

Vorlesung über Modulformen

Sommersemester 2007

Universität Duisburg-Essen

Gabor Wiese

`gabor.wiese@uni-due.de`

Version vom 23. August 2007

Vorwort

Die Vorlesung soll eine elementare Einführung in die klassische Theorie der Modulformen zu Standardkongruenzuntergruppen der Modulgruppe geben. Dabei sollen moderne Aspekte soweit möglich berücksichtigt werden. Die Darstellung soll möglichst elementar gehalten werden.

Die Darstellung folgt keinem einzelnen Werk, sondern macht Anleihen aus verschiedenen Quellen, die jeweils geeignet erscheinen. Neben den im Literaturverzeichnis erwähnten Quellen sind dies auch Mitschriften von Vorlesungen von W. Kohlen und J. Nekovar.

Inhaltsverzeichnis

1	Einleitung	5
2	Elliptische Kurven und Modulformen	18
2.1	Quotienten von Gruppenoperationen	18
2.1.1	Die komplexe Ebene als topologischer Raum	18
2.1.2	Gruppen-Operationen	20
2.2	Torus und elliptische Funktionen	24
2.2.1	Torus	24
2.2.2	Elliptische Funktionen	26
2.2.3	Holomorphe Abbildungen von Tori	27
2.3	Weierstraß-Funktionen, elliptische Kurven und Eisenstein-Reihen	29
2.3.1	Weierstraß'sche- \wp -Funktion	30
2.3.2	Komplexe elliptische Kurven	32
2.4	Definition von Modulformen (der Stufe 1)	35
2.4.1	Beispiele	35
2.4.2	Definition und Beispiele	35
2.4.3	Gitter-Funktionen und Funktionen auf elliptischen Kurven	37
2.4.4	Nochmal Eisenstein-Reihen	38
2.5	Modulformen höherer Stufe	42
2.5.1	Kongruenzuntergruppen	42
2.5.2	Spitzen	45
2.5.3	Definition	47
2.5.4	Ausartungs-Abbildungen und Altformen	50
2.5.5	Die Eisenstein-Reihe G_2	51
2.6	Theta-Reihen	54
3	Modulkurven	56
3.1	Der Fundamentalbereich für $SL_2(\mathbb{Z})$ und Anwendungen	56
3.1.1	Der Standard-Fundamentalbereich	56
3.1.2	Kompaktifizierung des Fundamentalbereichs	59

3.1.3	Version des Residuensatzes	61
3.1.4	Dimensionsformeln für Modulformen der Stufe 1	62
3.1.5	Die j -Invariante	63
3.2	Fundamentaltbereiche und Modulkurven	65
3.2.1	Fundamentaltbereiche für allgemeine Γ	65
3.2.2	Moduli-Interpretation für Standardkongruenzuntergruppen	66
3.2.3	Modulkurven für stabilisatorfreie Untergruppen	69
3.2.4	Modulkurven für Kongruenzuntergruppen	72
3.3	Modulkurven und Modulformen	74
3.3.1	Modulformen als Differentialformen	74
3.3.2	Das Geschlecht von Modulkurven	79
3.3.3	Dimensionsformeln	81
3.4	Hecke-Theorie	86
3.4.1	Modulkorrespondenzen	86
3.4.2	Hecke-Operatoren auf Modulformen	90
3.4.3	Hecke-Algebren und -Eigenformen	92
A	Notationen, Sätze, Lösungen	95
1.1	Notationen	95
1.2	Sätze aus Funktionen-Theorie und Topologie	95
1.3	Lösungen	96

Kapitel 1

Einleitung

[4.4.2007] In dieser Einleitung wollen wir die große zahlentheoretische Bedeutung von Modulformen und insbesondere ihrer Koeffizienten aufzeigen. Dabei werden zunächst einige Themen gestreift, die in der Vorlesung später im Detail behandelt werden. Danach werden wir aber auch auf entscheidende Sätze überblicksartig eingehen, die erst vor kürzester Zeit bewiesen worden sind und weit über diese Vorlesung hinausgehen.

Zunächst erinnern wir an die Gruppe

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}) \mid \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = 1 \right\},$$

die ganz zentral in der Theorie der Modulformen ist und die man deshalb auch *Modulgruppe* nennt. Diese Gruppe ist unendlich. Man kann aber trotzdem von Untergruppen $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ endlichen Index sprechen. Das sind nämlich solche, die eine endliche disjunkte Nebenklassenzerlegung

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=1}^n \Gamma g_i$$

haben mit gewissen $g_i \in \mathrm{SL}_2(\mathbb{Z})$.

Sei \mathbb{H} die obere Halbebene, d.h.

$$\mathbb{H} := \{ \tau = x + iy \in \mathbb{C} \mid y > 0 \}.$$

Die Modulgruppe operiert auf der oberen Halbebene durch die sogenannten *gebrochen linearen Transformationen* oder auch die *Möbius-Transformationen*, die wie folgt gegeben sind: Sei $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ und $\tau = x + iy \in \mathbb{H}$, dann setzen wir

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

Lemma 1.0.1 Die gerade gegebene Formel benutzt man auch allgemeiner mit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R})$ (und weiterhin $\tau \in \mathbb{H}$). Es gelten:

(a) $\operatorname{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{\operatorname{Im}(\tau) \operatorname{Det}\begin{pmatrix} a & b \\ c & d \end{pmatrix}}{|c\tau+d|^2}$ für alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \operatorname{GL}_2(\mathbb{R})$. Ist die Determinante positiv, dann liegt $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau$ also auch wieder in \mathbb{H} .

(b) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \tau = \tau$.

(c) $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} r & s \\ t & u \end{pmatrix} \cdot \tau = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r & s \\ t & u \end{pmatrix} \cdot \tau$ für alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \operatorname{GL}_2(\mathbb{R})$.

Zusammen bedeutet dies, dass $\operatorname{SL}_2(\mathbb{Z})$ auf \mathbb{H} operiert (im Sinne der Algebra - wir werden diesen Begriff später noch einmal wiederholen). Genauso gilt, dass $\operatorname{GL}_2^+(\mathbb{R})$ (die Untergruppe von $\operatorname{GL}_2(\mathbb{R})$ der Matrizen mit positiver Determinante) auch auf \mathbb{H} operiert.

Aufgabe 1.0.2 Beweise das Lemma.

Als Nächstes erinnern wir uns an den Begriff einer holomorphen Funktion auf einer offenen Menge $M \subset \mathbb{C}$. Dabei heißt M *offen*, wenn es um jeden Punkt $z \in M$ eine offene Scheibe eines positiven Radius gibt, die ganz in M enthalten ist. In Formeln:

$$\forall z \in M \exists \epsilon > 0 : U_\epsilon(z) := \{z' \in \mathbb{C} \mid |z - z'| < \epsilon\} \subset M.$$

Ein schönes Beispiel einer offenen Menge in \mathbb{C} ist \mathbb{H} . Eine Funktion $f : M \rightarrow \mathbb{C}$ heißt *holomorph*, wenn sie in jedem Punkt der offenen Menge M komplex ableitbar ist. Um jeden Punkt $z \in M$ gibt es dann, und das ist eine der fundamentalen Aussagen der Funktionentheorie, eine offene Scheibe obiger Form, so dass f auf dieser Menge durch eine gleichmäßig absolut konvergente Potenzreihe $f(z') = \sum_{n=0}^{\infty} a_n (z' - z)^n$ gegeben ist. Deswegen nennt man holomorphe Funktionen auch *analytische Funktionen*.

Jetzt können wir bereits Modulformen definieren.

Definition 1.0.3 Sei $\Gamma \leq \operatorname{SL}_2(\mathbb{Z})$ eine Untergruppe endlichen Indexes. Wir nehmen an, dass die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in Γ enthalten ist. Eine schwache Modulform vom Gewicht k zur Untergruppe $\Gamma \leq \operatorname{SL}_2(\mathbb{Z})$ ist eine holomorphe Funktion

$$f : \mathbb{H} \rightarrow \mathbb{C},$$

die der Transformationsregel

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau\right) = f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \quad \forall \tau \in \mathbb{H} \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$$

genügt. Ist eine zusätzliche Bedingung (Holomorphizität in den Spitzen) erfüllt, die wir erst später in der Vorlesung erklären wollen, so heißt f eine Modulform.

Als erstes Beispiel von Modulformen nennen wir die konstanten Funktionen, also $f : \mathbb{H} \rightarrow \mathbb{C}$ mit $f(\tau) = a \in \mathbb{C}$ für alle $\tau \in \mathbb{H}$. Diese sind Modulformen zu $\Gamma = \operatorname{SL}_2(\mathbb{Z})$ (und natürlich zu jeder Untergruppe Γ wie in der Definition) von Gewicht 0.

Was bedeutet diese Transformationsregel? Darauf werden wir in dieser Einleitung keine befriedigende Antwort geben können; die werden wir erst später in der Vorlesung im Zusammenhang mit

den Modulkurven sehen. Jetzt können wir aber bereits die Transformationsregel mit der Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ anwenden, deren Existenz in Γ wir ja gefordert haben.

$$f\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \tau\right) = f\left(\frac{1 \cdot \tau + 1}{0 \cdot \tau + 1}\right) = f(\tau + 1) = (0 \cdot \tau + 1)^k f(\tau) = f(\tau).$$

Wir finden also

$$f(\tau + 1) = f(\tau) \quad \forall \tau \in \mathbb{H}.$$

Damit ist f periodisch mit der Periode 1.

Aus der reellen Analysis ist bekannt, dass man periodische Funktionen mittels einer Fourier-Reihe ausdrücken kann. Dies wollen wir auch im Komplexen tun, aber ohne Rückgriff auf die reelle Analysis. Zunächst gibt es eine Standard-Funktion mit der Periode 1, nämlich:

$$q : \mathbb{C} \rightarrow \mathbb{C}, z \mapsto e^{2\pi iz}.$$

Es gilt $q(z) = q(z')$ genau dann, wenn $z - z' \in \mathbb{Z}$. Weiterhin ist das Bild $q(\mathbb{H})$ gleich der punktierten Einheitskreisscheibe $U_1(0)^\bullet := U_1(0) - \{0\} = \{z \in \mathbb{C} \mid 0 < |z| < 1\}$, denn

$$|e^{2\pi i(x+iy)}| = |e^{2\pi ix}| \cdot |e^{-2\pi y}| = e^{-2\pi y}.$$

Die Funktion q ist, wie wir aus der Funktionentheorie wissen, holomorph und ihre Ableitung verschwindet nirgends. Das bedeutet (z. B. nach dem Satz über implizite Funktionen), dass sie “lokal holomorph umkehrbar ist”, dass es also um jeden Punkt $z \in \mathbb{C}$ eine offene Kreisscheibe eines Radius (wie oben) gibt, so dass die Einschränkung von q auf diese Kreisscheibe eine Umkehrfunktion besitzt, die auch holomorph ist. Diese ist natürlich gleich $\frac{1}{2\pi i} \ln$ (wobei natürlich der Logarithmus die aus der Funktionentheorie bekannten Schwierigkeiten bereitet, diese sind aber nur global und nicht lokal).

Ist $f : \mathbb{H} \rightarrow \mathbb{C}$ also eine holomorphe Funktion der Periode 1, dann gibt es wegen der lokalen Umkehrbarkeit von q eine holomorphe Funktion $g : U_1(0)^\bullet \rightarrow \mathbb{C}$, so dass

$$g(q(\tau)) = f(\tau) \quad \forall \tau \in \mathbb{H}.$$

Jetzt machen wir einen Notations-Trick. Wir schreiben q auch für die komplexe Variable auf $U_1(0)^\bullet$. Nun können wir g um den Punkt 0 in eine Laurent-Reihe entwickeln:

$$g(q) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

Wir schreiben von nun an für $g(q)$ auch einfach

$$f(q) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

Ein Teil der Bedingung “Holomorphizität in den Spitzen” ist, dass diese Potenzreihe sogar eine Taylor-Reihe ist, also von der Form $f(q) = \sum_{n=0}^{\infty} a_n q^n$ ist. Wir erhalten somit (in unserer Notation):

$$f(\tau) = f(q) = \sum_{n=0}^{\infty} a_n q^n = \sum_{n=0}^{\infty} a_n e^{2\pi in\tau}.$$

Dies ist die *Fourier-Entwicklung* von f . Die Koeffizienten a_n heißen *Fourier-Koeffizienten* und spielen eine herausragende Rolle in der Theorie der Modulformen. Darauf wollen wir im Rest der Einleitung ausführlich eingehen.

Aufgabe 1.0.4 Zeige unter Benutzung der Integralformel für Koeffizienten in Laurent-Reihen, dass für jedes $y > 0$ gilt:

$$a_n = \int_0^1 f(x + iy) e^{-2\pi i n(x+iy)} dx.$$

Aufgabe 1.0.5 Wie sieht die Fourier-Entwicklung einer holomorphen Funktion $f : \mathbb{H} \rightarrow \mathbb{C}$ mit Periode $h \in \mathbb{Z}$, also $f(\tau + h) = f(\tau)$ für alle $\tau \in \mathbb{H}$, aus?

Zunächst lernen wir überblicksartig zwei nicht-triviale Sorten von Modulformen kennen: die Eisenstein-Reihen und die Theta-Reihen.

1. Beispiel: Eisenstein-Reihen

Definition 1.0.6 Sei $k \geq 4$ gerade. Wir nennen die Reihe (für $\tau \in \mathbb{H}$)

$$G_k(\tau) = \sum_{(0,0) \neq (a,b) \in \mathbb{Z}^2} (a\tau + b)^{-k}$$

die Eisenstein-Reihe von Gewicht k .

[Füge formale Rechnung ein, die zeigt, dass G_k die Transformationseigenschaft einer Modulform für $SL_2(\mathbb{Z})$ und Gewicht k hat, falls man umordnen darf.]

Lemma 1.0.7 Die Reihe

$$\sum_{(c,d) \in \mathbb{Z}^2, (c,d) \neq (0,0)} \frac{1}{(c^2 + d^2)^s}$$

konvergiert für reelle $s > 1$.

Beweis. Da alle Terme positiv sind, genügt es, die Aussage für eine beliebig umgeordnete Reihe zu zeigen. [Bild in der Vorlesung zur Aufteilung von $\mathbb{Z}^2 - \{(0,0)\}$.] Wir teilen die Menge der Paare $(c, d) \in \mathbb{N}^2$ in drei Teilmengen ein: in der ersten gilt $c > d$, in der zweiten $c < d$ und in der dritten $c = d$. Es reicht offenbar, wenn wir die Konvergenz von

$$\sum_{c=1}^{\infty} \sum_{d=1}^{c-1} \frac{1}{(c^2 + d^2)^s}$$

zeigen, denn die zweite Teilmenge liefert den selben Beitrag und die dritte ergibt $\frac{1}{2^s} \sum_{c=1}^{\infty} \frac{1}{c^{2s}} < \infty$. Nun ist aber für festes $c \geq 1$

$$\sum_{d=1}^{c-1} \frac{1}{(c^2 + d^2)^s} \leq (c-1) \frac{1}{c^{2s}} < \frac{1}{c^{2s-1}}.$$

Wegen $2s - 1 > 1$ konvergiert aber die Summe über die Terme $\frac{1}{c^{2s-1}}$. □

Satz 1.0.8 Sei $k \geq 4$ gerade. Die Eisenstein-Reihe $G_k(\tau)$ konvergiert lokal gleichmäßig absolut und definiert somit eine holomorphe Funktion $G_k : \mathbb{H} \rightarrow \mathbb{C}$. Für jede Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ gilt:

$$G_k\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau\right) = G_k\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k G_k(\tau).$$

Damit ist G_k eine schwache Modulform von Gewicht k zur Modulgruppe $\mathrm{SL}_2(\mathbb{Z})$.

Beweis. (Vgl. [FB], S. 313.) Wir werden zeigen, dass G_k für alle $\delta > 0$ und alle $C > 0$ auf der Menge

$$R_{\delta, C} := \{\tau = x + iy \mid |x| \leq C, y > \delta\}$$

gleichmäßig absolut konvergiert. Da für $C \rightarrow \infty$ und $\delta \rightarrow 0$ das Innere dieser Mengen ganz \mathbb{H} ausfüllt, beweist dies den Satz.

Zunächst zeigen wir, dass es für gegebene $\delta > 0$ und $C > 0$ ein $\epsilon > 0$ gibt, so dass für alle $c, d \in \mathbb{R}$ und alle $\tau \in R_{\delta, C}$ die Ungleichung

$$|c\tau + d|^2 \geq \epsilon(c^2 + d^2)$$

gilt. Dazu stellen wir fest, dass diese Ungleichung bereits aus der folgenden Ungleichung folgt. Für gegebene $\delta > 0$ und $C > 0$ gibt es ein $\epsilon > 0$, so dass für alle $c, d \in \mathbb{R}$ mit $c^2 + d^2 = 1$ und alle $\tau \in R_{\delta, C}$ die Ungleichung

$$|c\tau + d|^2 \geq \epsilon$$

gilt. Wir brauchen nämlich nur c und d durch $\sqrt{c^2 + d^2}$ zu teilen (für $c = d = 0$ gilt die Ungleichung trivial).

Nun gilt mit $\tau = x + iy \in R_{\delta, C}$, dass

$$|c\tau + d|^2 = (cx + d)^2 + c^2y^2 > (cx + d)^2 + c^2\delta^2 \neq 0.$$

Da die Menge $\{(c, d, x) \in \mathbb{R}^3 \mid c^2 + d^2 = 1, |x| \leq C\}$ kompakt ist, nimmt die stetige Funktion $(cx + d)^2 + c^2\delta^2$ auf ihr ihr Minimum an. Dieses funktioniert als ϵ , da es insbesondere größer als 0 ist. \square

Bemerkung 1.0.9 Die nicht-genannte Bedingung “Holomorphizität in den Spitzen” ist auch erfüllt, denn in diesem Fall bedeutet sie, wie wir später sehen werden, nur, dass die Fourier-Entwicklung von G_k keine negativen Terme hat, also von der Form $\sum_{n=0}^{\infty} a_n q^n$ ist. Dies und die auftretenden a_n werden wir im Folgenden berechnen. Somit ist G_k eine Modulform zur vollen Modulgruppe $\mathrm{SL}_2(\mathbb{Z})$ von Gewicht k .

[5.4.2007]

Aufgabe 1.0.10 Für $k \geq 3$ ungerade kann man G_k mittels der gleichen Formeln definieren. Welche einfache Aussage über solche G_k drängt sich auf? Man beweise diese.

Wir erinnern an die Riemannsche ζ -Funktion. Diese ist wie folgt definiert für $z \in \mathbb{C}$ mit $\operatorname{Re}(z) > 1$:

$$\zeta(z) = \sum_{n=1}^{\infty} n^{-z}.$$

Bemerkung 1.0.11 Es gelten $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$, $\zeta(6) = \pi^6/945$. Der Beweis erfolgt später. Er steht im Zusammenhang mit der folgenden Bemerkung (siehe [FB], S. 183ff).

Bemerkung 1.0.12 Es gilt die Identität

$$\pi \cot \pi \tau = \frac{1}{\tau} + \sum_{n=1}^{\infty} \left(\frac{1}{\tau + n} + \frac{1}{\tau - n} \right)$$

auf \mathbb{H} . Die auftretende Reihe ist auf \mathbb{H} lokal gleichmäßig absolut konvergent. Der Beweis erfolgt später (siehe [FB], S. 183ff).

Wegen der lokal gleichmäßig absoluten Konvergenz von G_k (für $k \geq 4$) dürfen wir die Reihe umordnen und erhalten

$$G_k(\tau) = 2\zeta(k) + 2 \sum_{c=1}^{\infty} \left(\sum_{d=-\infty}^{\infty} \frac{1}{(c\tau + d)^k} \right).$$

Lemma 1.0.13 Sei $k \geq 2$ eine ganze Zahl. Setze

$$\sigma_{k-1}(n) = \sum_{0 \leq d \leq n, d|n} d^{k-1}.$$

Die Reihe

$$\sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

mit $q = e^{2\pi i \tau}$ definiert eine holomorphe Funktion auf \mathbb{H} und ist gleich der Reihe $\sum_{c=1}^{\infty} \sum_{d=1}^{\infty} d^{k-1} q^{cd}$.

Beweis. Es gilt $\sigma_{k-1}(n) \leq nn^{k-1} = n^k$. Daher genügt es für den ersten Teil zu zeigen, dass $\sum_{n=1}^{\infty} n^k q^n$ eine auf \mathbb{H} holomorphe Funktion definiert. Dazu fassen wir nun q wieder als Variable auf $U_1(0)$ auf. Dann müssen wir nämlich nur sehen, dass der Konvergenzradius dieser Reihe (mindestens) 1 ist. Das zeigt man aber zum Beispiel mit dem Quotientenkriterium.

Wenn wir die Reihe $\sum_{c=1}^{\infty} \sum_{d=1}^{\infty} d^{k-1} q^{cd}$ umordnen, indem wir Terme mit dem selben cd zusammenfassen, dann erhalten wir die gerade betrachtete Reihe. Diese Umordnung ist wegen der absoluten Konvergenz erlaubt. \square

Korollar 1.0.14 Es gilt für alle $k \geq 2$ die Gleichheit lokal gleichmäßig absolut konvergenter Reihen auf \mathbb{H} :

$$(-1)^k \sum_{n=-\infty}^{\infty} \frac{1}{(\tau + n)^k} = \frac{1}{(k-1)!} (2\pi i)^k \sum_{n=1}^{\infty} n^{k-1} q^n.$$

Beweis. Durch Differentiation nach τ der Entwicklung des Kotangens aus vorstehender Bemerkung erhält man

$$\frac{\pi^2}{(\sin \pi\tau)^2} = \sum_{n=-\infty}^{\infty} \frac{1}{(\tau+n)^2}.$$

Wir beweisen die Aussage des Korollars zunächst für $k = 2$ und erinnern, dass $\cos(i\phi) = \frac{1}{2}(e^{i\phi} + e^{-i\phi})$ und $\sin(i\phi) = \frac{1}{2i}(e^{i\phi} - e^{-i\phi})$ für $\phi \in \mathbb{R}$. Dies ergibt

$$\pi \cot(\pi\tau) = \pi \frac{\cos(\pi\tau)}{\sin(\pi\tau)} = \pi i \frac{e^{\pi i\tau} + e^{-\pi i\tau}}{e^{\pi i\tau} - e^{-\pi i\tau}} = \pi i \frac{q+1}{q-1} = \pi i - 2\pi i \frac{1}{q-1}.$$

Gebrauchen wir nun die geometrische Reihe (wegen $|q| < 1$ für $\tau \in \mathbb{H}$)

$$\frac{1}{q-1} = \sum_{n=0}^{\infty} q^n,$$

so folgt die Aussage.

Mittels $k-2$ -maligem Differenzieren der Gleichung für $k = 2$ erhält man die Aussage. Man darf nämlich Differentiation und Summation wegen der lokal gleichmäßig absoluten Konvergenz vertauschen. \square

Theorem 1.0.15 Für gerades $k \geq 2$ gilt die Gleichheit

$$2\zeta(k) + 2 \sum_{c=1}^{\infty} \left(\sum_{d=-\infty}^{\infty} \frac{1}{(c\tau+d)^k} \right) = 2\zeta(k) + 2 \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

holomorpher Funktionen auf \mathbb{H} . Ist zudem $k \geq 4$, so sind diese Funktionen gleich der Eisenstein-Reihe G_k von Gewicht k . Für $k = 2$ bezeichnen wir die auftretende Funktion mit P . Sie wird, wie so viele Funktionen, auch nach Ramanujan benannt.

Insbesondere gelten:

$$\begin{aligned} P(\tau) &= -8\pi^2 \left(-\frac{1}{24} + \sum_{n=1}^{\infty} \sigma_1(n) q^n \right), \\ G_4(\tau) &= \frac{16}{3} \pi^4 \left(\frac{1}{240} + \sum_{n=1}^{\infty} \sigma_3(n) q^n \right), \\ G_6(\tau) &= -\frac{16}{15} \pi^6 \left(-\frac{1}{504} + \sum_{n=1}^{\infty} \sigma_5(n) q^n \right). \end{aligned}$$

Beweis. Wir brauchen nur noch das zuvor Gesagte zusammensetzen. \square

Es sei noch einmal explizit darauf hingewiesen, dass man die Reihe links im Theorem für $k = 2$ nicht umordnen darf.

Bemerkung 1.0.16 Die Funktion $G_2(\tau) = P(\tau) - 2P(2\tau)$ definiert eine Modulform von Gewicht 2 zur Kongruenzuntergruppe

$$\Gamma_0(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{2} \right\}.$$

Der Beweis erfolgt später.

An diesem Beispiel haben wir ein Phänomen gesehen, dass sich durch die ganze Theorie der Modulformen hindurchzieht: Die Fourier-Koeffizienten sind hoch interessante zahlentheoretische Funktionen! Ein nächstes Beispiel folgt sogleich.

2. Beispiel: Theta-Reihen

Definition 1.0.17 Die Reihe $\theta(\tau) := \sum_{n=-\infty}^{\infty} e^{2\pi i n^2 \tau} = \sum_{n=-\infty}^{\infty} q^{n^2}$ heißt Θ -Reihe, sprich Theta-Reihe.

Lemma 1.0.18 Die Theta-Reihe $\sum_{n=-\infty}^{\infty} e^{2\pi i n^2 \tau}$ konvergiert auf \mathbb{H} lokal gleichmäßig absolut und definiert somit eine holomorphe Funktion.

Beweis. Es genügt zu zeigen, dass die Reihe auf Bereichen der Form

$$R_\delta := \{\tau = x + iy \in \mathbb{C} \mid y > \delta\}$$

für beliebiges $\delta > 0$ gleichmäßig absolut konvergiert. Man hat mit $\tau = x + iy \in R_\delta$ die Ungleichung

$$\sum_{n=0}^{\infty} |e^{2\pi i n^2 \tau}| = \sum_{n=0}^{\infty} (e^{-2\pi y})^{n^2} \leq \sum_{n=0}^{\infty} (e^{-2\pi \delta})^{n^2} \leq \sum_{n=0}^{\infty} (e^{-2\pi \delta})^n \leq \frac{1}{1 - e^{-2\pi \delta}},$$

woraus die Aussage folgt. □

Lemma 1.0.19 Es gilt die Identität:

$$(\theta(\tau))^k = \sum_{n=0}^{\infty} A_k(n) q^n$$

mit $q = e^{2\pi i \tau}$, wobei

$$A_k(n) = \#\{(x_1, \dots, x_n) \in \mathbb{Z}^k \mid x_1^2 + x_2^2 + \dots + x_k^2 = n\}$$

die Anzahl aller möglicher Darstellungen von n als Summe von k Quadraten ist.

Beweis. Dies ist eine einfache Rechnung. Man benutzt dabei natürlich, dass man die Reihe wegen der oben gezeigten lokal gleichmäßig absoluten Konvergenz beliebig umordnen darf. □

Bemerkung 1.0.20 Es gilt für k , die durch 4 teilbar sind, dass θ^k eine Modulform vom Gewicht $k/2$ zur Kongruenzuntergruppe

$$\Gamma_0(4) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{4} \right\}$$

ist. Dies folgt aus der Jacobischen Theta-Transformationsformel, die wir später behandeln werden. Genauer gilt diese Bemerkung sogar für alle ganzen k ; dann muss man aber Modulformen halbganzen Gewichtes betrachten, was wir in diesem Rahmen nicht möchten.

Anwendung

Für $N \in \mathbb{N}$ definiert man die Kongruenzuntergruppe

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

in Verallgemeinerung zu den oben gesehenen zwei Fällen.

Bemerkung 1.0.21 Der \mathbb{C} -Vektorraum der Modulformen von Gewicht 4 zu $\mathrm{SL}_2(\mathbb{Z})$ ist 1-dimensional und wird erzeugt von G_4 . Der \mathbb{C} -Vektorraum der Modulformen von Gewicht 2 zu $\Gamma_0(2)$ ist 1-dimensional und wird erzeugt von der Funktion G_2 aus obiger Bemerkung. Die Beweise erfolgen später.

Bemerkung 1.0.22 Der \mathbb{C} -Vektorraum der Modulformen von Gewicht 2 zu $\Gamma_0(4)$ ist 2-dimensional. Der \mathbb{C} -Vektorraum der Modulformen von Gewicht 4 zu $\Gamma_0(4)$ ist 3-dimensional. Die Beweise erfolgen später.

Bemerkung 1.0.23 Ist $f = \sum_{n=0}^{\infty} a_n q^n$ mit $q = e^{2\pi i \tau}$ eine Modulform von Gewicht k zu $\Gamma_0(N)$ und ist $r \in \mathbb{N}$, dann ist $f(q^r) = \sum_{n=0}^{\infty} a_n q^{rn}$ eine Modulform von Gewicht k zu $\Gamma_0(Nr)$. Der Beweis erfolgt später.

Korollar 1.0.24 Der \mathbb{C} -Vektorraum der Modulformen von Gewicht 2 zu $\Gamma_0(2)$ hat $\{G_2(q), G_2(q^2)\}$ als Basis. Der \mathbb{C} -Vektorraum der Modulformen von Gewicht 4 zu $\Gamma_0(4)$ hat $\{G_4(q), G_4(q^2), G_4(q^4)\}$ als Basis.

Beweis. Dies folgt unmittelbar aus den vorstehenden Bemerkungen. □

Theorem 1.0.25 Es gelten:

$$A_4(n) = 8 \sum_{d|n, d \geq 1, 4 \nmid d} d$$

und

$$A_8(n) = 16 \sum_{d|n, d \geq 1} (-1)^{n-d} d^3.$$

Beweis. Hier beweisen wir nur die erste Identität. Die zweite funktioniert analog.

Aus einer der Bemerkungen wissen wir, dass der Raum der Modulformen von Gewicht 2 zu $\Gamma_0(4)$ 2-dimensional ist und eine Basis hat bestehend aus

$$G_2(q) = -\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} (\sigma_1(n) - 2\sigma_1(\frac{n}{2})) q^n = -\frac{\pi^2}{3} - 8\pi^2 q + O(q^2)$$

und

$$G_2(q^2) = -\frac{\pi^2}{3} - 8\pi^2 \sum_{n=1}^{\infty} (\sigma_1(\frac{n}{2}) - 2\sigma_1(\frac{n}{4})) q^n = -\frac{\pi^2}{3} + O(q^2).$$

Dabei ist σ_1 von einer nicht ganzen Zahl als 0 zu interpretieren. Das Symbol $O(q^n)$ zeigt an, dass wir nur die Terme mit q^m für $m < n$ aufgelistet haben.

Offenbar beginnt die Fourier-Entwicklung von θ^4 wie folgt:

$$\theta^4(q) = 1 + 8q + O(q^2),$$

da wir 1 auf genau 8 verschiedene Arten als Summe von 4 Quadraten ganzer Zahlen darstellen können.

Aus einer anderen Bemerkung oben wissen wir, dass θ^4 eine Modulform von Gewicht 2 zu $\Gamma_0(4)$ ist. Daher lässt sie sich als Linearkombination obiger beider Funktionen schreiben. An den ersten beiden Fourier-Koeffizienten lässt sich bereits ablesen, dass gilt:

$$\theta^4(q) = -\frac{1}{\pi^2}G_2(q) - \frac{2}{\pi^2}G_2(q^2).$$

Davon schreiben wir nun die Fourier-Entwicklung hin:

$$\begin{aligned} \theta^4(q) &= \left(\frac{1}{3} + 8 \sum_{n=1}^{\infty} (\sigma_1(n) - 2\sigma_1(\frac{n}{2}))q^n\right) + \left(\frac{2}{3} + 8 \sum_{n=1}^{\infty} (2\sigma_1(\frac{n}{2}) - 4\sigma_1(\frac{n}{4}))q^n\right) \\ &= 1 + 8 \sum_{n=1}^{\infty} (\sigma_1(n) - 4\sigma_1(\frac{n}{4}))q^n. \end{aligned}$$

Da wir bereits gesehen haben, dass

$$\theta^4(q) = \sum_{n=0}^{\infty} A_4(n)q^n$$

gilt, sind wir fertig. □

Aufgabe 1.0.26 *Beweise die zweite Identität aus dem Theorem.*

Wiles' Modularitätssatz (Taniyama-Shimura-Weil)

[11.4.2007] Grob gesprochen sind elliptische Kurven Punktemengen der Form

$$\{(x, y) | y^2 = x^3 - ax - b\}$$

für feste Zahlen a, b . Man fordert, dass die Diskriminante $\Delta = a^3 - 27b^2$ nicht 0 ist. Dabei können wir zum Beispiel a, b in den ganzen Zahlen und x, y in den reellen Zahlen wählen. Genauso gut könnten wir aber auch $a, b, x, y \in \mathbb{C}$ oder $a, b, x, y \in \overline{\mathbb{F}}_p$ fordern.

Um Wiles' Satz zu erklären, wählen wir nun $a, b \in \mathbb{Z}$. Wann immer l eine Primzahl ist, schreiben wir \bar{a}, \bar{b} für die Reduktion von a, b modulo l , also für den Rest beim Teilen durch l .

Wir können uns dann für die Lösungen $x, y \in \overline{\mathbb{F}}_l$ der Gleichung

$$y^2 = x^3 - \bar{a}x - \bar{b}$$

interessieren. Das sind aber unendlich viele. Deshalb beschränken wir uns auf die Lösungen in einer endlichen Körpererweiterung \mathbb{F}_{l^r} von \mathbb{F}_l . Da es offenbar maximal l^{2r} viele geben kann, ist die Punktezahl endlich.

Wir möchten wissen, wieviele Punkte die gegebene Kurve über \mathbb{F}_{l^r} genau hat und definieren die Punktezahl

$$A_E(l^r) = \#\{(x, y) \in \mathbb{F}_{l^r} \mid y^2 = x^3 - \bar{a}x - \bar{b}\}.$$

Für sie kennt man die Hasse-Schranke:

$$|l^r - A_E(l^r)| \leq 2l^{r/2}.$$

Theorem 1.0.27 (Wiles und andere, 1994, 1999) *Es gibt eine Modulform f von Gewicht 2 für eine Untergruppe $\Gamma_0(N)$ für ein N , das man aus a, b ausrechnen kann, so dass alle Koeffizienten der Fourier-Entwicklung $f = \sum_{n=1}^{\infty} a_n q^n$ in \mathbb{Z} liegen, $a_0 = 0$ gilt und so, dass für alle Primzahlen l bis auf endlich viele gilt:*

$$a_{l^r} = l^r - A_E(l^r).$$

Hier sieht man wiederum die große zahlentheoretische Bedeutung der Koeffizienten von Modulformen. Die Lösungsanzahlen über endlichen Körpern von Gleichungen, die elliptische Kurven über \mathbb{Z} beschreiben, tauchen als Koeffizienten von Modulformen auf!

Die berühmte Anwendung ist Fermats letzter Satz.

Korollar 1.0.28 (Wiles) *Sei $p \geq 3$ eine Primzahl. Dann gibt es keine natürlichen Zahlen $a, b, c > 0$, die die Fermat-Gleichung*

$$a^p + b^p = c^p$$

erfüllen.

Beweis. Die Beweisidee geht auf Gerhard Frey von der Universität Duisburg-Essen zurück. Von der Idee bis zum Beweis war es aber ein weiter Weg.

Man nimmt nun an, dass es doch solche Zahlen a, b, c gibt. Dann betrachtet man die Gleichung

$$y^2 = x(x - a^p)(x + b^p),$$

die eine elliptische Kurve beschreibt. Man berechnet, dass $N = 2$ gilt. Wiles' Satz sagt nun, dass es eine Modulform von Gewicht 2 zu $\Gamma_0(2)$ gibt, die die Punktzahl über endlichen Körpern obiger elliptischer Kurve beschreibt. Wir wissen aber nach einer Bemerkung oben, dass der Raum dieser Modulformen 1-dimensional ist und von G_2 erzeugt wird. Der 0-te Koeffizient von G_2 ist aber nicht 0, so dass wir einen Widerspruch erhalten. \square

Mod p Modularitätssatz

Wir wiederholen kurz einen Begriff aus der algebraischen Zahlentheorie. Sei K/\mathbb{Q} ein galoisscher Zahlkörper, der bei einer Primzahl l unverzweigt ist. Das bedeutet, dass die Primidealfaktorisierung von l von der Form

$$l\mathcal{O}_K = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_r,$$

ist mit $rf = [K : \mathbb{Q}]$. Für den Körpergrad gilt $[\mathcal{O}/\mathfrak{p}_i : \mathbb{F}_l] = f$ für alle $i = 1, \dots, r$. Die Galois-Gruppe $G = \text{Gal}(K/\mathbb{Q})$ operiert auf der Menge der Primideale $\{\mathfrak{p}_1, \mathfrak{p}_2, \dots, \mathfrak{p}_r\}$. Dann ist die Zerlegungsgruppe von \mathfrak{p}_1 die Untergruppe $G_{\mathfrak{p}_1} \leq G$ der $\sigma \in G$, die \mathfrak{p}_1 festhalten: $\sigma\mathfrak{p}_1 = \mathfrak{p}_1$. Die Einschränkung auf \mathcal{O}_K jedes $\sigma \in G_{\mathfrak{p}_1}$ gibt durch Reduktion modulo \mathfrak{p}_1 einen Körperautomorphismus von $\mathbb{F} := \mathcal{O}_K/\mathfrak{p}_1$, also ein Element der Galoisgruppe $\text{Gal}(\mathbb{F}/\mathbb{F}_l)$. Wie wir aus der Algebra wissen, gibt es in $\text{Gal}(\mathbb{F}/\mathbb{F}_l)$ ein ausgezeichnetes Element, den *Frobenius-Automorphismus*, der durch $x \mapsto x^l$ gegeben ist.

In dieser Diskussion hätten wir statt \mathfrak{p}_1 auch jedes andere \mathfrak{p}_i nehmen können. Wir nennen jedes Element in $\text{Gal}(K/\mathbb{Q})$ ein *Frobenius-Element bei l* (notiert als Frob_l), falls es in einer der Zerlegungsgruppen $G_{\mathfrak{p}_i}$ liegt und seine Reduktion modulo \mathfrak{p}_i den Frobenius-Automorphismus ergibt.

Der Beweis des folgenden Theorems wurde im Januar 2007 beendet und stellt einen Höhepunkt der modernen Mathematik dar! Dieser Satz war 1987 von dem französischen Abel-Preisträger Jean-Pierre Serre vermutet worden und wird noch stets häufig einfach die *Serre-Vermutung* genannt.

