Geometrische Form des Additionstheorems

Jae Hee Lee

29. Mai 2006

Zusammenfassung

Der Additionstheorem lässt sich mithilfe des Abelschen Theorems elegant beweisen. Dieser Beweis und die Isomorphie zwischen $\mathbb{C}/L$ und der elliptischen Kurve $\tilde{X}(g_2, g_3)$ erlaubt es, die Gruppenstruktur der elliptischen Kurve geometrisch zu interpretieren, nämlich: genau dann haben drei Punkte auf der elliptischen Kurve die Summe Null, wenn sie die Schnittpunkte von der Kurve und einer Geraden sind.

Bemerkung. Für das Verständnis dieser Ausarbeitung ist zusätzlich das Wissen über die projektive Ebene erforderlich. Die Bezeichnung L wird hier stets für das Gitter, zu dem die jeweilige $\wp$-Funktion konstruiert ist, verwendet. Man beachte außerdem, dass $\wp$ eine gerade und $\wp'$ eine ungerade Funktion ist und dass $\wp(u) \neq \wp(v)$, $\wp(u+v) \neq \wp(u)$ und $\wp(u+v) \neq \wp(v)$ aus $u, v, u+v, u-v, u+2v, 2u+v \neq 0$ folgt.

Lemma. *Es gilt für $u, v \in \mathbb{C}/L$ und $u, v, u+v, u-v \neq 0$:*

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

Beweis. Die Funktion

$$\begin{aligned} f : \mathbb{C}/L - \{0\} &\longrightarrow \mathbb{C} \\ f(z) = \det &\begin{pmatrix} 1 & \wp(z) & \wp'(z) \\ 1 & \wp(v) & \wp'(v) \\ 1 & \wp(u) & \wp'(u) \end{pmatrix} \\ &= (\wp(u) - \wp(v))\wp'(z) + (\wp'(v) - \wp'(u))\wp(z) \\ &\quad + \wp(v)\wp'(u) - \wp(u)\wp'(v) \end{aligned}$$

ist eine elliptische Funktion. Sie hat $\mod L$ genau eine Polstelle der Ordnung 3, nämlich in $z = 0$. Aus dem 3. Liouvilleschem Satz folgt, dass auch die Nullstellenordnung von f gleich 3 ist. Bei $z = u$ und $z = v$ ist die Determinante gleich Null. Sie sind also zwei Nullstellen von f. Außerdem gilt nach dem Abelschen Theorem mit Berücksichtigung der Vielfachheit

$$0 = \text{Nullstellensumme} - \text{Polstellensumme} = (u + v + z) - 0$$

Daraus folgt, dass $z = -(u + v)$ die dritte Nullstelle ist. □

Satz (Additionstheorem)**.** *Es seien* $z, w \in \mathbb{C}/L - \{0\}$ *und* $z, w, z+w, z-w, 2z+w, z+2w \neq 0$. *Dann gilt*

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

Beweis. Es gilt

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

Aus dem Verschwinden der Determinante folgt, dass die Punkte $(\wp(z), \wp'(z))$, $(\wp(w), \wp'(w))$, $(\wp(z+w), -\wp'(z+w))$ linear abhänging sind und daher auf einer Geraden

$$y = mx + b \quad \text{mit} \quad m = \frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}$$

liegen. Aus der algebraischen Differentialgleichung $0 = 4\wp(u)^3 - g_2\wp(u) - g_3 - \wp'(u)^2$ folgt, dass $\wp(z), \wp(w), \wp(z+w)$ Nullstellen des kubischen Polynoms

$$4X^3 - g_2X - g_3 - (mX+b)^2$$

sind. Da sie paarweise verschieden sind, gibt es keine weiteren Nullstellen. Es gilt dann

$$(4X^3 - g_2X - g_3 - (mX+b)^2) = 4(X-\wp(z))(X-\wp(w))(X-\wp(z+w))$$

und durch Koeffizientenvergleich bei den quadratischen Termen erhält man für ihre Summe

$$\begin{aligned} & \wp(z) + \wp(w) + \wp(z+w) = \frac{m^2}{4} \\ \iff \quad & \wp(z+w) = \frac{1}{4}\left[\frac{\wp'(z)-\wp'(w)}{\wp(z)-\wp(w)}\right]^2 - \wp(z) - \wp(w) \end{aligned}$$

