Konstruktion elliptischer Kurven hohen Ranges über $\mathbb{F}_p(t)$

Diplomarbeit
Berichtigte Fassung

Eric F. W. Hofmann

Betreuer: ***Prof. Dr. Wolfgang Ruppert***
Gutachter: ***Prof. Dr. Wulf-Dieter Geyer***

Inhaltsverzeichnis

Einführung **v**
Die Konstruktion von Tate und Shafarevich vi
Überblick viii

1 Geometrische Hilfsmittel **1**
1.1 Elliptische Kurven 1
1.1.1 Weierstraßgleichungen 1
1.1.2 Das Gruppengesetz 4
1.1.3 Abelsche Varietäten 7
1.1.4 Die Struktur der Gruppen 8
1.1.5 Offene Fragen 9
1.2 Isogenien und Endomorphismen 11
1.2.1 Definitionen und allgemeine Aussagen 11
Der Frobenius-Endomorphismus 13
1.2.2 Endomorphismen elliptischer Kurven 15
Die duale Isogenie 15
Die Struktur der Torsionsgruppen 16
Anzahl der rationalen Punkte von E 18
1.2.3 Endomorphismen abelscher Varietäten 20
1.3 Zetafunktionen 21
1.3.1 von elliptischen Kurven und abelschen Varietäten . . . 23
1.3.2 von glatten projektiven Kurven 25
Jacobische Varietäten von Kurven 26
1.4 Supersinguläre elliptische Kurven 28
1.5 Tates Ergebnisse von 1966 34
1.5.1 Der Hauptsatz von Tate 34
1.5.2 Weitere Ergebnisse 36

2 Zahlentheoretische Hilfsmittel **39**
2.1 Gaußsche Summen und Jacobi-Summen 39
2.1.1 Gaußsche Summen 39

2.1.2 Jacobi-Summen 41
2.1.3 Gauß- und Jacobi-Summen bei Körpererweiterungen . 43
2.2 Die klassische Bestimmung von Zetafunktionen 47
2.2.1 Weils Ergebnisse von 1949 48
Die Anzahl der Lösungen von Gleichungen über endlichen Körpern 48
Die Zetafunktion für $a_0x_0^n + \cdots + a_rx_r^n$ 53
2.2.2 Weils Ergebnisse von 1952 55
Die Zetafunktion der affinen Kurve 55
Die Zetafunktion der nichtsingulären projektiven Kurve 61

3 Rangkonstruktionen 65
3.1 Tate und Shafarevich 65
3.1.1 Quadratische Twists 67
3.1.2 Elliptische Kurven über $k(C)$ und die Jacobische $J(C)$ 71
3.1.3 Zetafunktionen und der Rang 74
3.1.4 Die Zetafunktion von C^F 77
3.1.5 Der Rang von E^F 83
3.1.6 Die Teiler von $t^f - 1$ 84
3.2 Nicht konstante j-Invariante 88
3.2.1 Die Konstruktion von Shioda 88
Shiodas Algorithmus für die Picard-Zahl 90
Anwendung auf elliptische Kurven 92
3.2.2 Die Konstruktion von Ulmer 95

Einführung

Die Theorie elliptischer Kurven hat sich als ein Gebiet erwiesen, dem eine Schlüsselfunktion in der Entwicklung der arithmetischen Geometrie zukommt. Gleichzeitig handelt es sich auch um einen Bereich, der durch Anwendungen in der Kryptographie oder der Codierungstheorie zusehends auch praktische Bedeutung im Sinne einer angewandten Forschung erlangt hat. Trotzdem bleiben viele naheliegende Fragen unbeantwortet oder zumindest nicht vollständig geklärt.
Ist eine elliptische Kurve E über einem Körper k definiert, so tragen die k-rationalen Punkte von E die Struktur einer abelschen Gruppe. Für $k = \mathbb{Q}$ ist dies, wenn auch nicht mit der selben Begrifflichkeit, bereits seit der Renaissance bekannt. Ist etwa $k = \mathbb{Q}$ oder k eine endliche algebraische Erweiterung von $\mathbb{Q}$, also ein Zahlkörper, so besagt der Satz von Mordell-Weil, dass $E(k)$ endlich erzeugt ist. Nach dem Struktursatz für endlich erzeugte abelsche Gruppen gilt dann also

$$E(k) \simeq \mathbb{Z}^r \times \prod_i \big(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\big),$$

mit einer ganzen Zahl $r \geq 0$, dem *Rang* von $E(k)$, d.h. der Anzahl unabhängiger freier erzeugender Elemente von $E(k)$.

Man kann sich nun folgende Frage stellen: Variiert man E und betrachtet jeweils den Rang r von $E(k)$ über festem k, welche Werte können für r auftreten? Insbesondere, kann r für verschiedene Kurven beliebig hoch werden, oder ist r für alle E beschränkt? Man vermutet, dass r beliebig hoch werden kann. Ein allgemeiner Beweis dieser Vermutung ist jedoch bislang nicht gelungen.

Man kann nun diese Fragestellung auch über Körpern k, welche keine Zahlkörper sind, untersuchen. Ein besonders aussichtsreicher Fall ist der, dass k ein Funktionenkörper ist. Die endliche Erzeugtheit von $E(k)$ ist auch in dieser Situation bekannt, hier stellt der Satz von Néron-Lang die analoge Aussage zu Mordell-Weil bereit, unter der Voraussetzung, dass k endlich über seinem Primkörper erzeugt ist. Da nun Funktionenkörper ebenso wie

Zahlkörper globale Körper sind, kann die Untersuchung des Problems möglicherweise auch helfen, neue Aufschlüsse über die Situation im Zahlkörperfall zu gewinnen. Besonders interessant sind in diesem Kontext die rationalen Funktionenkörper über endlichen Grundkörpern, d.h. $k = \mathbb{F}_q(t)$, mit $q = p^m$, $m \geq 1$, da hier einerseits häufig weitreichende Analogien zu Zahlkörpern bestehen, und andererseits aber manche Aussagen leichter zu gewinnen sind, etwa weil solche Körper nur nicht-archimedische Stellen haben.

Hier, über $k = \mathbb{F}_p(t)$, ist es tatsächlich gelungen, die eingangs gestellte Frage zu beantworten:

TATE-SHAFAREVICH, 1967, ULMER, 2002: *Der Rang elliptischer Kurven über $\mathbb{F}_p(t)$ ist nicht nach oben beschränkt.*

Dabei gaben TATE und SHAFAREVICH in [TS67] einen konstruktiven Beweis, für $p \neq 2$. ULMER fand eine gänzlich andere Konstruktion, die auch für $p = 2$ funktioniert, in [Ul02]. Das Ziel der vorliegenden Diplomarbeit ist es, die Konstruktion von TATE und SHAFAREVICH im Detail nachzuzeichnen.

Die Konstruktion von Tate und Shafarevich

Die Konstruktion elliptischer Kurven mit beliebig hohem Rang gelingt TATE und SHAFAREVICH, indem sie zu einer festen elliptischen Kurve E, die über k definiert ist, *quadratische Twists* E^{twist} bezüglich der Funktionenkörper $k(C)$ von hyperelliptischen Kurven C durchführen.

Ist C eine gegebene Kurve mit $C(k) \neq \emptyset$, und $L = k(C)$, dann ist $E(L) \simeq \text{Mor}_k(C, E)$, und weiter $\text{Mor}_k(C, E) \simeq \text{Hom}_k(J(C), E) \oplus E(k)$, wo $J(C)$ die jacobische Varietät von C ist, also $E(L)/E(k) \simeq \text{Hom}_k(J(C), E)$. Über einem endlichen Körper k ist $E(k)$ aber eine reine Torsionsgruppe. Somit ist $\text{Rang}\, E(L) = \text{Rang}\, \text{Hom}_k(J(C), E)$.

Bei TATE und SHAFAREVICH wird nun für C eine hyperelliptische Kurve gewählt, und es werden quadratische Twists E^{twist} von E relativ zum Funktionenkörper von $L = k(C)$ betrachtet. In diesem Fall ist $E^{\text{twist}}(L) \simeq E(L)$ und $E^{\text{twist}}(k(t))$ ist isomorph zu $E(L)$ modulo der Operation der Galois-Gruppe der quadratischen Erweiterung $L/k(t)$, also $E^{\text{twist}}(k(t)) \simeq E(L)/\sigma$ mit den einzigen nichttrivialen $\sigma \in \text{Gal}(L \mid k(t))$. Da allgemein gilt $E(k(t)) \simeq E(k)$, kann man nun, wieder für endliches k zeigen, dass

$$\text{Rang}\, E^{\text{twist}}\big(k(t)\big) = \text{Rang}\, E\,(L) = \text{Rang}\, \text{Hom}_k\big(J(C), E\big).$$

Gelingt es nun, C so zu wählen, dass $J(C)$ eine Zerlegung der Form $J(C) \sim E^r \times A$ zulässt, mit einer abelschen Varietät A und einer möglichst hohen Zahl an Faktoren, die isogen zu E sind, so ist auch der Rang von $\text{Hom}_k(J(C), E)$ hoch.

Dabei, eine geeignete Familie von Kurven C zu wählen und die Ränge konkret zu bestimmen, helfen bei der Konstruktion von TATE und SHAFAREVICH zwei Ergebnisse:

Das eine Ergebnis stammt aus einer Arbeit von TATE über die Endomorphismenringe abelscher Varietäten über endlichen Körpern, [Ta66]. Dieser Arbeit kommt eine große Bedeutung für die Theorie abelscher Varietäten zu. Neben vielen anderen Resultaten stellt sie auch einen Zusammenhang zwischen den Zetafunktionen abelscher Varietäten und ihren Homomorphismen her. Sind die Zetafunktionen von C und E bekannt, so kann dieser Zusammenhang eingesetzt werden, um $\operatorname{Rang}\operatorname{Hom}_k(J(C), E)$ zu bestimmen. Insbesondere ist der Rang von $\operatorname{Hom}_k(J(C), E)$ hoch, wenn der Zähler der Zetafunktion von E denjenigen von C zu einer möglichst hohen Ordnung teilt, was gerade äquivalent dazu ist, dass $J(C)$ möglichst viele zu E isogene Faktoren aufweist.

Das andere Ergebnis ist ein Resultat aus der Arbeit [Wei52] von ANDRÉ WEIL. WEIL ermittelt für einen allgemeinen Typ von Kurven, der auch viele hyperelliptische Kurven umfasst, eine Darstellung der zugehörigen Zetafunktion. Es wird dadurch möglich, eine Familie hyperelliptischer Kurven dieses Typs so zu wählen, dass deren Zetafunktionen einen Zähler aufweisen, der in hoher Ordnung durch einen Faktor teilbar ist, wie er im Zähler der Zetafunktion einer über k *supersingulären* elliptischen Kurve auftritt. Wählt man also E so, dass E supersingulär über k ist, erhält man einen hohen Rang für $E^{\text{twist}}(k(t))$.

Eine Besonderheit der Konstruktion mit quadratischen Twists ist, dass die so entstehenden Kurven *isotrivial* sind, das heißt, sie werden über einer Körpererweiterung, in diesem Fall bereits L selbst, isomorph zu der über dem Konstantenkörper k definierten Grundkurve E. Zu dieser Situation, welche so nur über Funktionenkörpern auftritt, gibt es über $\mathbb{Q}$ oder über einem Zahlkörper keine Entsprechung. Insofern ist hier nicht wahrscheinlich, dass die Methoden von TATE und SHAFAREVICH benutzt werden können, um neue Einsichten im Zahlkörperfall zu gewinnen. Durchaus anwendbar könnte ein solches Vorgehen jedoch über $\mathbb{Q}(t)$ sein, siehe beispielsweise [RS01], von A. SILVERBERG und K. RUBIN, die quadratische twists über $\mathbb{Q}$ und $\mathbb{Q}(t)$ sehr eingehend studiert haben, etwa in [RS02], [RS04] und [Sb04]. Eine Aufstellung einiger Fragen, bei deren Behandlung die Analogien zwischen Zahlkörpern und Funktionenkörpern von Nutzen sein können, findet sich in [Ul04].

Überblick

Mit der vorliegenden Arbeit wollen wir die Konstruktion von TATE und SHAFAREVICH aus [TS67] verständlich machen. Wir werden zunächst das theoretische Grundgebäude an Aussagen, wie man sie der Standardliteratur entnehmen kann, aufbauen, wobei wir Grundbegriffe der algebraischen Geometrie und der Theorie algebraischer Kurven voraussetzen. Weiterhin werden wir die benötigten Ergebnisse aus den Arbeiten TATES und WEILS darstellen. Dies geschieht in den Kapiteln 1 und 2, wobei das erste Kapitel geometrischen und das zweite zahlentheoretischen Hilfsmitteln gewidmet ist.

In Abschnitt 1.1 nähern wir uns dem Begriff elliptischer Kurven aus verschiedenen Blickwinkeln, die Gruppenstruktur wird eingeführt, grundlegende Begriffe wie abelsche Varietäten werden definiert und einige offene Fragestellungen diskutiert.

In Abschnitt 1.2 werden Endomorphismenringe abelscher Varietäten definiert und deren Struktur näher untersucht. Insbesondere werden die Frobenius-Endomorphismen eingeführt, und zumindest das Grundgerüst der Theorie elliptischer Kurven wird entworfen.

In Abschnitt 1.3 werden die Zetafunktionen definiert und die historische Entwicklung der Weil-Vermutungen dargestellt. Entsprechende Sätze für elliptische Kurven und für abelsche Varietäten werden bewiesen, ausgehend von vorher angeführten Resultaten. An dieser Stelle werden auch die jacobischen Varietäten von Kurven eingeführt und deren wichtigste Eigenschaften beschrieben.

In Abschnitt 1.4 wird die Theorie supersingulärer elliptischer Kurven systematisch entwickelt.

Abschließend, in Abschnitt 1.5, werden diejenigen Resultate aus [Ta66], welche für die Konstruktion elliptischer Kurven hohen Ranges relevant sind, zusammengestellt und einige Folgerungen aus diesen bewiesen.

In Kapitel 2 werden zunächst in Abschnitt 2.1 die gaußschen und die jacobischen Summen als klassische Hilfsmittel der Zahlentheorie eingeführt, die für die Untersuchung von Zetafunktionen nach WEIL benötigt werden. Der Satz von HASSE-DAVENPORT, welcher das Verhalten der Gauß- und Jacobi-Summen unter Körpererweiterungen beschreibt, wird diskutiert und bewiesen.

Aus diesem Kontext wird dann die grundlegende Arbeit WEILS über Zetafunktionen, [Wei49], in Abschnitt 2.2.1 nachgezeichnet. Im Anschluss, Abschnitt 2.2.2, werden wir mit diesen Methoden einen vollständigen Beweis für die in [Wei52] angegebene Produktzerlegung der Zetafunktionen bestimmter

Kurven führen, der sich in dieser Form nicht in der Literatur findet.

Im Kaptel 3 schließlich wird die Konstruktion von TATE und SHAFAREVICH detailliert dargestellt. Der Begriff des quadratischen Twists wird allgemein eingeführt und die oben angedeuteten Zusammenhänge werden Schritt für Schritt entwickelt.

Abschließend wird noch in Abschnitt 3.2 ein Ausblick auf neuere Arbeiten gegeben, in denen mit anderen Methoden als bei TATE und SHAFAREVICH elliptische Kurven hohen Ranges über $\mathbb{F}_p(t)$ konstruiert werden. Das Vorgehen SHIODAS in [Shi86] wird skizziert und das wesentliche Resultat ULMERS aus [Ul02] wiedergegeben.

Kapitel 1

Geometrische Hilfsmittel

1.1 Elliptische Kurven

Definition 1 (Elliptische Kurven)**.** Elliptische Kurven lassen sich auf verschiedene Arten definieren:

- Eine *elliptische Kurve* über einem Körper k ist ein Paar $\big(E, \mathcal{O}\big)$, bestehend aus einer nichtsingulären Kurve vom Geschlecht 1 über k und einem Punkt $\mathcal{O} \in E$. Eine elliptische Kurve ist über einem Körper k *definiert*, wenn E als Kurve über k definiert ist, und $\mathcal{O} \in E(k)$. Meist werden wir eine elliptische Kurve nur mit E bezeichnen, wenn die Wahl von $\mathcal{O}$ klar ist.

- Eine elliptische Kurve E ist eine vollständige, zusammenhängende Gruppenvarietät der Dimension 1 über einem Grundkörper k.

- Eine elliptische Kurve E ist eine nichtsinguläre projektive Kurve, die durch eine Gleichung der Form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \qquad (1.1)$$

  über einem Grundkörper k definiert ist.

Wir wollen auf den folgenden Seiten sehen, wie diese unterschiedlichen Definitionen zusammenhängen.

1.1.1 Weierstraßgleichungen

Standardreferenz zum Folgenden ist [Sil86], Ch. III, das meiste hier Benötigte findet sich auch kürzer in [Sto00], Kap. 2, S.17ff.

Im Folgenden bezeichne k einen Körper und $\bar{k}$ seinen algebraischen Abschluss.

Definition 2. Eine homogene Gleichung der Form (1.1), als auch ihre inhomogene Form in den affinen Koordinaten (x, y),

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_1, \ldots, a_6 \in k, \tag{1.2}$$

bezeichnen wir als *Weierstraßgleichung*.

Setzt man in (1.1) $Z = 0$, so bleibt nur die Gleichung $X^3 = 0$ übrig, was den folgenden Satz impliziert.

Satz 1. *Eine projektive Kubik C, die durch eine Weierstraßgleichung* (1.1) *definiert ist, hat genau einen Punkt $\mathcal{O} = \big(0 : 1 : 0\big) \in C(k)$ im Unendlichen.*

Bemerkung 1. Der Punkt $\mathcal{O} \in C(k)$ ist ein nichtsingulärer Punkt, denn für

$$f(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

sind die partiellen Ableitungen

$$\frac{\partial}{\partial X}f(X, Y, Z)|_{\mathcal{O}} = \frac{\partial}{\partial Y}f(X, Y, Z)|_{\mathcal{O}} = 0, \text{ aber } \frac{\partial}{\partial Z}f(X, Y, Z)|_{\mathcal{O}} \neq 0.$$

Es ist gebräuchlich, einige weitere Größen zu einer Weierstraßgleichung bzw. der durch sie gegebenen Form einer Kurve zu definieren:

$$\begin{gathered} b_2 = a_1^2 + 4a_2,\ b_4 = a_1a_3 + 2a_4,\ b_6 = a_3^2 + 4a_6, \\ b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2, \\ c_4 = b_2^2 - 24b_4,\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6, \\ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \\ \text{sowie } j = \frac{c_4^3}{\Delta}, \text{ wenn } \Delta \neq 0 \end{gathered} \tag{1.3}$$

Man bezeichnet c_4 und c_6 als Invarianten der Kurve, Δ als deren *Diskriminante* und j als *j-Invariante* der Kurve.

Satz 2. *Eine durch eine Weierstraßgleichung definierte kubische Kurve C ist genau dann nichtsingulär, also elliptisch, wenn die zugehörige Diskriminante $\Delta \neq 0$ ist.*

Satz 3. *Sind zwei Kurven C, C' über k durch Weierstraßgleichungen mit Koeffizienten $a_j, a'_j, j = 1, \ldots, 6$ definiert, so sind diese genau dann isomorph über k, wenn zwischen ihnen eine Abbildung der Form*

$$\phi : \begin{cases} C & \longrightarrow & C' \\ (x, y) & \longmapsto & \big(u^2x + r, u^3y + su^2x + t\big) \end{cases}$$
$$\text{mit} \qquad r, s, t \in k, \text{ und } u \in k^\times$$

besteht. Es gelten dann die folgenden Aussagen:

- $\phi(\mathcal{O}_C) = \mathcal{O}_{C'}$.
- *Für die Koeffizienten hat man die Beziehungen*

$$\begin{aligned} ua_1 &= a_1' + 2s \\ u^2a_2 &= a_2' + sa_1' + 3r - s^2 \\ u^3a_3 &= a_3' + ra_1' + 2t \\ u^4a_4 &= a_4' - sa_3' + 2ra_2' - (t + rs)a_1' + 3r^2 - 2st \\ u^6a_6 &= a_6' + ra_4' - ta_3' + r^2a_2' - rta_1' + r^3 - t^2. \end{aligned}$$

- *Für die Invarianten gilt*

$$u^4c_4 = c_4',\ u^6c_6 = c_6',\ u^{12}\Delta = \Delta',\ \textit{und}\ \ j = j',\ \textit{sofern definiert.}$$

Mit solchen Koordinatentransformationen lässt sich nun meist eine etwas handlichere Form der Kurvengleichung erzielen:

Satz 4. *Sei C über einem Körper k durch eine Weierstraßgleichung definiert.*

- *Ist $char(k) \neq 2$, so ist C isomorph zu einer Kubik mit der (affinen) Gleichung*
$$C' \ : \ y^2 = x^3 + a_2'x^2 + a_4'x + a_6'.$$
- *Ist $char(k) \neq 2, 3$, so ist C isomorph zu einer Kubik mit der (affinen) Gleichung*
$$C' \ : \ y^2 = x^3 + a_4'x + a_6'.$$
Die Formeln für die Diskriminante und die j-Invariante der Kurven vereinfachen sich dann zu

$$\Delta' = -16\big(4{a_4'}^3 + 27{a_6'}^2\big), \qquad j' = -\frac{1728\big(4a_4'\big)^3}{\Delta'} = \frac{1728\big(4{a_4'}^3\big)}{4{a_4'}^3 + 27{a_6'}^2}.$$

Man spricht in beiden Fällen von einer kurzen Weierstraßgleichung. (Außerdem gilt jeweils $\mathcal{O}_C = \mathcal{O}_{C'}$.)

Bemerkung 2. Sofern $char(k) \neq 2, 3$, lassen sich die beiden verkürzten Weierstraßgleichungen jeweils in der Form

$$\begin{aligned} y^2 &= x^3 + b_2x^2 + 8b_4x + 16b_6 \\ \text{bzw.} \quad y^2 &= x^3 - 27c_4x - 54c_6, \end{aligned}$$

schreiben, mit den Konstanten der alten Gleichung, aus (1.3), Seite 2.

Satz 5. *Zwei elliptische Kurven E, E' über einem Körper k sind genau dann isomorph über $\bar{k}$, wenn $j(E) = j(E')$. Umgekehrt gibt es zu jedem $j \in k$ eine elliptische Kurve E über k mit $j(E) = j$.*

Definition 3. Eine Weierstraßgleichung liegt in *Legendre-Form* vor, wenn sie sich (in affinen Koordinaten) schreiben lässt als

$$y^2 = x\big(x-1\big)\big(x-\lambda\big), \qquad \text{mit } 0,1 \neq \lambda \in \bar{k}.$$

Satz 6 (vgl. [Sil86], S. 54)**.** *Sei $char(k) \neq 2$. Jede über k definierte elliptische Kurve E ist über $\bar{k}$ isomorph zu einer elliptischen Kurve E_λ in Legendre-Form.*

1.1.2 Das Gruppengesetz

Sei E eine projektiv gegebene elliptische Kurve über einem Grundkörper k mit dem ausgezeichneten Punkt $\mathcal{O}$. Nach dem Satz von Bézout (vgl. [Har77], I.7.8) schneidet jede Gerade $L \subset \mathbb{P}^2$ die Kurve E in 3 Punkten (mit Vielfachheit gezählt) über dem algebraischen Abschluss, da E eine Kurve vom Grad 3 ist.

Wir definieren nun folgendermaßen eine Verknüpfung $\oplus$ auf E:

Definition 4 (Verknüpfungsregel)**.** Sei E eine elliptische Kurve, $P, Q \in E$ und L die Gerade durch P und Q, bzw. die Tangente an E in P, falls $P = Q$. Sei R der dritte Schnittpunkt von L mit E, L' die Verbindungsgerade von R mit $\mathcal{O}$ (bzw. die Tangente, falls $R = \mathcal{O}$). Dann ist $P \oplus Q$ der Punkt auf E so, dass $L' \cap E$ aus den Punkten $\mathcal{O}$, R, $P \oplus Q$ besteht, wobei möglicherweise Punkte zusammenfallen.

Lemma 1 ([Sil86], Prop 2.2, S. 55)**.** *Die Verknüpfung $\oplus$ auf E hat folgende Eigenschaften:*

1. *Schneidet eine Gerade L die Kurve E in den (nicht notwendig verschiedenen) Punkten $R, P, Q \in E$, so gilt $(P \oplus Q) \oplus R = \mathcal{O}$.*
2. *$P \oplus \mathcal{O} = P$ für alle $P \in E$.*
3. *$P \oplus Q = Q \oplus P$ für alle $P, Q \in E$*
4. *Zu jedem $P \in E$ gibt es einen Punkt $P' \in E$, mit $P \oplus P' = \mathcal{O}$*
5. *Für jedes Tripel $P, Q, R \in E$ gilt*

$$\big(P \oplus Q\big) \oplus R = P \oplus \big(Q \oplus R\big)$$

Beweisskizze. 1. Dies ist klar aus Definition 4

2. Setzt man in Definition 4 ein $Q = \mathcal{O}$, so ist $L = L'$ und damit $(P, \mathcal{O}, R) = (R, \mathcal{O}, P \oplus \mathcal{O})$ also $P \oplus \mathcal{O} = P$.

3. $P \oplus Q = Q \oplus P$ ist klar, da die Konstruktion der Summe $\oplus$ symmetrisch in P und Q ist.

4. Ist R der dritte Schnittpunkt der Verbindungsgeraden von P, $\mathcal{O}$ mit E, so folgt aus 1. und 2., dass $P \oplus R = (P \oplus \mathcal{O}) \oplus R = \mathcal{O}$.

5. Dieses Assoziativgesetz lässt sich grundsätzlich auf drei Arten nachprüfen:

   - Man verwendet explizite Formeln (s.u., Satz 7) in den Koordinaten, um dies nachzurechnen, wobei man zu vielen Fallunterscheidungen gezwungen ist.
   - Man arbeitet auf der Ebene von Divisoren. Das Assoziativgesetz wird dann zu einer Konsequenz des Satzes von Riemann-Roch und es stellt sich heraus, dass die durch $\oplus$ definierte Struktur als abelsche Gruppe isomorph zu $\mathrm{Pic}^0(E)$ ist, der Gruppe der Divisoren vom Grad 0 modulo Hauptdivisoren. Dies ist sicherlich von einem systematischen Standpunkt aus der beste Weg, da wir allerdings bislang keine Divisoren verwendet haben, werden wir dem nicht weiter nachgehen.
   - Man zieht allgemeinere geometrische Aussagen zu Hilfe. Dieser Weg wird in [Sto00], S. 23ff beschritten. Hauptsächliches Hilfsmittel ist dabei folgende Aussage:

     > Seien $L_i, L_j \subset \mathbb{P}^2$ (für $i, j = 1, 2, 3$) paarweise verschiedene Geraden in allgemeiner Lage, so, dass die Schnittpunkte $P_{ij} = L_i \cap L_j$ paarweise verschieden sind. Sei außerdem C eine ebene projektive Kubik, so, dass 8 der Punkte P_{ij} auf C liegen. Dann liegt auch der 9te Punkt auf C.

     Wendet man diese Aussage auf die in der Konstruktion von $P \oplus Q$, $(P \oplus Q) \oplus R$, $Q \oplus R$, $P \oplus (Q \oplus R)$ gemäß der Konstruktion in Definition 4 jeweils auftretenden Geraden und Hilfsgeraden L, L' an, so ergibt sich die gewünschte Aussage. Da E als irreduzible Kurve von Grad $3 > 1$ keine Gerade enthält, ist die Voraussetzung allgemeiner Lage dann gegeben, wenn keine der beteiligten Punkte zusammenfallen. Ansonsten sind noch weitere Überlegungen nötig, vgl. [Sto00].

□

Theorem 1. *Mit der Verknüpfung $\oplus$ erhält $E(\bar{k})$ die Struktur einer abelschen Gruppe mit dem Nullelement $\mathcal{O}$, die wir ab jetzt additiv mit Gruppenoperation $+$ und Inversionsabbildung $-$ schreiben werden.*
Es gilt außerdem: Ist k ein Körper, über dem E definiert ist, so ist die Menge $E(k)$ der k-rationalen Punkte von E eine Untergruppe von $E(\bar{k})$.

Bemerkung 3. Die Gruppenstruktur auf E kann auch mit einem anderen ausgezeichneten Punkt als $(0 : 1 : 0)$ weitgehend analog definiert werden. Durch die Wahl dieses Punktes ist die Gruppenstruktur dann eindeutig festgelegt.

Wir wollen nun noch explizite Formeln für die Summe zweier Punkte in E angeben.

Satz 7. *Sei E durch eine Weierstraßgleichung*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

über einem Körper k affin gegeben. Dann gilt:

1. *Für $P = (x, y) \in E(k)$ ist $-P = \big(x, -y - a_1x - a_3\big)$.*
2. *Sind $E(k) \ni P_i = (x_i, y_i)$, $i = 1, 2, 3$ Punkte mit $P_1 + P_2 = P_3$. Falls nun $x_1 = x_2$ sowie $y_1 + y_2 + a_1x_2 + a_3 = 0$, dann ist*

$$P_1 + P_2 = \mathcal{O}.$$

Andernfalls gilt

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \qquad y_3 = -\big(\lambda + a_1\big)x_3 - \nu - a_3, \quad (1.4)$$

wobei λ, ν definiert sind durch

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{wenn } x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{wenn } x_1 = x_2 \end{cases}$$

$$\nu = \begin{cases} \dfrac{y_1x_2 - y_2x_1}{x_2 - x_1} & \text{wenn } x_1 \neq x_2 \\ \dfrac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3} & \text{wenn } x_1 = x_2\ . \end{cases}$$

1.1.3 Abelsche Varietäten

Zum Folgenden stellen [MilAb] sowie [MilAV] Grundreferenzen dar.

Eine *Gruppenvarietät* über einem Körper k ist eine Varietät G, zusammen mit regulären Abbildungen

$$\begin{aligned} \mu : G \times_k G \to G \qquad & \text{Multiplikation} \\ \text{inv} : G \to G \qquad & \text{Inversion,} \end{aligned}$$

und einem Element $\mathcal{O} \in G(k)$, so, dass die durch μ, inv definierte Struktur auf $G(\bar{k})$ eine Gruppe mit neutralem Element $\mathcal{O}$ darstellt, d.h. es gilt $\mu\big(g, \mathcal{O}\big) = \mu\big(\mathcal{O}, g\big) = g$ für jedes $g \in G$, und die folgenden Diagramme kommutieren:

$$\begin{array}{ccc} G \times_k G & \xrightarrow{\text{id}\times\text{inv}} & G \times_k G \\ {\scriptstyle \text{inv}\times\text{id}}\downarrow & & \downarrow{\scriptstyle \mu} \\ G \times_k G & \xrightarrow{\mu} & \mathcal{O} \in G \end{array} \qquad \begin{array}{ccc} G \times_k G \times_k G & \xrightarrow{\text{id}\times\mu} & G \times_k G \\ {\scriptstyle \mu\times\text{id}}\downarrow & & \downarrow{\scriptstyle \mu} \\ G \times_k G & \xrightarrow{\mu} & G \end{array}$$

Gilt zusätzlich $\mu\big(p, q\big) = \mu\big(q, p\big)$ für alle $p, q \in G$, so nennt man die Gruppenvarietät G *kommutativ*.