Theorem 1.0.29 (Khare, Kisin, Wintenberger) *Seien p eine Primzahl und K/\mathbb{Q} eine endliche Galois-Erweiterung mit Galois-Gruppe $G := \text{Gal}(K/\mathbb{Q}) \subset \text{GL}_2(\overline{\mathbb{F}}_p)$ derart, dass*

- (i) *für keine Matrix $M \in \text{GL}_2(\overline{\mathbb{F}}_p)$ die konjugierte Gruppe MGM^{-1} in den oberen Dreiecksmatrizen von $\text{GL}_2(\overline{\mathbb{F}}_p)$ enthalten ist und*
- (ii) *die Determinante der komplexen Konjugation (via einer Einbettung $K \hookrightarrow \mathbb{C}$) gleich -1 ist.*

Dann gibt es einen Zahlkörper F und eine Modulform $f = \sum_{n=1}^{\infty} a_n q^n$ mit $a_n \in \mathcal{O}_F$ für alle $n \in \mathbb{N}$, so dass für alle in K/\mathbb{Q} unverzweigten Primzahlen l ungleich p der folgende erstaunliche Zusammenhang gilt:

$$a_l \equiv \text{Spur}(\text{Frob}_l) \pmod{\mathfrak{P}},$$

wobei $\mathfrak{P} \triangleleft \mathcal{O}_F$ ein Primideal ist, das p teilt.

Die Bedingung (i) im Satz ist keine schlimme Einschränkung. Falls nämlich (i) nicht erfüllt ist, kann man Methoden der Klassenkörpertheorie benutzen, um die Erweiterung K/\mathbb{Q} zu verstehen. Die Bedingung (ii) hingegen ist sehr wichtig. Ohne sie kann man im Moment keine ähnliche Aussage beweisen.

In den meisten Fällen kann man an der Spur eines Elementes in $\text{GL}_2(\overline{\mathbb{F}}_p)$ zum Beispiel seine Ordnung ablesen. [Genauer sollte man hier sagen, dass wir auch die Determinante von Frob_l kennen, und somit das charakteristische Polynom von Frob_l , also

$$h(X) = X^2 - \text{Spur}(\text{Frob}_l)X + \text{Det}(\text{Frob}_l) \in \overline{\mathbb{F}}_p[X].$$

Ist dieses gleich dem Minimalpolynom von Frob_l , dann ist die Ordnung von Frob_l die kleinste positive Zahl n , so dass $h(X) \mid X^n - 1$. Oder, anders herum, die einzigen Matrizen in $\text{GL}_2(\overline{\mathbb{F}}_p)$, deren charakteristisches Polynom nicht zur Bestimmung ihrer Ordnung ausreicht, sind von der Form $\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ (nach Konjugation).] Die Ordnung von Frob_l gibt den Restklassengrad von $\mathcal{O}_K/\mathfrak{p}_i$ (in der Notation

von oben) an. Dann liest sich obiger Satz so: Zu einem Zahlkörper wie im Satz kann man den Restklassengrad der meisten unverzweigten Primzahlen an der Reduktion modulo einem Primideal der Koeffizienten einer Modulform ablesen!

An dieser Stelle sollte betont werden, dass das Ausrechnen von Koeffizienten von Modulformen sehr einfach ist, so dass sich uns plötzlich viele Eigenschaften von Zahlkörpern offenbaren!

Wir erläutern dies an einem einfachen Beispiel. Sei $K = \mathbb{Q}(\sqrt{-23})$ der imaginär-quadratische Zahlkörper der Diskriminante -23 . Die Klassenzahl von K ist 3, das heißt es gibt eine unverzweigte zyklische Erweiterung H/K von Grad 3. Die Erweiterung H/\mathbb{Q} ist galoissch mit Gruppe S_3 , da sie nicht-abelsch von der Ordnung 6 ist. Es gilt $S_3 = \text{SL}_2(\mathbb{F}_2)$ (Grund: nicht-abelsch und Ordnung 6).

Es gibt eine Modulform $f = \sum_{n=1}^{\infty} a_n q^n$ mit $a_n \in \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ (dies ist der Ring der ganzen Zahlen von $\mathbb{Q}(\sqrt{5})$). Die Primzahl 2 ist träge in diesem Körper, d. h.

$$\mathbb{Z}[\frac{1+\sqrt{5}}{2}]/(2) = \mathbb{F}_4.$$

Nun gilt der folgende Zusammenhang: Eine ungerade Primzahl $l \neq 23$ hat genau dann den Trägheitsgrad 3 in H/\mathbb{Q} , wenn $a_l \equiv 1 \pmod{2}$; sonst gilt $a_l \equiv 0 \pmod{2}$ und l hat den Trägheitsgrad 1 oder 2.

Kapitel 2

Elliptische Kurven und Modulformen

Wir wollen uns zunächst den einfachsten Modulformen zuwenden, nämlich denen, die “von Stufe 1” genannt werden und auf ganz natürliche Weise auftreten. Dabei wollen wir die Modulform nicht nur als eine holomorphe Funktion der oberen Halbebene betrachten, sondern sie auch als eine Zuordnungsvorschrift verstehen, die jeder vorgegebenen (komplexen) elliptischen Kurve eine komplexe Zahl zuweist.

Obwohl wir gleich mit der Definition von Modulformen beginnen könnten (siehe Einleitung), ziehen wir es doch vor, erst Grundbegriffe elliptischer Kurven einzuführen, so dass Modulformen ganz von selbst auftreten.

2.1 Quotienten von Gruppenoperationen

2.1.1 Die komplexe Ebene als topologischer Raum

Wir erinnern an den Begriff des topologischen Raums anhand des Beispiels der komplexen Ebene \mathbb{C} . Auf einer Menge eine Topologie zu geben, heißt zu sagen, welches die offenen Mengen sind.

Die “Topologie” von \mathbb{C} ist per Definition die von \mathbb{R}^2 ; d. h. dann, dass eine Teilmenge $M \subset \mathbb{C}$ offen ist, wenn es um jeden Punkt $x \in M$ eine Scheibe der Form $U_\delta(x) = \{z \in \mathbb{C} \mid |z - x| < \delta\}$ gibt, die vollständig in M enthalten ist. Es ist offensichtlich, dass bei dieser Definition gilt, dass erstens beliebige Vereinigungen offener Mengen wieder offen sind, dass zweitens der Durchschnitt zweier offener Menge auch wieder offen ist und dass drittens die gesamte komplexe Ebene offen ist, ebenso wie die leere Menge, denn an diese stellt man ja gar keine Bedingung. Die abgeschlossenen Mengen sind per Definition die Komplemente der offenen.

Dies fasst man axiomatisch wie folgt zusammen.

Definition 2.1.1 Sei X eine Menge und \mathcal{O} eine Menge von Teilmengen von X . Dann heißt \mathcal{O} eine Topologie auf X , wenn die drei folgenden Punkte gelten:

- (i) Sei I eine Indexmenge und seien $M_i \in \mathcal{O}$ für $i \in I$. Dann gilt $\bigcup_{i \in I} M_i \in \mathcal{O}$.

(ii) Seien $M_1, M_2 \in \mathcal{O}$. Dann gilt: $M_1 \cap M_2 \in \mathcal{O}$.

(iii) Es gilt: $X \in \mathcal{O}$ und $\emptyset \in \mathcal{O}$.

Die Elemente von \mathcal{O} heißen offene Mengen.

Aus (ii) folgt übrigens sofort, dass endliche Durchschnitte offener Mengen wieder offen sind. Auch der Begriff der Stetigkeit läßt sich in der Sprache der Topologie einfach fassen.

Definition 2.1.2 Seien X und Y Mengen mit Topologien \mathcal{O}_X bzw. \mathcal{O}_Y (wir sagen auch einfach demnächst, dass X und Y topologische Räume sind) und sei $f : X \rightarrow Y$ eine Abbildung (von Mengen). Dann heißt f stetig, wenn gilt:

$$\forall M \in \mathcal{O}_Y : f^{-1}(M) \in \mathcal{O}_X.$$

Ferner sagt man, dass die Abbildung f offen ist, wenn gilt:

$$\forall M \in \mathcal{O}_X : f(M) \in \mathcal{O}_Y.$$

Aufgabe 2.1.3 Beweise, dass die obige Definition von Stetigkeit mit der ϵ - δ -Definition aus der Analysis bzw. Funktionentheorie übereinstimmt.

Definition 2.1.4 Sei X ein topologischer Raum und $M \subset X$ irgendeine Teilmenge.

Seien $U_i \in \mathcal{O}_X$ für eine beliebige Indexmenge I offene Mengen. Die $(U_i)_{i \in I}$ heißen offene Überdeckung von M , falls gilt:

$$\bigcup_{i \in I} U_i \supset M.$$

Die Menge M heißt kompakt, wenn jede offene Überdeckung $(U_i)_{i \in I}$ von M eine endliche Teilüberdeckung besitzt, das heißt, dass es eine endliche Teilmenge $J \subset I$ gibt derart, dass $(U_i)_{i \in J}$ auch eine offene Überdeckung von M ist.

Aus der Funktionentheorie ist bekannt, dass eine Menge $M \subset \mathbb{C}$ kompakt ist, wenn sie beschränkt und abgeschlossen ist. Dies liefert uns dann gleich ganz viele Beispiele. Der Leser ist eingeladen, das gerade gemachte Zitat anhand einiger Beispiele zu überprüfen.

Lemma 2.1.5 Seien X, Y topologische Räume, $f : X \rightarrow Y$ eine stetige Abbildung und $K \subset X$ eine kompakte Teilmenge. Dann ist auch die Bildmenge $f(K) \subset Y$ eine kompakte Menge.

Beweis. Sei $(U_i)_{i \in I}$ eine beliebige offene Überdeckung von $f(K)$. Dann ist $(f^{-1}(U_i))_{i \in I}$ eine offene Überdeckung von K . Aufgrund der Kompaktheit von K gibt es also eine endliche Menge $J \subset I$, so dass $(f^{-1}(U_i))_{i \in J}$ eine endliche offene Überdeckung von K ist. Dann ist aber auch $(U_i)_{i \in J}$ eine endliche offene Überdeckung von $f(K)$. Damit sind wir fertig. \square

Aufgabe 2.1.6 Zeige, dass jede stetige Funktion $f : X \rightarrow \mathbb{R}$ auf einem kompakten topologischen Raum X ihr Maximum und Minimum annimmt.

In der Vorlesung werden wir es häufig mit Punktmengen zu tun haben, derart dass sich die Punkte nicht beliebig nahe kommen, das heißt sich nicht häufen. Solche Menge heißen diskret. Hier ist die Definition.

Definition 2.1.7 Sei X ein topologischer Raum und $M \subset X$ eine Teilmenge. Die Menge M heißt diskret, wenn gilt:

$$\forall x \in M \exists U \in \mathcal{O}_X : U \cap M = \{x\}.$$

Aufgabe 2.1.8 Seien $D \subset \mathbb{C}$ eine diskrete Teilmenge und $K \subset \mathbb{C}$ eine kompakte Teilmenge. Zeige, dass dann $D \cap K$ endlich ist.

Konstruiere einen topologischen Raum X mit einer kompakten Menge $K \subset X$, und einer diskreten Menge $D \subset X$, so dass $D \cap K$ nicht endlich ist. Wie sieht es mit Hausdorffschen topologischen Räumen aus? Dabei heißt ein topologischer Raum X Hausdorffsch, falls es zu je zwei Punkten $x, y \in X$ jeweils offene Mengen $U \ni x$ und $V \ni y$ gibt mit $U \cap V = \emptyset$.

2.1.2 Gruppen-Operationen

[12.4.2007] Wir erinnern zunächst an einen einfachen Begriff aus der Algebra.

Definition 2.1.9 (Gruppenoperationen auf Mengen) Sei G eine Gruppe und M eine Menge. Man sagt dann, dass G von links auf M operiert, falls es eine Abbildung $G \times M \rightarrow M$ gibt, notiert als $(g, m) \mapsto g.m$, so dass $1.m = m$ (mit 1 dem neutralen Element von G) und $g.(h.m) = (gh).m$ für alle $g, h \in G$.

Dies ist äquivalent dazu, dass es einen Gruppenhomomorphismus $\phi : G \rightarrow \text{Aut}(M)$ gibt, nämlich $\phi(g) : M \rightarrow M, m \mapsto g.m$. Hier ist $\text{Aut}(M)$ die Menge der bijektiven Abbildungen $M \rightarrow M$ ist.

Entsprechend zu den Operationen von links definiert man Operationen von rechts. Dann erhält man aber keinen Gruppenhomomorphismus, sondern einen Gruppen-Anti-Homomorphismus, d.h. einen, der $\phi(gh) = \phi(h)\phi(g)$ erfüllt.

Beispiel 2.1.10 S_n operiert von links auf $\{1, 2, \dots, n\}$.

Beispiel 2.1.11 \mathbb{Z} (als Gruppe vermöge "+") operiert (von links und von rechts, das ist egal wegen der Kommutativität von \mathbb{Z}) auf \mathbb{R} durch Addition. Also für $n \in \mathbb{Z}$ und $x \in \mathbb{R}$ setze $n.x := n + x$.

Beispiel 2.1.12 Seien $\omega_1, \omega_2 \in \mathbb{C}$. Die Gruppe \mathbb{Z}^2 (mit koordinatenweiser Addition) operiert auf \mathbb{C} vermöge $(a, b).z = z + a\omega_1 + b\omega_2$ für $z \in \mathbb{C}$ und $(a, b) \in \mathbb{Z}^2$.

Beispiel 2.1.13 $\text{SL}_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid \text{Det} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc = 1 \right\}$ operiert von links auf der oberen Halbebene $\mathbb{H} = \{ \tau = x + iy \in \mathbb{C} \mid x \in \mathbb{R}, y \in \mathbb{R}_{>0} \}$ vermöge $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau = \frac{a\tau + b}{c\tau + d}$ für $\tau \in \mathbb{H}$, wie wir in der Einleitung gesehen haben.

Definition 2.1.14 Sei G eine Gruppe, die von links auf der Menge M operiert. Sei $m \in M$.

Dann heißt die Menge $G.m = \{g.m \mid g \in G\}$ die Bahn (oder der Orbit) von m unter G .

Die Untergruppe $G_m = \{g \in G \mid g.m = m\} \leq G$ heißt die Stabilisatorgruppe bzw. die Isotropiegruppe von m .

Die Menge aller Bahnen

$$G \backslash M = \{G.m \mid m \in M\}$$

heißt die Bahnenmenge von G auf M oder auch der Quotient von M nach G .

Wir schreiben hier die Gruppe nach links um anzuzeigen, dass es sich um eine Linksoperation handelt. Ist die Gruppe abelsch, dann kann man Linksoperationen auch von rechts schreiben und umgekehrt. Daher schreiben wir bei abelschen Gruppen die Gruppe häufig nach rechts.

Beispiel 2.1.15 Die Bahn von $x \in \mathbb{R}$ unter der Operation von \mathbb{Z} auf \mathbb{R} von oben ist $\{x + n \mid n \in \mathbb{N}\}$. Der Stabilisator von x ist die triviale Gruppe, denn aus $x + n = x$ folgt $n = 0$. Den Quotienten $\mathbb{Z} \backslash \mathbb{R}$ können wir identifizieren mit dem halb-offenen Intervall $[0, 1)$. Dies ist ein ganz einfaches Beispiel eines Fundamentalbereiches, von denen wir im Laufe der Vorlesung noch viele sehen werden.

Wenden wir die Abbildung

$$[0, 1) \rightarrow \{z \in \mathbb{C} \mid |z| = 1\}, \phi \mapsto e^{2\pi i \phi}$$

an, so erhalten wir eine Bijektion auf den Einheitskreis.

Beispiel 2.1.16 Die Bahn von $i \in \mathbb{H}$ unter $\mathrm{SL}_2(\mathbb{R})$ ist ganz \mathbb{H} . Denn sei $z = x + iy$ mit $x, y \in \mathbb{R}$ ein beliebiger Punkt auf \mathbb{H} . Offenbar ist $\begin{pmatrix} \sqrt{y} & x/\sqrt{y} \\ 0 & 1/\sqrt{y} \end{pmatrix} i = x + iy$. Der Stabilisator ist

$$\begin{aligned} \mathrm{SL}_2(\mathbb{R})_i &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} i = i \right\} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \right\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \right\} \\ &= \left\{ \begin{pmatrix} \cos(\phi) & \sin(\phi) \\ -\sin(\phi) & \cos(\phi) \end{pmatrix} \mid \phi \in [0, \dots, 2\pi) \right\} = \mathrm{SO}_2(\mathbb{R}), \end{aligned}$$

also die spezielle orthogonale Gruppe.

Beispiel 2.1.17 Seien $0 \neq \omega_1, \omega_2 \in \mathbb{C}$. Wir fassen beide als Vektoren im \mathbb{R}^2 auf. Diese sind \mathbb{R} -linear abhängig, wenn es ein $r \in \mathbb{R}$ gibt mit $r\omega_1 = \omega_2$. Mit anderen Worten: ω_1 und ω_2 sind linear unabhängig, wenn $\omega_1/\omega_2 \notin \mathbb{R}$.

Die Gruppe \mathbb{Z}^2 operiert auf \mathbb{C} durch $(a, b).z = z + a\omega_1 + b\omega_2$.

Definition 2.1.18 Eine Teilmenge $M \subset \mathbb{C}$ heißt Gitter, wenn es $0 \neq \omega_1, \omega_2 \in \mathbb{C}$ mit $\omega_1/\omega_2 \notin \mathbb{R}$ gibt, so dass M die Bahn von 0 unter der Operation von \mathbb{Z}^2 bzgl. ω_1, ω_2 ist.

Konkret sind Gitter also einfach von der Form

$$\Lambda_{\omega_1, \omega_2} := \{a\omega_1 + b\omega_2 \mid a, b \in \mathbb{Z}\}.$$

Die komplexen Zahlen ω_1, ω_2 werden häufig Perioden genannt. Sie bilden per Definition eine Gitterbasis.

[Bild]

Bemerkung 2.1.19 Wir können ohne Einschränkung annehmen, dass $\omega_1/\omega_2 \in \mathbb{H}$, denn sonst ersetzen wir einfach ω_1 durch $-\omega_1$, was das Gitter offenbar nicht verändert.

Definition 2.1.20 Seien $\omega_1, \omega_2 \in \mathbb{C}$ mit $\omega_1/\omega_2 \notin \mathbb{R}$. Jeder Quotient von der Form $\mathbb{C}/\Lambda_{\omega_1, \omega_2}$ heißt Torus.

Tori sind komplexe elliptische Kurven und werden als solche im Folgenden noch eine große Rolle spielen.

Definition 2.1.21 Die Gruppenoperation von G auf der Menge M heißt frei, falls für alle $m \in M$ der Stabilisator G_m die triviale Gruppe ist.

Die Operationen von \mathbb{Z} auf \mathbb{R} und die von \mathbb{Z}^2 auf \mathbb{C} von oben sind daher frei, die von $\mathrm{SL}_2(\mathbb{R})$ auf \mathbb{H} jedoch nicht.

Aufgabe 2.1.22 Sei $\tau \in \mathbb{H}$. Zeige Folgendes. Falls der Stabilisator $\mathrm{SL}_2(\mathbb{Z})_\tau$ ungleich $\{\pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\}$ ist, dann gibt es eine Matrix $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, derart dass $\sigma.\tau = i$ oder $\sigma.\tau = \zeta_3$ gilt. Dabei ist $i = e^{\pi i/2} \in \mathbb{H}$, wie gewohnt, und $\zeta_3 = e^{2\pi i/3}$. Im ersten Fall ist $\mathrm{SL}_2(\mathbb{Z})_\tau$ zyklisch von Ordnung 4 und im zweiten zyklisch von Ordnung 6.

Definition 2.1.23 (Stetige Gruppenoperation) Sei nun G wiederum eine Gruppe, die auf einer Menge X von links operiert. Ist nun zusätzlich X ein topologischer Raum und sind alle Abbildungen $X \rightarrow X, x \mapsto g.x$ Homöomorphismen (also bijektiv und stetig mit stetiger Umkehrabbildung), so spricht man von einer stetigen Gruppenoperation.

Aufgabe 2.1.24 Zeige, dass die oben betrachteten Gruppenoperationen (von \mathbb{Z} auf \mathbb{R} , von \mathbb{Z}^2 auf \mathbb{C} (via ω_1, ω_2 wie oben) und von $\mathrm{SL}_2(\mathbb{R})$ auf \mathbb{H}) stetig sind.

Satz 2.1.25 Sei X ein topologischer Raum, auf dem die Gruppe G von links stetig operiert. Sei $\pi : X \rightarrow G \backslash X, x \mapsto G.x$ die natürliche Abbildung.

Das Mengensystem

$$\mathcal{O}_{G \backslash X} = \{U \subset G \backslash X \mid \pi^{-1}(U) \in \mathcal{O}\}$$

bildet eine Topologie auf dem Quotient $G \backslash X$ und die Abbildung π ist stetig und offen. Damit sind die offenen Mengen von $G \backslash X$ gerade die Bilder unter π der offenen Mengen von X .

Beweis. Dass es sich um eine Topologie handelt, ist unmittelbar ersichtlich. Die Abbildung π ist nach Definition der Topologie stetig: so haben wir die Topologie ja gerade gemacht. Wir könnten auch sagen, dass die gewählte Topologie die feinste ist, so dass π stetig ist.

Die Offenheit von π sieht man so: Sei $U \in \mathcal{O}_X$. Ist nun $\pi(U)$ offen? Ja, denn $\pi^{-1}(\pi(U)) = \bigcup_{g \in G} g.U$ ist als Vereinigung der offenen Mengen $g.U = \{g.x \mid x \in U\}$ (die Abbildung $x \mapsto g.x$ ist ja per Definition ein Homöomorphismus, also selbst offen) wieder offen. \square

Beispiel 2.1.26 Die Topologie auf $\mathbb{Z}\backslash\mathbb{R}$ ist unter der Identifikation mit $[0, 1)$ dadurch gegeben, dass eine Menge $U \subset [0, 1)$ genau dann offen ist, wenn es um jeden Punkt $0 \neq x \in U$ ein offenes Intervall $x \in (a, b)$ gibt mit $0 < a < b < 1$ und, falls $0 \in U$, dann muss es $0 < a < 1$ und $0 < b < 1$ geben mit $(a, 1) \subset U$ und $[0, b) \subset U$ (denn unter der Operation von \mathbb{Z} werden ja 0 und 1 identifiziert: $0 + 1 = 1$).

Aufgabe 2.1.27 Wir beschreiben nun $\mathbb{Z}\backslash\mathbb{R}$ als Einheitskreis, wie oben ausgeführt. Man zeige, dass die Abbildung $\phi \mapsto e^{2\pi i\phi}$ einen Homöomorphismus von $\mathbb{Z}\backslash\mathbb{R}$ auf den Einheitskreis definiert, unter der sich die Topologie auf $\mathbb{Z}\backslash\mathbb{R}$ mit der Topologie, die durch offene Intervalle auf dem Einheitskreis gegeben ist, identifiziert.

In diesem Fall sieht man sofort, dass der Einheitskreis lokal, d.h. in einer genügend kleinen Umgebung um jeden Punkt, "genauso aussieht" wie \mathbb{R} : Man hat kleine Intervalle, die in diesem Fall unter dem Homöomorphismus $\phi \mapsto e^{2\pi i\phi}$ aufeinander abgebildet werden. Dies ist eine besonders schöne Eigenschaft, die allerdings nicht immer erfüllt sein wird. Aber wir wollen in der Vorlesung stets versuchen, uns auf diesen Fall zurückzuziehen (für die Spezialisten: Wir versuchen in der ganzen Vorlesung, den kompliziert anmutenden Begriff der eigentlichen Diskontinuität zu vermeiden). Wir werden diese schöne Eigenschaft jetzt in einen Begriff fassen und näher studieren.

Definition 2.1.28 Sei G eine Gruppe, die von links stetig auf dem topologischen Raum X operiert. Wir sagen, dass die Operation gleichmäßig diskrete Bahnen besitzt, wenn es zu jedem $x \in X$ eine offene Menge $x \in U \subset X$ gibt derart, dass für alle $g \in G$ mit $g.x \neq x$ gilt: $gU \cap U = \emptyset$.

Man achte auf die Reihenfolge der Quantoren: Wenn es zu jedem $x \in X$ und zu jedem $g \in G$ mit $g.x \neq x$ eine offene Menge $g.x \in U_{g,x} \subset X$ gibt mit $U_{g,x} \cap U_{h,x} = \emptyset$ für $g.x \neq h.x$, dann hat G diskrete Bahnen. Denn wir haben nur die Definition von Diskretheit auf die Bahn $G.x$ angewendet und ausgeschrieben. Oben fordern wir also mehr. Wir wollen nämlich ausschließen, dass die Mengen $U_{g,x}$ beliebig klein werden müssen, um $U_{g,x} \cap U_{h,x} = \emptyset$ für $g.x \neq h.x$ zu gewährleisten.

Satz 2.1.29 Sei G eine Gruppe, die von links stetig und frei auf dem topologischen Raum X mit gleichmäßig diskreten Bahnen operiert. Dann ist die Quotientenabbildung $\pi : X \rightarrow G\backslash X$ ein lokaler Homöomorphismus, d.h. für alle $x \in X$ gibt es eine offene Menge $x \in U \subset X$, so dass $\pi|_U : U \rightarrow \pi(U)$ ein Homöomorphismus ist.

Beweis. Wir haben den Begriff der gleichmäßig diskreten Bahnen gerade so gewählt, dass dieser Satz gilt. Denn die Definition zusammen mit der Freiheit der Operation besagt nun ja gerade, dass es um jeden Punkt $x \in X$ eine offene Menge $x \in U \subset X$ gibt, so dass $gU \cap U = \emptyset$ für alle $G \ni g \neq 1$. Die Einschränkung der Quotientenabbildung auf U ist nun natürlich bijektiv (und damit ein Homöomorphismus wegen ihrer Stetigkeit und ihrer Offenheit). Denn, wenn $y, z \in U$ mit $\pi(y) = \pi(z)$, dann gibt es ein $g \in G$ mit $g.y = z$, also $g.U \cap U = \{z\} \neq \emptyset$ und somit $g = 1$ und $y = z$. \square

Somit erhalten wir sofort das folgende Korollar.

Korollar 2.1.30 Sei $\Lambda = \Lambda_{\omega_1, \omega_2}$ ein Gitter. Der Torus \mathbb{C}/Λ ist ein topologischer Raum und die Quotientenabbildung $\pi : \mathbb{C} \rightarrow \mathbb{C}/\Lambda$ ist stetig und offen. Außerdem gibt es für jeden Punkt $x \in \mathbb{C}/\Lambda$ und jedes $z \in \mathbb{C}$ mit $\pi(z) = x$ eine offene Menge $z \in U \subset \mathbb{C}$, so dass $\pi : U \rightarrow \pi(U)$ ein Homöomorphismus ist. \square

Bemerkung 2.1.31 Sei $d > 0$ der kleinste Abstand zwischen zwei verschiedenen Gitterpunkten. Die offene Menge U im Korollar können wir stets als $U_\delta(z) = \{z' \in \mathbb{C} \mid |z - z'| < \delta\}$ für jedes $\delta < d/2$ wählen.

Beweis. Wir müssen nur sicher stellen, dass $\gamma U \cap U = \emptyset$ für alle $\gamma \neq 1$. Speziell bedeutet das nur, dass Kreise vom Radius δ um zwei verschiedene Gitterpunkte sich nicht schneiden können. Nun, das wir aber gerade dadurch erreicht, dass die Gitterpunkte mehr als zwei Radien von einander entfernt liegen. \square

Bemerkung 2.1.32 Wir werden später sehen, dass $\mathrm{SL}_2(\mathbb{Z})$ gleichmäßig diskrete Bahnen für die Operation auf $\mathbb{H} = \mathrm{SO}_2(\mathbb{R}) \backslash \mathrm{SL}_2(\mathbb{R})$ hat. Da die Operation aber nicht frei ist, ist $\mathbb{H} \rightarrow \mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ kein lokaler Homöomorphismus; insbesondere muss man für die "komplexe Struktur" mehr arbeiten als beim Torus. Dies werden wir am Schluss des Kapitels über Modulkurven tun.

2.2 Torus und elliptische Funktionen

[18.04.07] In diesem Abschnitt widmen wir näher uns den Tori und den damit zusammenhängenden elliptischen Funktionen.

2.2.1 Torus

Definition 2.2.1 (Gruppenoperationen auf R -Moduln) Seien R ein Ring, G eine Gruppe und M ein R -Modul.

Man sagt in diesem Fall, dass G auf dem R -Modul M von links operiert, wenn G auf M aufgefasst als Menge von links operiert und alle Abbildungen $M \rightarrow M, m \mapsto g.m$ R -Modulhomomorphismen sind.

Einen R -Modul M mit G -Operation von links nennt man auch einen $R[G]$ -Links-Modul. Entsprechende Definitionen macht man für den Fall einer Operation von rechts.

Beispiel 2.2.2 Matrix-Vektor-Multiplikation der Gruppe $\mathrm{SL}_2(\mathbb{Z})$ auf dem \mathbb{Z} -Modul \mathbb{Z}^2 gibt uns ein Beispiel eines $\mathrm{SL}_2(\mathbb{Z})$ -Moduls (mit $R = \mathbb{Z}$). Damit operiert $\mathrm{SL}_2(\mathbb{Z})$ auch auf den Gittern $\Lambda_{\omega_1, \omega_2}$.

Satz 2.2.3 Für $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ gilt

$$\Lambda_{\omega_1, \omega_2} = \Lambda_{a\omega_1 + b\omega_2, c\omega_1 + d\omega_2}.$$

Ist umgekehrt $\Lambda_{\omega_1, \omega_2} = \Lambda_{\omega'_1, \omega'_2}$ mit $\omega_1/\omega_2 \in \mathbb{H}$ und $\omega'_1/\omega'_2 \in \mathbb{H}$, dann gibt es $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ mit $\omega'_1 = a\omega_1 + b\omega_2$ und $\omega'_2 = c\omega_1 + d\omega_2$.

Beweis. Beim ersten Teil ist die Inklusion “ \subseteq ” klar. Indem man aber die inverse Matrix zu $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ anwendet, erhält man aus demselben Grund die andere Inklusion.

Nun zum zweiten Teil. Es gilt nach Voraussetzung, dass $\omega'_1 = a\omega_1 + b\omega_2$ und $\omega'_2 = c\omega_1 + d\omega_2$ für gewisse eindeutige $a, b, c, d \in \mathbb{Z}$ bzw. $\begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$. Wir müssen also nur nachweisen, dass $\text{Det} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1$ ist. Dafür tauschen wir wieder die Rollen und schreiben $\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix}$ für gewisse eindeutige $a', b', c', d' \in \mathbb{Z}$. Nun gilt aber außerdem

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix},$$

woraus wegen der linearen Unabhängigkeit von ω_1 und ω_2 sofort $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ folgt. Deshalb ist die Determinante von $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ eine Einheit in \mathbb{Z} , also ± 1 . Die Bedingung im Satz stellt gerade sicher, dass die Determinante gleich 1 ist. \square

Bemerkung 2.2.4 (Standardform) Seien $\omega_1, \omega_2 \in \mathbb{C}$ wie oben mit $\tau := \omega_1/\omega_2 \in \mathbb{H}$. Das Bild von $\Lambda_{\omega_1, \omega_2}$ unter dem Isomorphismus (abelscher Gruppen)

$$\mathbb{C} \rightarrow \mathbb{C}, z \mapsto z/\omega_2$$

ist gleich $\Lambda_{\tau, 1} =: \Lambda_\tau$. Wir sagen, dass die Basis $\{\tau, 1\}$ des Gitters Λ_τ in Standardform ist.

Transformieren wir ein Gitter mit Basis in Standardform Λ_τ wie im Satz mit einer Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, so erhalten wir das Gitter $\Lambda_{a\tau+b, c\tau+d}$, dessen Basis-Standardform $\Lambda_{\frac{a\tau+b}{c\tau+d}}$ ist. Wir haben also die Operation von $\text{SL}_2(\mathbb{Z}) \leq \text{SL}_2(\mathbb{R})$ auf \mathbb{H} , die wir oben behandelt haben, auf natürliche Weise zurückgefunden.

Satz 2.2.5 Sei Λ wie oben ein Gitter. Der Torus \mathbb{C}/Λ trägt folgende stetige Gruppenoperation:

$$+ : \mathbb{C}/\Lambda \times \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\Lambda, (z_1 + \Lambda) + (z_2 + \Lambda) := (z_1 + z_2) + \Lambda.$$

Insbesondere gibt es für jede natürliche Zahl n die “Multiplikation mit n -Abbildung”:

$$n : \mathbb{C}/\Lambda \rightarrow \mathbb{C}/\Lambda, z + \Lambda \mapsto nz + \Lambda.$$

Diese ist stetig.

Beweis. Dass es sich um eine Gruppenoperation handelt, folgt unmittelbar aus dem Fakt, dass $+$ auf \mathbb{C} eine Gruppenoperation ist. Die Stetigkeit folgt unmittelbar aus der Stetigkeit der Addition von \mathbb{C} . Daraus folgt auch schon der zweite Teil. \square

Definition 2.2.6 Sei $n \geq 1$ eine natürliche Zahl. Wir definieren

$$(\mathbb{C}/\Lambda)[n] := \text{Kern}(n).$$

Satz 2.2.7 Es gibt einen Gruppenisomorphismus

$$(\mathbb{C}/\Lambda)[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$$

Aufgabe 2.2.8 Beweise den Satz.

2.2.2 Elliptische Funktionen

Wir haben gesehen, dass ein Torus “lokal”, das heißt in einer offenen Umgebung um jeden Punkt, durch eine offene Teilmenge der komplexen Zahlen gegeben ist. Dies werden wir benutzen, um zu sagen, was holomorphe und meromorphe Funktionen des Torus sind.

Definition 2.2.9 Eine Funktion $f : \mathbb{C}/\Lambda \rightarrow \mathbb{C}$ heißt holomorph bzw. meromorph, falls es für alle $x \in \mathbb{C}/\Lambda$ eine offene Menge $U \subset \mathbb{C}$ und eine holomorphe (bzw. meromorphe) Funktion $F : U \rightarrow \mathbb{C}$ gibt, so dass $\pi(U) \ni x$ und für alle $y \in U$ gilt:

$$f(\pi(y)) = F(y),$$

wobei $\pi : \mathbb{C} \rightarrow \mathbb{C}/\Lambda$ die natürliche Abbildung ist. [Bild]

Satz 2.2.10 Sei $f : \mathbb{C}/\Lambda \rightarrow \mathbb{C}$ eine holomorphe (bzw. meromorphe) Funktion auf dem Torus. Dann ist die Funktion $F : \mathbb{C} \rightarrow \mathbb{C}$, die als $F(z) := f(\pi(z))$ definiert ist, holomorph (bzw. meromorph). Insbesondere gilt $F(z + \lambda) = F(z)$ für alle $\lambda \in \Lambda$.

Beweis. Wir müssen nur überprüfen, dass F holomorph bzw. meromorph ist, also in jedem Punkt durch eine konvergente Taylor-Reihe (bzw. Laurent-Reihe) gegeben ist. Dies ist aber nach Definition der holomorphen (bzw. meromorphen) Funktionen auf dem Torus der Fall. \square

Definition 2.2.11 Jede meromorphe Funktion $F : \mathbb{C} \rightarrow \mathbb{C}$, für die es wie im Satz ein Gitter Λ gibt, so dass $F(z + \lambda) = F(z)$ für alle $\lambda \in \Lambda$, heißt elliptische Funktion.

Satz 2.2.12 (Liouville) Jede holomorphe elliptische Funktion ist konstant. Ebenso ist jede elliptische Funktion ohne Nullstellen konstant.

Beweis. Sei f eine holomorphe elliptische Funktion. Der Abschluss der Fundamentalmasche ist kompakt und holomorphe Funktionen nehmen auf einem Kompaktum ihr Maximum an. Wegen der Periodizität ist f also global beschränkt und nach dem Satz von Liouville aus der Funktionentheorie konstant. Im Falle, dass f keine Nullstellen hat, kann man obiges Argument auf die Funktion $1/f$ anwenden. \square

Wir wiederholen nun zunächst den Residuensatz aus der Funktionentheorie und beginnen mit den benötigten Begriffen.

Definition 2.2.13 Sei $f : U_\delta(a)^\bullet \rightarrow \mathbb{C}$ eine holomorphe Funktion und sei $\sum_{n=-\infty}^{\infty} a_n(z - a)^n$ die Laurent-Entwicklung von f um a .

Die Ordnung von f in a ist das minimale n , für das $a_n \neq 0$ gilt. Wir notieren die Ordnung mit $\text{Ord}(f; a)$. Ist $f(a) = 0$, dann ist die Ordnung also positiv (und die natürliche Ordnung der Nullstelle). Ist die Ordnung negativ, so liegt bei a ein Pol, welcher eine wesentliche Singularität ist, falls $a = -\infty$.

Das Residuum von f in a ist $\text{Res}(f; a) := a_{-1}$.

Theorem 2.2.14 (Residuensatz der Funktionentheorie) Sei $D \subset \mathbb{C}$ ein einfach zusammenhängendes Gebiet (also zum Beispiel eine Kreisscheibe) und seien $\{z_1, z_2, \dots, z_n\}$ paarweise verschiedene Punkte von D , die von einer stückweise glatten, geschlossenen Kurve $\alpha \subset D$ im mathematisch positiven Sinn genau einmal umlaufen werden.

Ist dann $f : D - \{z_1, z_2, \dots, z_n\} \rightarrow \mathbb{C}$ holomorph, so gilt

$$\int_{\alpha} f(z) dz = \sum_{j=1}^n \operatorname{Res}(f; z_j).$$

Sei im Folgenden $f : \mathbb{C} \rightarrow \mathbb{C}$ eine meromorphe elliptische Funktion zum Gitter Λ . Damit sind natürlich die Nullstellen und die Polstellen auch periodisch mit Λ .

Wir werden die Liouvilleschen Sätze im folgenden Abschnitt benötigen.

Satz 2.2.15 (Liouville) Sei im Folgenden $f : \mathbb{C} \rightarrow \mathbb{C}$ eine meromorphe elliptische Funktion zum Gitter Λ . Dann gelten:

(a) $\sum_{z \in \mathbb{C}/\Lambda} \operatorname{Res}(f; z) = 0$ und

(b) $\sum_{z \in \mathbb{C}/\Lambda} \operatorname{Ord}(f; z) = 0$.

Dabei wird die Summe über Punkte in einer Fundamentalmasche genommen, wobei wir vom Rand gerade so viel hinzunehmen, dass jeder Punkt in \mathbb{C} durch Addition eines geeigneten $\lambda \in \Lambda$ zu genau einem Punkt der Fundamentalmasche transportiert werden kann. [Bild]

Beweis. Für diesen Beweis brauchen wir nur den Rand der Fundamentalmasche als stückweise glatte geschlossene Kurve aufzufassen. Sollte eine Pol- oder Nullstelle auf dem Rand liegen, dann verschieben wir die Kurve um eine geeignete kleine Konstante. Diese Konstante existiert wegen der Diskretheit des Gitters. Aus dem Residuensatz folgt dann bereits (a), da das Integral wegen der Periodizität verschwindet, denn gegenüberliegende Seiten heben sich im Integral gerade weg.

Für (b) stellen wir zunächst fest, dass mit f auch f' und mithin auch f'/f elliptisch sind. Das Residuum der Funktion $f'(z)/f(z)$ an einer Stelle a ist gerade die Ordnung von f in a . Also folgt (b) aus (a). \square

Auf die elliptischen Funktionen kommen wir in Kürze noch weiter zu sprechen.