□

Bemerkung (Additive Struktur der elliptischen Kurve). Sei

$$\begin{aligned} \tilde{X}(g_2, g_3) &= \left\{[z_0, z_1, z_2] \in P^2\mathbb{C} \mid \ z_0 z_2^2 = 4z_1^3 - g_2 z_0^2 z_1 - g_3 z_0^3\right\} \\ &= \left\{[1, \wp(z), \wp'(z)] \in P^2\mathbb{C} \mid \ z \in \mathbb{C}/L \ - \{0\}\right\} \ \cup \ \{[0,0,1]\} \end{aligned}$$

die zum Gitter L gehörige elliptische Kurve. Wir wissen, dass zwischen $\mathbb{C}/L$ und $\tilde{X}(g_2, g_3)$ eine bijektive Abbildung φ erklärt ist durch

$$\varphi: \quad \mathbb{C}/L \longrightarrow \tilde{X}(g_2, g_3)$$

$$\varphi(z) = \begin{cases} [1, \wp(z), \wp'(z)] & \text{falls } z \notin L \\ [0,0,1] & \text{falls } z \in L \end{cases}$$

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

(Beachte, dass $z^3\wp'(z)$ bei $z=0$ wohl definiert und $\neq 0$ ist.) Bezüglich der Verknüpfung $\oplus$ mit

$$p_1 \oplus p_2 = \varphi\left(\varphi^{-1}(p_1) + \varphi^{-1}(p_2)\right), \qquad p_1,\, p_2 \in \tilde{X}(g_2, g_3)$$

wird folglich eine additive Gruppenstruktur auf $\tilde{X}(g_2, g_3)$ definiert; das Nullelement dieser Gruppe ist $[0,0,1]$ und das Inverse zu $[z^3, z^3\wp(z), z^3\wp'(z)]$ ist $[-z^3, -z^3\wp(z), z^3\wp'(z)]$.

Beispiel.

$$\begin{aligned}[0,0,1] \oplus [2, \wp(2), \wp'(2)] &= \varphi\left(\varphi^{-1}([0,0,1]) + \varphi^{-1}([2, \wp(2), \wp'(2)])\right) \\ &= \varphi(0+2) \\ &= [2, \wp(2), \wp'(2)]\end{aligned}$$

Definition. Eine Teilmenge $G \subset P^2\mathbb{C}$ heißt Gerade, wenn es zwei verschiedene Punkte $[z_0, z_1, z_2]$ und $[w_0, w_1, w_2]$ gibt mit

$$G = \left\{[\lambda z_0 + \mu w_0, \lambda z_1 + \mu w_1, \lambda z_2 + \mu w_2] \mid \ (\lambda, \mu) \in \mathbb{C}^2 \backslash \{(0,0)\}\right\}$$

Proposition 1. *Eine Gerade in $P^2\mathbb{C}$ hat mit der elliptischen Kurve $\tilde{X}(g_2, g_3)$ drei Schnittpunkte (mit Berücksichtigung der Vielfachheit).*

Beweis. Sei $[z, x, y]$ die Koordinate für $P^2\mathbb{C}$. Dann ist die Gleichung der Kurve

$$y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3$$

und die unendlich ferne Gerade bezüglich x, y ist

$$G = \{[0, x, y] \mid x, y \in \mathbb{C}]\}$$

1) Schnitt der Kurve mit G:

Da $z = 0$ ist auch $x = 0$ und es bleibt $[0,0,1]$. Um die Schnittvielfachheit dieses Punktes zu bestimmen, rechne man in (z, x) mit $(0,0)$ als Ursprung. Dann ist G gegeben durch $\{[0, u, 1] \mid u \in \mathbb{C}\}$, und der Schnitt mit der Kurve ist gegeben durch $0 = 4u^3$. Also, $[0,0,1]$ ist Nullstelle der Ordnung 3.

