Die geometrische Form des Additionstheorems

Vortrag im Seminar Funktionentheorie
Daniel Dräger

11.12.2013

1 Ebene affine Kurven in $\mathbb{C}^2$

Als ebene affine Kurve in $\mathbb{C}^2$ bezeichnen wir eine Menge der Form

$$M = \{(z_1, z_2) \in \mathbb{C}^2 : P(z_1, z_2) = 0\}$$

wobei P ein Polynom ist.
Zur Erinnerung: Für die $\wp$-Funktion zu einem gegebenen Gitter L gilt die Differenzialgleichung $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ wobei g_2 und g_3 von der Wahl des Gitters L abhängen. Zu einem festen Gitter definieren wir nun die zugehörige ebene affine Kurve als:

$$X(g_2, g_3) = \{(z_1, z_2) : z_2^2 = 4z_1^3 - g_2 z_1 - g_3\} \subset \mathbb{C}^2$$

Dann ist $z \mapsto (\wp(z), \wp'(z))$ eine Abbildung $\mathbb{C}/L - \{0\} \to X(g_2, g_3)$. Diese Abbildung ist bijektiv denn:
Surjektivität: Sei $(z_1, z_2) \in X(g_2, g_3)$. Da die $\wp$-Funktion jeden Wert annimmt, existiert $u \in \mathbb{C}/L$ mit $\wp(u) = z_1$. Aus der algebraischen Differenzialgleichung folgt nun:

$$\wp'(u) = z_2 \text{ oder } \wp'(-u) = z_2$$

Das bedeutet u oder $-u$ ist der gesuchte Punkt.
Injektivität: Seien $u, v \in \mathbb{C}/L$ mit $\wp(u) = \wp(v)$ und $\wp'(u) = \wp'(v)$, aus $\wp(u) = \wp(v)$ folgt dann $u = v$ oder $u = -v$. Ist nun $u = -v$ folgt daraus

$$\wp'(u) = \wp'(-v) = -\wp'(v) = -\wp'(u)$$

Also

$$\wp'(u) = 0$$

Dann ist aber $u + u = 0$ also $u = v$.

Bem: Es gilt $(\wp(-z), \wp'(-z)) = (\wp(z), -\wp'(z))$ Die Negation $z \mapsto -z$ auf $\mathbb{C}/L$ entspricht also der Spiegelung $(z_1, z_2) \mapsto (z_1, -z_2)$

Um eine Kurve zu erhalten, die auch den Punkt $0 \in \mathbb{C}/L$ enthält, betrachten wir nun den projektiven Raum $P^2\mathbb{C}$.

2 Der projektive Raum

2.1 Definition

Als *projektiven Raum* bezeichnen wir $P^n\mathbb{C} = (\mathbb{C}^{n+1} - \{0\})/\sim$ wobei $a \sim b \Leftrightarrow a = tb : t \in \mathbb{C} - \{0\}$.

2.2 Der endliche Teil des projektiven Raums

Als den *endlichen Teil* des projektiven Raums bezeichnen wir:

$$\{[a_0, a_1, a_2] \in P^2\mathbb{C} : a_0 \neq 0\}$$

Durch $f : \mathbb{C}^2 \to P^2\mathbb{C}$ mit

$$f(z_1, z_2) = [1, z_1, z_2]$$
$$f^{-1}([z_0, z_1, z_2]) = (\frac{z_1}{z_0}, \frac{z_2}{z_0})$$

erhalten wir eine Bijektion von $\mathbb{C}^2$ in den endlichen Teil des projektiven Raums und können $\mathbb{C}^2$ als Teilmenge des projektiven Raums $P^2\mathbb{C}$ auffassen. Das Komplement des endlichen Teils nennt man den *unendlich fernen Teil*.

2.3 Der Abschluss der ebenen affinen Kurve $X(g_2, g_3)$

Eine Kurve im projektiven Raum $P^2\mathbb{C}$ ist eine Teilmenge

$$M = \{a = [a_0, a_1, a_2] \in P^2\mathbb{C} : P(a_0, a_1, a_2) = 0\}$$

wobei das Polynom P homogen ist, das heißt, es existiert ein $d \in \mathbb{N}$ sodass $P(ta) = t^d P(a)$ für alle $t \in \mathbb{C} - \{0\}$.
Wir können nun $X(g_2, g_3)$ auf $P^2\mathbb{C}$ durch

$$\tilde{X}(g_2, g_3) = \{[z_0, z_1, z_2] \in P^2\mathbb{C} : z_2^2 z_0 = 4z_1^3 - g_2 z_1 z_0^2 - g_3 z_0^3\}$$