Für jede k-Algebra R trägt dann auch $G(R)$ eine Gruppenstruktur.

Beispiel. ([Sil94], Example 1.1.2, S. 291) Die additive und die multiplikative Gruppe von k sind kommutative Gruppenvarietäten $\mathbb{G}_a$, $\mathbb{G}_m$:

$$\mathbb{G}_a \simeq \mathbb{A}^1, \quad \mathbb{G}_m \simeq \big\{x \in \mathbb{A}^1 \ : \ x \neq 0\big\},$$

dabei werden die Gruppengesetze jeweils definiert durch

$$\mu \ : \ \begin{array}{ccc} \mathbb{G}_a \times \mathbb{G}_a & \to & \mathbb{G}_a \\ \big(x, y\big) & \mapsto & x + y \end{array} \quad \text{und} \qquad \mu \ : \ \begin{array}{ccc} \mathbb{G}_m \times \mathbb{G}_m & \to & \mathbb{G}_m \\ \big(x, y\big) & \mapsto & xy \end{array}.$$

Mittels $\mathbb{G}_m \xrightarrow{\sim} \big\{(x, y) \in \mathbb{A}^2 \ : \ xy = 1\big\}$, $x \mapsto (x, 1/x)$ kann $\mathbb{G}_m$ ebenfalls als affine Varietät realisiert werden.

Beispiel. Elliptische Kurven sind kommutative Gruppenvarietäten, mit der im vorherigen Abschnitt definierten Gruppenstruktur.

Definition 5. Für $a \in G$, definieren wir die *Translation mit a* als die Abbildung

$$t_a \ : \ \begin{cases} G & \to & G \\ g & \mapsto & \mu(a, g) \end{cases}.$$

Bemerkung 4. Jede Gruppenvarietät ist automatisch nichtsingulär. Denn als Varietät enthält G eine offene nichtsinguläre Untervarietät $U \subset G$, $U \neq \emptyset$. Deren Translate $t_a U$, $a \in G$, bedecken dann ganz G. Da durch einen nichtsingulären Punkt nur eine Zusammenhangskomponente gehen kann, folgt weiter, dass jede zusammenhängende Gruppenvarietät auch irreduzibel ist.

Definition 6 ([MilAV], §1)**.** Eine *abelsche Varietät* über einem Grundkörper k ist eine vollständige, zusammenhängende Gruppenvarietät über k.

Satz 8 ([MilAV], Cor. 2.2)**.** *Jede reguläre Abbildung $\alpha : A \to B$ zwischen abelschen Varietäten ist die Komposition eines Gruppenhomomorphismus mit einer Translation.*

Aus diesem Satz ergibt sich, dass die Gruppenstruktur einer abelschen Varietät durch die Wahl des neutralen Elements $\mathcal{O}$ eindeutig bestimmt wird.

Korollar 1 ([MilAV], Cor. 2.4)**.** *Die Gruppenstruktur einer abelschen Varietät ist kommutativ.*

Beweis. Aus dem vorherigen Satz ergibt sich, dass die Inversionsabbildung $\mathrm{inv} : A \to A$ ein Homomorphismus ist, da $\mathrm{inv}(\mathcal{O}) = \mathcal{O}$. Dass die Inversion ein Homomorphismus ist, charakterisiert aber gerade abelsche Gruppen. □

Satz 9 ([MilAV], Th. 7.1, S.113)**.** *Jede abelsche Varietät A ist projektiv, d.h. es gibt eine abgeschlossene Einbettung ϕ und ein m mit $\phi : A \hookrightarrow \mathbb{P}^m$.*

1.1.4 Die Struktur der Gruppen

Wir wissen nun also, dass die rationalen Punkte einer abelschen Varietät die Struktur einer abelschen Gruppe tragen. Wenn diese endlich erzeugt ist, dann ist damit die Frage nach der Struktur dieser Gruppen im wesentlichen beantwortet. Dies ist allerdings zunächst nur über endlichen Körpern klar, denn wenn A über $k = \mathbb{F}_q$ definiert ist, so ist $A(k) \subset \mathbb{P}^m_k$ und damit endlich. In Charakteristik 0 haben wir folgende Antwort:

Theorem 2 (Mordell-Weil, vgl. [LEM], S. 26f, Th. 4.1)**.** *Ist A eine abelsche Varietät über einem Zahlkörper k, so ist $A(k)$ endlich erzeugt.*

Für elliptische Kurven über $\mathbb{Q}$, d.h. im Falle $\dim A = 1$ wurde dies bereits von H. Poincaré vermutet und von Mordell 1921 bewiesen. André Weil konnte dies dann auf Zahlkörper und beliebige Dimensionen erweitern, und Néron bewies das Theorem schließlich auch für k endlich erzeugt über $\mathbb{Q}$. Wegen der großen Bedeutung dieses Theorems bezeichnet man im Falle elliptischer Kurven die Gruppe $E(k)$ als *Mordell-Weil Gruppe* von E über k.

Ein weiterer arithmetisch interessanter Fall ist der von Funktionenkörpern. Hierfür gibt es eine analoge Antwort, das Theorem von NÉRON und LANG, die allerdings im Detail etwas komplizierter ausfällt, ibid. Theorem 4.2.

Für die Verwendung im Rahmen dieser Diplomarbeit genügt folgende Fassung:

Theorem 3 (ibid. Corollary 4.3)**.** *Sei L endlich erzeugt über seinem Primkörper und sei A eine abelsche Varietät, die über L definiert ist. Dann ist $A(L)$ endlich erzeugt.*

Wendet man nun den Struktursatz für abelsche Gruppen auf $A(k)$ an, so erhält man

Satz 10. *Sei k ein Körper und entweder k endlich, oder k endlich erzeugt über $\mathbb{Q}$ oder k ein Funktionenkörper, der endlich erzeugt über seinem Primkörper ist. Sei A eine über k definierte abelsche Varietät. Dann gilt*

$$A(k) \simeq \mathbb{Z}^r \times \prod_i \big(\mathbb{Z}/p_i^{e_i}\mathbb{Z}\big), \tag{1.5}$$

mit einem freien Anteil $\simeq \mathbb{Z}^r$, $r \geq 0$, und einem Torsionsanteil $A_{tors}(k)$.

Definition 7. Man bezeichnet den Rang r des freien Anteils in (1.5) als den *Rang von $A(k)$*.

Bemerkung 5. Im Fall $k = \mathbb{F}_q$ ist dieser Satz klar, s.o., insbesondere ist der Rang $r = 0$ und $\sharp A(k)_{tors}$ endlich. Genauer gilt für eine abelsche Varietät A der Dimension g über k

$$\sharp A\big(\mathbb{F}_q\big) \leq \big(1 + \sqrt{q}\big)^{2g},$$

vgl. hierzu [Sb00], S. 13.

1.1.5 Offene Fragen

Es gibt nun eine Reihe von Ergebnissen und Vermutungen, welche den Rang und die Torsionsgruppe von abelschen Varietäten betreffen. Ein Aufstellung davon findet sich in [Sb00], Ch. 2 und 3, mehrere Beispiele gibt auch [LEM]. Wir wollen einiges davon wiedergeben:

Vermutung 1 ((starke) Torsions-Vermutung)**.** *Ist A eine abelsche Varietät der Dimension d, die über einem Zahlkörper k (vom Grad m) definiert ist, dann gilt $\sharp A(k)_{tors} < C$ mit einer nur von d und k (nur von d und m) abhängigen Konstante C.*

Für $d = 1$ und $m = 1$ ist die starke Torsionsvermutung schon seit längerem durch MAZUR bewiesen:

Satz 11 (Mazur, 1975)**.** *Ist E eine über $\mathbb{Q}$ definierte elliptische Kurve, so ist $E(\mathbb{Q})_{tors}$ isomorph zu einer der folgenden 15 Gruppen:*

$$\begin{array}{ll} \mathbb{Z}/m\mathbb{Z} & \text{mit } m = 1, 2, \ldots, 10 \text{ oder } m = 12 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \text{mit } m = 2, 4, 6, 8 \end{array}$$

Für elliptische Kurven wurden einige weitere Fälle nach und nach gezeigt, bis schließlich MEREL den Beweis für alle m erbrachte:

Satz 12 (Merel, 1996)**.** *Ist E eine elliptische Kurve über einem Zahlkörper k vom Grad m, so ist $\sharp E(k)_{tors}$ nach oben durch eine Konstante beschränkt, die nur von m abhängt.*

Für abelsche Varietäten über Zahlkörper sind ebenfalls einige spezielle Fälle bekannt, die allgemeine Vermutung bleibt jedoch offen. Man kann die Torsionsvermutung auch auf andere globale Körper verallgemeinern, vgl. [Sb00], S. 14, insbesondere vermutet man:

Vermutung. *Ist A eine abelsche Varietät, ohne konstanten Teil, über einem Funktionenkörper k, und sei d die Dimension von A. So gilt: $\sharp A(k)_{tors}$ wird nach oben durch eine Schranke begrenzt, welche nur von d und k abhängig ist.*

Für $d = 1$, also für elliptische Kurven, ist auch hier einiges bekannt. Beispielsweise zeigte LEVIN die absolute Beschränktheit von $E(k)_{tors}$ im Falle, dass k ein Funktionenkörper einer Variable ist.

Rangvermutung Auch über den Rang einer abelschen Varietät gibt es Vermutungen. Für sehr warscheinlich hält man die folgende Aussage, die bereits in der Einführung erwähnt wurde, SILVERBERG bezeichnet sie als „Teil der Folklore“.

Vermutung 2. *Der Rang elliptischer Kurven über $\mathbb{Q}$ ist nicht nach oben beschränkt.*

Allgemeiner:

Vermutung 3. *Der Rang elliptischer Kurven über globalen Körpern ist nicht nach oben beschränkt.*

Für Funktionenkörper sind tatsächlich einige Fälle bewiesen, sogar konstruktiv:

Der Beweis über $\mathbb{F}_p(t)$, für $p \neq 2$, durch TATE und SHAFAREVICH in [TS67] ist das Hauptthema der vorliegenden Diplomarbeit, der Fall $\mathbb{F}_2(t)$ ist in dem neuerlichen Beweis durch ULMER in [Ul02] beinhaltet, siehe Abschnitt 3.2.2, ab Seite 95

Beweise über $\overline{\mathbb{F}}_p(t)$, sowie eine Zusammenstellung weiterer Konstruktionen, finden sich in der Arbeit von BOUW, DIEM und SCHOLTEN, [BDS04], siehe dazu auch [DS05]. Der Fall $\overline{\mathbb{F}}_p(t)$ mit $p \equiv -1 \bmod 4$ geht auch aus der Konstruktion von SHIODA, [Shi86], hervor, siehe Abschnitt 3.2.1, Theorem 9, auf Seite 93.

Im Gegensatz zur Situation über Funktionenkörpern ist jedoch über Zahlkörpern kein Beweis in Sicht. Tatsächlich erweist es sich als sehr schwierig, überhaupt Beispiele elliptischer Kurven hohen Ranges über $\mathbb{Q}$ zu finden. So war etwa bis 1977 keine elliptische Kurve bekannt, deren Rang über $\mathbb{Q}$ die Wert 7 übersteigt. MESTRE konstruierte 1986 ein Beispiel einer Kurve mit Rang ≥ 14. In den 1990er Jahren stieg die Bestmarke hier nach und nach auf 23 (durch MARTIN und MCMILLEN, 1998). Im Jahr 2000 stand der Rekord schließlich bei 24 (ebenfalls MARTIN-MCMILLEN). Eingehend wird die Suche nach elliptischen Kurven hohen Rangs in der Diplomarbeit von W. KROWORSCH behandelt [Kr05].

Auch für allgemeinere abelsche Varietäten gibt es in diesem Zusammenhang Vermutungen, auf die wir hier jedoch nicht weiter eingehen wollen.

1.2 Isogenien und Endomorphismen

1.2.1 Definitionen und allgemeine Aussagen

Wir geben für den grundlegenden Begriff der Isogenie im Fall elliptischer Kurven eine Definition, die sich an dem Begriff der projektiven Kurve mit einem ausgezeichneten Punkt orientiert, wie in Definition 1 auf Seite 1:

Definition 8. Eine *k-Isogenie* elliptischer Kurven E, E' über einem Grundkörper k ist ein nicht-konstanter k-Morphismus (von Kurven)

$$\begin{aligned} &\phi : E \to E' \\ \text{mit} \qquad &\phi(\mathcal{O}_E) = \mathcal{O}_{E'}. \end{aligned}$$

Zwei elliptische Kurven E, E' heißen *isogen* (über k), in Formeln $E \sim_k E'$, wenn zwischen ihnen eine k-Isogenie $\phi : E \to E'$ besteht. Für $E \sim_{\bar{k}} E'$ schreibt man meist nur $E \sim E'$.

Bemerkung 6. Häufig wird der Begriff Isogenie für elliptische Kurven auch so definiert, dass auch konstante Isogenien, $\phi(E) = \mathcal{O}_{E'}$, zugelassen sind, so etwa bei SILVERMAN [Sil86], S. 70.

Satz 13 (vgl. [Sil86], S. 70, Th. 4.8, S. 75)**.** *Ist $\phi : E \to E'$ ein Homomorphismus mit $\phi(\mathcal{O}_E) = \mathcal{O}_{E'}$, so gilt entweder $\phi(E) = E'$ oder $\phi(E) = \{\mathcal{O}_{E'}\}$. Seien außerdem $P_1, P_2 \in E$, so gilt:*

$$\phi(P_1 + P_2) = \phi(P_1) + \phi(P_2).$$

Insbesondere induziert jede Isogenie einen Gruppenhomomorphismus.

Durch diesen Satz sehen wir, dass unsere Definition mit der folgenden allgemeineren Definition kompatibel ist.

Definition 9 (vgl. z.B. [MilAb], S. 30)**.** Eine *k-Isogenie* abelscher Varietäten A, A' über einem Körper k ist ein surjektiver k-Homomorphismus ϕ mit endlichem Kern (d.h. $\operatorname{Ker}\phi$ hat Dimension 0). Zwei abelsche Varietäten heißen *isogen* (über k), $A \sim_k A'$, wenn zwischen ihnen eine k-Isogenie besteht.

Auch hier spricht man über dem algebraischen Abschluss meist nur „A isogen zu A'“ und schreibt $A \sim A'$.

Satz 14 ([MilAb], Prop. 6.1, S. 30)**.** *Für einen Homomorphismus $\phi : A \to B$ abelscher Varietäten sind die folgenden Aussagen äquivalent:*

- *ϕ ist eine Isogenie*
- *$\dim A = \dim B$ und ϕ ist surjektiv*
- *$\dim A = \dim B$ und $\operatorname{Ker}\phi$ ist endlich.*

Das wichtigste Beispiel für Isogenien sind die im Folgenden definierten Multiplikations-Abbildungen.

Satz ([MilAb], Th. 6.2, S. 30)**.** *Ist A eine abelsche Varietät der Dimension g über einem Körper k so ist für jedes $n \in \mathbb{Z}$ die Abbildung*

$$[n] : \begin{Bmatrix} A & \to & A \\ a & \mapsto & na = \sum_i^n a \end{Bmatrix}$$

eine Isogenie. Für $n \neq 0$ ist $[n]$ eine nicht-konstante Abbildung vom Grad $\deg(n) = n^{2g}$. Außerdem ist $[n]$ separabel, wenn $\mathrm{char}(k) = 0$ oder $\mathrm{char}(k) \nmid n$.

Definition 10. Seien A, A' abelsche Varietäten über k. Wir definieren

$$\mathrm{Hom}_k\big(A, A'\big) = \big\{\, k\text{-Homomorphismen } A \to A' \big\},$$

und

$$\mathrm{End}_k\big(A\big) = \mathrm{Hom}_k\big(A, A\big)$$

Durch $\big(\phi + \psi\big)(P) = \phi(P) + \psi(P)$ sowie $\big(\phi \circ \psi\big) = \phi\big(\psi(P)\big)$ erhalten $\mathrm{Hom}_k(A, A')$ und $\mathrm{End}_k(A)$ jeweils die Struktur eines Ringes, mit der konstanten Isogenie $A \to \mathcal{O}$ als Nullelement. Mittels $\mathbb{Z} \hookrightarrow \mathrm{End}_k(A)$, $n \mapsto [n]$ kann $\mathbb{Z}$ als Unterring von $\mathrm{End}_k(A)$ aufgefasst werden. Es gilt: $\mathrm{Hom}_k(A, A')$ ist torsionsfreier $\mathbb{Z}$-Modul.

Bemerkung 7. Sind A, A' über einen Körper k definiert, so kann $\mathrm{Hom}_k(A, A') \subsetneq \mathrm{Hom}_{\bar{k}}(A, A') = \mathrm{Hom}(A, A')$ gelten. Entsprechendes gilt auch für die Endomorphismenringe.

Definition 11. Die Menge $A[m]$ der m-Teilungspunkte von A zu $m \in \mathbb{Z}$ wird definiert als

$$A[m] = \big\{P \in A \,:\, [m](P) = \mathcal{O}\big\}.$$

Der Frobenius-Endomorphismus

Definition 12. Sei k ein Körper der Charakteristik $p > 0$. Und sei $q = p^m$, $m \geq 1$. Zu jedem Polynom

$$f = \sum_i c_i X_1^{a_{i,1}} \cdots X_n^{a_{i,n}} \qquad \in k\big[X_1, \ldots, X_n\big]$$

bezeichne

$$f^{(q)} = \sum_i c_i^q X_1^{a_{i,1}} \cdots X_n^{a_{i,n}}$$

das Polynom, welches man aus f durch Anwendung der Frobenius-Abbildung $k \to k$, $x \mapsto x^q$ auf die Koeffizienten erhält.

Sei nun V eine algebraische Varietät, die über k definiert ist durch Gleichungen

$$f_1 = f_2 = \cdots = f_r = 0 \qquad \text{mit} \qquad f_i \in k[X_1, \ldots, X_n].$$

Dann bezeichnen wir mit $V^{(q)}$ die Varietät, die durch die Gleichungen

$$f_1^{(q)} = \cdots = f_r^{(q)} = 0$$

definiert wird.

Durch Anwendung des Frobenius $x \to x^q$ auf die Koordinaten der Punkte von V erhalten wir eine natürliche Abbildung

$$Fr_q : \begin{cases} V & \to & V^{(q)} \\ (x_1, \ldots, x_n) & \mapsto & (x_1^q, \ldots, x_n^q) \end{cases},$$

diese heißt *q-Frobenius Morphismus*.

Um zu sehen, dass tatsächlich $Fr_q(V) = V^{(q)}$, genügt es, $f_i^{(q)}(Fr_q(P)) = 0$ für $P \in V$ nachzurechnen:

$$\begin{aligned} f_i^{(q)}(Fr(P)) &= f_i^{(q)}(x_1^q, \ldots, x_n^q) \\ &= \big(f_i(x_1, \ldots, x_n)\big)^q \quad (\text{da } char(k) = p). \\ &= 0 \qquad\qquad\qquad\quad (\text{da } f_i(P) = 0). \end{aligned}$$

Sei nun speziell k der endliche Körper $\mathbb{F}_q$, und $\bar{k}$ dessen algebraischer Abschluss. Dann wird $\mathrm{Gal}(\bar{k} \mid k)$ durch die Frobenius-Abbildung $x \to x^q$ erzeugt. Anderseits ist $k \subset \bar{k}$ eindeutig bestimmt durch $x^q = x$ für jedes x in k. Ist also die Varietät V über k definiert, so gilt

$$V = V^{(q)} \qquad \text{und auch } V = V^{(q^m)},\ m \geq 1.$$

Damit ist Fr_{q^m} ein Endomorphismus von V, der sogenannte *q^m-Frobenius-Endomorphismus*. Es gilt dann

$$Fr_{q^m} V\big(\mathbb{F}_{q^m}\big) = V\big(\mathbb{F}_{q^m}\big) \qquad \text{für } m = 1, 2, 3, \ldots .$$

Ist k vollkommen, so ist die Frobenius-Abbildung surjektiv. Für Varietäten, welche über solchen Körpern definiert sind, ist der Frobenius-Morphismus somit auch surjektiv.

Für eine Abelsche Varietät A, die über einem endlichen Körper der Charakteristik p definiert ist, ist $Fr_q \in \mathrm{End}(A)$ eine Isogenie nach Definition 9, da der Kern Null ist.

Satz 15 (siehe [Sil86], S. 30f)**.** *Ist k ein vollkommener Körper mit $char(k) = p > 0$, $q = p^r$. C eine über k definierte Kurve und $Fr : C \to C^{(q)}$ der q-Frobenius-Morphismus, so gilt*

$$\begin{gathered} Fr^* k\big(C^{(q)}\big) = k\big(C\big)^q \\ Fr \quad \textit{ist rein inseparabel} \\ \deg Fr = q \end{gathered}$$

Korollar 2 ([Sil86]. S. 31, [Har77], S. 302)**.** *Jeder Abbildung $\psi : C_1 \to C_2$ zwischen nichtsingulären Kurven über einem (vollkommenen) Körper der Charakteristik p lässt sich als Komposition schreiben*

$$C_1 \xrightarrow{Fr} C_1^{(q)} \xrightarrow{\lambda} C_2,$$

wobei $q = \deg_{\text{insep}}(\psi)$, Fr der q-Frobenius-Morphismus und λ eine separable Abbildung ist.

Satz 16 (siehe [Sil86], Cor. 5.5, S. 83)**.** *Sei $k = \mathbb{F}_q$, und E über k definierte elliptische Kurve, und sei Fr deren q-Frobenius-Endomorphismus. Seien außerdem m, $n \in \mathbb{Z}$. Dann gilt*

$$m + n \circ Fr \in \text{End}(E)$$

ist separabel genau dann, wenn $p \nmid m$. Insbesondere ist $1 - Fr$ immer separabel.

1.2.2 Endomorphismen elliptischer Kurven

Wir wollen nun die zuletzt eingeführten Begriffe für elliptische Kurven eingehender betrachten, und auch einige der allgemeinen Aussagen in diesem Fall zeigen.

Die duale Isogenie

Satz 17 (und Definition)**.** *Ist $\phi : E_1 \to E_2$ eine nichtkonstante Isogenie vom Grad $\deg(\phi) = m$, so existiert eine eindeutig definierte Isogenie $\hat{\phi} : E_2 \to E_1$ mit der Eigenschaft*

$$\phi \circ \hat{\phi} = [m] \in \text{End}(E_2) \text{ und}$$
$$\hat{\phi} \circ \phi = [m] \in \text{End}(E_1).$$

Man bezeichnet $\hat{\phi}$ als die duale Isogenie *zu ϕ. Die Abbildung $\phi \leftrightarrow \hat{\phi}$ hat folgende Eigenschaften:*

- *Ist $\lambda : E_2 \to E_3$ eine weitere Isogenie, so gilt*

$$\widehat{\lambda \circ \phi} = \hat{\phi} \circ \hat{\lambda}.$$

- *Ist $\psi : E_1 \to E_2$ eine weitere Isogenie, so gilt*

$$\widehat{\psi + \phi} = \hat{\phi} + \hat{\psi}.$$

- *Für alle* $m \in \mathbb{Z}$ *gilt*

$$\widehat{[m]} = [m] \qquad \textit{und} \qquad \deg[m] = m^2$$

- *Es ist* $\deg(\hat{\phi}) = \deg(\phi)$ *und* $\hat{\hat{\phi}} = \phi$.

Beweise für die in Satz 17 gesammelten Aussagen finden sich z.B. in [Sil86], III.6, ab Seite 84.

Satz 18 (ibid., Coroll. 6.3)**.** *Die Gradabbildung* $\deg : Hom(E_1, E_2) \to \mathbb{Z}$ *ist eine positiv definite quadratische Form.*

Beweis. Wir zeigen, dass

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$$

bilinear ist. Durch $\langle \phi, \psi \rangle \in \mathbb{Z}$ kann man in $\mathrm{End}(E_1)$ rechnen:

$$\begin{aligned} \big[\langle \phi, \psi \rangle\big] &= \big[\deg(\phi + \psi)\big] - \big[\deg(\phi)\big] - \big[\deg(\psi)\big] \\ &= \widehat{(\phi + \psi)} \circ (\phi + \psi) - \hat{\phi} \circ \phi - \hat{\psi} \circ \psi \\ &= \hat{\phi} \circ \psi + \hat{\psi} \circ \phi \end{aligned}$$

Dieser Ausdruck ist sowohl in ϕ als auch in ψ linear. Wegen $\deg(-\phi) = \deg(\phi)$ und $\deg(\phi) \geq 0$, mit Gleichheit genau für $\phi = 0$, folgt die Behauptung. □

Korollar. *Der Endomorphismenring* $\mathrm{End}(E)$ *einer elliptischen Kurve* E *ist nullteilerfrei.*

Beweis. Aus $\phi \circ \psi = 0$ folgt $0 = \deg(\phi \circ \psi) = \deg(\phi)\deg(\psi)$, da $\mathbb{Z}$ Integritätsring und die Gradabbildung nicht-entartet ist, muss dann bereits $\phi = 0$ oder $\psi = 0$ in $\mathrm{End}(E)$ gelten. □

Die Struktur der Torsionsgruppen

Korollar 3 (ibid., Coroll. 6.4)**.** *Ist* E *eine elliptische Kurve über einem Körper* k *und* $m \in \mathbb{Z}$, $m \neq 0$. *Wenn* $char(k) = 0$ *oder* m *prim zu* $char(k)$ *ist, so gilt*

$$E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z}).$$

Für $char(k) = p$ *hingegen gilt entweder*

$$E[p^r] = \{\mathcal{O}\}, \qquad \textit{für alle } r = 1, 2, \ldots$$

oder

$$E[p^r] \simeq (\mathbb{Z}/p^r\mathbb{Z}), \qquad \textit{für alle } r = 1, 2, \ldots \ .$$

Beweis. (Nach [Sil86] S. 89f.) Unter den angegebenen Voraussetzungen ist $[m]$ eine finite, separable Abbildung. Da $\deg([m]) = m^2$, gilt dann $\sharp E[m] = deg[m] = m^2$ und für jedes d mit $d \mid m$ gilt $\sharp E[d] = d^2$. Daraus ergibt sich $E[m] \simeq (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$.

Bezeichne Fr den p-Frobenius-Endomorphismus. Für $E[p^r]$ gilt

$$\begin{aligned}\sharp E[p^r] = \deg_{sep}[p^r] = (\deg_{sep}(Fr \circ \widehat{Fr}))^r \\ = (\deg_{sep} \widehat{Fr})^r.\end{aligned}$$

Ist nun $\widehat{Fr}$ inseparabel, so ist $\deg_{sep} \widehat{Fr} = 1$ und somit $\sharp E[p^r] = 1$, ist $\widehat{Fr}$ hingegen separabel, so ist

$$\deg_{sep} \widehat{Fr} = \deg \widehat{Fr} = \deg Fr = p,$$

folglich also $\sharp E[p^r] = p^r$. Daraus ergibt sich die Behauptung. □

Definition 13. Ist E eine elliptische Kurve über einem Körper k der Charakteristik $p > 0$, so heißt E *supersingulär*, wenn E triviale p-Torsion hat, d.h. wenn $E[p^r] = \{\mathcal{O}\}$. Sonst heißt E *gewöhnlich*.

Aus dem Beweis ergibt sich noch:

Korollar 4. *Bezeichne Fr_r den p^r-Frobenius-Endomorphismus. Dann sind die folgenden Aussagen äquivalent:*

- *E supersingulär*
- *$\widehat{Fr}_r$ (rein) inseparabel für ein (und somit alle) $r \geq 1$*
- *$\sharp E[p^r] = 1$ für ein (und somit alle) $r \geq 1$.*

Beweis. Es ist $\deg_{\text{sep}} \widehat{Fr}_r = (\deg_{\text{sep}} Fr)^r$. D.h. nach dem vorherigen Beweis

$$1 = \deg_{\text{sep}} \widehat{Fr} \Leftrightarrow 1 = \deg_{\text{sep}} \widehat{Fr}_r \Leftrightarrow \sharp E[p^r] = 1,$$

für ein beliebiges $r \geq 1$. □

Wir werden uns im Abschnitt 1.4 nochmals näher mit supersingulären elliptischen Kurven befassen.

Wir wollen hier noch einen Satz angeben, der die grundsätzliche Frage, welche Struktur $\text{End}(E)$ haben kann, beantwortet. Vorher wiederholen wir eine Definition aus der Algebra:

Definition 14. Eine $\mathbb{Q}$-Algebra $\mathcal{A}$ der Form

$$\mathcal{A} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta, \quad \text{mit}$$
$$\alpha^2, \beta^2 \in \mathbb{Q}, \qquad \alpha^2 < 0, \qquad \beta^2 < 0, \qquad \alpha\beta = -\beta\alpha$$

bezeichnet man als (definite) Quaternionenalgebra (über $\mathbb{Q}$).

Beispiel. Das wohl einfachste Beispiel ist die Quaternionalgebra $\mathcal{Q}$ mit

$$\alpha^2 = \beta^2 = -1.$$

Tensoriert man diese mit $\mathbb{R}$, so erhält man die hamiltonschen Quaternionen.

Satz 19 ([Sil86], Theorem III.9.4, S. 100f)**.** *Ist E eine elliptische Kurve, so ist* $\mathrm{End}(E)$ *entweder isomorph zu $\mathbb{Z}$, oder zu einer Ordnung eines imaginärquadratischen Zahlkörpers, oder zu einer Ordnung in einer Quaternionenalgebra.*

Bemerkung 8. Zum Beweis dieses Satzes werden tatsächlich nur folgende Aussagen verwendet, die wir bis auf die letzte alle schon kennengelernt haben:

- $\mathrm{End}(E)$ ist ein (freier) $\mathbb{Z}$-Modul
- Die Existenz einer Involution $\phi \to \hat{\phi}$ auf $\mathrm{End}(E)$
- Die Existenz einer positiv definiten quadratischen Form auf $\mathrm{End}(E)$, der Gradabbildung.
- $\dim_{\mathbb{Q}} \mathrm{End}(E) \otimes \mathbb{Q} \leq 4$.