2) Schnitt der Kurve mit einer anderen Geraden, d.h mit $ax + by + cz = 0$, wobei $(a, b) \neq (0,0)$:

2.1) $b = 0$

Dann ist die Gerade die durch $x = -\frac{c}{a}$ gegebene Parallele zur y-Achse und enthält $[0,0,1]$. Die endlichen Schnittpunkte mit der Kurve sind in (x, y)-Koordinaten gegeben durch

$$y^2 = -4\left(\frac{c}{a}\right)^3 + g_2\left(\frac{c}{a}\right) - g_3,$$

es sind also $[1, -c/a, y_0]$ und $[1, -c/a, -y_0]$ mit $y_0 = \sqrt{-4\left(\frac{c}{a}\right)^3 + g_2\left(\frac{c}{a}\right) - g_3}$

2.2) $b \neq 0$

Dann enthält die Gerade $[0,0,1]$ nicht, und die endlichen Schnittpunkte mit der Kurve sind in (x, y)-Koordinaten gegeben durch

$$y = -\frac{a}{b}x - \frac{c}{b}$$

und

$$\left(\frac{a}{b}x + \frac{c}{b}\right)^2 = 4x^3 - g_2 x - g_3,$$

es sind also (evtl. mit Vielfachheit) drei. □

Proposition 2. *Drei Punkte auf der elliptischen Kurve $\tilde{X}(g_2, g_3)$ haben genau dann die Summe Null, wenn sie die Schnittpunkte von $\tilde{X}(g_2, g_3)$ und einer Geraden in $P^2\mathbb{C}$ sind. D.h. für $a, b, c \in P^2\mathbb{C}$ gilt*

$$a \oplus b \oplus c = 0 \Longleftrightarrow \exists \text{ Gerade } G \subset P^2\mathbb{C} \text{ mit } G \cap \tilde{X}(g_2, g_3) = \{a, b, c\}$$

Beweis. „⇒“

Es reicht zu zeigen, dass für $a, b, c \in \tilde{X}(g_2, g_3)$ mit $a = [v^3, v^3\wp(v), v^3\wp'(v)]$, $b = [w^3, w^3\wp(w), w^3\wp'(w)]$, $c = [z^3, z^3\wp(z), z^3\wp'(z)]$, $v, w, z \in \mathbb{C}$

$$D := \det \begin{pmatrix} v^3 & v^3\wp(v) & v^3\wp'(v) \\ w^3 & w^3\wp(w) & w^3\wp'(w) \\ z^3 & z^3\wp(z) & z^3\wp'(z) \end{pmatrix} = 0$$

ist. Aus

$$\begin{aligned} a \oplus b \oplus c &= [v^3, v^3\wp(v), v^3\wp'(v)] \oplus [w^3, w^3\wp(w), w^3\wp'(w)] \oplus [z^3, z^3\wp(z), z^3\wp'(z)] \\ &= [(v+w+z)^3, (v+w+z)^3\wp(v+w+z), (v+w+z)^3\wp'(v+w+z)] \\ &= 0 \qquad (= [0,0,1]\ ). \end{aligned}$$

folgt $v + w + z = 0$. Für $v = w = z = 0$ ist offenbar $D = 0$. Sei etwa $v = 0, w = -z \neq 0$. Dann ist

$$D = \det \begin{pmatrix} 0 & 0 & v^3\wp'(v) \\ -z^3 & -z^3\wp(z) & z^3\wp'(z) \\ z^3 & z^3\wp(z) & z^3\wp'(z) \end{pmatrix}$$

(Beachte $v^3\wp'(v) \neq 0$ bei $v = 0$). Ist zusätzlich $\wp'(z) = 0$, so hat die Matrix folgende Form

$$\begin{pmatrix} 0 & 0 & v^3\wp'(v) \\ -z^3 & -z^3\wp(z) & 0 \\ z^3 & z^3\wp(z) & 0 \end{pmatrix},$$

woraus $D = 0$ folgt; für $\wp'(z) \neq 0$ lässt sich die erste Zeile der Matrix durch die anderen beiden darstellen und somit ist ihre Determinante gleich Null. Für $v, w, z \neq 0$ folgt die Behauptung aus dem am Anfang bereits bewiesenen Lemma.

„⇐“

Nach **Proposition 1** sind entweder alle drei Schnittpunkte gleich dem unendlich fernen Punkt, also $a = b = c = [0, 0, 1]$ *(1)*, oder genau einer liegt im unendlich fernen Teil und die anderen zwei liegen im endlichen Teil, also o.B.d.A, $a = [0, 0, 1]$ und $b, c \in \tilde{X}(g_2, g_3)\backslash\{[0, 0, 1]\}$ *(2.1)*, oder sie sind alle im endlichen Teil, d.h. $a, b, c \in \tilde{X}(g_2, g_3)\backslash\{[0, 0, 1]\}$ *(2.2)*.