2.2.3 Holomorphe Abbildungen von Tori

Als Nächstes wollen wir sagen, was wir unter holomorphen bzw. meromorphen Funktionen von einem Torus in einen anderen verstehen.

Definition 2.2.16 Eine Funktion $f : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2$ heißt holomorph, falls es für alle $x \in \mathbb{C}/\Lambda_1$ eine offene Menge $U \subset \mathbb{C}$ und eine holomorphe Funktion $F : U \rightarrow \mathbb{C}$ gibt, so dass für alle $y \in U$ gilt:

$$f(\pi_1(y)) = \pi_2(F(y)),$$

wobei $\pi_i : \mathbb{C} \rightarrow \mathbb{C}/\Lambda_i$ die natürlichen Abbildungen sind. [Bild]

[19.04.07] Der folgende Satz ist ein allgemeines Prinzip der algebraischen Topologie. Was wir implizit benutzen ist, dass \mathbb{C} einfach zusammenhängend und somit die sogenannte universelle Überlagerung der Tori ist. Hier geben wir aber einen einfachen und direkten Beweis.

Satz 2.2.17 Sei $f : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2$ eine holomorphe Funktion und seien $\pi_1 : \mathbb{C} \rightarrow \mathbb{C}/\Lambda_1$ und $\pi_2 : \mathbb{C} \rightarrow \mathbb{C}/\Lambda_2$ die Quotientenabbildungen. Dann gibt es zu jedem Paar von Punkten $a, b \in \mathbb{C}$ mit $f(a + \Lambda_1) = b + \Lambda_2$ eine holomorphe Abbildung $F : \mathbb{C} \rightarrow \mathbb{C}$ derart, dass $f \circ \pi_1 = \pi_2 \circ F$ und $F(a) = b$.

Beweis. Wir zeigen den Satz in zwei Schritten.

1. Schritt: Zu $a, b \in \mathbb{C}$ mit $f(\pi_1(a)) = \pi_2(b)$ gibt es eine Umgebung $U \ni a$ und eine holomorphe Funktion $F : U \rightarrow \mathbb{C}$ mit $F(a) = b$ und $\pi_2 \circ F|_U = f \circ \pi_1|_U$.

Nach Voraussetzung gibt es nämlich eine offene Menge $\tilde{U} \subset \mathbb{C}$ mit $\pi_1(\tilde{U}) \ni \pi_1(a)$ und eine holomorphe Funktion $\tilde{F} : \tilde{U} \rightarrow \mathbb{C}$ mit $\pi_2 \circ \tilde{F}|_{\tilde{U}} = f \circ \pi_1|_{\tilde{U}}$. Aber es gibt dann ein $\lambda_1 \in \Lambda_1$ mit $a + \lambda_1 \in \tilde{U}$, d. h. $a \in \tilde{U} - \lambda_1$. Weiter gilt $\tilde{F}(a + \lambda_1) = b + \lambda_2$ für ein $\lambda_2 \in \Lambda_2$. Setze nun

$$F : U := \tilde{U} - \lambda_1 \xrightarrow{z \mapsto z + \lambda_1} \tilde{U} \xrightarrow{\tilde{F}} \mathbb{C} \xrightarrow{z \mapsto z - \lambda_2} \mathbb{C},$$

die holomorph ist, a auf b abbildet und $\pi_2 \circ F = f \circ \pi_1$ erfüllt, was den ersten Schritt beendet.

2. Schritt: Der Konvergenzradius der holomorphen Funktion $F =: F_a$ aus dem 1. Schritt ist unendlich.

Zum Beweis nehmen wir an, er wäre endlich, sagen wir gleich R . Wir betrachten nun die abgeschlossene und damit kompakte Kreisscheibe $\overline{U_{R+1}(a)}$ vom Radius $R + 1$. Auf diese wollen wir F ausdehnen, was dann den gewünschten Widerspruch liefert.

Um jeden Punkt $x \in \overline{U_{R+1}(a)}$ wählen wir nun nach dem 1. Schritt eine zusammenhängende Umgebung $U_x \ni x$ und eine holomorphe Funktion $F_x : U_x \rightarrow \mathbb{C}$ mit der üblichen Eigenschaft $\pi_2 \circ F_x = f \circ \pi_1$ eingeschränkt auf U_x ; den Wert $F_x(x)$ werden wir in Kürze anpassen. Diese U_x überdecken $\overline{U_{R+1}(a)}$. Wegen der Kompaktheit genügen aber schon endlich viele zum Überdecken, sagen wir $x_1 = a, x_2, \dots, x_n$. Jedes U_{x_i} hat einen nicht-leeren Durchschnitt mit einem U_{x_j} (für ein $i \neq j$). Nun passen wir die Bilder von $F_{x_i}(x_i)$ für $i > 1$ wie folgt an.

Wir wählen ein $i > 1$, so dass $U_{x_i} \cap U_a \neq \emptyset$. Weiter wählen wir nun ein z aus diesem Durchschnitt. Dann gibt es ein $\lambda_2 \in \Lambda_2$ mit $F_a(z) = F_{x_i}(z) + \lambda_2$. Wir ersetzen nun F_{x_i} durch $F_{x_i} + \lambda_2$. Dann sind die Potenzreihen, die F_a und F_{x_i} in einer Umgebung von z beschreiben, identisch; somit sind sie auf $U_a \cup U_{x_i}$ identisch.

Wir wählen nun ein $j > 1, j \neq i$, so dass $U_{x_j} \cap (U_a \cup U_{x_i}) \neq \emptyset$, und verfahren wie eben, so dass die Potenzreihendarstellung von F_a, F_{x_i}, F_{x_j} auf $U_a \cup U_{x_i} \cup U_{x_j}$ identisch sind. So machen wir weiter, bis wir die Potenzreihen von F_{x_l} identisch sind für alle $l = 1, \dots, n$. Dann ist also F auf ganz $\overline{U_{R+1}(a)}$ durch diese Potenzreihe gegeben und wir sind fertig. \square

Diesen Satz können wir benutzen, um zu zeigen, dass holomorphe Abbildungen zwischen Tori, die den Nullpunkt festhalten, alle von der besonders einfachen Form sind, die wir in der folgenden Bemerkung einführen.

Bemerkung 2.2.18 Seien Λ_1, Λ_2 zwei Gitter und sei $a \in \mathbb{C}^\times$. Falls $a\Lambda_1 \subseteq \Lambda_2$ gilt, ist die Abbildung

$$f_a : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2, z + \Lambda_1 \mapsto az + \Lambda_2$$

wohldefiniert und holomorph und es gilt $f_a(0) = 0$.

Aufgabe 2.2.19 Beweise die Bemerkung.

Satz 2.2.20 Seien Λ_1, Λ_2 zwei Gitter und sei $f : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2$ eine holomorphe Abbildung mit $f(0) = 0$. Dann gibt es ein eindeutiges $a \in \mathbb{C}$ mit $a\Lambda_1 \subseteq \Lambda_2$ und $f = f_a$ in der Notation der vorherigen Bemerkung.

Beweis. Die Eindeutigkeit von a ist klar, da π_i lokale Homöomorphismen sind.

Sei $\lambda_1 \in \Lambda_1$. Die Funktion $z \mapsto F(z) - F(z + \lambda_1) \in \Lambda_2$ ist stetig. Eine stetige Funktion von einer zusammenhängenden Menge (hier \mathbb{C}) in eine diskrete Menge ist notwendig konstant, weshalb ihre Ableitung 0 ist. Also gilt

$$F'(z + \lambda_1) = F'(z) \quad \forall \lambda_1 \in \Lambda_1 \forall z \in \mathbb{C}.$$

Damit ist F' eine holomorphe elliptische Funktion, und deshalb ist sie konstant nach dem Satz von Liouville: $F'(z) = a$, woraus unter der Nebenbedingung $F(0) = 0$ die Behauptung $F(z) = az$ folgt. \square

Definition 2.2.21 Eine nicht-konstante holomorphe Abbildung von Tori $f : \mathbb{C}/\Lambda_1 \rightarrow \mathbb{C}/\Lambda_2$, die ein Gruppensomorphismus ist, heißt eine Isogenie.

Ist f zusätzlich ein Homöomorphismus, so heißt f Isomorphismus.

Beispiel 2.2.22 Seien $w_1, w_2 \in \mathbb{C}$ mit $\tau := w_1/w_2 \in \mathbb{H}$. Die Tori $\mathbb{C}/\Lambda_{w_1, w_2}$ und \mathbb{C}/Λ_τ sind isomorph.

Aufgabe 2.2.23 Isogenien sind surjektiv und haben einen endlichen Kern.

2.3 Weierstraß-Funktionen, elliptische Kurven und Eisenstein-Reihen

Wir beginnen mit einer anderen Sichtweise von Eisenstein-Reihen, nämlich als Funktionen, die einem Gitter eine Zahl zuordnen.

Definition 2.3.1 Sei $k \in \mathbb{N}$. Für ein Gitter Λ definieren wir die Eisenstein-Reihe $G_k(\Lambda)$ als die Reihe

$$G_k(\Lambda) := \sum_{\lambda \in \Lambda, \lambda \neq 0} \lambda^{-k}.$$

Ist das Gitter Λ von der Form $\Lambda_\tau = \Lambda_{\tau, 1}$ mit $\tau \in \mathbb{H}$, so finden wir die Funktionen der Einleitung wieder:

$$G_k(\tau) = G_k(\Lambda_\tau) = \sum_{(0,0) \neq (a,b) \in \mathbb{Z}} (a\tau + b)^{-k}.$$

Satz 2.3.2 Sei $k \geq 3$. Für jedes Gitter Λ ist $G_k(\Lambda)$ absolut konvergent und es gilt für jedes $s \in \mathbb{C}^\times$, dass

$$G_k(s\Lambda) = s^{-k} G_k(\Lambda).$$

Beweis. Die Transformationsformel ist sofort aus der Reihendarstellung ersichtlich, so dass die Konvergenz von $G_k(\Lambda)$ stets auf die Konvergenz für ein Gitter mit Basis in Standardform Λ_τ zurückgeführt werden kann. Für diese haben wir in der Einleitung die absolute Konvergenz gezeigt. \square

Auf Eisenstein-Reihen kommen wir später in diesem Kapitel noch zurück.

2.3.1 Weierstraß'sche- \wp -Funktion

Wir kommen nur zur Definition einiger wichtiger elliptischer Funktionen, die in engem Zusammenhang zu Eisenstein-Reihen stehen, wie wir auch sehen werden.

Definition 2.3.3 Sei $\Lambda \subset \mathbb{C}$ ein Gitter. Die Weierstraß'sche- \wp -Funktion (zu Λ) wird durch die Reihe

$$\wp(z) = \wp(z; \Lambda) = \frac{1}{z^2} + \sum_{\lambda \in \Lambda, \lambda \neq 0} \left(\frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right)$$

gegeben.

Satz 2.3.4 Die Reihe $\wp(z; \Lambda)$ konvergiert lokal gleichmäßig absolut auf $\mathbb{C} - \Lambda$. Sie definiert eine elliptische Funktion mit einem Pol der Ordnung 2 in jedem $\lambda \in \Lambda$ (also $\text{Ord}(\wp; \lambda) = -2$) und keinem anderen Pol. Außerdem gilt $\wp(-z) = \wp(z)$, d. h. dass \wp eine gerade Funktion ist.

Die Ableitung \wp' von \wp ist eine ungerade elliptische Funktion und hat die Reihendarstellung

$$\wp' = -2 \sum_{\lambda \in \Lambda} \frac{1}{(z - \lambda)^3},$$

die auf $\mathbb{C} - \Lambda$ lokal gleichmäßig absolut konvergiert.

Beweis. Wir zeigen, dass für gegebenes $R > 0$ die Reihe \wp auf $U_R(0) - \Lambda$ gleichmäßig absolut konvergiert. Es genügt offenbar, die absolute Konvergenz der Reihe

$$\sum_{\lambda \in \Lambda, |\lambda| > 2R} \left(\frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right)$$

zu zeigen, da sie sich nur um endlich viele Terme von \wp unterscheidet.

Nun ist nach einfacher Rechnung

$$\frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} = \frac{z}{\lambda^3} \frac{z/\lambda - 2}{(z/\lambda - 1)^2}.$$

Wegen $|z| < R$ und $|\lambda| > 2R$ ist $|z/\lambda - 1| > 1/2$ und $|z/\lambda - 2| < 5/2$. Damit folgt die Abschätzung

$$\left| \frac{z/\lambda - 2}{(z/\lambda - 1)^2} \right| < \frac{5}{2} \cdot \frac{4}{1} = 10$$

und weiter

$$\sum_{\lambda \in \Lambda, |\lambda| > 2R} \left| \frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} \right| < 10|z| \sum_{\lambda \in \Lambda, |\lambda| > 2R} \lambda^{-3}.$$

Die letzte Reihe ist aber die Betragsreihe zu $G_3(\Lambda)$, von der wir die absolute Konvergenz kennen. Somit folgt die erste Behauptung.

An der Reihe liest man nun die Pole und deren Ordnung direkt ab. Außerdem ist klar, dass $\wp(z) = \wp(-z)$ gilt, dass also \wp eine gerade Funktion ist. Wegen der lokal gleichmäßigen absoluten Konvergenz von \wp können wir \wp' durch gliedweises Ableiten berechnen und erhalten die behauptete Formel. Aus dieser liest man auch sofort ab, dass sich der Wert nicht ändert, wenn man z durch $z + \lambda$ ersetzt für jedes $\lambda \in \Lambda$. Damit ist \wp' eine elliptische Funktion. Sie ist offenbar ungerade.

Daraus folgt nun, dass auch \wp eine elliptische Funktion ist. Denn für festes $\lambda \in \Lambda$ können sich $\wp(z)$ und $\wp(z + \lambda)$ nur durch eine Integrationskonstante $k(\lambda)$ unterscheiden:

$$\wp(z) = \wp(z + \lambda) + k(\lambda).$$

Mit $z = -\lambda/2$ folgt also

$$\wp(-\lambda/2) = \wp(\lambda/2) + k(\lambda).$$

Da \wp aber gerade ist, muss $k(\lambda) = 0$ sein und wir sind fertig. □

[25.4.07] Wir kennen nun alle elliptischen Funktionen für ein gegebenes Gitter, wie uns der folgende Satz sagt. Die Idee dabei ist, dass nach den Liouville'schen Sätzen eine elliptische Funktion bereits durch ihre Pole und Nullstellen eindeutig bestimmt ist. Somit wird die Klassifikation darauf hinauslaufen, alle möglichen Kombinationen von Polen und Nullstellen durch die Weierstraß'sche- \wp -Funktion und ihre Ableitung auszudrücken.

Satz 2.3.5 *Jede elliptische Funktion (bzgl. Λ) ist von der Form*

$$f(z) = \frac{F(\wp(z), \wp'(z))}{G(\wp(z), \wp'(z))}$$

mit Polynomen $F, G \in \mathbb{C}[X]$ mit $G \neq 0$.

Beweis. 1. Schritt: Rückführung auf gerade elliptische Funktionen.

Die Funktion $g(z) := f(z) + f(-z)$ ist eine gerade elliptische Funktion, die Funktion $u(z) := f(z) - f(-z)$ ist eine ungerade und $w(z) := \wp'(z)u(z)$ ist wiederum eine gerade. Wegen

$$f(z) = \frac{1}{2}(g(z) + u(z))$$

genügt es, den Satz für gerade elliptische Funktionen zu beweisen.

2. Schritt: Sei H die "untere Hälfte der Fundamentalmasche", so dass zu jedem $z' \in H$ mit $2z' \notin \Lambda$ kein Translat von $-z'$ in H liegt. [Bild]

Hat dann f eine Null- oder Polstelle in $z' \in H$ mit $2z' \notin \Lambda$, so hat f eine weitere Null- oder Polstelle derselben Ordnung in $-z'$. Hat f eine Null- oder Polstelle in $z' \in H - \Lambda$ mit $2z' \in \Lambda$, dann hat diese eine gerade Ordnung.

Der erste Teil ist klar, weil f gerade ist. Wir zeigen nun, dass $\text{Ord}(f; \lambda)$ gerade ist im Falle $2\lambda \in \Lambda$ und $\lambda \notin \Lambda$.

Die Ableitung einer geraden Funktion ist ungerade und die einer ungeraden gerade:

$$f(z) = f(-z) \Rightarrow f'(z) = -f'(-z) \Rightarrow f^{(i)}(z) = (-1)^i f^{(i)}(-z).$$

Für ungerade i ist also $f^{(i)}(\lambda) = -f^{(i)}(-\lambda) = f^{(i)}(\lambda)$ (wegen $2\lambda \in \Lambda$) und somit $f^{(i)}(\lambda) = 0$. Ist $\text{Ord}(f; \lambda) = m > 0$ mit m ungerade, so leiten wir f jetzt m -mal ab: Die Ordnung von $f^{(m)}$ in λ ist dann 0, was $f^{(m)}(\lambda) = 0$ widerspricht. Ist $\text{Ord}(f; \lambda) < 0$, so wenden wir das gerade Gesagte auf $1/f$ an.

3. Schritt: Die Funktion $\wp(z) - \wp(z')$ für festes $z' \notin \Lambda$ in der Fundamentalmasche hat einen Pol der Ordnung 2 in 0 und eine doppelte Nullstelle bei z' , falls $2z' \in \Lambda$, und sonst eine einfache Nullstelle in z' und eine weitere einfache Nullstelle in dem Translat von $-z'$, das in der Fundamentalmasche liegt.

Dass die einzigen Pole in den Gitterpunkten liegen, wissen wir bereits. Die Ordnung bei 0 ist -2 , was aus der Reihendarstellung von \wp folgt. Wegen der Liouvilleschen Sätze muss es demnach in einer Fundamentalmasche entweder eine doppelte Nullstelle geben oder zwei einfache, denn die Ordnungen müssen sich zu 0 aufaddieren.

4. Schritt: Die elliptische Funktion

$$g(z) = \prod_{z' \in H - \{0\}, 2z' \notin \Lambda} (\wp(z) - \wp(z'))^{\text{Ord}(f; z')} \cdot \prod_{z' \in H - \{0\}, 2z' \in \Lambda} (\wp(z) - \wp(z'))^{\text{Ord}(f; z')/2}$$

ist bis auf eine Konstante gleich f .

Nach den vorherigen Schritten hat g bei $z' \in H - \{0\}$ dieselbe Ordnung wie f . Da sich nach den Liouvilleschen Sätzen die Ordnung bei 0 als minus die Summe über die Ordnung bei den anderen Punkten ergibt, muss sie bei 0 auch gleich sein. Daher ist f/g eine holomorphe elliptische Funktion ohne Null- oder Polstelle, also eine Konstante. \square

2.3.2 Komplexe elliptische Kurven

Sei Λ ein Gitter. Setze $g_2(\Lambda) := 60G_4(\Lambda)$ und $g_3(\Lambda) := 140G_6(\Lambda)$.

Satz 2.3.6 Sei Λ ein Gitter.

(a) Die Laurent-Reihe von $\wp(z)$ um 0 ist

$$\wp(z; \Lambda) = \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1)G_{2k+2}(\Lambda)z^{2k}.$$

(b) Für alle $z \in \mathbb{C} - \Lambda$ gilt

$$\wp'(z; \Lambda)^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda).$$

Beweis. Siehe [Silv], Prop. 3.5.

(a) Wir berechnen die Laurent-Reihe in einer Umgebung $U_\delta(0)$, die außer 0 keinen weiteren Punkt von Λ enthält und so, dass $|z/\lambda| < \epsilon < 1$ für alle $0 \neq \lambda \in \Lambda$ und alle $z \in U_\delta(0)$ gilt.

Durch Ableitung der geometrischen Reihe erhält man

$$\frac{1}{(1 - z/\lambda)^2} = \sum_{n=0}^{\infty} (n+1) \left(\frac{z}{\lambda}\right)^n.$$

Weiter gilt dann

$$\frac{1}{(z - \lambda)^2} - \frac{1}{\lambda^2} = \frac{1}{\lambda^2} \left(\frac{1}{(1 - z/\lambda)^2} - 1 \right) = \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\lambda^{n+2}}.$$

Die Reihe

$$\sum_{\lambda \in \Lambda, \lambda \neq 0} \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\lambda^{n+2}}$$

ist gleichmäßig absolut konvergent auf $U_\delta(0)$, wie man ganz ähnlich wie im Beweis der lokal gleichmäßigen absoluten Konvergenz von \wp zeigt. Daher dürfen wir im Folgenden die Reihen umordnen.

Wir berechnen:

$$\sum_{\lambda \neq 0} \left(\frac{1}{(1 - z/\lambda)^2} - \frac{1}{\lambda^2} \right) = \sum_{\lambda \neq 0} \sum_{n=1}^{\infty} (n+1) \frac{z^n}{\lambda^{n+2}} = \sum_{n=1}^{\infty} (n+1) z^n G_{n+2}.$$

Aus einer Aufgabe folgte, dass $G_k = 0$ für ungerade $k \geq 3$. Dies liefert Teil (a).

(b) Dies folgt daraus, dass die elliptische Funktion

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6$$

holomorph außerhalb von Λ ist und bei 0 verschwindet. Denn dann sagt ja der Satz von Liouville, dass f konstant gleich null sein muss.

Dass $f(z)$ bei 0 verschwindet, berechnet man einfach an der Laurent-Entwicklung aus Teil (a). □

Aufgabe 2.3.7 Beende den Beweis von Teil (b).

Satz 2.3.8 Sei Λ ein Gitter. Dann ist die Diskriminante des Polynoms $f(x) := 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ durch

$$\Delta(\Lambda) := g_2(\Lambda)^3 - 27g_3(\Lambda)^2$$

gegeben und sie ist stets ungleich null. Damit hat $f(x)$ also drei verschiedene Nullstellen.

Beweis. Siehe [Silv], Prop. 3.6 a.

Die Formel für die Diskriminante kann man in den meisten Algebra-Büchern nachlesen (oder selbst berechnen). Wir werden jetzt drei Nullstellen des Polynoms auflisten und zeigen, dass diese verschieden sind.

Seien w_1, w_2 eine Basis für Λ . Setze $w_3 := w_1 + w_2$. Dann gilt

$$\wp'(w_i/2) = -\wp'(-w_i/2) = -\wp'(w_i/2),$$

da \wp' eine ungerade elliptische Funktion ist. Also ist $\wp'(w_i/2) = 0$. Somit verschwindet f in $\wp(w_i/2)$ nach obigem Satz, Teil (b).

Die elliptische Funktion $\wp(z) - \wp(w_i/2)$ hat eine Nullstelle gerader Ordnung bei $w_i/2$ (nach dem 2. Schritt im Beweis der Darstellbarkeit von elliptischen Funktionen). Nach den Liouvilleschen Sätzen hat diese Funktion also einen Pol der Ordnung 2 bei 0 und eine doppelte Nullstelle bei $w_i/2$. Insbesondere ist $w_j/2$ keine Nullstelle für $j \neq i$, also ist auch $\wp(w_i/2) \neq \wp(w_j/2)$. \square

Satz 2.3.9 Sei Λ ein Gitter. Dann ist die Abbildung

$$\mathbb{C}/\Lambda - \{0\} \rightarrow \{(x, y) \in \mathbb{C}^2 \mid y^2 = f(x)\}, \quad z \mapsto (\wp(z), \wp'(z))$$

wohldefiniert und bijektiv.

Beweis. Siehe [FB], S. 275. Die Wohldefiniertheit ist gerade der Inhalt von Satz 2.3.6.

Wir zeigen zunächst die Surjektivität. Sei (u, v) gegeben mit $v^2 = f(u)$. Die Funktion $\wp : \mathbb{C} \rightarrow \mathbb{C}$ ist surjektiv, denn zu gegebenem $b \in \mathbb{C}$ hat die Funktion $\wp(z) - b$ in der Fundamentalmasche einen Pol der Ordnung 2 und somit nach den Liouvilleschen Sätzen auch mindestens eine Nullstelle. Insbesondere gibt es also ein z mit $\wp(z) = u$. Dann gilt aber $\wp'(z) = \pm v$. Insgesamt ist also $(u, v) = (\wp(z), \wp'(z))$ oder $(u, v) = (\wp(-z), \wp'(-z))$.

Als Nächstes wenden wir uns der Injektivität zu. Wir nehmen an, dass $\wp(z) = \wp(t)$ und $\wp'(z) = \wp'(t)$ sind. Wie wir jetzt schon oft gesehen haben, hat $\wp(z) - \wp(t)$ in der Fundamentalmasche entweder genau eine doppelte Nullstelle oder zwei einfache, die dann bei t und $-t$ liegen (nach Translation). Somit folgt aus $\wp(z) = \wp(t)$, dass sich $z - t \in \Lambda$ oder $z + t \in \Lambda$. Tritt der erste Fall ein, so sind wir schon fertig. Im zweiten Fall benutzen wir, dass \wp' ungerade ist:

$$\wp'(z) = \wp'(-t) = -\wp'(t) = -\wp'(z),$$

also $\wp'(z) = 0$. Dann ist nach der Differentialgleichung aber $z = w_i/2$ für ein i (siehe vorigen Beweis), also $2z \in \Lambda$ und daher $t + z = t - z + 2z \in \Lambda$, also $t - z \in \Lambda$. \square

Man nennt Punktemengen der obigen Form *elliptische Kurven*. Der Satz sagt also, dass Tori ohne den Nullpunkt elliptische Kurven sind. Benutzt man projektive Kurven, was wir jetzt nicht tun möchten, so kann man der Kurve einen “unendlich fernen” Punkt hinzufügen, der dann dem Nullpunkt des Torus entspricht.

Außerdem kann man von obiger Abbildung zeigen, dass sie holomorphe Strukturen (in einem geeigneten Sinn) erhält. Dies interessiert uns jetzt nicht, da wir uns mit der holomorphen Struktur auf dem Torus zufrieden geben können.

2.4 Definition von Modulformen (der Stufe 1)

2.4.1 Beispiele

[26.4.2007] Aus den im vorigen Abschnitt behandelten Funktionen machen wir nun schwache Modulformen.

Definition 2.4.1 (a) $g_2(\Lambda) := 60G_4(\Lambda)$, $g_2(\tau) := 60G_4(\tau)$

(b) $g_3(\Lambda) := 140G_6(\Lambda)$, $g_3(\tau) := 140G_6(\tau)$

(c) $\Delta(\Lambda) = g_2(\Lambda)^3 - 27g_3(\Lambda)^2$, $\Delta(\tau) = g_2(\tau)^3 - 27g_3(\tau)^2$

(d) $j(\Lambda) := g_2^3(\Lambda)/\Delta(\Lambda)$, $j(\tau) := g_2^3(\tau)/\Delta(\tau)$

Bemerkung 2.4.2 Die Funktionen G_4 und G_6 sind schwache Modulformen von Gewicht 4 und 6 zu $\mathrm{SL}_2(\mathbb{Z})$, wie wir aus der Einleitung wissen.

Die Funktion $\Delta : \mathbb{H} \rightarrow \mathbb{C}$ ist holomorph und erfüllt

$$\Delta\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^{12} \Delta(\tau)$$

für alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Damit ist sie eine schwache Modulform von Gewicht 12 zu $\mathrm{SL}_2(\mathbb{Z})$.

Wir haben gesehen (Satz 2.3.8), dass Δ keine Nullstelle besitzt. Daher ist die Funktion $j(\tau) : \mathbb{H} \rightarrow \mathbb{C}$ ebenfalls holomorph und erfüllt

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau)$$

für alle $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Damit ist sie eine schwache Modulform von Gewicht 0 ebenfalls zu $\mathrm{SL}_2(\mathbb{Z})$.

2.4.2 Definition und Beispiele

In diesem Abschnitt kommen wir zur Definition von Modulformen der Stufe 1.

Wir erinnern an den Satz der Einleitung der besagt, dass jede holomorphe Funktion $f : \mathbb{H} \rightarrow \mathbb{C}$, die periodisch der Periode 1 ist, also

$$f(\tau + 1) = f(\tau) \quad \forall \tau \in \mathbb{H},$$

eine Fourier-Reihe

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i \tau n}$$

besitzt. Ferner erinnern wir an die Operation von $\mathrm{SL}_2(\mathbb{Z})$ auf \mathbb{H} :

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

Insbesondere ist also

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tau = \tau + 1.$$

Definition 2.4.3 Eine Modulfunktion vom Gewicht k zu $SL_2(\mathbb{Z})$ ist eine holomorphe Funktion

$$f : \mathbb{H} \rightarrow \mathbb{C},$$

die der Transformationsregel

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau\right) = f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \quad \forall \tau \in \mathbb{H} \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

genügt (und damit $f\left(\begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix} \cdot \tau\right) = f(\tau + 1) = f(\tau)$) und deren Fourier-Entwicklung eine Laurent-Reihe ist:

$$f(\tau) = \sum_{n=-m}^{\infty} a_n e^{2\pi i \tau n}$$

(für ein $m \in \mathbb{Z}$).

Definition 2.4.4 Eine Modulfunktion f von Gewicht k zu $SL_2(\mathbb{Z})$ heißt Modulform, falls ihre Fourier-Entwicklung eine Taylor-Reihe ist:

$$f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i \tau n}.$$

Definition 2.4.5 Eine Modulform f von Gewicht k zu $SL_2(\mathbb{Z})$ heißt Spitzenform, falls ihre Fourier-Entwicklung eine Taylor-Reihe ohne konstanten Term ist:

$$f(\tau) = \sum_{n=1}^{\infty} a_n e^{2\pi i \tau n}.$$

Bemerkung 2.4.6 Modulformen von Gewicht k zu $SL_2(\mathbb{Z})$ nennt man auch Modulformen von Gewicht k der Stufe 1. Für Modulfunktionen und Spitzenformen benutzt man die analoge Terminologie.

Im folgenden Kapitel über Modulformen zu Kongruenzuntergruppen wird die Bezeichnung ‘‘Stufe 1’’ erklärt.

Beispiel 2.4.7 (a) Die konstanten Funktionen sind Modulformen vom Gewicht 0 und Stufe 1.

(b) Die Eisenstein-Reihen $G_k(\tau)$ für gerade $k \geq 4$ sind Modulformen von Gewicht k und Stufe 1.

(c) Die Δ -Funktion ist eine Spitzenform von Gewicht 12 und Stufe 1. Die Koeffizienten der Taylor-Entwicklung bezeichnet man traditionell mit $\tau(n)$. Man nennt τ die Ramanujan-Funktion.

Die noch stets unbewiesene Lehmer-Vermutung behauptet, dass $\tau(n) \neq 0$ für alle $n \geq 1$.

(d) Die j -Funktion ist eine Modulfunktion vom Gewicht 0 und Stufe 1.

Bemerkung 2.4.8 Sei $k = 4a + 6b$. Dann ist $(G_4)^a (G_6)^b$ eine Modulform vom Gewicht k und Stufe 1. Wir werden später sehen (Satz 3.1.15), dass die so erhaltenen Modulformen eine Basis für den Vektorraum aller Modulformen vom Gewicht k und Stufe 1 bilden.

Bemerkung 2.4.9 Modulformen ungeraden Gewichtes und Stufe 1 sind konstant gleich 0. Denn durch Anwendung der Matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ erhält man $f(\tau) = f\left(\frac{-1\tau+0}{0\tau-1}\right) = (-1)^k f(\tau) = -f(\tau)$ für alle τ , also $f = 0$.

2.4.3 Gitter-Funktionen und Funktionen auf elliptischen Kurven

Wir erinnern uns an die Eisenstein-Reihe $G_k(\Lambda)$. Diese erfüllt

$$G_k(s\Lambda) = s^{-k}G_k(\Lambda),$$

wie wir gesehen haben.

Definition 2.4.10 *Eine Funktion*

$$F : \{\text{Gitter}\} \rightarrow \mathbb{C}$$

heißt Gitter-Funktion von Gewicht k , falls gilt

$$F(s\Lambda) = s^{-k}F(\Lambda) \quad \forall \text{ Gitter } \Lambda.$$

Somit ist G_k also eine Gitter-Funktion von Gewicht k . Viel allgemeiner gilt aber, dass alle (schwachen) Modulformen Gitter-Funktionen ergeben.

Satz 2.4.11 *Sei $f : \mathbb{H} \rightarrow \mathbb{C}$ eine Modulfunktion von Gewicht k und Stufe 1. Dann wird durch die Zuordnung*

$$F(\Lambda_{\omega_1, \omega_2}) = \omega_2^{-k} f\left(\frac{\omega_1}{\omega_2}\right)$$

(Spezialfall: $F(\Lambda_\tau) = f(\tau)$), wobei wir ohne Einschränkung $\omega_1/\omega_2 \in \mathbb{H}$ annehmen, eine eindeutige Gitter-Funktion von Gewicht k definiert.

Beweis. Wir müssen die Wohldefiniertheit und die Transformationsregel überprüfen. Fangen wir unter Annahme der Wohldefiniertheit mit Letzterem an:

$$F(s\Lambda_{\omega_1, \omega_2}) = F(\Lambda_{s\omega_1, s\omega_2}) = s^{-k} \omega_2^{-k} f\left(\frac{s\omega_1}{s\omega_2}\right) = s^{-k} F(\Lambda_{\omega_1, \omega_2}).$$

Nun die Wohldefiniertheit. Die Frage ist, ob die Definition von der Wahl der Basis ω_1, ω_2 von $\Lambda_{\omega_1, \omega_2}$ unabhängig ist. Wie wir aber gesehen haben, ergibt sich jede andere Basis als $a\omega_1 + b\omega_2, c\omega_1 + d\omega_2$ mit gewissen $a, b, c, d \in \mathbb{Z}$, die eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\text{SL}_2(\mathbb{Z})$ bilden. Berechnen wir also die Gleichheit:

$$\begin{aligned} F(\Lambda_{a\omega_1 + b\omega_2, c\omega_1 + d\omega_2}) &= (c\omega_1 + d\omega_2)^{-k} f\left(\frac{a\omega_1 + b\omega_2}{c\omega_1 + d\omega_2}\right) \\ &= \omega_2^{-k} \left(c\frac{\omega_1}{\omega_2} + d\right)^{-k} f\left(\frac{a\frac{\omega_1}{\omega_2} + b}{c\frac{\omega_1}{\omega_2} + d}\right) = \omega_2^{-k} f\left(\frac{\omega_1}{\omega_2}\right) = F(\Lambda_{\omega_1, \omega_2}). \end{aligned}$$

Dies war zu zeigen. □

Bemerkung 2.4.12 *Da wir ja wissen, dass für ein Gitter Λ der Torus \mathbb{C}/Λ eine komplexe elliptische Kurve ist, können wir Gitter-Funktionen auch als Funktionen auf der Menge der komplexen elliptischen Kurven betrachten:*

$$F : \{\text{Komplexe elliptische Kurven}\} \rightarrow \mathbb{C},$$

die $F(\mathbb{C}/s\Lambda) = s^{-k}F(\mathbb{C}/\Lambda)$ erfüllen.

Der Spezialfall $k = 0$ ist besonders interessant. Fassen wir erstmal einige Resultate über komplexe elliptische Kurven in einem Satz zusammen.

Satz 2.4.13 *Die Abbildung*

$$\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \longrightarrow \{\text{Komplexe elliptische Kurven}\} / \cong,$$

die durch $\tau \mapsto \mathbb{C}/\Lambda_\tau$ gegeben ist, ist bijektiv.

Hierbei bedeutet \cong die Äquivalenzrelation, die durch Isomorphie von elliptischen Kurven gegeben ist. Den Bahnraum $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ betrachten wir jetzt gerade einfach als eine Menge. Das folgende Kapitel wird dem Studium analytischer Strukturen auf dieser und ähnlicher Mengen gewidmet sein.

Beweis. Wir haben bereits alles gesehen, es aber nicht so formuliert. Die Abbildung ist wohldefiniert, denn die elliptischen Kurven \mathbb{C}/Λ_τ und $\mathbb{C}/\Lambda_{\frac{a\tau+b}{c\tau+d}}$ sind isomorph, da die letztere isomorph ist zu $\mathbb{C}/\Lambda_{a\tau+b, c\tau+d}$, welche gleich der ersten ist, da ja die Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ die Determinante 1 hat und somit nur einen Basiswechsel durchführt.

Seien nun umgekehrt \mathbb{C}/Λ_τ und $\mathbb{C}/\Lambda_\sigma$ isomorph. Wir haben in dem Abschnitt über elliptische Kurven bewiesen, dass jeder Isomorphismus von der Multiplikation mit einer Zahl $x \in \mathbb{C}^\times$ kommt. Insbesondere ist also $x\Lambda_\sigma = \Lambda_{x\sigma, x}$ gleich Λ_τ , weshalb es $a, b, c, d \in \mathbb{Z}$ gibt mit $x\sigma = a\tau + b$ und $x = c\tau + d$. Daher erhalten wir $\sigma = \frac{a\tau+b}{c\tau+d}$. Genauso wie im Kapitel über elliptische Kurven sieht man, dass $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ liegt. Dies zeigt die Injektivität.

Schließlich die Surjektivität. Sei eine beliebige elliptische Kurve $\mathbb{C}/\Lambda_{\omega_1, \omega_2}$ gegeben. Diese ist, wie wir gesehen haben, isomorph zu $\mathbb{C}/\Lambda_{\frac{\omega_1}{\omega_2}}$, wobei der Isomorphismus durch ω_2^{-1} gegeben wird. Diese ist aber offensichtlich im Bild. \square

Bemerkung 2.4.14 *Kommen wir nun zum Spezialfall $k = 0$ von Funktionen auf elliptischen Kurven wie in der vorherigen Bemerkung. Dann gilt also*

$$F(\mathbb{C}/s\Lambda) = F(\Lambda).$$

Damit ist also F eine Funktion

$$F : \{\text{Komplexe elliptische Kurven}\} / \cong \longrightarrow \mathbb{C}.$$

Wir werden später sehen, dass die j -Funktion (genauer, die zur j -Funktion zugeordnete Funktion auf Gittern bzw. elliptischen Kurven) eine Bijektion zwischen den komplexen elliptischen Kurven bis auf Isomorphie und \mathbb{C} herstellt.

Damit ist jede komplexe elliptische Kurve \mathbb{C}/Λ eindeutig durch $j(\Lambda)$ bestimmt.

2.4.4 Nochmal Eisenstein-Reihen

[2.5.2007] Wir werden in diesem Abschnitt noch einige in der Einleitung offen gebliebene Aussagen beweisen und die Fourier-Entwicklung der Eisenstein-Reihen noch einmal schöner aufschreiben.

Wir beginnen mit der Definition der Bernoulli-Zahlen. Dazu betrachten wir die Funktion

$$f(z) := \frac{z}{e^z - 1} = \frac{z}{\sum_{n=1}^{\infty} z^n/n!} = \frac{1}{\sum_{n=0}^{\infty} z^n/(n+1)!}.$$

Diese ist also holomorph in 0 und wir können dort ihre Taylor-Reihe betrachten. Diese schreiben wir in der folgenden Form:

$$f(z) = \sum_{n=0}^{\infty} \frac{B_n}{n!} z^n.$$

Die Koeffizienten B_n heißen *Bernoulli-Zahlen*.

