ELLIPTISCHE KURVEN

Grundlagen

Eine *elliptische Kurve* ist eine reguläre algebraische Kurve vom *Geschlecht* 1, also ein 1-dimensionales reguläres, integres, eigentliches Schema E vom endlichen Typ über einem Körper k.
Es ist also $\deg K = 2g-2 = 0$ für den kanonischen Divisor K auf E und

$$\dim \Gamma(E, \mathcal{O}_E(D)) = \deg D$$

für jeden Divisor mit $\deg D > 0$.
Wählt man einen Punkt $P \in E$ fest und betrachtet die Divisoren $\mathcal{O}_E(nP)$, so kann man rationale Funktionen $x, y \in K(E)$ wählen, so daß $1, x$ die Schnitte von $\mathcal{O}_E(2P)$ und $1, x, y$ die Schnitte von $\mathcal{O}_E(3P)$ erzeugen.
Es hat also x einen Pol der Ordnung 2 in P und y einen Pol der Ordnung 3. Da $\dim \mathcal{O}_E(6P) = 6$, besteht zwischen den 7 Funktionen $1, x, y, x^2, xy, x^3, y^2$ nach Skalierung von x und y eine Relation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{1}$$

die mit $\mathrm{wt}(a_i) = i$ und $\mathrm{wt}(x) = 2$ sowie $\mathrm{wt}(y) = 3$ homogen vom Gewicht 6 ist und *Weierstraßgleichung* heißt.

Proposition 0.1. *Die Abbildung $\phi : E \to \mathbb{P}^2_k$ mit $\phi(P) = (x(P) : y(P) : 1)$ ist eine abgeschlossene Immersion.*

Beweis. Es ist $\dim \mathcal{O}_E(3P-Q) = 2$ und $\dim \mathcal{O}_E(3P-Q-R) = 1$. Das Linearsystem $[1, x, y]$ trennt also Punkte und Tangentenvektoren und vermittelt daher eine abgeschlossene Immersion.
Alle Punkte von E liegen in $D_+(Z)$ bis auf den Punkt $O = (0:1:0)$, der oft als ausgezeichneter Punkt von $E = (E, O)$ dient.
Ist $\mathrm{char}\, k \neq 2, 3$ so kann man mit $y \mapsto y + 1/2\, a_1 x$ den Koeffizienten a_1 und danach mit $y \mapsto y + 1/2\, a_3$ den Koeffizienten a_3 beseitigen. Mit $x \mapsto x + 1/3\, a_2$ beseitigt man dann a_2 und erhält die *(spezielle) Weierstraßform von $E = E(x, y, a, b)$* mit

$$y^2 = x^3 + ax + b = f(x), \quad E \to \mathbb{P}^2_k, \quad P \mapsto (x(P) : y(P) : 1) \tag{2}$$

Eine durch diese Form beschriebene kubische Kurve ist regulär, also eine elliptische Kurve, wenn

$$\mathrm{disc}\, f = 4a^3 + 27b^2$$

nicht verschwindet. Wir schreiben

$$\Delta = \mathrm{disc}\, f = (4a^3 + 27b^2).$$

Für die Kubik E, die durch (2) beschrieben wird, gilt

Proposition 0.2. *Hat $f(x)$*

- *a) zwei verschiedene Nullstellen, so ist E eine* nodale Kubik *mit einem Knoten als Singularität am Ort der doppelten Nullstelle. Jede dieser E ist biregulär zu $y^2 = x^3 + a^2 x^2$.*
- *b) eine Nullstelle, so ist E* cuspidal *und hat eine Spitze am Ort der dreifachen Nullstelle. E ist biregulär zu $y^2 = x^3$.*

Die nodale Kubik ist birational zu $\mathbb{G}_m$, die cuspidale zu $\mathbb{G}_a$.
Beweis. Es sei $y^2 = x^3 + a^2 x^2$. Man projiziert E mit $\rho = (y + ax)/(y - ax)$ auf $\mathbb{P}^1 - \{0, \infty\}$. Schneidet man E mit der Geraden L, gegeben durch $px + qy + r = 0$, so gelten für x, y, ρ drei Gleichungen. Man eliminiert x, y und erhält eine Kubik $A\rho^3 + B\rho^2 + C\rho + D = 0$ für die $D/A = -1$ ist. Also $\rho_1\rho_2\rho_3 = 1$, für die drei Werte ρ_1, ρ_2, ρ_3, die den drei Schnittpunkten von L mit E entsprechen.