Die letzte Aussage benötigt tieferliegende Hilfsmittel, die wir später darstellen werden, siehe Korollar 8 auf Seite 37.

Anzahl der rationalen Punkte von E

Satz 20. *Sei E eine elliptische Kurve, die über dem endlichen Körper $k = \mathbb{F}_q$ definiert ist. Weiterhin sei $Fr \in \mathrm{End}_k(E)$ der q-Frobenius-Endomorphismus von E. Dann gilt:*

1. *Die Anzahl der rationalen Punkte von E über k, $\sharp E(k)$ ist*

$$\sharp E(k) = \deg\big(Fr - 1\big) = q + 1 - t,$$
$$\text{mit} \qquad t = Fr + \widehat{Fr},$$

wobei die ganzen Zahlen t, q mittels $\mathbb{Z} \hookrightarrow \mathrm{End}_k(E)$ mit $[t]$ und $[q]$ identifiziert werden.

2. *Man hat die Abschätzung*

$$\big|\sharp E(k) - (q+1)\big| \leq 2\sqrt{q},$$

insbesondere ist $|t| \leq 2\sqrt{q}$.

3. *In* $\mathrm{End}_k(E)$ *gilt die Relation*

$$Fr^2 - tFr + q = 0.$$

Beweis. Zu 1.: Da $\mathrm{Gal}(\bar{k} \mid k)$ als topologische Gruppe von Fr erzeugt wird, liegt ein Punkt $P \in E(\bar{k})$ genau dann in $E(k)$, wenn $Fr(P) = P$. Also

$$\ker\big(Fr - 1\big) = E(k),$$

und somit

$$\begin{aligned}\sharp\big(E(k)\big) = \deg\big(Fr-1\big) &= \big(Fr-1\big)\big(\widehat{Fr}-1\big)\\ &= Fr\widehat{Fr} - (Fr + \widehat{Fr}) + 1 = q - t + 1.\end{aligned}$$

Zu 2.: Wir haben in Satz 18 gesehen, dass die Gradabbildung eine positiv definite quadratische Form $\deg : \mathrm{End}(E) \to \mathbb{Z}$ darstellt. Also gilt für jedes $r, s \in \mathbb{Z}$, $s \neq 0$

$$0 \leq \frac{1}{s^2}\deg\big(r - sFr\big) = \frac{1}{s^2}\big(r^2 - trs + qs^2\big) = \big(\frac{r}{s}\big)^2 - t\frac{r}{s} + q.$$

Es folgt, dass das Polynom $X^2 - tX + q \in \mathbb{Q}[X]$ nicht-positive Diskriminante hat, $t^2 - 4q \leq 0$, und somit

$$\big|\sharp E(k) - q - 1\big| = \big|t\big| \leq 2\sqrt{q}.$$

Zu 3.: Es gilt

$$\begin{aligned}0 &= (Fr - \widehat{Fr})(Fr - Fr)\\ &= Fr^2 - (Fr + \widehat{Fr})Fr + Fr\widehat{Fr}\\ &= Fr^2 - tFr + q.\end{aligned}$$

Dies war zu zeigen.

□

Definition 15. Wir bezeichnen das durch die polynomiale Relation in 3. gegebene Polynom

$$X^2 - tX + q$$

als das *charakteristische Polynom* des Frobenius Fr von E, und

$$t = (Fr + \widehat{Fr})$$

als seine *Spur*.

Dann gilt:

$$E \text{ supersingulär } \Leftrightarrow \widehat{Fr} \text{ inseparabel } \Leftrightarrow t \equiv 0 \mod p,$$

nach Satz 20 zusammen mit Korollar 4. Die letzte Äquivalenz ergibt sich, indem man 16 auf $\widehat{Fr} = t - Fr$ anwendet. Ist aber $\mathrm{End}\big(E\big) = \mathrm{End}_k\big(E\big)$, so werden wir später, in Abschnitt 1.5.2, sehen:

$$E \text{ supersingulär } \Leftrightarrow t = \pm 2\sqrt{q} \text{ mit } \sqrt{q} \in \mathbb{N}.$$

1.2.3 Endomorphismen abelscher Varietäten

Man kann viele der Aussagen, die wir auf den letzten Seiten über elliptische Kurven gemacht haben, auf abelsche Varietäten verallgemeinern.

Im Folgenden sei A eine abelsche Varietät der Dimension g und k ihr Grundkörper.

Satz 21 ([MilAb], Prop 9.13, S. 44)**.** *Die Gradabbildung deg* : $\mathrm{End}(A) \to \mathbb{Z}$, $\alpha \mapsto \deg \alpha$ *ist eine homogene polynomiale Abbildung vom Grad* $2g$*.*

Satz 22 ([MilAb], Th. 9.9, S.43)**.** *Sei A eine abelsche Varietät der Dimension g über einem Grundkörper k, und $\alpha \in \mathrm{End}(A)$, so gibt es ein eindeutig bestimmtes normiertes Polynom $P_\alpha \in \mathbb{Z}[X]$ vom Grad $2g$ mit*

$$P_\alpha\big(r\big) = \deg\big(\alpha - r\big) \textit{ für alle } r \in \mathbb{Z}.$$

Bemerkung 9. Die beiden vorangehenden Sätze behalten über $\mathrm{End}(A) \otimes \mathbb{Q}$ ihre Richtigkeit, wenn man für $\alpha \notin \mathrm{End}(A)$, $n\alpha \in \mathrm{End}(A)$ die Definitionen von $\deg(\alpha)$ und $P_\alpha(X)$ durch

$$\deg_\alpha = n^{-2g} \deg_{n\alpha}, \qquad P_\alpha\big(X\big) = n^{-2g} P_{n\alpha}\big(nX\big)$$

erweitert.

Definition 16. Wir bezeichnen das Polynom P_α als das *charakteristische Polynom* von α und definieren die *Spur* $\mathrm{Tr}(\alpha)$ durch die Gleichung

$$P_\alpha(X) = X^{2g} - \mathrm{Tr}\big(\alpha\big) X^{2g-1} + \cdots + \deg\big(\alpha\big).$$

Der Frobenius-Endomorphismus einer abelschen Varietät
Ist der Grundkörper von A endlich, $k = \mathbb{F}_q$, so ist die Frobenius-Abbildung

$$Fr \,:\, \big(x_0 : \cdots : x_n\big) \mapsto \big(x_0^q : \cdots : x_n^q\big)$$

ein Endomorphismus von A. Es gilt dann der folgende Satz:

Satz 23 ([MilAV], Th. 19.1)**.** *Sei $P_{Fr}(X)$ das charakteristische Polynom des Frobenius-Endomorphismus von A und $P_{Fr}(X) = \prod_i^{2g}\big(X - a_i\big)$ dessen Zerlegung in Linearfaktoren über $\overline{\mathbb{Q}}$, so gilt:*

$$\sharp A\big(\mathbb{F}_{q^m}\big) = \prod_{i=1}^{2g}\big(1 - a_i^m\big) \text{ für alle } m \geq 1, \tag{1.6}$$

$$\text{und} \qquad |a_i| = q^{1/2}. \qquad \text{(Riemann-Hypothese)}$$

daher hat man die Abschätzung

$$\big|\sharp A\big(\mathbb{F}_q\big)\big| \leq 2gq^{g-1/2} + \big(2^{2g} - 2g - 1\big)q^{g-1}.$$

1.3 Zetafunktionen

Im Folgenden ist $k = \mathbb{F}_q$, ein endlicher Körper der Charakteristik $p > 0$, $\bar{k} = \overline{\mathbb{F}}_q$ der algebraische Abschluss.

Definition 17 (Weilsche Zetafunktion)**.** Ist V eine über $k = \mathbb{F}_q$ definierte glatte projektive Varietät, so ist die *Zetafunktion* von V durch die folgende Potenzreihe $\in \mathbb{Q}\big[[X]\big]$ definiert:

$$Z\big(V, X\big) = \exp\bigg(\sum_{m=1}^{\infty} N_m \frac{X^m}{m}\bigg), \qquad \text{mit } N_m = \sharp V\big(\mathbb{F}_{q^m}\big). \tag{1.7}$$

Beispiel. Das einfachste Beispiel ist $V = \mathbb{P}^1$. Da die projektive Gerade über $\mathbb{F}_{q^m}$ für jedes $m \geq 1$ aus $q^m + 1$ Punkten besteht, ist

$$Z\big(\mathbb{P}^1, X\big) = \exp\bigg(\sum_{m=1}^{\infty}(q^m + 1)\frac{X^m}{m}\bigg) = \\ = \exp\Big(\log\frac{1}{1-X} \;+\; \log\frac{1}{1-qX}\Big) = \frac{1}{(1-X)(1-qX)}.$$

Entsprechend erhält man für $V = \mathbb{P}^n$

$$\sharp\mathbb{P}^n\big(\mathbb{F}_{q^m}\big) = \big(1 + q^m + (q^m)^2 + \cdots + (q^m)^n\big) \\ \Rightarrow\; Z\big(\mathbb{P}^n\big) = \frac{1}{(1-X)(1-qX)\cdots(1-q^nX)}.$$

André Weil vermutete 1949 in [Wei49] eine Reihe von Eigenschaften der Zetafunktion $Z(V, X)$, für jede Varietät V über k.

Theorem 4 (Weil-Vermutungen)**.** *Sei V eine glatte projektive Varietät der Dimension n über dem endlichen Körper k, so hat die Zetafunktion $Z\big(V,X\big)$ von V folgende Eigenschaften*

1. Rationaliät:
$$Z\big(V,X\big) \ \in \mathbb{Q}(X).$$

2. Funktionalgleichung:
$$Z\Big(V,\frac{1}{q^n X}\Big) = \pm\, q^{nE/2} X^E Z\big(V,X\big), \tag{1.8}$$
dabei ist E die Schnittzahl der Diagonale $\Delta = V \times V$ mit sich selbst und entspricht der Euler-Poincaré Charakteristik von V.

3. Riemann-Vermutung:
$$Z\big(V,X\big) = \frac{P_1(X)P_3(X)\cdots P_{2n-1}(X)}{P_0(X)P_2(X)\cdots P_{2n}(X)}, \tag{1.9}$$
hierbei sind $P_0(X) = 1-X$, $P_{2n}(X) = 1-q^nX$ und für jedes $i = 1,\ldots,2n$ ist $P_i(X)$ ein Polynom $\in \mathbb{Z}[X]$, dass sich über $\overline{\mathbb{Q}}$ schreiben lässt als
$$P_i(X) = \prod_j \big(1-\alpha_{ij}X\big),$$
mit ganzen algebraischen Zahlen α_{ij}, für die $|\alpha_{ij}| = q^{i/2}$.

Bemerkung 10. Die Analogie zur riemannschen Zetafunktion wird nach einer Substitution $t \to q^{-s}$ deutlicher. Setzt man
$$\zeta\big(V,s\big) = Z\big(V,q^{-s}\big)$$
mit komplexen Argumenten s, so wird aus der (formalen) Potenzreihe eine meromorphe Funktion, mit der Funktionalgleichung
$$\zeta\big(V,n-s\big) = \pm\, q^{E(n/2-s)}\zeta\big(V,s\big).$$

Bemerkung 11 (Zur Geschichte des Theorems 4). Eine Reihe von Aussagen, die man heute als Speziallfälle des Theorems ansehen kann, finden sich schon bei Gauss. E. Artin zeigte in seiner Dissertation die obigen Eigenschaften für einige spezielle elliptische und hyperelliptische Kurven, Hasse konnte sie dann für elliptische Kurven allgemein nachweisen, und Weil erbrachte 1948 in [Wei48] den allgemeinen Beweis für Kurven. 1949 äußerte er dann, nachdem er dort entsprechende Aussagen für bestimmte Flächen bewiesen hatte,

siehe Abschnitt 2.2, in seiner Arbeit [Wei49] das allgemeine Theorem als Vermutung. Damit gab er ein Programm vor, welches die weitere Entwicklung der algebraischen Geometrie maßgeblich beeinflussen sollte. DWORK zeigte 1959 die Rationalität und die Funktionalgleichung, aber erst P. DELIGNE konnte 1973 durch den Nachweis der Riemann-Vermutung den Beweis des Theorems abschließen.

1.3.1 Weil-Vermutung für elliptische Kurven und abelsche Varietäten

Elliptische Kurven Wir wollen nun die Weil-Vermutungen für elliptische Kurven beweisen. Das wesentliche Hilfsmittel dazu haben wir schon mit Satz 20 auf Seite 18 bereitgestellt.

Satz 24. *Ist E eine elliptische Kurve über einem endlichen Körper $k = \mathbb{F}_q$, so hat die Zetafunktion von E folgende Form:*

$$Z\big(E,X\big) = \frac{1 - tX + qX^2}{\big(1-X\big)\big(1-qX\big)} \quad \textit{mit } t = \operatorname{Tr} Fr \in \mathbb{Z}. \tag{1.10}$$

Der Zähler von $Z(E,X)$ faktorisiert dabei über $\overline{\mathbb{Q}}$ als

$$\begin{gathered} 1 - tX + qX^2 = \big(1-\alpha X\big)\big(1-\overline{\alpha}X\big), \\ \textit{mit} \qquad \big|\alpha\big| = \sqrt{q}. \end{gathered} \tag{1.11}$$

Nach [Sto00], S.36f. In Satz 20 haben wir bereits gesehen, dass die Spur t des Frobenius Fr ganzzahlig ist und die Ungleichung $|t| \leq 2\sqrt{q}$ erfüllt. Das charakteristische Polynom des Frobenius aus Definition 15 hat somit Diskriminante ≤ 0, folglich gilt

$$X^2 - tX + q = \big(X-\alpha\big)\big(X-\overline{\alpha}\big),$$

mit $\alpha, \overline{\alpha} \in \overline{\mathbb{Q}}$, $|\alpha| = \sqrt{q}$ und $\overline{\alpha}$ konjugiert zu α. Hieraus folgt die Zerlegung (1.11) für die behauptete Form des Zählers. Andererseits ergibt nach Satz 20 das Einsetzen von Fr in sein charakteristisches Polynom Null, und somit gilt über $\mathbb{Z}[Fr]$:

$$X^2 - tX + q = \big(X - Fr\big)\big(X - \widehat{Fr}\big).$$

Damit haben wir einen Ringisomorphismus

$$\begin{aligned} \mathbb{Z}[\alpha] \;&\to\; \mathbb{Z}[Fr] \hookrightarrow \operatorname{End}(E) \\ \alpha &\mapsto Fr, \end{aligned}$$

der auch für $t = 0$, i.e. $\alpha = \pm\imath\sqrt{q}$ definiert ist, da $\mathrm{End}(E)$ ein Integritätsring ist. Aus dem Beweis von Satz 20 wissen wir

$$\sharp E(k) = q + 1 - Fr - \widehat{Fr},$$

womit nun

$$\sharp E(k) = q + 1 - \alpha - \overline{\alpha}.$$

Da Fr^m für $m \geq 1$ der Frobenius-Endomorphismus von $\mathbb{F}_{q^m}$ ist, gilt ebenso

$$\sharp E\big(\mathbb{F}_{q^m}\big) = q^m + 1 - Fr^m - \widehat{Fr}^m = q + 1 - \alpha^m - \overline{\alpha}^m.$$

Damit können wir den Beweis abschließen:

$$\begin{aligned} Z\big(E, X\big) &= \exp\Big(\sum_{m=1}^{\infty} \frac{\sharp E(\mathbb{F}_{q^m})}{m} X^m\Big) \\ &= \exp\Big(\sum_{m=1}^{\infty} \frac{\big(qX\big)^m}{m} + \sum_{m=1}^{\infty} \frac{X^m}{m} - \sum_{m=1}^{\infty} \frac{\big(\alpha X\big)^m}{m} - \sum_{m=1}^{\infty} \frac{\big(\overline{\alpha} X\big)^m}{m}\Big) \\ &= \exp\Big(\log \frac{1}{1-qX} + \log \frac{1}{1-X} - \log \frac{1}{1-\alpha X} - \log \frac{1}{1-\overline{\alpha} X}\Big) \\ &= \frac{\big(1-\alpha X\big)\big(1-\overline{\alpha} X\big)}{\big(1-X\big)\big(1-qX\big)} = \frac{1 - tX + qX^2}{\big(1-X\big)\big(1-qX\big)}. \end{aligned}$$

□

Bemerkung 12. Die Funktionalgleichung von $Z(E, X)$ lautet

$$Z\big(E, \frac{1}{qX}\big) = Z\big(E, X\big).$$

Als nächstes wollen wir die Rationalität und die Riemann-Vermutung auch allgemeiner für die Zetafunktionen einer abelschen Varietät zeigen, vgl. hierzu [MilAb], oder [MilAV], § 19.

Satz 25 ([MilAV], Cor. 19.4)**.** *Sei A eine abelsche Varietät der Dimension g über $k = \mathbb{F}_q$. Weiterhin sei $P_{Fr}(X)$ das charakteristische Polynom des q-Frobenius-Endomorphismus von A, mit der Faktorisierung $P_{Fr}(X) = \prod_i^{2g}\big(X - a_i\big)$ über $\overline{\mathbb{Q}}$, wie in Satz 23, auf Seite 21. Dann gilt*

$$Z\big(A, X\big) = \frac{P_1(X) \cdots P_{2g-1}(X)}{P_0(X) P_2(X) \cdots P_{2g-2}(X) P_{2g}(X)},$$

mit $P_k(X) = \prod\big(1 - a_{i,k}X\big)$ für $k = 1, 2, \ldots, 2g$, wobei $a_{i,k}$ für festes k über alle Produkte $a_{i_1} \cdots a_{i_k}$, $0 < i_1 < \cdots < i_r \leq 2g$ läuft.

Beweis. Aus Satz 23 wissen wir bereits

$$\sharp A\big(F_{q^m}\big) = \prod_{i=1}^{2g}\big(1 - a_i^m\big)$$

Damit ergibt sich ergibt sich in Analogie zum vorherigen Beweis

$$\begin{aligned} Z\big(A,X\big) &= \exp\Big(\sum_{m=1}^{\infty} \frac{\prod_{i=1}^{2g}(1-a_i^m)}{m} X^m\Big) \\ &= \exp\Big(\sum_{m=1}^{\infty}\Big(1 + \sum_{k=1}^{2g}(-1)^k \sum_{(i)=(i_1,\dots,i_k)} \prod_{j=1}^{k} a_{i_j}^m\Big)\frac{X^m}{m}\Big) \\ &= \exp\Big(\log\frac{1}{1-X} + \sum_{k=1}^{2g}(-1)^k \sum_{(i)=(i_1,\dots,i_k)} \log\frac{1}{1 - X\prod_{j=1}^{k} a_{i_j}}\Big) \\ &= \frac{P_1(X)\cdots P_{2g-1}(X)}{P_0(X)P_2(X)\cdots P_{2g-2}(X)P_{2g}(X)}, \end{aligned}$$

wobei in der 2. und 3. Zeile die a_{i_j} aus $\{a_i \,:\, i = 1,\dots,2g\}$ sind und $\operatorname{grad} P_k(X) = \binom{2g}{k}$. □

Da die a_i alle nach Satz 23 $|a_i| = q^{1/2}$ erfüllen, ist $|a_{i,k}| = q^{k/2}$, damit ist klar:
Für abelsche Varietäten über endlichen Körpern gilt die Riemann-Vermutung aus Theorem 4.

1.3.2 Zetafunktionen von Kurven und jacobische Varietäten

Der nachfolgende Satz, den wir ohne Beweis angeben wollen, schließt Satz 24 als Spezialfall ein und stellt ein weiteres Beispiel für Theorem 4 dar.

Satz 26 (Weil-Vermutung für Kurven)**.** *Sei C eine glatte projektive Kurve über k, und sei g das Geschlecht von C, dann gilt*

1. $Z\big(C,X\big) \in \mathbb{Q}[t]$ *ist eine rationale Funktion*
2. $Z\big(C,1/(qX)\big) = q^{1-g}X^{2-2g}Z\big(C,X\big))$
3. $Z\big(C,X\big) = P(X)/\big((1-X)(1-qX)\big)$ *mit einem Polynom* $P(X) \in \mathbb{Z}[X]$ *vom Grad* $2g$*, welches (über* $\mathbb{C}$*) folgermaßen faktorisiert*

$$P(X) = \prod_{j=1}^{g}(1-\alpha_j X)(1-\bar{\alpha}_j X),$$

wobei α_j ganzalgebraisch mit $|\alpha_j| = q^{1/2}$.

Zu diesem Satz vergleiche etwa [Sto00], S. 37, ein Beweis mittels Schnittzahlen wird in [Har77], App. C, Ex. 5.7 und V, Ex. 1.10 skizziert. Die Hauptaussage dieses Satz wird sich bald als Korollar zu Satz 28 ergeben.

Jacobische Varietäten von Kurven

Zu einer glatten projektiven Kurve C vom Geschlecht g, die über einem Körper k definiert ist, gibt es eine abelsche Varietät der Dimension g, die Jacobische von C, die durch eine Reihe äquivalenter Eigenschaften bestimmt ist und jeweils über diese definiert werden kann. Als Grundreferenz für diesen Abschnitt dient hierbei [MilJV].

Definition 18. Sei C eine nichtsinguläre projektive Kurve über einem Körper k und $C^r = C \times \cdots \times C$ das r-fache Produkt von C mit sich selbst. Wir definieren die *r-fache symmetrische Potenz* $C^{\langle r \rangle}$ durch den Quotienten

$$C^{\langle r \rangle} = C^r / S_r,$$

wo S_r die symmetrische Gruppe mit $r!$ Elementen ist, d.h. $C^{\langle r \rangle}$ besteht aus den ungeordneten r-Tupel von Punkten von C. Weiterhin bezeichnen wir mit π die Quotientenabbildung $C^r \to C^{\langle r \rangle}$, $(P_1, \ldots, P_r) \mapsto \sum_i P_i$.

es gilt dann

Lemma 2. *Für eine nichtsinguläre Kurve C ist $C^{\langle r \rangle}$ eine nichtsinguläre Varietät.*

Bemerkung 13. Zu genaueren Details der Konstruktion siehe [MilJV], §3, ab S. 174.

Satz 27. *Sei C eine nichtsinguläre projektive Kurve vom Geschlecht $g > 0$ über einem Körper k. Dann gibt es eine abelsche Varietät J der Dimension g, sowie eine kanonische Abbildung $f : C \to J$. die durch jede der folgenden Eigenschaften eindeutig bestimmt sind:*

1. *J ist birational äquivalent zu $C^{\langle g \rangle}$*
   (vgl. [MilJV], §5 ab S. 182 insbesondere Theorem 5.1, Remark 5.6, sowie §7 ab S. 189)

2. *Ist $h : C \to A$ eine rationale Abbildung von C in eine abelsche Varietät, dann gibt es einen eindeutig bestimmten Homomorphismus $\alpha : J \to A$, so, dass $h = \alpha \circ f + a$ mit einem $a \in A$. Sind f, h über k definiert und $C(k) \neq \emptyset$, so ist auch α über k definiert und $a \in A(k)$. ([La], Theorem 9 auf S. 35, vgl. auch [MilJV] Prop. 6.1 und 6.4, S. 185f)*

Definition 19. Die abelsche Varietät J aus Satz 27 heißt die *jacobische Varietät* von C, wir schreiben $J(C)$.

Satz 28 ([MilJV], Th. 11.1, S. 200)**.** *Sei C eine nichtsinguläre projektive Kurve vom Geschlecht g über einem endlichen Körper $k = \mathbb{F}_q$. Sei weiterhin J die Jacobische von C, $P_J(X)$ das charakteristische Polynom des k-Frobenius-Endomorphismus von J und $P_J(X) = \prod_{i=1}^{2g}\big(X - a_i\big)$ dessen kanonische Zerlegung in irreduzible Faktoren. Dann gilt: Die Anzahl der k-rationalen Punkte von C erfüllt*

$$\sharp C(k) = 1 - \sum_{i=1}^{2g} a_i + q.$$

Insbesondere ist $\big|\sharp C(k) - q - 1\big| \leq 2gq^{1/2}$.

Korollar 5. *Für die Zetafunktion von $Z(C, X)$ von C gilt*

$$Z\big(C, X\big) = \frac{\prod_{i=1}^{2g}\big(1 - a_i X\big)}{\big(1 - X\big)\big(1 - qX\big)}, \tag{1.12}$$

mit den a_i aus Satz 28.

Beweis. Bezeichne $P_J^m(X)$ das charakteristische Polynom des q^m-Frobenius-Endomorphismus von J, so folgt durch Anwendung von Satz 23 auf die abelsche Varietät J, dass $P_J^m(X) = \prod_{i=1}^{2g}\big(X - a_i^m\big)$. Damit ergibt sich

$$\sharp C\big(\mathbb{F}_{q^m}\big) = 1 - \sum_{i=1}^{2g} a_i^m + q^m.$$

Analog zum Beweis von Satz 24 erhält man nun

$$\begin{aligned} Z\big(C, X\big) &= \exp\Big(\sum_{m=1}^{\infty}\big(1 + q^m - \sum_{i=1}^{2g} a_i^m\big)\frac{X^m}{m}\Big) \\ &= \exp\Big(\log\frac{1}{1-X} + \log\frac{1}{1-qX} - \sum_{i=1}^{2g}\log\frac{1}{1-a_iX}\Big) \\ &= \frac{\prod_{i=1}^{2g}\big(1 - a_iX\big)}{\big(1 - X\big)\big(1 - qX\big)}. \end{aligned}$$

□

1.4 Supersinguläre elliptische Kurven

In Definition 13, auf Seite 17, hatten wir supersinguläre elliptische Kurven durch die Eigenschaft $E[p^r] = 0$, für jedes r, definiert. Aus dem Beweis 3, Seite 17 hatten wir außerdem gesehen, dass E supersingulär genau dann, wenn $\widehat{Fr}$ rein inseparabel ist (Korollar 4). Wir wollen nun einige weitere Eigenschaften supersingulärer elliptischer Kurven kennenlernen. Basisreferenz sind hierbei [Sil86], Chapter V, besonders § 3 und § 4 ab Seite 137, sowie [Hus], Ch. 13 ab S. 242. Ein großer Teil der hier behandelten Aussagen geht auf die grundlegenden Untersuchungen von Max Deuring zurück, [Deu41].

Um die Notation zu vereinfachen, werden wir nachfolgend für eine p-Potenz p^r, $r \geq 1$, den p^r-Frobenius durch Fr_r statt Fr_{p^r} notieren.

Lemma 3. *E ist supersingulär genau dann, wenn $[p]$ (rein) inseparabel ist.*

Beweis. Es ist

$$\deg_{\text{sep}}[p] = \deg_{\text{sep}}(Fr \circ \widehat{Fr}) = \deg_{\text{sep}} \widehat{Fr}$$

also

$$\deg_{\text{sep}} \widehat{Fr} = 1 \;\Leftrightarrow\; \deg_{\text{sep}}[p] = 1,$$

was äquivalent zur Behauptung ist. □

Lemma 4. *Gibt es (mindestens) ein $r \geq 1$, für welches der p^r-Frobenius $Fr_r \in \mathbb{Z}$, dann gilt E ist supersingulär.*

Beweis. Ist $Fr_r \in \mathbb{Z} \subset \text{End}(E)$. Da

$$[p^r] = \widehat{Fr_r} \circ Fr_r = \deg {Fr_r}^2$$

folgt nun $Fr_r = [\pm p^{r/2}]$ (und r muss gerade sein), dann ist aber

$$\sharp E[p^{r/2}] = \deg_{\text{sep}} Fr_r = 1,$$

da der Frobenius rein inseparabel ist. Also hat E triviale $p^{r/2}$ Torsion und ist somit supersingulär. □

Lemma 5. *Ist $\text{End}_{\bar{k}} E$ eine Ordnung in einer Quaternionenalgebra, so ist E supersingulär.*

Beweis. Ist $\phi \in \text{End}(E)$ über k_r definiert, so gilt

$$\phi \circ Fr_r = Fr_r \circ \phi,$$

denn ϕ ist eine polynomiale Abbildung $(x, y) \to \big(f(x, y), g(x, y)\big)$, die genau dann über k_r definiert ist, wenn $f, g \in k_r[x, y]$, d.h. also wenn

$$Fr_r\big(f(x, y)\big) = f(x, y).$$

Außerdem gilt natürlich für $n \in \mathbb{Z}$

$$\phi \circ [n] = [n] \circ \phi.$$

Also: $\mathbb{Q}[Fr_r]$ ist Teilmenge des Zentrums von von $\mathrm{End}_{k_r}(E) \otimes \mathbb{Q}$. Ist nun aber $\mathrm{End}_{\bar{k}}(E)$ eine Ordnung einer Quaternionenalgebra, so ist das Zentrum von $\mathrm{End}_k(E) \otimes \mathbb{Q}$ gleich $\mathbb{Q}$. Das bedeutet, es gibt ein s, so, dass $Fr_r \in \mathbb{Z}$ für jedes $r \geq s$ mit $s \mid r$. Nach dem vorherigen Lemma ist dann E supersingulär. □

Bemerkung 14. Tatsächlich ist $\mathbb{Q}[Fr_r]$ *gleich* dem Zentrum von $\mathrm{End}_{k_r}(E) \otimes \mathbb{Q}$.

Es gilt auch die Umkehrung:

Lemma 6 (ohne Beweis, vgl. z.B. [Sil86], Th. V 3.1, S. 137)**.** *Ist E supersingulär, so ist $\mathrm{End}_{\bar{k}}(E)$ eine Ordnung in einer Quaternionenalgebra.*

Wir werden später noch einen eigenen Beweis hierfür erbringen, Korollar 8 in Abschnitt 1.5.

Satz 29. *Sei k ein endlicher Körper der Charakteristik p. Und sei E eine elliptische Kurve über k. Es gilt dann:*

1. *E ist supersingulär genau dann, wenn*
   - $\mathrm{End}_{\bar{k}}(E)$ *eine Ordnung in einer Quaternionenalgebra ist*
   - $Fr_r \in \mathbb{Z}$ *für ein $r \geq 1$*
2. *E ist gewöhnlich genau dann, wenn*
   - $\mathrm{End}_{\bar{k}}(E)$ *eine Ordnung in einem quadratischen Zahlkörper ist*
   - $Fr_r \notin \mathbb{Z}$ *für alle $r \geq 1$*

Beweis. Wir haben bereits gesehen: Die Tatsache, dass $\mathrm{End}(E)$ in einer Quaternionenalgebra liegt, ist äquivalent dazu, dass E supersingulär. Im Beweis von Lemma 5 haben wir außerdem gesehen, dass die Nichtkommutativität von $\mathrm{End}(E)$ die Ganzzahligkeit des Frobenius impliziert, woraus wiederum E supersingulär folgt, nach Lemma 4.
Es bleibt also nur noch zu zeigen: Ist E gewöhnlich, so ist $\mathrm{End}_{\bar{k}}(E)$ Ordnung in einem quadratischen Zahlkörper. Aus E gewöhnlich folgt $Fr_r \notin \mathbb{Z}$, $\forall r$, dann ist aber $\mathrm{End}_{\bar{k}}(E) > \mathbb{Z}$, es handelt sich aber nicht um eine Ordnung in einer Quaternionenalgebra. Dies ergibt die Behauptung. □

Satz 30 ([Sil86], Th. V.3.1a, (iii))**.** *Sei k ein endlicher Körper der Charakteristik p und E eine supersinguläre elliptische Kurve über k. Es gilt dann $j(E) \in \mathbb{F}_{p^2}$.*

Jede supersinguläre elliptische Kurve in Charakteristik p ist also (bis auf Isomorphie) bereits über $\mathbb{F}_p$ oder $\mathbb{F}_{p^2}$ definiert.

