$e(N) = kgV(p-1, q-1),$$

dies ist der Exponent der Gruppe $(\mathbf{Z}/N)^\times$. Man konstruiert sich jetzt mit dem euklidischen Algorithmus eine natürliche Zahl ℓ mit

$$k\ell \equiv 1 \bmod e(N),$$

also $k\ell = 1 + me(N)$. Dann gilt für $x \in (\mathbf{Z}/N)^\times$:

$$f(x)^\ell \equiv x^{k\ell} = x^{1+me(N)} \equiv x \bmod N.$$

Da N quadratfrei ist, überlegt man sich schnell, daß diese Aussage für alle $x \in \mathbf{Z}/N$ gilt. Damit haben wir erhalten:

$$f^{-1}(x) \equiv x^\ell \bmod N,$$

wobei ℓ die Gleichung

$$k\ell \equiv 1 \bmod e(N)$$

erfüllt. f^{-1} erhält man also wieder durch Potenzieren.
Hat man die Primfaktorzerlegung von N, so kann man leicht ℓ berechnen. Hat man die Primfaktorzerlegung von N nicht, so kennt man kein allgemeines Verfahren um ℓ aus k und N zu berechnen. Primfaktorzerlegung ist aber schwer. Daher kann man so vorgehen:

- Wähle zwei große Primzahlen p und q und bilde $N = pq$; N sollte heutzutage zwischen 100 und 200 Stellen haben.
- Teste mit allen gängigen Faktorisierungsverfahren, ob sich N faktorisieren läßt. Ist dies der Fall, nimm andere Primzahlen p und q.
- Wähle ein k und berechne dazu ℓ mit

$$k\ell \equiv 1 \bmod kgV(p-1, q-1).$$

- Gib N und k öffentlich bekannt.

Will jemand die Entschlüsselungsfunktion f^{-1} bestimmen, muß er nach heutigen Erkenntnissen N faktorisieren, was aber praktisch nicht geht.

Beispiel: Für unser Beispiel gilt

$$N = 31627 \cdot 316189.$$

Es ist $kgV(31626, 316188) = 555542316$, so daß sich ℓ zu

$$\ell = 187014245$$

berechnet.

Bemerkung: Die Sicherheit des RSA-Kryptosystems beruht also darauf, daß es leicht ist, große Primzahlen p, q zu produzieren, aber schwer, ein Produkt pq zu faktorisieren. Bei entsprechenden Fortschritten in der Faktorisierung großer Zahlen geht also die Sicherheit des RSA-Kryptosystems verloren bzw. man muß immer größere Zahlen N wählen.

Idee: Halte Ausschau nach Funktionen f in der Mathematik mit der Eigenschaft, daß sich f schnell berechnen läßt, daß sich aber f^{-1} aus f praktisch nicht bestimmen läßt. Teste, ob sich zu kryptographisch nutzen läßt.

Das DL-Problem: (DL wie diskreter Logarithmus) Ist G eine endliche zyklische Gruppe, $g \in G$ und $m \in \mathbf{N}$, so kann man (durch Binärzerlegung von m) schnell

$$h = m \cdot g \quad \text{bzw. multiplikativ geschrieben } h = g^m$$

in G berechnen. Ist umgekehrt $h \in G$ gegeben, so gibt es ein (modulo $|G|$ eindeutig bestimmtes) $m \in \mathbf{N}$ mit $h = m \cdot g$ bzw. multiplikativ geschrieben $h = g^m$. Die Zahl m heißt diskreter Logarithmus von h. Die Berechnung des diskreten Logarithmus kann sehr schwer sein.

Beispiel: Wir betrachten $G = \mathbf{F}_p$ mit $p = 3 \cdot 10^{11} + 121$. Dann ist

$$|G| = p - 1 = 2^3 \cdot 3 \cdot 5 \cdot 2500000001.$$

Durch Probieren findet man schnell

$$ord(2) = 5 \cdot 2500000001, \quad ord(3) = 2^2 \cdot 3 \cdot 5 \cdot 2500000001,$$

also ist die Gleichung $2^m \equiv 3 \bmod p$ nicht lösbar, wohingegen die Gleichung

