ELLIPTISCHE KURVEN

Grundlagen

Isogenien

Duale Isogenie

Proposition 0.1. *Es sei* (E, O_E) *eine elliptische Kurve und* $\mathrm{Pic}^0(E)$ *die Gruppe der Divisoren vom Grad* 0 *auf* E. *Dann ist die Zuordnung*

$$\Phi_E : E \to \mathrm{Pic}^0(E), \quad P \mapsto [P]-[O_E] \tag{1}$$

ein Gruppenisomorphismus

Definition 0.1. *Es sei* $f : E_1 \to E_2$ *eine Isogenie elliptischer Kurven. Das Diagramm*

$$\begin{array}{ccc} \mathrm{Pic}^0(E_1) & \xleftarrow{\Phi_{E_1}} & E_1 \\ {\scriptstyle f^*}\uparrow & & \uparrow{\scriptstyle \hat{f}} \\ \mathrm{Pic}^0(E_2) & \xleftarrow[\Phi_{E_2}]{} & E_2 \end{array} \tag{2}$$

definiert eine Isogenie $\hat{f} : E_2 \to E_1$, *die* duale Isogenie.

Es sei E/k eine elliptische Kurve über dem Körper k. Weiter sei

$$\mu : E \times_k E \to E \tag{3}$$

der Morphismus der Addition auf der elliptischen Kurve.
Es seien $p_1, p_2 : E \times_k E \to E$ die kanonischen Projektionen auf den ersten und zweiten Faktor und es sei $\mathscr{L} = \mathscr{L}(D)$ das Linienbündel auf E zu einem Divisor D auf E vom Grad $\deg D = 0$.

Lemma 0.1. *Es sei*

$$\mathscr{L} \in \mathrm{Pic}^0(E) \tag{4}$$

Dann gilt mit obigen Bezeichnungen die Beziehung

$$\mu^*\mathscr{L} = p_1^*\mathscr{L} \otimes p_2^*\mathscr{L} \tag{5}$$

Beweis. Wir zeigen zunächst, daß $\mu^*\mathscr{L} \otimes (p_1^*\mathscr{L})^{-1}$ auf den Fasern $p_2^{-1}(P) = E \times P$ für einen Punkt $P \in E$ immer trivial ist, also

$$\left(\mu^*\mathscr{L} \otimes (p_1^*\mathscr{L})^{-1}\right)|_{E\times P} \cong \mathscr{O}_{E\times P} \tag{6}$$

ist.
Es ist nämlich $\mu^*\mathscr{L}|_{E\times P} \cong \tau_P^*\mathscr{L}|_E$, wobei $\tau_P : E \to E$ die Abbildung $Q \mapsto P+Q$ ist. Weiterhin ist $\left(p_1^*\mathscr{L}\right)|_{E\times P} \cong \mathscr{L}|_E$. Nun ist aber der Divisor D, der zu $\mathscr{L}$ gehört vom Grad 0, also

$$D = \sum_i n_i P_i, \quad \sum_i n_i = 0 \tag{7}$$

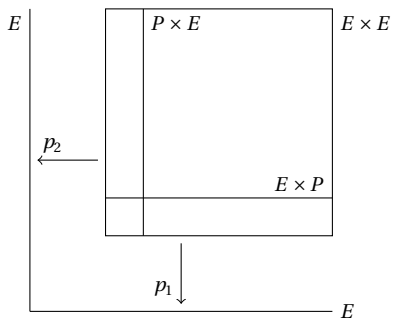
Damit ist $\tau_P^*(D) = \sum_i n_i(P_i - P) \sim \sum_i n_i P_i = D$. Also ist $\tau_P^*\mathscr{L} = \mathscr{L}$ auf E und damit $\left(\mu^*\mathscr{L} \otimes (p_1^*\mathscr{L})^{-1}\right)|_{E\times P} = \mathscr{O}_{E\times P}$ wie behauptet.
Nach den Halbstetigkeitssätzen ist dann

$$\mu^*\mathscr{L} \otimes \left(p_1^*\mathscr{L}\right)^{-1} = p_2^*\mathscr{N} \tag{8}$$

