Prof. Dr. H. Brenner **Osnabrück WS 2021/2023**

Elliptische Kurven

Vorlesung 27

Modulfunktionen

Wir erinnern an die Modulsubstitution, also an die Gruppenoperation der speziellen linearen Gruppe $\mathrm{SL}_2(\mathbb{Z})$ auf der oberen Halbebene $\mathbb{H}$ durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau := \frac{a\tau + b}{c\tau + d}.$$

Ein Punkt $\tau \in \mathbb{H}$ legt das Gitter $\Lambda = \langle 1, \tau \rangle$ und damit den komplexen Torus $\mathbb{C}/\Lambda$ bzw. die zugehörige elliptische Kurve fest. Wir interessieren uns für Funktionen $f\colon \mathbb{H} \to \mathbb{C}$, die mit der Gruppenoperation (in einem gewissen Sinne) verträglich sind. Wegen der angegebenen Bedeutung eines Punktes der oberen Halbebene sollte man solche Funktionen stets auch so interpretieren, dass sie komplexen Tori bzw. elliptischen Kurven einen Wert zuweisen.

Definition 27.1. Es sei $k \in \mathbb{Z}$. Eine meromorphe Funktion $f\colon \mathbb{H} \to \mathbb{C}$ auf der oberen Halbebene $\mathbb{H}$ heißt *schwach modular* vom Gewicht k, wenn

$$f(Mz) = (cz + d)^k f(z)$$

für alle

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

gilt, wobei M durch Modulsubstitution auf $\mathbb{H}$ operiert.

Explizit bedeutet die Bedingung, dass

$$f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z)$$

für alle $z \in \mathbb{H}$ gilt. Ein direktes Korollar aus Satz 9.2 ist die folgende Aussage.

Lemma 27.2. *Es sei $f\colon \mathbb{H} \to \mathbb{C}$ eine meromorphe Funktion auf der oberen Halbebene $\mathbb{H}$. Dann ist f genau dann schwach modular vom Gewicht k, wenn sie die beiden Bedingungen $f(z+1) = f(z)$ und $f\left(-\frac{1}{z}\right) = z^k f(z)$ für alle $z \in \mathbb{H}$ erfüllt.*

Beweis. Siehe Aufgabe 26.1. □

Wir betrachten die komplexe Exponentialfunktion auf der oberen Halbebene in der Form

$$\psi\colon \mathbb{H} \longrightarrow \mathbb{C},\ z \longmapsto e^{2\pi \mathrm{i} z}.$$

Das Bild dieser Abbildung ist die punktierte offene Einheitskreisscheibe

$$U(0,1) \setminus \{0\}\,.$$

Mit

$$z \,=\, a + b\mathrm{i}$$

gilt ja

$$\begin{aligned} e^{2\pi \mathrm{i} z} &= e^{2\pi \mathrm{i}(a+b\mathrm{i})} \\ &= e^{2\pi \mathrm{i} a - 2b\pi} \\ &= e^{2\pi \mathrm{i} a} \cdot e^{-2b\pi} \\ &= e^{-2b\pi} \cdot (\cos a, \sin a) \end{aligned}$$

und wegen $b > 0$ ist $e^{-2b\pi} < 1$. Es gilt die Periodizitätsbedingung

$$\psi(z+n) \,=\, \psi(z)$$

für $n \in \mathbb{Z}$. Wenn man den Wertebereich auf $U(0,1) \setminus \{0\}$ einschränkt, so erhält man eine holomorphe Überlagerung. Die Geraden parallel zur x-Achse werden zu Kreisen aufgewickelt, wobei die Geraden nah an der Achse auf einen Kreis nah an der Einheitssphäre abgebildet werden und die fernen Geraden auf kleine Kreise um den Nullpunkt. Die Halbgeraden parallel zur y-Achse werden auf eine offene Radiusstrecke abgebildet.

Wenn $f\colon \mathbb{H} \to \mathbb{C}$ eine Funktion ist, die die Periodizitätsbedingung $f(z) = f(z+n)$ zu $n \in \mathbb{Z}$ erfüllt, so gibt es eine Faktorisierung von f über die Exponentialabbildung

$$\begin{array}{ccc} \mathbb{H} & \stackrel{e^{2\pi \mathrm{i} z}}{\longrightarrow} & U(0,1) \setminus \{0\} \subseteq \mathbb{C} \\ & f \searrow & \downarrow \tilde{f} \\ & & \mathbb{C} \end{array}$$