Im Fall der cuspidalen Kubik $y^2 = x^3$ benutzen wir denselben Ansatz für L und setzen $\rho = x/y$. Die Eliminationskubik in ρ hat keinen ρ^2-Term, also ist $\rho_1 + \rho_2 + \rho_3 = 0$.

Die Gleichung (2) geht durch

$$y \mapsto u^3 y, \quad x \mapsto u^2 x \tag{3}$$

in

$$y^2 = x^3 + a\, u^{-4} x + b\, u^{-6}$$

über, also (a, b) in $(u^{-4}a, u^{-6}b)$, also Δ in $u^{-12}\Delta$. Der Ausdruck

$$j = 1728 \frac{4a^3}{4a^3 + 27b^2} = 1728 \frac{4a^3}{\Delta}$$

geht also in sich über (die Zahlenkoeffizienten sind so gewählt, damit die Kurve mit $b = 0$ die j-Invariante 1728 erhält).
Sind $E_1 = E(x, y, a, b)$ und $E_2 = E(x', y', a', b')$ zwei über k isomorphe elliptische Kurven, so kann man annehmen, daß für $\phi : E_1 \xrightarrow{\sim} E_2$ auch $\phi(O) = O$ ist. Identifiziert man so $E_1 = E_2 = X$, so sind x, y, x', y' rationale Funktionen auf X mit x, x' von der Ordnung 2 und y, y' von der Ordnung 3 in O.
Also

$$x' = px + q \tag{4}$$

$$y' = ry + sx + t \tag{5}$$

Da aber x, y und x', y' beide der Weierstraßform genügen, muss $p = u^2$ und $r = u^3$ sowie $q = s = t = 0$ sein. Es ist also $j_{E_1} = j_{E_2}$.
Umgekehrt, ist $j_{E_1} = j_{E_2}$, so folgt aus $a = u^4 a'$ und $b = v^6 b'$ und $j \neq 0, 1728$, daß $v = \zeta u$ mit $\zeta^{12} = 1$ ist. Also kann man immer ein u wählen, für das $a = u^4 a'$ und $b = u^6 b'$ ist.
Also $x' = u^2 x$ und $y' = u^3 y$ und $E_1 \cong E_2$ über dem algebraischen Abschluß $\bar{k}$.

Gruppenstruktur

Theorem 0.1. *Die Abbildung $\Phi : E \to \mathrm{Pic}^0(E)$ mit $P \mapsto P - O$ ist eine Bijektion von abgeschlossenen Punkten von E in Divisoren vom Grad Null.*

Beweis. *Injektivität:* Ist $P - O \sim Q - O$, so ist $P - Q = (f)$, was aber für $P \neq Q$ ausgeschlossen ist, da kein f nur einen Pol haben kann.
Surjektivität: Betrachte $D = P - Q + O$. Es gibt ein (f) mit $(f) + D \geqslant 0$, also mit $(f) = -P + Q - O + T$. Beachte, daß kein f nur einen Pol haben kann. Also ist $P - Q \sim T - O$ und damit $\sum_{i=1}^s P_i - \sum_{i=}^s Q_i = \sum_{i=1}^s S_i - sO$. Weiter ist mit $D = S_1 + S_2 - O$ und $(g) + D \geqslant 0$ auch $(g) = T + O - S_1 - S_2$, also $S_1 + S_2 \sim T + O$. Also induktiv $\sum_{i=1}^s S_i - sO \sim S - O$ und Φ ist surjektiv.

Wir können also mit $\Phi(P \oplus Q) = \Phi(P) + \Phi(Q)$ die Gruppenstruktur von $\mathrm{Pic}^0 E$ auf $(E, \oplus)$ übertragen. Das Nullelement ist dann der Punkt O.

Korollar 0.1 (Abel)**.** *Für einen Divisor $D = \sum n_i P_i$ auf E ist $D = (f)$ genau dann, wenn $\sum_i n_i = 0$ und $\sum n_i P_i = O$ wobei diese letzte Summe in E zu nehmen ist.*

Liegen $P, Q, R \in E$ auf einer Geraden l und ist m die dreifache Wendetangente an O, so ist $(l/m) = P + Q + R - 3O$. Es gilt also

Proposition 0.3. *Drei Punkte $P, Q, R \in E$ liegen genau dann auf einer Geraden, wenn $P \oplus Q \oplus R = O$ ist.*

Ist $P, Q \in E$, so ist Q der Schnittpunkt der Tangenten t an E in P, genau dann, wenn $2P + Q = O$ in E. Die Beziehung $3P = 0$ ist genau dann erfüllt, wenn P ein Wendepunkt von E ist.