Aufgabe 2.4.15 Zeige (zum Beispiel durch Invertieren der Potenzreihe zu $1/f$) die Gleichung

$$\binom{n+1}{1} B_n + \binom{n+1}{2} B_{n-1} + \cdots + \binom{n+1}{n} B_1 + \binom{n+1}{n+1} B_0 = 0.$$

Folgere

$$B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}$$

und $B_n = 0$ für alle ungeraden $n \geq 3$.

Wir werden nun im Folgenden einen Satz von Euler beweisen, der die Werte der Riemannschen ζ -Funktion an positiven geraden Zahlen berechnet.

Satz 2.4.16 (Euler) Für $k \in \mathbb{N}$ gilt die Identität

$$\zeta(2k) = \frac{(-1)^{k+1} (2\pi)^{2k}}{2(2k)!} B_{2k}.$$

Insbesondere hat man $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$ und $\zeta(6) = \pi^6/945$.

Zum Beweis benötigen wir zunächst den folgenden Satz, den wir bereits in der Einleitung verwendet haben.

Satz 2.4.17 Es gilt die Identität

$$\pi \cot \pi z = \frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right)$$

auf $\mathbb{C} - \mathbb{Z}$. Die auftretende Reihe ist auf $\mathbb{C} - \mathbb{Z}$ lokal gleichmäßig absolut konvergent.

Beweis. Wir folgen [FB], S. 183, und zeigen, dass

$$\pi \cot \pi z = \frac{1}{z} + \sum_{n \in \mathbb{Z}, n \neq 0} \frac{z}{(z-n)n}$$

gilt, wobei die Reihe rechts lokal gleichmäßig absolut auf $\mathbb{C} - \mathbb{Z}$ konvergiert. Dann dürfen wir sie nämlich umordnen und erhalten die Aussage des Satzes wegen

$$\frac{z}{(z-n)n} = \frac{1}{z-n} + \frac{1}{n}.$$

Die lokal gleichmäßig absolute Konvergenz folgt übrigens sofort aus der Konvergenz der Reihe $\sum_{n=1}^{\infty} \frac{1}{n^2}$ wegen $\frac{z}{(z-n)n} = z \frac{n}{z-n} \frac{1}{n^2}$.

Wir betrachten für den Beweis obiger Gleichheit für festes $z \in \mathbb{C} - \mathbb{Z}$ die Funktion

$$f(w) = \frac{z}{w(z-w)} \pi \cot \pi w$$

und berechnen ihre Polstellen. Dazu schauen wir uns kurz den Kotangens bei 0 an:

$$\pi \cot \pi w = \pi \frac{\cos \pi w}{\sin \pi w} = \pi \frac{1 + \dots}{\pi w + \dots} = \pi \frac{1}{w} \frac{1 + \dots}{1 + \dots} = \frac{1}{w} \frac{1 + \dots}{1 + \dots}.$$

Daher hat $\pi \cot \pi w$ bei 0 und somit wegen der Periodizität (die Periode ist π) bei allen ganzen Zahlen einen Pol der Ordnung 1 mit Residuum 1. Somit hat f also

- bei $w = z$ einen Pol 1. Ordnung mit Residuum $-\pi \cot \pi z$,
- bei $w = n \in \mathbb{Z} - \{0\}$ einen Pol 1. Ordnung mit Residuum $\frac{z}{(z-n)z}$,
- bei $w = 0$ einen Pol 2. Ordnung mit Residuum $\frac{1}{z}$ (das muss man etwas länglich nachrechnen),
- und sonst keine weiteren Pole.

Wir wollen nun den Residuensatz anwenden. Dazu integrieren wir entlang dem Quadrat, dessen Seiten parallel zu den Achsen sind und von diesen den Abstand $N + \frac{1}{2}$ haben für ein $N \in \mathbb{N}$ [Bild]. Dann liegt auf dem Integrationsweg kein Pol, falls wir $N > |z|$ wählen. Der Residuensatz liefert dann:

$$\frac{1}{2\pi i} \int f(w) dw = -\pi \cot \pi z + \frac{1}{z} + \sum_{0 < |n| \leq N} \frac{z}{n(z-n)}.$$

Nun wollen wir zeigen, dass für $N \rightarrow \infty$, die linke Seite gegen 0 geht.

Dazu überlegen wir uns zuerst, dass der Kotangens auf den Quadratseiten beschränkt ist. Wir berechnen

$$\cot \pi w = i \frac{e^{\pi i w} + e^{-\pi i w}}{e^{\pi i w} - e^{-\pi i w}} = i \frac{e^{2\pi i w} + 1}{e^{2\pi i w} - 1} = i + \frac{2i}{e^{2\pi i w} - 1} = i + \frac{2i}{e^{2\pi i x} e^{-2\pi y} - 1}$$

für $w = x + iy$. Ist $|y|$ weg von 1, z. B. $|y| > 1$, ist dieser Ausdruck offenbar betragsmäßig nach oben beschränkt. Nun setzen wir $w = N + \frac{1}{2} + iy$ oder $w = -(N + \frac{1}{2}) + iy$ ein.

$$\frac{2i}{e^{2\pi i x} e^{-2\pi y} - 1} = \frac{-2i}{e^{-2\pi y} + 1}.$$

Dies ist offenbar auch beschränkt. Also ist $|\pi \cot \pi w|$ entlang dem ganzen Quadrat nach oben beschränkt, sagen wir durch $C > 0$.

Nun schätzen wir das Integral ab.

$$\left| \int f(w) dw \right| \leq \int |f(w)| dw \leq C \int \left| \frac{z}{w(w-z)} \right| dw.$$

Dies schätzen wir weiter ab, indem wir den Integranden gegen eine Konstante abschätzen. Es gilt nämlich auf allen vier Wegstücken:

$$|w| \geq N + \frac{1}{2}$$

und

$$|w - z| \geq ||w| - |z|| \geq N + \frac{1}{2} - |z|.$$

Somit folgt:

$$\left| \int f(w) dw \right| \leq 4(2N + 1) \frac{|z|}{(N + \frac{1}{2})(N + \frac{1}{2} - |z|)}.$$

Dies geht aber offensichtlich gegen 0 für $N \rightarrow \infty$, was zu zeigen war. \square

Beweis des Satzes von Euler. Siehe [FB], S. 185. Der Beweis besteht daraus, dass man zwei verschiedene Reihendarstellungen von $\pi \cot \pi z$ miteinander vergleicht. Beginnen wir mit der aus obigem Satz:

$$z\pi \cot \pi z = 1 + \sum_{n=1}^{\infty} \left(\frac{z}{z+n} + \frac{z}{z-n} \right) = 1 + \sum_{n=1}^{\infty} \frac{2z^2}{z^2 - n^2}.$$

Jetzt verwenden wir wieder die geometrische Reihe

$$\frac{1}{z^2 - n^2} = -\frac{1}{n^2} \sum_{k=0}^{\infty} \left(\frac{z^2}{n^2} \right)^k$$

und setzen diese ein:

$$z\pi \cot \pi z = 1 + 2z^2 \sum_{n=1}^{\infty} \left(-\frac{1}{n^2} \sum_{k=0}^{\infty} \left(\frac{z^2}{n^2} \right)^k \right).$$

Diese Reihe ist wiederum gleichmäßig absolut konvergent (in einer Umgebung von 0), da für reelles positives z , das keine ganze Zahl ist, alle Terme positiv sind. Daher können wir die Reihe umsortieren, insbesondere die beiden Summen vertauschen:

$$z\pi \cot \pi z = 1 - 2 \sum_{k=0}^{\infty} \left(\sum_{n=1}^{\infty} \frac{1}{n^{2k+2}} \right) z^{2k+2} = 1 - 2 \sum_{k=1}^{\infty} \left(\sum_{n=1}^{\infty} \frac{1}{n^{2k}} \right) z^{2k} = 1 - 2 \sum_{k=1}^{\infty} \zeta(2k) z^{2k}.$$

Nun leiten wir einen zweiten Ausdruck für die linke Seite her. So wie im letzten Beweis erhalten wir

$$\pi z \cot \pi z = \pi i z + \frac{2\pi i z}{e^{2\pi i z} - 1}.$$

Rechts steht jetzt aber die definierende Funktion der Bernoulli-Zahlen (in der Variablen $2\pi i z$). Somit können wir die Gleichung umschreiben:

$$\begin{aligned} \pi z \cot \pi z &= \pi i z + \sum_{k=0}^{\infty} \frac{B_k}{k!} (2\pi i z)^k = 1 + \sum_{k=1}^{\infty} \frac{B_{2k}}{(2k)!} (2\pi i z)^{2k} \\ &= 1 + \sum_{k=1}^{\infty} \frac{B_{2k}}{(2k)!} 2^{2k} \pi^{2k} (-1)^k z^{2k}, \end{aligned}$$

wobei wir $B_0 = 1$, $B_1 = -\frac{1}{2}$ und $B_k = 0$ für ungerade $k \geq 3$ benutzt haben.

Der Beweis wird durch Koeffizientenvergleich abgeschlossen. \square

Korollar 2.4.18 Sei $k \geq 4$ gerade. Dann gilt

$$G_k(\tau) = \frac{2(2\pi)^k (-1)^{k/2}}{(k-1)!} \left(-\frac{B_k}{2k} + \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n \right).$$

Beweis. Einsetzen. □

Bis auf einen transzendenten Faktor hat die Eisenstein-Reihe G_k also rationale Fourier-Koeffizienten, die sogar mit Ausnahme des konstanten Terms ganze Zahlen sind.

2.5 Modulformen höherer Stufe

2.5.1 Kongruenzuntergruppen

Lemma 2.5.1 Sei $N \in \mathbb{N}$. Reduktion modulo N definiert einen surjektiven Gruppenhomomorphismus $\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\pi} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Aufgabe 2.5.2 Beweise das Lemma.

Definition 2.5.3 Der Kern der Reduktion modulo N -Abbildung heißt Hauptkongruenzuntergruppe der Stufe N und wird mit $\Gamma(N)$ bezeichnet.

Jede Untergruppe $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$, die ein $\Gamma(N)$ enthält, wird Kongruenzuntergruppe genannt.

Wir kommen nun zu den Kongruenzuntergruppen, mit denen wir hauptsächlich arbeiten werden, nämlich $\Gamma_0(N)$ und $\Gamma_1(N)$. Die erstere haben wir bereits in der Einleitung kennen gelernt.

Dazu betrachten wir in Anbetracht obigen Lemmas zwei Untergruppen von $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, nämlich

$$G_0(N) := \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}$$

und

$$G_1(N) := \left\{ \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \right\}.$$

Wir definieren nun für $\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\pi} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ die Gruppe $\Gamma_0(N)$ als $\pi^{-1}(G_0)$ und die Gruppe $\Gamma_1(N)$ als $\pi^{-1}(G_1)$.

Explizit bedeutet dies:

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

und

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Die Gruppen $\Gamma_1(N)$ und $\Gamma_0(N)$ sind keine Normalteiler von $\mathrm{SL}_2(\mathbb{Z})$, sobald $N > 1$. Die Hauptkongruenzuntergruppe ist als Kern eines Gruppenhomomorphismus natürlich wohl ein Normalteiler.

Lemma 2.5.4 Die Abbildung

$$\Gamma_1(N) \backslash \Gamma_0(N) \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \pmod N} (\mathbb{Z}/N\mathbb{Z})^\times$$

ist ein Gruppenisomorphismus.

Beweis. Das ist einfach nachzurechnen. □

Als Nächstes wollen wir den Index der oben eingeführten Gruppen in $SL_2(\mathbb{Z})$ berechnen. Dazu werden wir jeweils Bijektionen der Nebenklassen auf einfachere Mengen hinschreiben, die es auch im Prinzip erlauben, Repräsentanten der Nebenklassen hinzuschreiben.

Dazu zunächst eine Definition.

Definition 2.5.5 Sei R ein Ring (kommutativ mit Eins). Wir definieren die projektive Gerade über R als

$$\mathbb{P}^1(R) := \{(a : b) \mid a, b \in R, \exists r, s \in R : 1 = ar + bs\} / \sim,$$

wobei zwei Paare $(a : b)$ und $(a' : b')$ äquivalent sind, falls es $r \in R^\times$ gibt mit $ar = a'$ und $br = b'$.

Lemma 2.5.6 Sei N eine natürliche Zahl. Dann gelten:

(a) $\varphi(N) = \#(\mathbb{Z}/N\mathbb{Z})^\times = N \prod_{l \mid N} (1 - \frac{1}{l})$.

(b) $\#\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = N \prod_{l \mid N} (1 + \frac{1}{l})$.

(c) $\#\{(a, b) \mid a, b \in \mathbb{Z}/N\mathbb{Z}, \exists r, s \in \mathbb{Z}/N\mathbb{Z} : 1 = ar + bs\} = N^2 \prod_{l \mid N} (1 - \frac{1}{l^2})$.

Beweis. (a) ist aus der elementaren Zahlentheorie bekannt und folgt einfach daraus, dass es in $(\mathbb{Z}/p^r\mathbb{Z})^\times$ genau p^{r-1} Nicht-Einheiten gibt.

(b) Zunächst gilt die Multiplikativität bezüglich teilerfremder Zahlen, also insbesondere

$$\#\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = \prod_{i=1}^n \#\mathbb{P}^1(\mathbb{Z}/l_i^{e_i}\mathbb{Z})$$

für $N = \prod_{i=1}^n l_i^{e_i}$. Dazu können wir uns die Tupel komponentenweise geschrieben vorstellen. Wir überlegen uns leicht, dass die Menge

$$\{(a : 1) \mid a \text{ ist Nicht-Einheit}\} \dot{\cup} \{(1 : b) \mid b \in \mathbb{Z}/p^e\mathbb{Z}\}$$

ein Repräsentantensystem für $\mathbb{P}^1(\mathbb{Z}/p^e\mathbb{Z})$ ist. Somit ist ihre Anzahl gleich $p^{e-1} + p^e = p^e(1 + \frac{1}{p})$. Daraus folgt die behauptete Formel.

(c) folgt sofort aus (a) und (b) durch Multiplikation mit $\varphi(N)$. □

[3.5.2007]

Satz 2.5.7 (a) Die Abbildung

$$\Gamma_0(N) \backslash \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\text{mod } N} G_0(N) \backslash \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (c:d) \text{ mod } N} \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$$

ist eine Bijektion und es gilt $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{l|N} (1 + \frac{1}{l})$.

(b) Die Abbildung

$$\Gamma_1(N) \backslash \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\text{mod } N} G_1(N) \backslash \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto (c,d) \text{ mod } N} \{(c,d) | c, d \in \mathbb{Z}/N\mathbb{Z}, \exists r, s \in \mathbb{Z}/N\mathbb{Z} : 1 = cr + ds\}$$

ist eine Bijektion und es gilt $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = N^2 \prod_{l|N} (1 - \frac{1}{l^2})$.

(c) Die Abbildung

$$\Gamma(N) \backslash \mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\text{mod } N} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

ist eine Bijektion und es gilt $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{l|N} (1 - \frac{1}{l^2})$.

Beweis. Die Bijektionen folgen unmittelbar aus den Definitionen. Für die Formeln berechnet man ganz einfach, dass $G_1(N)$ genau aus N und $G_0(N)$ aus $N\varphi(N)$ Elementen besteht. Dann wendet man das vorangehende Lemma an. \square

Aufgabe 2.5.8 (a) Beweise, dass $\Gamma(2)$ erzeugt wird von den Matrizen $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ und $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

Anleitung:

- *Bemerke zunächst, dass $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$ genau dann, wenn a, d ungerade, b, c gerade und $ad - bc = 1$. Insbesondere sind also $\mathrm{ggT}(a, b) = 1$ und $\mathrm{ggT}(a, c) = 1$.*

- *Beweise nun, dass man durch Rechtsmultiplikation von $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ jede Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(2)$ auf die Form $\begin{pmatrix} * & 0 \\ * & * \end{pmatrix}$ bringen kann.*

*Dazu kann man eine Form des euklidischen Algorithmus verwenden: Ist $|a| < |b|$, dann gibt es ein $n \in \mathbb{Z}$, so dass $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 2na+b \\ * & * \end{pmatrix}$ und $|2na + b| < |a|$. Ist $0 < |b| < |a|$, dann gibt es ein $m \in \mathbb{Z}$, so dass $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2m & 1 \end{pmatrix} = \begin{pmatrix} a+2mb & b \\ * & * \end{pmatrix}$ und $|a + 2mb| < |b|$. Folgere hieraus die Behauptung dieses Punktes.*

- *Zeige nun, dass jede Matrix der Form $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix} \in \Gamma(2)$ ein Produkt von $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ und $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ ist.*

(b) Die Θ -Gruppe Γ_θ ist die Untergruppe von $\mathrm{SL}_2(\mathbb{Z})$, die von $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ erzeugt wird.

Zeige, dass sie $\Gamma(2)$ enthält und somit eine Kongruenzuntergruppe ist.

2.5.2 Spitzen

Die geometrische Erklärung des Begriffs der Spitze wird erst im folgenden Kapitel deutlich werden.

Definition 2.5.9 Die Menge der Spitzen ist $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, wobei wir $(a : b)$ als $\frac{a}{b}$ für $b \neq 0$ und $(a : 0)$ als ∞ auffassen.

Die Gruppe $\mathrm{SL}_2(\mathbb{Z})$ operiert auf der Menge der Spitzen wie auf \mathbb{H} durch gebrochen lineare Transformationen, d.h.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \frac{r}{s} = \frac{a\frac{r}{s} + b}{c\frac{r}{s} + d} = \frac{ar + bs}{cr + ds}.$$

Lemma 2.5.10 Fasst man die Spitze $\frac{r}{s}$ als Vector $\begin{pmatrix} r \\ s \end{pmatrix}$ auf, so ergibt sich die Operation von $\mathrm{SL}_2(\mathbb{Z})$ wie folgt. Es sei $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r \\ s \end{pmatrix} = \begin{pmatrix} r' \\ s' \end{pmatrix}$. Dann ist $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \frac{r}{s} = \frac{r'}{s'}$. Diese Darstellung funktioniert auch für $\infty = \frac{r}{0}$.

Beweis. Dies ist eine einfache Rechnung. □

Lemma 2.5.11 Die Bahn der Spitze ∞ unter der Operation von $\mathrm{SL}_2(\mathbb{Z})$ ist die Menge aller Spitzen. Der Stabilisator von ∞ ist

$$\mathrm{SL}_2(\mathbb{Z})_\infty = \left\{ \pm \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \mid n \in \mathbb{Z} \right\} = \langle \pm 1, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle.$$

Beweis. Dass ∞ in der Bahn liegt, ist klar. Sei $\frac{a}{c} \neq \infty$ eine Spitze in gekürzter Bruchdarstellung. Dann sind a und c teilerfremd, es gibt also $b, d \in \mathbb{Z}$ mit $1 = ad - bc$ (nach dem Euklidischen Algorithmus). Damit ist $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ und $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \frac{a}{c}$.

Nun bleibt noch der Stabilisator zu berechnen:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \frac{a}{c} = \infty.$$

Dann ist also $c = 0$ und $a \neq 0$. Wegen $1 = ad - bc = ad$ folgt, dass $a = d = \pm 1$. Damit ist also $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$ mit $a = \pm 1$, wie behauptet. □

Eine Umformulierung des Lemmas ist zu sagen, dass der Bahnenraum

$$\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{P}^1(\mathbb{Q})$$

aus nur einem Element besteht.

Definition 2.5.12 Sei $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ eine Untergruppe endlichen Indexes. Dann heißt der Bahnenraum $\Gamma \backslash \mathbb{P}^1(\mathbb{Q})$ die Menge der Spitzenklassen von Γ .

Lemma 2.5.13 Sei $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ eine Untergruppe von endlichem Index. Die Menge der Spitzenklassen von Γ ist kleiner gleich dem Index $(\mathrm{SL}_2(\mathbb{Z}) : \Gamma)$.

Beweis. Aus dem ersten Teil des vorigen Lemmas folgt die Surjektion

$$\mathrm{SL}_2(\mathbb{Z}) \xrightarrow{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty} \mathbb{P}^1(\mathbb{Q}).$$

Diese ergibt eine Surjektion

$$\Gamma \backslash \mathrm{SL}_2(\mathbb{Z}) \rightarrow \Gamma \backslash \mathbb{P}^1(\mathbb{Q}),$$

die die Behauptung beweist. □

Satz 2.5.14 Sei $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ eine Untergruppe endlichen Indexes. Sei $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Dann ist der Stabilisator in Γ der Spitze $\frac{a}{c}$ gleich

$$\Gamma_{\frac{a}{c}} = \Gamma \cap \sigma \langle \pm 1, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle \sigma^{-1} = \Gamma \cap \langle \pm 1, \sigma \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \sigma^{-1} \rangle.$$

Ferner gibt es eine kleinste positive Zahl h , die Weite der Spitze $\frac{a}{c}$, derart dass $\sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \sigma^{-1} \in \Gamma_{\frac{a}{c}}$ oder $\sigma \begin{pmatrix} -1 & -h \\ 0 & -1 \end{pmatrix} \sigma^{-1} \in \Gamma_{\frac{a}{c}}$. Dann ist $\Gamma_{\frac{a}{c}}$ entweder gleich $\langle \sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \sigma^{-1} \rangle$, gleich $\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \sigma \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \sigma^{-1} \rangle$ oder gleich $\langle \sigma \begin{pmatrix} -1 & -h \\ 0 & -1 \end{pmatrix} \sigma^{-1} \rangle$. In den ersten beiden Fällen heißt die Spitze $\frac{a}{c}$ regulär und im letzten Fall irregulär.

Beweis. Die Darstellung des Stabilisators folgt sofort aus der von ∞ . Als Nächstes ist es einfach einzusehen, dass ausser der trivialen Gruppe und $\langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$ alle Untergruppen von der Form am Ende des Satzes sind. Zur Existenz der Weite müssen wir also nur beweisen, dass der Stabilisator nicht endlich ist. Wäre er aber endlich, so hätten wir die unendliche disjunkte Vereinigung

$$\bigcup_{n \in \mathbb{Z}} \Gamma \sigma T^n \sigma^{-1},$$

die vollständig in $\mathrm{SL}_2(\mathbb{Z})$ enthalten wäre. Dies widerspricht dann der Voraussetzung, dass Γ in $\mathrm{SL}_2(\mathbb{Z})$ endlichen Index hat. □

Bemerkung 2.5.15 Irreguläre Spitzen sind die absolute Ausnahme. Für $\Gamma_0(N)$ gibt es für kein N irreguläre Spitzen, denn $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in \Gamma_0(N)$. Für $\Gamma_1(N)$ gibt es keine irregulären Spitzen für $N \geq 5$.

Die Spitze $\frac{1}{2}$ ist irregulär für die Gruppe $\Gamma_1(4)$. Denn $\frac{1}{2} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \infty$ und

$$\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 3 & -1 \\ -2 & 1 \end{pmatrix} = \begin{pmatrix} 1-2h & h \\ -4h & 1+2h \end{pmatrix}.$$

Wir sehen, dass für $h = \pm 1$ diese Matrix nicht in $\Gamma_1(4)$ liegt, erst für $h = \pm 2$ tut sie dies. Aber für $h = 1$ liegt das Negative der Matrix in $\Gamma_1(4)$. Somit ist der Stabilisator der Spitze $\frac{1}{2}$ gleich $\begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix} \langle - \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}^{-1}$. Die Spitze $\frac{1}{2}$ ist also irregulär.

Aufgabe 2.5.16 Sei p eine Primzahl. Zeige, dass die Menge der Spitzenklassen von $\Gamma_0(p)$ aus zwei Elementen besteht, die durch ∞ und 0 repräsentiert werden können. Berechne die Weite beider Spitzenklassen.

2.5.3 Definition

Wir können nun bereits zur Definition von Modulformen zu Untergruppen von endlichem Index kommen. Zuerst führen wir aber eine praktische Notation ein.

Definition 2.5.17 Seien $k \in \mathbb{Z}$, $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$ und $f : \mathbb{H} \rightarrow \mathbb{C}$ eine holomorphe Funktion. Wir definieren die Funktion

$$(f|_k(\gamma)) : \mathbb{H} \rightarrow \mathbb{C}, \quad (f|_k(\gamma))(\tau) := \det(\gamma)^{k-1} (c\tau + d)^{-k} f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau\right).$$

Der Operator

$$f \mapsto (f|_k(\gamma))$$

heißt Petersson'scher Strichoperator.

Lemma 2.5.18 (a) Sei f wie in der Definition. Dann ist $(f|_k(\gamma))$ auch eine holomorphe Funktion $\mathbb{H} \rightarrow \mathbb{C}$.

(b) Es seien $\gamma, \sigma \in \mathrm{SL}_2(\mathbb{R})$. Dann gilt

$$(f|_k(\gamma))|_k(\sigma) = f|_k(\gamma\sigma).$$

(c) Es gilt $(f|_k\left(\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}\right))(\tau) = f(\tau + n)$.

(d) Ist f eine schwache Modulform von Gewicht k zu einer Untergruppe $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ endlichen Indexes, dann gilt

$$(f|_k(\gamma)) = f$$

für alle $\gamma \in \Gamma$.

Beweis. Es ist klar, dass $(c\tau + d)$ für kein $\tau \in \mathbb{H}$ eine Nullstelle hat. Das zeigt schon (a). (b) rechnet man nach. (c) ist klar. Der Teil (d) ist nur eine Umschreibung der Transformationsregel. \square

Satz 2.5.19 Sei $f : \mathbb{H} \rightarrow \mathbb{C}$ eine schwache Modulform von Gewicht k zu einer Untergruppe $\Gamma < \mathrm{SL}_2(\mathbb{Z})$ endlichen Indexes. Sei ferner $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Die Spitze $\frac{a}{c}$ habe die Weite \tilde{h} . Ist $\frac{a}{c}$ regulär, setze $h := \tilde{h}$, sonst setze $h := 2\tilde{h}$.

Dann hat die Funktion $f|_k(\sigma)$ eine Fourier-Entwicklung der Form

$$(f|_k(\sigma))(\tau) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i \tau n/h} = \sum_{n=-\infty}^{\infty} a_n q^{\frac{n}{h}}.$$

Beweis. Es genügt zu zeigen, dass $f|_k(\sigma)$ periodisch mit der Periode h ist, denn dann können wir den Satz aus der Einleitung anwenden. Dies berechnen wir nun unter Zuhilfenahme aller Teile des vorangehenden Lemmas:

$$(f|_k(\sigma))(\tau + h) = (f|_k(\sigma))|_k\left(\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}\right)(\tau) = (f|_k((\sigma\left(\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}\sigma^{-1})\sigma))(\tau) = (f|_k(\sigma))(\tau).$$

Damit ist der Satz gezeigt. \square

Definition 2.5.20 Seien f und σ wie im obigen Satz.

Wir sagen, dass f in der Spitze $\frac{a}{c}$ meromorph ist, falls es $m \in \mathbb{Z}$ gibt mit

$$(f|_k(\sigma))(\tau) = \sum_{n=m}^{\infty} a_n q^{\frac{n}{h}}.$$

Ferner ist f in der Spitze $\frac{a}{c}$ holomorph, falls gilt:

$$(f|_k(\sigma))(\tau) = \sum_{n=0}^{\infty} a_n q^{\frac{n}{h}}.$$

Schließlich sagt man, dass f in der Spitze $\frac{a}{c}$ verschwindet, falls gilt:

$$(f|_k(\sigma))(\tau) = \sum_{n=1}^{\infty} a_n q^{\frac{n}{h}}.$$

Definition 2.5.21 Sei $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ eine Untergruppe endlichen Indexes.

Eine schwache Modulform f vom Gewicht k zu Γ heißt Modulfunktion vom Gewicht k zu Γ , falls sie in allen Spitzen meromorph ist.

Sie heißt Modulform vom Gewicht k zu Γ , falls sie in allen Spitzen holomorph ist.

Sie heißt Spitzenform vom Gewicht k zu Γ , falls sie in allen Spitzen verschwindet.

Aufgabe 2.5.22 Zeige, dass es genügt, die Bedingungen in den Spitzen an einem Vertretersystem der Spitzenklassen für Γ zu überprüfen.

Aufgrund der Aufgabe finden wir also insbesondere, dass die beiden Definitionen von Modulformen zu $\mathrm{SL}_2(\mathbb{Z})$, die wir gegeben haben, übereinstimmen.

[9.5.2007]

Bemerkung 2.5.23 Es ist klar, dass $q \rightarrow 0$ gehen zu lassen, dasselbe ist, wie einen Limes über τ zu bilden, bei dem der Imaginärteil von τ gegen unendlich geht (und der Realteil von τ beschränkt bleibt, z. B. ohne Einschränkung zwischen 0 und 1). Für Letzteres schreiben wir $\lim_{\mathrm{Im}(\tau) \rightarrow \infty}$.

Man berechnet, dass

$$\lim_{\mathrm{Im}(\tau) \rightarrow \infty} \frac{a\tau + b}{c\tau + d} = \frac{a}{c}$$

gilt. Denn der Ausdruck $\mathrm{Re}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{|\tau|^2 ac + bc + \mathrm{Re}(\tau)}{|c\tau+d|^2}$ geht gegen $\frac{a}{c}$ und $\mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}$ geht gegen 0. Daher stellen wir uns ∞ auch als $i\infty$, das heißt "ganz oben" vor.

Bemerkung 2.5.24 Wir erinnern an die aus der Funktionentheorie bekannte Gamma-Funktion. Diese ist definiert auf der rechten Halbebene $\mathrm{Re}(z) > 0$ durch

$$\Gamma(z) := \int_0^{\infty} t^{z-1} e^{-t} dt$$

und stellt dort eine holomorphe Funktion dar (siehe [FB], Satz IV.1.1).

Satz 2.5.25 Sei $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ mit $\Gamma(N) \leq \Gamma$ und sei f eine schwache Modulform vom Gewicht k zu Γ , die in ∞ holomorph ist. Dann hat f eine Fourier-Entwicklung in ∞ von der Form

$$f(\tau) = \sum_{n=0}^{\infty} a_n e^{2\pi i \tau n / N}.$$

Gibt es eine Konstante $C > 0$, so dass für alle $n \in \mathbb{N}$

$$|a_n| \leq C n^r$$

gilt, dann ist f eine Modulform von Gewicht k zu Γ .

Beweis. Dass f eine Fourier-Entwicklung wie die behauptete besitzt, folgt unmittelbar daraus, dass die Weite einer jeden Spitze N teilt, da die Matrix $\begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix}$ offenbar in $\Gamma(N)$ enthalten und $\Gamma(N)$ ein Normalteiler von $\mathrm{SL}_2(\mathbb{Z})$ ist. Denn dann enthält der Stabilisator $\Gamma_{\sigma\infty}$ der Spitze $\sigma\infty$ die Untergruppe $\sigma \langle \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \rangle \sigma^{-1}$.

Behauptung: Es ist $|f(\tau)| \leq C_0 + C_1 \frac{1}{\mathrm{Im}(\tau)^r}$ für gewisse Konstanten $C_0, C_1 > 0$.

Um dies zu sehen, rechnen wir zunächst (schreibe $y = \mathrm{Im}(\tau)$):

$$\begin{aligned} |f(\tau)| &= \left| \sum_{n=0}^{\infty} a_n q^{n/N} \right| \leq \sum_{n=0}^{\infty} |a_n| e^{-2\pi y n / N} \\ &\leq |a_0| + C \sum_{n=0}^{\infty} n^r e^{-2\pi y n / N} \\ &= |a_0| + C \left(\frac{N}{2\pi} \right)^r \frac{1}{y^r} \sum_{n=0}^{\infty} \left(\frac{2\pi n y}{N} \right)^r e^{-\frac{2\pi n y}{N}}. \end{aligned}$$

Die Summe rechts kann einfach mit $\Gamma(r+1)$ verglichen werden (Substitution $t = \frac{2\pi n y}{N}$) und gegen eine von y unabhängige Konstante abgeschätzt werden. Das wird hier nicht ausgeführt. Damit erhält man die Behauptung.

Wir müssen nun zeigen, dass f holomorph in den Spitzen ist. Sei dazu für $\sigma \in \mathrm{SL}_2(\mathbb{Z})$

$$(f|_k(\sigma))(\tau) = \sum_{n=-\infty}^{\infty} b_n q^{n/N}.$$

Es genügt nun weiter, wie wir wissen, zu zeigen, dass $\lim_{\mathrm{Im}(\tau) \rightarrow \infty} q^{1/N} (f|_k(\sigma))(\tau)$ gleich 0 ist. Dies wollen wir mittels der Abschätzung aus der Behauptung nun beweisen. Wir erinnern an die Formel $\mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}$ für $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$. Außerdem verhält sich $|c\tau+d|$ für große $\mathrm{Im}(\tau)$ und $|\mathrm{Re}(\tau)| \leq N$ wie $|c|\mathrm{Im}(\tau)$. Wir berechnen

$$\begin{aligned} |(f|_k(\sigma))(\tau)| &= \frac{1}{|c\tau+d|^k} \left| f\left(\frac{a\tau+b}{c\tau+d}\right) \right| \leq \frac{1}{|c\tau+d|^k} |C_0 + C_1 \mathrm{Im}\left(\frac{a\tau+b}{c\tau+d}\right)^{-r}| \\ &= \frac{1}{|c\tau+d|^k} |C_0 + C_1 \frac{|c\tau+d|^{2r}}{\mathrm{Im}(\tau)^r}|. \end{aligned}$$

Für große $\text{Im}(\tau)$ verhält sich der Ausdruck rechts kleiner gleich $C_2 \text{Im}(\tau)^{r-k}$ für eine Konstante $C_2 > 0$. Damit folgt

$$\lim_{\text{Im}(\tau) \rightarrow \infty} |q^{1/N} (f|_k(\sigma))(\tau)| \leq \lim_{\text{Im}(\tau) \rightarrow \infty} |e^{-2\pi \text{Im}(\tau)} \text{Im}(\tau)^{r-k}| = 0,$$

was den Beweis abschließt. \square

Bemerkung 2.5.26 Seien $\Gamma \leq \tilde{\Gamma} \leq \text{SL}_2(\mathbb{Z})$ Untergruppen endlichen Indexes. Dann ist jede Modulform von Gewicht k zu $\tilde{\Gamma}$ auch eine Modulform von Gewicht k zu Γ . Gleiches gilt für Modulfunktionen und Spitzenformen.

Diese Bemerkung folgt unmittelbar aus der Definition.

Wir gehen jetzt noch auf Modulformen zu $\Gamma_1(N)$ mit Charakter ein, da diese in der Praxis sehr häufig vorkommen. Wir werden sie allerdings erst einmal nicht gesondert betrachten. Hier kommt es nur darauf an, dass die Definition schon einmal gesehen wurde.

Definition 2.5.27 Sei f eine Modulform von Gewicht k zu $\Gamma_1(N)$ und sei $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$ ein Dirichlet-Charakter, d. h. ein Gruppenhomomorphismus.

Wir sagen, dass f den Charakter χ bzw. den Nebentyp χ oder auch altertümlich den Nebentypus χ hat, falls für alle Matrizen $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ gilt:

$$f\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau\right) = \chi(d)(c\tau + d)^k f(\tau).$$

Bemerkung 2.5.28 Ist der Charakter χ trivial, d. h. $\chi(n) = 1$ für alle $n \in (\mathbb{Z}/N\mathbb{Z})^\times$, dann hat eine Modulform zu $\Gamma_1(N)$ genau dann den Charakter χ , wenn sie bereits eine Modulform zu $\Gamma_0(N)$ ist.

Notation 2.5.29 Den \mathbb{C} -Vektorraum der Modulformen von Gewicht k zur Gruppe $\Gamma \leq \text{SL}_2(\mathbb{Z})$ bezeichnen wir mit $M_k(\Gamma)$. Den Untervektorraum der Spitzenformen nennen wir $S_k(\Gamma)$.

Ist wie oben χ ein Dirichlet-Charakter $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$, dann bezeichnen $M_k(N, \chi)$ und $S_k(N, \chi)$ die Modulformen bzw. Spitzenformen vom Gewicht k für $\Gamma_1(N)$ mit Charakter χ .

2.5.4 Ausartungs-Abbildungen und Altformen

Seien $N, M \in \mathbb{N}$. Ist $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(NM)$, dann ist die Matrix $\begin{pmatrix} a & bm \\ c/m & d \end{pmatrix} \in \Gamma_0(N)$ für alle Teiler $m \mid M$, denn die Determinante ist offenbar unverändert und alle Einträge sind ganze Zahlen.

Satz 2.5.30 Sei f eine Modulform von Gewicht k und Stufe N . Dann ist für alle Teiler $m \mid M$ die Funktion

$$g(\tau) := f(m\tau)$$

eine Modulform von Gewicht k und Stufe NM . Das gleiche gilt auch für Spitzenformen.

Beweis. Dass g holomorph auf ganz \mathbb{H} ist, ist klar. Wir berechnen nun die Transformationseigenschaft für $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(NM)$:

$$g\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau\right) = f\left(m \frac{a\tau + b}{c\tau + d}\right) = f\left(\frac{a(m\tau) + bm}{\frac{c}{m}(m\tau) + d}\right) = \left(\frac{c}{m}(m\tau) + d\right)^k f(m\tau) = (c\tau + d)^k g(\tau).$$

Nun müssen wir uns noch um die Holomorphie in den Spitzen kümmern. Dazu sei nun $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Sei ferner $e = \mathrm{ggT}(c, ma)$, den wir als Linearkombination nach dem Euklidischen Algorithmus darstellen:

$$e = sc + rma$$

für geeignete $r, s \in \mathbb{Z}$. Damit ist die Matrix $\alpha := \begin{pmatrix} -r & -s \\ \frac{c}{e} & -\frac{ma}{e} \end{pmatrix}$ in $\mathrm{SL}_2(\mathbb{Z})$ und es gilt

$$\alpha \begin{pmatrix} ma & mb \\ c & d \end{pmatrix} = \begin{pmatrix} -r & -s \\ \frac{c}{e} & -\frac{ma}{e} \end{pmatrix} \begin{pmatrix} ma & mb \\ c & d \end{pmatrix} = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix}$$

mit $x, y, z \in \mathbb{Z}$ (deren genaue Darstellung uns egal ist). Mit $g = f|_k\left(\begin{pmatrix} m & 0 \\ 0 & 1 \end{pmatrix}\right)$ folgt

$$(g|_k(\sigma))(\tau) = (f|_k\left(\begin{pmatrix} ma & mb \\ c & d \end{pmatrix}\right))(\tau) = (f|_k(\alpha^{-1}\left(\begin{pmatrix} x & y \\ 0 & z \end{pmatrix}\right)))(\tau) = \frac{1}{z^k} (f|_k(\alpha^{-1})\left(\frac{x\tau + y}{z}\right)).$$

Wir wissen, da f eine Modulform ist, dass $(f|_k(\alpha^{-1}))(\tau)$ einen Grenzwert für $\mathrm{Im}(\tau) \rightarrow \infty$ annimmt, nennen wir ihn G . Dann ist

$$\lim_{\Im(\tau) \rightarrow \infty} \frac{1}{z^k} (f|_k(\alpha^{-1})\left(\frac{x\tau + y}{z}\right)) = \frac{G}{z^k},$$

und die Holomorphizität in der Spitze $\frac{a}{c}$ ist bewiesen. Ist f eine Spitzenform, so ist $G = 0$ und folglich verschwindet auch g in den Spitzen. \square

Definition 2.5.31 Eine Modulform von Gewicht k zu $\Gamma_0(N)$ heißt Altform, wenn sie eine Linearkombination von Modulformen $g_i(d_i\tau)$ ist, wobei $M_i > 1$ echte Teiler von N , die $d_i \geq 1$ Teiler von M_i und die g_i Modulformen von Gewicht k zu $\Gamma_0(N/M_i)$ sind.