Beweis. Da $\widehat{Fr}_1 : E^{(p)} \to E$ nach Voraussetzung inseparabel ist, vom Grad p, können wir Korollar 2, Seite 15, anwenden. Es ergibt sich dann, dass $\widehat{Fr}_r$ sich als Kompositum

$$E^{(p)} \xrightarrow{Fr'} E^{(p^2)} \xrightarrow{\psi} E$$

darstellen lässt, wobei Fr' die Frobenius-Abbildung $E^{(p)} \to E^{(p^2)}$ und ψ eine separable Abbildung mit $\deg \psi = 1$ ist. Ein Morphismus glatter Kurven vom Grad 1 ist aber ein Isomorphismus (siehe z.B. [Sil86], Cor. 2.4.1, S. 25), und somit ergibt sich:

$$j(E) = j(E^{(p^2)}) = j(E)^{p^2}.$$

Folglich ist $j(E) \in \mathbb{F}_{p^2}$. □

Satz 31 (Kriterien für Supersingularität)**.** *Sei k ein endlicher Körper mit $p = char(k) > 2$.*

- *Ist E eine elliptische Kurve über k mit einer Weierstraß-Gleichung*

  $$E : y^2 = f(x),$$

  wo $f(x) \in k(x)$ ein kubisches Polynom mit (paarweise) verschiedenen Wurzeln in $\bar{k}$ ist. Dann ist E supersingulär genau dann, wenn der Koeffizient von x^{p-1} in $f(x)^{(p-1)/2}$ verschwindet.

- *Ist E eine elliptische Kurve in Legendre-Normalform,*

  $$E : y^2 = x(x-1)(x-\lambda), \qquad 0, 1 \neq \lambda \in \overline{k},$$

  so ist E genau dann supersingulär, wenn das sogenannte Deuring-Polynom,

  $$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i, \qquad \textit{für} \qquad m = \frac{p-1}{2},$$

  bei λ eine Nullstelle hat.

Vergleiche [Sil86], V. Th. 4.1 auf S. 140, sowie [Hus], S. 348ff.

Beweis. (Nach [Sil86], S. 141f) Es sei $q = \sharp k$. Sei $\chi : k^\times \to \{\pm 1\}$ der eindeutig bestimmte nichttriviale Charakter der Ordnung 2, d.h. $\chi(x) = 1$ genau wenn x ein Quadrat in $k^\times$ ist. Erweitert man die Definition von χ auf k durch $\chi(0) = 0$, so kann χ benutzt werden, um die Punkte von $E(k)$ zu zählen, denn

$$\mathcal{O} \neq P = (x, y) \in E(k) \Leftrightarrow f(x) = y^2 \Leftrightarrow \chi\big(f(x)\big) \neq -1.$$

Ist $\chi\big(f(x)\big) = 0$, so erhält man zu x genau einen Punkt, $(x, 0)$, während man für $\chi\big(f(x)\big) = 1$ zwei verschiedene Punkte, $(x, \pm y)$ erhält. Unter Berücksichtigung des zusätzlichen Punktes $\mathcal{O}$ ergibt sich

$$\sharp E(k) = 1 + q + \sum_{x \in k} \chi\big(f(x)\big) = 1 + q + \sum_{x \in k} \big(f(x)\big)^{\frac{q-1}{2}}, \tag{1.13}$$

dabei wurde verwendet, dass $\chi(z) = z^{(q-1)/2}$ für alle $z \in k$, da $\chi(z) = 0$ genau für z gleich 0 und $z^{(q-1)/2} = 1$ genau dann, wenn $\chi(z) = +1$, wegen $z^{q-1} = 1$ für alle $z \in k^\times$. Nun ist aber, ebenfalls wegen $z^{q-1} = 1$ in $k^\times$,

$$\sum_{x \in k^\times} x^i = \begin{cases} -1 & \text{wenn } q - 1 \mid i \\ 0 & \text{wenn } q - 1 \nmid i. \end{cases}$$

Wir multiplizieren nun $f(x)^{(q-1)/2}$ auf der rechten Seite von (1.13) aus. Da $\operatorname{grad} f(x) = 3$, ist der einzige Summand der Form $a_i x^i$, mit $i \mid q - 1$, der zu x^{q-1} gehörige. Also ist

$$\sharp E(K) \equiv 1 - A_q \mod p, \text{ wenn } A_q = \text{Koeffizient von } x^{q-1} \text{ in } f(x)^{(q-1)/2}. \tag{1.14}$$

Dabei ist natürlich $A_q \bmod p$ zu betrachten, da in k summiert wird. Andererseits ist nach Satz 20 auf Seite 18

$$\sharp E(k) = \deg(Fr - 1) = q - t + 1,$$
$$\text{mit } t = Fr + \widehat{Fr}.$$

Vergleicht man dies mit (1.14), so erhält man

$$A_q \equiv +t \pmod p,$$

da aber $\widehat{Fr} = [t] - Fr$, folgt hieraus mit Satz 16, vgl. die Bemerkung nach Definition 15

$$A_q \equiv 0 \bmod p \Leftrightarrow t \equiv 0 \bmod p \Leftrightarrow \widehat{Fr} \text{ inseparabel} \Leftrightarrow E \text{ supersingulär}.$$

Um den Beweis des ersten Teils abzuschließen, müssen wir noch zeigen, dass $A_q = 0$ genau wenn $A_p = 0$, für $q = p^m$, $m > 1$. Wegen $p^{r+1} - 1 = (p^r - 1) + p^r(p-1)$ ist

$$f(x)^{(p^{r+1}-1)/2} = f(x)^{(p^r-1)/2}\big(f(x)^{(p-1)/2}\big)^{p^r}$$

und damit (da $\operatorname{grad} f = 3$)

$$A_{p^{r+1}} = A_{p^r} A_p^{p^r},$$

und die Behauptung folgt per Induktion.

Der zweite Teil des Satzes ist ein Spezialfall des ersten Teils. Denn der Koeffizient A_p von x^{p-1} in $[x(x-1)(x-\lambda)]^m$ ist gleich dem Koeffizienten von x^m in $[(x-1)(x-\lambda)]^n$ und dieser ist gerade

$$A_p = \sum_{i=0}^{m} \binom{m}{i} (-\lambda)^i \binom{m}{m-i} (-1)^{m-i} = (-1)^m H_p(\lambda).$$

□

Eine höchst interessante Folgerung erhält man aus (1.13) und dem Beweis des zweiten Teils.

Korollar 6 ([Hus], Prop. 13.3.9, S. 251)**.** *Sei $k = \mathbb{F}_p$ und E eine über k definierte elliptische Kurve mit*

$$E : y^2 = x\big(x-1\big)\big(x-\lambda\big), \qquad \lambda \in \bar{k}.$$

Dann gilt

$$\sharp E(k) \equiv 1 - (-1)^m H_p(\lambda) \mod p.$$

Insbesondere ist E supersingulär genau dann, wenn $\sharp E(k) \equiv 1 \mod p$, also, wegen Satz 20, Seite 18, genau wenn $\sharp E(k) = p + 1$.

Hieraus ergibt sich mit $\sharp E(k) = p+1-t$ (Satz 20) sofort $t = Fr + \widehat{Fr} = 0$ und mit Satz 24, Seite 23, somit

Korollar 7. *Ist E eine supersinguläre elliptische Kurve, die über $k = \mathbb{F}_p$ definiert ist, so gilt*

$$Z\big(E, X\big) = \frac{1 + pX^2}{\big(1-X\big)\big(1-pX\big)}.$$

Neben den verschiedenen Kriterien, die es erlauben, eine elliptische Kurve als supersingulär zu erkennen, ist auch folgende Bemerkung für die praktische Anwendung wichtig:

Bemerkung 15. Es gibt zu jeder Primzahl p (mindestens) eine elliptische Kurve, die über $\mathbb{F}_p$ supersingulär ist, vgl. [Hus], S. 261.

Wir wollen nun noch einige Beispiel für supersinguläre Kurven angeben:

Beispiel. Betrachten wir folgende Weierstraßgleichung über $k = \mathbb{F}_p$, mit einer ungeraden Primzahl p,

$$E \,:\, y^2 = x^3 + ax, \qquad a \in k.$$

Behauptung: Ist $p \equiv 3 \bmod 4$, so ist E supersingulär.
Wir untersuchen nachfolgend die beiden Endomorphismen $Fr, \lambda \in \mathrm{End}_{\bar{k}}(E)$,

$$\begin{aligned} Fr \,:\, \big(x,y\big) &\longmapsto \big(x^p, y^p\big) \\ \lambda \,:\, \big(x,y\big) &\longmapsto \big(-x, \imath y\big), \end{aligned}$$

wobei $\imath \in \overline{\mathbb{F}}_p$, mit $\imath^2 = -1$. Ist nun (x,y) ein Punkt auf E, so gilt:

$$\begin{aligned} \big(\lambda \circ Fr\big)\,\big(x,y\big) &= \lambda\big(Fr\big(x,y\big)\big) = \lambda\big(x^p, y^p\big) = \big(-x^p, \imath y^p\big) \\ \big(Fr \circ \lambda\big)\,\big(x,y\big) &= Fr\big(\lambda\big(x,y\big)\big) = Fr\big(-x, \imath y\big) = \big((-1)^p x^p, \imath^p y^p\big). \end{aligned}$$

Da p nach Voraussetzung ungerade ist, $(-1)^p = -1$ und $\imath^p = \imath$, wenn $p \equiv 1 \bmod 4$, und $\imath^p \neq \imath$ sonst, also wenn $p \equiv 3 \bmod 4$. In letzteren Fall gilt also

$$Fr \circ \lambda\,\big(x,y\big) = \big(-x^p, \imath^p y^p\big) \neq \big(-x^p, \imath y^p\big) = \lambda \circ Fr\,\big(x,y\big).$$

Damit ist aber $\mathrm{End}_{\bar{k}}(E)$ nicht kommutativ und somit E supersingulär.

Beispiel. Betrachten wir nun über $k = \mathbb{F}_p$, $p \neq 2, 3$, die elliptische Kurve zu der Gleichung

$$E \,:\, y^2 = x^3 + b, \qquad b \in k.$$

Behauptung: Ist $p \equiv 2 \bmod 3$, so ist E supersingulär.
Der Beweis läuft analog wie im vorherigen Beispiel, wir betrachten den Frobenius Fr sowie folgendes $\lambda \in \mathrm{End}_{\bar{k}}(E)$:

$$\lambda \,:\, \big(x,y\big) \longmapsto \big(\zeta x, y\big),$$

mit einer dritten Einheitswurzel $\zeta \in \bar{k}$, also $\zeta^3 = 1$, $\zeta \neq 1$. Es gilt dann

$$\begin{aligned} \big(\lambda \circ Fr\big)\,\big(x,y\big) &= \lambda\big(Fr\big(x,y\big)\big) = \lambda\big(x^p, y^p\big) = \big(\zeta x^p, y^p\big) \\ \big(Fr \circ \lambda\big)\,\big(x,y\big) &= Fr\big(\lambda\big(x,y\big)\big) = Fr\big(\zeta x, y\big) = \big(\zeta^p x^p, y^p\big). \end{aligned}$$

Da $\zeta^2 \neq \zeta$, folgt im Falle $p \equiv 2 \bmod 3$

$$Fr \circ \lambda\,\big(x,y\big) = \big(\zeta^2 x^p, y^p\big) \neq \big(\zeta x^p, y^p\big) = \lambda \circ Fr\,\big(x,y\big),$$

somit ist E supersingulär.

1.5 Tates Ergebnisse von 1966

Wir wollen uns in diesem Abschnitt mit der Arbeit „Endomorphisms of Abelian Varieties over Finite Fields“, [Ta66], von JOHN T. TATE befassen, auch wenn eine genauere Darstellung den Rahmen dieser Diplomarbeit überschreiten würde.

1.5.1 Der Hauptsatz von Tate

Sei im folgenden k ein endlicher Körper der Charakteristik p und $\bar{k}$ sein algebraischer Abschluss.

Definition 20. Sei A eine abelsche Varietät der Dimension g über k, l eine Primzahl, $l \neq p$, so bilden die l^m-Torsionspunkte von A für $m \geq 1$ ein projektives System mit den Abbildungen $A[l^{m+1}] \overset{x \mapsto lx}{\to} A[l^m]$. Der *Tate-Modul* $T_l(A)$ wird nun definiert als der projektive Limes

$$T_l(A) = \varprojlim A[l^m].$$

Außerdem definiert man

$$V_l(A) = \mathbb{Q}_l \otimes_{\mathbb{Z}_l} T_l(A),$$

wo $\mathbb{Z}_l, \mathbb{Q}_l$ der Ring der ganzen l-adischen Zahlen, bzw. der Körper der l-adischen Zahlen sind.

Der Tate-Modul hat folgende Eigenschaften

- $T_l(A)$ ist ein freier $\mathbb{Z}_l$-Modul vom Rang $2g$, und entsprechend ist $V_l(A)$ ein $\mathbb{Q}_l$-Vektorraum der Dimension $2g$.
- Die Galois-Gruppe $G = \mathrm{Gal}(\bar{k} \mid k)$ operiert auf $T_l(A)$.
- Ist B eine weitere abelsche Varietät über k, so gibt es eine kanonische Injektion

$$\mathbb{Z}_l \otimes \mathrm{Hom}_k\big(A, B\big) \hookrightarrow \mathrm{Hom}_G\big(T_l(A), T_l(B)\big).$$

Diese Abbildung ist der Grund, warum dem Tate-Modul große Bedeutung für das Studium der Endomorphismen abelscher Varietäten zukommt. Die meisten $\mathrm{End}(A)$ betreffenden Aussagen, die wir in 1.2.1 und in 1.2.3 angegeben haben, werden üblicherweise unter Rückgriff auf diese Darstellung des Endomorphismenrings bewiesen.

TATES wichtigstes Ergebnis war nun das folgende Theorem.

Theorem 5 (Hauptsatz von Tate)**.** *Die Abbildung*

$$\mathbb{Z}_l \otimes \mathrm{Hom}_k\big(A, B\big) \;\to\; \mathrm{Hom}_G\big(T_l(A), T_l(B)\big)$$

ist eine Bijektion. (Äquivalent dazu ist:
$\mathbb{Q}_l \otimes \mathrm{Hom}_k\big(A, B\big) \to \mathrm{Hom}_G\big(V_l(A), V_l(B)\big)$ *ist bijektiv.)*

Bemerkung 16. Die Arbeit [Ta66] steht methodisch und inhaltlich in engem Zusammenhang sowohl mit den Untersuchungen Deurings [Deu41] über die Endomorphismenringe elliptischer Kurven als auch mit grundlegenden späteren Arbeiten von Yu. G. Zarhin [Zh75] und G. Faltings [Fal83]:
Zarhin gelang es 1975 die Methoden Tates auf den Funktionenkörperfall $k = \mathbb{F}_q(t)$ zu übertragen und das zu Theorem 5 analoge Ergebnis für abelsche Varietäten über $\mathbb{F}_q(t)$ zu zeigen, [Zh75] und [Zh74].
Man vermutete nun, dass dieses Resultat auch über Zahlkörpern seine Richtigkeit behalten würde, was unter der (nicht ganz eindeutigen) Bezeichnung *Tate-Vermutung* bekannt wurde. Diese Vermutung gehörte zu einem ganzen Geflecht von Vermutungen, die zu einander in enger Wechselbeziehung standen, und sich teilweise gegenseitig implizierten. Unter anderem gehörten dazu mehrere Endlichkeitssätze über abelsche Varietäten, wie etwa der folgende:

> *Ist A eine abelsche Varietät über einem Zahlkörper k, so gibt es bis auf Isomorphie nur endlich viele abelsche Varietäten B über k, welche zu A isogen sind.*

Ganz besonders interessant war in diesem Kontext jedoch, dass diese Endlichkeitsaussagen, auf jacobische Varietäten angewandt, über den Umweg der sogannten *Shafarevich-Vermutung* die berühmte Vermutung von Mordell implizierten, ein Zusammenhang, der 1968 von Parshin erkannt worden war.

Vermutung von Mordell: *Ist C eine nichtsinguläre projektive Kurve vom Geschlecht $g \geq 2$ über einem Zahlkörper k, so ist $C(k)$ endlich.*

Diese Vermutung war von Mordell bereits 1922 aufgestellt worden, in [Mor22]. Sie hatte jedoch bislang jedem Versuch eines Beweises widerstanden. In seiner Arbeit [Fal83] gelang es nun Gerd Faltings, die Arakelov-Theorie, die er weiter verfeinert hatte, einzusetzen, um einige abgeschwächte Endlichkeitssätze zu beweisen. Daraufhin nutzte er diese dabei, die Methoden Tates und Zarhins in die Sprache der Zahlkörper zu übersetzen, und daraufhin über die nun bewiesene Tate-Vermutung die obige Endlichkeitsaussage nachzuweisen, womit auch die Richtigkeit der Vermutung Mordells gezeigt war. Für diese Leistung erhielt Faltings 1986 die Fields-Medaille.

1.5.2 Weitere Ergebnisse

Definition 21. Seien f_1, f_2 normierte Polynome in $\mathbb{Q}[X]$, und sei jeweils

$$f_i(X) = \prod_p p^{e_i(p)}, \quad \text{für } i = 1, 2,$$

die kanonische Zerlegung von f_i in paarweise verschiedene irreduzible Polynome über einer Körpererweiterung K von $\mathbb{Q}$. Wir definieren nun

$$r\big(f_1,\, f_2\big) = \sum_p e_1(p)e_2(p) \operatorname{grad} p.$$

Die so definierte ganze Zahl $r\big(f_1,\, f_2\big)$ ist unabhängig von der Wahl des Erweiterungskörpers K. Man kann also beispielsweise K als einen gemeinsamen Zerfällungskörper von f_1 und f_2 wählen, dann ist $\operatorname{grad} p = 1$.

Satz 32 ([Ta66], Theorem 1)**.** *Sind A, B abelsche Varietäten über einem endlichen Körper k, und $P^A_{Fr}(X)$ und $P^B_{Fr}(X)$ die charakteristischen Polynome der Frobenius-Endomorphismen bezüglich k von A bzw. B. Dann gilt:*

1. *Die folgenden beiden Aussagen sind äquivalent:*

$$\begin{aligned} &B \text{ ist } k\text{-isogen zu einer abelschen Untervarietät von } A \\ \iff\quad &P^B_{Fr}(X) \text{ teilt } P^A_{Fr}(X) \end{aligned} \tag{1.15}$$

2. *Der Rang von* $\operatorname{Hom}_k(A, B)$ *erfüllt*

$$\operatorname{Rang} \operatorname{Hom}_k\big(A,\, B\big) = r\Big(P^A_{Fr}(X),\, P^B_{Fr}(X)\Big), \tag{1.16}$$

   mit $r : \mathbb{Q}[X] \times \mathbb{Q}[X] \to \mathbb{Z}$ wie oben definiert.

3. *Die folgenden Aussagen sind äquivalent:*

   (a) *A und B sind k-isogen, $A \sim_k B$*

   (b) *$P^A_{Fr}(X) = P^B_{Fr}(X)$*

   (c) *Ihre Zetafunktionen stimmen überein, $Z_A(X) = Z_B(X)$*

   (d) *$\sharp A(k') = \sharp B(k')$ für jede endliche Körpererweiterung k' von k.*

Wir wollen für den Fall elliptischer Kurven einige Folgerungen aus diesem Satz ziehen.

Korollar 8. *Für elliptische Kurven über $k = \mathbb{F}_q$ gilt:*

$$\operatorname{Rang}\operatorname{End}_k(E) \in \begin{cases} \{2,4\} & \text{falls } q = p^{2m}, m \geq 1 \\ \{2\} & \text{sonst.} \end{cases}$$

Insbesondere ist $\operatorname{Rang}\operatorname{End}_k(E) \leq 4$*, vgl. die Bemerkung zu Satz 19 auf Seite 18.*

Beweis. Wir benutzen (1.16):

$$\operatorname{Rang}\operatorname{Hom}_k\big(A,B\big) = r\left(P_{Fr}^A, P_{Fr}^B\right).$$

In $\operatorname{End}(E)$ gilt:

$$P_{Fr}^E\big(Fr\big) = Fr^2 - (\operatorname{Tr} Fr)Fr + q = 0.$$

Dabei ist $|\operatorname{Tr} Fr| \leq 2\sqrt{q}$. Das quadratische Polynom $P_{Fr}^E(X)$ hat nicht positive Diskriminante und somit verfügt es entweder über keine Wurzel in $\mathbb{Q}$ oder aber eine doppelt auftretende.

- Ist $P_{Fr}^E(X)$ ein Quadrat über $\mathbb{Q}$, d.h. $P_{Fr}^E(X) = \pm\big(X - \sqrt{q}\big)^2$, so gilt

  $$r\big(P_{Fr}^E(X), P_{Fr}^E(X)\big) = 2^2 = 4.$$

  Dieser Fall kann nur für $\sqrt{q} \in \mathbb{Q}$, also $q = p^{2m}$, $m \geq 1$, auftreten.

- Ist $P_{Fr}^E(X)$ irreduzibel über $\mathbb{Q}$, i.e. $P_{Fr}^E(X) = \big(X - \alpha\big)\big(X - \overline{\alpha}\big)$, so gilt

  $$r\big(P_{Fr}^E(X), P_{Fr}^E(X)\big) = 1^2 + 1^2 = 2.$$

□

Lemma 7. *Der Frobenius bezüglich $k = \mathbb{F}_{p^r}$, Fr_r, ist ganzzahlig, genau dann, wenn* $\operatorname{End}_k(E)$ *eine Ordnung in einer Quaternionenalgebra ist.*

Beweis.

- Ist $Fr_r \in \mathbb{Z}$, so ist

  $$[p^r] = Fr \circ \widehat{Fr} = \deg(Fr)^2 \;\Rightarrow Fr = [\pm p^{r/2}],$$

  und r eine gerade Zahl, vergleiche den Beweis von Lemma 4. Dann ist aber $|\operatorname{Tr} Fr_r| = 2p^{r/2} \in \mathbb{Z}$ und somit

  $$P_{Fr}^E(X) = \big(X \pm p^{r/2}\big)^2,$$

  also $\operatorname{Rang}\operatorname{End}_k(E) = \operatorname{Rang}\operatorname{End}_{\bar{k}}(E) = 4$. Damit ist aber $\operatorname{End}_k(E)$ eine Quaternionenalgebra, nach Satz 19, Seite 18.

- Die Richtung $\mathrm{End}_k(E)$ Quaternionenalgebra $\Rightarrow Fr_r \in \mathbb{Z}$ wurde schon gezeigt (siehe Lemma 5 auf Seite 28): Es ist nämlich $\mathbb{Q}[Fr_r]$ im Zentrum von $\mathrm{End}_k(E) \otimes \mathbb{Q}$, aber das Zentrum einer Quaternionenalgebra (über $\mathbb{Q}$) besteht nur aus $\mathbb{Q}$.

□

Bemerkung 17. Man sieht $\mathrm{End}_k(E) = \mathrm{End}_{\bar{k}}(E)$ in diesem Falle auch, ohne zu wissen, dass 4 der höchste mögliche Rang ist: Denn $\mathbb{Z}$ liegt im Zentrum von $\mathrm{End}_{\bar{k}}(E)$. Aus $Fr_r \in \mathbb{Z}$ folgt also, dass jedes $\phi \in \mathrm{End}_{\bar{k}}(E)$ mit dem p^r-Frobenius kommutiert und somit schon über k definiert ist, also $\phi \in \mathrm{End}_k(E)$.

Beim Beweis von Korollar 7 hatten wir Folgendes gesehen: Ist E eine supersinguläre elliptische Kurve über $\mathbb{F}_p$, dann ist $\mathrm{Tr}\, Fr_E = 0$. Damit ergibt sich:

Korollar 9. *Ist E supersingulär über $k = \mathbb{F}_p$, so gilt:*

- $P^E_{Fr}(X) = \big(X - i\sqrt{p}\big)\big(X + i\sqrt{p}\big)$, *insbesondere ist $P^E_{Fr}(X)$ irreduzibel über $\mathbb{Q}$.*
- $\mathrm{End}_k\big(E\big) \subsetneqq \mathrm{End}_{\bar{k}}\big(E\big)$.

Ist E supersinguläre elliptische Kurve über $k = \mathbb{F}_p$, so haben wir in Satz 7, Seite 32, die Zetafunktion $Z(E, X)$ von E angegeben. Nach dem eben Gesagten ist klar, dass diese nach Körpererweiterung eine deutlich andere Form annehmen muss. Nach Satz 30 ist zu erwarten, dass dies bereits über $\mathbb{F}_{p^2}$ der Fall ist. Wir wollen das nachprüfen:

Ist E supersingulär über k definiert, so ist der Zähler von $Z(E, X)$ von der Form $1 + pX^2$. Durch eine quadratische Erweiterung $U^2 = X$ erhalten wir die Zetafunktion von E über k^2. Insbesondere ist hier der Zähler ein Quadrat, und $0 \neq \mathrm{Tr}\, Fr = \pm 2\sqrt{q} = \pm 2p$:

$$\begin{aligned} Z\big(E, U^2\big)_{\mathbb{F}_{p^2}} &= Z\big(E, U\big)_k Z\big(E, -U\big)_k \\ &= \frac{1 + pU^2}{(1 - U)(1 - pU)} \cdot \frac{1 + pU^2}{(1 + U)(1 + pU)} \\ &= \frac{(1 + pU^2)^2}{(1 - U^2)(1 - p^2U^2)} = \frac{1 + 2pU^2 + p^2U^4}{(1 - U^2)(1 - p^2U^2)}. \end{aligned} \tag{1.17}$$

Also

$$Z\big(E, X\big)_{\mathbb{F}_{p^2}} = \frac{1 \pm 2pX + p^2X^2}{(1 - X)(1 - p^2X)}.$$

in der Tat ist dies genau die Form, die man nach Korollar 8 erwarten würde, mit $q = p^2$ und $\mathrm{Tr}\, Fr_q = \pm 2p \in \mathbb{Z}$.

Kapitel 2

Zahlentheoretische Hilfsmittel

2.1 Gaußsche Summen und Jacobi-Summen

In diesem Abschnitt wollen wir zwei wichtige Hilfsmittel, die zueinander in enger Beziehung stehen, einführen. Als grundlegende Referenzen dienen hierbei [Wei49], [Wei52] sowie [IR82].

2.1.1 Gaußsche Summen

Die gaußschen Summen begegnen einem in der Zahlentheorie wie auch in der algebraischen Geometrie auf Schritt und Tritt, so werden sie etwa in der Zahlentheorie zum Beweis der quadratischen Reziprozität oder in der Theorie der L-Reihen verwendet, vgl. beispielsweise das Buch von Neukirch, [Neu92], oder von Ireland, Rosen, [IR82].

Definition 22. Sei $k = \mathbb{F}_{q^n}$, mit $n \geq 1$, $q = p^m, m > 0$. Sei χ ein nichttrivialer Charakter von $k^\times$ und ψ ein nichttrivaler Charakter der additiven Gruppe von k, d.h. $\psi : k^+ \to \overline{\mathbb{Q}}^\times$, mit $\psi \not\equiv 1$. Wir definieren die *gaußsche Summe* $g(\chi, \psi)$ als

$$g(\chi, \psi) = \sum_{u \in k^\times} \chi(u)\psi(u), \tag{2.1}$$

wobei die Summation durch die Vereinbarung $\chi(0) = 0$ auch über ganz k erstreckt werden kann. Bleibt der additive Charakter ψ fest, schreibt man oft auch vereinfachend $g(\chi)$.

Für einen nichttrivialen multiplikativen Charakter χ der Ordnung m auf $k^\times$ ist χ^a für jedes zu m teilerfremde $a > 0$ wieder ein solcher Charakter. Häufig variiert man die betrachteten Charaktere von $k^\times$ nur über eine solche

Menge $\{\chi^a : a = 1, 2, \dots\}$. Man definiert deshalb für fest gewähltes ψ, χ

$$g(a) = g(\chi^a, \psi) = \sum_{u \in k^\times} \chi(u)^a \psi(u). \tag{2.2}$$

Satz 33. *Für die über $k = \mathbb{F}_{q^n}$ definierte gaußsche Summe $g(\chi, \psi)$ gilt:*

$$\begin{aligned} g(\chi,\psi)\,\overline{g}(\chi,\psi) &= q^n \\ \textit{also} \qquad |g(\chi,\psi)| &= \sqrt{q}^n \end{aligned} \tag{2.3}$$

Beweis.

$$\begin{aligned} g(\chi,\psi)\,\overline{g}(\chi,\psi) &= \Big(\sum_{u\in k^\times} \chi(u)\,\psi(u)\Big)\cdot\Big(\sum_{v\in k^\times} \chi(v^{-1})\,\psi(-v)\Big) \\ &= \sum_{v\in k^\times}\sum_{u\in k^\times} \chi(uv^{-1})\,\psi(u-v) = \sum_{u\in k^\times}\chi\big(u\big)\sum_{v\in k^\times}\psi\big((u-1)v\big) \\ &= \sum_{u\neq 1}\chi(u)\Big(\sum_{v\in k}\psi\big((u-1)v\big) - \psi(0)\Big) + 1\Big(\sum_{v\in k^\times}\psi(0)\Big) \\ &= \sum_{u\neq 1}\chi(u)\big(0-1\big) + \big(q^n-1\big) \\ &= -\Big(\sum_{u\in k^\times}\chi(u) - \chi(1)\Big) + q^n - 1 = q^n. \end{aligned}$$

Hierbei wurde ausgenutzt, dass die Summen $\sum_{v\in k}\psi(v)$ und $\sum_{u\in k^\times}\chi(u)$ jeweils 0 ergeben, wenn ψ, χ nichttrivial. Denn dann gibt es ein $t \in k^\times$ mit $\chi(t) \neq 1$. Ist $T = \sum_{u\in k^\times}\chi(u)$, so gilt

$$\chi(t)T = \sum_{u\in k^\times}\chi(t)\chi(u) = \sum_{tu\in k^\times}\chi(tu) = T.$$

Da $\chi(t) \neq 1$ folgt $T = 0$. Analog sieht man $\sum_{v\in k}\psi(v) = 0$ für ψ nichttrivial. □

Ersetzt man in (2.1) u durch tu, mit einem $t \in k, t \neq 0$,

$$g\big(\chi,\psi\big) = \chi(t)\sum_{u\in k^\times}\chi(u)\psi(tu),$$

so erhält man

Korollar 10 (Fourier-Entwicklung von $\chi(u)$)**.**

$$\chi(u) = \frac{g\big(\chi,\psi\big)}{q}\sum_{t\in k\setminus\{0\}}\overline{\chi}(t)\overline{\psi}(tu)$$

2.1.2 Jacobi-Summen

Die folgende Darstellung richtet sich zum großen Teil nach [Wei49].