mit einer eindeutig bestimmten Funktion

$$\tilde{f}\colon\, U(0,1) \setminus \{0\} \longrightarrow \mathbb{C}.$$

Dabei ist f genau dann holomorph oder meromorph, wenn $\tilde{f}$ holomorph oder meromorph auf der punktierten Kreisscheibe ist. Man bezeichnet in dieser Situation die Variable der komplexen Zahlen rechts oben oft mit q und hat dann die Beziehung $\tilde{f}(q) = f(z)$, $q = e^{2\pi \mathrm{i} z}$. Diesen Übergang kann man insbesondere für eine schwache Modulfunktion f machen, für die es somit eine meromorphe Funktion

$$\tilde{f}\colon\, U(0,1) \setminus \{0\} \longrightarrow \mathbb{C}$$

gibt, die wegen der Modularitätsbedingung noch weitere Bedingungen erfüllen muss. Dabei ist es für $\tilde{f}$ eine natürliche Frage, ob man sie in den Nullpunkt hinein sinnvoll meromorph oder holomorph fortsetzen kann.

Definition 27.3. Es sei $f\colon \mathbb{H} \to \mathbb{C}$ eine meromorphe Funktion, die die Periodizität $f(z) = f(z+1)$ für alle $z \in \mathbb{H}$ erfüllt und sei

$$\tilde{f}\colon\, U(0,1) \setminus \{0\} \longrightarrow \mathbb{C}$$

die zugehörige Funktion auf der punktierten Einheitskreisscheibe. Man sagt, dass f *meromorph im Unendlichen* ist, wenn sich $\tilde{f}$ meromorph in den Nullpunkt fortsetzen lässt.

Definition 27.4. Es sei $f\colon \mathbb{H} \to \mathbb{C}$ eine meromorphe Funktion, die die Periodizität $f(z) = f(z+1)$ für alle $z \in \mathbb{H}$ erfüllt und sei

$$\tilde{f}\colon U(0,1) \setminus \{0\} \longrightarrow \mathbb{C}$$

die zugehörige Funktion auf der punktierten Einheitskreisscheibe. Man sagt, dass f *holomorph im Unendlichen* ist, wenn sich $\tilde{f}$ holomorph in den Nullpunkt fortsetzen lässt.

In diesem Fall setzt man $f(\infty) = \tilde{f}(0)$. Im Fall der meromorphen Fortsetzbarkeit von $\tilde{f}$ im Nullpunkt liegt dort eine Laurent-Entwicklung der Form

$$\tilde{f}(q) = \sum_{n=n_0}^{\infty} a_n q^n$$

vor, wobei im holomorphen Fall $n_0 \geq 0$ ist. Es ist dann $f(z) = \sum_{n=n_0}^{\infty} a_n e^{2\pi i n}$ und die a_n nennt man auch *Fourierkoeffizienten* von f.

Definition 27.5. Es sei $k \in \mathbb{Z}$. Eine meromorphe Funktion $f\colon \mathbb{H} \to \mathbb{C}$ auf der oberen Halbebene $\mathbb{H}$ heißt *Modulfunktion* vom Gewicht k, wenn

$$f(Mz) = (cz+d)^k f(z)$$

für alle

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

gilt und wenn f meromorph in ∞ ist.

Es handelt sich also einfach um eine schwache Modulfunktion, die zusätzlich meromorph im Unendlichen ist.

Definition 27.6. Eine Modulfunktion $f\colon \mathbb{H} \to \mathbb{C}$ auf der oberen Halbebene $\mathbb{H}$ vom Gewicht k heißt *Modulform*, wenn sie holomorph in $\mathbb{H}$ und holomorph in ∞ ist.

Lemma 27.7. *Die k-te Eisenstein-Reihe*

$$G_k(\tau) = G_k(\langle 1, \tau \rangle) = \sum_{(m,n)\neq 0} \frac{1}{(m+n\tau)^k}$$

zu $k \geq 3$ ist eine Modulform vom Gewicht k.

Beweis. Die Funktionalgleichung folgt aus

$$G_k\left(\frac{a\tau+b}{c\tau+d}\right) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\frac{a\tau+b}{c\tau+d})^k}$$

$$\begin{aligned} &= (c\tau+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{(m(c\tau+d)+n(a\tau+b))^k} \\ &= (c\tau+d)^k \sum_{(m,n)\neq(0,0)} \frac{1}{((mc+na)\tau+(md+nb))^k} \\ &= (c\tau+d)^k \sum_{(r,s)\neq(0,0)} \frac{1}{(r\tau+s)^k} \\ &= (c\tau+d)^k G_k(\tau), \end{aligned}$$

wobei die vorletzte Gleichung darauf beruht, dass

$$\begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} n \\ m \end{pmatrix}$$

stets eine eindeutige Lösung besitzt. Die Holomorphie beruht aus Sätzen der Funktionentheorie. □

Wir erinnern an die Festlegungen aus der zwölften Vorlesung, geschrieben in der Variablen $\tau \in \mathbb{H}$, $g_2(\tau) = 60G_4(\tau)$, $g_3(\tau) = 140G_6(\tau)$, die Diskriminante $\Delta(\tau) = g_2^3(\tau) - 27g_3^2(\tau)$ und die j-Invariante $j(\tau) := \frac{(12g_2(\tau))^3}{\Delta(\tau)}$.