Bemerkung 2.5.32 Gibt es Altformen, so erwartet man, dass es auch Neuformen gibt. Diese werden wir später als das orthogonale Komplement zu den Altformen bzgl. eines noch zu definierenden Skalarproduktes definieren. Wie man sich leicht vorstellen kann, spielen die Neuformen die gewichtigere Rolle.

2.5.5 Die Eisenstein-Reihe G_2

In diesem Abschnitt wollen wir die Aussagen der Einleitung bezüglich der Eisenstein-Reihe G_2 beweisen. Dazu erinnern wir an die Definition und an das, was wir bereits gezeigt haben:

$$P(\tau) = \frac{\pi^2}{3} + 2 \sum_{c=1}^{\infty} \left(\sum_{d=-\infty}^{\infty} \frac{1}{(c\tau + d)^2} \right) = -8\pi^2 \left(-\frac{1}{24} + \sum_{n=1}^{\infty} \sigma_1(n)q^n \right).$$

Die links auftretende Reihe ist nicht absolut konvergent und die oben bewiesene Gleichheit gilt nur für diese Summationsreihenfolge.

Satz 2.5.33 Sei $N \geq 2$ eine natürliche Zahl. Dann ist

$$G_{2,N}(\tau) := P(\tau) - NP(N\tau)$$

eine Modulform von Gewicht 2 zu $\Gamma_0(N)$.

Um diesen Satz zu beweisen, benötigen wir einige Vorbereitungen.

Satz 2.5.34 Es gilt $\frac{1}{\tau^2}P\left(\frac{-1}{\tau}\right) = P(\tau) - \frac{2\pi i}{\tau}$.

Aufgabe 2.5.35 Beweise den Satz 2.5.34. Eine Anleitung findet sich in [DS] und der ganze Beweis in [FB], S. 390-393.

Bemerkung 2.5.36 Wir benötigen leider einen winzigen Vorgriff auf eine der nächsten Stunden, nämlich, dass $\mathrm{SL}_2(\mathbb{Z})$ erzeugt wird von den Matrizen $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Lemma 2.5.37 (a) Für alle $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ gilt

$$(P|_2(\sigma))(\tau) = P(\tau) - \frac{2\pi ic}{c\tau + d}.$$

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

$$\left(\frac{1}{\mathrm{Im}(\tau)}|_2(\sigma)\right)(\tau) = \frac{1}{(c\tau + d)^2 \mathrm{Im}(\sigma\tau)} = \frac{1}{\mathrm{Im}(\tau)} - \frac{2ic}{c\tau + d}.$$

(c) Die Funktion $f(\tau) := P(\tau) - \frac{\pi}{\mathrm{Im}(\tau)}$ erfüllt $(f|_2(\sigma))(\tau) = f(\tau)$.

Beweis. (a) Zunächst stellen wir fest, dass die geforderte Identität für $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ direkt aus der Existenz der Fourier-Entwicklung folgt, da der Bruch rechts verschwindet, und für $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ der Inhalt von Satz 2.5.34 ist. Aufgrund dessen, dass $\mathrm{SL}_2(\mathbb{Z})$ von diesen beiden Matrizen erzeugt wird, genügt es zu überprüfen, dass aus der geforderten Identität für zwei Matrizen α und β auch die Identität für $\alpha\beta$ und α^{-1} folgt. Das ist eine einfache, etwas langwierige Rechnung, die wir uns hier ersparen.

(b) Auch dies rechnet man nach.

(c) Dies folgt unmittelbar:

$$\left(\left(P(\tau) - \frac{p}{\mathrm{Im}(\tau)}\right)|_2(\sigma)\right)(\tau) = P(\tau) - \frac{2\pi ic}{c\tau + d} - \left(\frac{\pi}{\mathrm{Im}(\tau)}|_2(\sigma)\right)(\tau) = P(\tau) - \frac{p}{\mathrm{Im}(\tau)}.$$

□

Beweis von Satz 2.5.33. Da P auf \mathbb{H} holomorph ist, ist $G_{2,N}(\tau)$ es auch. Nun bemerken wir

$$P(\tau) - NP(N\tau) = \left(P(\tau) - \frac{\pi}{\mathrm{Im}(\tau)}\right) - N\left(P(N\tau) - \frac{\pi}{\mathrm{Im}(N\tau)}\right).$$

Da nach Teil (c) die Funktion $f(\tau)$ die Transformationseigenschaft einer schwachen Modulform von Gewicht 2 zu ganz $\mathrm{SL}_2(\mathbb{Z})$ besitzt, folgt genauso wie im Satz zu den Altformen, dass $f(N\tau)$, und folglich auch $G_{2,N}(\tau)$, die Transformationseigenschaft einer Modulform von Gewicht 2 zu $\Gamma_0(N)$ erfüllt.

Die Holomorphizität in den Spitzen ist eine Konsequenz von Satz 2.5.25. Denn die Koeffizienten der Fourier-Entwicklung von P erfüllen die geforderte Schranke offensichtlich. □

Die Dedekindsche η -Funktion

[10.5.2007]

Definition 2.5.38 Die Dedekindsche η -Funktion ist definiert als das unendliche Produkt

$$\eta(\tau) := e^{2\pi i\tau/24} \prod_{n=1}^{\infty} (1 - q^n),$$

wobei wie immer $q = e^{2\pi i\tau}$ ist.**Aufgabe 2.5.39** Das in der Definition auftretende Produkt ist konvergent und definiert eine holomorphe Funktion $\eta : \mathbb{H} \rightarrow \mathbb{C}$.Dazu nehme man den Logarithmus des Produktes, also $\frac{\pi i\tau}{12} + \sum_{n=1}^{\infty} \log(1 - q^n)$, und zeige, dass diese Reihe lokal gleichmäßig absolut konvergiert. Dazu kann man die Taylor-Reihe von $\log(1 - q^n)$ zu Hilfe ziehen.**Lemma 2.5.40** Es gilt die Transformationsformel $\eta\left(\frac{-1}{\tau}\right) = \sqrt{-i\tau} \eta(\tau)$.**Beweis.** Vergleiche [DS], S. 20. Die Konvergenz des Produktes bedeutet die lokal gleichmäßig absolute Konvergenz der Reihe $\sum_{n=1}^{\infty} \log(1 - q^n)$. Es stellt sich heraus, dass es einfacher ist, mit dieser Reihe zu arbeiten als mit dem Produkt. Ferner dürfen wir wegen der Konvergenz, Differentiation und Summation vertauschen und erhalten

$$\begin{aligned} \frac{d}{d\tau} \log(\eta(\tau)) &= \frac{d}{d\tau} \left(\frac{\pi i\tau}{12} + \sum_{c=1}^{\infty} \log(1 - q^c) \right) = \frac{\pi i}{12} - 2\pi i \sum_{c=1}^{\infty} \frac{cq^c}{1 - q^c} \\ &= \frac{\pi i}{12} - 2\pi i \sum_{c=1}^{\infty} c \sum_{d=1}^{\infty} q^{cd} = \frac{\pi i}{12} - 2\pi i \sum_{c=1}^{\infty} \sum_{d=1}^{\infty} cq^{cd} \\ &= \frac{\pi i}{12} - 2\pi i \sum_{c=1}^{\infty} \sigma_1(c) q^c = -2\pi i \left(\frac{1}{24} - \sum_{c=1}^{\infty} \sigma_1(c) q^c \right) = \frac{i}{4\pi} P(\tau). \end{aligned}$$

Nun verwenden wir die Kettenregel:

$$\frac{d}{d\tau} \log\left(\eta\left(\frac{-1}{\tau}\right)\right) = \frac{1}{\tau^2} \left(\frac{d}{d\tilde{\tau}} \log(\eta(\tilde{\tau})) \right) \Big|_{\tilde{\tau} = \frac{-1}{\tau}} = \frac{i}{4\pi} \frac{1}{\tau^2} P\left(\frac{-1}{\tau}\right).$$

Außerdem haben wir

$$\begin{aligned} \frac{d}{d\tau} \log(\sqrt{-i\tau} \eta(\tau)) &= \frac{d}{d\tau} \log(\sqrt{-i\tau}) + \frac{d}{d\tau} \log(\eta(\tau)) = \frac{1}{2\tau} + \frac{i}{4\pi} P(\tau) \\ &= \frac{i}{4\pi} \left(P(\tau) - \frac{2\pi i}{\tau} \right). \end{aligned}$$

Wegen Satz 2.5.34 stimmen also $\frac{d}{d\tau} \log(\sqrt{-i\tau} \eta(\tau))$ und $\frac{d}{d\tau} \log\left(\eta\left(\frac{-1}{\tau}\right)\right)$ überein, woraus

$$\log(\sqrt{-i\tau} \eta(\tau)) = c \cdot \log\left(\eta\left(\frac{-1}{\tau}\right)\right)$$

mit einer Konstante c folgt. Setzen wir nun $\tau = i$, so erhalten wir

$$\log(\sqrt{-ii}\eta(i)) = \log(\eta(i)) = c \cdot \log(\eta(\frac{-1}{i})) = c \cdot \log(\eta(i)),$$

weshalb $c = 1$ folgt. Man muss und kann sich dazu überlegen, dass $P(i) \neq 0$ ist, was man zum Beispiel durch Einsetzen von $\tau = i$ in die Fourier-Entwicklung erhält. \square

Satz 2.5.41 Die Funktion $\eta^{24} = q \prod_{n=1}^{\infty} (1 - q^{2n})^{24}$ ist eine Modulform von Gewicht 12 zu $\mathrm{SL}_2(\mathbb{Z})$.

Beweis. Die Funktion η^{24} erfüllt sicherlich die Transformationsregel für Modulformen von Gewicht k für $(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix})$ (wegen der Produkt-Entwicklung) und $(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix})$ (wegen des vorangehenden Lemmas). Wenn wir wie oben vorgehen, dass $\mathrm{SL}_2(\mathbb{Z})$ von diesen beiden Matrizen erzeugt wird, sind wir fertig, da η^{24} auf \mathbb{H} und wegen der Produkt-Entwicklung auch in den Spitzen holomorph ist. \square

Bemerkung 2.5.42 Wir werden später sehen, dass der Raum der Modulformen von Gewicht 12 zu $\mathrm{SL}_2(\mathbb{Z})$ 1-dimensional ist. Daher ist η^{24} gleich Δ mal einer Konstante. Somit haben wir also eine Produktentwicklung von Δ gefunden!

2.6 Theta-Reihen

Wir betrachten hier zunächst eine etwas andere Θ -Reihe als in der Einleitung, nämlich

$$\tilde{\theta}(\tau) := \sum_{n \in \mathbb{Z}} e^{\pi i n^2 \tau}.$$

In der Einleitung hatten wir

$$\theta(\tau) := \sum_{n \in \mathbb{Z}} e^{2\pi i n^2 \tau}$$

benutzt. Somit gilt:

$$\theta(\tau) = \tilde{\theta}(2\tau).$$

Wir wenden uns erst der “neuen” Θ -Reihe zu und beweisen die Jacobische Θ -Transformationsformel.

Satz 2.6.1 (Jacobi) Für $\tau \in \mathbb{H}$ und $w \in \mathbb{C}$ gilt

$$\sqrt{\frac{\tau}{i}} \sum_{n=-\infty}^{\infty} e^{\pi i (n+w)^2 \tau} = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 \frac{-1}{\tau} + 2\pi i n w},$$

wobei die Quadratwurzel mittels des Hauptzweiges des Logarithmus definiert ist.

Beweis. [FB], S.343-345 \square

Korollar 2.6.2 In einer Aufgabe im letzten Abschnitt haben wir die Θ -Gruppe $\Gamma_\theta := \langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$ eingeführt und $\Gamma(2) = \langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$ gezeigt. Setze $G := \langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$. Aus dieser Aufgabe folgt, dass

$$\chi : \Gamma_\theta/G \rightarrow \langle i \rangle, \quad \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \mapsto -i$$

ein Charakter (Gruppenhomomorphismus) ist.

Die Funktion $\tilde{\theta}^2$ ist holomorph auf \mathbb{H} und erfüllt die Transformationseigenschaft

$$\tilde{\theta}^2(\gamma.\tau) = (c\tau + d)\chi(\gamma)\tilde{\theta}^2(\tau)$$

für alle $\gamma := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_\theta$.

Beweis. Die Holomorphie auf \mathbb{H} haben wir für θ bereits in der Einleitung gezeigt. Aus ihr folgt sofort die Holomorphie von $\tilde{\theta}^2$. Die Transformationseigenschaft braucht nur auf Erzeugern geprüft zu werden. Für $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ ist diese anhand der Definition offensichtlich, für $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ist sie gerade der Inhalt der Jacobischen Θ -Transformationsformel für $w = 0$. \square

Nun wenden wir uns θ zu und beweisen die in der Einleitung benutzten Aussagen.

Lemma 2.6.3 Die Abbildung

$$\Gamma_0(4) \rightarrow \Gamma(2), \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & 2b \\ c/2 & d \end{pmatrix}$$

ist eine Bijektion.

Beweis. Die Wohldefiniertheit ist klar. Die Umkehrabbildung ist offenbar gegeben durch $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b/2 \\ 2c & d \end{pmatrix}$. \square

Satz 2.6.4 Für gerade $k \geq 2$ ist θ^k eine Modulform vom Gewicht $k/2$ für $\Gamma_1(4)$ zum Charakter $\psi : (\mathbb{Z}/4\mathbb{Z})^\times \xrightarrow{\sim} \{\pm 1\}$.

Insbesondere ist θ^k eine Modulform von Gewicht $k/2$ für $\Gamma_0(4)$, falls $4 \mid k$.

Beweis. Die Transformationseigenschaft können wir nun einfach aus dem Lemma und dem Satz oben ablesen:

$$\theta^k\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\tau\right) = \tilde{\theta}^k\left(2\begin{pmatrix} a & b \\ c & d \end{pmatrix}.\tau\right) = \tilde{\theta}^k\left(\frac{a2\tau + 2b}{c2\tau + d}\right) = (c\tau + d)^{k/2}\chi(\gamma)^{k/2}\theta^k(\tau)$$

mit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4)$. Dabei benutzen wir $\Gamma(2) < \Gamma_\theta$ und, dass χ eingeschränkt auf $\Gamma(2)$ der Charakter nach $\{\pm 1\}$ ist, der $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ auf $\psi(d)$ schickt und somit auf $\langle \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rangle$ trivial ist.

Die Holomorphizität in den Spitzen folgt wiederum aus dem Kriterium in Satz 2.5.25. \square

Bis auf die Dimensionsformeln haben wir nun das Theorem aus der Einleitung zur Darstellungszahl bewiesen. Den Dimensionsformeln wenden wir uns im Folgenden zu.

Kapitel 3

Modulkurven

3.1 Der Fundamentalbereich für $SL_2(\mathbb{Z})$ und Anwendungen

Wir erinnern daran, dass der Bahnenraum für die Operation von $SL_2(\mathbb{Z})$ auf \mathbb{H} mit der Menge der komplexen elliptischen Kurven bis auf Isomorphie identifiziert werden kann (vgl. Satz 2.4.13):

$$SL_2(\mathbb{Z}) \backslash \mathbb{H} \longrightarrow \{\text{Komplexe elliptische Kurven}\} / \cong, \quad \tau \mapsto \mathbb{C} / \Lambda_\tau.$$

In diesem Kapitel wollen wir $SL_2(\mathbb{Z}) \backslash \mathbb{H}$ und allgemeiner Bahnräume $\Gamma \backslash \mathbb{H}$ für Kongruenzuntergruppen Γ näher untersuchen. Dabei gehen wir in zwei Schritten vor:

1. Wir wollen $\Gamma \backslash \mathbb{H}$ als Menge verstehen, genauer als eine Teilmenge von \mathbb{H} . Dazu führen wir den Begriff des Fundamentalbereiches ein.
2. Wir machen aus $\Gamma \backslash \mathbb{H}$ ein geometrisches Objekt: einen topologischen Raum und sogar eine Riemannsche-Fläche, eine sogenannte Modulkurve.

3.1.1 Der Standard-Fundamentalbereich

Bei der Definition des Fundamentalbereiches folgen wir in etwa Kohnen.

Definition 3.1.1 Sei $\Gamma \leq SL_2(\mathbb{Z})$ eine Untergruppe endlichen Indexes. Ein Fundamentalbereich für die Operation von Γ auf \mathbb{H} ist eine Teilmenge $\mathcal{F} \subset \mathbb{H}$, so dass die folgenden Punkte gelten:

- (i) \mathcal{F} ist offen.
- (ii) Für alle $\tau \in \mathbb{H}$ gibt es $\gamma \in \Gamma$, so dass $\gamma \cdot \tau \in \overline{\mathcal{F}}$.
- (iii) Falls $\gamma \cdot \tau \in \mathcal{F}$ für $\tau \in \mathcal{F}$ und $\gamma \in \Gamma$, dann ist $\gamma = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Mit anderen Worten ist ein Fundamentalbereich eine offene Menge, die so klein ist, dass sie keine zwei unter der Operation von Γ äquivalenten Punkte enthält, aber so groß ist, dass jeder Punkt der oberen Halbebene durch eine Matrix aus Γ in einen Punkt des Abschlusses des Fundamentalbereiches überführt werden kann.

Notation 3.1.2 Wir setzen $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ (Translation) und $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (Spiegelung).

Satz 3.1.3 Die Menge

$$\mathcal{F} := \left\{ \tau \in \mathbb{H} \mid |\tau| > 1 \text{ und } -\frac{1}{2} < \operatorname{Re}(\tau) < \frac{1}{2} \right\}$$

[Bild] ist ein Fundamentalbereich für die Operation von $SL_2(\mathbb{Z})$ auf \mathbb{H} .

Beweis. Die Offenheit ist klar. Für (ii) benutzen wir das folgende Lemma.

Lemma 3.1.4 Sei $\tau \in \mathbb{H}$ fest. In der Bahn $SL_2(\mathbb{Z}) \cdot \tau$ gibt es einen Punkt $\gamma \cdot \tau$ mit maximalem Imaginärteil (auch geometrisch betrachtet “Höhe” genannt), d. h.

$$\operatorname{Im}(\gamma \cdot \tau) \geq \operatorname{Im}(g \cdot \tau) \quad \forall g \in SL_2(\mathbb{Z}).$$

Ein Punkt τ ist von maximaler Höhe, falls $|c\tau + d| \geq 1$ ist für alle teilerfremden $c, d \in \mathbb{Z}$.

Beweis. Wir erinnern mal wieder an die Formel

$$\operatorname{Im}(\gamma \cdot \tau) = \frac{\operatorname{Im}(\tau)}{|c\tau + d|^2}.$$

Aus ihr liest man ab

$$\operatorname{Im}(\tau) \leq \operatorname{Im}(\gamma \cdot \tau) \Leftrightarrow |c\tau + d| \leq 1.$$

Mit $\tau = x + iy$ ist aber

$$1 \geq |c\tau + d|^2 = (cx + d)^2 + c^2y^2.$$

Dieser Ausdruck hat aber nur endlich viele Lösungen in ganzen Zahlen c, d (für feste x, y). Aus diesen endlich vielen können wir ein teilerfremdes Paar (c, d) auswählen, für das $|c\tau + d|$ minimal ist. Wie wir schon oft gesehen haben, finden wir mit dem euklidischen Algorithmus eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Diese hat dann die gewünschte Eigenschaft. \square

Wir zeigen nun mit einem einfachen Trick den Punkt (ii). Sei also τ gegeben. Wir wählen nun $\gamma \in SL_2(\mathbb{Z})$ mit $\gamma \cdot \tau$ mit maximalem Imaginärteil. Nun “transportieren” wir $\gamma \cdot \tau$ mittels einer geeigneten Translation T^n so, dass $-1/2 \leq \operatorname{Re}(T^n \gamma \cdot \tau) < 1/2$. Die Höhe bleibt dabei offenbar unverändert. Nun gilt $|T^n \gamma \cdot \tau| \geq 1$, denn sonst hätte $T^n \gamma \cdot \tau$ keine maximale Höhe, da $|1T^n \gamma \cdot \tau + 0| < 1$ gälte (mit anderen Worten, mittels der Spiegelung könnten wir die Höhe noch größer machen). Es gilt genauer:

Lemma 3.1.5 Jeder Punkt maximaler Höhe kann durch Translation in den Abschluss $\overline{\mathcal{F}}$ überführt werden. Umgekehrt enthält $\overline{\mathcal{F}}$ nur Punkte maximaler Höhe.

Beweis. Den ersten Teil haben wir gerade gesehen. Der andere ergibt sich aus der Rechnung

$$|c\tau + d|^2 = (cx + d)^2 + c^2y^2 = c^2|\tau|^2 + 2cdx + d^2 \geq c^2|\tau|^2 - |cd| + d^2 \geq (|c| - |d|)^2 + |cd| \geq 1$$

für alle teilerfremden c, d , wobei wir wieder $\tau = x + iy$ geschrieben haben. \square

Wir halten fest, dass die beiden Senkrechten der Figur unter T ineinander überführt werden. Außerdem hält S den Einheitskreisbogen fest, genauer wird ein Element auf dem Einheitskreis an der imaginären Achse gespiegelt, da der Imaginärteil und der Betrag gleich bleiben.

Sei $\tau \in \mathcal{F}$. Dann hat nach dem vorletzten Lemma τ maximale Höhe. Nun impliziert $|c\tau + d| = 1$, dass $c = 0$ gilt. Denn die Ungleichheiten im Beweis des Lemmas werden Gleichheiten, was wegen $|\tau| > 1$ nur bei $c = 0$ der Fall sein kann. Die einzigen Matrizen mit $c = 0$ sind aber $\pm T^n$. Diese führen aus \mathcal{F} hinaus mit den Ausnahmen $\pm \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Dies beweist den Punkt (iii) und damit den Satz. \square

Satz 3.1.6 Die Gruppe $SL_2(\mathbb{Z})$ wird erzeugt von den Matrizen S und T .

Beweis. Sei $\Gamma = \langle S, T \rangle$ und sei $\tau \in \mathbb{H}$. Da Γ eine Untergruppe von $SL_2(\mathbb{Z})$ ist, gibt es in der Bahn $\Gamma \cdot \tau$ auch Punkte maximaler Höhe. Translatiert man diese so, dass ihr Realteil zwischen $-1/2$ und $1/2$ liegt, so sieht man genauso wie oben, dass ihr Betrag dann größer oder gleich 1 ist, denn sonst würde wiederum die Anwendung von S einen größeren Imaginärteil liefern. Also ist auch \mathcal{F} ein Fundamentalbereich für Γ .

Sei nun ein Punkt $\tau \in \mathcal{F}$ gegeben und eine Matrix $M \in SL_2(\mathbb{Z})$ gegeben. Wir betrachten nun $M \cdot \tau$. Diesen Punkt können wir mittels eines Elementes $\gamma \in \Gamma$ wieder nach \mathcal{F} transportieren. Dann ist also $\gamma M \cdot \tau \in \mathcal{F}$, nach Punkt (iii) der Definition des Fundamentalbereichs folgt dann aber $\gamma M = \pm \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, also $M = \pm \gamma \in \Gamma$. Da $S^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, ist der Satz bewiesen. \square

Bemerkung 3.1.7 Setze $\tau = TS^{-1} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$. Die Gruppe $SL_2(\mathbb{Z}) / \langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$ ist das freie Produkt der zyklischen Gruppe $\langle S \rangle / \langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$ der Ordnung 2 und der zyklischen Gruppe $\langle \tau \rangle / \langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$ der Ordnung 3. In anderer Schreibweise bedeutet dies:

$$SL_2(\mathbb{Z}) / \langle \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \rangle \cong \langle \sigma, \tau \mid \sigma^2 = \tau^3 = 1 \rangle.$$

Einen Beweis geben wir hiervon (voraussichtlich) nicht.

Wir betrachten noch den Rand des Fundamentalbereiches genauer.

Lemma 3.1.8 (a) Sind $\tau \neq \tau' \in \overline{\mathcal{F}}$ mit $\gamma \cdot \tau = \tau'$, dann liegen τ und τ' auf dem Rand von \mathcal{F} und es gilt $|\operatorname{Re}(\tau)| = |\operatorname{Re}(\tau')| = 1/2$ und $\tau' = \tau \pm 1$ oder $|\tau| = 1$ und $\tau = -1/\tau$.

(b) Es gilt für $\tau \in \overline{\mathcal{F}}$:

$$SL_2(\mathbb{Z})_\tau = \begin{cases} \langle \pm ST \rangle, & \text{falls } \tau = \zeta_3, \\ \langle \pm TS \rangle, & \text{falls } \tau = \zeta_6, \\ \langle \pm S \rangle, & \text{falls } \tau = \zeta_4 = i \text{ und} \\ \langle \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \rangle & \text{sonst,} \end{cases}$$

wobei wir ζ_n als $e^{2\pi i/n}$ definieren. Die auftretenden Gruppen sind zyklisch der Ordnungen 6, 6, 4 bzw. 2.

Beweis. Nach der Definition des Fundamentalbereichs können Punkte τ wie in (a) oder solche mit $\gamma \cdot \tau = \tau$ für $\gamma \neq \pm \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ nur auf dem Rand liegen.

Wie wir nach einem der Lemmata oben wissen, enthält $\overline{\mathcal{F}}$ nur Punkte maximaler Höhe. Insbesondere ist daher die Höhe von τ gleich der Höhe von τ' . Wir schließen wie oben. Wir haben wiederum die Gleichheit

$$1 = |c\tau + d|^2 = (cx + d)^2 + c^2y^2 = c^2|\tau|^2 + 2cdx + d^2 \geq (|c| - |d|)^2 + |cd| \geq 1.$$

Da $y \geq \frac{\sqrt{3}}{2}$ ist, folgt $|c| \in \{0, 1\}$. Ist $c = 0$, dann ist $|d| = 1$ und $\gamma = \pm T^n$. Wie wir gesehen haben, ist dies der einzig mögliche Fall, falls $|\tau| > 1$. Nun sei also $|\tau| = 1$ und $|c| = 1$. Aus der Gleichung $1 = |\tau|^2 + 2dx + d^2$ ergibt sich $d = 0$ oder $x = \frac{-d}{2} \in \{\pm \frac{1}{2}\}$. Ist $d = 0$, dann folgt

$$\gamma = \pm T^a S = \pm \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \pm \begin{pmatrix} a & -1 \\ 1 & 0 \end{pmatrix}.$$

Das heißt $\tau' = a - \frac{1}{\tau}$. Wir wissen aber, dass $\frac{-1}{\tau}$ auch auf dem Einheitskreis geschnitten $\overline{\mathcal{F}}$ liegt (denn es wird nur an der imaginären Achse gespiegelt). Ist also $|\operatorname{Re}(\tau)| < 1/2$, dann muss $a = 0$ sein und $\tau' = \frac{-1}{\tau}$. Ist $|d| = 1$ (und immer noch $|c| = 1$), dann ist

$$\gamma = \pm T^a S T = \pm \begin{pmatrix} a & a-1 \\ 1 & 1 \end{pmatrix} \quad \text{oder} \quad \gamma = \pm T^a S T S^{-1} = \pm \begin{pmatrix} 1-a & a \\ -1 & 1 \end{pmatrix}.$$

Im ersten Fall ist $\gamma\zeta_3 = \zeta_3 + a$ und $\gamma\zeta_6$ liegt außerhalb des Fundamentalbereiches. Im zweiten Fall ist es umgekehrt: $\gamma\zeta_6 = \zeta_6 + a - 1$ und $\gamma\zeta_3$ ist außerhalb des Fundamentalbereiches. Damit ist (a) bewiesen.

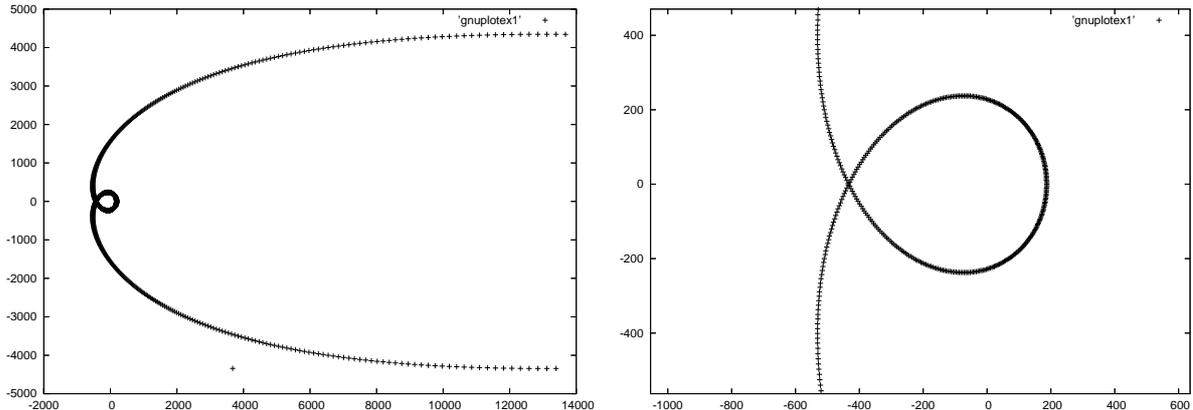
(b) folgt aus (a) mit einigen Rechnungen. Zunächst kann ein Punkt τ mit $\gamma\tau = \tau$ für $\gamma \neq \pm \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ nach (a) nur auf dem Einheitskreis liegen. Hat er $|\operatorname{Re}(\tau)| < 1/2$, dann muss er $\tau = -\frac{1}{\tau}$ erfüllen und ist somit gleich i . Dass der Stabilisator von i wie angegeben ist, ist eine triviale Rechnung. Es bleiben folglich nur noch die Punkte ζ_3 und ζ_6 zu überprüfen, deren Stabilisatoren sich auch trivial errechnen lassen. \square

3.1.2 Kompaktifizierung des Fundamentalbereichs

[24.05.2007] Wir wollen nun den Abschluss des Standardfundamentalbereiches kompaktifizieren (er ist ja "oben offen" und daher unbeschränkt und nicht kompakt). Dies machen wir hier ganz informell und wollen eigentlich nur eine Idee geben. Später wird es im Kontext der Riemannschen Flächen richtig getan. Wir verwenden die surjektive Abbildung q :

$$q : \mathbb{H} \rightarrow \{z \in \mathbb{C} \mid 1 > |z| > 0\}.$$

Beschränken wir uns auf den Streifen $-1/2 \leq \operatorname{Re}(\tau) < 1/2$, dann ist die Abbildung sogar bijektiv. Wie sieht jetzt das Bild des Fundamentalbereiches unter q aus? Die Senkrechte bei $-1/2$ (also "von $-1/2$ bis $i\infty$ ") wird zur geraden Linie von -1 bis 0 (denn $i\infty$ wird zu 0). In den sehr schnell erstellten folgenden Bildern sieht man das Bild des Einheitshalbkreises. Das zweite ist eine Vergrößerung um 0 des ersten. Die Achseneinteilungen sind durch 100000 zu teilen.



Das heißt, dass das Bild von \mathcal{F} (also des Fundamentalbereiches) genau das Innere der Schleife ist, abgesehen vom Punkt 0, der fehlt. Somit ist es ganz natürlich, den Punkt 0 hinzuzufügen. Nehmen wir den Rand der Schleife noch hinzu, so erhält man ein beschränktes und abgeschlossenes Gebiet in \mathbb{C} , das somit kompakt ist. Daher nennt man das Hinzufügen von ∞ (oder $i\infty$, je nach Geschmack) auch “Kompaktifizierung”.

Wir diskutieren noch das Bild ein bisschen. Der Punkt im rechten Bild, der am weitesten rechts liegt, ist das Bild von i , also $e^{-2\pi}$. Der Schnittpunkt der Schleife, der das Bild des Fundamentalbereiches links abschließt, entspricht dem Bild von ζ_3 und ζ_6 , denn es ist der Schnittpunkt der Senkrechten bei $-1/2$ mit dem Einheitskreis. Dieser Punkt sieht nicht differenzierbar aus. Dies ist er auch nicht, denn er entspricht der Ecke von \mathcal{F} bei ζ_3 . Dies ist ein Problem vieler Fundamentalbereiche, das uns auch später noch begegnen wird. Für $\Gamma_1(N)$ mit $N \geq 5$ kommt solch ein Punkt aber nicht mehr vor, wie wir auch sehen werden.

Als Nächstes studieren wir die Topologie auf \mathbb{H} bzw. \mathcal{F} , die von der Standardtopologie auf der Kreisscheibe herkommt. Dies ist ganz einfach: der offene Kreis um 0 vom Radius r entspricht unter q^{-1} der Menge $\{\tau \in \mathbb{H} \mid \text{Im}(\tau) > \frac{-\ln r}{2\pi}\}$. Mit anderen Worten: Die “offenen Kreise um ∞ ” sind gerade die horizontalen, nach oben offenen Streifen.

Es gibt noch eine andere Methode, die Kompaktifizierung zu verstehen, nämlich mittels der uns gut bekannten gebrochen linearen Transformationen. Zum Beispiel transportiert die Matrix S ja auch ∞ nach 0. Der so transformierte Fundamentalbereich $S\mathcal{F}$ sieht so aus: [Bild] Das Hinzufügen von 0 ist also auch eine Kompaktifizierung.

Das Bild unter S des horizontalen Streifens $\{\tau \in \mathbb{H} \mid \text{Im}(\tau) > y\}$, der ja eine Umgebung von ∞ ist, ist ein Horokreis (leider kenne ich die deutsche Übersetzung des Wortes horocycle nicht), d. h. es ist ein Kreis, der die reelle Achse (bei 0) berührt.

Dies rechnen wir nach. Der Kreis hat Radius $\frac{1}{2y}$ und damit den Mittelpunkt $\frac{i}{2y}$, denn

$$\left| -\frac{1}{x+iy} - \frac{i}{2y} \right|^2 = \dots = \frac{1}{4y^2}.$$

[Rechnung]

Aufgabe 3.1.9 Sei $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ eine Matrix mit $c \neq 0$. Dann ist das Bild eines horizontalen Streifens wie oben ein Horokreis, der die reelle Achse am Punkt $\frac{a}{c}$ berührt.

3.1.3 Version des Residuensatzes

Die Essenz dieses Abschnittes ist der Beweis des Residuensatzes für Riemannsche Flächen in dem Spezialfall der Modulkurve für $SL_2(\mathbb{Z})$. Zur Illustration gehen wir hier elementar vor. Im weiteren Verlauf der Vorlesung werden wir dann aber schon Riemannsche Flächen verwenden und Sätze zu ihnen zitieren.

Satz 3.1.10 Für $\tau \in \mathbb{H}$ setze $e_\tau := \frac{1}{2}|SL_2(\mathbb{Z})_\tau| \in \{1, 2, 3\}$. Sei $f : \mathbb{H} \rightarrow \mathbb{C}$ eine meromorphe Funktion, die $SL_2(\mathbb{Z})$ -invariant ist, d. h.

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = f(\tau) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

und die in ∞ meromorph ist. Dann gilt:

$$0 = \text{Ord}(f; \infty) + \sum_{\tau} \frac{\text{Ord}(f; \tau)}{e_\tau},$$

wobei τ ein Repräsentantensystem von \mathbb{H} modulo $SL_2(\mathbb{Z})$ durchläuft (zum Beispiel nehmen wir \mathcal{F} zusammen mit der "Hälfte" des Randes).

Beweis. Siehe [FB], S. 332 für $k = 0$. □

Korollar 3.1.11 ($k/12$ -Formel) Sei $f : \mathbb{H} \rightarrow \mathbb{C}$ eine meromorphe Funktion, die die Transformations-eigenschaft einer Modulform von Gewicht k für $SL_2(\mathbb{Z})$ erfüllt, d. h.

$$f\left(\frac{a\tau + b}{c\tau + d}\right) = (c\tau + d)^k f(\tau) \quad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

und die meromorph in ∞ ist. Dann gilt:

$$\frac{k}{12} = \text{Ord}(f; \infty) + \sum_{\tau} \frac{\text{Ord}(f; \tau)}{e_\tau},$$

wobei τ ein Repräsentantensystem von \mathbb{H} modulo $SL_2(\mathbb{Z})$ durchläuft.

Beweis. Wir folgern das Korollar aus dem Satz, indem wir die Funktion $g(\tau) := \frac{f(\tau)^{12}}{\Delta(\tau)^k}$ benutzen. Diese erfüllt nämlich die Voraussetzungen des Satzes. Folglich gilt

$$\begin{aligned} 0 &= \text{Ord}(g; \infty) + \sum_{\tau} \frac{\text{Ord}(g; \tau)}{e_\tau} \\ &= 12(\text{Ord}(f; \infty) + \sum_{\tau} \frac{\text{Ord}(f; \tau)}{e_\tau}) - k(\text{Ord}(\Delta; \infty) + \sum_{\tau} \frac{\text{Ord}(\Delta; \tau)}{e_\tau}). \end{aligned}$$

Jetzt erinnern wir uns, dass Δ keine Nullstelle in \mathbb{H} hat und sowieso keinen Pol. An der Fourier-Entwicklung von Δ lesen wir ab, dass $\text{Ord}(\Delta; \infty) = 1$. Damit erhalten wir die gewünschte Formel. □

3.1.4 Dimensionsformeln für Modulformen der Stufe 1

[30.5.07] Die $\frac{k}{12}$ -Formel ist unscheinbar, aber sie hat eine ganze Reihe erstaunlicher und wichtiger Konsequenzen, die wir in diesem und dem folgenden Abschnitt beweisen.

Satz 3.1.12 *Sei k gerade. Dann gelten:*

- (a) $M_k(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$ für $k < 0$.
- (b) $M_0(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}$.
- (c) $M_2(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$.
- (d) $M_k(\mathrm{SL}_2(\mathbb{Z})) = \mathbb{C}G_k \oplus S_k(\mathrm{SL}_2(\mathbb{Z}))$ für $k \geq 4$.
- (e) $S_k(\mathrm{SL}_2(\mathbb{Z})) = \{0\}$ für $k < 12$.

Beweis. (a) In der $k/12$ -Formel stehen rechts nur nicht-negative Zahlen. Somit folgte ein Widerspruch.

(b) Da die linke Seite der $k/12$ -Formel 0 ist, hat eine solche Funktion keinen Pol und ist auch in ∞ beschränkt, womit sie nach dem Satz von Liouville eine Konstante ist.

(c) Die Gleichung $\frac{1}{6} = a + \frac{b}{2} + \frac{c}{3}$ hat keine Lösung in positiven natürlichen Zahlen a, b, c .

(d) Wir erinnern uns, dass der 0-te Fourier-Koeffizient der Eisenstein-Reihe G_k ungleich 0 ist. Also können wir aus jeder Modulform, die kein Vielfaches von G_k ist, eine Spitzenform machen, indem wir ein geeignetes Vielfaches von G_k abziehen.