fortsetzten. Für $z_0 = 1$ erhalten wir genau die Kurve $X(g_2, g_3) \subset \mathbb{C}^2$. Für $z_0 = 0$ erhalten wir (da $z_1 = 0$ folgt) den Punkt $(0, 0, 1)$. Weiter lässt sich die Bijektion vom Anfang durch

$$f : \mathbb{C}/L \to \tilde{X}(g_2, g_3)$$

$$f(z) = \begin{cases} [1, \wp(z), \wp'(z)] & \text{falls } z \neq 0 \\ [0, 0, 1] & \text{falls } z = 0. \end{cases}$$

fortsetzen. Das f in 0 stetig ist sieht man, indem man f in einer Umgebung von $0 \in \mathbb{C}$ als

$$f(z) = [z^3, z^3\wp(z), z^3\wp'(z)]$$

schreibt. Da $\mathbb{C}/L$ kompakt ist, f stetig ist und $\tilde{X}(g_2, g_3)$ mit der Quotiententopologie auf $\mathbb{C}^3$ Hausdorf ist, ist f ein Homöomorphismus. $\tilde{X}(g_2, g_3)$ nennt man die zum Gitter L gehörende elliptische Kurve.

2.4 Geraden im projektiven Raum $P^2\mathbb{C}$

Eine Gerade zwischen zwei Punkten $a = [a_0, a_1, a_2]$ und $b = [b_0, b_1, b_2]$ im projektiven Raum ist eine Menge der Form $G = \{[a_0z + b_0w, a_1z + b_1w, a_2z + b_2w] \in P^2\mathbb{C} : (z, w) \in \mathbb{C}^2 - \{0\}\}$. Ist a oder b in $\mathbb{C}^2 \subset P^2\mathbb{C}$, entspricht $G \cap \mathbb{C}^2$ gerade einer Gerade in $\mathbb{C}^2$. Denn:
Sei OBdA $a \in \mathbb{C}^2 \subset P^2\mathbb{C}$. Wenn wir die Addition von $\mathbb{C}^2$ auf $P^2\mathbb{C}$ übertragen erhalten wir:

$$[a_0, a_1, a_3] + [c_0, c_1, c_2] = [a_0c_0, a_0c_1 + c_0a_1, a_0c_2 + c_0a_2]$$

Wobei diese Verknüpfung nur definiert ist falls mindestens eine der Komponenten aus dem endlichen Teil ist. Subtrahieren wir nun den Punkt a von der Gerade so erhalten wir :

$$G-a = \{[(a_0z+b_0w)a_0, (a_1z+b_1w)a_0-(a_0z+b_0w)a_1, (a_2z+b_2w)a_0-(a_0z+b_0w)a_2] : (z, w) \in \mathbb{C}^2-\{0\}\}$$

$$G - a = \{[a_0^2z + a_0b_0w, (b_1a_0 - b_0a_1)w, (b_2a_0 - b_0a_2)w] : (z, w) \in \mathbb{C}^2 - \{0\}\}$$

Sind nun a und b Punkte in $\mathbb{C}^2 \subset P^2\mathbb{C}$ können wir annehmen $a_0 = b_0 = 1$, und es gilt:

$$G - a = \{[z + w, (b_1 - a_1)w, (b_2 - a_2)w] : (z, w) \in \mathbb{C}^2 - \{0\}\}$$

Dies entspricht einer Geraden durch den Nullpunkt mit der Steigung $m = \frac{(b_2-a_2)}{(b_1-a_1)}$, vereinigt mit dem unendlich fernen Punkt $[0, b_1 - a_1, b_2 - a_2]$ für $z = -w$.
Ist nun b nicht in $\mathbb{C}^2 \subset P^2\mathbb{C}$ können wir annehmen $a_0 = 1, b_0 = 0$, und:

$$G - a = \{[z, b_1w, b_2w] : (z, w) \in \mathbb{C}^2 - \{0\}\}$$

Sind a und b beide nicht in $\mathbb{C}^2 \subset P^2\mathbb{C}$ erhalten wir:

$$G = \{[0, a_1z + b_1w, a_2z + b_2w] : (z, w) \in \mathbb{C}^2 - \{0\}\}$$

Dies entspricht offenbar genau dem unendlich fernen Teil des projektiven Raums.

3 Lemma

Sei L ein Gitter. Jede Gerade G schneidet die zu L gehörende elliptische Kurve $\tilde{X}(g_2, g_3)$ in genau 3 Punkten (mit Vielfachheiten).