Isogenien

Definition 0.1. *Ein Morphismus $f : E_1 \to E_2$ mit $f(0_{E_1}) = 0_{E_2}$ heißt* Isogenie von E_1 nach E_2

Proposition 0.4. *Für Isogenien gilt*

- *a) Die Isogenien bilden eine abelsche Gruppe* $\mathrm{Hom}(E_1, E_2)$ *mit $(f+g)(P) = f(P) + g(P)$ und $(-f)(P) = -f(P)$.*
- *b) Jedes $m \in \mathbb{Z}$ induziert ein $[m] = m \cdot \mathrm{id}_E \in \mathrm{Hom}(E, E)$. Es ist kein $[m]$ mit $m \neq 0$ konstant.*
- *c) Die Gruppe* $\mathrm{Hom}(E_1, E_2)$ *ist ein* torsionsfreier $\mathbb{Z}$*-Modul, die Gruppe* $\mathrm{End}(E, E)$ *ein* nullteilerfreier Ring.

Jeder Morphismus $f : E_1 \to E_2$ kann also als $f = f_1 \circ t_Q$ mit einer Isogenie f_1 und einer *Translation* t_Q mit $t_Q(P) = Q + P$ geschrieben werden.

Theorem 0.2. *Eine Isogenie $f : E_1 \to E_2$ ist ein Gruppenhomomorphismus: $f(P_1 + P_2) = f(P_1) + f(P_2)$.*

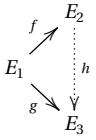
Beweis. Betrachte die Abbildung $h : E_1 \times E_1 \to E_2$ mit $h(P, Q) = f(P+Q) - f(P) - f(Q)$. Sie nimmt auf $E_1 \times 0$ und $0 \times E_1$ den Wert 0_{E_2} an. Nach dem Rigidity-Lemma ist sie deshalb konstant. (Eine Abbildung $a : X \times T \to V$ mit $a(x_0 \times T) = a(X \times t_0) = v_0$ für ein $t_0 \in T$ und ein $x_0 \in X$ ist für eine eigentliche Varietät X konstant gleich v_0).

Proposition 0.5. *Ist $f : E_1 \to E_2$ eine Isogenie, so ist $N = \ker f = \{P \in E_1 \mid f(P) = 0\}$ eine endliche Untergruppe.*

Proposition 0.6. *Die Isogenie $f : E_1 \to E_2$ induziert eine Inklusion $K(E_2) \subseteq K(E_1') \subseteq K(E_1)$ in der die erste Inklusion* separabel *und die zweite* rein inseparabel *ist.*

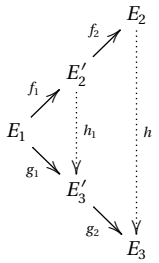
- *a) Es ist $\deg_s f = \#\ker f$ und $f = f_1 \circ \phi$ mit $\phi : E_1 \to E_1'$ rein inseparabel $\deg_i \phi = \deg_i f$ und $f_1 : E_1' \to E_2$ separabel mit $\deg f_1 = \deg_s f$.*
- *b) Die Punkte von E_1 sind über E_1' von der Ordnung $e = e_\phi = \deg \phi$ verzweigt und über jedem Punkt von E_2 liegen $\#\ker f$ verschiedene Punkte von E_1'.*
- *c) Ist $f : E_1 \to E_2$ separabel, so ist die Erweiterung $K(E_1)/K(E_2)$ galoissch mit $\mathrm{Gal}(K(E_1) : K(E_2)) \cong N = \ker f$. Die Operation von $Q \in N$ ist $\alpha^Q = t_Q^*(\alpha)$ also von einer Translation erzeugt.*

Proposition 0.7. *Im Diagramm*



in $\ker f \subseteq \ker g$ ist, findet sich immer eine passende Isogenie h.

Beweis. Der Graph Γ_h von h ist gleich dem schematheoretischen Bild von $\theta : E_1 \to E_2 \times E_3$ mit $\theta : P \mapsto (f(P), g(P))$. Aus $f(P_1) = f(P_2)$ folgt ja $g(P_1) = g(P_2)$ und weil alle Schemata reduziert und noethersch sind, sowie θ eigentlich, ist Γ_h die Menge $\theta(E_1)$ mit der reduzierten induzierten Unterschemastruktur.
Weiter ist $w : \Gamma_h \to E_2$ wegen $w = p_1 \circ i$ eigentlich, surjektiv und injektiv, also nach Zariskis Hauptsatz endlich mit genau einem Punkt in den Fasern. Definiert man $v : E_1 \to \Gamma_h$ mit $iv = f \times g$ so ist $f = wv$ und damit w separabel, also ein Isomorphismus, wenn f separabel ist.
Wir können auf f separabel verzichten: In dem Diagramm