mit einem zunächst unbekannten Linienbündel $\mathscr{N}$ auf E.
Wir betrachten nun $(p_2^*\mathscr{N})|_{P\times E}$. Es ist $\mu^*\mathscr{L}|_{P\times E} = \tau_P^*\mathscr{L}|_E = \mathscr{L}|_E = p_2^*\mathscr{L}|_{P\times E}$. Weiter ist $p_1^*\mathscr{L}|_{P\times E} = \mathscr{O}_{P\times E}$, da $p_1^{-1}(P) = P \times E$ ist. Also ist $p_2^*\mathscr{N}|_{P\times E} = p_2^*\mathscr{L}|_{P\times E}$ für alle $P \in E$ und damit

$$\mu^*\mathscr{L} \otimes \left(p_1^*\mathscr{L}\right)^{-1} = p_2^*\mathscr{L} \tag{9}$$

was offensichtlich äquivalent zur Behauptung ist.
Siehe zur Veranschaulichung der einzelnen Abbildungen und Einschränkungen auf die Fasern auch das folgende Bild:



Proposition 0.2. *Es seien* $f, g : E_1 \to E_2$ *zwei Isogenien. Dann ist*

$$\widehat{(f+g)} = \hat{f} + \hat{g}$$

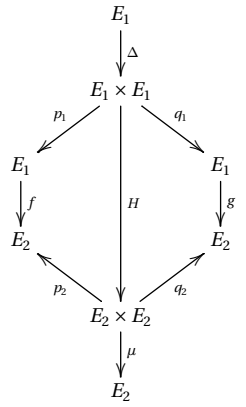
Beweis. Es ist zu zeigen, daß für jedes $\mathscr{L} \in \mathrm{Pic}^0(E_2)$ immer

$$(f+g)^*\mathscr{L} = f^*\mathscr{L} \otimes_{\mathscr{O}_{E_1}} g^*\mathscr{L}$$

ist.

Betrachte das Diagramm

(10)



Es ist

$$(f+g)^*\mathscr{L} = \Delta^*H^*\mu^*\mathscr{L} = \Delta^*H^*(p_2^*\mathscr{L} \otimes q_2^*\mathscr{L}).$$

Weiterhin ist aber auch $p_2 \circ H \circ \Delta = f \circ p_1 \circ \Delta = f$ und $q_2 \circ H \circ \Delta = g \circ q_1 \circ \Delta = g$. Also $\Delta^*H^*p_2^*\mathscr{L} = f^*\mathscr{L}$ und $\Delta^*H^*q_2^*\mathscr{L} = g^*\mathscr{L}$. Insgesamt also

$$\Delta^*H^*(p_2^*\mathscr{L} \otimes q_2^*\mathscr{L}) = f^*\mathscr{L} \otimes g^*\mathscr{L}$$

Weilpaarung

Es sei E/K eine elliptische Kurve und $[m] : E \to E$ die Multiplikation mit m. Wir wollen für $S, T \in E[m]$ eine Weilpaarung $e(S,T) \in \mu_m(K)$ definieren.
Die Details der Definition der Weilpaarung sind am einfachsten rückwärts zu merken:
Wir wollen für ein $S \in E[m]$ eine Funktion $g(X) \in K(E)$ definieren, die von einem $T \in E[m]$ abhängt und für die

$$(g(X+S)/g(X))^m = 1$$

gilt. Es wird dann $e(S,T) = g(X+S)/g(X)$ eine m-te Wurzel in K, die *Weilpaarung von* S *und* T sein. Eine solche Funktion g ist zum Beispiel eine, die

$$g(X)^m = f([m]X)$$

für eine geeignete Funktion $f = f_T$ erfüllt, denn es ist dann ja

$$g(X+S)^m = f([m](X+S)) = f([m]X) = g(X)^m$$

Wir brauchen also eine Funktion $f(X)$, so daß man aus $f([m]X)$ die m-te Wurzel in $K(E)$ ausziehen kann.
Diese ist aber durch $\mathrm{div}(f) = m[T] - m[0] = m([T]-[0])$ definierbar. Es ist ja mit einem T', für das $[m]T' = T$ gilt

$$\mathrm{div}\, f([m]X) = m\left(\sum_{W\in E[m]} [T'+W] - \sum_{W\in E[m]} [W]\right),$$

da man für $\mathrm{div}\, f([m]X)$ die Urbilder von T und 0 unter $[m]$ aufzusuchen hat. Zwei Urbilder $[m]T' = T$ und $[m]T'' = T$ unterscheiden sich dann um ein $T' - T''$ mit $[m](T'-T'') = 0$. Daher die obige Formel.
Nun definiert aber schon der Divisor