Beweis

Sei $G = \{[a_0z+b_0w, a_1z+b_1w, a_2z+b_2w] : (z, w) \in \mathbb{C}^2-\{0\}\}$. Falls nicht gerade $a = [a_0, a_1, a_2]$ und $b = [b_0, b_1, b_2]$ unendlich ferne Punkte sind, hat G die Form: $G = \{[z, m_1w, m_2w] + b : (z, w) \in \mathbb{C}^2 - \{0\}\}$ und es gilt: $(0, 0, 1) \in G \Leftrightarrow m_1 = 0$.
Fall $(0, 0, 1) \in G$:
Es ist zu zeigen, dass es noch genau 2 weitere Punkte gibt.
Der endliche Teil der Gerade ist gegeben durch die Gleichung $\{(z_1, z_2) \in \mathbb{C}^2 : z_1 = c\}$ für ein festes $c \in \mathbb{C}$. Die Gleichung

$$z_2^2 = 4z_1^3 - g_2z_1 + g_3$$

hat offenbar 2 Lösungen (mit Vielfachheiten) da die rechte Seite konstant ist.
Fall $(0, 0, 1) \notin G$:
Der endliche Teil der Gerade ist gegeben durch die Gleichung $z_2 = mz_1 + b$, wobei $m = \frac{m_2}{m_1}$ Die Gleichung

$$z_2^2 = 4z_1^3 - g_2z_1 + g_3$$

hat dann 3 Lösungen.

Falls nun G gerade der unendlich ferne Teil des projektiven Raums ist, betrachten wir die Darstellung der Kurve:

$$0 = 4z_1^3 - g_2 z_1 z_0^2 - g_3 z_0^3 - z_2^2 z_0$$

Für die Schnittpunkte mit der Gerade $z_0 = 0$ ergibt sich:

$$0 = 4z_1^3$$

also eine dreifache Nullstelle in dem Punkt $(0, 0, 1)$.

4 Lemma

Falls u, v, $u + v \in \mathbb{C}/L$ von null verschieden sind gilt:

$$det \begin{pmatrix} 1 & \wp(u+v) & -\wp'(u+v) \\ 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \end{pmatrix} = 0$$

Beweis

Falls 2 Punkte von $u, v, -u-v$ gleich sind ist die Aussage trivial. Wir betrachten die Nullstellen von

$$f(z) = det \begin{pmatrix} 1 & \wp(z) & \wp'(z) \\ 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \end{pmatrix} = 0$$

$$f(z) = \wp(u)\wp'(v) + \wp(z)\wp'(u) + \wp(v)\wp'(z) - \wp(z)\wp'(v) - \wp(u)\wp'(z) - \wp(v)\wp'(u)$$

$$f(z) = A + B\wp(z) + C\wp'(z)$$

mit $C = \wp(v) - \wp(u) \neq 0$. f hat einen dreifachen Pol in 0 da $\wp'$ dort einen dreifachen Pol hat. Nach dem Abelschen Theorem hat f drei (möglicherweise gleiche) Nullstellen a, b, c mit $a + b + c = 0$. u und v sind Nullstellen, die dritte Nullstelle ist also $c = -u - v$. Es gilt $\wp(u + v) = \wp(-u - v)$ und $-\wp'(u + v) = \wp'(-u - v)$

5 Geometrische Form des Additionstheorems

Drei paarweise verschiedene Punkte $u, v, w \in \mathbb{C}/L$ haben genau dann die Summe null wenn sie in $P^2\mathbb{C}$ auf einer Geraden liegen.

Beweis

"⇒": Angenommen u, v, w haben die Summe null und sind jeweils ungleich null. Dann gilt $w = -u - v$. Nach Lemma 4 gilt

$$det \begin{pmatrix} 1 & \wp(w) & \wp'(w) \\ 1 & \wp(u) & \wp'(u) \\ 1 & \wp(v) & \wp'(v) \end{pmatrix} = 0$$

d.h. die Punkte liegen auf einer Geraden (da die Geraden in $P^2\mathbb{C} = \mathbb{C}^3 - \{0\}/\sim$ gerade die 2-dimensionalen Untervektorrume ohne den Ursprung in $\mathbb{C}^3$ sind).
Sei nun $w = 0$, $u = -v$. Die Punkte liegen dann auf der Geraden