(e) Da $k/12 < 1$, muss $\mathrm{Ord}(f; \infty) = 0$ sein, weshalb f keine Spitzenform ist. \square

Lemma 3.1.13 *Die Abbildung*

$$M_k(\mathrm{SL}_2(\mathbb{Z})) \rightarrow S_{k+12}(\mathrm{SL}_2(\mathbb{Z})), \quad f \mapsto f\Delta$$

ist ein Isomorphismus.

Beweis. Die Abbildung ist offenbar wohldefiniert, linear und injektiv. Sei $f \in S_{k+12}(\mathrm{SL}_2(\mathbb{Z}))$. Wir zeigen, dass $g(\tau) := \frac{f(\tau)}{\Delta(\tau)}$ eine Modulform vom Gewicht k ist. Die Transformationseigenschaft ist natürlich erfüllt. Zu überprüfen ist also nur, dass g holomorph auf \mathbb{H} und in ∞ ist. Ersteres folgt daraus, dass Δ auf \mathbb{H} keine Nullstelle hat (Satz 2.3.8). Letzteres gilt wegen

$$\mathrm{Ord}(g; \infty) = \mathrm{Ord}(f; \infty) - \mathrm{Ord}(\Delta; \infty) = \mathrm{Ord}(f; \infty) - 1,$$

was größer oder gleich 0 ist, da f eine Spitzenform ist. \square

Satz 3.1.14 (Dimensionsformel für $\mathrm{SL}_2(\mathbb{Z})$) *Sei $k \geq 0$ gerade. Dann gilt:*

$$\dim M_k(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{für } k \equiv 2 \pmod{12}, \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{sonst.} \end{cases}$$

Beweis. Für $0 \leq k \leq 10$ folgt dies unmittelbar aus dem Satz oben. Für die größeren k sagt das Lemma, dass bei Erhöhung des Gewichtes um 12 die Dimension um 1 steigt. \square

Wir beweisen nun einen Satz, den wir in der Einleitung angekündigt haben, nämlich, dass die Eisenstein-Reihen eine Basis der Modulformen bilden.

Satz 3.1.15 *Sei $k \geq 0$ gerade. Dann bilden die Modulformen*

$$G_4^a G_6^b$$

für alle $a, b \in \mathbb{N}$ mit $4a + 6b = k$ eine Basis von $M_k(SL_2(\mathbb{Z}))$.

Beweis. Wir zeigen per Dimension über k , dass die Anzahl der (a, b) mit $k = 4a + 6b$ gleich der Dimension von $M_k(SL_2(\mathbb{Z}))$ ist. Als Induktionsanfang überprüft man elementar, dass die Aussage für $0 \leq k \leq 10$ gilt. Wir betrachten nun die injektive Abbildung

$$\{(a, b) | k = 4a + 6b\} \xrightarrow{(a,b) \mapsto (a,b+2)} \{(a', b') | k + 12 = 4a' + 6b'\}.$$

Die rechte Menge hat genau ein Element mehr als die linke. Denn sei (a, b) in der linken Menge mit maximalem a . Dann ist $(a + 3, b)$ in der rechten Menge, aber nicht im Bild der Abbildung. Ist umgekehrt (a', b') in der rechten Menge, ohne dass a' maximal ist, dann ist $b' \geq 2$ und folglich ist $(a', b') = (a', (b' - 2) + 2)$ im Bild der Abbildung.

Wir schließen den Beweis ab, indem wir per Induktion über k beweisen, dass die angegebenen Modulformen ein Erzeugendensystem bilden. Als Induktionsanfang folgt die Aussage für $k \leq 10$ aus der Dimensionsformel. Sei nun $f \in M_k(SL_2(\mathbb{Z}))$ und $4a + 6b = k$. Es gibt $c \in \mathbb{C}$, so dass $f - cG_4^a G_6^b$ eine Spitzenform ist, also gleich Δg für ein $g \in M_{k-12}(SL_2(\mathbb{Z}))$. Nach Induktionsvoraussetzung ist g aber eine Linearkombination aus $G_4^r G_6^s$ mit $k - 12 = 4r + 6s$. Wir erinnern uns, dass Δ selbst Linearkombination aus G_4 und G_6 ist. Somit folgt der Satz. \square

3.1.5 Die j -Invariante

Wir erinnern an die j -Funktion. Sie ist definiert als $j(\tau) := \frac{(60G_4(\tau))^3}{\Delta(\tau)}$ und ist eine Modulfunktion von Gewicht 0 zu $SL_2(\mathbb{Z})$. Sie ist holomorph auf \mathbb{H} und hat einen Pol der Ordnung 2 in ∞ .

Satz 3.1.16 *Die j -Funktion definiert eine Bijektion $SL_2(\mathbb{Z}) \backslash \mathbb{H} \rightarrow \mathbb{C}$. Damit ist jede komplexe elliptische Kurve durch ihre j -Invariante eindeutig bestimmt. (Dies haben wir in einer früheren Bemerkung genauer behandelt.)*

Beweis. Sei $\lambda \in \mathbb{C}$. Wir betrachten $f(\tau) = G_4^3(\tau) - \lambda \Delta(\tau)$. Dies ist eine Modulform von Gewicht 12 zu $SL_2(\mathbb{Z})$, deren Ordnung bei ∞ gleich 0 ist, da Δ eine Spitzenform ist und $G_4(\tau)^3$ nicht. Die $k/12$ -Formel liefert also die Gleichheit

$$1 = \sum_{\tau} \frac{\text{Ord}(f; \tau)}{e_{\tau}},$$

aus der folgt, dass f genau eine Nullstelle hat (eventuell mit Vielfachheit 2 oder 3). Deshalb nimmt $j(\tau) = \frac{G_4^3(\tau)}{\Delta(\tau)}$ den Wert λ genau einmal an. \square

Satz 3.1.17 Sei $f : \mathbb{H} \rightarrow \mathbb{C}$ eine meromorphe Funktion. Dann sind äquivalent:

- (i) f meromorphe Modulfunktion vom Gewicht 0 zu $\mathrm{SL}_2(\mathbb{Z})$ (d. h. wie in Satz 3.1.10).
- (ii) f ist Quotient zweier Modulformen gleichen Gewichts zu $\mathrm{SL}_2(\mathbb{Z})$.
- (iii) f ist eine rationale Funktion in j , d. h. $f = \frac{F(j)}{G(j)}$ für zwei Polynome $F, G \in \mathbb{C}[X]$ mit $G \neq 0$.

Beweis. “(iii) \Rightarrow (ii)”: Seien $F(X) = \sum_{i=0}^m a_i X^i$ und $G(X) = \sum_{j=0}^n b_j X^j$. Dann haben wir

$$\frac{F(j)}{G(j)} = \frac{\Delta(\tau)^n \Delta(\tau)^m \sum_{i=0}^m a_i \left(\frac{60^3 G_4(\tau)^3}{\Delta(\tau)}\right)^i}{\Delta(\tau)^m \Delta(\tau)^n \sum_{j=0}^n b_j \left(\frac{60^3 G_4(\tau)^3}{\Delta(\tau)}\right)^j} = \frac{\Delta(\tau)^n \sum_{i=0}^m a_i 60^{3i} G_4(\tau)^{3i} \Delta(\tau)^{m-i}}{\Delta(\tau)^m \sum_{j=0}^n b_j 60^{3j} G_4(\tau)^{3j} \Delta(\tau)^{n-j}}.$$

Dies ist offenbar ein Quotient von Modulformen vom Gewicht $12(m+n)$.

“(ii) \Rightarrow (i)”: Dies ist klar.

“(i) \Rightarrow (iii)”: Seien z_1, \dots, z_r Repräsentanten der Polstellen von f modulo $\mathrm{SL}_2(\mathbb{Z})$. Diese haben die Ordnungen n_i . Setze

$$P(\tau) = \prod_{i=1}^r (j(z) - j(z_i))^{n_i}.$$

Diese Funktion ist so gemacht, dass sie eine Nullstelle der Ordnung mindestens n_i in z_i hat. Folglich ist $f(\tau)P(\tau)$ holomorph auf \mathbb{H} . Da f ja meromorph in ∞ ist, gibt es ein $m \in \mathbb{N}$, so dass $g(\tau) := f(\tau)P(\tau)\Delta(\tau)^m$ holomorph in ∞ und auf \mathbb{H} ist. Folglich ist $g(\tau)$ eine Modulform vom Gewicht $12m$ für $\mathrm{SL}_2(\mathbb{Z})$. Wir wissen aber bereits, dass sich g dann als Linearkombination von $G_4(\tau)^a G_6(\tau)^b$ (mit $12n = 4a + 6b$) schreiben lässt. Folglich genügt es zu zeigen, dass sich jedes $\frac{G_4(\tau)^a G_6(\tau)^b}{\Delta(\tau)^n}$ (mit $12n = 4a + 6b$) als rationale Funktion in j schreiben lässt.

Die Gleichung $12n = 4a + 6b$ impliziert $2 \mid b$ und $3 \mid a$, also $a = 3c$ und $b = 2d$ für $c, d \in \mathbb{N}$ und $n = c + d$. Für die folgende Rechnung erinnern wir uns an die Definition von Δ als

$$\Delta(\tau) = 60^3 G_4(\tau)^3 - 27 \cdot 140^2 G_6(\tau)^2.$$

Damit haben wir nun

$$\begin{aligned} \frac{G_4(\tau)^a G_6(\tau)^b}{\Delta(\tau)^n} &= \frac{(G_4(\tau)^3)^c (G_6(\tau)^2)^d}{\Delta(\tau)^c \Delta(\tau)^d} = j(\tau)^c \left(\frac{60^3 G_4(\tau)^3 - \Delta(\tau)}{27 \cdot 140^2 \Delta(\tau)} \right)^d \\ &= j(\tau)^c \left(\frac{60^3}{27 \cdot 140^2} j(\tau) - \frac{1}{27 \cdot 140^2} \right)^d, \end{aligned}$$

was den Beweis abschließt. \square

3.2 Fundamentalbereiche und Modulkurven

3.2.1 Fundamentalbereiche für allgemeine Γ

In diesem Abschnitt gehen wir kurz auf Fundamentalbereiche für Untergruppen endlichen Indexes von $\mathrm{SL}_2(\mathbb{Z})$ ein.

Satz 3.2.1 Sei $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ eine Untergruppe von Index n mit gegebenen Nebenklassenvertretern

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=1}^n \Gamma g_i.$$

Dann ist

$$\mathcal{F}_\Gamma = \bigcup_{i=1}^n g_i \mathcal{F}$$

ein Fundamentalbereich für Γ .

Beweis. Siehe auch [Gu], Theorem 4. Die Offenheit ist klar. Jeder Punkt $\tau \in \mathbb{H}$ kann durch ein $\gamma \in \Gamma$ in den Abschluss $\overline{\mathcal{F}_\Gamma}$ transportiert werden. Dies sieht man so: Sei $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ mit $\sigma^{-1} \cdot \tau \in \mathcal{F}$. Unter obiger Nebenklassenzerlegung erhalten wir $\sigma^{-1} = \gamma g_i$ für ein $\gamma \in \Gamma$ und ein $i \in \{1, \dots, n\}$. Es folgt: $\gamma^{-1} \tau \in g_i \mathcal{F}$. Ist nun $\tau \in \mathcal{F}_\Gamma$ und $\gamma \tau \in \mathcal{F}_\Gamma$, dann gibt es $i, j \in \{1, \dots, n\}$ mit $g_i^{-1} \cdot \tau \in \mathcal{F}$ und $g_j^{-1} \gamma \cdot \tau \in \mathcal{F}$, weshalb $g_i \gamma = \pm g_j$ und daher $i = j$ und $\gamma = \pm 1$. \square

Wir schauen uns einige Beispiele an:

- Sei $\Gamma := \Gamma_0(2)$. Wir haben

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma \cup \Gamma S \cup \Gamma ST.$$

Der Index ist nämlich 3 und weder S noch ST oder STS sind in Γ . Damit erhalten wir den Fundamentalbereich: [Bild] Dabei wird $S\mathcal{F}$ abgegrenzt von den Halbkreisbögen von -1 nach 1 , von -2 nach 0 und von 0 nach 2 (denn diese sind gerade die Transformationen unter S von $-1/2$, $1/2$ und ∞). Genauso sieht man, dass $ST\mathcal{F}$ abgegrenzt wird von den Halbkreisbögen $-3/2$ nach 0 , von 0 nach -2 und von $-1/2$ nach ∞ (also der Senkrechten bei $-1/2$).

- Sei $\Gamma := \Gamma_0(3)$. Der Index ist nun 4 und wir haben

$$\mathrm{SL}_2(\mathbb{Z}) = \Gamma \cup \Gamma S \cup \Gamma ST \cup \Gamma ST^{-1}.$$

Damit ergibt sich der folgende Fundamentalbereich: [Bild]

Am Bild erkennt man nun auch, woher die Spitzen ihren Namen haben.

3.2.2 Moduli-Interpretation für Standardkongruenzuntergruppen

[31.05.2007] Für algebraische Verallgemeinerungen von Modulformen, die wir in dieser Vorlesung nicht behandeln, sind strukturelle Interpretationen der Bahnen $\Gamma \backslash \mathbb{H}$ von entscheidender Bedeutung. Wir haben bereits die Bijektion

$$\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H} \longrightarrow \{\text{Komplexe elliptische Kurven}\} / \cong, \quad \tau \mapsto \mathbb{C} / \Lambda_\tau$$

in Satz 2.4.13 gesehen. Damit entspricht also jede Bahn $\mathrm{SL}_2(\mathbb{Z}) \cdot \tau$ für ein $\tau \in \mathbb{H}$ (oder auch jeder Punkt von \mathcal{F} vereinigt mit der ‘‘Hälfte’’ des Randes) einer komplexen elliptischen Kurve bis auf Isomorphie.

Diese Beobachtung wollen wir nun auf die Bahnräume $\Gamma(N) \backslash \mathbb{H}$, $\Gamma_1(N) \backslash \mathbb{H}$ und $\Gamma_0(N) \backslash \mathbb{H}$ verallgemeinern. Dazu erinnern wir, dass es für jede komplexe elliptische Kurve und jedes $n \in \mathbb{N}$ nach Satz 2.2.7 einen Gruppenisomorphismus

$$(\mathbb{Z}/N\mathbb{Z})^2 \stackrel{\alpha}{\cong} E[N] \quad (N\text{-Torsion})$$

gibt. Solch einen Gruppenhomomorphismus können wir auch als ‘‘Basiswahl’’ in $E[N]$ verstehen; er ist nämlich eindeutig durch die Bilder von $(1, 0)$ und $(0, 1)$, also zwei Punkte $P, Q \in E[N]$ gegeben. Dass α ein Isomorphismus ist, bedeutet dann einfach, dass P, Q die Gruppe $E[N]$ erzeugen. Ein Isomorphismus α bzw. die Vorgabe zweier erzeugender Punkte von $E[N]$ heißt eine (*volle*) *Drinfeldsche Stufenstruktur*.

Ist die komplexe elliptische Kurve als Torus, also als \mathbb{C}/Λ gegeben, dann ist der Gruppenisomorphismus explizit

$$(\mathbb{Z}/N\mathbb{Z})^2 \xrightarrow{(1,0) \mapsto \frac{r\omega_1 + s\omega_2}{N} + \Lambda, (0,1) \mapsto \frac{t\omega_1 + u\omega_2}{N} + \Lambda} \frac{1}{N} \Lambda / \Lambda \cong \mathbb{C} / \Lambda[N]$$

für $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$. Wir führen nun eine Kurzschreibweise für die N -Torsionspunkte ein, nämlich

$$\frac{r\omega_1 + s\omega_2}{N} + \Lambda = \frac{1}{N} (r, s) \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} + \Lambda.$$

Dabei sind r und s natürlich nur modulo N eindeutig bestimmt. Wir wählen sie daher häufig stillschweigend in $\mathbb{Z}/N\mathbb{Z}$. Eine Basis von $E[N]$ ist somit genau dann gegeben durch

$$\frac{1}{N} \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} + \Lambda,$$

wenn $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ ist.

Ist nun $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, dann haben wir gesehen, dass $\omega'_1 := a\omega_1 + b\omega_2, \omega'_2 := c\omega_1 + d\omega_2$ eine weitere Basis von Λ bilden. Wir wollen nun den Torsionspunkt $\frac{r\omega_1}{N} + \frac{s\omega_2}{N} + \Lambda$ in der neuen Basis ausdrücken. Wir erhalten wegen

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

dass

$$\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix}$$

und also

$$\omega_1 = d\omega'_1 - b\omega'_2 \text{ und } \omega_2 = -c\omega'_1 + a\omega'_2$$

gilt. Schließlich ist

$$\frac{1}{N}(r\omega_1 + s\omega_2) + \Lambda = \frac{1}{N}(r, s) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} + \Lambda.$$

In der neuen Basis stellt sich somit der Torsionspunkt $\frac{r\omega_1}{N} + \frac{s\omega_2}{N} + \Lambda$ als

$$\frac{r\omega_1}{N} + \frac{s\omega_2}{N} + \Lambda = \frac{(rd - sc)\omega'_1}{N} + \frac{(-rb + sa)\omega'_2}{N} + \Lambda$$

dar.

Bemerkung 3.2.2 *Da es sich später als nützlich herausstellen wird, bemerken wir hier, dass aus der Nebenklassenzerlegung $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) = \bigcup_{\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}$ folgt, dass es zu jeder Basis von $E[N]$, die durch $\begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ gegeben ist, eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ und eine Einheit $\alpha \in (\mathbb{Z}/N\mathbb{Z})^\times$ gibt, so dass*

$$\frac{1}{N} \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} + \Lambda = \frac{1}{N} \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} + \Lambda = \frac{1}{N} \begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} + \Lambda$$

gilt.

Ist weiter ein einziger N -Torsionspunkt als $\frac{1}{N}(r, s) \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} + \Lambda$ gegeben, so existiert eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$ derart, dass der Punkt in der neuen Basis zu $\frac{1}{N}(0, 1) \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} + \Lambda$ wird.

Ist wiederum ein N -Torsionspunkt als $\frac{1}{N}(r, s) \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} + \Lambda$ gegeben, so existiert eine Matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ derart, dass der Punkt in der neuen Basis zu $\frac{1}{N}(0, q) \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} + \Lambda$ wird für ein $q \in (\mathbb{Z}/N\mathbb{Z})^\times$. Wir bemerken dass $\frac{1}{N}(0, q) \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} + \Lambda$ und $\frac{1}{N}(0, 1) \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} + \Lambda$ dieselbe zyklische Untergruppe der Ordnung N aufspannen.

Γ_1 -Stufenstruktur

Wir betrachten nun die Menge der Paare (E, P) , wobei E eine komplexe elliptische Kurve und $P \in E$ ein N -Torsionspunkt (d. h. er hat genaue Ordnung N) ist. Zwei Paare (E_1, P_1) und (E_2, P_2) heißen *isomorph*, wenn es einen Isomorphismus $\phi : E_1 \rightarrow E_2$ gibt, so dass $\phi(P_1) = P_2$. Isomorphie ist klarerweise eine Äquivalenzrelation.

Satz 3.2.3 *Die Abbildung*

$$\Gamma_1(N) \backslash \mathbb{H} \rightarrow \{(E, P)\} / \cong, \quad \tau \mapsto (\mathbb{C}/\Lambda_\tau, \frac{1}{N})$$

ist eine Bijektion.

Beweis. Zunächst die Wohldefiniertheit der Abbildung. Sei $\gamma \in \Gamma_1(N)$. Wir führen einen Basiswechsel mit γ des Gitters Λ_τ aus und erhalten $\Lambda_{a\tau+b, c\tau+d}$. In der neuen Basis schreibt sich der Punkt $\frac{1}{N}$, also $(0, 1) \begin{pmatrix} \tau \\ 1 \end{pmatrix}$, als

$$\frac{1}{N}(0, 1) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} a\tau+b \\ c\tau+d \end{pmatrix} + \Lambda = \frac{1}{N}(-c, a) \begin{pmatrix} a\tau+b \\ c\tau+d \end{pmatrix} + \Lambda = \frac{1}{N}(0, 1) \begin{pmatrix} a\tau+b \\ c\tau+d \end{pmatrix} + \Lambda.$$

Die Kurven $\mathbb{C}/\Lambda_{a\tau+b, c\tau+d}$ und $\mathbb{C}/\Lambda_{\gamma\tau}$ sind isomorph unter Streckung mit $\frac{1}{c\tau+d}$ (wie wir schon oft benutzt haben). Dieser Isomorphismus transportiert den Punkt $\frac{c\tau+d}{N}$ auf $\frac{1}{N}$, wie gewünscht.

Aus derselben Rechnung ersieht man auch die Injektivität.

Zur Surjektivität. Sei (E, P) gegeben. Man nimmt sich zunächst irgendeine Kurve \mathbb{C}/Λ_τ , die zu E isomorph ist. Der Isomorphismus wird den Punkt auf irgendeinen N -Torsionspunkt $\frac{r\tau+s}{N} + \Lambda_\tau$ abbilden. Nach Bemerkung 3.2.2 existiert eine Matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, so dass nach Basiswechsel mit dieser Matrix und dem Isomorphismus $(c\tau + d)^{-1}$ der obige N -Torsionspunkt auf $\frac{1}{N} + \Lambda_{\gamma\tau}$ abgebildet wird. \square

Γ_0 -Stufenstruktur

Wir betrachten nun die Menge der Paare (E, C) , wobei E eine komplexe elliptische Kurve und $C \subset E$ eine zyklische Untergruppe der Ordnung N ist. Zwei Paare (E_1, C_1) und (E_2, C_2) heißen *isomorph*, wenn es einen Isomorphismus $\phi : E_1 \rightarrow E_2$ gibt, so dass $\phi(C_1) = C_2$.

Satz 3.2.4 *Die Abbildung*

$$\Gamma_0(N) \backslash \mathbb{H} \rightarrow \{(E, P)\} / \cong, \quad \tau \mapsto (\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} \rangle)$$

ist eine Bijektion.

Aufgabe 3.2.5 *Beweise den Satz.*

Γ -Stufenstruktur

Wir betrachten nun die Menge der Paare (E, α) , wobei E eine komplexe elliptische Kurve und $\alpha : (\mathbb{Z}/N\mathbb{Z})^2 \cong E[N]$ ein Gruppenisomorphismus ist. Zwei Paare (E_1, α_1) und (E_2, α_2) heißen *isomorph*, wenn es einen Isomorphismus $\phi : E_1 \rightarrow E_2$ gibt, so dass $\phi_1 \circ \alpha_1 = \alpha_2$.

Wir skizzieren nun einen Satz wie zur Γ_1 -Stufenstruktur. Dazu betrachten wir die Abbildung

$$\bigsqcup_{\beta \in (\mathbb{Z}/N\mathbb{Z})^\times} \Gamma(N) \backslash \mathbb{H} \rightarrow \{(E, \alpha)\} / \cong, \quad \tau \mapsto (\mathbb{C}/\Lambda_\tau, (\frac{1}{N}, \frac{\beta_\tau \tau}{N})),$$

wobei β_τ die Komponente sei, auf der τ liegt. Man rechnet nach, dass diese Abbildung wohl-definiert und bijektiv ist.

Modulformen als Funktionen auf elliptischen Kurven mit Stufenstruktur

Wir beschränken uns hier auf eine Interpretation von Modulformen zu $\Gamma_1(N)$ von einem Gewicht k . Diese Interpretation ist eine einfache Verallgemeinerung der Situation, die wir für die Stufe 1 gesehen haben. Wir betrachten nun Funktionen des Typs

$$F : \{(E, P)\} \rightarrow \mathbb{C},$$

wobei (E, P) wie zuvor eine elliptische Kurve E zusammen mit einem Punkt $P \in E$ der exakten Ordnung P ist. Von den Funktionen F verlangen wir, dass sie für jedes $s \in \mathbb{C} - \{0\}$ die Gleichung

$$F((\mathbb{C}/s\Lambda, sP)) = s^{-k} F((\mathbb{C}/\Lambda, P)) \quad (3.2.1)$$

erfüllen, wobei wir die Multiplikation mit s als Abbildung

$$\mathbb{C}/\Lambda \xrightarrow{\cdot s} \mathbb{C}/\Lambda, \quad P \mapsto s \cdot P$$

ansehen sollten. Sei nun eine Modulform f zu $\Gamma_1(N)$ von Gewicht k gegeben. Wir setzen genauso wie zuvor

$$F((E, P)) = (\omega'_2)^{-k} f\left(\frac{\omega'_1}{\omega'_2}\right),$$

wobei $E = \mathbb{C}/\Lambda_{\omega_1, \omega_2}$, $P = \frac{1}{N}(r, s) \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} + \Lambda_{\omega_1, \omega_2}$ und $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ mit $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix}$ und $\frac{1}{N}(r, s) \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix} = \frac{1}{N}(0, 1) \begin{pmatrix} \omega'_1 \\ \omega'_2 \end{pmatrix}$ sind.

Aufgabe 3.2.6 Rechne nach, dass F wohl-definiert ist (vgl. Satz 2.4.11).

Bemerkung 3.2.7 Nicht jede Funktion F , die Gleichung 3.2.1 erfüllt kommt von einer Modulform: Wir benötigen Holomorphie und Holomorphie in den Spitzen. Aber man kann diese Eigenschaften auch algebraisch fassen, was aber über den Rahmen der jetzigen Vorlesung hinausgeht.

Aufgabe 3.2.8 Formuliere ähnliche Aussagen für $\Gamma_0(N)$ und $\Gamma(N)$.

3.2.3 Modulkurven für stabilisatorfreie Untergruppen

Wir beginnen mit einem Satz, der uns zeigt, dass die Untergruppen im Titel häufig vorkommen.

Satz 3.2.9 Für $N \geq 3$ ist die Gruppe $\Gamma(N)$ stabilisatorfrei. Gleiches gilt für $\Gamma_1(N)$, falls $N \geq 4$.

Beweis. Der Betrag der Spur elliptischer Matrizen beträgt 0 oder 1. Im beiden Fällen betrachten wir Matrizen des Typs $\begin{pmatrix} 1+Na & b \\ c & 1+Nd \end{pmatrix}$, deren Spur $2 + N(a + d)$ ist. Man sieht unmittelbar, dass für $N \geq 4$ der Betrag dieses Ausdrucks nicht 0 oder 1 sein kann. Für $N = 3$ und $\Gamma(N)$ bleibt der Fall $a + d = -1$ zu betrachten. Wir nehmen nun die Determinante zu Hilfe. Aus $1 = (1 + Na)(1 + Nd) - bc = 1 + N(a + d) - bc = 1 - N - bc$ folgt $N = bc$, was einen Widerspruch darstellt, denn sowohl b als auch c sind durch N teilbar. \square

[13.06.2007] Die Konstruktion von Modulkurven für stabilisatorfreie Untergruppen ist einfacher, da die Gruppenoperation dann als eine "Vertauschung" von Umgebungen um jeden Punkt einer Bahn angesehen werden kann, vorausgesetzt, die Umgebungen sind hinreichend klein. Wir sollten folgendes Bild vor Augen haben [Bild].

Davon haben wir bereits im ersten Kapitel im Zusammenhang mit der Konstruktion von Tori Gebrauch gemacht. Wir verweisen ganz ausdrücklich auf Satz 2.1.29.

Seien G, X wie in Satz 2.1.29. Unser Ziel ist es nun, aus $G \backslash X$ eine Riemannsche Fläche zu machen, wenn X eine ist. Grob gesprochen ist eine Riemannsche Fläche ein topologischer Raum, so dass jeder Punkt eine Umgebung hat, die zu $U_1(0)$ homöomorph ist, und der eine holomorphe Struktur trägt. Beispiele für eine erste Vorstellung sind \mathbb{C}, \mathbb{H} und $U_1(0)$. Bezüglich $\Gamma_1(N) \backslash \mathbb{H}$ wissen wir schon für $N \geq 4$, dass zumindest jeder Punkt eine Umgebung besitzt, die zu $U_1(0)$ homöomorph ist. Wir müssen uns im Folgenden also hauptsächlich um die holomorphe Struktur kümmern.

Definition 3.2.10 Sei X ein topologischer Raum und I eine Indexmenge. Für jedes $i \in I$ sei ein Tripel (U_i, V_i, ϕ_i) gegeben mit:

- $U_i \subseteq X$ eine offene Menge,
- $V_i \subseteq \mathbb{C}$ eine offene Menge,
- $\phi_i : U_i \rightarrow V_i$ ein Homöomorphismus.

Dann heißt X zusammen mit $(U_i, V_i, \phi_i)_{i \in I}$ eine Riemannsche Fläche, falls die folgenden Punkte gelten:

- $X = \bigcup_{i \in I} U_i$,
- $\mathbb{C} \supseteq \phi_i^{-1}(U_i \cap U_j) \xrightarrow{\phi_i^{-1}} U_i \cap U_j \xrightarrow{\phi_j^{-1}} \phi_j(U_i \cap U_j) \subseteq \mathbb{C}$ ist eine holomorphe Abbildung für alle $i, j \in I$ und
- für jeden Punkt $x \in X$ ist in $\{U_i\}_{i \in I}$ eine Umgebungsbasis von x enthalten, d.h. um für jede offene Menge $M \ni x$ gibt es ein i , so dass $x \in U_i \subseteq M$ gilt.

Die (U_i, V_i, ϕ_i) heißen Karten und die Menge der Karten $\{(U_i, V_i, \phi_i)\}_{i \in I}$ heißen Atlas.

Definition 3.2.11 Seien X, Y Riemannsche Flächen und $f : X \rightarrow Y$ eine stetige Abbildung. Sei $\{(U_i, V_i, \phi_i)\}_{i \in I}$ ein Atlas von X und $\{(\tilde{U}_j, \tilde{V}_j, \tilde{\phi}_j)\}_{j \in J}$ ein Atlas von Y . Die Abbildung f heißt holomorph oder auch Morphismus Riemannscher Flächen, falls es für jeden Punkt $y \in Y$ und jedes \tilde{U}_j im Atlas von Y um jedes $x \in X$ mit $f(x) = y$ ein U_i im Atlas von X gibt, so dass

- $f(U_i) \subseteq \tilde{U}_j$ und
- die Abbildung $\mathbb{C} \supseteq V_i \xrightarrow{\phi_i^{-1}} U_i \xrightarrow{f} \tilde{U}_j \xrightarrow{\tilde{\phi}_j} \tilde{V}_j \subseteq \mathbb{C}$ holomorph ist.

Bemerkung 3.2.12 Sei X eine Riemannsche Fläche mit einem Atlas $\{(U_i, V_i, \phi_i)\}_{i \in I}$. Man sagt, dass der Atlas $\{(\tilde{U}_j, \tilde{V}_j, \tilde{\phi}_j)\}_{j \in J}$ von X feiner ist als der ursprüngliche, wenn er alle Karten aus dem ursprünglichen enthält. Wir betrachten die Identität $X \rightarrow X$. Diese ist eine holomorphe Abbildung, wenn wir das rechte X mit dem groben und das linke X mit dem feinen Atlas ausstatten. Dies nehmen wir als Rechtfertigung dafür, dass wir in den folgenden Beweisen Atlanten nach Belieben verfeinern.

Die hier vorgestellte Definition von Riemannschen Flächen ist nicht die "Standarddefinition", welche mit "maximalen Atlanten" arbeitet. Es sollte aber durchweg genügen, die Existenz einer Umgebungsbasis um jeden Punkt im Atlas zu fordern, was wir ja getan haben.

Definition 3.2.13 Sei X eine Riemannsche Fläche und G eine Gruppe, die stetig auf X operiert. Diese Operation heißt holomorph, wenn die Abbildung $X \xrightarrow{x \mapsto g \cdot x} X$ für jedes $g \in G$ holomorph ist.

Satz 3.2.14 Seien X eine Riemannsche Fläche und Γ eine Gruppe, die auf X holomorph, frei und mit gleichmäßig diskreten Bahnen operiert. Dann ist $\Gamma \backslash X$ eine Riemannsche Fläche und die natürliche Projektion $\pi : X \rightarrow \Gamma \backslash X$ ist eine holomorphe Abbildung Riemannscher Flächen.

Beweis. Wir nehmen zunächst ohne Einschränkung einen etwas gröberen Atlas auf X , indem wir zu einer Teilmenge $J \subset I$ übergehen, so dass für jedes $j \in J$ aus $\gamma U_j \cap U_j \neq \emptyset$ folgt, dass $\gamma = 1$ ist. Dies dürfen wir annehmen, da wir die Freiheit der Operation und gleichmäßig diskrete Bahnen vorausgesetzt haben. Da es bei der Struktur von Riemannschen Flächen nur um das lokale Aussehen, also das in kleinen Umgebungen um jeden Punkt geht, verlieren wir so keine Information.

Wegen dieser Vergrößerung haben wir nun, dass für alle $j \in J$ die Einschränkung

$$\pi : U_j \rightarrow \pi(U_j)$$

ein Homöomorphismus ist. Diesen benutzen wir, um in natürlicher Weise einen Atlas auf dem Quotienten zu definieren.

Die Indexmenge für den Atlas des Quotienten sei auch J . Als Karten benutzen wir

$$(\pi(U_j), V_j, \bar{\phi}_j : \pi(U_j) \xrightarrow{\pi^{-1}} U_j \xrightarrow{\phi_j} V_j)_{j \in J}.$$

Dieser Atlas enthält offenbar Umgebungsbasen um jeden Punkt des Quotienten. Außerdem rechnet man nach, dass die Kartenwechselabbildungen holomorph sind, da sie bis auf eine holomorphe Translation mit einem Element aus Γ mit einer Kartenwechselabbildung von X übereinstimmen. Dass der Quotient eine holomorphe Abbildung ist, ergibt sich unmittelbar. \square

Korollar 3.2.15 Sei $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ eine stabilisatorfreie Untergruppe. Dann ist $Y_\Gamma = \Gamma \backslash \mathbb{H}$ eine Riemannsche Fläche und die natürliche Projektion ist eine holomorphe Abbildung. \square

Satz 3.2.16 Sei $\Gamma \leq \mathrm{SL}_2(\mathbb{Z})$ eine stabilisatorfreie Untergruppe. Dann ist $X_\Gamma = Y_\Gamma \cap \Gamma \backslash \mathbb{P}^1(\mathbb{Q})$ eine kompakte Riemannsche Fläche und die natürliche Projektion ist eine holomorphe Abbildung.

Beweis. Zunächst müssen wir einen Atlas beschreiben und dann die Kompaktheit zeigen. Natürlich soll der Atlas auf Y_Γ mit dem oben definierten übereinstimmen. Wir müssen also nur Karten auf Umgebungen der Spitzen angeben. Jede Spitze kann mit einem $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ nach ∞ transportiert werden. Ohne Einschränkung betrachten wir daher nun die Spitze ∞ , die die Weite h habe. Als Karte auf einer Standardumgebung $\{t = x + iy \mid y > T\}$ benutzen wir $q_h = e^{2\pi i \tau / h}$, deren Bild in $U_{e^{-2\pi T}}(0)$ liegt. Man rechnet nach, dass die Kartenwechsel holomorph sind.

Nun zur Kompaktheit. Sei $X_\Gamma = \bigcup_{k \in K} M_k$ eine offene Überdeckung von X_Γ . Wir erhalten die offene Überdeckung $\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) = \bigcup_K \pi^{-1}(M_k)$. Insbesondere ist dies eine offene Überdeckung des Standardfundamentalbereiches \mathcal{F} zusammen mit den endlich vielen Spitzen, die diesen berühren. Für

jede dieser Spitzen s wählen wir nun ein $k_s \in K$, so dass $\pi^{-1}(M_{k_s})$ diese Spitze enthält. Dann ist $\overline{\mathcal{F}} - \bigcup_s \pi^{-1}(M_{k_s})$ kompakt und wird daher von endlich vielen M_k überdeckt. Folglich wird auch $\overline{\mathcal{F}}$ zusammen mit den berührenden Spitzen von endlich vielen $\pi^{-1}(M_k)$ überdeckt, indem wir einfach die $\pi^{-1}(M_{k_s})$ hinzunehmen. Da die Projektion auf den Quotienten surjektiv ist, überdecken diese M_k bereits X_Γ . \square

3.2.4 Modulkurven für Kongruenzuntergruppen

Der Anschaulichkeit halber beschränken wir uns auf Kongruenzuntergruppen, da wir von diesen wissen, dass sie eine stabilisatorfreie Untergruppe (sogar einen Normalteiler) haben. Alles in diesem Abschnitt zu sagende gilt aber auch für allgemeine Untergruppen von $SL_2(\mathbb{Z})$ von endlichem Index.

Unser Vorgehen ist wie folgt. Ist Γ eine Kongruenzuntergruppe, dann enthält sie per Definition ein $\Gamma(N)$, wobei wir ohne Einschränkung $N \geq 3$ annehmen können. Wir werden dann zur Konstruktion von $Y_\Gamma = \Gamma \backslash \mathbb{H}$ zunächst $Y_{\Gamma(N)} = \Gamma(N) \backslash \mathbb{H}$ benutzen, dem wir im vorigen Abschnitt die Struktur einer Riemannschen Fläche gegeben haben. Es ist dann $Y_\Gamma = (\Gamma/\Gamma(N)) \backslash Y_{\Gamma(N)}$. Wir brauchen daher nur noch Quotienten von Riemannschen Flächen nach endlichen Gruppen zu betrachten.

Beispiel 3.2.17 *Dieses Beispiel ist das allerwichtigste zur Konstruktion von Quotienten von Riemannschen Flächen nach endlichen Gruppen, da alle solchen lokal aussehen wie im Beispiel.*

Wir betrachten $U_1(0)$ als Riemannsche Fläche (mit den offensichtlichen Karten: die Identitäten in \mathbb{C}). Darauf operiere die zyklische Gruppe $G = \mathbb{Z}/e\mathbb{Z}$ via

$$U_1(0) \xrightarrow{z \mapsto \zeta_e^i z} U_1(0)$$

mit $\zeta_e = e^{2\pi i/e}$. Diese Operation ist holomorph, der Punkt 0 ist der einzige nicht-triviale stabilisierte Punkt und der Stabilisator in 0 ist die gesamte Gruppe G .

Wir machen $U_1(0)/G$ zu einer Riemannschen Fläche via dem Atlas, der aus folgenden Karten besteht.

- *Umgebungsbasis der 0: Für jedes $1 > \delta > 0$ betrachten wir die Karte $U_\delta(0)/G \xrightarrow{z \mapsto z^e} U_0(\delta) \subset \mathbb{C}$. Die Abbildung ist ein Homöomorphismus.*
- *Sei $x \neq 0$. Umgebungsbasis von x : Für jedes $\delta > 0$, so dass $U_\delta(x) \cap \zeta_e^i U_\delta(x) = \emptyset$ für $i \not\equiv 0 \pmod{e}$, betrachten wir die Karte $U_\delta(x)/G \xrightarrow{\pi^{-1}} U_\delta(x) \subset \mathbb{C}$. Die Abbildung ist wiederum ein Homöomorphismus.*

Man rechnet nach, dass es sich um eine Riemannsche Fläche handelt. [Bild eines Fundamentalbereiches]

Das folgende Lemma von Schwartz sagt uns schon einmal, dass obiges Beispiel nicht ganz so speziell ist, wie es vielleicht auf den ersten Blick aussieht.

