**Prof. Dr. H. Brenner** **Osnabrück WS 2021/2023**

# Elliptische Kurven

## Vorlesung 24

### Die Zeta-Funktion

Es sei $X$ eine Varietät, die über dem endlichen Körper $\mathbb{F}_q$ mit $q$ Elementen definiert sei. Diese Varietät besitzt endlich viele Punkte, die über $\mathbb{F}_q$ definiert sind. Nennen wir diese Anzahl $N_1$. Aufgrund der Körpererweiterung $\mathbb{F}_q \subseteq \mathbb{F}_{q^r}$ (siehe Korollar 16.10 (Körper- und Galoistheorie (Osnabrück 2018-2019))) kann man $X$ auch über $\mathbb{F}_{q^r}$ auffassen und dessen Punkteanzahl, nennen wir sie $N_r$, bestimmen. Wenn $X$ in einem affinen oder projektiven Raum durch Gleichungen beschrieben wird, so kann man direkt die Gleichungen über $\mathbb{F}_{q^r}$ auffassen und die Punkte zählen, deren Koordinaten zu $\mathbb{F}_{q^r}$ gehören. Wenn $X$ nicht eingebettet vorliegt, so muss man $X \times_{\mathbb{F}_q} \mathbb{F}_{q^r}$ betrachten und dort die Anzahl der Punkte mit Restekörper $\mathbb{F}_{q^r}$ bestimmen. Eine faszinierende Frage ist nun, ob es bei den Anzahlen $N_1, N_2, \ldots$ Gesetzmäßigkeiten gibt, und wie diese mit weiteren Eigenschaften von $X$ zusammenhängen. Die Suche nach diesen Gesetzmäßigkeiten war eine treibende Kraft in der Entwicklung der algebraischen Geometrie in der zweiten Hälfte des 20.sten Jahrhunderts (Weil, Grothendieck, Deligne). Es ist auf den ersten Blick überraschend, dass die folgende formale Funktion der richtige Ansatz ist, die Teilinformationen der $N_r$ in ein einziges analytisches (funktionentheoretisches) Objekt zusammenzufassen.

Definition 24.1. Es sei $X$ eine Varietät über einem endlichen Körper $\mathbb{F}_q$ und es bezeichne $N_r$ die Anzahl der Punkte von $X(\mathbb{F}_{q^r})$. Dann nennt man

$$Z(t) \, = \, Z(X;t) \, = \, \exp\left( \sum_{r=1}^{\infty} N_r \frac{t^r}{r} \right)$$

die *Zeta-Funktion* von $X$.

Genauer spricht man von der Weilschen Zeta-Funktion. Formal handelt es sich einfach um eine Potenzreihe in $t$ mit rationalen Koeffizienten. Aufgrund der Definition der Exponentialreihe handelt es sich um die Reihe

$$1 + \left( N_1 t + N_2 \frac{t^2}{2} + N_3 \frac{t^3}{3} + \ldots \right) + \frac{1}{2} \left( N_1 t + N_2 \frac{t^2}{2} + N_3 \frac{t^3}{3} + \ldots \right)^2 + \frac{1}{6} \left( N_1 t + N_2 \frac{t^2}{2} + N_3 \frac{t^3}{3} + \ldots \right)^3 + \ldots .$$

Beispiel 24.2. Der $n$-dimensionale projektive Raum $\mathbb{P}^n_{\mathbb{F}_q}$ über dem endlichen Körper $\mathbb{F}_q$ besitzt $1+q+q^2+\cdots+q^n$ Elemente, siehe Aufgabe 3.11, somit ist

$$N_r \;=\; 1+q^r+q^{2r}+\cdots+q^{rn}.$$

Es ist

$$Z(t) \;=\; \frac{1}{(1-t)(1-qt)(1-q^2t)\cdots(1-q^nt)}.$$

Dies bestätigt man, indem man beidseitig den Logarithmus anwendet. Es ist also

$$\sum_{r=1}^{\infty} N_r \frac{t^r}{r} \;=\; \sum_{r=1}^{\infty}(1+q^r+q^{2r}+\cdots+q^{rn})\frac{t^r}{r} \;=\; \sum_{i=0}^{n} \ln \frac{1}{1-q^it}$$

zu zeigen. Mit der Logarithmusreihe ist aber für jedes $i$

$$\ln \frac{1}{1-q^it} \;=\; -\ln\left(1-q^it\right) \;=\; -\sum_{r=1}^{\infty}(-1)^{r+1}\frac{(-q^it)^r}{r} \;=\; \sum_{r=1}^{\infty} q^{ir}\frac{t^r}{r}.$$