Satz 27.8. *Die j-Invariante $j\colon \mathbb{H} \to \mathbb{C}$ ist eine Modulfunktion vom Gewicht 0, die auf $\mathbb{H}$ holomorph und im Unendlichen einen einfachen Pol besitzt.*

Kongruenzuntergruppen

Wir möchten eine Reihe von Untergruppen der speziellen linearen Gruppe $\mathrm{SL}_2(\mathbb{Z})$ einführen, die durch gewisse modulare Bedingungen charakterisiert sind und Kongruenzuntergruppen heißen. Es sei eine natürliche Zahl N fixiert. Zunächst induziert der Ringhomomorphismus $\mathbb{Z} \to \mathbb{Z}/(N)$ einen Gruppenhomomorphismus

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/(N)),$$

bei dem einfach sämtliche Einträge modulo N genommen werden. Da die Matrizenmultiplikation und die Determinante durch polynomiale Ausdrücke gegeben sind, folgt direkt, dass dies ein wohldefinierter Gruppenhomomorphismus ist.

Definition 27.9. Es sei $N \in \mathbb{N}$. Die Untergruppe

$$\begin{aligned} \Gamma(N) &= \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid M = E_2 \mod N \right\} \\ &= \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a,d = 1 \mod N,\, b,c = 0 \mod N \right\} \\ &\subseteq \mathrm{SL}_2(\mathbb{Z}) \end{aligned}$$

heißt *Hauptkongruenzgruppe* zur Stufe N.

Es geht also einfach um die Matrizen, deren Diagonalelemente modulo N zu 1 und deren Nebendiagonalelemente modulo N zu 0 werden. Als Kern eines Gruppenhomomorphismus handelt es sich um eine Untergruppe und um einen Normalteiler. Da die Bildgruppe bei $N \geq 1$ endlich ist und die spezielle lineare Gruppe unendlich, ist $\Gamma(N)$ unendlich. Beispielsweise ist $\begin{pmatrix} N+1 & N \\ -N & 1-N \end{pmatrix} \in \Gamma(N)$.

Wir interessieren uns nun für Untergruppen

$$\Gamma(N) \subseteq \Gamma \subseteq \mathrm{SL}_2(\mathbb{Z}),$$

wovon es bei gegebenem N endlich viele gibt. Solche Untergruppen nennt man *Kongruenzuntergruppen*. Neben der Hauptkongruenzgruppe erwähnen wir die folgenden.

Definition 27.10. Es sei $N \in \mathbb{N}$. Die Untergruppe

$$\Gamma_0(N) = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid c = 0 \mod N \right\} \subseteq \mathrm{SL}_2(\mathbb{Z})$$

heißt *Hecke-Kongruenzgruppe* zur Stufe N.

Definition 27.11. Zu $N \in \mathbb{N}$ setzt man

$$\begin{array}{rl} & \Gamma_1(N) \\ = & \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \mid a = 1 \mod N \right\} \\ = & \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid a = d = 1 \mod N, c = 0 \mod N \right\} \\ \subseteq & \mathrm{SL}_2(\mathbb{Z}). \end{array}$$

Es ist

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N).$$

Bei $N \geq 2$ ist beispielsweise $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma(N)$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$, aber $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \notin \Gamma(N)$, $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma_0(N)$, aber $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \notin \Gamma_1(N)$. Ferner ist $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \notin \Gamma_1(N)$.

Kongruenzuntergruppen und Torsion

Eine reelle Basis u, v von $\mathbb{C}$ legt ein Gitter $\Lambda = \mathbb{Z}u + \mathbb{Z}v$ und einen komplexen Torus $\mathbb{C}/\Lambda$ fest, siehe Satz 8.6, wobei der komplexe Torus nur vom Gitter, nicht aber von den Erzeugern abhängt. Wir besprechen eine Sichtweise, in der eine Teilinformation, die in den Erzeugern drinsteckt, beibehalten wird und die die Rolle der Kongruenzuntergruppen erläutert. Dazu fixieren wir eine