$$3^n \equiv 2 \bmod p$$

lösbar ist. Was ist n? Zunächst ist

$$3^{n\frac{p-1}{8}} \equiv 2^{\frac{p-1}{8}} \equiv 1,$$

was $n \equiv 0 \bmod 4$ liefert. Analog folgt aus

$$3^{n\frac{p-1}{3}} \equiv 2^{\frac{p-1}{3}} \equiv 1$$

sofort $n \equiv 0 \bmod 3$, sowie aus

$$3^{n\frac{p-1}{5}} \equiv 2^{\frac{p-1}{5}} \equiv 1,$$

$$217456407032^n \equiv 94319176517 \bmod p,$$

woraus die Probieren $n \equiv 2 \bmod 5$ folgt. Die letzte Gleichung lautet

$$3^{120n} \equiv 2^{120} \bmod p.$$

Aufgabe: Bestimme n. (Lösung: $n = 50762187192$.)

Die Schwierigkeit, diskrete Logarithmen zu berechnen, kann man nun kryptographisch ausnutzen.

DL-Kryptosysteme: Sei eine endliche abelsche Gruppe G gegeben zusammen mit der Gruppenordnung $|G|$. Man vereinbart eine Möglichkeit vereinbart, Text oder Worte in Gruppenelemente $g \in G$ umzusetzen. Jeder Teilnehmer A wählt sich eine Zufallszahl $e_A \in \mathbf{N}$ mit $ggT(e_A, |G|) = 1$ und berechnet sich d_A mit

$$e_A d_A \equiv 1 \bmod |G|.$$

Will A an B eine Nachricht in Form eines Gruppenelements $h \in G$ senden, so sendet er $e_A h$. B empfängt dies und schickt $e_B e_A h$ an A zurück. A schickt dann an B $d_A e_B e_A h$, woraus B durch Anwendung von d_B dann

$$d_B d_A e_B e_A h = h$$

erhält, die gewünschte Nachricht.
Gefahr: Unterwegs tauchen nur $e_A h, e_B e_A h, e_B h$ auf. Dies sind alles Elemente der von h erzeugten Gruppe H, sogar Erzeuger. Kann jemand das DL-Problem für H lösen, so findet er $m \in \mathbf{N}$ mit $e_A h = m e_B e_A h$, also

$$e_A \equiv m e_B e_A \bmod |H|$$

und damit $1 \equiv m e_B \bmod |H|$, womit man sofort

$$h = m e_B h$$

berechnen kann. Sind also diskrete Logarithmen praktisch nicht zu berechnen in H bzw. G, so ist die Verschlüsselung recht sicher.
Vorteil: Man muß bis auf G überhaupt keine Schlüssel vereinbaren.

Nachteil: Drei Übertragungen sind nötig um eine Nachricht zu übermitteln. Außerdem ist die Authentifikation schwierig.

Schlüsselaustausch: Manchmal wollen A und B eine gemeinsame geheime Information haben, z.B. für einen Schlüssel eines klassischen Kryptosystem. Ist G wieder gegeben mit einem Element $g \in G$, so wählen A und B zufällig natürliche Zahlen e_1, e_2, A schickt an B das Element $e_1 g$, B an A das Element $e_2 g$, woraus beide dann durch Multiplikation mit e_1 bzw. e_2 das Element $e_1 e_2 g$ berechnen, das demnach nur ihnen bekannt ist. Heutzutage kennt man nur ein Verfahren, um das Element $e_1 e_2 g$ aus $e_1 g$ und $e_2 g$ zu berechnen, nämlich den Logarithmus zu berechnen.

Frage: Was sind geeignete Kandidaten G? Man hat folgende Forderungen:

- Die Multiplikation bzw. Exponentiation sollte schnell ausführbar sein.
- Da Logarithmusproblem sollte praktisch zu schwer sein.

Beispiele:

- $(\mathbf{Z}/p\mathbf{Z})^\times$, wo p eine große Primzahl ist,
- $\mathbf{F}_{p^k}^\times$, wo p^k groß ist,
- große Klassengruppen imaginärquadratischer Zahlkörper,
- $E(\mathbf{F}_{p^k})$, wo E eine elliptische Kurve über $\mathbf{F}_{p^k}$ ist,
- $A(\mathbf{F}_{p^k})$, wo A eine abelsche Fläche mit komplexer Multiplikation über $\mathbf{F}_{p^k}$ ist [**Spallek**].