Das Ergebnis im vorstehenden Beispiel ist typisch und zeigt bereits die Stärke und Prägnanz der Zeta-Funktion: Sie ist für eine glatte projektive Varietät $X$ stets eine rationale Funktion in $t$. Wenn $n$ die Dimension von $X$ ist, so gibt es ganzzahlige Polynome $P_i(t)$ für $0 \leq i \leq 2n$ mit

$$Z(t) \;=\; \frac{P_1(t)\cdot P_3(t)\cdot P_5(t)\cdots P_{2n-1}(t)}{P_0(t)\cdot P_2(t)\cdot P_4(t)\cdots P_{2n}(t)}.$$

Diese starke Aussage beinhaltet insbesondere die keineswegs selbstverständliche Aussage, dass endlich viele der Anzahlen $N_r$ bereits alle Anzahlen bestimmen.

In die Zeta-Funktion zu einer Varietät über $\mathbb{F}_q$ wird für $t$ oft $q^{-s}$ eingesetzt, wobei $s$ eine komplexe Variable (typischerweise mit einer Beschränkung durch den Realteil) ist, wodurch dann eine Funktion in $s$ entsteht.

## Die Zeta-Funktion einer elliptischen Kurve

Im Falle einer glatten projektiven Kurve hat die Zeta-Funktion die Gestalt

$$Z(t) \;=\; \frac{P_1(t)}{(1-t)(1-qt)}$$

und das Zählerpolynom $P_1(t)$ ist ein Polynom vom Grad $2g$, wenn $g$ das Geschlecht der Kurve bezeichnet. Im Fall einer elliptischen Kurve werden wir dieses Zählerpolynom vom Grad 2 bestimmen.

Satz 24.3. *Es sei $E$ eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$, $q=p^e$, mit $N_1 = \#\left(E(\mathbb{F}_q)\right)$ und es sei $\ell$ eine von der Charakteristik von $\mathbb{F}_q$ verschiedene Primzahl. Es sei*

$$\Phi\colon\; E_{\overline{K}} \longrightarrow E_{\overline{K}}$$

*der e-te $\overline{K}$-lineare Frobenius auf $E_{\overline{K}}$ und $\Phi_\ell\colon T_\ell(E) \to T_\ell(E)$ die zugehörige Abbildung auf dem $\ell$-adischen Tate-Modul. Dann gelten folgende Aussagen.*

(1) *Das charakteristische Polynom von $\Phi_\ell$ ist*
$$T^2 - (q+1-N_1)T + q\,.$$
(2) *Dieses Polynom ist als reelles Polynom nichtnegativ.*
(3) *Die komplexen Nullstellen $\alpha$ und $\beta$ des charakteristischen Polynoms sind zueinander komplex-konjugiert und ihr Betrag ist $\sqrt{q}$.*
(4) *Das charakteristische Polynom von $\Phi_\ell^n$ ist*
$$(T-\alpha^n)(T-\beta^n) \;=\; T^2 - (\alpha^n+\beta^n)T + \alpha^n\beta^n.$$
(5) *Die Anzahl der Punkte von $E$ über $\mathbb{F}_{q^n}$ ist*
$$\#\left(E(\mathbb{F}_{q^n})\right) \;=\; q^n + 1 - \alpha^n - \beta^n.$$

*Beweis.* (1) Wir ziehen Satz 18.14 heran. Es ist
$$\det\left(\Phi_\ell\right) \;=\; \mathrm{Grad}\left(\Phi\right) \;=\; q$$
nach Lemma 23.1. Es ist
$$\mathrm{Spur}\left(\Phi_\ell\right) \;=\; 1 + \mathrm{Grad}\left(\Phi\right) - \mathrm{Grad}\left(\mathrm{Id}_E - \Phi\right) \;=\; 1 + q - N_1$$
unter Verwendung von Lemma 23.6. Daraus ergibt sich das charakteristische Polynom von $\Phi_\ell$ zu
$$T^2 - (q+1-N_1)T + q \;=\; T^2 + (N_1 - q - 1)T + q.$$