sei $f = f_2 f_1$ und $g = g_2 g_1$ und f_1, g_1 seien die inseparablen Anteile. Weiter sei $\ker f \subseteq \ker g$, aufgefaßt als endliche Gruppenschemata, in denen die Punkte aus $\ker f$ die Multiplizität $\deg_i f$ und die aus $\ker g$ die Multiplizität $\deg_i g$ tragen. Damit ist die Existenz von h_1 gesichert als $h_1 = F^m$ mit $p^m = \deg_i g_1 / \deg_i f_1$ und damit nach vorigem auch die von h.

Proposition 0.8. *Ist $N \subseteq E$ eine endliche Untergruppe, so gibt es eine separable Isogenie $f : E \to E'$ mit $\ker f = N$. (Man schreibt auch manchmal E/N für E'.)*

Duale Isogenie

Definition 0.2. *Es sei $f : E_1 \to E_2$ eine Isogenie elliptischer Kurven. Das Diagramm*

$$\begin{array}{ccc} \mathrm{Pic}^0(E_1) & \xleftarrow{\Phi_{E_1}} & E_1 \\ {\scriptstyle f^*}\uparrow & & \uparrow{\scriptstyle \hat{f}} \\ \mathrm{Pic}^0(E_2) & \xleftarrow[\Phi_{E_2}]{} & E_2 \end{array} \tag{6}$$

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

Wohldefiniertheit: Wegen $\widehat{f} \circ f = [n]$ folgt dies aus Proposition 0.7 für $E_3 = E_1$ und $g = [n]$.

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

$$\mu : E \times_k E \to E \tag{7}$$

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*

$$\mathscr{L} \in \mathrm{Pic}^0(E) \tag{8}$$

Dann gilt mit obigen Bezeichnungen die Beziehung

$$\mu^*\mathscr{L} = p_1^*\mathscr{L} \otimes p_2^*\mathscr{L} \tag{9}$$

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

$$\left(\mu^*\mathscr{L} \otimes (p_1^*\mathscr{L})^{-1}\right)|_{E\times P} \cong \mathscr{O}_{E\times P} \tag{10}$$

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

$$D = \sum_i n_i P_i, \quad \sum_i n_i = 0 \tag{11}$$

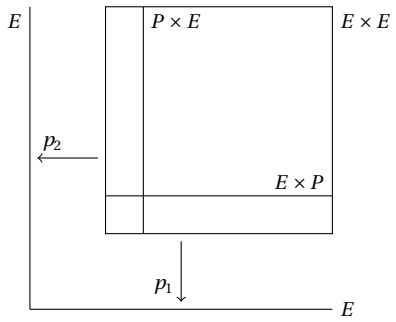
Damit ist $\tau_P^*(D) = \sum_i n_i(P_i - P) \sim \sum_i n_i P_i = D$. Also ist $\tau_P^*\mathscr{L} = \mathscr{L}$ auf E und damit $\left(\mu^*\mathscr{L} \otimes (p_1^*\mathscr{L})^{-1}\right)|_{E\times P} = \mathscr{O}_{E\times P}$ wie behauptet.
Nach den Halbstetigkeitssätzen ist dann

$$\mu^*\mathscr{L} \otimes \left(p_1^*\mathscr{L}\right)^{-1} = p_2^*\mathscr{N} \tag{12}$$

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

$$\mu^*\mathscr{L} \otimes \left(p_1^*\mathscr{L}\right)^{-1} = p_2^*\mathscr{L} \tag{13}$$

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



Proposition 0.9. *Es seien* $f, g : E_1 \to E_2$ *zwei Isogenien. Dann ist*

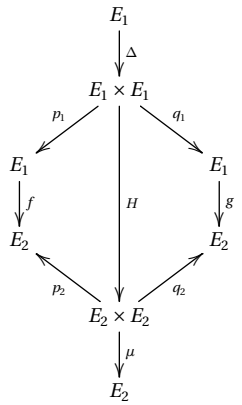
$$(f+g)\widehat{\ } = \widehat{f} + \widehat{g}$$

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

(14)



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 0.3. *Die Abbildung*

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

ist die sogenannte Weilpaarung.

Proposition 0.10. *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* $G_{\bar{K}|K}$*:*
$$e(S,T)^\sigma = e(S^\sigma, T^\sigma) \tag{15}$$
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

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

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.