Definition 23. Seien $\chi_0, \ldots, \chi_r$ nichttriviale multiplikative Charaktere von $\mathbb{F}_q$, $\chi : {\mathbb{F}_q}^\times \to \bar{\mathbb{Q}}^\times$, mit der Eigenschaft, dass ihr Produkt, $\chi_0 \cdots \chi_r$, trivial ist. Wir definieren dann die *Jacobi-Summe*

$$\begin{aligned} j\big(\chi_0, \ldots, \chi_r\big) &= \sum_{\substack{v_1,\ldots,v_r \,\in\, \mathbb{F}_q^\times \\ 1+v_1+\cdots+v_r=0}} \chi_1(v_1)\ldots\chi_r(v_r) \\ &= \frac{1}{q-1} \sum_{\substack{u_0,u_1,\ldots,u_r \,\in\, \mathbb{F}_q^\times \\ u_0+u_1+\cdots+u_r=0}} \chi_0(u_0)\ldots\chi_r(u_r). \end{aligned} \tag{2.4}$$

Aus Symmetriegründen gilt natürlich auch

$$j\big(\chi_0, \ldots, \chi_r\big) = \sum_{\substack{v_0,\ldots,v_{r-1} \,\in\, \mathbb{F}_q^\times \\ v_0+\cdots+v_{r-1}+1=0}} \chi_0(v_0)\ldots\chi_{r-1}(v_{r-1}).$$

Lemma 8. *Es gilt* $j(\chi_0, \ldots, \chi_r) = j(\chi_0^p, \ldots, \chi_r^p)$.

Beweis. Mit u durchläuft u^p ebenfalls $k^\times$. Also

$$\begin{aligned} (q-1)\; j\big(\chi_0, \ldots, \chi_r\big) &= \sum_{\substack{u_0,\ldots,u_r \,\in\, \mathbb{F}_q^\times \\ u_0^p+\cdots+u_r^p=0}} \chi_0(u_0)\ldots\chi_r(u_r) \\ &= \sum_{\substack{u_0^p,\ldots,u_r^p \,\in\, \mathbb{F}_q^\times \\ u_0^p+\cdots+u_r^p=0}} \chi_0(u_0^p)\ldots\chi_r(u_r^p) \\ &= \sum_{\substack{u_0,\ldots,u_r \,\in\, \mathbb{F}_q^\times \\ u_0+\cdots+u_r=0}} \chi_0^p(u_0)\ldots\chi_r^p(u_r), \\ &= (q-1)\; j\big(\chi_0^p, \ldots, \chi_r^p\big), \end{aligned}$$

da $\chi(u^p) = \chi^p(u)$ für jedes $u \in k^\times$. □

Satz 34. *Für die Jacobi-Summe* $j(\chi_0, \ldots, \chi_r)$ *über* $\mathbb{F}_q$ *gilt:*

$$j\big(\chi_0, \ldots, \chi_r\big) = \frac{1}{q} \prod_{i=0}^{r} g\big(\chi_i, \psi\big), \tag{2.5}$$

Beweis. Wendet man auf die Definition Korollar 10 an, und setzt für jedes χ_i, $i = 0, \ldots, r$, die Fourier-Entwicklung mit einem für alle i fest gewählten additiven Charakter ψ ein, so erhält man

$$(q-1)\, j\big(\chi_0, \ldots, \chi_r\big) = \\ q^{-r}\Big(\prod_{i=0}^{r} g\big(\chi_i, \psi_i\big)\Big) \sum_t \Big(\prod_i \overline{\chi}_i(t_i)\Big) \sum_{\sum_i u_i = 0} \overline{\psi}\Big(\sum_i t_i u_i\Big),$$

wobei der Summationsindex i jeweils von 0 bis r läuft.

Durch $\sum_i u_i = 0$ wird eine q^{r-1}-elementige Untergruppe der additiven Gruppe $(\mathbb{F}_q)^r$ festgelegt. Auf dieser wirkt $\overline{\psi}\left(\sum_i t_i u_i\right)$ als Charakter, der nur genau dann konstant gleich 1 ist, wenn $t_0 = \cdots = t_r$. Andernfalls kann man nämlich für ein $z \in k$ mit $\psi(z) \neq 1$ das Gleichungssystem $\sum_i u_i = 0$, $\sum_i t_i u_i = z$ auflösen und erhält u_i mit $\overline{\psi}\left(\sum_i t_i u_i\right) \neq 1$.
Da die Summe auf der rechten Seite über alle Elemente der Untergruppe läuft, ist sie für einen konstanten Charakter gleich q^{r-1}, und sonst 0, vgl. den Beweis zu Satz 33. □

Mit Gleichung (2.3) erhält man noch:

Korollar 11. *Ist $j(\chi_0, \ldots, \chi_r)$ eine Jacobi-Summe über $\mathbb{F}_q$, so gilt:*

$$j\big(\chi_0, \ldots, \chi_r\big)\, \overline{j}\big(\chi_0, \ldots, \chi_r\big) = q^{r-1},$$

insbesondere ist $|j(\chi_0, \ldots, \chi_r)| = \sqrt{q^{r-1}}$.

In manchen Situationen ist außerdem folgende Erweiterung der Definition (2.4) sinnvoll:

Definition 24. Sind $\chi_1, \ldots, \chi_t$ multiplikative Charaktere von $\mathbb{F}_q$, die nicht alle trivial sind, ohne Einschränkung seien $\chi_0, \ldots, \chi_{s-1}$ die trivalen und $\chi_s, \ldots, \chi_t$ die nichttrivalen Charaktere. Dann definiert man

$$j(\chi_0, \ldots, \chi_t) = (-1)^s j(\chi_s, \ldots, \chi_t). \tag{2.6}$$

Offenbar gilt Lemma 8 weiterhin unverändert auch für die so definierten Jacobi-Summen, die anderen Formeln lassen sich jeweils auf den Faktor $j(\chi_s, \ldots, \chi_t)$ anwenden.

2.1.3 Gauß- und Jacobi-Summen bei Körpererweiterungen

Wir haben bislang Gauß- und Jacobi-Summen über endlichen Körpern $k = \mathbb{F}_q$ betrachtet, wo $q = p^m, m \geq 1$. Was ist nun die Beziehung zwischen den entsprechend definierten Summen auf $\mathbb{F}_q$ und auf einer Körpererweiterung $\mathbb{F}_{q^n}$? Wir wollen zunächst unsere Notation festlegen:

- Sei $k = \mathbb{F}_q$. Mit k_n bezeichnen wir dann die Erweiterung $\mathbb{F}_{q^n}$, $n \geq 1$, und $k_1 = k$.
- Wir wählen ein festes erzeugendes Element w der zyklischen Gruppe $k^\times$. Jeder Charakter χ von $k^\times$ wird dann eindeutig durch seinen Wert $\chi(w)$ bestimmt.
- Wir gehen nun induktiv vor und wählen für jedes n ein erzeugendes Element w_n der zyklischen Gruppe ${k_n}^\times$, mit der Eigenschaft

  $$\mathrm{N}_{k_n|k_m}(w_n) = w_m, \qquad \text{für alle } m \text{ mit } m \mid n,$$

  was wegen der Surjektivität der Norm möglich ist.
- Nun können wir nichttriviale Charaktere χ_n von ${k_n}^\times$ durch

  $$\chi_n(w_n) = \chi_m\big(\mathrm{N}_{k_n|k_m}(w_n)\big), \qquad \text{für alle } m \text{ mit } \ m \mid n,$$

  festlegen. Es gilt dann

  $$\chi_n = \chi_m \circ \mathrm{N}_{k_n|k_m}\,.$$

  Außerdem erweitern wir die Definition der χ_n durch $\chi_n(0) = 0$ auf ganz k_n .
- Analog können wir nun mit den additiven Gruppen der k_i, $i = 1, \ldots$ verfahren: Man wählt einen nichttrivialen Charakter ψ von k und erhält mit der Definition

  $$\psi_n = \psi_m \circ \mathrm{Tr}_{k_n|k_m}$$

  für jedes n einen nichttrivialen additiven Charakter von k_n.

Die Antwort auf die Frage, was mit einer gaußschen Summe bei Erweiterung ihres Definitsionskörpers geschieht, wurde nun von H. Hasse und H. Davenport in [DH35] gegeben. Ihre Ergebnisse finden sich z.B. auch in [Wei49], mit einem vollständigem Beweis, der kürzer ist, als der im Original. Ein weiterer, auf P. Monsky zurückgehender, Beweis findet sich in [IR82], 11.4, Seite 163ff.

Theorem 6 (Hasse-Davenport)**.** *Sei $k = \mathbb{F}_q$, k_n eine endliche Erweiterung mit $[k_n : k] = n$, χ_n und ψ_n nichttriviale Charaktere von ${k_n}^\times$ und k_n^+, für die $\chi_n = \chi \circ \mathrm{N}_{k_n|k}$ und $\psi_n = \psi \circ \mathrm{Tr}_{k_n|k}$, mit nichttrivialen Charakteren χ, ψ von $k^\times$, k, gilt. Seien jeweils $g(\chi, \psi)$ und $g_n(\chi_n, \psi_n)$ mittels χ, ψ bzw. χ_n, ψ_n gebildete gaußsche Summen auf k und k_n. Dann gilt:*

$$-g_n\big(\chi_n, \psi_n\big) = \Big[-g\big(\chi, \psi\big)\Big]^n \tag{2.7}$$

Wir werden den Beweis aus [IR82] nachzeichnen, vorher wollen wir jedoch eine wichtige Folgerung angeben:

Korollar 12. *Seien k, k_n wie oben und $\chi_{j,i}$ für $i = 0, \ldots, r$, $j = 1, \ldots, n$ nichttriviale multiplikative Charaktere von k_j, mit $\chi_{n,i} = \chi_{1,i} \circ \mathrm{N}_{k_n|k}$. Seien weiter $j_1(\chi_{1,0}, \ldots, \chi_{1,r})$ und $j_n(\chi_{n,0}, \ldots, \chi_{n,r})$ mit diesen gebildete Jacobi-Summen, so gilt*

$$j_n(\chi_{n,0}, \ldots, \chi_{n,r}) = (-1)^{(n-1)(r+1)}\big(j_1(\chi_{1,0}, \ldots, \chi_{1,r})\big)^n. \tag{2.8}$$

Beweis.

$$\begin{aligned} j_n(\chi_{n,0}, \ldots, \chi_{n,r}) &= \frac{1}{q^n} g_n(\chi_{n,0}) \cdots g_n(\chi_{n,r}) \\ &= \frac{1}{q^n} (-1)^{n-1} g_1(\chi_{1,0})^n \cdots (-1)^{n-1} g_1(\chi_{1,r})^n \\ &= (-1)^{(n-1)(r+1)}\big(j_1(\chi_{1,0}, \ldots, \chi_{1,r})\big)^n, \end{aligned}$$

mit (2.5), Seite 41. □

Beweis des Theorems von Hasse-Davenport: Der Beweis verläuft in mehreren Schritten.

Zu jedem nichtkonstanten normierten Polynom $f \in k[x]$, $f = x^m - c_1 x^{m-1} + \cdots + (-1)^m c_m$, definiere

$$\lambda(f) = \psi(c_1)\, \chi(c_m).$$

Es gilt

Lemma 9. *$\lambda(fh) = \lambda(f)\lambda(h)$, für alle normierten $f, h \in k[x]$.*

Beweis. Ist $f(x) = x^m - c_1 x^{m-1} + \cdots + (-1)^m c_m$ und $h(x) = x^l - b_1 x^{l-1} + \cdots + (-1)^l b_l$, so ist $f(x)h(x) = x^{l+m} - (b_1 + c_1)x^{l+m-1} + \cdots + (-1)^{m+l} c_m b_l$. Also

$$\lambda(fh) = \psi(b_1 + c_1)\chi(c_m b_l) = \psi(b_1)\psi(c_1)\chi(c_m)\chi(b_l) = \lambda(f)\lambda(h)$$

□

Lemma 10. *Sei $\alpha \in k_n$ (mit $\alpha \notin k$) und $f(x)$ ein normiertes, über k irreduzibles Polynom mit $f(\alpha) = 0$. Dann gilt*

$$\lambda\big(f\big)^{n/d} = \psi_n(\alpha)\chi_n(\alpha), \qquad \text{wo } d = \operatorname{grad} f.$$

Beweis. Ist $f(x) = x^d - c_1x^{d-1} + \cdots + c_d$, so hat man

$$\operatorname{Tr}_{k_n|k}(\alpha) = \frac{n}{d}c_1 \qquad \text{und} \qquad \operatorname{N}_{k_n|k}(\alpha) = c_d^{n/d}.$$

Nun ergibt sich

$$\begin{aligned}\lambda\big(f\big)^{n/d} &= \psi(c_1)^{n/d}\chi(c_d)^{n/d} = \psi\big(\frac{n}{d}c_1\big)\chi\big(c_d^{n/d}\big)\\ &= \psi\big(\operatorname{Tr}_{k_n|k}(\alpha)\big)\chi\big(\operatorname{N}_{k_n|k}(\alpha)\big) = \psi_n(\alpha)\chi_n(\alpha).\end{aligned}$$

□

Lemma 11. *Es ist*

$$g\big(\chi_n, \psi_n\big) = \sum_f (\operatorname{grad} f)\lambda\big(f\big)^{n/\operatorname{grad} f},$$

wo über alle normierten $f \in k[x]$ mit $\operatorname{grad} f \mid n$ und f irreduzibel über k summiert wird.

Beweis. Jedes α in k_n ist Wurzel eines normierten, über k irreduziblen Polynoms f mit $d = \operatorname{grad} f \mid n$. Seien $\alpha_1, \ldots \alpha_d$, dessen Wurzeln, dann liegen diese alle in k_n (und haben gleiche Norm und Spur). Nach dem vorherigen Lemma ist

$$\sum_{i=1}^{d} \chi_n(\alpha_i)\psi_n(\alpha_i) = d\lambda(f)^{n/d}.$$

Summiert man nun über alle normierten irreduziblen Polynome, deren Grad n teilt, so erfasst man alle $\alpha \in k_n$, und es folgt die Behauptung. □

Wir erweitern die Definition von λ, indem wir $\lambda(1) = 1$ setzen.

Lemma 12. *Es gilt folgende Identität*

$$\sum_{f \text{ normiert}} \lambda(f)t^{\operatorname{grad} f} = \prod_{f \text{ irred.,normiert}} \big(1 - \lambda(f)t^{\deg f}\big)^{-1}.$$

Beweis. Durch Entwicklung als geometrische Reihe ist

$$\big(1-\lambda(f)t^{\deg f}\big)^{-1}=\sum_{\nu=0}^{\infty}\big(\lambda(f)t^{\deg f}\big)^{\nu}.$$

Damit steht auf der rechten Seite

$$\prod_{f}\sum_{\nu=0}^{\infty}\big(\lambda(f)t^{\operatorname{grad} f}\big)^{\nu}=\sum_{\nu=0}^{\infty}\prod_{f_{i_1},\dots,f_{i_\nu}}t^{\sum_1^\nu \operatorname{grad} f_{i_j}}\lambda\big(\prod_{1}^{\nu}f_{i_j}\big),$$

es wird hierbei für jedes ν über alle ν-Tupel irreduzibler normierter Polynome in $k[x]$ multipliziert. Da sich aber jedes normierte Polynom in $k[x]$ als Produkt normierter irreduzibler Polynome ausdrücken lässt, ist dies einfach

$$\sum_{f\,\text{normiert}}\lambda(f)t^{\operatorname{grad} f}.$$

□

Als nächstes zeigen wir

Lemma 13.

$$\sum_{f}\lambda(f)t^{\operatorname{grad} f}=1+g\big(\chi,\psi\big)t, \tag{2.9}$$

wobei auch hier über alle normierten Polynome in $k[x]$ summiert wird.

Beweis. Zunächst hat man

$$\sum_{f}\lambda(f)t^{\operatorname{grad} f}=\sum_{\nu=0}^{\infty}\Big(\sum_{\operatorname{grad} f=\nu}\lambda(f)\Big)t^{\nu}.$$

Betrachtet man auf der rechten Seite dieser Gleichung den Summanden für $\nu=1$, so ist

$$\sum_{\operatorname{grad} f=1}\lambda(f)=\sum_{a\in k}\lambda(x-a)=\sum_{a\in k}\chi(a)\psi(a)=g\big(\chi,\psi\big).$$

Für $\nu>1$ ergibt sich hingegen

$$\begin{aligned}\sum_{\operatorname{grad} f=\nu}\lambda(f)&=\sum_{(c_1,\dots c_\nu)\in k^\nu}\lambda\big(x^\nu-c_1x^{\nu-1}+\cdots+(-1)^\nu c_\nu\big)\\&=q^{n-2}\sum_{c_1,c_\nu\in k}\psi(c_1)\chi(c_\nu)=q^{\nu-2}\Big(\sum_{c\in k}\chi(c)\Big)\Big(\sum_{c\in k}\psi(c)\Big)=0.\end{aligned}$$

□

Nun haben wir also

$$1 + g(\chi,\psi)t = \prod_{f \text{ irred.}} \big(1 - \lambda(f)t^{\operatorname{grad} f}\big)^{-1}.$$

Logarithmiert man beide Seiten und bildet die Ableitungen, so erhält man

$$\frac{g(\chi,\psi)}{1 + g(\chi,\psi)t} = \sum_f \frac{\lambda(f)(\operatorname{grad} f)t^{\operatorname{grad} f - 1}}{1 - \lambda(f)t^{\operatorname{grad} f}}.$$

Wir multiplizieren beide Seiten mit t (um auf der rechten Seite wieder $t^{\operatorname{grad} f}$ im Zähler zu haben) und entwickeln die Brüche dann als geometrische Reihen:

$$\sum_{\nu=1}^{\infty} (-1)^{\nu-1} g(\chi,\psi)^\nu t^\nu = \sum_f \Big(\sum_{\nu=1}^{\infty} (\operatorname{grad} f)\big(\lambda(f)\big)^\nu t^{\nu \operatorname{grad} f} \Big).$$

Koeffizientenvergleich liefert nun

$$(-1)^{\nu-1} g(\chi,\psi)^\nu = \sum_{\operatorname{grad} f \mid \nu} (\operatorname{grad} f)\lambda\big(f\big)^{\nu/\operatorname{grad} f}.$$

Mit Lemma 11 ergibt sich die Behauptung des Theorems.

2.2 Die klassische Bestimmung von Zetafunktionen

Für die Arbeiten [Wei49] und [Wei52] haben wir folgende grundlegende Situation: Wir wollen die Anzahl der Lösungen gewisser algebraischer Gleichungen über endlichen Körpern allgemein bestimmen, und so die rationalen Punkte auf den zugehörigen algebraischen Varietäten zählen. Nach Untersuchung des Verhaltens unter Körpererweiterung lassen sich dann deren Zetafunktionen bestimmen. Das wesentliche Hilfsmittel bei dieser Untersuchung sind die im vorherigen Abschnitt definierten Gauß- und Jacobi-Summen und das Theorem von Hasse-Davenport.

Vereinbarungen. Sei k_n für $n \in \mathbb{N}$ der endliche Körper $\mathbb{F}_{q^n}$ (und $k_1 = \mathbb{F}_q$). Wir wählen dann für jedes n ein erzeugendes Element w_n der zyklischen Gruppe ${k_n}^\times$, mit

$$\mathrm{N}_{k_n|k_m}(w_n) = w_m, \qquad \text{für } m \mid n,$$

wie auf Seite 43 erläutert.

Ist $\alpha \in \mathbb{Q}$, mit $(q^n - 1)\alpha \equiv 0 \bmod 1$, so wird durch

$$\chi_{\alpha,n} \,:\, w_n^l \longmapsto e^{2\pi\imath\alpha l}, \tag{2.10}$$

ein Charakter von ${k_n}^\times$ definiert, der nichttrival ist, genau wenn $\alpha \not\equiv 0 \bmod 1$. Wir setzen diesen auf ganz k_n fort durch

$$\chi_{\alpha,n}(0) = \begin{cases} 0 & \text{für } \alpha \not\equiv 0 \bmod 1 \\ 1 & \text{für } \alpha \equiv 0 \bmod 1. \end{cases}$$

Da mit $(q^m - 1)\alpha \equiv 0 \bmod 1$ auch $(q^{ml} - 1)\alpha \equiv 0 \bmod 1$, für $l = 1, 2, \ldots$, gilt, lässt sich zu jedem $\chi_{\alpha,m}$ auch ein $\chi_{\alpha,ml}$ analog definieren und es gilt dann

$$\chi_{\alpha,ml} = \chi_{\alpha,m} \circ \mathrm{N}_{k_{ml}|k_m}\,.$$

Wir definieren nun Jacobi-Summen

$$j_n\big(\alpha_0, \ldots, \alpha_r\big) = j\big(\chi_{\alpha_0,n}, \ldots, \chi_{\alpha_r,n}\big).$$

sowie gaußsche Summen

$$g(\chi_{\alpha,n}),$$

mit entsprechend definierten nichttrivialen additiven Charakteren ψ_n, $n = 1, 2, \ldots$, so, dass $\psi_n = \psi \circ \mathrm{Tr}_{k_n|k}$, wie auf Seite 43.

2.2.1 Weils Ergebnisse von 1949

Die Anzahl der Lösungen von Gleichungen über endlichen Körpern

Wir wollen das Vorgehen Weils in [Wei49] kurz darstellen. Sein Ziel war es, zunächst die Anzahl N der Lösungen einer Gleichung der Form

$$a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} = 0, \qquad \text{mit } a_i \in k,\ n_i > 0, \tag{2.11}$$

über k anzugeben.

Bezeichne $N_i(u)$ für ein gegebens $u \in k$ die Anzahl der Lösungen von $x^{n_i} = u$, so ist

$$N_i(u) = \begin{cases} 1 & \text{wenn } u = 0 \\ d_i = \mathrm{ggT}(n_i, q-1) & \text{wenn } u \text{ } d_i\text{-te Potenz in } k \\ 0 & \text{sonst.} \end{cases}$$

Es gilt dann

$$N = \sum_{L(u)=0} N_0(u_0) \cdots N_r(u_r), \tag{2.12}$$

wo über alle Punkte $u = (u_0, \ldots, u_r)$ summiert wird, die auf der durch

$$L(u) = \sum_{i=0}^{r} a_i u_i = 0$$

definierten linearen Varietät in ${A_k}^{r+1}$ liegen.

Wir benutzen nun die weiter oben für $\alpha \in \mathbb{Q}$, $(q-1)\alpha \equiv 0 \bmod 1$, definierten Charaktere $\chi_{\alpha,n}$ von ${k_n}^{\times}$. Da hier durchgehend $n = 1$ gilt, schreiben wir der Übersichtlichkeit halber nur χ_α.

Lemma 14. *Es gilt $N_i(u) = \sum_\alpha \chi_\alpha(u)$, die Summe läuft dabei über $0 \le \alpha < 1$, $\alpha \in \mathbb{Q}$, $(q-1)\alpha, d_i\alpha \equiv 0 \bmod 1$.*

Beweis. Für $u = 0$ ist $N_i(0) = \sum \chi_\alpha(0) = 1$, $i = 0, \ldots, r$, und die Identitiät ist trivial. Für $u \neq 0$ gilt

$$\sum_\alpha \chi_\alpha(u) = \sum_{\nu=0}^{d_i - 1} \zeta^\nu,$$

wo $\zeta = \chi_{1/d_i}(u)$, eine d_i-te Einheitswurzel ist. Es ist $\zeta = 1$ genau dann, wenn $u \in \left(k^{\times}\right)^{d_i}$. Für $\zeta \neq 1$ wird $\sum_\nu \zeta^\nu = 0$, da $0 = 1 - \zeta^{d_i} = (1-\zeta)\sum_\nu \zeta^\nu$. □

Damit folgt sofort

Lemma 15.

$$N = \sum_{L(u)=0} \sum_{\alpha_i} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r),$$
$$wo \qquad \alpha_i \in \mathbb{Q},\ 0 \le \alpha_i < 1,\ d_i\alpha_i \equiv 0 \bmod 1.$$

Lemma 16. *Es gilt*

$$N = q^r + \sum_{u,\alpha} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r),\ \ mit$$
$$u, \alpha\ so,\ dass\, L(u) = 0,\ d_i\alpha_i \equiv 0 \bmod 1,\ 0 < \alpha_i < 1.$$

Beweis. Ist $\alpha_0 = \cdots = \alpha_r = 0$, so ist $\chi_{\alpha_i}(u)$ konstant gleich 1 für alle i. Die Summe für $\alpha = 0$ ist somit gleich der Anzahl der Punkte u auf der r-dimensionalen Hyperfläche $L(u) = 0 \subset k^{r+1}$, also gleich q^r. Sind einige, aber nicht alle der α_i gleich 0, also ohne Einschränkung

$$\alpha_0, \ldots, \alpha_{s-1} \neq 0,\ \alpha_s = \cdots = \alpha_r = 0,\ \text{ mit } s < r,$$

so gibt es q^{r-s} Punkte u mit $u_s, \ldots, u_r \in k$ beliebig. Summiert man nun über alle α, mit $\alpha_0, \ldots, \alpha_{s-1} \in \{\gamma_0, \ldots, \gamma_{s-1}\}$ mit $d_i\gamma_i \in \mathbb{Z}$, $0 < \gamma_i < 1$ für alle i, so ergibt sich

$$\sum_{\alpha} \prod_{i=0}^{s-1} \chi_{\alpha_i}(u_i) = q^{r-s} \prod_{i=0}^{s-1} \sum_{L(u)=0} \chi_{\gamma_i}(u_i) = 0,$$

da jeder Faktor 0 ist. □

Mit $u_i' = a_i u_i$ gilt

$$\sum_{\substack{\alpha,u \\ L(u)=0}} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r) = \sum_{\substack{\alpha,u' \\ \sum_i u_i'=0}} \chi_{\alpha_0}(a_0^{-1}u_0') \cdots \chi_{\alpha_r}(a_r^{-1}u_r'),$$

ersetzt man also u_i mit u_i/a_i und definiert

$$S(\alpha) = S(\alpha_0, \ldots, \alpha_r) = \sum_{\sum_i u_i=0} \chi_{\alpha_0}(u_0) \cdots \chi_{\alpha_r}(u_r)$$

so erhält man

$$N = q^r + \sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) S(\alpha),$$
$$\text{mit } d_i\alpha \equiv 0 \bmod 1,\ 0 < \alpha < 1.$$

Lemma 17. *Es gilt $S(\alpha) = 0$, wenn $\sum_i \alpha_i \notin \mathbb{Z}$, und*

$$S(\alpha) = (q-1) \sum_{1+\sum_i v_i=0} \chi_{\alpha_1}(v_1) \cdots \chi_{\alpha_r}(v_r)$$

sonst.