Lemma 3.2.18 (Schwartz) Sei G eine endliche Gruppe, die auf $U_1(0)$ holomorph und treu operiert, so dass $g \cdot 0 = 0$ für alle $g \in G$ gilt. Setze $e = \#G$. Dann gibt es einen Gruppenisomorphismus $\phi : G \rightarrow \langle \zeta_e \rangle$, so dass die Operation von $g \in G$ auf $U_1(0)$ die Multiplikation mit $\phi(g)$ ist.

Beweis. Nach dem Lemma von Schwartz ([FB], S. 125/126) ist jede biholomorphe Abbildung mit $0 \mapsto 0$ von der Form $z \mapsto \zeta z$ für ein ζ mit $|\zeta| = 1$. Wegen $g^e = 1$ ist $\zeta^e = 1$. Also erhalten wir die Abbildung $\phi : G \rightarrow \langle \zeta_e \rangle$. Wegen der Treue ist diese injektiv. Sie ist auch surjektiv, da die Ordnungen links und rechts identisch sind. \square

Lemma 3.2.19 Sei X eine zusammenhängende Riemannsche Fläche, auf der die endliche Gruppe G holomorph und treu operiert. Dann sind die nicht-trivial stabilisierten Punkte $x \in X$ diskret.

Beweis. Sei $1 \neq g \in G$ fest. Es genügt zu zeigen, dass die Punkte x mit $g \cdot x = x$ diskret sind. Wären sie es nicht, dann gäbe es einen Häufungspunkt. Die holomorphe Abbildung $X \xrightarrow{x \mapsto g \cdot x} X$ wäre dann aber gleich der Identität, da sie auf einer Menge, die einen Häufungspunkt enthält, mit der Identität übereinstimmt (dies folgt aus einem Satz der Theorie der Riemannschen Flächen, der sich genauso wie der entsprechende Satz der Funktionentheorie beweist). Dass g via der Identität operiert, haben wir aber durch die Forderung der Treue ausgeschlossen. \square

Sei X eine zusammenhängende Riemannsche Fläche, auf der die endliche Gruppe G treu und holomorph operiert. Nach dem Lemma sind die nicht-trivial stabilisierten Punkte diskret. Sei x ein solcher und sei U eine Umgebung von x , so dass $U \cap gU = \emptyset$ für alle $g \notin G_x$. Wir können ohne Einschränkung annehmen, dass U unter der Operation von G_x stabil und einfach zusammenhängend ist. Dies muss man sich überlegen; dazu startet man zunächst mit einem einfach zusammenhängenden U , bildet dann $\bigcup_{g \in G_x} gU$. Ist diese Menge nicht einfach zusammenhängend, dann hat sie endlich viele Löcher. Durch Verkleinerung der Startmenge U kann man dann erreichen, dass $\bigcup_{g \in G_x} gU$ einfach zusammenhängend ist. Nach dem Riemannschen Abbildungssatz ist jede einfach zusammenhängende beschränkte Menge biholomorph zu $U_1(0)$. Die Operation von G_x wird unter dieser Identifikation zu einer treuen holomorphen Operation auf $U_1(0)$, die wir unter Zuhilfenahme des Lemmas von Schwartz wie im obigen Beispiel beschreiben können.

Somit sehen die Stabilisatoren der Gruppenoperation auf einer Riemannschen Fläche lokal genau wie im Beispiel aus. Insbesondere ist die Gruppe G_x zyklisch. [Bild] Über dem Punkt $\pi(x)$ liegen also $\#(G/G_x)$ verschiedene Punkte (für π die natürliche Projektion).

Definition 3.2.20 Ist x ein nicht-trivial stabilisierter Punkt, dann heißt die natürliche Projektion $\pi : X \rightarrow G \backslash X$ bei x verzweigt und $e_x := \#G_x$ heißt der Verzweigungsindex.

[14.06.2007]

Satz 3.2.21 Sei X eine zusammenhängende (kompakte) Riemannsche Fläche, auf der die endliche Gruppe G holomorph operiert. Dann ist $G \backslash X$ eine (kompakte) Riemannsche Fläche und die natürliche Projektion ist eine holomorphe Abbildung.

Beweis. Wir skizzieren den Beweis nur. Als Karten benutzen wir die folgenden:

$$\pi(U_j) \cong U_j/G_x \cong U_1(0)/\langle \zeta_{e_x} \rangle \xrightarrow{z \mapsto z^{e_x}} U_1(0) \subset \mathbb{C},$$

wobei U_j eine Umgebung von x sei, die hinreichend klein ist (wie vorne).

Um die Kompaktheit von $G \setminus X$ für kompaktes X zu sehen, genügt es, eine gegebene Überdeckung von $G \setminus X$ auf X zurückzuziehen und dort die Kompaktheit auszunutzen. \square

Korollar 3.2.22 Sei Γ eine Kongruenzuntergruppe. Dann sind Y_Γ und X_Γ Riemannsche Flächen und X_Γ ist kompakt. \square

3.3 Modulkurven und Modulformen

3.3.1 Modulformen als Differentialformen

Definition 3.3.1 • Sei $U \subseteq \mathbb{C}$ eine offene Menge. Wir setzen

$$\Omega_{\text{hol}}^m(U) = \{f(z)(dz)^m \mid f : U \rightarrow \mathbb{C} \text{ holomorph}\}$$

und

$$\Omega_{\text{mer}}^m(U) = \{f(z)(dz)^m \mid f : U \rightarrow \mathbb{C} \text{ meromorph}\}.$$

Dabei ist $(dz)^m$ einfach als Symbol zu verstehen und somit ist $\Omega_{\text{mer}}^m(U) = \mathfrak{M}(U)(dz)^m$, wobei $\mathfrak{M}(U)$ die meromorphen Funktionen auf U sind (ähnlich für die holomorphen).

Für eine Funktion f wie oben heißt $f(dz)^m$ das assoziierte m -Differential.

- Seien $U, U' \subseteq \mathbb{C}$ offene Mengen und $\phi : U \rightarrow U'$ sei eine holomorphe Abbildung. Ferner sei $\omega' = f(z')(dz')^m$ ein m -Differential auf U' . Dann ist

$$\phi^*(\omega) = f(\phi(z)) \left(\frac{d\phi}{dz}\right)^m (dz)^m = f(\phi(z))(d(\phi(z)))^m$$

ein m -Differential auf U' . Wir erhalten also eine Abbildung

$$\Omega_{\text{mer}}^m(U') \xrightarrow{\phi^*} \Omega_{\text{mer}}^m(U).$$

Es heißt $\phi^*(\omega)$ zurückgezogenes Differential. Ähnliches haben wir für die holomorphen Differentiale.

- Sei X nun eine Riemannsche Fläche mit Karten $(U_i, V_i, \phi_i)_{i \in I}$. Eine meromorphe m -Differentialform auf X ist eine Familie

$$(\omega_i)_{i \in I} = (f_i(z_i)(dz_i)^m)_{i \in I}$$

von meromorphen m -Differentialformen auf $\phi(U_i) = V_i$, so dass unter den Kartenwechselabbildungen

$$\phi_{i,j} : \phi(U_i \cap U_j) \xrightarrow{\phi_i^{-1}} U_i \cap U_j \xrightarrow{\phi_j} \phi_j(U_i \cap U_j)$$

gilt, dass $\phi_{i,j}^*(\omega_j) = \omega_i$, bzw. $f_i(z_i)(dz_i)^m = f_j(\phi_{i,j}(z_j))\left(\frac{d\phi_{i,j}}{dz_i}\right)^m (dz_i)^m$. Der Vektorraum der meromorphen m -Differentialen auf X wird mit $\Omega_{\text{mer}}^m(X)$ bezeichnet. Eine ähnliche Definition machen wir auch für holomorphe Differentiale. [Übrigens gebrauchen wir die Wörter “Differential” und “Differentialform” als Synonyme.]

- Seien X, Y Riemannsche Flächen und $\phi : X \rightarrow Y$ eine holomorphe Abbildung. Dann definiert man durch Zurückziehen auf den Karten eine Abbildung

$$\Omega_{\text{mer}}^m(Y) \xrightarrow{\phi^*} \Omega_{\text{mer}}^m(X)$$

und ähnlich für holomorphe Differentialformen.

Bemerkung 3.3.2 Sei X eine kompakte Riemannsche Fläche.

- $\Omega_{\text{mer}}^0(X) = \mathfrak{M}(X)$.
- $\Omega_{\text{hol}}^0(X) = \mathbb{C}$, da jede holomorphe Funktion, die auf ganz X definiert ist, konstant sein muss.
- $\dim_{\mathfrak{M}(X)} \Omega_{\text{mer}}^m(X) = 1$.
- Für eine nicht-konstante holomorphe Abbildung $\phi : X \rightarrow Y$ zwischen Riemannschen Flächen ist die Zurückziehabbildung $\phi^* : \Omega_{\text{mer}}^m(Y) \rightarrow \Omega_{\text{mer}}^m(X)$ injektiv. Denn wäre ϕ^* nicht injektiv, dann wäre die Ableitung von ϕ überall 0.

[20.06.2007] Wir begeben uns nun in die Situation von Modulkurven, die wir näher untersuchen wollen. Sei also von nun an Γ eine Kongruenzuntergruppe. Wir haben

$$\mathbb{H} \xrightarrow{\phi} Y_\Gamma \xrightarrow{j} X_\Gamma.$$

Die $SL_2(\mathbb{R})$ -Operation auf \mathbb{H} ergibt durch Zurückziehen eine $SL_2(\mathbb{R})$ -Operation auf $\Omega_{\text{mer}}^m(\mathbb{H})$. Diese machen wir nun explizit. Dafür sei $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ und $\omega = f(\tau)(d\tau)^m \in \Omega_{\text{mer}}^m(\mathbb{H})$. Dazu bemerken wir erst eben, dass wegen des einfachen Zusammenhangs von \mathbb{H} alle Differentiale auf \mathbb{H} von dieser einfachen Form sind. Für das zurückgezogene Differential $g^*\omega$ ergibt sich:

$$f(g\tau)(d(g\tau))^m = f\left(\frac{a\tau + b}{c\tau + d}\right)d\left(\frac{a\tau + b}{c\tau + d}\right)^m = f\left(\frac{a\tau + b}{c\tau + d}\right)(c\tau + d)^{-2m}(d\tau)^m = (f|_{2m}(g))(\tau)(d\tau)^m.$$

Dies erinnert uns natürlich schon wieder sehr stark an Modulformen. Genauer haben wir folgenden Zusammenhang:

Lemma 3.3.3 Sei $\Gamma \subseteq SL_2(\mathbb{Z})$ eine Untergruppe endlichen Indexes. Die Abbildungen

$$\{f : \mathbb{H} \rightarrow \mathbb{C} \text{ holomorph} \mid f|_{2m}(\gamma) = f \ \forall \gamma \in \Gamma\} \xrightarrow{f \mapsto f(\tau)(d\tau)^m} \Omega_{\text{hol}}^m(\mathbb{H})^\Gamma$$

und

$$\{f : \mathbb{H} \rightarrow \mathbb{C} \text{ meromorph} \mid f|_{2m}(\gamma) = f \ \forall \gamma \in \Gamma\} \xrightarrow{f \mapsto f(\tau)(d\tau)^m} \Omega_{\text{mer}}^m(\mathbb{H})^\Gamma$$

sind bijektiv. Dabei bezeichnet $(\cdot)^\Gamma$ die Γ -Invarianten.

Die erste Menge links ist bis auf die Bedingung in den Spitzen die Menge der Modulformen von Gewicht $2m$ zu Γ . Diese werden wir in Kürze auch noch behandeln. □

Nun wollen und können wir eine erste Beziehung zwischen Modulformen und Modulkurven herstellen. Es gilt nämlich der Satz:

Satz 3.3.4 Die natürliche Projektion $\pi : \mathbb{H} \rightarrow Y_\Gamma$ induziert durch Zurückziehen Bijektionen

$$\Omega_{\text{mer}}^m(Y_\Gamma) \rightarrow \Omega_{\text{mer}}^m(\mathbb{H})^\Gamma$$

und

$$\Omega_{\text{hol}}^m(Y_\Gamma) \rightarrow \Omega_{\text{hol}}^m(\mathbb{H})^\Gamma.$$

Beweis. Der Beweis ist etwas länglich, aber einfach. Die technische Komplikation tritt im Falle einer nicht-freien Operation von Γ auf, denn dann muss man die etwas komplizierteren Karten von Y_Γ benutzen. Für die Details siehe den Aufschrieb während der Vorlesung. \square

Definition 3.3.5 Sei Γ eine Untergruppe von $\text{SL}_2(\mathbb{Z})$ von endlichem Index. Für $k \in \mathbb{N}$ sei $A_k(\Gamma)$ der \mathbb{C} -Vektorraum der meromorphen Modulformen von Gewicht k zu Γ , d.h. dass $f : \mathbb{H} \rightarrow \mathbb{C}$ eine meromorphe Funktion ist, die $f|_k(\gamma) = f$ für alle $\gamma \in \Gamma$ erfüllt, und die meromorph in den Spitzen ist (mit der inzwischen offensichtlichen Definition dafür). [Wir haben meromorphe Modulformen inzwischen auch schon benutzt. Ich sollte diese Definition also etwas nach vorne schieben.]

Der folgende Satz gibt uns eine geometrische Beschreibung meromorpher Modulformen und somit einen ersten echten Zusammenhang zwischen Modulformen und Modulkurven.

Satz 3.3.6 Seien Γ eine Kongruenzuntergruppe und π, j wie oben. Das Bild der zusammengesetzten injektiven Abbildung

$$\Omega_{\text{mer}}^m(X_\Gamma) \xrightarrow{j^*} \Omega_{\text{mer}}^m(Y_\Gamma) \xrightarrow{\pi^*} \Omega_{\text{mer}}^m(\mathbb{H})^\Gamma$$

ist gleich der Menge $\{f(\tau)(d\tau)^m \mid f \in A_{2k}(\Gamma)\}$.

Beweis. Das einzige, was zu testen ist, ist die Meromorphie in den Spitzen. Wir können uns wiederum auf die Spitze ∞ beschränken, deren Weite h sei. Wir setzen wie immer $q_h = e^{2\pi i\tau/h}$ und erhalten

$$\frac{dq_h}{q_h} = \frac{2\pi i}{h} d\tau.$$

Wir wissen und benutzen, dass jede meromorphe Funktion $f : \mathbb{H} \rightarrow \mathbb{C}$, die der Transformationsregel $f|_{2m}(\gamma) = f$ für alle $\gamma \in \Gamma$ genügt, eine Fourier-Entwicklung besitzt. Damit folgt:

$$f(\tau)(d\tau)^m = \sum_{n \in \mathbb{Z}} a_n q_h^n (d\tau)^m = \left(\frac{h}{2\pi i}\right)^m \sum_{n \in \mathbb{Z}} a_n q_h^{n-m} (dq_h)^m = \omega. \quad (3.3.2)$$

Somit ist f genau dann meromorph in ∞ , wenn ω in ∞ meromorph ist. \square

Um nun von meromorphen Modulformen zu holomorphen zu gelangen, werden wir noch etwas mehr Notation einführen und einige Vorarbeiten leisten, die uns erlauben werden, den Holomorphiebegriff von Differentialen auf Quotienten nach nicht-freien Gruppenoperationen in den Griff zu bekommen.

Definition 3.3.7 Sei $\pi : Y \rightarrow X$ eine nicht-konstante holomorphe Abbildung Riemannscher Flächen. Sei $y \in Y$ beliebig. Nach Definition gibt es eine "kleine" Umgebung $Y \supseteq U \ni y$, so dass $\pi : U \rightarrow \pi(U)$ auf Karten (ohne Einschränkung mit $y \mapsto 0$ und $\pi(y) \mapsto 0$) durch eine Taylor-Reihe

$$\pi(z) = \sum_{n=e_y} a_n z^n$$

mit $a_{e_y} \neq 0$ beschrieben wird.

Dann heißt e_y der Verzweigungsindex von π bei y .

Bemerkung 3.3.8 • Nach geeigneten Transformationen können wir annehmen, dass das Bild der Karten jeweils $U_1(0)$ ist und π auf diesen Karten durch $z \mapsto z^{e_y}$ gegeben ist.

- Ist $\pi^{-1}(x)$ für $x \in X$ endlich, dann ist die Zahl

$$\sum_{y \in \pi^{-1}(x)} e_y$$

unabhängig von x . Sie heißt der Grad von π .

- Dies verallgemeinert die Definition von Verzweigung von Quotientenabbildungen $\pi : G \backslash X \rightarrow X$. Der Grad dieser Abbildung ist $\#G$, falls G endlich ist und treu und holomorph auf X operiert.

Lemma 3.3.9 Sei $\pi : Y \rightarrow X$ eine holomorphe Abbildung Riemannscher Flächen, die nicht konstant ist. Seien $y \in Y$ und $x \in X$ mit $\pi(y) = x$ und sei $\omega \in \Omega_{\text{mer}}^m(X)$. Dann gilt:

$$\frac{1}{e_y} \text{Ord}_y(\pi^* \omega) = \text{Ord}_x(\omega) + m \left(1 - \frac{1}{e_y}\right).$$

Beweis. Siehe Vorlesung. □

Definition 3.3.10 Sei X eine Riemannsche Fläche. Setze

$$\text{Div}_{\mathbb{Z}}(X) = \text{Div}(X) = \mathbb{Z}[X]$$

und

$$\text{Div}_{\mathbb{Q}}(X) = \mathbb{Q}[X].$$

Die Elemente beider heißen Divisoren von X . Dies sind also formale Linearkombinationen von Punkten aus X mit Koeffizienten in \mathbb{Z} oder \mathbb{Q} , von denen nur endlich viele nicht 0 sind.

Wir schreiben $\bar{\Gamma} = \Gamma / (\Gamma \cap \{\pm 1\})$.

Definition 3.3.11 Sei $\omega \in \Omega_{\text{mer}}^m(X)$ eine m -Differentialform für eine Riemannsche Fläche X . Wir setzen

$$\text{Div}(\omega) = \sum_{x \in X} \text{Ord}_x(\omega) x \in \text{Div}(X).$$

Dabei ist f_i , so dass $f_i(z_i)(dz_i)^m$ die Differentialform ω auf U_i beschreibt. (Man überprüft, dass die Definition unabhängig von der Wahl der Umgebung von x und der entsprechenden Karte ist.)

Definition 3.3.12 Sei $0 \neq f \in A_{2m}(\Gamma)$. Setze

$$\text{Div}(f) := \sum_{P \in X_\Gamma} \text{Ord}_P(f)P \in \text{Div}_\mathbb{Q}(X_\Gamma)$$

mit

$$\text{Ord}_P(f) = \begin{cases} \frac{1}{e_\tau} \text{Ord}_\tau(f), & \text{falls } \tau \in \mathbb{H} \text{ mit } \pi(\tau) = P \\ \text{Ord}_P(f(q)), & \text{falls } P \text{ Spitze} \end{cases}$$

Dabei ist $e_\tau = \#\bar{\Gamma}_\tau$ und $\text{Ord}_0(f|(\sigma))$ ist die Ordnung der Funktion $(f|(\sigma))(q) = \sum_{n \in \mathbb{Z}} a_n q^n$, wobei $\sigma_\infty = P$ und $q = e^{2\pi i \tau/h}$ mit der Weite h der Spitze P (das haben wir schon eher so benutzt).

Diese beiden Definitionen bringen wir nun im Falle der Modulformen zusammen.

Satz 3.3.13 Seien $f \in A_{2m}(\Gamma)$ und $\omega \in \Omega_{\text{mer}}^m(X_\Gamma)$ mit $j^* \pi^* \omega = f(\tau)(d\tau)^m$ (vgl. Satz 3.3.6). Dann gilt:

$$\text{Div}(f) = \text{Div}(\omega) + m \sum_{P \in Y_\Gamma} \left(1 - \frac{1}{e_P}\right)P + m(\text{Spitzen}_\Gamma) \in \text{Div}_\mathbb{Q}(X_\Gamma)$$

mit $(\text{Spitzen}_\Gamma) = \sum_{P \in X_\Gamma - Y_\Gamma} P$.

Beweis. Nach Gleichung 3.3.2 gilt $\text{Ord}_\infty(\omega) = \text{Ord}_\infty(f) - m$. Nun genügt es, das Lemma auf $\pi : \mathbb{H} \rightarrow \Gamma \backslash \mathbb{H}$ anzuwenden. \square

Definition 3.3.14 Sei X eine kompakte Riemannsche Fläche und $D = \sum_{P \in X} n_P P \in \text{Div}_\mathbb{Q}(X)$.

Wir setzen

$$\Omega_X^m(D) := \{\omega \in \Omega_{\text{mer}}^m(X) \mid \text{Div}(\omega) + D \geq 0\}$$

(dabei heißt “ \geq ”, dass alle Koeffizienten ≥ 0 sind). Ferner setzen wir

$$[D] := \sum_{P \in X} [n_P]P$$

mit der Gauß-Klammer (d.h. $[x]$ ist die größte ganze Zahl kleiner gleich x).

Korollar 3.3.15 Setze $E = \sum_{P \in Y_\Gamma} \left(1 - \frac{1}{e_P}\right)P + (\text{Spitzen}_\Gamma) \in \text{Div}_\mathbb{Q}(X_\Gamma)$. Dabei ist zur Erinnerung $e_P = \#\bar{\Gamma}_\tau$ für ein (jedes) $\tau \in \mathbb{H}$, in dessen Γ -Bahn P liegt. Dann haben wir die folgenden Isomorphismen (von \mathbb{C} -Vektorräumen):

$$\begin{aligned} \Omega_{\text{mer}}^m(X_\Gamma) &\xrightarrow{\omega \mapsto f} A_{2m}(\Gamma) \\ \Omega_{X_\Gamma}^m([mE]) &\xrightarrow{\omega \mapsto f} M_{2m}(\Gamma) \\ \Omega_{X_\Gamma}^m([mE] - (\text{Spitzen}_\Gamma)) &\xrightarrow{\omega \mapsto f} S_{2m}(\Gamma). \end{aligned}$$

Die Zuordnung erfolgt dabei unter Zuhilfenahme von Satz 3.3.6.

Insbesondere ist $\Omega_{X_\Gamma}^1(0) = \Omega_{\text{hol}}^1(X_\Gamma)$ isomorph zu $S_2(\Gamma)$.

Beweis. Laut vorherigem Satz gilt $\text{Div}(f) = \text{Div}(\omega) + E$. Die erste Zeile ist Satz 3.3.6. Die zweite Zeile entspricht der Bedingung $\text{Div}(f) \geq 0$ und die dritte der Bedingung $\text{Div}(f) \geq (\text{Spitzen}_\Gamma)$. \square

3.3.2 Das Geschlecht von Modulkurven

In diesem Abschnitt berechnen wir das Geschlecht von Modulkurven. Es ist gleich der Dimension des zugehörigen Vektorraumes von Modulkurven von Gewicht 2.

Lemma 3.3.16 *Ist $g : X \rightarrow \mathbb{C}$ eine meromorphe Abbildung und ist $f : Y \rightarrow X$ eine nicht-konstante holomorphe Abbildung Riemannscher Flächen, dann gilt die Formel*

$$e_y \text{Ord}_{f(y)}(g) = \text{Ord}_y(g \circ f)$$

mit $y \in Y$.

Lemma 3.3.17 *Es sei $\Gamma \leq \text{SL}_2(\mathbb{Z})$ eine Kongruenzuntergruppe und $\pi : X_\Gamma \rightarrow X_{\text{SL}_2(\mathbb{Z})}$ die natürliche Projektion. Dann gelten:*

(a) $\text{Grad}(\pi) = (\overline{\text{SL}_2(\mathbb{Z})} : \bar{\Gamma}),$

(b) $e_y = (\overline{\text{SL}_2(\mathbb{Z})}_y : \bar{\Gamma}_y)$ für $y \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$.

Aufgabe 3.3.18 *Beweise beide Lemmata.*

Definition 3.3.19 *Sei X eine kompakte zusammenhängende Riemannsche Fläche. Wir definieren das Geschlecht von X als*

$$g(X) = \dim_{\mathbb{C}} \Omega_{\text{hol}}^1(X).$$

Anschaulich ist das Geschlecht die Anzahl der Löcher in der Riemannschen Fläche und somit gleich $\dim_{\mathbb{C}} H_1(X, \mathbb{C})$. [Bild] Wir werden aber nur die Formel in der Definition benutzen.

Wir werden die Berechnung des Geschlechtes von X_Γ mit der Riemann-Hurwitz-Formel auf das Geschlecht von $X_{\text{SL}_2(\mathbb{Z})}$ zurückführen.

Lemma 3.3.20 *Es gilt $g(X_{\text{SL}_2(\mathbb{Z})}) = 0$.*

Beweis. Nach Korollar 3.3.15 ist das Geschlecht von $X_{\text{SL}_2(\mathbb{Z})}$ gleich der Dimension des Raumes der Spitzenformen von Gewicht 2 zu $\text{SL}_2(\mathbb{Z})$. Von dieser wissen wir aber, dass sie 0 ist. \square

Theorem 3.3.21 (Riemann-Hurwitz) *Sei $\pi : Y \rightarrow X$ eine nicht-konstante holomorphe Abbildung kompakter zusammenhängender Riemannscher Flächen. Dann gilt*

$$2g(Y) - 2 = (2g(X) - 2)\text{Grad}(\pi) + \sum_{y \in Y} (e_y - 1).$$

Den Beweis führen wir später auf S. 85.

Wir sind nun in der Lage, eine Formel für das Geschlecht von X_Γ anzugeben.

Theorem 3.3.22 *Sei $\Gamma \leq \text{SL}_2(\mathbb{Z})$ eine Kongruenzuntergruppe. Wir setzen:*

- $\mu := (\overline{\mathrm{SL}_2(\mathbb{Z})} : \bar{\Gamma})$,
- $\nu_\infty := \#\mathrm{Spitzen}_\Gamma = \#(\Gamma \backslash \mathbb{P}^1(\mathbb{Q}))$,
- $\nu_2 := \text{Anzahl der Punkte } \tau \in Y_\Gamma, \text{ so dass } \bar{\Gamma}_\tau \neq \{1\} \text{ und } \tau = \sigma i \text{ f\"ur ein } \sigma \in \mathrm{SL}_2(\mathbb{Z}),$
- $\nu_3 := \text{Anzahl der Punkte } \tau \in Y_\Gamma, \text{ so dass } \bar{\Gamma}_\tau \neq \{1\} \text{ und } \tau = \sigma e^{2\pi i/3} \text{ f\"ur ein } \sigma \in \mathrm{SL}_2(\mathbb{Z}).$

Dann gilt

$$g(X_\Gamma) = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}.$$

Beweis. Wir betrachten für den gesamten Beweis die natürlichen Projektionen

$$\mathbb{H} \cup \mathbb{P}^1(\mathbb{Q}) \xrightarrow{\Pi} X_\Gamma \xrightarrow{\pi} X_{\mathrm{SL}_2(\mathbb{Z})}.$$

Nach obigem Lemma ist das Geschlecht der rechten Riemannschen Fläche 0 und somit ergibt die Riemann-Hurwitz-Formel für π :

$$g(X_\Gamma) = 1 - \mu + \frac{1}{2} \sum_{y \in X_\Gamma} (e_y - 1),$$

da μ gleich dem Grad von π ist. Wir wollen nun also $\sum_{y \in X_\Gamma} (e_y - 1)$ berechnen.

Wir betrachten zunächst solche $\tau \in \mathbb{H}$ mit $\Pi(\tau) = y$ und $\pi(y) = i$. Es gibt zwei Möglichkeiten, je nach dem, ob $\bar{\Gamma}_y$ trivial ist oder nicht. Im ersten Fall folgt, dass π bei y verzweigt mit $e_y = 2$ und im zweiten Fall ist π unverzweigt, also $e_y = 1$. Mit unserer Definition von ν_2 folgt unmittelbar, dass es $\frac{\mu - \nu_2}{2}$ Punkte $y \in Y_\Gamma$ gibt, die in den ersten Fall fallen, und ν_2 Punkte im zweiten Fall.

Weiter betrachten wir nun solche $\tau \in \mathbb{H}$ mit $\Pi(\tau) = y$ und $\pi(y) = e^{2\pi i/3}$. Es gibt zwei Möglichkeiten, je nach dem, ob $\bar{\Gamma}_y$ trivial ist oder nicht. Im ersten Fall folgt, dass π bei y verzweigt mit $e_y = 3$ und im zweiten Fall ist π unverzweigt, also $e_y = 1$. Mit unserer Definition von ν_3 folgt unmittelbar, dass es $\frac{\mu - \nu_3}{3}$ Punkte $y \in Y_\Gamma$ gibt, die in den ersten Fall fallen, und ν_3 Punkte im zweiten Fall.

Außerdem wissen wir, dass für jedes $\tau \in \mathbb{H}$ mit $\overline{\mathrm{SL}_2(\mathbb{Z})}_\tau \neq \{1\}$ entweder $\pi(\Pi(\tau)) = i$ oder $\pi(\Pi(\tau)) = e^{2\pi i/3}$ gilt. Daher brauchen wir uns nun nur noch den Spitzen zuzuwenden. Es gibt ν_∞ Spitzen, die alle auf ∞ abbilden.

Somit folgt insgesamt:

$$\begin{aligned} \sum_{y \in X_\Gamma} (e_y - 1) &= \frac{\mu - \nu_2}{2}(2 - 1) + \frac{\mu - \nu_3}{3}(3 - 1) + \left(\sum_{y \in \mathrm{Spitzen}_\Gamma} e_y \right) - \nu_\infty \\ &= \frac{13}{6}\mu - \frac{1}{2}\nu_2 - \frac{2}{3}\nu_3 - \nu_\infty, \end{aligned}$$

wobei wir $\mu = \mathrm{Grad}(\pi) = \sum_{y \in \mathrm{Spitzen}_\Gamma} e_y$ benutzt haben. Die behauptete Formel folgt sofort. \square

Korollar 3.3.23 Sei $N \geq 3$. Setze $\mu_N = \frac{1}{2}N^3 \prod_{l|N} \text{Primzahl}(1 - \frac{1}{l^2})$. Es gilt:

$$g(X_{\Gamma(N)}) = 1 + \mu_N \frac{N - 6}{12N}.$$

Beweis. Wir haben vorne gesehen, dass $2 \cdot \mu_N = (\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N))$ ist, weshalb $\mu_N = (\overline{\mathrm{SL}_2(\mathbb{Z})} : \overline{\Gamma(N)})$ folgt. Außerdem wissen wir, dass $\nu_2 = \nu_3 = 0$ ist. Es gilt $\overline{\Gamma(N)}_\infty = \Gamma(N)_\infty = \langle T^N \rangle$ mit $T = \begin{pmatrix} 1 & \\ 0 & 1 \end{pmatrix}$, weshalb $e_\infty = N$ ist. Da $\Gamma(N)$ ein Normalteiler von $\mathrm{SL}_2(\mathbb{Z})$ ist, haben wir auch $e_{\sigma\infty} = N$ für alle $\sigma \in \mathrm{SL}_2(\mathbb{Z})$, denn

$$\Gamma(N)_{\sigma\infty} = \sigma \langle T^N \rangle \sigma^{-1} \cap \Gamma(N) = \sigma \langle T^N \rangle \sigma^{-1}.$$

Folglich ist nach der Gradformel $\nu_\infty = \mu_N/N$. Einsetzen in obiges Theorem ergibt die Behauptung. \square

Beispiel 3.3.24 Wir haben das Beispiel $\Gamma_0(2)$ anhand seines Fundamentalbereiches diskutiert und $\mu = 3$, $\nu_2 = 1$, $\nu_3 = 0$ und $\nu_\infty = 2$ gefunden, woraus $g(X_{\Gamma_0(2)}) = 0$ folgt.

[27.06.2007] Bei der Berechnung des Geschlechtes von $X_{\Gamma_0(N)}$ ist es sehr praktisch, Kriterien für $\nu_2 = 0$ und $\nu_3 = 0$ zu haben. Diese werden von der folgenden Aufgabe bereit gestellt.

Aufgabe 3.3.25 Benutze algebraische Zahlentheorie, um folgende Aussagen zu zeigen, in denen sich ν_2 und ν_3 auf die Modulkurve $X_{\Gamma_0(N)}$ beziehen:

- (a) $\nu_2 = 0 \Leftrightarrow N$ ist teilbar durch eine Primzahl $q \equiv 3 \pmod{4}$ oder N ist teilbar durch 4.
 (b) $\nu_3 = 0 \Leftrightarrow N$ ist teilbar durch eine Primzahl $q \equiv 2 \pmod{3}$ oder N ist teilbar durch 9.

Aufgabe 3.3.26 (a) Benutze Lemma 2.5.6 und Satz 2.5.7, um ein Vertretersystem von $\Gamma_0(N) \backslash \mathrm{SL}_2(\mathbb{Z})$ anzugeben (Achtung, die Formel, die ich in der Vorlesung angegeben hatte, ist leider falsch für N die keine Primzahlpotenzen sind).

- (b) Folgere, dass $X_{\Gamma_0(p)}$ mit einer Primzahl p genau zwei Spitzen hat, die von 0 und ∞ repräsentiert werden können. Dabei ist die Weite der Spitze 0 gleich p und die der Spitze ∞ gleich 1.
 (c) Folgere: $g(X_{\Gamma_0(4)}) = 0$ und $g(X_{\Gamma_0(11)}) = 1$.
 (d) Was sind $g(X_{\Gamma_0(35)})$ und $g(X_{\Gamma(2)})$?

3.3.3 Dimensionsformeln

Definition 3.3.27 Sei X eine Riemannsche Fläche und $D = \sum_{P \in X} n_P P \in \mathrm{Div}_{\mathbb{Q}}(X)$ ein Divisor. Der \mathbb{C} -Vektorraum

$$\mathcal{L}(D) := \{f : X \rightarrow \mathbb{C} \text{ meromorph} \mid \mathrm{Div}(f) + D \geq 0\}$$

heißt der Linearraum zu D . Wir setzen

$$l(D) := \dim_{\mathbb{C}} \mathcal{L}(D)$$

und

$$\mathrm{Grad}(D) := \sum_{P \in X} n_P.$$

Bemerkung 3.3.28 Sei X eine Riemannsche Fläche und $D = \sum_{P \in X} n_P P \in \text{Div}_{\mathbb{Q}}(X)$ ein Divisor.

- $\text{Grad}(\text{Div}(g)) = 0$ für jede meromorphe Funktion $g : X \rightarrow \mathbb{C}$. Dies ist eine recht einfache Konsequenz des Residuensatzes. Den Beweis geben wir aber nicht.

Damit gilt: $\text{Grad}(\text{Div}(g) + D) = \text{Grad}(D)$ und $\text{Grad}(\text{Div}(g\omega)) = \text{Grad}(\text{Div}(\omega))$ für jedes Differential $\omega \in \Omega_{\text{mer}}^m(X)$.

- Ist $\text{Grad}(D) < 0$, dann ist $l(D) = 0$. Dies ist eine triviale Aussage, die sich aber als ungeheuer wichtig herausstellen wird.
- Ist $D' \in \text{Div}_{\mathbb{Q}}(X)$ mit $D = D' + \text{Div}(g)$ für eine meromorphe Funktion $g : X \rightarrow \mathbb{C}$, dann haben wir den Isomorphismus

$$\mathcal{L}(D) \rightarrow \mathcal{L}(D'), \quad f \mapsto f \cdot g$$

und somit $l(D) = l(D')$.

Definition 3.3.29 Jeder Divisor $\text{Div}(\omega)$ für $0 \neq \omega \in \Omega_{\text{mer}}^1(X)$ heißt kanonischer Divisor und wird mit K bezeichnet.

Wir wissen, dass jedes $\omega' \in \Omega_{\text{mer}}^1(X)$ von der Form $g\omega$ mit einem $g \in \mathfrak{M}(X)$ ist. Daher gilt $\text{Div}(\omega') = \text{Div}(g) + \text{Div}(\omega)$.

Theorem 3.3.30 (Riemann-Roch) Sei X eine kompakte zusammenhängende Riemannsche Fläche. Für $D \in \text{Div}(X)$ gilt die Formel

$$l(D) - l(K - D) = \text{Grad}(D) - g(X) + 1.$$

Von diesem Satz geben wir hier keinen Beweis; er würde den Rahmen dieser Vorlesung sprengen.

Bemerkung 3.3.31 • Die Abbildung

$$\mathcal{L}(K + D) \rightarrow \Omega^1(D), \quad g \mapsto g\omega$$

für $\text{Div}(\omega) = K$ ist ein Isomorphismus. Dies folgt unmittelbar aus der Definition.

- Wir setzen $D = 0$ in der Riemann-Roch-Formel und erhalten:

$$\dim \Omega_{\text{hol}}^1(X) = l(K) = l(0) - 1 + g(X) = g(X),$$

da $l(0)$ gleich der Dimension des Vektorraumes der holomorphen Abbildungen $X \rightarrow \mathbb{C}$, der nur aus den konstanten Funktionen besteht. Somit haben wir die Definition von $g(X)$ zurückgefunden.

- Wir setzen $K = D$ in der Riemann-Roch-Formel und erhalten:

$$l(K) = l(0) + \text{Grad}(K) - g(X) + 1$$

und somit $\text{Grad}(K) = 2g(X) - 2$.

- Falls $\text{Grad}(D) > 2g(X) - 2$ ist, dann ist $l(K - D) = 0$ nach obiger Bemerkung und folglich ergibt sich

$$l(D) = \text{Grad}(D) - g(X) + 1.$$

Diese Formel ist ungeheuer wichtig, da sie rechts nur einfach auszuwertende Terme enthält. Es ist nämlich im Allgemeinen nicht leicht, $l(K - D)$ zu bestimmen. Diese Formel wird der Schlüssel für die Dimensionsformeln von Modulformen sein, wie wir im nächsten Satz sehen werden.

Satz 3.3.32 Sei $\Gamma \leq \text{SL}_2(\mathbb{Z})$ eine Kongruenzuntergruppe und sei $K = \text{Div}(\omega)$ ein kanonischer Divisor von X_Γ . Der Divisor E sei wie oben definiert. Dann haben wir Isomorphismen:

$$\begin{aligned} M_{2m}(\Gamma) &\cong \Omega^m([mE]) && \leftarrow && \mathcal{L}(mK + [mE]) \\ & && f(\omega^m) && \leftarrow && f \\ S_{2m}(\Gamma) &\cong \Omega^m([mE] - (\text{Spitzen}_\Gamma)) && \leftarrow && \mathcal{L}(mK + [mE] - (\text{Spitzen}_\Gamma)). \end{aligned}$$

Beweis. Der linke Isomorphismus ist der aus Korollar 3.3.15 und der rechte folgt aus obigen Bemerkungen. □

Damit ergeben sich $\dim M_{2m}(\Gamma) = l(mK + [mE])$ und $\dim S_{2m}(\Gamma) = l(mK + [mE] - (\text{Spitzen}_\Gamma))$. Wir wollen nun den Satz von Riemann-Roch benutzen, um diese Größen auszurechnen. Wir beginnen mit einem Lemma.