Wir wollen jetzt sehen, wie man elliptische Kurven einsetzen kann.

Einbettung von Text in eine elliptische Kurve: Wir denken uns Text bzw. Worte gegeben durch Zahlen m mit $0 \le m < M$. Wir wählen eine natürliche Zahl k, z.B. $k = 30$. Dann suchen wir eine Primzahl p mit $p > Mk$. Wir wählen eine elliptische Kurve E über $\mathbf{F}_p$ mit der Gleichung $y^2 = x^3 + ax + b$.
Sei jetzt m vorgegeben mit $0 \le m < M$. Wir setzen an $x = mk + j$ und beginnen mit $j = 1$. Wir schreiben $y_2 = x^3 + ax + b$. Wir testen, ob y_2 ein Quadrat ist in $\mathbf{F}_p$. Wenn nicht, ersetzen wir x durch $x+1$, solange $x \le mk + k$. Andernfalls berechnen wir $y \in \mathbf{F}_p$ mit $y^2 = y_2$. Dann ist $(x, y) \in E(\mathbf{F}_p)$ und wir ordnen m den Punkt $P_m = (x, y)$ zu. (Die Wahrscheinlichkeit, daß alle k berechneten Zahlen y_2 keine Quadrate modulo p sind, beträgt ungefähr 0.5^k.)
Ist umgekehrt $P = (x, y)$ gegeben, so schreiben wir $x = mk + j$ mit $1 \le j \le k$. Dann ist $m = [\frac{x-1}{k}]$.

Beispiel: Wir wollen wieder $M = 10^{10}$ Zahlen benutzen, setzen $k = 30$. Die Primzahl $p = 3 \cdot 10^{11} + 121$ erfüllt dann $p > Mk$. Wir wählen die elliptische Kurve E mit der Gleichung

$$y^2 = x^3 - 30 \cdot 7^2 \cdot x - 56 \cdot 7^3.$$

Mit obiger Vorschrift erhalten wir dann folgende Umsetzung:

$m = T_i$	j	$P_m = (x, y)$
831474631	1	(24944238931,228348531691)
32354030	2	(970620902,21711597057)
3146003031	1	(94380090931,76680956753)
4400094045	1	(132002821351,10604724090)
4635464746	1	(139063942381,199533064480)
4527474532	5	(135824235965,201145824177)
3847330045	1	(115419901351,157303999937)
4627464663	1	(138823939891,137196185642)

Frage: Wie konstruiert man geeignete elliptische Kurven? Natürlich lassen sich leicht elliptische Kurven E anschreiben. Die Berechnung von $\#E(\mathbf{F}_p)$ ist aber im allgemeinen ein schwieriges Problem. Außerdem sollte $\#E(\mathbf{F}_p)$ eine große zyklische Untergruppe haben.

Beispiel:

1. Wir starten mit einer über $\mathbf{Q}$ definierten elliptischen Kurve E, die komplexe Multiplikation hat. Wir wählen hier komplexe Multiplikation mit $\mathbf{Z}[\sqrt{-2}]$. Eine Möglichkeit haben wir im letzten Semester kennengelernt:
$$y^2 = x^3 - 30x - 56.$$
2. Wir betrachten jetzt E über $\mathbf{F}_p$. Man sieht schnell, daß E über $\mathbf{F}_p$ für $p \neq 2, 3$ nichtsingulär ist. Sei also p prim mit $p > 3$. Sei R_p der Endomorphismenring von E über $\mathbf{F}_p$. Ein wichtiges Element von R_p ist der Frobeniusendomorphismus π mit $(x, y) \mapsto (x^p, y^p)$, der Norm p hat.
Behauptung: Ist $p \equiv 1, 3 \bmod 8$, so ist $R_p = \mathbf{Z}[\sqrt{-2}]$. Ist $p \equiv 5, 7 \bmod 8$, so ist $\mathbf{Q} \otimes_{\mathbf{Z}} R_p = Q_{a,b}$ ein Quaternionenschiefkörper mit $(a, b)_\infty = (a, b)_p = -1$ und $(a, b)_\ell = 1$ sonst.
Beweis: Natürlich gilt
$$\mathbf{Z}[\sqrt{-2}] \subseteq R_p.$$
Aus der Theorie der elliptischen Kurven über endlichen Körpern weiß man, daß es genau die oben erwähnten zwei Möglichkeiten gibt. Für Quaternionenschiefkörper dieser Bauart gilt nun:
$$\begin{aligned} \sqrt{-2} \in Q_{a,b} &\iff -2 \notin \mathbf{Q}_\infty^{\times 2} \text{ und } -2 \notin \mathbf{Q}_p^{\times 2} \\ &\iff (\frac{-2}{p}) = -1 \iff p \equiv 5, 7 \bmod 8. \end{aligned}$$
In $\mathbf{Z}[\sqrt{-2}]$ gilt für ein Element $\pi = x + y\sqrt{-2}$:
$$\begin{aligned} \pi \text{ hat Norm } p &\iff x^2 + 2y^2 = p \\ &\iff (\frac{-2}{p}) = 1 \iff p \equiv 1, 3 \bmod 8. \end{aligned}$$
Also kann man die zwei Fälle an p mod 8 unterscheiden.
3. Im Fall $p \equiv 5, 7 \bmod 8$ ist $\mathbf{Q}R_p$ ein Quaternionenschiefkörper und $\pi = \sqrt{p}$. Man nennt E dann supersingulär über $\mathbf{F}_p$. Weiter gilt:
$$\#E(\mathbf{F}_p) = p + 1.$$
4. Wir betrachten jetzt den Fall $p \equiv 1, 3 \bmod 8$. Dann ist $R_p = \mathbf{Z}[\sqrt{-2}]$ und es gibt $x, y \in \mathbf{Z}$ mit $\pi = x + y\sqrt{-2}$. Dann ist
$$p = \pi\overline{\pi} = x^2 + 2y^2.$$
Mit dem Algorithmus von Cornacchia kann man diese Gleichung schnell lösen, wobei man allerdings nur $|x|$ und $|y|$ erhält. Die Anzahl der Punkte von $E(\mathbf{F}_p)$ ist dann
$$\#E(\mathbf{F}_p) = (1 - \pi)(1 - \overline{\pi}) = 1 - 2x + p = p + 1 - 2x = p + 1 \pm 2|x|.$$
5. Noch eine andere elliptische Kurve E' gibt es, die über $\overline{\mathbf{F}_p}$ isomorph zu E ist, nicht jedoch über $\mathbf{F}_p$:
$$E' : y^2 = x^3 - 30\ell^2 x - 56\ell^3,$$
wo $(\frac{\ell}{p}) = -1$ gilt. Für die Punkteanzahlen gibt es jetzt zwei Möglichkeiten:
$$\#E(\mathbf{F}_p) = p + 1 - 2|x| \text{ und } \#E'(\mathbf{F}_p) = p + 1 + 2|x|$$
oder
$$\#E(\mathbf{F}_p) = p + 1 + 2|x| \text{ und } \#E'(\mathbf{F}_p) = p + 1 - 2|x|.$$
6. Wir wählen nun
$$p = 3 \cdot 10^{11} + 121$$
und finden mit dem Algorithmus von Cornacchia
$$|x| = 511673 \text{ und } |y| = 138186.$$
Es ist
$$\begin{aligned} N_1 &= p + 1 - 2|x| = 2^3 \cdot 37499872097 \\ N_1 &= p + 1 + 2|x| = 2^2 \cdot 3^2 \cdot 569 \cdot 14645627 \end{aligned}$$
Durch Ausprobieren mit dem Schoof-Algorithmus findet man zugehörig:
$$\begin{aligned} E_1 &: y^2 = x^3 - 30 \cdot 7^2 x - 56 \cdot 7^3, \\ E_2 &: y^2 = x^3 - 30x - 56. \end{aligned}$$