Beweis. Nach Voraussetzung sind $\alpha_i \notin \mathbb{Z}$, $(q-1)\alpha_i \in \mathbb{Z}$. Per Definition gilt dann $\chi_{\alpha_i}(0) = 0$, und somit ist das Produkt $\prod_i \chi_{\alpha_i}(u_i) = 0$ für $u_i = 0$. Sei ohne Einschränkung $u_0 \neq 0$. Schreibe $v_i = \frac{u_i}{u_0}$ für $1 \leq i \leq r$ und $\beta = \sum_i \alpha_i$. Es gilt dann

$$S(\alpha) = \sum_{1+\sum_i v_i=0} \chi_{\alpha_1}(v_1) \cdots \chi_{\alpha_r}(v_r) \sum_{u_0 \in k^\times} \chi_\beta(u_0).$$

Die Behauptung folgt nun, da $\sum_{u_0} \chi_\beta(u_0)$ für $\beta \notin \mathbb{Z}$ gleich 0 ist und sich für $\beta \in \mathbb{Z}$ zu $q - 1 = \sharp k^\times$ summiert, wegen $\chi_\beta = 1$. □

Mit Lemma 17 ergibt sich (unter Verwendung der oben definierten Jacobi-Summen):

Satz 35.

$$\begin{gathered} N = q^r + (q-1)\sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1})\, j(\alpha_0, \ldots, \alpha_r), \\ \text{wo } d_i\alpha_i \equiv 0 \bmod 1,\ \sum_i \alpha_i \equiv 0 \bmod 1,\ 0 < \alpha_i < 1. \end{gathered} \tag{2.13}$$

Setzt man noch, gemäß der erweiterten Definition 2.6, Seite 42, $j(\beta) = (-1)^s j(\alpha)$, für $\beta = (\beta_0, \ldots \beta_{s+r})$ mit $\beta_{i_j} = \alpha_j \notin \mathbb{Z}$ für $j = 0, \ldots, s-1$ und $\beta_{i_j} \in \mathbb{Z}$ für $j = s, \ldots, r$, so erhält man

Korollar 13. *Die Anzahl N_1 der Lösungen der Gleichung $\sum_{i=0}^r a_i x_i^{n_i} + 1 = 0$ ist*

$$\begin{gathered} N_1 = q^r + \sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1})\, j(\alpha_0, \ldots, \alpha_r, -\sum_{i=0}^r \alpha_i), \\ \text{wo } d_i\alpha_i \equiv 0 \bmod 1,\ 0 < \alpha_i < 1. \end{gathered} \tag{2.14}$$

Beweis. Ist N' die Anzahl der Lösungen von $\sum_{i=0}^r a_i x_i^{n_i} + x_{r+1}^{q-1} = 0$, so gilt

$$N' = (q-1)N_1 + N,$$

da $u_{r+1}^{q-1} = 1$ für $u_{r+1} \in k^\times$ und $u_{r+1}^{q-1} = 0$ für $u_{r+1} = 0$. N' lässt sich aber leicht aus dem vorherigen Satz bestimmen, mit $d_{r+1} = n_{r+1} = q-1$, $a_{r+1} = 1$:

$$N' = q^{r+1} + \big(q-1\big)\sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) \chi_{\alpha_{r+1}}(1^{-1})\, j\big(\alpha_0, \ldots, \alpha_r, \alpha_{r+1}\big),$$

wobei, wie üblich, summiert wird über α mit

$$0 < \alpha_i < 1,\ d_i\alpha_i \equiv 0 \bmod 1,\ \ i = 0, \ldots, r+1, \quad \text{und} \quad \sum_{i=0}^{r+1} \alpha_i \equiv 0 \bmod 1.$$

Nun gilt

$$\begin{aligned} &\sum_{i=0}^{r+1} \alpha_i \equiv 0 \bmod 1,\ \alpha_i \notin \mathbb{Z},\ i = 1, \ldots, r+1 \\ &\qquad\qquad \Leftrightarrow\ \sum_{i=0}^{r} \alpha_i \not\equiv 0 \bmod 1,\ \alpha_i \notin \mathbb{Z},\ i = 1, \ldots, r,\ \alpha_{r+1} = -\sum_{i=0}^{r} \alpha_i. \end{aligned}$$

Damit lässt sich die Summe folgendermaßen umschreiben:

$$\sum_{\substack{\alpha \\ \sum \alpha \not\equiv 0 \bmod 1}} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) \cdot 1 \cdot j(\alpha_0, \ldots, \alpha_r, -\sum_{i=0}^{r} \alpha_i).$$

Entsprechend ist N gleich

$$N = q^{r+1} + \big(q-1\big) \sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1})\, j\big(\alpha_0, \ldots, \alpha_r, \big),$$

mit $0 < \alpha_i < 1$, $d_i \alpha_i \equiv 0 \bmod 1$, $i = 0, \ldots, r$, und $\sum_{i=0}^{r} \alpha_i \equiv 0 \bmod 1$. Wir definieren hierzu noch ein $\alpha_{r+1} \in \mathbb{Z}$, indem wir

$$\alpha_{r+1} = \sum_{i=0}^{r} \alpha_i \quad \equiv 0 \bmod 1$$

setzen. Der zugehörige Charakter ist dann trival, $\chi_{\alpha_{r+1}} \equiv 1$. Mit der erweiterten Definition der Jacobi-Summen ist jetzt

$$\sum_{\substack{\alpha_0, \ldots, \alpha_r \\ \alpha_0 + \cdots + \alpha_r \equiv 0 \bmod 1}} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1})\, j\big(\alpha_0, \ldots, \alpha_r\big) =$$

$$- \sum_{\substack{\alpha_0, \ldots, \alpha_r \\ \alpha_0 + \cdots + \alpha_r \equiv 0 \bmod 1}} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) \cdot 1 \cdot j\big(\alpha_0, \ldots, \alpha_r, -\sum_{i=0}^{r} \alpha_i\big).$$

Nun können wir N_1 ausrechnen:

$$\begin{aligned}
N_1 &= \frac{N' - N}{q-1} \\
&= \frac{q^{r+1} - q^r}{q-1} \\
&\quad + \sum_{\substack{\alpha \\ \sum \alpha \not\equiv 0 \bmod 1}} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) \cdot 1 \cdot j(\alpha_0, \ldots, \alpha_r, -\sum_{i=0}^{r} \alpha_i) \\
&\quad - \sum_{\substack{\alpha \\ \sum \alpha \equiv 0 \bmod 1}} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1}) \cdot 1 \cdot j(\alpha_0, \ldots, \alpha_r, -\sum_{i=0}^{r} \alpha_i) \\
&= q^r + \sum_{\alpha} \chi_{\alpha_0}(a_0^{-1}) \cdots \chi_{\alpha_r}(a_r^{-1})\, j(\alpha_0, \ldots, \alpha_r, -\sum_{i=0}^{r} \alpha_i),
\end{aligned}$$

wobei noch $0 < \alpha_i < 1$, $d_i \alpha_i \equiv 0 \bmod 1$ gilt. Es ergibt sich die Behauptung. □

Die Ergebnisse für k_n Wir behalten unsere Notation bei, schreiben aber nun wieder den Index n an $\chi_{\alpha,n}$ und j_n aus. Wir wollen unsere bisherigen Ergebnisse noch einmal allgemein für k_n, statt nur für k_1, aufschreiben. Die Gleichung (2.13) wird dann

$$N_n = q^{nr} + \big(q^n - 1\big) \sum_{\substack{0<\alpha_i<1 \\ d_i\alpha_i \equiv 0 \bmod 1 \\ (q^n-1)\alpha_i \equiv \bmod 1}} \chi_{\alpha_0,n}(a_0^{-1}) \cdots \chi_{\alpha_r,n}(a_r^{-1}) j_n(\alpha_0, \ldots, \alpha_r),$$

und für $N_{1,n}$, der Lösungsanzahl von $a_0 x_0^{n_0} + \cdots + a_r x_r^{n_r} + 1 = 0$ über k_n, ergibt sich aus (2.14)

$$N_{1,n} = q^{nr} + \big(q^n - 1\big) \sum_{\substack{0<\alpha_i<1 \\ d_i\alpha_i \equiv 0 \bmod 1 \\ \alpha_i \equiv \bmod 1}} \chi_{\alpha_0,n}(a_0^{-1}) \cdots \chi_{\alpha_r,n}(a_r^{-1}) j_n(\alpha_0, \ldots, \alpha_r).$$

Die Zetafunktion für $a_0 x_0^n + \cdots + a_r x_r^n$

Wir betrachten die Gleichung

$$a_0 x_0^n + \cdots + a_r x_r^n = 0,$$

welche eine für $r > 1$ eine affine Varietät $\subset {A_k}^{r+1}$ festlegt. Da es sich um eine homogene Gleichung handelt, definiert sie aber auch eine projektive Varietät $F_r^n \subset {\mathbb{P}_k}^{n-1}$. Für $p = char(k) \nmid n$ weist diese offenbar keine Singularitäten auf. Wir wollen nun die Zetafunktion von F_r^n bestimmen. Sei wie bisher N die Anzahl der k-rationalen Punkte der affinen und $\bar{N}$ die Anzahl der k-rationalen Punkte auf der projektiven Varietät F_r^n. Da jedem projektiven Punkt eine affine Gerade durch den rationalen Nullpunkt mit $(q-1)$ k-rationalen Punkten $\neq 0$ entspricht, und auch der Nullpunkt k-rational ist, gilt

$$N = 1 + (q-1)\bar{N}.$$

Es ist also

$$\bar{N} = 1 + q + \cdots + q^{r-1} + \sum_{\alpha} \overline{\chi}_{\alpha_0,1}(a_0) \cdots \overline{\chi}_{\alpha_r,1}(a_r) j(\alpha_0, \ldots, \alpha_r), \qquad (2.15)$$

mit $\mathrm{ggT}(n, q-1) = d$, $d\alpha_i \in \mathbb{Z}$, $0 < \alpha_i < 1$.

Definition 25. Für $\alpha = (\alpha_0, \ldots, \alpha_r)$ sei

$$\mu(\alpha) = \min\big\{m \in \mathbb{Z} \,:\, (q^m - 1)\alpha_i \in \mathbb{Z} \text{ alle } i\big\}.$$

Es gilt dann offenbar $(q^{\lambda\mu} - 1)\alpha_i \in \mathbb{Z}$, $i = 0, \ldots, r$, für jedes $\lambda \geq 1$.

Auf k_m, $m = 1, 2, \ldots$, benutzen wir nun die anfangs definierten Charaktere $\chi_{\alpha,m}$ von ${k_m}^\times$, ψ_m von k_m^+ und die gaußschen Summen $g_m(\chi_\alpha)$ sowie die Jacobi-Summen $j_m(\alpha_0, \ldots, \alpha_r)$.

Da $a_i \in k$ ist $\overline{\chi}_{\alpha,m}(a_i) = \overline{\chi}_\alpha(a_i)^m$ für jedes m, mit $\chi_\alpha = \chi_{\alpha,1}$. Nach (2.8) und (2.7) auf Seite 44 gilt wegen Hasse-Davenport

$$\begin{aligned} g_{nl}(\chi_\alpha) &= (-1)^{(l-1)} g_n(\chi_\alpha)^l \\ j_{nl}(\alpha_0, \ldots, \alpha_r) &= (-1)^{(l-1)(r-1)} j_n(\alpha_0, \ldots, \alpha_r)^l. \end{aligned}$$

Wir definieren noch $\bar{N}_\nu = \sharp F_r^n(k_\nu)$. Nach diesen Vorbereitungen können wir nun den Logarithmus der Zetafunktion von F_r^n, nach Definition 17, auf Seite 21, angeben:

$$\begin{aligned} \sum_{\nu=1}^{\infty} \bar{N}_\nu \frac{U^\nu}{\nu} &= \sum_{\nu=1}^{\infty} \sum_{m=0}^{r-1} q^{m\nu} \frac{U^\nu}{\nu} \\ &\quad + \sum_{\alpha} \sum_{\lambda=1}^{\infty} (-1)^{(r-1)(\lambda-1)} \Big(\overline{\chi}_{\alpha_0}(a_0) \cdots \overline{\chi}_{\alpha_r}(a_r) j(\alpha) \Big)^\lambda \frac{U^{\mu(\alpha)\lambda}}{\mu(\alpha)\lambda}. \end{aligned}$$

Die erste Summe auf der rechten Seite ist

$$\sum_{\nu=1}^{\infty} \sum_{m=0}^{r-1} q^{m\nu} \frac{U^\nu}{\nu} = \sum_{m=0}^{r-1} \sum_{\nu=1}^{\infty} \big(q^m\big)^\nu \frac{U^\nu}{\nu} = -\sum_{m=0}^{r-1} \log(1 - q^m U).$$

Die zweite Summe lässt sich folgendermaßen umformen:

$$\begin{aligned} &\sum_{\alpha} \sum_{\lambda=1}^{\infty} (-1)^{r-1} \Big((-1)^{r-1} \overline{\chi}_{\alpha_0}(a_0) \cdots \overline{\chi}_{\alpha_r}(a_r) j(\alpha) \Big)^\lambda \frac{U^{\mu(\alpha)\lambda}}{\mu(\alpha)\lambda} \\ &= (-1)^{r-1} \sum_{\alpha} \sum_{\lambda=1}^{\infty} \frac{1}{\mu(\alpha)} \Big((-1)^{r-1} \overline{\chi}_{\alpha_0}(a_0) \cdots \overline{\chi}_{\alpha_r}(a_r) j(\alpha) \Big)^\lambda \frac{\big(U^{\mu(\alpha)}\big)^\lambda}{\lambda} \\ &= (-1)^r \sum_{\alpha} \frac{1}{\mu(\alpha)} \log\big(1 - C(\alpha) U^{\mu(\alpha)}\big), \end{aligned}$$

dabei haben wir $C(\alpha) = (-1)^{r-1} \overline{\chi}_{\alpha_0}(a_0) \cdots \overline{\chi}_{\alpha_r}(a_r)\, j(\alpha)$ definiert.
Zusammen erhält man

$$\begin{aligned} \sum_{\nu=1}^{\infty} \bar{N}_\nu \frac{U^\nu}{\nu} &= -\sum_{m=0}^{r-1} \log(1 - q^m U) \\ &\quad + (-1)^r \sum_{\alpha} \frac{1}{\mu(\alpha)} \log\big(1 - C(\alpha) U^{\mu(\alpha)}\big). \end{aligned} \tag{2.16}$$

Bemerkung 18.

- Weil betrachtet statt des Logarithmus der Zetafunktion die erzeugende Funktion der $\bar{N}_\nu$, $\sum_\nu \bar{N}_\nu U^\nu$. Um zu seinen Formeln zu gelangen, muss man lediglich hier $\log(\dots)$ durch $\frac{d}{dU}\log(\dots)$ ersetzen.

- Der störende Nenner $\frac{1}{\mu(\alpha)}$ lässt sich beseitigen, da $C(\alpha) = C(q\alpha) = \dots = C(q^{\mu-1}\alpha)$ aufgrund von (8), auf Seite 41. Damit wird auch die Rationalität der Zetafunktion zu 2.16, $Z(F_r^n, U)$, ersichtlich.

- Ist $k = \mathbb{F}_q$, mit $q \equiv 1 \bmod n$, so vereinfacht sich die Rechnung erheblich: Es ist dann $d = \mathrm{ggT}(n, q-1) = n$ und $n\alpha_i \in \mathbb{Z}, \forall i$. Damit wird $\mu(\alpha) = 1$ und für eine Fermatfläche $X : x_0^n + \dots + x_r^n = 0$ über k ist $C(\alpha) = (-1)^{r-1} j(\alpha)$ und somit

$$Z(X,U) = \frac{P(U)^{(-1)^{r-1}}}{(1-U)(1-qU)\dots(1-q^{r-1}U)}$$
$$\text{mit } P(U) = \prod_\alpha (1 - (-1)^{r-1} j(\alpha) U),$$
$$n\alpha \equiv 0, \alpha \not\equiv 0, \sum_{i=0}^{r} \alpha_i \equiv 0 \mod 1.$$

  Vergleiche hierzu auch [SK79], S. 107.

2.2.2 Weils Ergebnisse von 1952

Unser Ziel ist es nun, die Zetafunktion der nichtsingulären projektiven Kurve zu bestimmen, die durch die Gleichung

$$y^e = \gamma x^f + \delta,$$

mit $\gamma, \delta \in k^\times$, und $e, f \in \mathbb{N}$, mit $p \nmid e, f$ und $2 \le e \le f$, definiert wird. Für diese Zetafunktion gibt Weil in [Wei52] eine Produktzerlegung an, wobei er einen Beweis nur knapp andeutet. Der nachfolgend dargestellte Beweis findet sich so nicht in der Literatur.

Die Zetafunktion der affinen Kurve

Wir betrachten zunächst die affine Kurve zu der Gleichung

$$y^e = \gamma x^f + \delta. \tag{2.17}$$

Wir stellen diese Gleichung um, in die Form

$$\frac{\gamma}{\delta} x^f - \frac{1}{\delta} y^e + 1 = 0. \tag{2.18}$$

Bezeichnet man die Anzahl von Lösungen (x, y), mit $x, y \in {k_n}^\times$, dieser Gleichung durch N_n, so erhält man aus (2.14)

$$N_n = q^n + \sum_{\substack{0<\alpha_0,\alpha_1<1 \\ f\alpha_0\equiv e\alpha_1\equiv 0 \bmod 1 \\ (q^n-1)\alpha_0\equiv(q^n-1)\alpha_1\equiv 0 \bmod 1}} \chi_{\alpha_0,n}\big(\frac{\delta}{\gamma}\big)\chi_{\alpha_1,n}\big(-\delta\big)j_n\big(\alpha_0,\alpha_1,-\alpha_0-\alpha_1\big).$$

Die Bedingungen $f\alpha_0 \equiv 0 \mod 1$ und $0 < \alpha < 1$ lassen für α_0 nur die Form $\alpha_0 = \frac{a}{f}$ zu, mit $0 < a < f$. Da α_0 nur modulo 1 verwendet wird, ist hierbei auch a nur modulo f zu betrachten. Analog ist $\alpha_1 = \frac{b}{e}$, $0 < b < 1$ und b nur modulo e bestimmt. Die Formel für N_n lautet nun

$$N_n = q^n + \sum_{\substack{0<a<f \\ 0<b<e \\ \frac{a}{f}(q^n-1)\equiv 0 \bmod 1 \\ \frac{b}{e}(q^n-1)\equiv 0 \bmod 1}} \chi_{\frac{a}{f},n}\big(\frac{\delta}{\gamma}\big)\chi_{\frac{b}{e},n}\big(-\delta\big)\, j_n\big(\frac{a}{f},\, \frac{b}{e}, -\frac{a}{f}-\frac{b}{e}\big). \qquad (2.19)$$

Als nächstes wollen wir den Logarithmus der Zetafunktion der affinen Kurve aufschreiben,

$$\log Z_0(U) = \sum_{n\geq 1} N_n \frac{U^n}{n}.$$

Bevor wir dies explizit durchführen, lohnt sich jedoch erst, die Bedingungen in der Summe genauer in Abhängigkeit von k_n zu analysieren:

Lemma 18. *Sei $m_0 = m_0(a,b)$ der kleinste gemeinsame Nenner von $\frac{a}{f}$ und $\frac{b}{e}$ und $d = d(a,b)$ die Ordnung von q in $(\mathbb{Z}/m_0\mathbb{Z})^\times$, der multiplikativen Gruppen modulo m_0. Dann gilt*

$$\frac{a}{f}\big(q^n-1\big) \equiv \frac{a}{f}\big(q^n-1\big) \equiv 0 \bmod 1 \qquad \Longleftrightarrow \qquad d \mid n.$$

Beweis. Wir bringen $\frac{a}{f}$ und $\frac{b}{e}$ auf ihren gemeinsamen Nenner:

$$\frac{a}{f} = \frac{a_0}{m_0},\ \frac{b}{e} = \frac{b_0}{m_0} \qquad \text{mit } \ \mathrm{ggT}(a_0, b_0, m_0) = 1.$$

Es gilt nun

$$\begin{aligned}
\frac{a}{f}\big(q^n-1\big) \equiv \frac{b}{e}\big(q^n-1\big) \equiv 0 \bmod 1 \Leftrightarrow\ & \frac{a_0}{m_0}\big(q^n-1\big) \equiv \frac{a_0}{m_0}\big(q^n-1\big) \equiv 0 \bmod 1 \\
\Leftrightarrow\ & m_0 \mid a_0\big(q^n-1\big) \ \wedge\ m_0 \mid b_0\big(q^n-1\big) \\
\Leftrightarrow\ & m_0 \mid \mathrm{ggT}\big(a_0,\, b_0\big)\big(q^n-1\big) \\
\Leftrightarrow\ & m_0 \mid \big(q^n-1\big) \\
\Leftrightarrow\ & q^n \equiv 1 \mod m_0.
\end{aligned}$$

□

Unser nächstes Zwischenergebnis ist die folgende Aussage:

Lemma 19. *Es gilt*

$$\log Z_0(U) = \log \frac{1}{1-qU} + \sum_{\substack{0<a<f\\0<b<e}} \frac{1}{d(a,b)} \log\bigl(1+\xi(a,b)U^{d(a,b)}\bigr), \tag{2.20}$$

dabei ist $\xi(a,\,b)$ *definiert durch*

$$\begin{aligned} \xi(a,\,b) &= \chi_{\frac{1}{m_0},d}\Bigl(\bigl(\frac{\delta}{\gamma}\bigr)^{a_0}\bigl(-\delta\bigr)^{b_0}\Bigr)\, j_d\bigl(\frac{a_0}{m_0},\,\frac{b_0}{m_0},-\frac{a_0+b_0}{m_0}\bigr) \\ &= \chi_{\frac{1}{m_0},d}\Bigl(\bigl(\frac{\delta}{\gamma}\bigr)^{a_0}\bigl(-\delta\bigr)^{b_0}\Bigr)\, j_d\bigl(\frac{a}{f},\,\frac{b}{e},-\frac{a}{f}-\frac{b}{e}\bigr). \end{aligned} \tag{2.21}$$

Beweis.

$$\begin{aligned} \log Z_0\bigl(U\bigr) &= \sum_{n\geq 1} N_n \frac{U^n}{n} \\ &= \sum_{n\geq 1}\left[q^n + \sum_{a,b} \chi_{\frac{a}{f},n}\bigl(\frac{\delta}{\gamma}\bigr)\chi_{\frac{b}{e},n}\bigl(-\delta\bigr)\, j_n\bigl(\frac{a}{f},\,\frac{b}{e},-\frac{a}{f}-\frac{b}{e}\bigr)\right]\frac{U^n}{n} \\ &= \sum_{a,b}\frac{\bigl(qU\bigr)^n}{n} + \sum_{a,\,b}\left[\sum_{n\geq 1}\chi_{\frac{a}{f},n}\bigl(\frac{\delta}{\gamma}\bigr)\chi_{\frac{b}{e},n}\bigl(-\delta\bigr)\, j_n\bigl(\frac{a}{f},\,\frac{b}{e},-\frac{a}{f}-\frac{b}{e}\bigr)\frac{U^n}{n}\right], \end{aligned}$$

wo jeweils über a, b mit $0<a<f$, $0<b<e$, und $\frac{a}{f}(q^n-1)$, $\frac{b}{e}(q^n-1)\equiv 0 \bmod 1$ summiert wird. Zu der Summe in der letzten Zeile liefern, laut Lemma 18, für ein festes Paar (a,b) nur diejenigen n, wo $n=dl$, $l\geq 1$, einen Beitrag. Also

$$\begin{aligned} &\log Z_0(U) = \\ &\qquad \log\frac{1}{1-qU} + \sum_{a,\,b}\left[\sum_{l\geq 1}\chi_{\frac{a}{f},dl}\bigl(\frac{\delta}{\gamma}\bigr)\chi_{\frac{b}{e},dl}\bigl(-\delta\bigr)\, j_{dl}\bigl(\frac{a}{f},\,\frac{b}{e},-\frac{a}{f}-\frac{b}{e}\bigr)\frac{U^{dl}}{dl}\right]. \end{aligned}$$

Wir formen nun die Summe weiter um, mittels Hasse-Davenport und (2.8):

$$\sum_{a,\,b}\Bigg[\sum_{l\geq 1}(-1)^{(l-1)}\chi_{\frac{a}{f},d}\big(\frac{\delta}{\gamma}\big)^{l}\chi_{\frac{b}{e},d}\big(-\delta\big)^{l}\,j_d\big(\frac{a}{f},\,\frac{b}{e},-\frac{a}{f}-\frac{b}{e}\big)^{l}\frac{U^{dl}}{dl}\Bigg]=$$

$$\sum_{a,\,b}\frac{(-1)}{d}\sum_{l\geq 1}\frac{1}{l}\Bigg(-\chi_{\frac{a}{f},d}\big(\frac{\delta}{\gamma}\big)\chi_{\frac{b}{e},d}\big(-\delta\big)\,j_d\big(\frac{a}{f},\,\frac{b}{e},-\frac{a}{f}-\frac{b}{e}\big)U^{d}\Bigg)^{l}=$$

$$\sum_{a,\,b}\frac{1}{d}\log\Bigg(1+\chi_{\frac{a}{f},d}\big(\frac{\delta}{\gamma}\big)\chi_{\frac{b}{e},d}\big(-\delta\big)\,j_d\big(\frac{a}{f},\,\frac{b}{e},-\frac{a}{f}-\frac{b}{e}\big)U^{d}\Bigg)=$$

$$\sum_{a,\,b}\frac{1}{d}\log\Bigg(1+\chi_{\frac{a_0}{m_0},d}\big(\frac{\delta}{\gamma}\big)\chi_{\frac{b_0}{m_0},d}\big(-\delta\big)\,j_d\big(\frac{a_0}{m_0},\,\frac{b_0}{m_0},-\frac{a_0+b_0}{m_0}\big)U^{d}\Bigg)=$$

$$\sum_{a,\,b}\frac{1}{d}\log\Bigg(1+\chi_{\frac{1}{m_0},d}\big(\big(\frac{\delta}{\gamma}\big)^{a_0}(-\delta)^{b_0}\big)j_d\big(\frac{a_0}{m_0},\,\frac{b_0}{m_0},-\frac{a_0+b_0}{m_0}\big)U^{d}\Bigg).$$

Mit der obigen Definition von $\xi(a,\,b)$,

$$\xi(a,b)=\chi_{\frac{1}{m_0},d}\Big(\big(\frac{\delta}{\gamma}\big)^{a_0}\big(-\delta\big)^{b_0}\Big)\;\cdot\;j_d\big(\frac{a_0}{m_0},\,\frac{b_0}{m_0},-\frac{a_0+b_0}{m_0}\big),$$

vereinfacht sich die Schreibweise zu

$$\log Z_0(U)=\log\frac{1}{1-qU}+\sum_{\substack{0<a<f\\0<b<e}}\frac{1}{d(a,b)}\log\big(1+\xi(a,b)U^{d(a,b)}\big),$$

wie behauptet. □

Um die Zetafunktion geschlossen als rationale Funktion darstellen zu können, müssen wir als nächstes versuchen, den für jedes Paar $(a,\,b)$ einzeln zu bestimmenden Nenner $d(a,b)$ aus (2.20) zu eliminieren.

Satz 36. *Für die Zetafunktion der durch* (2.18) *definierten affinen Kurve über k gilt*

$$Z_0(U)=\frac{1}{1-qU}\cdot\prod_{i=1}^{r}\Big(1+\xi(a_i,\,b_i)U^{d(a_i,b_i)}\Big).\tag{2.22}$$

Dabei ist für jedes $i=1,\ldots,r$ das Paar (a_i,b_i) so gewählt, dass sich die Menge der (a,b) als disjunkte Zerlegung

$$\{(a,\,b)\,:\,0<a<f,\,0<b<e\}=\biguplus_{i=1}^{r}B(a_i,\,b_i)$$

schreiben lässt, mit

$$B(a_i,\, b_i) = \left\{(q^j a_i \bmod f,\, q^j b_i \bmod e) \,:\, j = 0, 1, 2, \dots \right\}.$$

Beweis. Hat man zwei Größen a', b', mit $0 < a' < f$ und $0 < b' < e$, für die gilt $a' \equiv qa \mod f$, $b' \equiv qb \mod e$ (mit $0 < a < f$, $0 < b < e$), und definiert zu diesen die entsprechenden Größen m_0', d', a_0', b_0' aus Lemma 18, so gilt

$$\begin{aligned} &m_0'(a', b') = m_0(a, b), \quad d'(a', b') = d(a, b), \\ &a_0' \equiv qa_0 \mod m_0, \quad b_0' \equiv qb_0 \mod m_0. \end{aligned}$$

Neben $d(a', b') = d(a, b)$ ist auch $\xi(a', b') = \xi(a, b)$, denn der Charakter $\chi_{\frac{1}{m_0}, d}$ hat die Ordnung m_0 und über dem Grundkörper $\mathbb{F}_q$ gilt

$$\begin{aligned} \left(\frac{\delta}{\gamma}\right)^{qa_0} &= \left(\frac{\delta}{\gamma}\right)^{a_0}, \text{ sowie} \\ j_d\left(q\alpha_0, q\alpha_1, q\alpha_3\right) &= j_d\left(\alpha_0, \alpha_1, \alpha_3\right). \end{aligned}$$

Dies verallgemeinert sich für $a^{(j)}, b^{(j)}$ mit $a^{(j)} \equiv q^j a \mod f$, $b^{(j)} \equiv q^j b \mod e$ folgendermaßen:

$$\begin{aligned} \xi\left(q^j a \bmod f,\, q^j b \bmod e\right) &= \xi\left(a,\, b\right), \\ d\left(q^j a \bmod f,\, q^j b \bmod e\right) &= d\left(a,\, b\right), \end{aligned}$$

für $j = 0, 1, 2 \dots$. Nun gilt

$$\begin{aligned} (a,\, b) = (q^n a \bmod f, q^n \bmod e) &\Leftrightarrow\ q \equiv q^n \bmod f, b \equiv q^n \bmod e \\ &\Leftrightarrow\ \frac{a}{f}(q^n - 1) \equiv \frac{b}{e}(q^n - 1) \equiv 0 \bmod 1 \\ &\Leftrightarrow\ q^n \equiv 1 \bmod m_0 \\ &\Leftrightarrow\ d \mid n, \end{aligned}$$

nach dem Beweis von Lemma 18. Damit hat die oben definierte Menge $B(a, b)$ genau $d(a, b)$ Elemente. Wir können die a_i, b_i nun so wählen, dass

$$\{(a,\, b) \,:\, 0 < a < f,\, 0 < b < e\} = \biguplus_{i=1}^{r} B(a_i,\, b_i).$$

Dies liefert für die Zetafunktion

$$\begin{aligned}\log Z_0(U) &= \log\frac{1}{1-qU} + \sum_{\substack{0<a<f\\0<b<e}} \frac{1}{d(a,b)} \log\bigl(1+\xi(a,\,b)\,U^{d(a,b)}\bigr)\\ &= \log\frac{1}{1-qU} + \sum_{i=1}^{r} \sum_{(a,b)\in B(a_i,b_i)} \frac{1}{d(a_i,b_i)} \log\bigl(1+\xi(a_i,\,b_i)\,U^{d(a_i,b_i)}\bigr)\\ &= \log\frac{1}{1-qU} + \sum_{i=1}^{r} \log\bigl(1+\xi(a_i,\,b_i)\,U^{d(a_i,b_i)}\bigr),\end{aligned}$$

wegen des zuletzt Gesagten. Damit folgt die Behauptung. □

Wir wollen nun die Faktoren in (2.22) näher untersuchen.

Lemma 20. *Ist* $\frac{a}{f}+\frac{b}{e} \equiv 0 \mod 1$*, so sind die Nullstellen von* $1+\xi(a,b)U^{d(a,b)}$ *Einheitswurzeln, insbesondere haben sie Absolutbetrag 1.*

Beweis. Die Bedingung $\frac{a}{f}+\frac{b}{e} \equiv 0 \mod 1$ ist gleichbedeutend mit $b_0 \equiv -a_0 \mod m$. Die (erweiterte) Definition der Jacobi-Summen liefert

$$j_d(\alpha_0,\,\alpha_1,\,0) = (-1)^1 \chi_{\alpha_0,d}(-1),$$

für den Fall $\alpha_0+\alpha_1 \equiv 0 \mod 1$. Damit ergibt sich

$$\begin{aligned}\xi(a,b) &= \chi_{\frac{1}{m_0},d}\Bigl(\bigl(\frac{\delta}{\gamma}\bigr)^{a_0}(-\delta)^{b_0}\Bigr)\, j_d\bigl(\frac{a_0}{m_0},\,\frac{b_0}{m_0},\,0\bigr)\\ &= \chi_{\frac{1}{m_0},d}\Bigl(\bigl(\frac{\delta}{\gamma}\bigr)^{a_0}(-\delta)^{b_0}\Bigr)\cdot\bigl(-\chi_{\frac{a_0}{m_0},d}(-1)\bigr)\\ &= -\chi_{\frac{1}{m_0},d}\Bigl(\bigl(\frac{\delta}{\gamma}\bigr)^{a_0}(-\delta)^{b_0}(-1)^{a_0}\bigr)\Bigr) = -\chi_{\frac{1}{m_0},d}\Bigl(\bigl(\frac{1}{\gamma}\bigr)^{a_0}\Bigr).\end{aligned}$$

Da $\chi_{1/m_0,d}$ als Gruppencharakter nur Werte in den Einheitswurzeln annimmt, folgt die Behauptung. □

Lemma 21. *Ist* $\frac{a}{f}+\frac{b}{e} \not\equiv 0 \mod 1$*, so haben die Nullstellen von* $1+\xi(a,b)T^{d(a,b)}$ *den Absolutbetrag* $q^{-1/2}$*.*

Beweis. Die Bedingung $\frac{a}{f}+\frac{b}{e} \not\equiv 0 \mod 1$ ist gleichwertig mit $a_0+b_0 \not\equiv 0 \mod m_0$. Damit ergibt sich unter Verwendung von (2.5), Seite 41,

$$\begin{aligned}\xi(a,\,b) &= \chi_{\frac{1}{m_0},d}\Bigl(\bigl(\frac{\delta}{\gamma}\bigr)^{a_0}(-\delta)^{b_0}\Bigr)\, j_d\bigl(\frac{a_0}{m_0},\,\frac{b_0}{m_0},\,\frac{a_0+b_0}{m_0}\bigr)\\ &= \chi_{\frac{1}{m_0},d}\Bigl(\bigl(\frac{\delta}{\gamma}\bigr)^{a_0}(-\delta)^{b_0}\Bigr)\\ &\qquad\cdot\frac{1}{q^d} g_d\bigl(\chi_{\frac{a_0}{m_0},d}\bigr) g_d\bigl(\chi_{\frac{b_0}{m_0},d}\bigr) g_d\bigl(\chi_{-\frac{a_0+b_0}{m_0},d}\bigr).\end{aligned}$$

Da die gaußschen Summen $g_d(\dots)$ den Absolutbetrag $q^{d/2}$ haben, ist

$$|\xi(a,\, b)| = q^{\frac{d}{2}}.$$

Für eine Nullstelle ω von $1 + \xi(a,b)T^{d(a,b)}$ gilt folglich

$$|\omega|^d = |\omega^d| = |-\frac{1}{\xi(a,\, b)}| = \frac{1}{q^{d/2}}, \qquad \text{also } |\omega| = \frac{1}{\sqrt{q}}.$$

□

Wir wollen die Anwendung der letzten beiden Lemmata durch ein Beispiel illustrieren.