positive natürliche Zahl N. Die Erzeuger werden unter der kanonischen Abbildung auf das neutrale Element des Torus abgebildet. Die Punkte $\frac{u}{N}$ und $\frac{v}{N}$ werden unter der kanonischen Abbildung auf N-Torsionspunkte des komplexen Torus abgebildet. Wegen Lemma 18.1 ist $\mathrm{Tor}_N(\mathbb{C}/\Lambda) \cong \mathbb{Z}/(N) \times \mathbb{Z}/(N)$ und diese Elemente werden durch $i[\frac{u}{N}] + j[\frac{v}{N}]$, $0 \leq i, j < N$, repräsentiert. D.h. die Erzeuger definieren in kanonischer Weise eine Basis des $\mathbb{Z}/(N)$-Moduls $\mathrm{Tor}_N(\mathbb{C}/\Lambda)$. Wenn N eine Primzahl ist, so handelt es sich um eine Basis eines zweidimensionalen Vektorraumes. In diesem Sinne liefert ein (geordnetes) Erzeugendensystem eines Gitters einen Datensatz bestehend aus einem komplexen Torus (bzw. der zugehörigen elliptischen Kurve) E und einem (geordneten) Punktepaar (P, Q), das ein Erzeugendensystem für die N-Torsion ist. Nach Korollar 8.5 definieren zwei reelle Basen das gleiche Gitter, wenn sie durch eine ganzzahlige invertierbare Matrix ineinander überführt werden können. Dabei wird aber nicht nur die Basis selbst, sondern im Allgemeinen auch die durch die Basis definierte N-Torsionsbasis verändert. Da es aber nur endlich viele N-Torsionsbasen gibt, gibt es wiederum eine Vielzahl an ganzzahligen invertierbaren Matrizen, die eine N-Torsionsbasis in sich selbst überführen. Wir beschränken uns auf die spezielle lineare Gruppe, wo sich ein direkter Zusammenhang zu den Hauptkongruenzgruppen ergibt.

LEMMA 27.12. *Es sei N eine positive natürliche Zahl. Es sei $M \in \mathrm{SL}_2(\mathbb{Z})$ und sei u, v eine reelle Basis von $\mathbb{C}$ mit dem zugehörigen Gitter Λ und dem zugehörigen komplexen Torus $\mathbb{C}/\Lambda$. Dann definieren u, v und die durch M transformierte Basis u', v' genau dann die gleiche N-Torsionsbasis von $\mathbb{C}/\Lambda$, wenn M zur Hauptkongruenzgruppe $\Gamma(N)$ gehört.*

Beweis. Es sei

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Die transformierte Basis ist $u' = au + bv$ und $v' = cu + dv$. In $\mathbb{C}/\Lambda$ gelten dann die Beziehungen

$$[\frac{u'}{N}] = a[\frac{u}{N}] + b[\frac{v}{N}]$$

und

$$[\frac{v'}{N}] = c[\frac{u}{N}] + d[\frac{v}{N}].$$

Dies ist eine Identität im $\mathbb{Z}/(N)$-Modul

$$\mathrm{Tor}_N(\mathbb{C}/\Lambda) \cong \mathbb{Z}/(N) \times \mathbb{Z}/(N),$$

daher können wir die Zahlen a, b, c, d modulo N nehmen. Die Gleichheit der Basen bedeutet dann einfach, dass modulo N die Gleichheiten $a = d = 1$ und $b = c = 0$ vorliegen. Dies bedeutet $M \in \Gamma(N)$. □

Zu einer Streckung mit $s \in \mathbb{C}^\times$ sind Λ und $s\Lambda$ verschiedene Gitter, es gibt aber nach Lemma 9.11 einen kanonischen Isomorphismus

$$\mathbb{C}/\Lambda \cong \mathbb{C}/s\Lambda.$$

Eine Gitterbasis u, v wird auf die Gitterbasis su, sv abgebildet und die zugehörige N-Torsionsbasis des komplexen Torus wird auf die entsprechende Torsionsbasis abgebildet.

Zu $\tau \in \mathbb{H}$ besteht der Datensatz aus dem komplexen Torus $\mathbb{C}/\langle 1, \tau \rangle$ und der N-Torsionsbasis $[\frac{1}{N}]$, $[\frac{\tau}{N}]$. Für die Wirkungsweise der Hauptkongruenzgruppe auf $\mathbb{H}$ durch Modulsubstitution gilt Lemma 27.12 entsprechend. Man beachte, dass die Beziehung $M\tau = \tau'$ nach Lemma 9.6 bedeutet, dass $\mathbb{C}/\langle 1, \tau \rangle$ und $\mathbb{C}/\langle 1, \tau' \rangle$ streckungsäquivalent sind, nicht, dass sie gleich sind. Insbesondere dürfen die beiden $[\frac{1}{N}]$ nicht miteinander identifiziert werden.

Auch für die Wirkungsweise von $\Gamma_0(N)$ und $\Gamma_1(N)$ auf Gittern gibt es ähnliche Interpretationen, die auf Torsionseigenschaften des Torus Bezug nehmen, siehe Aufgabe 27.16 und Aufgabe 27.17.

Abbildungsverzeichnis