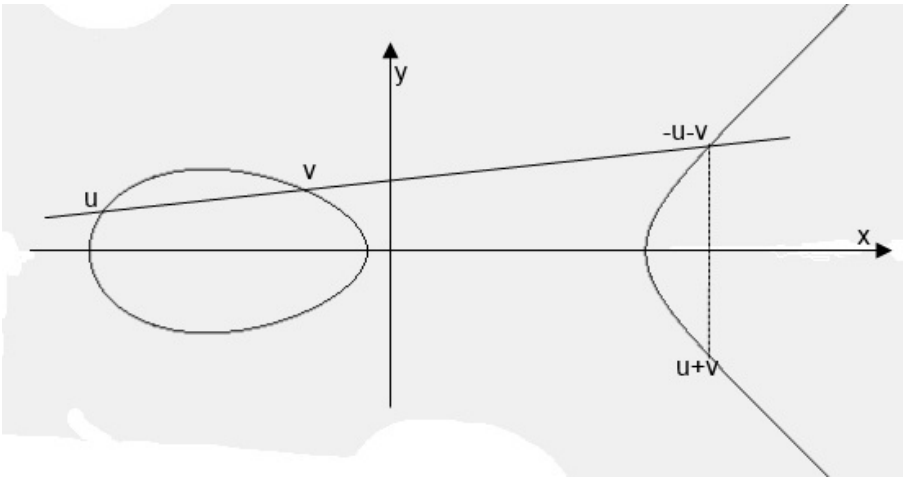
$$G = \{(s, s\wp(u), t) \in P^2\mathbb{C} : (z, w) \in \mathbb{C}^2 - \{0\}\}$$

wie man durch Einsetzen leicht einsieht.
"$\Leftarrow$": Angenommen u, v, w liegen auf einer Geraden.
Im Fall $u \neq 0$, $v \neq 0$ und $w \neq 0$, können wir OBdA annehmen, dass u, v, $-u - v$ paarweise verschieden sind. Nach "$\Rightarrow$" liegen u, v, $-u - v$ auch auf der Geraden. Nach Lemma 3 gibt es aber nur höchstens 3 Punkte in der Kurve, die auch auf der Geraden liegen. Also folgt $w = -u - v$.
Betrachten wir nun den anderen Fall: sei OBdA $u \neq 0$, $v \neq 0$, $w = 0$. Dann hat die Gerade durch u und w die Form:

$$\{(s, s\wp(u), t) \in P^2\mathbb{C} : (z, w) \in \mathbb{C}^2 - \{0\}\}$$

Der einzige dritte Punkt (mit Vielfachheiten) ist dann $-u$, wie wir schon in Lemma 3 gesehen haben.

Dadurch haben wir die (durch $\mathbb{C}/L \cong \tilde{X}(g_2, g_3) \subset P^2\mathbb{C}$ induzierte) Addition auf der Elliptischen Kurve vollständig beschrieben:
Zu Punkten $u, v \in \tilde{X}(g_2, g_3)$ finden wir den Punkt $-(u + v)$ indem wir durch u und v eine Gerade bilden und den eindeutigen dritten Schnittpunkt mit der Kurve suchen. Der Punkt $u + v$ ist dann $-(u + v)$ gespiegelt an der X-Achse.



6 Analytische Form des Additionstheorems

Sind u, v, $u + v$, $u - v$ von null verschieden, so gilt:

$$\wp(u + v) = \frac{1}{4}\left(\frac{\wp'(u) - \wp'(v)}{\wp(u) - \wp(v)}\right)^2 - \wp(u) - \wp(v)$$

Beweis

Die Punkte $(\wp(u), \wp'(u))$, $(\wp(v), \wp'(v))$, $(\wp(-u-v), \wp'(-u-v))$ liegen auf einer Geraden der Form: $mz + b$ mit $m = \frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}$. Also sind $\wp(u), \wp(v), \wp(-v-u)$ Nullstellen des Polynoms

$$P(X) = \left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}X + b\right)^2 - 4X^3 + g_2X + g_3$$

Das heißt P hat die Form:

$$P(X) = (X - \wp(u))(X - \wp(-v))(X - \wp(-u-v))K$$

mit $K \in \mathbb{C}$. Durch Koeffizientenvergleich der quadratischen Terme erhält man:

$$(\wp(u)) + \wp(-v) + \wp(-u-v)) = \frac{1}{4}\left(\frac{\wp'(z) - \wp'(w)}{\wp(z) - \wp(w)}\right)^2$$

Also genau das Additionstheorem in der analytischen Form.

Quellen

E. Freitag und R. Busam, *Funktionentheorie 1*, 4. Auflage, Springer-Lehrbuch, 2006