ANHANG A

1. Vorlesungsankündigung

Abelsche Varietäten sind projektive Varietäten, also durch polynomiale Gleichungen beschreibbare Teilmengen eines projektiven Raums, auf denen sich geometrisch eine Gruppenstruktur einführen läßt.
Die 1-dimensionalen abelschen Varietäten werden auch elliptische Kurven genannt, sie lassen sich als ebene Kurven durch Gleichungen der Form $y^2 = x^3 + ax + b$ beschreiben; die Verknüpfung erhält man über Sekanten- und Tangentenbildungen.
Über dem Körper der komplexen Zahlen sind abelsche Varietäten isomorph zu Quotienten $\mathbf{C}^n/\Lambda$, wo Λ ein Gitter in $\mathbf{C}^n$ ist. Die Gruppenstruktur ist dann sofort sichtbar. Um $\mathbf{C}^n/\Lambda$ als Teilmenge eines projektiven Raums zu realisieren, muß man Funktionen auf $\mathbf{C}^n/\Lambda$ studieren, die aber genau den Funktionen auf $\mathbf{C}^n$ entsprechen, die periodisch bezüglich Λ sind. Dies ermöglicht einen einfachen Zugang zu abelschen Varietäten. (Im 1-dimensionalen Fall stößt man dabei auf die in der Funktionentheorie betrachteten doppeltperiodischen Funktionen.)

Abelsche Varietäten spielen eine wichtige Rolle in der Algebraischen Geometrie und der Zahlentheorie. Inzwischen gibt es auch Anwendungen in der Kryptographie.

In der Vorlesung werden abelsche Varietäten zunächst elementar komplex analytisch eingeführt und studiert. Dann sollen einige zahlentheoretisch interessante Aspekte betrachtet werden. Am Ende stehen abelsche Varietäten über endlichen Körpern mit Anwendungen in der Kryptographie.

Die vierstündige Vorlesung setzt zunächst nur Grundkenntnisse der Algebra und Funktionentheorie voraus. Begriffe aus der Algebraischen Geometrie können später bei Bedarf eingeführt bzw. wiederholt werden.

Zeit und Ort: Di, Do 8–10, Übungsraum 3

2. Ausblick

Wir haben in der Vorlesung begonnen, abelsche Varietäten als komplexe Tori $\mathbf{C}^n/\Lambda$ zu studieren. Wie könnte es weitergehen?

- Man kann den komplex-analytischen Weg weiter verfolgen, z.B. an Hand von [**LB**].
- Eine abelsche Varietät über einem algebraisch abgeschlossenen Körper K ist eine irreduzible nichtsinguläre projektive Varietät, die eine damit verträgliche Gruppenstruktur trägt. Für $K = \mathbf{C}$ bzw. $char(K) = 0$ hat man die Darstellung als $\mathbf{C}^n/\Lambda$. Im allgemeinen Fall übertragen sich zwar viele Sätze, man muß aber deutlich mehr Aufwand treiben. [**Mumford**]
- In der Zahlentheorie studiert man unter anderem abelsche Varietäten über $\mathbf{Q}$ und über endlichen Körpern.
- Abelsche Varietäten über endlichen Körpern finden auch Anwendungen bei Primzahlbeweisen und in der Kryptographie.

3. Brief von Chad Schoen

```
From schoen@math.duke.edu Tue Jul 16 19:09:14 1996
From: schoen@math.duke.edu (Chad Schoen)
Date: Tue, 16 Jul 96 13:00:58 EDT
To: ruppert@mi.uni-erlangen.de
Content-Length: 3774
```

Lieber Wolfgang,

ich gratuliere Dir und Susanne und hoffe, dass es Mutter und Kind gut geht!

Sei A eine Abelsche Varietaet der Dimension 2m mit einem imaginaer-
quadratischen Koerper K im Endomorphismenring. Man findet gegen das Ende
der gesammelten Abhandlungen von Weil eine Arbeit, in der er eine
2 dimensionale Hodge-Struktur in H^{2m}(A,Q) konstruiert. Diese
Hodge-Struktur hat Hodge-Typ (m,m), wenn K geeignet auf Lie(A)
operiert. Nehmen wir mal an m=1. Wenn K geeignet auf Lie(A) operiert,
hat die Weilsche Hodge-Struktur den Hodge-Typ (1,1) und wird nach dem
Satz von Lefschetz durch Divisoren erzeugt. Wenn wir nun die Polarisierung
dazu nehmen, erkennen wir, dass der Rank der Neron-Severi-Gruppe mindestens
3 ist. Die Neron-Severi-Gruppe ist mit der Invarianten der Rosatti-INvolution
zu identifizieren. Auf diese weise erhalten wir eine Einbettung einer
nicht definiten Quaternionen-Algebra in den Endomorphismenring von A.