Beispiel. Wir betrachten den Fall $e = f = 2$, d.h. die Gleichung (2.18) hat hier die Form $y^2 = \gamma x^2 + \delta$ und beschreibt einen Kegelschnitt. $0 < a < f$ und $0 < b < e$ lassen als einzige Möglichkeit $a = b = 1$ zu, also

$$\frac{a}{f} = \frac{1}{2}, \quad \frac{b}{e} = \frac{1}{2}, \quad \frac{a}{f} + \frac{b}{e} \equiv 0 \bmod 1.$$

Es ergibt sich dann $m_0 = 2$ und $a_0 = b_0 = 1$. Da d als minimale Zahl mit der Eigenschaft $q^d \equiv 1 \bmod m_0$ definiert ist, ergibt sich hier $d = 1$. Wir wählen also einen Erzeuger w_1 von ${k_1}^\times$ und definieren damit den Charakter

$$\chi_{\frac{1}{m_0}} : \qquad w_1 \longmapsto e^{2\pi\imath\cdot\frac{1}{2}} = e^{\pi\imath} = -1.$$

Es folgt dann

$$\xi(1,\, 1) = -\chi_{\frac{1}{2},1}\big(\frac{1}{\gamma}\big)^{a_0} = -\chi_{\frac{1}{2},1}\big(\frac{1}{\gamma}\big) = \chi_{\frac{1}{2},1}\big(\gamma\big).$$

Damit erhalten wir die Zetafunktion des affinen Kegelschnitts

$$Z_0(U) = \frac{1 - \chi_{\frac{1}{2},1}\big(\gamma\big)U}{1 - qU}.$$

Die Zetafunktion der nichtsingulären projektiven Kurve

Bislang haben wir uns nur mit der affinen Kurve C_0 befasst, die zu der Gleichung $y^e = \delta x^f + \gamma$ gehört. Diese ist nichtsingulär, wie man leicht sieht. Nun wollen wir die nichtsinguläre projektive Kurve C betrachten, die durch diese Gleichung festgelegt wird, d.h. die nichtsinguläre projektive Kurve mit dem Funktionenkörper $k(C_0)$.

C entsteht aus C_0 durch hinzufügen von Punkten im Unendlichen, dies sind endlich viele, denn die rationale Funktion $x(P) \in k(C) = k(C_0)$, die einem $P \in C$ seine x-Koordinate zuordnet, hat nur endlich viele Polstellen. Also:

$$C = C_0 \cup \{P_0, \ldots, P_u\}, \qquad \text{mit } x\big(P_i\big) = y\big(P_i\big) = \infty,\ i = 1, \ldots, u.$$

Wir wollen nun den Beitrag, den diese Punkte zur Zetafunktion von C_0 leisten, ermitteln.

Die Menge $\{P_0, \ldots, P_u\}$ bleibt unter Galois-Operationen invariant und zerfällt somit in Bahnen unter der Operation der Galois-Gruppe.

Sei nun $\{Q_0, \ldots, Q_m\} \subset \{P_0, \ldots P_u\}$ eine solche Bahn. Dann sind die Punkte Q_i, $i = 1, \ldots, m$, über dem Körper k_m definiert und damit auch über allen Erweiterungen k_{ml}, für $l \geq 1$. Hingegen sind diese Punkte über k_n mit $m \nmid n$ nicht sichtbar. Wir wollen für diese Punktmenge eine Zetafunktion aufstellen:

$$\log Z_{\{Q_1,\ldots,Q_m\}}(U) = \sum_{l\geq 1} m\frac{U^{ml}}{ml} = \sum_{l\geq 1} \frac{\big(U^m\big)^l}{l} = \log \frac{1}{1-U^m}.$$

Halten wir dies fest:

Lemma 22. *Sei $\{Q_1, \ldots, Q_m\} \subset \{P_0, \ldots P_u\}$ eine Bahn unter der Operation der Galois-Gruppe. Dann gilt*

$$Z_{\{Q_1,\ldots,Q_m\}}(U) = \frac{1}{1-U^m}.$$

Lemma 23. *Sind X und Y disjunkte, über k_n, $n \geq 1$, definierte algebraische Mengen, so gilt*

$$Z_{X\cup Y}(U) = Z_X(U) \cdot Z_Y(U).$$

Beweis. Da X, Y nach Voraussetzung disjunkt sind, gilt

$$\begin{aligned} \log Z_{X\cup Y}(U) &= \sum_{l\geq 1} \sharp\big(X \cup Y\big)(k_{ln})\frac{U^{ln}}{ln} = \sum_{l\geq 1} \big(\sharp X(k_{ln}) + \sharp Y(k_{ln})\big)\frac{U^{ln}}{ln} \\ &= \log Z_X(U) + \log Z_Y(U). \end{aligned}$$

Es folgt die Behauptung. □

Dies ergibt sofort

Korollar 14. *Die Zetafunktion der Punktmenge $\{P_1, \ldots, P_u\}$ hat die Gestalt*

$$Z_{\{P_0,\ldots,P_u\}}(U) = \prod_{j=1}^{s} \frac{1}{1-U^{m_j}},$$

wobei s die Anzahl der Bahnen unter Galois-Operationen ist.

Da die Punkte im Unendlichen zur restlichen Kurve disjunkt sind, können wir nun die Zetafunktion von C angeben.

Theorem 7 ([Wei52], S. 493)**.** *Sei C die nichtsinguläre projektive Kurve, welche durch die Gleichung*

$$y^e = \delta x^f + \gamma, \qquad \text{mit } \gamma, \delta \in k^\times,\ e, f \in \mathbb{N},\ p \nmid ef,$$

festgelegt wird. Dann hat die Zetafunktion von C die Gestalt

$$Z(C,U) = \frac{\prod_{a_i,\, b_i} \big(1 - \xi\big(a_i, b_i\big) U^{d(a_i,b_i)}\big)}{\big(1-U\big)\big(1-qU\big)} \tag{2.23}$$

mit a_i, b_i wie in Satz 36 auf Seite 58, mit $\dfrac{a_i}{f} + \dfrac{b_i}{e} \not\equiv 0 \bmod 1$.

Beweis. Aus den bisherigen Resultaten haben wir

$$\begin{aligned} Z(C,U) &= Z_{C_0 \cup \{P_0,\ldots,P_u\}} = Z_{C_0}(U) \cdot Z_{\{P_0,\ldots,P_u\}}(U) \\ &= \frac{1}{1-qU} \prod_{i=1}^{s} \big(1 - \xi\big(a_i, b_i\big) U^{d(a_i,b_i)}\big) \prod_{j=1}^{s} \frac{1}{1-U^{m_j}}. \end{aligned} \tag{2.24}$$

Da $Z(C,U)$ die Zetafunktion einer (geometrisch irreduziblen) nichtsingulären projektiven Kurve ist, lässt sie sich nach Satz 26, auf Seite 25, auf folgende Form bringen:

$$Z(C,U) = \frac{P(U)}{(1-U)(1-qU)}$$

$$\text{mit} \qquad P(U) = \prod_{j=1}^{2g} \big(1 - \alpha_j U\big) \text{ und } |\alpha_j| = \sqrt{q},\ j = 1, \ldots, 2g.$$

Da außerdem $\alpha_i \neq \alpha_j$ für $i \neq j$, ist diese Darstellung (als Bruch $\in \overline{\mathbb{Q}}(U)$) vollständig gekürzt.

Wir müssen nun untersuchen, welche der Faktoren in (2.24) sich dabei wegkürzen.

- $1+\xi(a_i,b_i)U^{d(a_i,b_i)}$ mit $\frac{a_i}{f}+\frac{b_i}{e}\equiv 0 \bmod 1$: Wir haben gesehen, dass die Nullstellen hier den Absolutbetrag 1 haben. Also kommt keiner dieser Terme mehr im Zähler von $Z(C,U)$ vor, sie kürzen sich gegen Faktoren $1-U^{m_j}$ im Nenner.

- $1+\xi(a_i,b_i)U^{d(a_i,b_i)}$ mit $\frac{a_i}{f}+\frac{b_i}{e}\not\equiv 0 \bmod 1$: Hier haben die Nullstellen Absolutbetrag $q^{-1/2}$, dies bedeutet keiner dieser Faktoren kann gekürzt werden, sie bleiben im Zähler erhalten.

- Entsprechend fallen alle der Faktoren $1-U^{m_j}$ mit $m_j>1$ weg. Nur ein Faktor, $1-U$, bleibt. Nach dem bislang Gesagten ist der zugehörige Punkt im Unendlichen über allen k_n, $n=1,2,\ldots$, sichtbar.

□

Bemerkung 19. Die im Beweis benutzte Aussage über Zetafunktionen nichtsingulärer projektiver Kurven, war 1952 bereits wohl bekannt. Schon 1931 hatte F. Schmidt gezeigt, dass eine solche Zetafunktion die Form

$$Z(U)=\frac{P(U)}{\big(1-U\big)\big(1-qU\big)}$$

hat, und Weil selbst hatte 1948 in [Wei48] die von uns benutzte Version dieser Aussage allgemein bewiesen, wie schon auf Seite 22 erwähnt.

Kapitel 3

Rangkonstruktionen

3.1 Die Konstruktion von Tate und Shafarevich

Der erste Beweis für die Existenz von Familien elliptischer Kurven mit asymptotisch beliebig hohem Rang über Funktionenkörpern über endlichen Körpern stammt von Tate und Shafarevich, [TS67]. Das Ziel dieses Abschnitts ist es, diesen Beweis nachzuzeichnen. Wir werden dabei folgendes Theorem zeigen:

Theorem 8. *Ist E eine über $k = \mathbb{F}_p$, $p \neq 2$, definierte supersinguläre elliptische Kurve, mit einer Gleichung der Form*

$$E \,:\, y^2 = x^3 + ax^2 + bx + c, \;\; \textit{mit } a, b, c \in k,$$

und ist $F(t) \in k[t]$ ein Polynom der Form

$$F(t) = \gamma t^f + \delta,$$

mit $\gamma, \delta \in k^\times$, und ganzzahligem $f \geq 2$, welches $p^n + 1$ teilt für ein ungerades n, dann ist für jedes solche $F(t)$ eine elliptische Kurve E^F über $k(t)$ durch

$$E^F \,:\, y^2 = x^3 + aF(t)x^2 + bF(t)^2x + cF(t)^3 \tag{3.1}$$

gegeben, und es gilt:

$$\operatorname{Rang} E^F\big(k(t)\big) = 2h, \;\; \textit{wo}$$

h die Anzahl der normierten irreduziblen Teiler g von $t^f - 1$ ist, mit

$$g \neq \begin{cases} x - 1 & \textit{für } f \textit{ gerade} \\ x \pm 1 & \textit{für } f \textit{ ungerade.} \end{cases}$$

Man kann nun $\gamma, \delta \in k^\times$ fest wählen und für verschiedene Werte von f den Rang der resultierenden elliptischen Kurve E^F in Abhängigkeit von f betrachten. Insbesondere erhält man mit $f = p^n + 1$, für $n = 1, 3, 5, \ldots$, wo n die ungeraden Primzahlen durchläuft, das folgende Korollar.

Korollar 15. *Bezeichne E_n für eine ungerade Primzahl n die elliptische Kurve E^F zu dem Polynom*

$$F(t) = \gamma t^{p^n+1} + \delta,$$

gemäß Theorem 8, mit fest gewähltem $\gamma, \delta \in k^\times$. Dann gilt:

$$\operatorname{Rang} E^{F_f}\big(\mathbb{F}_p(t)\big) = \frac{p^n - p}{n} + p - 1,$$

insbesondere gibt es in der Familie $\big\{E_n \,:\, n = 1, 3, 5, 7 \ldots\big\}$ zu jeder vorgegeben Schranke N eine elliptische Kurve mit Rang $> N$.

Beweis. Für $f = p^n + 1$, mit n prim, $n \neq 2$, ist

$$h = \frac{p^n - p}{2n} + \frac{p - 1}{2},$$

eine Aussage, deren Beweis wir abschließend, nach dem Beweis des Theorems 8, nachtragen werden, siehe Lemma 32 auf Seite 84.

Damit ergibt sich nach Theorem 8

$$\operatorname{Rang} E^{F_f}\big(\mathbb{F}_p(t)\big) = 2 \cdot h = \frac{(p^n - p)}{n} + p - 1,$$

wie behauptet, was offenbar

$$\lim_{n\to\infty} \operatorname{Rang} E_n\big(\mathbb{F}_p(t)\big) \longrightarrow \infty$$

impliziert. □

Das Vorgehen beim Beweis lässt sich folgendermaßen umreißen, wie bereits in der Einführung angedeutet: Zu einem Polynom $F(t)$ der obigen Form sei C^F das nichtsinguläre vollständige Modell der durch

$$C^F \,:\, s^2 = F(t) \tag{3.2}$$

definierten irreduziblen algebraischen Kurve. Nun entsteht E^F durch einen quadratischen Twist der Kurve E bezüglich des Funktionenkörpers $L = k(C^F)$, wodurch ein enger Zusammenhang zwischen $E^F(k(t))$ und $E(k(C^F))$ besteht. Andererseits ist $\operatorname{Rang} E(k(C^F))$ gleich $\operatorname{Rang} \operatorname{Hom}_k(J(C^F), E)$, mit

der Jacobischen $J(C^F)$ der Kurve C^F. Damit lassen sich die in Abschnitt 1.5 behandelten Ergebnisse TATES aus [Ta66] über Homomorphismen abelscher Varietäten mit den Resultaten WEILS über Zetafunktionen aus [Wei52], Theorem 7 in Abschnitt 2.2.2, verbinden, um Rang von E^F über $k(t)$ zu ermitteln.

Im einzelnen werden wir zum Beweis des Theorems folgende Schritte durchführen

- Wir betrachten allgemein quadratische Twists E_L^{twist} einer über einem Körper k definierten elliptischen Kurve E bezüglich einer quadratischen Körpererweiterung L von $k(t)$. Wir werden dann für $L = k(C)$ sehen, dass $E_L^{\text{twist}}(L) \simeq E(L)$ und $E_L^{\text{twist}}(k(t)) \simeq E(L)/\sigma$, mit (dem einzigen) nichttrivialem $\sigma \in \text{Gal}(L \mid k(t))$. Daraus erhalten wir für endliches k: $\text{Rang}\, E_L^{\text{twist}}(k(t)) = \text{Rang}\, E(L)$.

- Ist C eine nichtsinguläre, geometrisch irreduzible vollständige Kurve und $L = k(C)$ ihr Funktionenkörper, so werden wir zeigen: Für eine über k definierte elliptische Kurve E ist $E(L) \simeq \text{Mor}_k(C, E)$ und weiter $\text{Mor}_k(C, E) \simeq \text{Hom}_k(J(C), E) \oplus E(k)$. Für endliches k ergibt sich daraus wiederum $\text{Rang}\, E(L) = \text{Rang}\, \text{Hom}_k(J(C), E)$.

- Aus den Ergebnissen von TATE, aus Theorem 32, das wir in Abschnitt 1.5 dargestellt haben, leiten wir her, dass über einem endlichen Körper k gilt $\text{Rang}\, \text{Hom}_k(J(C), E) = 2h$, wo h definiert ist über die Ordnung zu der P_E, der Zähler der Zetafunktion von E, P_C, den Zähler der Zetafunktion von C, teilt.

- Schließlich werden wir unter Verwendung von Theorem 7, auf Seite 63, welches $P_C(U)$ für Kurven des Typs C^F angibt, $\text{Rang}\, E^F$ ermitteln, wobei wir noch $P(E) = 1 + pU^2$, aus Korollar 7, Seite 32, ausnutzen.

3.1.1 Quadratische Twists

Wir definieren in diesem Abschnitt den Begriff des quadratischen Twists. Definitionen und einfache Beispiele hierfür finden sich z.B. bei [Sb00], 3.4 auf S. 17f. und in [Har77], Example 7.8.5, S. 159. Der allgemeine Begriff des Twists einer Kurve C bzw. elliptischen Kurve E als einer zu über $\bar{k}$ zu C respektive E isomorphen Kurve findet sich z.B. in [Sil86], Chap. X, S. 306ff.

Definition 26. Sei E eine elliptische Kurve, über einem Körper K, $char(K) \neq 2$, definiert durch eine Gleichung der Form

$$E : y^2 = x^3 + ax^2 + bx + c \text{ mit } a, b, c \in K.$$

Für ein $D \in K^\times$ bezeichnen wir die elliptische Kurve E_D^{twist} mit der Gleichung

$$E_D^{\text{twist}} \,:\, y^2 = x^3 + aDx^2 + bD^2x + cD^3$$

als *quadratischen Twist* von E mit D, oder auch als quadratischen Twist bezüglich $L = K(\sqrt{D})$.

Beispiel. $K = \mathbb{Q}$ und D eine ganze Zahl $\neq 0$, E ist gegeben in der Form

$$E \,:\, y^2 = x^3 + ax + b \text{ mit } \; a, b \in \mathbb{Q},\, b \neq 0 \;\text{ und}$$
$$E^D \,:\, y^2 = x^3 + D^2ax + D^3b$$

ist der quadratische Twist mit D, was häufig auch in der isomorphen Form

$$E^D \,:\, Dy^2 = x^3 + ax + b$$

angegeben wird, L ist hier, falls $D \notin \mathbb{Q}^2$, der Zahlkörper $\mathbb{Q}(\sqrt{D})$, andernfalls ist $L = \mathbb{Q}$. (Zu diesem Beispiel vgl. [Sb00], S. 17).

Lemma 24. *Für E, E_D^{twist} wie oben gilt $E \simeq E_D^{\text{twist}}$ über L, explizit vermittelt durch*

$$\phi \,:\, \left\{ \begin{array}{ccc} E & \to & E_D^{\text{twist}} \\ (x,y) & \mapsto & (Dx, D\alpha y) \end{array} \right\} \qquad \textit{und} \qquad \phi^{-1} \,:\, \left\{ \begin{array}{ccc} E_D^{\text{twist}} & \to & E \\ (x,y) & \mapsto & (\frac{x}{D}, \frac{y}{\alpha D}) \end{array} \right\},$$

mit $\alpha \in L$, $\alpha^2 = D$.

Korollar. *Für E, E_D^{twist} wie oben gilt*

$$j(E) = j(E_D^{\text{twist}})$$

Beweis. Da E, E_D^{twist} isomorph über $L \subset \bar{K}$ sind, haben sie gleiche j-Invarianten. Man kann dies natürlich auch explizit nachrechen, z.B. für *char* $K \neq 2, 3$

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2} = 1728\frac{4(D^2a)^3}{4(D^2a)^3 + 27(bD^3)^2} = j(E_D^{\text{twist}}),$$

und analog (durch etwas längere Rechnung) auch für *char* $K = 3$. □

Wir werden uns speziell mit folgender Situation befassen: E ist über einem Körper k, $char(k) \neq 2$ definiert, $K = k(t)$, der Funktionenkörper in einer Variable und $D = f(t)$ ein Polynom aus $k[t]$, $f(t)$ nicht konstant und separabel, mit grad $f(t) \geq 2$.

Weiter sei C das nichtsinguläre vollständige Modell der durch

$$C \,:\, s^2 = f(t)$$

über $k(t)$ definierten geometrisch irreduziblen algebraischen Kurve, und $L = k(C)$ ihr Funktionenkörper.

Den quadratischen Twist (bezüglich $K = k(t)$) von E mit $f(t)$ bezeichnen wir nun mit $E^{\text{twist}}_{f(t)}$,

$$\begin{aligned} E &: y^2 = x^3 + ax^2 + bx + c, \\ E^{\text{twist}}_{f(t)} &: y^2 = x^3 + af(t)\, x^2 + bf(t)^2\, x + cf(t)^3. \end{aligned}$$

Wir formulieren Lemma 24 für unsere Situation um und erhalten:

Lemma 25. *Über $L = k(C)$ sind E und $E^{\text{twist}}_{f(t)}$ isomorph,*

$$E \overset{L}{\simeq} E^{\text{twist}}_{f(t)},$$

explizit:

$$\phi : \left\{ \begin{array}{ccc} E & \to & E^{\text{twist}}_{f(t)} \\ (x,y) & \mapsto & (f(t)x, f(t)sy) \end{array} \right\}, \qquad \phi^{-1} : \left\{ \begin{array}{ccc} E^{\text{twist}}_{f(t)} & \to & E \\ (x,y) & \mapsto & \left(\frac{x}{f(t)}, \frac{y}{f(t)s}\right) \end{array} \right\}.$$

Bemerkung 20. Es ist also $E \simeq E^{\text{twist}}_{f(t)}$ über L, einer quadratischen Erweiterung von $k(t)$. Allgemeiner liegt somit folgende Situation vor: Eine über einem Funktionenkörper $k(t)$ definierte elliptische Kurve E' ist nach einer endlichen Erweiterung zu einer Kurve E über dem Grundkörper k isomorph. Eine elliptische Kurve E' mit dieser Eigenschaft bezeichnet man als *isotrivial*. Ein offensichtliches Kriterium hierfür ist $j(E') = j(E) \in k$.

Anhand der Gleichung von $E^{\text{twist}}_{f(t)}$ ist ersichtlich, dass $E^{\text{twist}}_{f(t)}$ als elliptische Kurve bereits über $k(t)$ definiert ist. Offenbar ist $E^{\text{twist}}_{f(t)}(k(t)) \subset E^{\text{twist}}_{f(t)}(L)$ und damit isomorph zu einer Teilmenge von $E(L)$. Wie sieht diese Teilmenge genau aus?

Lemma 26. *Ist σ der Galois-Automorphismus der quadratischen Körpererweiterung $[L : k(t)]$,*

$$\sigma \; : \; \left\{ \begin{array}{l} t \mapsto t \\ s \mapsto -s \end{array} \right. ,$$

so liefert σ einen Gruppenautomorphismus von $E(L)$ und es gilt:

$$E^{\text{twist}}_{f(t)}(k(t)) \simeq \big\{ P \in E(L) \; : \; \sigma(P) = -P \big\}.$$

Beweis. Ist $P = (x, y)$ ein Punkt aus $E(L)$, so liegt $\sigma(P) = (\sigma(x), \sigma(y))$ ebenfalls in $E(L)$, da $k(t)$ unter σ fest bleibt. Somit definiert σ einen Gruppenautomorphismus von $E(L)$. Ist ϕ der Isomorphismus von $E(L)$ auf $E^{\text{twist}}_{f(t)}(L)$

und $P \in E(L)$ so ist

$$\sigma\big(\phi(P)\big) = \sigma\big(\phi(x,y)\big) = \sigma\big(f(t)x, f(t)ys\big) = \\ = \big(f(t)\sigma(x), -f(t)\sigma(y)s\big) = -\big(f(t)\sigma(x), f(t)\sigma(y)s\big) = -\phi\big(\sigma(P)\big).$$

Das heißt, der Punkt $Q = \phi(P) \in E^{\text{twist}}_{f(t)}(L)$ ist genau dann invariant unter σ, wenn $\sigma(P) = -P$ in $E(L)$ gilt. Da $E^{\text{twist}}_{f(t)}$ und E über L isomorph sind, bedeutet dies, ein Punkt $Q \in E^{\text{twist}}_{f(t)}(L)$ ist genau dann schon über $k(t)$, dem Fixkörper von σ, rationaler Punkt von $E^{\text{twist}}_{f(t)}$, wenn $P = \phi^{-1}(Q)$ die Beziehung $\sigma(P) = -P$ erfüllt. □

Lemma 27. *Für eine elliptische Kurve E, die über einem Körper k definiert ist, gilt:*

$$E\big(k(t)\big) = E\big(k\big).$$

Beweis. Jeder Punkt $P = \big(\alpha(t), \beta(t)\big) \in E\big(k(t)\big)$ definiert vermöge $t \mapsto \big(\alpha(t), \beta(t)\big)$ eine k-rationale Abbildung $\phi : \mathbb{P}^1 \to E$. Diese induziert eine rationale Abbildung $\phi^* : k(E) \to k(\mathbb{P}^1) \simeq k(t)$. Nehmen wir nun an, ϕ^* ist nicht konstant. Wir haben dann eine Injektion $k(E) \hookrightarrow k(t)$. Damit ist nach dem Satz von Lüroth $k(E) \simeq k(t)$ und somit auch $E \simeq \mathbb{P}^1$. Widerspruch! Folglich ist ϕ konstant in t, und $P \in E(k)$. □

Bemerkung. Alternativ kann man den Widerspruch im Beweis des Lemmas auch folgendermaßen erhalten: ϕ ist einen k-rationale Abbildung nichtsingulärer algebraischer Kurven, $\mathbb{P}^1 \xrightarrow{\phi} E$. Aus der Annahme, ϕ nicht konstant, folgt dann nach dem Satz von Riemann-Hurwitz $0 = g(\mathbb{P}^1) \geq g(E) = 1$.

Lemma 28. *Für jedes $P \in E(L)$ ist $P + \sigma(P) \in E(k)$.*

Beweis. Aus der Definition von σ ist klar, dass σ eine Involution ist, deshalb ist $P + \sigma(P)$ für jedes $P \in E(L)$ unter σ invariant und liegt somit in $E(k(t))$. Nach Lemma 27 folgt dann aber schon $P + \sigma(P) \in E(k)$. □

Aus den vorangegangenen Lemmata wissen wir

$$E^{\text{twist}}_{f(t)}(k(t)) \simeq \operatorname{Kern}\rho, \quad \text{mit } \rho : \left\{\begin{matrix} E(k(C)) & \to & E(k) \\ P & \mapsto & P + \sigma(P) \end{matrix}\right\},$$

also

$$0 \longrightarrow E^{\text{twist}}_{f(t)}(k(t)) \longrightarrow E(k(C)) \xrightarrow{\rho} E(k)$$

ist exakt.

Ist nun k ein endlicher Körper, so können wir hieraus den nachfolgenden Satz gewinnen.

Satz 37. *Sei k ein endlicher Körper, $\operatorname{char} k \neq 2$, E eine über k definierte elliptische Kurve, C das nichtsinguläre, vollständige Modell einer irreduziblen algebraischen Kurve mit der Gleichung $s^2 = f(t)$, $L = k(C)$, und $E^{\text{twist}}_{f(t)}$ der quadratische Twist von E mit $f(t)$ bezüglich L. Dann gilt:*

$$\operatorname{Rang} E^{\text{twist}}_{f(t)}\big(k(t)\big) \;=\; \operatorname{Rang} E(L).$$

Beweis. Wir zeigen: $\operatorname{Rang} \operatorname{Kern} \rho = \operatorname{Rang} E(L)$.
Da k endlich, ist $E(k)$ ebenfalls endlich. Sei $N = \operatorname{ord} E(k)$ und $r = \operatorname{Rang} E(L)$. Es gibt dann r unabhängige Elemente $P_1, \ldots, P_r$ unendlicher Ordnung in $E(L)$, mit $\langle P_1, \ldots, P_r \rangle \simeq \mathbb{Z}^r$. Auch $\langle nP_1, \ldots, nP_2 \rangle \simeq \mathbb{Z}^r$ für jedes ganzzahlige n. Insbesondere gilt dies für $n = N$. Aber $\rho\,(NP_i) = N\,\rho\,(P_i) = 0$ in $E(k)$ für jedes $i = 1, \ldots, r$. Also $\mathbb{Z}^r \simeq \langle NP_1, \ldots, NP_2 \rangle \subseteq Kern\,\rho$ und somit $\operatorname{Rang} \operatorname{Kern} \rho = \operatorname{Rang} E(L)$. Da $E^{\text{twist}}_{f(t)}(k(t)) \simeq \operatorname{Kern} \rho$ folgt die Behauptung. □

3.1.2 Elliptische Kurven über $k(C)$ und die Jacobische $J(C)$

In diesem Abschnitt bezeichnet k einen Körper, E eine über k definierte elliptische Kurve, und C eine vollständige, nichtsinguläre, geometrisch irreduzible Kurve über k und $L = k(C) \subseteq k(s,t)$ ihren Funktionenkörper sowie $J(C)$ ihre Jacobische Varietät.

Wir wollen die Gruppe $E\big(k(C)\big)$ der rationalen Punkte von E über $k(C)$ näher untersuchen.

Satz 38. *Unter den obigen Voraussetzungen gilt*

$$E\,\big(k(C)\big) \simeq \operatorname{Mor}_k\big(C,\, E\big).$$

Beweis. $E(L) \hookrightarrow \operatorname{Mor}_k\big(C,\, E\big)$:
Ist $P = (x, y) \in E\big(k(C)\big)$, so lassen sich die beiden Koordinaten von P als rationale Funktionen in t und s schreiben. $P = (\alpha(s,t), \beta(s,t))$ mit $\alpha, \beta \in k(C)$. Damit ist zu jedem P eine k-rationale Abbildung erklärt,

$$\begin{array}{ccc} C & \to & E \\ (s,t) & \mapsto & \big(\alpha(s,t),\, \beta(s,t)\big) \end{array}.$$

Da C, E nichtsinguläre, projektive algebraische Kurven sind, ist diese Abbildung sogar ein Morphismus $C \to E$. Also ist $E(L)$ isomorph zu einer Untergruppe von $\operatorname{Mor}_k(C, E)$.