Lemma 3.3.33 Es gilt $\text{Grad}(K + E) > 0$.

Beweis. Zunächst gilt

$$\begin{aligned} \text{Grad}(K + E) &= \text{Grad}(K) + \text{Grad}(E) \\ &= 2g(X_\Gamma) - 2 + \sum_{P \in Y_\Gamma} \left(1 - \frac{1}{e_P}\right) + \nu_\infty \\ &= 2g(X_\Gamma) - 2 + \frac{1}{2}\nu_2 + \frac{2}{3}\nu_3 + \nu_\infty \end{aligned}$$

mit Notationen wie in Theorem 3.3.22. Aus dem Beweis dieses Theorems erhalten wir die Gleichung

$$2g(X_\Gamma) - 2 = -2\mu + \frac{1}{2}(\mu - \nu_2) + \frac{2}{3}(\mu - \nu_3) + (\mu - \nu_\infty).$$

Durch Einsetzen in die obere Gleichung ergibt sich $\text{Grad}(K + E) = \frac{\mu}{6} > 0$. □

Theorem 3.3.34 Sei $\Gamma \leq \text{SL}_2(\mathbb{Z})$ eine Kongruenzuntergruppe und $\nu_\infty = \#\text{Spitzen}_\Gamma$. Dann gelten die Formeln:

(a)

$$\dim S_{2m}(\Gamma) = \begin{cases} (2m-1)(g(X_\Gamma) - 1) + \sum_{P \in Y_\Gamma} [m(1 - \frac{1}{e_P})] + (m-1)\nu_\infty, & \text{falls } m > 1 \\ g(X_\Gamma), & \text{falls } m = 1 \\ 0, & \text{falls } m = 0 \\ 0, & \text{falls } m < 0. \end{cases}$$

(b)

$$\dim M_{2m}(\Gamma) = \begin{cases} \dim S_{2m}(\Gamma) + \nu_\infty, & \text{falls } m > 1 \\ \dim S_2(\Gamma) + \nu_\infty - 1, & \text{falls } m = 1 \\ 1, & \text{falls } m = 0 \\ 0, & \text{falls } m < 0. \end{cases}$$

Beweis. Wir gehen Fall für Fall durch.

Für $m < 0$ folgt sofort aus dem Lemma, dass $\text{Grad}([mE] + mK) < 0$ ist und somit $l([mE] + mK) = \dim M_{2m}(\Gamma) = 0$ gilt.

Die Modulformen von Gewicht 0 sind gerade gleich den holomorphen Funktionen auf X_Γ , also konstant. Diese Konstante muss für eine Spitzenform aber 0 sein, da die Funktion ja in den Spitzen verschwinden muss. Dies zeigt den Fall $m = 0$.

Im Fall $m = 1$ gilt $[mE] = [E] = (\text{Spitzen}_\Gamma)$ und folglich haben wir $\dim S_2(\Gamma) = g(X_\Gamma)$ und $\dim M_2(\Gamma) = l(K + (\text{Spitzen}_\Gamma))$. Nach Riemann-Roch gilt damit:

$$\dim M_2(\Gamma) = l(-(\text{Spitzen}_\Gamma)) - \text{Grad}(-(\text{Spitzen}_\Gamma)) + g(X_\Gamma) - 1 = g(X) + \nu_\infty - 1.$$

Nun sei $m > 1$. Zunächst halten wir fest, dass

$$\begin{aligned} & \text{Grad}([mE] + mK - (\text{Spitzen}_\Gamma)) \\ &= m(2g(X_\Gamma) - 2) + \sum_{P \in Y_\Gamma} [m(1 - \frac{1}{e_P})] + (m-1)\nu_\infty > 2g(X) - 2 \end{aligned}$$

ist. Folglich ist nach Riemann-Roch und der anschließenden Bemerkung

$$\dim S_{2m}(\Gamma) = l([mE] + mK - (\text{Spitzen}_\Gamma)) = \text{Grad}([mE] + mK - (\text{Spitzen}_\Gamma)) + 1 - g(X_\Gamma).$$

Einsetzen ergibt die gewünschte Formel. Für $\dim M_{2m}(\Gamma)$ geht man wörtlich genauso vor, außer, dass der Term (Spitzen_Γ) an den entsprechenden Stellen gestrichen werden muss. \square

Beispiel 3.3.35 • $\dim M_2(\Gamma_0(4)) = 0 + 3 - 1 = 2$

• $\dim S_4(\Gamma_0(4)) = (4-1)(0-1) + (2-1)3 = 0$

• $\dim M_4(\Gamma_0(4)) = 3$

- $\dim S_2(\Gamma_0(11)) = 1$
- $\dim S_4(\Gamma_0(11)) = 2$

Aufgabe 3.3.36 Berechne $\dim S_2(\Gamma_0(35))$, $\dim S_{12}(\Gamma_0(35))$, $\dim M_{18}(\Gamma_0(35))$ und $S_{10}(\Gamma_0(2))$.

Beweis der Riemann-Hurwitz-Formel (Theorem 3.3.21). Es sei $0 \neq \omega \in \Omega_{\text{mer}}^1(X)$. Dann haben wir $\text{Grad}(\omega) = 2g(X) - 2$ und $\text{Grad}(\pi^*\omega) = 2g(Y) - 2$ nach Riemann-Roch. Wir können mittels π^* auch Divisoren zurückziehen: Sei $D = \sum_{P \in X} n_P P$; dann setze $\pi^*D = \sum_{P \in X} \sum_{Q \in \pi^{-1}(P)} e_Q Q$. Dann ist insbesondere $\text{Grad}(\pi^*D) = \text{Grad}(\pi)\text{Grad}(D)$. Mit dieser Definition folgt aus Lemma 3.3.9

$$\text{Div}(\pi^*\omega) = \pi^*(\text{Div}(\omega)) + \sum_{y \in Y} (e_y - 1).$$

Nun genügt es, den Grad auf beiden Seiten dieser Formel zu nehmen. \square

Wir haben an dieser Stelle den Beweis von Theorem 1.0.25 aus der Einleitung abgeschlossen, denn es fehlten nur noch die Dimensionsformeln. Dabei müssen wir allerdings eingestehen, dass der Beweis den Satz von Riemann-Roch benutzt, den wir nicht bewiesen haben. Über einige Details der Riemannschen Flächen sind wir auch etwas schnell hinweg gegangen. Ansonsten wurde alles bewiesen. Mit eigentlich jedem Buch zu Riemannschen Flächen kann nun der Leser den Beweis für sich selbst komplettieren.

Als Nächstes kommen wir zur sogenannten Sturm-Schranke (nach Jacob Sturm), die uns ein Kriterium liefert, wann zwei Modulformen identisch sind.

Satz 3.3.37 Sei $\Gamma \leq \text{SL}_2(\mathbb{Z})$ eine Kongruenzuntergruppe und seien $f, g \in M_{2m}(\Gamma)$. Ferner sei x eine Spitze. Falls

$$\text{Ord}_x(f - g) > m(2(g(X_\Gamma)) - 2) + m \sum_{P \in Y_\Gamma} \left(1 - \frac{1}{e_P}\right) + m \# \text{Spitzen}_\Gamma,$$

dann ist $f = g$.

Beweis. Wir nehmen $f \neq g$ an. Wir haben gesehen, dass $\text{Div}(f - g) = \text{Div}(\omega) + mE$ mit dem zu $f - g$ gehörigen $\omega \in \Omega_{\text{mer}}^m(X_\Gamma)$. Für den Grad erhalten wir

$$\text{Grad}(\text{Div}(f - g)) = m(2(g(X_\Gamma)) - 2) + m \sum_{P \in Y_\Gamma} \left(1 - \frac{1}{e_P}\right) + m \# \text{Spitzen}_\Gamma.$$

Da aber $\text{Div}(f - g)$ ein effektiver Divisor ist (d.h. alle Koeffizienten sind größer gleich 0), ergibt die Voraussetzung an $\text{Ord}_x(f - g)$ sofort einen Widerspruch und $f = g$ folgt. \square

Mit unserer mittlerweile gesammelten Erfahrung ist es ein Leichtes, die Formel in expliziteren Termen auszudrücken, zum Beispiel unter Verwendung von ν_2, ν_3 etc. und sie zum Beispiel für $\Gamma(N)$ zu spezialisieren.

3.4 Hecke-Theorie

3.4.1 Modulkorrespondenzen

Definition 3.4.1 Seien $N, n \in \mathbb{N}$ mit $(n, N) = 1$. Wir definieren

$$\begin{aligned}\Delta_0^n(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N}, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = n \right\}, \\ \Delta_1^n(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \pmod{N}, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = n \right\}, \\ \Delta_0(N) &= \bigcup_{n \in \mathbb{N} \text{ mit } (n, N) = 1} \Delta_0^n(N), \\ \Delta_1(N) &= \bigcup_{n \in \mathbb{N} \text{ mit } (n, N) = 1} \Delta_1^n(N).\end{aligned}$$

Im Folgenden sei stets $(\Delta, \Gamma) = (\Delta_1(N), \Gamma_1(N))$ oder $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$, es sei denn, wir sagen explizit etwas anderes.

Lemma 3.4.2 Sei $\alpha \in \Delta$. Wir setzen

$$\Gamma_\alpha = \Gamma \cap \alpha^{-1}\Gamma\alpha \text{ und } \Gamma^\alpha = \Gamma \cap \alpha\Gamma\alpha^{-1}.$$

Dann hat Γ_α endlichen Index in Γ und $\alpha^{-1}\Gamma\alpha$ (dazu sagt man auch, dass Γ und $\alpha^{-1}\Gamma\alpha$ kommensurabel sind) ebenso hat Γ^α endlichen Index in Γ und $\alpha\Gamma\alpha^{-1}$ (also Γ und $\alpha\Gamma\alpha^{-1}$ sind kommensurabel).

Beweis. Sei $n = \det \alpha$. Man rechnet mit Matrizen nach, dass

$$\alpha^{-1}\Gamma(Nn)\alpha \subset \Gamma(N).$$

Daher ist

$$\Gamma(Nn) \subset \alpha^{-1}\Gamma(N)\alpha \subset \alpha^{-1}\Gamma\alpha.$$

Damit ist $\Gamma(Nn) \subset \Gamma_\alpha$ und die erste Behauptung folgt. Ganz ähnlich geht man für die zweite vor. \square

Beispiel 3.4.3 Sei $\Gamma = \Gamma_0(N)$ und p sei eine Primzahl. Der wichtigste Fall für das Folgende ist $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$. Eine elementare Rechnung zeigt:

$$\Gamma^\alpha = \Gamma_0(Np).$$

Definition 3.4.4 Sei $\alpha \in \Delta$. Wir betrachten das Diagramm

$$\begin{array}{ccc} \Gamma_\alpha \backslash \mathbb{H} & \xrightarrow[\sim]{\tau \mapsto \alpha\tau} & \Gamma^\alpha \backslash \mathbb{H} \\ \downarrow \pi_\alpha & & \downarrow \pi_\alpha \\ \Gamma \backslash \mathbb{H} & & \Gamma \backslash \mathbb{H}, \end{array}$$

in dem π^α und π_α die natürlichen Projektionen sind. Man überprüft, dass dies wohl-definiert ist unter Verwendung von $\alpha\Gamma_\alpha\alpha^{-1} = \Gamma^\alpha$.

Die Modulkorrespondenz bzw. Hecke-Korrespondenz τ_α ist definiert als

$$\tau_\alpha : \text{Div}(Y_\Gamma) \xrightarrow{\pi_\alpha^*} \text{Div}(Y_{\Gamma_\alpha}) \xrightarrow{\alpha_*} \text{Div}(Y_{\Gamma^\alpha}) \xrightarrow{\pi_\alpha^*} \text{Div}(Y_\Gamma).$$

Dabei ist π^* das Zurückziehen von Divisoren, das wir schon eher gesehen haben, und α und π_α^* sind die Abbildungen, die sich durch Anwendung von α bzw. π^α auf die Punkte des Divisors ergeben.

Diese Modulkorrespondenzen werden wir sofort noch expliziter beschreiben. Zunächst ein Lemma. [Erinnerung an Doppelnebenklassen.]

Lemma 3.4.5 Seien $\alpha_i \in \Gamma$ für $i \in I$ für irgendeine Indexmenge I . Dann gilt

$$\Gamma = \bigsqcup_{i \in I} \Gamma_\alpha \alpha_i \Leftrightarrow \Gamma \alpha \Gamma = \bigsqcup_{i \in I} \Gamma \alpha \alpha_i.$$

Beweis. Siehe Vorlesung. Es ist eine einfache Rechnung. \square

Korollar 3.4.6 Sei $\alpha \in \Delta$. Ferner sei $\Gamma \alpha \Gamma = \bigsqcup_{i \in I} \Gamma \alpha \alpha_i$. Dann ist die Hecke-Korrespondenz $\tau_\alpha : \text{Div}(Y_\Gamma) \rightarrow \text{Div}(Y_\Gamma)$ durch $\tau \mapsto \sum_{i \in I} \alpha \alpha_i \tau$ auf Repräsentanten $\tau \in \mathbb{H}$ gegeben.

Beweis. Dazu genügt es, die Definition unter Zuhilfenahme des Lemmas zu überprüfen. \square

Bemerkung 3.4.7 Es gilt $\Delta^n = \bigcup_{\alpha \in \Delta, \det \alpha = n} \Gamma \alpha \Gamma$ und man kann endlich viele α_i für $i \in I$ auswählen, so dass $\Delta^n = \bigsqcup_{i \in I} \Gamma \alpha_i \Gamma$.

Definition 3.4.8 Es sei $\Delta^n = \bigsqcup_{i \in I} \Gamma \alpha_i \Gamma$. Der Hecke-Operator T_n auf $\text{Div}(Y_\Gamma)$ ist definiert als

$$T_n = \sum_{i \in I} \tau_{\alpha_i}.$$

Lemma 3.4.9 Für $(a, N) = 1$ gibt es eine Matrix $\sigma_a \in \Gamma_0(N)$ mit $\sigma_a \equiv \begin{pmatrix} a^{-1} & 0 \\ 0 & a \end{pmatrix} \pmod{N}$.

Beweis. Aus $(a, N) = 1$ folgt die Existenz von r, s mit $1 = ar - Ns$. Also ist die Matrix $\begin{pmatrix} r & s \\ N & a \end{pmatrix} \in \Gamma_0(N)$ und weiter gilt $\begin{pmatrix} r & s \\ N & a \end{pmatrix} \equiv \begin{pmatrix} a^{-1} & s \\ 0 & a \end{pmatrix} \pmod{N}$. Jetzt brauchen wir nur noch die rechte obere Ecke auszuräumen, um die gewünschte Matrix zu finden. Wir setzen $\sigma_a = \begin{pmatrix} r & s \\ N & a \end{pmatrix} \begin{pmatrix} 1 & -as \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$. Eine kurze Matrizenrechnung zeigt, dass σ_a die Anforderungen erfüllt. \square

[03.07.2007]

Satz 3.4.10 (a) Wir haben die Zerlegung

$$\Delta_0^n(N) = \bigsqcup_a \bigsqcup_b \Gamma_0(N) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

wobei a die positiven Zahlen durchläuft mit $a \mid n$ und $(a, N) = 1$ und b die ganzen Zahlen mit $0 \leq b < d =: n/a$.

(b) Für $(a, N) = 1$ wählen wir eine Matrix σ_a wie im Lemma. Dann haben wir die Zerlegung

$$\Delta_1^n(N) = \bigsqcup_a \bigsqcup_b \Gamma_1(N) \sigma_a \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

mit a, b, d wie in (a).

Beweis. Siehe Vorlesung. Auch dieser Beweis ist elementar. \square

Als Nächstes geben wir eine Interpretation des Hecke-Operators T_p in der Modulinterpretation der Modulkurve $Y_{\Gamma_0(N)}$.

Satz 3.4.11 Auf $Y_{\Gamma_0(N)}$ ist T_p mit einer Primzahl p gegeben durch

$$T_p : \tau \mapsto \begin{cases} \sum_{b=0}^{p-1} \frac{\tau+b}{p} + p\tau, & \text{falls } p \nmid N, \\ \sum_{b=0}^{p-1} \frac{\tau+b}{p}, & \text{falls } p \mid N. \end{cases}$$

Unter den Identifikationen

$$\Gamma_0(N) \backslash \mathbb{H} \rightarrow \{(E, C)\} / \cong, \quad \tau \mapsto (\mathbb{C}/\Lambda_\tau, \langle \frac{1}{N} \rangle)$$

und $\text{Div}(Y_{\Gamma_0(N)}) \cong \text{Div}(\{(E, C)\} / \cong)$ ergibt sich

$$T_p : (E, C) \mapsto \sum_{(E', C')} (E', C'),$$

wobei die Summe über alle p -Isogenien $E \rightarrow E'$ läuft und C' jeweils das Bild von C ist.

Beweis. Die erste Aussage folgt aus dem Satz. Für die zweite braucht man sich nur klar zu machen, wie die p -Isogenien für die elliptische Kurve \mathbb{C}/Λ_τ aussehen. Dies haben wir in der Vorlesung getan. Es ist eine leichte Rechnung. \square

Im nächsten Schritt wenden wir uns der abstrakten Hecke-Algebra als Doppelnebenklassenalgebra zu.

Definition 3.4.12 Der Hecke-Ring $R(\Delta, \Gamma)$ ist die freie abelsche Gruppe auf den Doppelnebenklassen $\Gamma\alpha\Gamma$ für $\alpha \in \Delta$.

Unser nächstes Ziel ist, eine Multiplikation zu definieren, die die Bezeichnung "Ring" dann auch rechtfertigt.

Zunächst seien $\Gamma\alpha\Gamma = \bigsqcup_{i=1}^n \Gamma\alpha_i$ und $\Gamma\beta\Gamma = \bigsqcup_{j=1}^m \Gamma\beta_j$. Wir rechnen einfach drauflos.

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \bigcup_j \Gamma\alpha\Gamma\beta_j = \bigcup_{i,j} \Gamma\alpha_i\beta_j.$$

Diese Vereinigung ist nicht notwendig disjunkt. Die linke Seite kann aber als disjunkte Vereinigung von Doppelnebenklassen $\bigsqcup_{k=1}^r \Gamma\gamma_k\Gamma$ geschrieben werden. Jede dieser Doppelnebenklassen ist aber auch wieder von der Form

$$\Gamma\gamma_k\Gamma = \bigsqcup_{l=1}^{n_k} \Gamma\gamma_{k,l}.$$

Hiermit erhalten wir insgesamt

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \bigcup_{i,j} \Gamma\alpha_i\beta_j = \bigsqcup_k \bigsqcup_l \Gamma\gamma_{k,l}.$$

Wir wollen nun eine Bezeichnung für die Vielfachheit einführen, mit der jede Nebenklasse rechts in der Mitte vorkommt. Dazu sei k fest und wir definieren für jedes l

$$m_{k,l} = \#\{(i,j) \mid \Gamma\gamma_{k,l} = \Gamma\alpha_i\beta_j\}.$$

Der wichtige Punkt ist nun das folgende Lemma.

Lemma 3.4.13 *Die Zahl $m_{k,l}$ ist unabhängig von l . Deshalb setzen wir $m_k := m_{k,l}$.*

Beweis. Siehe Vorlesung. Der Beweis ist kombinatorisch und recht direkt. □

Zusammengefasst erhalten wir nun mittels des Lemma, dass in

$$\bigcup_{i,j} \Gamma\alpha_i\beta_j = \Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \bigsqcup_k \Gamma\gamma_k\Gamma = \bigsqcup_k \bigsqcup_l \Gamma\gamma_{k,l}$$

die Nebenklasse $\Gamma\gamma_{k,l}$ links genau m_k mal vorkommt.

Definition 3.4.14 *Wir definieren eine Multiplikation auf $R(\Delta, \Gamma)$ durch*

$$\Gamma\alpha\Gamma \cdot \Gamma\beta\Gamma = \sum_{k=1}^n m_k \Gamma\gamma_k\Gamma,$$

wobei wir die vorausgehende Notation benutzen.

Man überprüft, dass $R(\Delta, \Gamma)$ tatsächlich ein Ring ist (Assoziativität und Distributivität). Die gerade gemachte Definition ist sinnvoll, denn sie ergibt für Hecke-Korrespondenzen:

$$\tau_\alpha \circ \tau_\beta = \sum_{k=1}^n m_k \tau_{\gamma_k}.$$

Definition 3.4.15 *Wir machen (wie oben) die Definition $T_n = \sum_\alpha \tau_\alpha \in R(\Delta, \Gamma)$, wobei die Summe über eine Menge von α s läuft mit $\Delta^n = \bigsqcup_\alpha \Gamma\alpha\Gamma$.*

Für $a \mid d$ und $(d, N) = 1$ setzen wir

$$T(a, d) = \Gamma\sigma_a \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \Gamma \in R(\Delta, \Gamma).$$

Aufgabe 3.4.16 *Zeige die Formel*

$$T_m T_n = \sum_{d \mid (m,n), (d,N)=1} d T(d, d) T_{\frac{mn}{d^2}}.$$

Zeige weiterhin, dass $R(\Delta, \Gamma)$ von den T_p und $T(p, p)$ für alle Primzahlen p erzeugt wird.

Hieraus ergibt sich unmittelbar das wichtige Korollar.

Korollar 3.4.17 *Es gilt $T_m T_n = T_n T_m$ und somit ist $R(\Delta, \Gamma)$ ein kommutativer Ring.* □

3.4.2 Hecke-Operatoren auf Modulformen

Im Folgenden sei stets $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$. Alles funktioniert aber auch für $(\Delta_0(N), \Gamma_0(N))$ mit kleinen Änderungen; z. B. muss man mit Modulformen mit Nebentyp (Dirichlet-Charakter) arbeiten.

Wir definieren nun eine Operation des Hecke-Ringes $R(\Delta, \Gamma)$ auf Modulformen.

Definition 3.4.18 Sei $\Gamma \alpha \Gamma = \bigsqcup_{i=1}^n \Gamma \alpha_i$ und sei $f \in M_k(\Gamma)$. Wir setzen:

$$f \cdot \tau_\alpha := \sum_{i=1}^n f|_k(\alpha_i).$$

Lemma 3.4.19 Es ist $f \cdot \tau_\alpha$ wiederum ein Element aus $M_k(\Gamma)$.

Beweis. Für $\gamma \in \Gamma$ rechnen wir die Transformationsregel nach:

$$\sum_i f|_k(\alpha_i)|_k(\gamma) = \sum_i f|_k(\alpha_i \gamma) = \sum_i f|_k(\alpha_i),$$

da die Nebenklassen $\Gamma(\alpha_i \gamma)$ eine Permutation der Nebenklassen $\Gamma \alpha_i$ sind.

Die Holomorphie von $f \cdot \tau$ ist klar und die Holomorphie in den Spitzen folgt so wie (irgendwo) vorne. \square

Somit erhalten wir also die gewünschte Operation von $R(\Delta, \Gamma)$ auf $M_k(\Gamma)$.

Satz 3.4.20 Sei $f \in M_k(\Gamma)$. Dann gelten die Formeln:

$$(a) (f \cdot T_m)(\tau) = \frac{1}{m} \sum_{a|m, (a, N)=1} \sum_{b=0}^{\frac{m}{a}-1} a^k f\left(\frac{a\tau+b}{m/a}\right),$$

$$(b) a_n(f \cdot T_m) = \sum_{a|(m, n), (a, N)=1} a^{k-1} a \frac{m}{a^2}.$$

Beweis. (a) folgt sofort aus Satz 3.4.10.

(b) ist eine einfache Rechnung, für die man

$$\sum_{b=0}^{d-1} e^{2\pi i \frac{b}{d} n} = \begin{cases} 0, & \text{falls } d \nmid n \\ d, & \text{falls } d \mid n \end{cases}$$

benutzt.

Für Details siehe die Vorlesung. \square

Für unsere Betrachtungen zur Hecke-Algebra ist die folgende unscheinbare Formel sehr wichtig, die sofort aus dem Satz folgt.

Korollar 3.4.21 Es gilt $a_1(f \cdot T_n) = a_n(f)$ für alle $n \in \mathbb{N}$. \square

Aufgabe 3.4.22 Der Hecke-Ring $R(\Delta, \Gamma)$ operiert auch auf $S_k(\Gamma)$ und $A_k(\Gamma)$.

Korollar 3.4.23 Für die Operation der Hecke-Operatoren auf $M_k(\Gamma)$, $S_k(\Gamma)$ und $A_k(\Gamma)$ gelten die Formeln:

- (a) $T_n T_m = T_{nm}$ für $(n, m) = 1$,
 (b) $T_{p^{r+1}} = T_p T_{p^r} - p^{k-1} T_{p^{r-1}}$, falls $p \nmid N$, und
 (c) $T_{p^{r+1}} = T_p T_{p^r}$, falls $p \mid N$.

Dabei bezeichnet p jeweils eine Primzahl.

Beweis. Diese folgen aus Aufgabe 3.4.16 und der Definition der Operation. \square

Die Formeln aus dem Korollar lassen sich auf elegante Weise ausdrücken.

Satz 3.4.24 (Euler-Produkt) Für die Operation der Hecke-Operatoren T_n auf Modulformen gilt die formale Identität:

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p \nmid N} (1 - T_p p^{-s} + p^{k-1-2s})^{-1} \cdot \prod_{p \mid N} (1 - T_p p^{-s})^{-1}.$$

Dass die Identität formal ist, bedeutet, dass wir Reihen und Produkte beliebig umordnen und uns keine Gedanken um Konvergenz machen.

Beweis. Der Beweis erfolgt in drei Schritten.

1. Schritt: Sei $g : \mathbb{Z} \rightarrow \mathbb{C}$ irgendeine Funktion. Dann gilt die formale Identität:

$$\prod_{p \text{ Primzahl}} \sum_{r=0}^{\infty} g(p^r) = \sum_{n=1}^{\infty} \prod_{p^r \parallel n} g(p^r).$$

Zum Beweis sei zunächst S eine endliche Primzahlmenge. Dann gilt die formale Identität:

$$\prod_{p \in S} \sum_{r=0}^{\infty} g(p^r) = \sum_{n=1, n \text{ hat nur Primfaktoren in } S}^{\infty} \prod_{p^r \parallel n} g(p^r),$$

wie man durch Ausmultiplizieren der linken Seite sieht (dabei ordnet man um!). Wir schließen den 1. Schritt ab, indem wir S immer größer werden lassen.

2. Schritt: Für $p \nmid N$ gilt

$$\left(\sum_{r=0}^{\infty} T_{p^r} p^{-rs} \right) (1 - T_p p^{-s} + p^{k-1-2s}) = 1$$

und für $p \mid N$ gilt

$$\left(\sum_{r=0}^{\infty} T_{p^r} p^{-rs} \right) (1 - T_p p^{-s}) = 1.$$

Der Beweis des 2. Schrittes besteht daraus, die Ausdrücke zu multiplizieren und das ‘‘Teleskop’’ zu finden. Für Details siehe Vorlesung.

3. Schritt: Der Satz folgt nun sofort daraus, dass man den 1. Schritt mit $g(p^r) = T_{p^r} p^{-rs}$ benutzt und die Formeln aus dem 2. Schritt einsetzt. \square

3.4.3 Hecke-Algebren und -Eigenformen

In diesem Abschnitt sei weiterhin $(\Delta, \Gamma) = (\Delta_0(N), \Gamma_0(N))$ und auch hier gilt alles in sehr ähnlicher Form auch für $(\Delta_1(N), \Gamma_1(N))$.

Wir erinnern zunächst an einen Satz aus der linearen Algebra.

Satz 3.4.25 *Sei K ein algebraisch abgeschlossener Körper und \mathbb{T} eine endlich-dimensionale kommutative K -Algebra. Weiter sei $V \neq (0)$ ein endlich-dimensionaler K -Vektorraum und $\mathbb{T} \rightarrow \text{End}(V)$ ein K -Vektorraum-Homomorphismus. Dann gibt es einen simultanen Eigenvektor $0 \neq v \in V$ für alle $T \in \mathbb{T}$.*

Beweis. Wegen der Endlichdimensionalität gibt es ein endliches Erzeugendensystem T_1, \dots, T_r von \mathbb{T} . Wir wissen, dass T_1 (damit meinen wir jetzt immer das Bild in den Endomorphismen von V) einen nicht-trivialen Eigenraum V_1 (zu irgendeinem Eigenwert λ_1) besitzt (zum Beispiel mittels der Jordanschen Normalform). Der wichtige Schritt ist nun, einzusehen, dass $T_i V_1 \subseteq V_1$ ist. Wegen $T_1 v = \lambda_1 v$ für alle $v \in V_1$ und der Kommutativität der Algebra folgt $T_1 T_i v = T_i T_1 v = T_i \lambda_1 v = \lambda_1 T_i v$ für $v \in V_1$. Also ist mit v auch $T_i v \in V_1$.

Nun wissen wir genauso wie gerade, dass V_1 einen Eigenraum $V_2 \neq (0)$ zu T_2 (mit irgendeinem Eigenwert λ_2) enthält. Genauso wie gerade sieht man, dass $T_i V_2 \subseteq V_2$. So macht man weiter und erhält schließlich $V_r \neq (0)$, der Eigenraum für alle T_i ist. Somit ist er auch Eigenraum für die gesamte Algebra \mathbb{T} . \square

Definition 3.4.26 *Eine Modulform $f \in M_k(\Gamma)$ heißt Hecke-Eigenform, falls f Eigenvektor für alle T_n mit $n \in \mathbb{N}$ ist. Sie heißt normiert, falls $a_1(f) = 1$ ist.*

Definition 3.4.27 *Wir definieren die Hecke-Algebra $\mathbb{T}(M_k(\Gamma))$ als das Bild des \mathbb{C} -Algebra-Homomorphismus*

$$R(\Delta, \Gamma) \rightarrow \text{End}_{\mathbb{C}}(M_k(\Gamma)).$$

Bemerkung 3.4.28 *Die Hecke-Algebra $\mathbb{T}(M_k(\Gamma))$ ist endlich-dimensional. Sie wird, wie man an Aufgabe 3.4.16 sieht, von den Hecke-Operatoren T_p mit allen Primzahlen p erzeugt, denn $T(p, p)$ operiert als p^{k-2} . Im Falle von $\Gamma_1(N)$ darf man übrigens die Diamanten-Operatoren nicht vergessen, oder man muss alle T_n nehmen. \square*

Es ergibt sich unmittelbar folgende Folgerung.

Korollar 3.4.29 *In $M_k(\Gamma)$ gibt es eine nicht-triviale Eigenform, vorausgesetzt, dass $M_k(\Gamma) \neq (0)$ ist. \square*

Notation 3.4.30 *Anstatt $f.T$ mit einem Hecke-Operator T und einer Modulform f schreiben wir meistens $T.f$ oder Tf .*

Satz 3.4.31 Die Paarung

$$M_k(\Gamma) \times \mathbb{T}(M_k(\Gamma)) \rightarrow \mathbb{C}, \quad (f, T) \mapsto a_1(Tf)$$

ist bilinear und nicht-ausgeartet.

Beweis. Die Bilinearität ist klar.

Sei nun $a_1(T_n f) = a_n(f) = 0$ für alle $n \in \mathbb{N}$. Es folgt sofort $f = 0$.

Sei weiter $a_1(Tf) = 0$ für alle $f \in M_k(\Gamma)$. Dann haben wir insbesondere

$$a_1(TT_n f) = a_1(T_n T f) = a_n(Tf) = 0$$

für alle $n \in \mathbb{N}$ und alle f . Es ist also $Tf = 0$ für alle f . Daraus folgt $T = 0$. Somit ist die Nicht-Ausgeartetheit bewiesen. \square

Korollar 3.4.32 (a) Die Abbildung

$$M_k(\Gamma) \longrightarrow \text{Hom}_{\mathbb{C}\text{-VR}}(\mathbb{T}(M_k(\Gamma)), \mathbb{C}), \quad f \mapsto (T \mapsto a_1(Tf))$$

definiert einen Isomorphismus von $\mathbb{T}(M_k(\Gamma))$ -Moduln.

(b) Sei $f \in M_k(\Gamma)$ eine normierte Hecke-Eigenform. Dann gilt

$$T_n f = a_n(f) f,$$

der n -te Koeffizient ist also der n -te Eigenwert.

(c) Die Abbildung

$$\{\text{Norm. Eigenformen in } M_k(\Gamma)\} \longrightarrow \text{Hom}_{\mathbb{C}\text{-Algebra}}(\mathbb{T}(M_k(\Gamma)), \mathbb{C}), \quad f \mapsto (T \mapsto a_1(Tf))$$

ist eine Bijektion.

Beweis. (a) ist eine allgemeine Konsequenz für nicht-ausgeartete bilineare Paarungen.

(b) und (c) rechnet man sehr einfach nach. Siehe Vorlesung für Details. \square

Wir beschließen diese Vorlesung mit einigen Beispielen, die historisch die Entwicklung der hier vorgestellten Theorie erst ausgelöst haben.

Beispiel 3.4.33 • Die Eisenstein-Reihen G_4 und G_6 sind Hecke-Eigenformen, da die Vektorräume $M_4(\text{SL}_2(\mathbb{Z}))$ und $M_6(\text{SL}_2(\mathbb{Z}))$ ein-dimensional sind. Übrigens sind alle G_k Hecke-Eigenformen.

• Die normierte Diskriminanten-Funktion $\Delta = \sum_{n=1}^{\infty} \tau(n) q^n \in S_{12}(\text{SL}_2(\mathbb{Z}))$ ist eine normierte Hecke-Eigenform, da sie in einem ein-dimensionalen Raum von Spitzenformen lebt. Es gilt also $T_n \Delta = \tau(n) \Delta$ und folglich gelten die Formeln in Korollar 3.4.23 auch mit $\tau(n)$ anstatt T_n .

Wir wenden jetzt das Euler-Produkt in Satz 3.4.24 auf Δ an. Man kann nun überprüfen, dass die Koeffizienten $\tau(n)$ schnell genug abfallen (das ist für jede Spitzenform der Fall), so dass die Reihen und Produkte jeweils absolut konvergieren. Daher erhalten wir die “echte” Gleichheit:

$$\sum_{n=1}^{\infty} \tau(n)n^{-s} = \prod_{p \nmid N} (1 - \tau(p)p^{-s} + p^{11-2s})^{-1} \cdot \prod_{p|N} (1 - \tau(p)p^{-s})^{-1}.$$

Anhang A

Notationen, Sätze, Lösungen

1.1 Notationen

[Hier sollte viel mehr stehen.]

- $U_\epsilon(z) = \{z' \in \mathbb{C} \mid |z - z'| < \epsilon\}$
- $U_\epsilon(z)^\bullet = \{z' \in \mathbb{C} \mid 0 < |z - z'| < \epsilon\} = U_\epsilon(z) - \{z\}$

1.2 Sätze aus Funktionen-Theorie und Topologie

[Hier sollte auch viel mehr stehen.]

- Eine Teilmenge des \mathbb{R}^n ist genau dann kompakt, wenn sie beschränkt und abgeschlossen ist (Heine-Borel).
- Eine nicht-konstante holomorphe Funktion ist offen.
- Jede Potenzreihe $\sum_{n=0}^{\infty} a_n z^n$ mit $a_n \in \mathbb{C}$ besitzt einen Konvergenzradius $r \geq 0$. Innerhalb des Konvergenzradius ist die Reihe lokal gleichmäßig absolut konvergent, außerhalb ist sie divergent. Innerhalb des Konvergenzradius darf man Differentiation und Summation vertauschen.
- Sei $a \in \mathbb{C}$. Sei $f : U_\epsilon(a)^\bullet \rightarrow \mathbb{C}$ eine holomorphe Funktion. Dann lässt sich f in eine Laurent-Reihe

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z - a)^n$$

entwickeln, die auf $U_\epsilon(a)^\bullet$ lokal gleichmäßig absolut konvergiert. Dabei gilt

$$a_n = \frac{1}{2\pi i} \int_{|z-a|=r} \frac{f(z)}{(z-a)^{n+1}} dz$$

für jedes $r < \epsilon$.

1.3 Lösungen

Hier sind Lösungsskizzen von ein paar Aufgaben.

- Lösung von Aufgabe 2.1.8.

Sei $X = \mathbb{Z} \cup \{\infty\}$. Die Topologie ist zunächst: $\mathcal{O}_X = \{X, \emptyset\} \cup \mathbb{P}(\mathbb{Z})$. Damit ist $\mathbb{Z} \in X$ diskret. Die einzige offene Menge, die ∞ enthält, ist X . Damit ist X kompakt. Denn jede Überdeckung von X muss ja dann X enthalten und hat die triviale endliche Überdeckung X . Nun ist $X \cap \mathbb{Z} = \mathbb{Z}$, welches diskret, aber nicht endlich ist.

Die Verfeinerung, die X Hausdorffsch sein lässt, ist, als offene Mengen wieder die Potenzmengen von \mathbb{Z} zu nehmen und nun noch X ohne beliebige endliche Teilmengen von \mathbb{Z} zuzulassen. Dann ist X wieder kompakt, aber \mathbb{Z} ist noch stets diskret. Darüber hinaus ist X Hausdorffsch, da wir je zwei Punkte durch offene Mengen trennen können. Eigentlich müssen wir ja nur ∞ von n trennen. Das geht dann ja durch $\{n\}$ und $X - \{n\}$.

- Lösung von Aufgabe 3.1.9.

Die Rechnung ersparen wir uns. Es gilt, dass der Radius des Horokreises gleich $\frac{1}{2c^2y}$ ist. Somit ist der Mittelpunkt gleich

$$\frac{a}{c} + i \frac{1}{2c^2y}.$$

Nun ist

$$\left| \frac{a(x+iy)+b}{c(x+iy)+d} - \left(\frac{a}{c} + i \frac{1}{2c^2y} \right) \right|^2 = \dots = \frac{1}{|2c^2y|^2}.$$

Ziehe für die Rechnung einfach $\frac{1}{|c(x+iy)+d|^2 \cdot |2c^2y|^2}$ heraus und multipliziere den Zähler aus. Mit anderen Worten wird die Parallele zur x -Achse auf Höhe y unter der Transformation zu dem Horokreis mit dem angegebenen Radius und Mittelpunkt. Daraus folgert man sofort die Aufgabe.

Literaturverzeichnis

- [DS] Diamond, Fred; Shurman, Jerry: *A first course in modular forms*. Graduate Text in Mathematics, 228. Springer-Verlag, 2005.
- [FB] Freitag, E., Busam, R. *Funktionentheorie*. Springer-Verlag, 1993. Mittlerweile gibt es mehrere korrigierte Neuauflagen mit veränderten Seitenzahlen.
- [Gu] Gunning, R. C.: *Lectures on Modular Forms*. Princeton University Press, 1962.
- [M] Milne, James: *Modular functions and modular forms*. <http://www.jmilne.org/math/index.html>
- [Silv] Silverman, Joseph H. *The arithmetic of elliptic curves*. Graduate Text in Mathematics, 106. Springer-Verlag, 1992.