J. Gamst 01.04.14

Vorlesung im SS 2014
Elliptische Kurven über $\mathbb{C}$: Klassische Theorie

V: Mo 10-12 , Do 10-12 in MZH 6340
Ü: Mi 12-14 in MZH 6340

Elliptische Kurven trugen ihren Namen, weil bei der Berechnung der Bogenlänge von Ellipsen Integrale der Form

$$\int \frac{dx}{\sqrt{(x-e_1)(x-e_{2)}(x-e_3)}}$$

auftreten; deren Umkehrfunktionen stellen sich als doppelt periodische meromorphe Funktionen heraus, welche der Differentialgleichung

$$(y')^2 = (y-e_1)(y-e_2)(y-e_3)$$

genügen und so eine Parametrisierung $(y(z), y'(z))$ der komplexen Punkte der dann elliptisch genannten Kurve (E) $y^2 = (x-e_1)(x-e_{2)}(x-e_3)$ liefern. Eine fundamentale Eigenschaft dieser Kurven ist es, dass man ein algebraisches Additionsgesetz für (E) hat, so dass die Punkte mit Koordinaten in einem Körper K eine abelsche Gruppe E(K) bilden. Diese Gruppen spielen eine Rolle in vielen Zusammenhängen - von der Zahlentheorie und dem Beweis des Satzes von Fermat durch Wiles bis zu diversen Anwendungen in der Kryptologie.

Im Kurs will ich die klassische Theorie behandeln, die bereits im 19. Jahrhundert entwickelt worden ist. Dabei geht es zunächst um die Weierstraßsche $\wp$-Funktion, welche auf $\mathbb{C}$ meromorph ist und ein Periodengitter L hat:

$$\wp(z+\omega) = \wp(z) \text{ für } \omega \in L$$

$(L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ mit reell unabhängigen $\omega_1, \omega_2 \in \mathbb{C})$
und die den Körper der L-periodischen meromorphischen Funktionen, d.h. der Funktionenkörper der elliptischen Kurve $\mathbb{C}$/L, erzeugt.
Gitter $L \subset \mathbb{C}$ lassen sich durch einen Punkt τ in der Halbebene H repräsentieren:

$$L = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \tau,$$

und die elliptischen Kurven über $\mathbb{C}$ entsprechen dann dem Quotienten von H nach der Operation der Modulgruppe $\Gamma = Sl_2(\mathbb{Z})$ durch gebrochen lineare Tranformationen

$\gamma_M(z) = \frac{az+b}{cz+d}$ für $M = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in Sl_2(\mathbb{Z})$.

Modulfunktionen sind nun meromorphe Funktionen auf H, welche invariant unter Γ sind, allgemein hat man Modulformen f zu betrachten, welche einem Transformationsgesetz

$$f(\gamma_M(z) = (cz+d)^k f(z)$$

genügen.
Hier entsteht eine reichhaltige Theorie mit einer Fülle von bemerkenswerten Identitäten, die oft verblüffende arithmetische Anwendungen haben.

Literatur

R. Busam, E. Freitag: „Funktionentheorie“, Springer 1993 ff
M. Koecher, A. Krieg: „Elliptische Funktionen und Modulformen“, Springer 1998
D. Zagier: „Elliptic Modular Forms and Their Applications“, in: J.H. Bruinier et al, „The 1-2-3 of Modular Forms“, Springer 2008.

Vorkenntnisse: Algebra I und Funktionentheorie bis zum Residuensatz.

Es kann ein Übungsschein erworben werden, auf Wunsch gibt es eine Modulprüfung.
I´ll be happy to teach the course in English, if that is what the participants desire.

Näheres bei J.Gamst
MZH 7110; gamst@math.uni-bremen.de