Wenn K nun nicht geeignet auf Lie(A) operiert hat die Weilsche Hodge-Struktur
den Hodge-Typ (2,0)+(0,2). Weil h^{2,0}(A)=1, muss die Zerlegung komplexer
Vektorraeume,
H^2(A)= H^{2,0}+H^{0,2} + H^{1,1},
einer Zerlegung von Hodge-Strukturen entsprechen. Hieraus schliessen wir, dass
der Rank der Neron-Severi-Gruppe 4 ist. Dies kommt nur dann vor, wenn
A zum Selbstprodukt einer elliptischen Kurve mit komplexen Multiplikation
isogen ist.

Enthaelt der Endomorphismenring der Abelschen Flaeche A eine definite
Quaterionenalgebra, so enthaelt er erst recht einen imaginaerquadratischen
Zahlkoerper. Wir haben jedoch oben gesehen, dass solche Abelsche Flaechen
entweder eine indefinite Quaternionenalgebra oder den Matrizenring zweiter
Ordnung ueber einem imaginaerquadratischen Zahlkoerper (der mit dem
Ursprunglichen nicht notwendigerweise uebereinstimmt) als Endomorphismenring
haben. Wir koennen auch offenbar hieraus schliessen, dass es keine Abelsche
Flaeche gibt, deren Endomorphismenring ein Zahlkoerper vom Grad 4 ueber Q
ist, der einen imaginaerquadratischen Unterkoerper besitzt.

Man wird auch obige Folgerungen aus der Theorie der klassischen Gruppe
herleiten koennen. Die Elemente in Sp(4,Q), die mit einer geeigneten
Operation eines imaginaerquadratischen Koerpers kommutieren, werden die
Elemente von der Norm 1 in einer indefiniten Quaternionenalgebra sein.
(Man muss hier
voraussetzen, dass die Operation des Koerpers die Polarisierung bis auf
Multplikation von Elementen aus Q invariant laesst.) Die Darstellung
dieser Quaternionenalgebra auf H^1(A) wird die (links) regulaere Darstellung
sein. Nun, dass wir die spezielle Mumford-Tate-Gruppe (M-T) berechnet haben,
koennen
wir den Endomorphismenring als alle mit der Operation von M-T kommutierenden
Endomorphismen von H^1(A) auffassen. Das heisst, der Endomorphismenring ist
der oben genannte Quaternionenalgebra die von rechts operiert.

Es muss auch eine "ungeeinete" Operation eines imaginaerquadratischen
Koerpers auf die Standarddarstellung von Sp(4,Q) geben. In diesem Fall
wird die spezielle M-T-Gruppe wohl mit dem Kern von Norm R_{L/Q}G_m -->

```
G_m uebereinstimmen. (L imaginaerquadratischer Koerper). Es wird wohl sein,
dass Hodge-Torus und M-T -Gruppe in diesem Fall ueberienstimmen.

Offengestanden habe ich mich nicht mit den Einzelheiten beschaeftigt.
Ich denke jedoch, dass diese Aussagen stimmen werden.

Es waere schoen auf rein geometrischer Weise einzusehen, warum die
Existenz eines Endomorphismus aus einem imaginaerquadratischen
Koerper die Existenz von anderen Endomorphismen impliziert.
Ein Spezielfall wird in meiner Arbeit Compositio 65 (2.12)
behandelt. Wie man allgemein vorgeht weiss ich nicht. Ich hatte
den Eindrueck, dass dieses Problem schwierig sein koennte.

viele Gruesse, Chad
```

4. Programme

Die folgende MAPLE-Funktion berechnet $a^b \bmod m$:

```
# Berechnet a^b mod m
p:=proc(a,b,m)
a1:=a;b1:=b;n1:=1;
while b1<>0 do
 if b1 mod 2=1 then n1:=n1*a1 mod m; fi;
 b1:=trunc(b1/2);
 a1:=a1^2 mod m;
od;
n1;
end;
```