$$D_g = \sum_{W\in E[m]} [T'+W] - \sum_{W\in E[m]} [W]$$

eine Funktion $g = g_T$, denn die Summe der Punkte der Divisoren addieren sich zu $0_E \in E$, weil $[m^2]T' = 0$ und auch die Koeffizienten addieren sich zu $0 \in \mathbb{Z}$.
Für diese Funktion g mit $\mathrm{div}\, g = D_g$ gilt dann unser gewünschtes

$$g(X)^m = f([m]X)$$

Definition 0.2. *Die Abbildung*

$$e : E[m] \times E[m] \to \mu_m, \quad (S,T) \mapsto e(S,T)$$

ist die sogenannte Weilpaarung.

Proposition 0.3. *Die Weilpaarung erfüllt folgende Beziehungen:*

1. *Bilinearität:*
$$e(S+S',T) = e(S,T)e(S',T)$$
$$e(S,T+T') = e(S,T)e(S,T')$$
für $S, S', T, T' \in E[m]$.
2. *Antisymmetrie:*
$$e(S,T) = e(T,S)^{-1}$$
für $S, T \in E[m]$.
3. *Verträglichkeit mit der Galoisoperation von* $G_{\bar{K}|K}$*:*
$$e(S,T)^\sigma = e(S^\sigma, T^\sigma) \tag{11}$$
für $\sigma \in G_{\bar{K}|K}$ *und* $S, T \in E[m]$.

Beweis. 1. Es ist zunächst

$$e(S+S',T) = g_T(X+S+S')/g_T(X) = \\ = \left(g_T(X+S+S')/g_T(X+S)\right)\left(g_T(X+S)/g_T(X)\right) = e(S',T)e(S,T)$$

denn es ist $g_T(X+S+S')/g_T(X+S) = g_T(Y+S')/g_T(Y) = e(S',T)$.
Weiterhin ist $g_{T+T'}(X)$ definiert durch den Divisor

$$\sum_{W\in E[m]} [\tilde{T}+\tilde{T}'+W] - \sum_{W\in E[m]} [W] = \\ \left(\sum_W [\tilde{T}+\tilde{T}'+W] - \sum_W [\tilde{T}'+W]\right) + \left(\sum_W [\tilde{T}'+W] - \sum_W [W]\right)$$

für $[m]\tilde{T} = T$ und $[m]\tilde{T}' = T'$. Das ist aber der Divisor von $g_T(X-\tilde{T}')g_{T'}(X)$, also gilt

$$g_{T+T'}(X) = c\, g_T(X-\tilde{T}')g_{T'}(X)$$

und somit

$$e(S,T+T') = g_{T+T'}(X+S)/g_{T+T'}(X) =$$
$$= g_T(X-\tilde{T}'+S)/g_T(X-\tilde{T}')g_{T'}(X+S)/g_{T'}(X) = e(S,T)e(S,T').$$

2. Es gilt nach 1.

$$e(S+T,S+T) = e(S,S)e(S,T)e(T,S)e(T,T).$$

Also genügt es zu zeigen, daß $e(T,T)=1$ für alle $T \in E[m]$ ist.
Betrachte die Funktion

$$w(X) = g(X)g(X+T')\cdot\cdots\cdot g(X+(m-1)T')$$

mit $g(X) = g_T(X)$ und $[m]T' = T$. Es ist

$$w(X)^m = f_T(mX)f_T(mX+T)\cdot\cdots\cdot f_T(mX+(m-1)T)$$

Nun ist aber mit $v(y) = f_T(y)f_T(y+T)\cdot\cdots\cdot f_T(y+(m-1)T)$ auch

$$\operatorname{div} v = \sum_{i=0}^{m-1}(X+iT)^*(m([T]-[0])) = m\sum_{i=0}^{m-1}([(1-i)T]-[-iT]) = 0$$

Also ist $v(y) = c$ konstant, also $w(X)^m = v([m]X) = c$ ebenfalls konstant. Damit ist auch $w(X)$ konstant und wir haben

$$w(X) = w(X+T').$$

Streicht man die rechts und links gleichen Terme $g(X+iT')$ so entsteht $g(X) = g(X+T)$, also $e(T,T)=1$, was zu beweisen war.