(2) Die Nichtnegativität des Polynoms kann man wegen der Stetigkeit mit rationalen Zahlen testen. Sei also $\frac{r}{s}$ eine rationale Zahl. Der Wert des charakteristischen Polynoms an der Stelle $\frac{r}{s}$ ist
$$\begin{aligned}
\det\left(T\,\mathrm{Id}_{T_\ell(E)} - \Phi_\ell\right)\left(\frac{r}{s}\right) &= \det\left(\frac{r}{s}\,\mathrm{Id}_{T_\ell(E)} - \Phi_\ell\right) \\
&= \frac{1}{s^2}\det\left(r\,\mathrm{Id}_{T_\ell(E)} - s\Phi_\ell\right) \\
&= \frac{1}{s^2}\,\mathrm{Grad}\left([r] - s\Phi\right) \\
&\geq 0.
\end{aligned}$$

(3) Nach (2) besitzt das charakteristische Polynom entweder eine doppelte reelle Nullstelle oder zwei nicht reelle zueinander komplex-konjugierte Nullstellen. So oder so ist ihr Betrag gleich, und wegen
$$\alpha\beta \;=\; q$$
ergibt sich $|\alpha| \;=\; |\beta| \;=\; \sqrt{q}$.

(4) Das charakteristische Polynom zu $\Phi_\ell$ kann man über $\mathbb{C}$ als $(X-\alpha)(T-\beta)$ schreiben. Eine solche Zerlegung hat man auch über dem algebraischen Abschluss von
$$Q(\hat{\mathbb{Z}}_\ell) \;=\; \mathbb{Q}_\ell$$

(bzw. schon in einer quadratischen Erweiterung von $\mathbb{Q}_\ell$). Dabei sind $\alpha, \beta$ (genauer $\alpha_\ell, \beta_\ell$) die Eigenwerte von $\Phi_\ell$. Somit sind $\alpha^n, \beta^n$ die Eigenwerte von $\Phi_\ell^n$ und das charakteristische Polynom zu $\Phi_\ell^n$ ist $(T-\alpha^n)(T-\beta^n)$. Die entstehenden Polynome haben wieder ganzzahlige Koeffizienten, daher ist es egal, ob man über $\mathbb{C}$ oder über $\overline{\mathbb{Q}_\ell}$ arbeitet.

(5) Die Anzahl der Punkte von $E$ über $\mathbb{F}_{q^n}$ ist unter Verwendung von Lemma 23.6 und Satz 18.14 gleich

$$\begin{aligned} \#\left(E(\mathbb{F}_{q^n})\right) &= \operatorname{Grad}\left(\operatorname{Id}_E - \Phi^n\right) \\ &= \det\left(\operatorname{Id}_{T_\ell(E)} - \Phi_\ell^n\right) \\ &= 1 + \det\left(\Phi_\ell^n\right) - \operatorname{Spur}\left(\Phi_\ell^n\right) \\ &= 1 + q^n - \alpha^n - \beta^n. \end{aligned}$$

□

Satz 24.4. *Es sei $E$ eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$ mit $N_1 = \#\left(E(\mathbb{F}_q)\right)$. Dann gilt für die Zeta-Funktion*

$$Z(E;t) = \frac{1 + (N_1 - q - 1)t + qt^2}{(1-t)(1-qt)}.$$

*Beweis.* Wir betrachten den Ausdruck $\sum_{r=1}^{\infty} N_r \frac{t^r}{r}$, wobei

$$N_r = \#\left(E(\mathbb{F}_{q^r})\right)$$

bezeichne. Nach Satz 24.3 (5) wissen wir

$$N_r = 1 + q^r - \alpha^r - \beta^r,$$

wobei $\alpha$ und $\beta$ die Nullstellen des charakteristischen Polynoms zu $\Phi_\ell$ sind (für eine zur Charakteristik teilerfremde Primzahl $\ell$). Es ist also

$$\begin{aligned} \sum_{r=1}^{\infty} N_r \frac{t^r}{r} &= \sum_{r=1}^{\infty} (1 + q^r - \alpha^r - \beta^r)\frac{t^r}{r} \\ &= \sum_{r=1}^{\infty} \frac{t^r}{r} + \sum_{r=1}^{\infty} \frac{(qt)^r}{r} - \sum_{r=1}^{\infty} \frac{(\alpha t)^r}{r} - \sum_{r=1}^{\infty} \frac{(\beta t)^r}{r} \\ &= -\ln(1-t) - \ln(1-qt) + \ln(1-\alpha t) + \ln(1-\beta t), \end{aligned}$$

wobei wir die Logarithmusreihe verwendet haben. Wenn wir auf diese Gleichung die Exponentialreihe anwenden, so erhalten wir

$$\begin{aligned} Z(E;t) &= \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right) \\ &= \frac{(1-\alpha t)(1-\beta t)}{(1-t)(1-qt)} \\ &= \frac{(1-(\alpha+\beta)t + \alpha\beta t^2}{(1-t)(1-qt)} \\ &= \frac{(1 + (N_1 - q - 1)t + qt^2}{(1-t)(1-qt)}, \end{aligned}$$

wobei wir im letzten Schritt die definierenden Eigenschaften von $\alpha$ und $\beta$ und Satz 24.3 (1) verwendet haben. □