Das Programm *corna.ub* berechnet x und y für $x^2 + dy^2 = p$:

```
  10   input "p=";P
  20   input "d=";D
  30   K=kro(-D,P):if K=-1 then print "keine Loesung mod p":goto 20
  40   Q=P-1:E=0:A=(-D)@P
  50   if Q@2=0 then Q=Q\2:E=E+1:goto 50
  60   N=2
  70   if kro(N,P)=1 then N=N+1:goto 70
  80   Z=modpow(N,Q,P)
  90   Y=Z:R=E:X=modpow(A,(Q-1)\2,P):B=(A*X*X)@P:X=(A*X)@P
 100   if B@P=1 then print "x=";X:goto 150
 110   M=1:Bb=(B*B)@P
 120   if Bb<>1 then M=M+1:Bb=(Bb*Bb)@P:goto 120
 130   if M=R then print A;" ist kein quadratischer Rest modulo ";P:goto 20
 140   T=modpow(Y,2^(R-M-1),P):Y=(T*T)@P:R=M:X=(X*T)@P:B=(B*Y)@P:goto 100
 150   if 2*X<P then X=P-X
 160   A=P:B=X:L=isqrt(P)
 170   if B>L then R=A@B:A=B:B=R:goto 170
 180   if (P-B^2)@D<>0 then print "keine Loesung":goto 20
 190   C=(P-B^2)\D:Y=isqrt(C):X=B
 200   if Y*Y<>C then print "keine Loesung":goto 20
 210   print "x=";X,"y=";Y:goto 20
```

Das Programm *sqrmp.ub* berechnet $\sqrt{a} \bmod p$:

```
 10  input "p=";P
 20  input "a=";A
 30  Q=P-1:E=0
 40  if Q@2=0 then Q=Q\2:E=E+1:goto 40
 50  N=2
 60  if kro(N,P)=1 then N=N+1:goto 60
 70  Z=modpow(N,Q,P)
 80  Y=Z:R=E:X=modpow(A,(Q-1)\2,P):B=(A*X*X)@P:X=(A*X)@P
 90  if B@P=1 then print "x=";X:goto 20
100  M=1:Bb=(B*B)@P
110  if Bb<>1 then M=M+1:Bb=(Bb*Bb)@P:goto 110
120  if M=R then print A;" ist kein quadratischer Rest modulo ";P:goto 20
130  T=modpow(Y,2^(R-M-1),P):Y=(T*T)@P:R=M:X=(X*T)@P:B=(B*Y)@P:goto 90
```

Literaturverzeichnis

[Beutelsbacher] A. Beutelsbacher, Kryptologie, 2. Auflage, Vieweg 1991.

[BSW] A. Beutelsbacher, J. Schwenk, K.-D. Wolfenstetter, Moderne Verfahren der Kryptographie, Vieweg 1995.

[CS] G. Cornell, J. H. Silverman (eds.), Arithmetic Geometry, Springer 1986.

[Hartshorne] R. Hartshorne, Algebraic Geometry, Springer-Verlag 1977.

[Hulek] K. Hulek, Projective Geometry of Elliptic Curves, Astérisque **137** (1986).

[Koblitz] N. Koblitz, A Course in Number Theory and Cryptography, GTM **114**, Springer-Verlag 1987.

[LangAAF] S. Lang, Introduction to Algebraic and Abelian Functions, Springer 1982.

[LangAV] S. Lang, Abelian Varieties, Springer-Verlag 1983, Nachdruck von 1959.

[LangCM] S. Lang, Complex Multiplication, Springer-Verlag 1983.

[LangDG] S. Lang, Number Theory III — Diophantine Geometry, Springer-Verlag 1991.

[LB] H. Lange, Ch. Birkenhake, Complex Abelian Varieties, Springer-Verlag 1992.

[Mumford] D. Mumford, Abelian Varieties, Oxford University Press 1974.

[Riesel] H. Riesel, Prime Numbers and Computer Methods for Factorization, PM **57**, Birkhäuser 1985.

[Serre] J.-P. Serre, Cours d'arithmétique, Paris 1970.

[Shimura] G. Shimura, On analytic families of polarized abelian varieties and automorphic functions, Ann. Math. **78** (1963), 149-193.

[ST] G. Shimura, Y. Taniyama, Complex multiplication of abelian varieties and its applications to number theory, Publ. Math. Soc. Japan **6**, The Math. Soc. of Japan, Tokyo 1961.

[Spallek] A.-M. Spallek, Kurven vom Geschlecht 2 und ihre Anwendung in Pubic-Key-Kryptosystemen, Institut für Experimentelle Mathematik, Universität GH Essen, Preprint **18** (1994).

[SD] H. P. F. Swinnerton-Dyer, Analytic Theory of Abelian Varieties, Cambridge University Press 1974.