Fall 1: ($a = b = c = [0, 0, 1]$)

Trivial.

Fall 2: a) ($a = [0, 0, 1]$ und $b, c \in \tilde{X}(g_2, g_3)\backslash\{[0, 0, 1]\}$)

Es gilt nach dem Beweis von **Proposition 1**

$$b = [1, \wp(w), \wp(w)] \quad \Longrightarrow \quad c = [1, \wp(w), -\wp(w)] = [1, \wp(-w), \wp(-w)].$$

Somit ist c das Inverse von b.

b) $(a, b, c \in \tilde{X}(g_2, g_3) \backslash \{[0, 0, 1]\})$

Falls mindenstens zwei Punkte verschieden sind, folgt die Behauptung nach dem Lemma am Anfang. Wir behaupten, dass kein Schnittpunkt von G mit der Kurve die Vielfachheit drei haben kann. Sei o.E. $a = [1, \wp(v), \wp'(v)]$ ein Schnittpunkt mit Vielfachheit 3. Wegen $v + v - 2v = 0$ liegt dann der Punkt $-2a := [1, \wp(-2v), \wp'(-2v)] = -a \oplus -a$ auch auf der Geraden. Ist $-2a \neq a$, dann schneidet die Gerade die elliptische Kurve mindestens in vier Punkten (mit Berücksichtigung der Vielfachheit), also ein Widerspruch zur **Proposition 1**. Ist aber $-2a = a$, dann muss a das Nullelement sein, was unserer Voraussetzung widerspricht. □

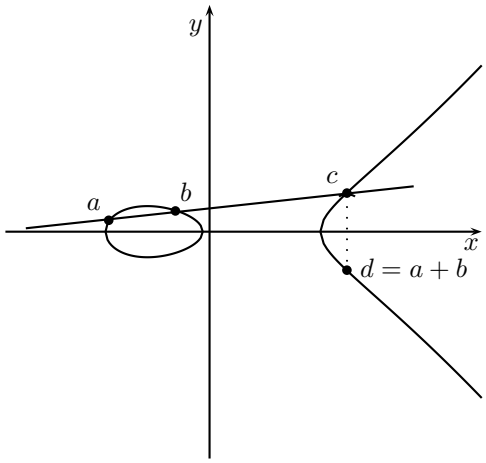

Abbildung 1: Reeller endlicher Teil der elliptischen Kurve $\tilde{X}(g_2, g_3)$. Die Summe der reellen Punkte a und b ist der Punkt d, der aus c durch Spieglung an der x-Achse hervorgeht.

Bemerkung. Wegen der obigen Eigenschaft der elliptischen Kurve $\tilde{X}(g_2, g_3)$ kann man zu jedem Element per Verbindung mit $[0, 0, 1]$ das Inverse finden. Möchte man außerdem ein Element verdoppeln, reicht es, an das Element eine Tangente zu legen, dann ist der andere Schnittpunkt von der Tangente mit der Kurve das gesuchte verdoppelte Element.

In **Proposition 1** *2.1)* ist es zu sehen, dass die Gerade $ax + cz = 0$, $(a \neq 0)$ durch den Punkt $[0, 0, 1]$ und die Punkte $[1, -c/a, y_0]$ und $[1, -c/a, -y_0]$ verläuft mit $y_0 = \sqrt{-4(c/a)^3 + g_2 c/a - g_3}$. Es gibt drei solche Geraden, die den Wert y_0 annulieren, da $\wp'$ drei paarweise verschiedene Nullstellen hat. (Im reelen Fall gibt es entweder eine oder drei solche Geraden). Der Punkt $[1, -c/a, y_0]$ ist dann zu sich invers, d.h. die Tangente an den Punkt enthält den Punkt $[0, 0, 1]$. Diese Punkte mit der Ordnung 2 bilden zusammen mit dem Nullpunkt eine abelsche Gruppe, die isomorph zur Kleinschen Vierergruppe ist.

Literatur

[1] E. Freitag, R. Busam: Funktionentheorie 1 , Springer Verlag, 2000, S.283-285