Satz 24.5. *Es sei $E$ eine elliptische Kurve über dem endlichen Körper $\mathbb{F}_q$. Dann erfüllt die Zeta-Funktion $Z(E;t)$ von $E$ die Funktionalgleichung*

$$Z(E;\frac{1}{qt}) \ = \ Z(E;t).$$

*Beweis.* Dies ergibt sich aus Satz 24.4 durch die Umformungen

$$\begin{aligned} Z(E;\frac{1}{qt}) &= \frac{1+(N_1-q-1)\frac{1}{qt}+q\left(\frac{1}{qt}\right)^2}{\left(1-\frac{1}{qt}\right)\left(1-q\frac{1}{qt}\right)} \\ &= \frac{(qt)^2+(N_1-q-1)qt+q}{(qt-1)(qt-q)} \\ &= \frac{q(1+(N_1-q-1)t+qt^2)}{q(1-t)(1-qt)} \\ &= \frac{1+(N_1-q-1)t+qt^2}{(1-t)(1-qt)} \\ &= Z(E;t). \end{aligned}$$

□

Beispiel 24.6. Wir betrachten über dem endlichen Körper $\mathbb{Z}/(5)$ die elliptische Kurve $E$, die durch

$$y^2 \ = \ x^3+1$$

gegeben ist. Sie besitzt nach Beispiel 23.11 sechs Elemente, also $N_1 = 6$. Das charakteristische Polynom der Darstellung des Frobenius auf dem Tate-Modul ist nach Satz 24.3 gleich

$$T^2+5 \ = \ (T-\sqrt{5}\mathrm{i})(T+\sqrt{5}\mathrm{i}),$$

also $\alpha, \beta = \pm\sqrt{5}\mathrm{i}$ in der Notation von Satz 24.3. Die Anzahl der Punkte von $E$ über $\mathbb{F}_{5^n}$ ist

$$\#\left(E(\mathbb{F}_{q^n})\right) \ = \ 5^n+1-(-\sqrt{5})^n\mathrm{i}^n-\sqrt{5}^n\mathrm{i}^n \ = \ 5^n+1-((-1)^n+1)\sqrt{5}^n\mathrm{i}^n.$$

Für $n$ ungerade ist also die Anzahl gleich $5^n+1$. Für $n = 2 \mod 4$ ist die Anzahl gleich $5^n+1+2\cdot 5^{n/2}$ und für $n = 0 \mod 4$ ist die Anzahl gleich $5^n+1-2\cdot 5^{n/2}$. Für gerades $n$ wird also die Hasse-Schranke ausgeschöpft. Die Zeta-Funktion von $E$ ist nach Satz 24.4 gleich

$$Z(E;t) \ = \ \frac{1+5t^2}{(1-t)(1-5t)}.$$

Bemerkung 24.7. Es sei eine ebene glatte projektive Kurve

$$C \ = \ V_+(F) \ \subseteq \ \mathbb{P}^2_{\mathbb{Z}/(p)}$$

durch eine Gleichung der Form

$$X^d \ = \ P(Y,Z)$$

gegeben, wobei $P(Y,Z)$ ein homogenes Polynom vom Grad $d$ sei. Es sei $q = p^n$ eine Potenz der Charakteristik $p$. Wenn der Grad $d$ teilerfremd zu $q-1$ ist, so lässt sich die Anzahl $\#\left(C(\mathbb{F}_q)\right)$ der Punkte der Kurve, die über $\mathbb{F}_q$ definiert sind, einfach bestimmen. Sei $(x,y,z) \in C$ ein solcher Punkt. Bei $z \neq 0$ können wir $z$ zu 1 normieren. Für $y$ können wir jedes Element aus $\mathbb{F}_q$ einsetzen. Aufgrund der vorausgesetzten Teilerfremdheit ist die Abbildung

$$\mathbb{F}_q \longrightarrow \mathbb{F}_q,\, x \longmapsto x^d,$$

bijektiv, da diese Abbildung auf $\mathbb{F}_q^\times$ der additiven Abbildung

$$\mathbb{Z}/(q-1) \longrightarrow \mathbb{Z}/(q-1),\, v \longmapsto dv,$$

entspricht (vergleiche Aufgabe 17.16 (Algebraische Zahlentheorie (Osnabrück 2020-2021))). Somit gehört zu $y$ genau ein Punkt der Kurve. Bei $z = 0$ ist $y \neq 0$ und man kann $y$ zu 1 normieren und erhält einen weiteren Punkt der Kurve. Unter dieser Bedingung ist also

$$\#\left(C(\mathbb{F}_q)\right) = q+1.$$

Wenn aber $q-1$ nicht teilerfremd zu $d$ ist, wird die Bestimmung ungleich schwieriger, da man dann im Detail untersuchen muss, welche Zahlen $P(y,1)$ wie viele $d$-te Wurzeln in $\mathbb{F}_q$ besitzen. Da im glatten Fall $p$ und $d$ teilerfremd sind, ist $p$ eine Einheit modulo $d$ und somit gibt es Exponenten $e$ mit $p^e = 1 \bmod d$. Das heißt, dass $p^e - 1$ und $d$ für gewisse Exponenten nicht teilerfremd sind, und daher (außer bei $d = 1$) der schwierige Fall definitiv eintritt.

Bemerkung 24.8. Es sei $X$ eine glatte projektive Varietät über einem endlichen Körper $K = \mathbb{F}_q$, es sei $N_r$ die Anzahl der $\mathbb{F}_{q^r}$-rationalen Punkte Punkte von $X$ mit der zugehörigen Zeta-Funktion

$$Z(t) = \exp\left(\sum_{r=1}^{\infty} N_r \frac{t^r}{r}\right).$$

André Weil formulierte 1949 eine Reihe von Vermutungen über das Verhalten dieser Funktion und damit der Anzahlen $N_r$, die er selbst für Kurven bewies. Diese Vermutungen motivierten Alexander Grothendieck zur Einführung der étalen bzw. der $\ell$-adischen Kohomologie (die Tate-Moduln kann man als $\ell$-adische Homologiegruppen ansehen), mit deren Hilfe 1973 Pierre Deligne letztlich die Vermutungen bestätigte. Die wichtigsten allgemeinen Resultate, die wir im elliptischen Fall gezeigt haben, sind die folgenden.

(1) Es gibt ganzzahlige Polynome $P_i(t)$ für $0 \leq i \leq 2n$ mit

$$Z(t) = \frac{P_1(t) \cdot P_3(t) \cdot P_5(t) \cdots P_{2n-1}(t)}{P_0(t) \cdot P_2(t) \cdot P_4(t) \cdots P_{2n}(t)}.$$

Insbesondere ist die Zeta-Funktion eine rationale Funktion. Dies bedeutet, dass endlich viele der Werte $N_r$ schon alle Werte festlegen (Dwork, Grothendieck). Es gilt $P_0(t) = 1-t$ und $P_{2n}(t) = 1-q^n t$. Für den elliptischen Fall siehe Satz 24.4.

(2) Die Grade der Polynome $P_i$ aus Teil (1) haben eine geometrische Bedeutung. Ihr Grad ist die Vektorraumdimension der $i$-ten $\ell$-adischen Kohomologie $H^i(X, \mathbb{Q}_\ell)$. Man spricht von den $\ell$-adischen Betti-Zahlen. Wenn $X$ durch Reduktion modulo $p$ von einer Varietät (Schema) $\mathcal{X}$ über $\mathbb{Z}$ (oder einem Zahlbereich) herrührt, so kann man auch die zugehörige Varietät über $\mathbb{Q}$ und über $\mathbb{C}$ betrachten. Diese Varietät hat (als komplexe Mannigfaltigkeit) topologische Betti-Zahlen, die man beispielsweise mit der singulären Kohomologie ausrechnen kann. Diese Betti-Zahlen stimmen mit den $\ell$-adischen Betti-Zahlen der Reduktion überein. Im Fall einer elliptischen Kurve sind die Betti-Zahlen gleich $1, 2, 1$.

(3) Die Polynome $P_i$ aus Teil (1) besitzen über $\mathbb{C}$ (bzw. über einer geeigneten algebraischen Erweiterung von $\mathbb{Q}$) eine Zerlegung in lineare Faktoren

$$P_i = \prod_j (1 - \alpha_{ij} t).$$

Dabei gilt

$$|\alpha_{ij}| = q^{i/2}.$$

Diese Eigenschaft ist analog zur Riemannschen Hypothese. Für den elliptischen Fall siehe Satz 24.3 (3)

(4) Es gilt eine Funktionalgleichung für die Zeta-Funktion, die Satz 24.5 verallgemeinert.

# Abbildungsverzeichnis