$\mathrm{Mor}_k\big(C,\, E\big) \hookrightarrow E(L)$:
Jedes $\phi \in \mathrm{Mor}_k\big(C,\, E\big)$ ist als Morphismus auch eine k-rationale Abbildung von C nach E. Es gibt zu ϕ also rationale Funktionen, $\alpha, \beta \in k(C)$, sodass ϕ sich für fast alle Punkte $Q \in C$ beschreiben lässt durch $\phi(Q) = (\alpha(Q),\, \beta(Q))$. Da $\phi(Q) \in E$, erfüllen α, β insbesondere die Kurvengleichung von E,

$$\beta^2 = \alpha^3 + a\alpha^2 + b\alpha + c,$$

also $(\alpha,\, \beta) \in E\big(k(C)\big)$.

□

Um fortzufahren, benötigen wir eine grundlegende Eigenschaft jacobischer Varietäten, die wir bereits in Satz 27, auf Seite 26, kennengelernt haben und hier noch einmal kurz wiederholen wollen:

Satz. *Sei C eine nichtsinguläre, geometrisch irreduzible projektive Kurve über k, mit $C(k) \neq \emptyset$, und $J(C)$ die zu C gehörige jacobische Varietät. Die kanonische Abbildung $f : C \to J(C)$ hat dann folgende Eigenschaft:*

Ist $h : C \to A$ eine rationale Abbildung von C auf eine abelsche Varietät, so gibt es einen eindeutig bestimmten Homomorphismus $\alpha : J(C) \to A$ abelscher Varietäten, so, dass h in der Form $h = \alpha \circ f + a$ faktoriert, mit einem $a \in A$. Sind f, h über k definiert, so ist auch α über k definiert und $a \in A(k)$.

Hieraus ergibt sich als unmittelbare Folgerung

Korollar 16.

$$\mathrm{Mor}_k(C, A) \simeq \mathrm{Hom}_k(J(C), A) \oplus A(k).$$

Satz 39. *Ist der Körper k endlich, und sind E, C und $J(C)$ über k wie oben definiert, so gilt*

$$\mathrm{Rang}\, E\big(k(C)\big) = \mathrm{Rang}\, \mathrm{Hom}_k\big(J(C),\, E\big).$$

Beweis. Mit $A = E$ erhält man aus dem letzten Korollar und Satz 38

$$E\big(k(C)\big) \simeq \mathrm{Hom}_k\big(J(C),\, E\big) \oplus E(k).$$

Da nun aber $E(k)$ endlich ist, wenn k endlich ist, kann der freie Anteil in der Zerlegung von $E(k(C))$, $E(k(C)) \simeq \mathbb{Z}^r \oplus E_{\mathrm{tors}}$ nur in $\mathrm{Hom}_k(J(C), E)$ liegen. Daraus ergibt sich sofort die Behauptung. □

Wir wollen das bisher Gezeigte durch ein einfaches Beispiel illustrieren.

Beispiel. Sei *char* $k \neq 2, 3$. In der Konstruktion von $E^{\text{twist}}_{f(t)}$ wählen wir $C = E$. Also:

$$E : y^2 = x^3 + ax + b, \qquad a, b \in k, \text{ nicht beide } 0,$$
$$C : s^2 = t^3 + at + b = f(t).$$

Zunächst bestimmen wir den Rang von $E^{\text{twist}}_{f(t)}$. Nach Satz 37 gilt

$$\operatorname{Rang} E^{\text{twist}}_{f(t)}\big(k(t)\big) = \operatorname{Rang} E\big(k(E^{\text{twist}}_{f(t)})\big),$$

woraus mit Satz 39 folgt

$$\operatorname{Rang} E^{\text{twist}}_{f(t)}\big(k(t)\big) = \operatorname{Rang} \operatorname{Mor}_k\big(J(E),\, E\big).$$

Nach Satz 27, Seite 26, gilt $J(E)$ birational äquivalent zu $E^{\langle g(E)\rangle}$. Da das Geschlecht $g(E) = 1$, ist somit

$$\operatorname{Mor}_k\big(J(E),\, E\big) \simeq \operatorname{End}_k\big(E,\, E\big).$$

Also ergibt sich

$$\operatorname{Rang} E^{\text{twist}}_{f(t)}\big(k(t)\big) = \operatorname{Rang} \operatorname{End}_k(E) \in \big\{1, 2, 4\big\},$$

nach Satz 19 in Abschnitt 1.2.2, wobei in Charakteristik $p > 0$ der $\operatorname{Rang} \operatorname{End}_k(E) = 2$ falls E gewöhnlich ist und ≥ 2 wenn E supersingulär, vergleiche Abschnitt 1.4.

Als Nächtes wollen wir nach rationalen Punkten von $E^{\text{twist}}_{f(t)}$ über $k(t)$ suchen.

- Sind $A(t),\, B(t) \in k(t)$ mit

$$\big(A(t),\, B(t)s\big) \in E,$$

so folgt

$$\begin{aligned}\big(B(t)f(t)^2\big)^2 &= B(t)^2 f(t)^4 = B(t)^2 s^2 \cdot f(t)^3 \\ &= \big(A(t)^3 + aA(t) + b\big) \cdot f(t)^3 \\ &= \big(A(t)f(t)\big)^3 + af(t)^2 \cdot A(t)f(t) + bf(t)^3,\end{aligned}$$

Also gilt

$$\big(A(t),\, B(t)f(t)^2\big) \in E^{\text{twist}}_{f(t)},$$

dieser Punkt ist sogar aus $E^{\text{twist}}_{f(t)}\big(k(t)\big)$, da $A(t), B(t), f(t)$ nach Voraussetzung Elemente von $k(t)$ sind.

- Insbesondere folgt für $A(t) = t$ und $B(t) = 1$, wegen $(t, s) \in E^{\text{twist}}_{f(t)}\big(k(E)\big)$,

$$\big(tf(t), f(t)^2\big) \in E^{\text{twist}}_{f(t)}\big(k(t)\big).$$

- Ist $k = \mathbb{F}_p$, $p \neq 2, 3$, so folgt aus $f(t)^p = f(t^p)$ zunächst $(t^p, s^p) \in E$. Da nun

$$\big(t^p, s^p\big) = \big(t^p, (s^2)^{\frac{p-1}{2}} \cdot s\big) = \big(t^p, f(t)^{\frac{p-1}{2}} \cdot s\big),$$

erhält man für $A(t) = t^p$, $B(t) = f(t)^{\frac{p-1}{2}}$ einen weiteren Punkt

$$\big(t^p f(t),\, f(t)^{\frac{p-1}{2}} \cdot f(t)^2\big) = \big(t^p f(t),\, f(t)^{\frac{p+3}{2}}\big) \in E^{\text{twist}}_{f(t)}\big(k(t)\big).$$

3.1.3 Zetafunktionen und der Rang

In diesem Abschnitt bezeichnet k einen endlichen Körper $k = \mathbb{F}_{p^n}$, $n \geq 1$ und $p \neq 2$. Wir führen die Bezeichnungen des vorherigen Abschnitts weiter, C ist eine nichtsinguläre, geometrisch irreduzible projektive Kurve über k, $L = k(C)$ ihr Funktionenkörper, $J(C)$ die Jacobische und E ist eine über k definierte elliptische Kurve.

Wir werden einen Zusammenhang zwischen $\text{Hom}_k(J(C),\, E)$ und den Zetafunktionen der beiden Kurven C und E herstellen. Dies ermöglichen uns Resultate aus der Arbeit Tates, [Ta66], die wir in Abschnitt 1.5 behandelt haben.

Satz (aus [Ta66], siehe Satz 32, Seite 36)**.** *Sind A, B abelsche Varietäten über $k = \mathbb{F}_{p^n}$ und f_A und f_B die jeweiligen charakteristischen Polynome des Frobenius-Endomorphismus bezüglich k von A und B.*

1. *B ist k-isogen zu einer abelschen Untervarietät von A genau dann, wenn f_B einer Teiler von f_A ist,*

$$B \sim_k A' \subset A \;\Leftrightarrow\; f_B \mid f_A. \tag{3.3}$$

2. *Für den Rang von $\text{Hom}_k\big(A,\, B\big)$ gilt*

$$\text{Rang}\Big(\text{Hom}_k\big(A,\, B\big)\Big) = r\big(f_A,\, f_B\big), \tag{3.4}$$

mit $r\,(\cdot,\, \cdot)$ aus Definition 21, Seite 36, d.h.

$$r\big(f_1,\, f_2\big) = \sum_p e_1(p)e_2(p),$$

wenn $f_i = \prod_p p^{e_i(p)}$ die kanonische Zerlegung von f_i, $i = 1, 2$, in Linearfaktoren über einem gemeinsamen Zerfällungskörper $K \subset \overline{\mathbb{Q}}$ von f_1, f_2 ist.

Satz 40. *Sei A eine abelsche Varietät und E eine elliptische Kurve, beide über einem endlichen Körper k definiert, und seien $f_A(U)$ sowie $f_E(U)$ die charakteristischen Polynome der Frobenius-Endomorphismen (bezüglich k) von A und E. Über $\overline{\mathbb{Q}}$ ist dann*

$$f_A(U) = f_E(U)^{\tilde{h}} g(U), \qquad \text{mit } \tilde{h} \in \frac{1}{2}\mathbb{N}_0, \ \operatorname{ggT}(g(U), f_E(U)^{\tilde{h}}) = 1.$$

Definiert man eine $h \in \mathbb{N}_0$ durch

$$h = \begin{cases} \tilde{h} & \text{falls } f_E(U) \text{ irreduzibel über } \mathbb{Q} \\ 2\tilde{h} & \text{falls } f_E(U) \text{ ein Quadrat über } \mathbb{Q} \end{cases},$$

so ist h wohldefiniert und es gilt

$$\operatorname{Rang} \operatorname{Hom}_k(A,\, E) = 2h.$$

Bemerkung 21. Es treten nur die beiden Fälle, die in der Definition von h angeführt wurden, auf, also $f_E(U)$ zerfällt nicht schon über $\mathbb{Q}$ in zwei verschiedene nichttriviale Faktoren, wie der folgende Beweis klar machen wird.
Der folgende Beweis liefert zunächst nur $2\tilde{h} \in \mathbb{N}_0$, wie in der Behauptung. Tatsächlich ist aber schon $\tilde{h} \in \mathbb{N}_0$, vgl. Bemerkung 22

Beweis. Nach Definition 15 und Satz 20, Seite 18f, ist $f_E(U)$ ein quadratisches Polynom. Wie im Beweis von Korollar 8, auf Seite 37, müssen wir nun zwei Fälle unterscheiden: Entweder

$$f_E(U) = \big(U - \alpha\big) \cdot \big(U - \beta\big), \qquad \alpha, \beta \in \overline{\mathbb{Q}}, \ \alpha \neq \beta,$$

oder

$$f_E(U) = \big(U - \alpha\big)^2, \qquad \alpha \in \overline{\mathbb{Q}}.$$

Im ersten Fall ist $\tilde{h} \in \mathbb{N}_0$, im zweiten Fall ist zumindest $2\tilde{h} \in \mathbb{N}_0$. Es gilt $\operatorname{ggT}\big(f_E(U)^{\tilde{h}},\, g(U)\big) = 1$ in beiden Fällen. Über $k = \mathbb{F}_q$ sind die Polynome $f_E(U)$ und $f_A(U)$ normiert und haben Koeffizienten aus $\mathbb{Z}$, nach Satz 20 sowie Satz 23, auf Seite 21. Nach Gleichung (3), Seite 19, ist

$$f_E\big(U\big) = U^2 - tU + q, \qquad \text{mit } t = \operatorname{Tr} Fr, \ |t| \leq 2\sqrt{q},$$

damit ist $t^2 - 4q \leq 0$, also ist die Diskriminante von $f_E(U)$ negativ oder Null, d.h. $f_E(U)$ ist genau dann irreduzibel über $\mathbb{Q}$, wenn es zwei verschiedene Wurzeln hat. Andernfalls ist $f_E(U)$ ein Quadrat in $\overline{\mathbb{Q}}[U]$, $f_E(U) = (U \pm \sqrt{q})^2$. Da dann $\mathbb{Z} \ni t = \pm 2\sqrt{q}$, ist in diesem Fall $\sqrt{q} \in \mathbb{Q}$.

Also ist $f_E(U)$ irreduzibel über $\mathbb{Q}$ genau dann, wenn $f_E(U)$ kein Quadrat in $\overline{\mathbb{Q}}[U]$ ist. Wir berechnen $r\big(f_E(U),\, f_A(U)\big)$ in beiden Fällen:

- Sei $f_E(U) = (U-\alpha)(U-\beta)$, mit $\alpha \neq \beta$.

$$r\big(f_A(U),\, f_E(U)\big) = \sum_{i=1,2} e_E(p_i)e_A(p_i) = \sum_{i=1,2} 1 \cdot \tilde{h} = 2\tilde{h} = 2h,$$

  da $\tilde{h} \in \mathbb{N}_0$, ist hier $h = \tilde{h}$ wohldefiniert.

- Sei $f_E(U) = (U-\alpha)^2 = p(U)^2$.

$$r\big(f_A(U),\, f_E(U)\big) = e_E(p)e_A(p) = 2 \cdot 2\tilde{h} = 4\tilde{h} = 2h,$$

  wobei hier $\tilde{h} \in \frac{1}{2}\mathbb{N}_0$ und somit $h = 2\tilde{h}$ wohldefiniert ist.

Der Rest der Behauptung ergibt sich aus (3.4) und (3.3). □

Satz 41. *Sei C eine nichtsinguläre, irreduzible projektive Kurve, über k definiert, mit jacobischer Varietät $J(C)$, und sei E eine elliptische Kurve über k. Bezeichnen wir mit $Z(C,U)$ und $Z(E,U)$ die Zetafunktionen von C und E,*

$$Z(C,\,U) = \frac{P_C(U)}{(1-U)(1-qU)} \qquad \textit{und} \qquad Z(E,\,U) = \frac{P_E(U)}{(1-U)(1-qU)},$$

so gilt:

$$\operatorname{Rang} E\big(k(C)\big) = 2h,$$

wo $h \in \mathbb{N}_0$ definiert ist über $P_C(U) = P_E(U)^h R(U)$ für $P_E(U)$ irreduzibel in $\mathbb{Q}[U]$, und $P_C(U) = P_E(U)^{h/2} R(U)$ für $P_E(U)$ ein Quadrat in $\mathbb{Q}[U]$, und R in beiden Fällen zu P_E teilerfremd.

Beweis. Nach Satz 26, auf Seite 25, haben E und C als Kurven Zetafunktionen der obigen Form, mit Nenner $(1-U)\,(1-qU)$. Ist $f(U)$ das charakteristische Polynom des Frobenius auf der Jacobi-Varietät der jeweiligen Kurve, und $f(U) = \prod_{i=1}^{2g}(U-a_i)$ dessen Zerlegung in Linearfaktoren, so hat nach Korollar 5, (1.12) der Zähler der Zetafunktion dieser Kurve die Form $P(U) = \prod_{i=1}^{2g}(1-a_iU)$. Also folgt $f_E(U) \mid f_{J(C)}(U) \Leftrightarrow P_E(U) \mid P_C(U)$, und auch das hier definierte h ist gleich dem in Satz 40. Damit erhält man $\operatorname{Rang}\operatorname{Hom}_k(J(C), E) = 2h$. Aus Satz 39 im vorherigen Abschnitt folgt nun die restliche Behauptung. □

Bemerkung 22. Aufgrund von Satz (3.3) und dem früheren Korollar 5 gilt

$$P_E(U) \text{ teilt } P_C(U) \quad \Longleftrightarrow$$
$$J(C) \sim E^r \times A, \quad r > 0,\ A \text{ abelsche Varietät über } k.$$

Dies lässt sich noch präzisieren: Ist nämlich $J(C) \sim E^r \times A$, mit A einer abelschen Varietät ohne zu E isogenen abelschen Untervarietäten, so gilt

$$\begin{aligned}\operatorname{Hom}_k\big(J(C), E\big) &\simeq \operatorname{Hom}_k\big(E^r, E\big)\\ &\simeq \operatorname{Hom}_k\big(E, E\big)^r\end{aligned}$$

also haben wir $\operatorname{Rang} E\big(k(C)\big) = r \cdot \operatorname{Rang} \operatorname{End}_k E$. Mit Korollar 8 und Lemma 7, auf Seite 37f sieht man aber, dass die beiden Fälle in der Definition von h in Satz 40 und Satz 41 genau den beiden Fällen entsprechen, dass entweder $\operatorname{End}_k E$ eine Ordnung in einer Quaternionenalgebra ist, oder in einem imaginärquadratischen Zahlkörper. Also

$$\operatorname{Rang} E\big(k(C)\big) = 2h = \left.\begin{cases} 4\tilde{h} & : \operatorname{Rang} \operatorname{End}_k E = 4 \\ 2\tilde{h} & : \operatorname{Rang} \operatorname{End}_k E = 2 \end{cases}\right\} = \tilde{h} \operatorname{Rang} \operatorname{End}_k E.$$

Das heißt $\tilde{h} = r$. Insbesondere folgt hieraus auch $\tilde{h} \in \mathbb{N}_0$.

3.1.4 Die Zetafunktion von C^F

Im Folgenden ist $k = \mathbb{F}_p$, $p \neq 2$, und $\bar{k}$ der algebraische Abschluss $\overline{\mathbb{F}}_p$. Unser Ziel ist es, Theorem 8 zu beweisen. Wir haben bereits in Satz 37 gesehen, dass $\operatorname{Rang} E^F\big(k(t)\big) = \operatorname{Rang} E\big(k(C^F)\big)$, was nach Satz 39 wiederum gleich $\operatorname{Rang} \operatorname{Hom}_k\big(C^F, E\big)$ ist. Aufgrund von Satz 41 können wir diesen Rang nun aus den Zetafunktionen von C^F und E bestimmen. Da E nach Voraussetzung eine über $\mathbb{F}_p$ supersinguläre elliptische Kurve ist, hat deren Zetafunktion die Form

$$Z\big(E, X\big) = \frac{1 + pX^2}{\big(1 - X\big)\big(1 - pX\big)},$$

aus Korollar 7 in Abschnitt 1.4. In Abschnitt 2.2.2 haben wir bereits einen Ausdruck für die Zetafunktion von Kurven eines C^F umfassenden Typs kennengelernt, Theorem 7 auf Seite 63. Die dort angegebene Form eignet sich jedoch noch schlecht, um h aus Satz 41 zu bestimmen, unser Ziel ist deshalb folgende Aussage:

Satz 42. *Sei C das nichtsinguläre, vollständige Modell einer irreduziblen algebraischen Kurve, die über k durch eine Gleichung der Form*

$$s^e = \gamma t^f + \delta, \qquad \gamma, \delta \in k^\times,$$

definiert ist, wobei e und f ganze Zahlen sind, mit

$$\begin{aligned} 2 \leq e \leq f, \qquad p \nmid ef \qquad &\textit{und}\\ m = \operatorname{kgV}\big(e, f\big) \;\mid\; \big(p^n + 1\big) \;&\textit{für ein } n > 0. \end{aligned}$$

Bezeichne k_ϕ für ein $\phi \in \mathrm{Hom}\big((\mathbb{Z}/e\mathbb{Z}) \times (\mathbb{Z}/f\mathbb{Z}),\, \bar{k}^\times\big)$ die Körpererweiterung

$$k_\phi = k\big(\phi(\xi),\, \phi(\eta)\big), \quad \textit{mit} \qquad \begin{matrix} \langle \xi \rangle = & (\mathbb{Z}/e\mathbb{Z}) \\ \langle \eta \rangle = & (\mathbb{Z}/f\mathbb{Z}) \end{matrix},$$

und $d_\phi = [k_\phi : k]$ deren Grad. Es gilt dann:

1. *Wird ϕ so gewählt, dass*

$$\phi(\xi) \neq 1,\ \phi(\eta) \neq 1,\ \phi(\xi\eta) \neq 1, \tag{3.5}$$

   für erzeugende Elemente ξ, η von $(\mathbb{Z}/e\mathbb{Z}) \times (\mathbb{Z}/f\mathbb{Z})$, so ist d_ϕ gerade, $d_\phi = 2c_\phi$.

2. *$P_C(U)$, der Zähler der Zetafunktion von C, lässt sich als Produkt*

$$P_C\big(U\big) \;=\; \prod_{\phi} \big(1 + p^{c_\phi} U^{d_\phi}\big) \tag{3.6}$$

   darstellen. Das Produkt läuft dabei über diejenigen Repräsentanten ϕ der Restklassen unter der Operation von $\mathrm{Gal}(k_\phi \mid k)$, welche (3.5) erfüllen.

Wir behalten im Rest dieses Abschnitts die Bezeichnungen und Voraussetzungen des Satzes bei. Im Folgenden sei ζ eine fest gewählte primitive m-te Einheitswurzel in $\bar{k}^\times$. Nach Definition sind e, f Teiler von m, sowie $e \leq f$. Da außerdem $\operatorname{ord} \phi(\xi) \mid e$ und $\operatorname{ord} \phi(\eta) \mid f$, gibt es ganze Zahlen a, b, so, dass

$$\phi(\xi) = \zeta^{maf^{-1}}, \qquad \phi(\eta) = \zeta^{mbf^{-1}}.$$

Wir setzten nun $m_\phi = \operatorname{ord} \phi$, sowie $a_0 = m_\phi a f^{-1}$, $b_0 = m_\phi a f^{-1}$, und wählen dann ein festes erzeugendes Element ω von ${k_\phi}^\times$, mit der Eigenschaft

$$\zeta^{m{m_\phi}^{-1}} = (\omega^{p^{d_\phi}-1})^{(m_\phi)^{-1}}.$$

Dann können wir einen Gruppencharakter χ definieren durch

$$\chi \,:\, \begin{cases} k_\phi^\times & \to \quad \overline{\mathbb{Q}}^\times \\ \omega & \mapsto \quad \exp\big(\frac{2\pi\imath}{m_\phi}\big) \end{cases}. \tag{3.7}$$

Beweis von 42, 1. Teil. **Behauptung:** d_ϕ ist gerade
Es gilt $m_\phi = \mathrm{kgV}(\operatorname{ord}_{k_\phi} \phi(\xi), \operatorname{ord}_{k_\phi} \phi(\eta))$, und $k_\phi = k(\zeta^{m{m_\phi}^{-1}})$.

Nun ist d_ϕ die kleinste ganze Zahl, für die $m_\phi \mid p^d - 1$, also ist $p^{d_\phi} \equiv 1 \bmod m_\phi$ und die Restklasse von p in $(\mathbb{Z}/m_\phi\mathbb{Z})^\times$ hat die Ordnung d_ϕ. Nach

Voraussetzung (3.5) ist $m_\phi > 2$, $m_\phi \mid m$. Aus $m \mid p^n+1$, also $p^n \equiv -1 \bmod m$, folgt somit $p^n \equiv -1 \bmod m_\phi$. Dann ist d_ϕ als Ordnung der Restklasse $p+m_\phi$ ein Teiler von $2n$. Da aus $d_\phi \mid n$ folgen würde $p^n \equiv 1 \bmod m_\phi$, muss d_ϕ gerade sein, $d_\phi = 2c_\phi$.

□

Korollar. *Setzt man $k_{c_\phi} = \mathbb{F}_{p^{c_\phi}}$, so ist χ auf $k_{c_\phi}^\times$ trivial, also $\chi\big(k_{c_\phi}^\times\big) = 1$.*

Beweis. Da $p^{d_\phi} \equiv 1 \bmod m_\phi$ ist $p^{c_\phi} \equiv p^n \equiv -1 \bmod m_\phi$, und somit ist per Definition von χ

$$\chi(\omega^{p^{c_\phi}+1}) = \exp\Big(\frac{2\pi\imath}{m_\phi}\big(p^{c_\phi}+1\big)\Big) = 1.$$

Für ein $x \in {k_\phi}^\times$, $x = \omega^l$, ist

$$N_{k_\phi|k_{c_\phi}}(x) = x \cdot x^{p^{c_\phi}} = \omega^{l(p^{c_\phi}+1)} = \Big(\omega^{p^{c_\phi}+1}\Big)^l.$$

Da die Norm surjektiv ist, folgt

$$k_{c_\phi}^\times = \Big\langle \omega^{p^{c_\phi}+1} \Big\rangle.$$

Es ergibt sich $\chi(u) = 1$ für jedes $u \in k_{c_\phi}^\times$. □

Wir hatten bereits in Abschnitt 2.2.2 die von Weil 1952, in [Wei52], gefundene Produktzerlegung für $P_C(U)$, hergeleitet, (2.23) in Theorem 7, auf Seite 63. An unsere bisherigen Notation angepasst lautet diese folgendermaßen:

Lemma 29 (Theorem 7, nach [Wei52])**.** *Für den Zähler $P_C(U)$ der Zetafunktion $Z(C,U)$ von C gilt die Produktdarstellung*

$$\begin{aligned} P_C(U) \;&=\; \prod_\phi L_\phi(U), \;\; \textit{mit} \\ L_\phi(U) &= 1 + \chi\Big(\big(\gamma^{-1}\delta\big)^{a_0}\big(-\delta\big)^{b_0}\Big)\, j\big(a_0,\, b_0\big)\, U^{d\phi}, \end{aligned} \tag{3.8}$$

mit den Jacobi-Summen

$$j\big(a_0, b_0\big) = \sum_{x+y+1=0} \chi(x)^{a_0}\chi(y)^{b_0}, \qquad \textit{wo } x, y \in {k_\phi}^\times, \tag{3.9}$$

und χ wie in (3.7) definiert.

Der zweite Teil des Beweises von Satz 42 besteht nun darin, (3.8) auf die Form (3.6) zu bringen.

Dabei nutzen wir den engen Zusammenhang zwischen Jacobi-Summen und den gaußschen Summen, die wir Abschnitt 2.1.1 kennengelernt haben,

$$g(r) = \sum_{x \in {k_\phi}^\times} \chi(x)^r \psi(x), \tag{3.10}$$

mit einem fest gewählten nichttrivialen additiven Charakter ψ von k_ϕ^+, wie in Definition 2.1.

Insbesondere gilt nun nach (2.5), auf Seite 41:

$$j\big(a_0,\, b_0\big) = p^{-d_\phi} g\big(a_0\big) g\big(b_0\big) g\big(-a_0 - b_0\big). \tag{3.11}$$

Dieser Ausdruck lässt sich mit dem folgenden Lemma weiter vereinfachen.

Lemma 30. *Sei $K = \mathbb{F}_q$, L eine quadratische Körperweiterung von K und $k = \mathbb{F}_p$ der Primkörper. Sei $\theta : L^\times \to \overline{\mathbb{Q}}^\times$ ein nichttrivialer Charakter, welcher auf $K^\times$ trivial ist, also $\theta(x) = 1$ für alle $x \in K^\times$ $(\subset L^\times)$. Weiterhin sei ψ_L ein nichttrivialer additiver Charakter von L^+, der wie auf Seite 43, in Abschnitt 2.1.3, erläutert, aus einem nichttrivialen additiven Charakter ψ_k von k^+ hervorgeht,*

$$\psi_L(x) = \psi_k\big(\mathrm{Tr}_{L|k}(x)\big), \qquad \text{für alle } x \in L.$$

Dann gilt

$$\sum_{x \in L^\times} \theta(x)\psi_L(x) = \theta(c)\, q,$$

mit einem $c \in L^\times$, für welches $\mathrm{Tr}_{L|K}(c) = 0$. Dieses c hängt nicht von θ ab.

Beweis. Wir zerlegen $L^\times$ in Nebenklassen bezüglich $K^\times$,

$$L^\times = \biguplus_i a_i K^\times, \;\; a_i \in L^\times \backslash K^\times.$$

Da θ auf K konstant 1 ist, erhält man so

$$\sum_{x \in L^\times} \theta(x)\psi_L(x) = \sum_i \theta(a_i) \sum_{y \in K^\times} \psi_L(a_i y).$$

Nun ist aber, da die $a_i K$ additive Gruppen sind,

$$\sum_{y \in K^\times} \psi_L(a_i y) = \sum_{y \in K} \psi_L(a_i y) - 1 = \begin{cases} -1 & \text{für } \psi_L \neq 1 \text{ auf } a_i K \\ q - 1 & \text{für } \psi_L = 1 \text{ auf } a_i K \end{cases}.$$

Nach Voraussetzung ist $\theta \neq 1$ auf $L^\times/K^\times$, also ist

$$\sum_{a_i \in L^\times/K^\times} \theta(a_i) = 0,$$

denn für nichttriviales θ gibt es $a \in L^\times/K^\times$ mit $\theta(a) \neq 1$. Für $T = \sum_{a_i} \theta(a_i)$ gilt dann aber $\theta(a)T = \sum_{a_i} \theta(a \cdot a_i) = T$ und somit $T = 0$, wie schon am Ende des Beweises zu Satz 2.3 erläutert. Zusammen erhält man also

$$\sum_{x \in L^\times} \theta(x)\psi_L(x) = \Big(\sum_{\substack{i \\ \psi_L(a_i K)=0}} \theta\big(a_i\big) \Big) \cdot q, \tag{3.12}$$

es wird dabei nur noch über solche i summiert, für die $\psi_L(a_i K)$ verschwindet. Wir wählen eines dieser a_i aus und setzen $c = a_i$. Nach Definition gilt

$$\psi_L\big(cy\big) = \psi_k\Big(\mathrm{Tr}_{L|k}\big(cy\big)\Big) \text{ sowie}$$
$$\mathrm{Tr}_{L|k}\big(cy\big) = \big(\mathrm{Tr}_{K|k} \circ \mathrm{Tr}_{L|K}\big)\,\big(cy\big),$$

da ψ_k nichttrivial ist, folgt unittelbar

$$\mathrm{Tr}_{L|K}\big(cy\big) = 0.$$

Nun bleibt noch zu zeigen, dass die Summe auf der rechten Seite von (3.12) nur aus dem Summanden $\theta(c)$ besteht.

Annahme: Die Summe enthält zwei verschiedene Summanden $\theta(a_i), \theta(a_j)$ mit $a_i \neq a_j$. Dann ist ψ_L trivial auf $a_iK + a_jK$. Nach Voraussetzung ist ψ_L aber nichttrivialer Charakter auf L, er kann also höchstens auf einer Nebenklasse a_iK konstant den Wert 1 annehmen, weil $a_iK + a_jK = L$ wegen $[L : K] = 2$. Es ergibt sich ein Widerspruch.
Damit ist das Lemma bewiesen. □

Lemma 31. *Für $j(a_0, b_0)$, die Jacobi-Summe aus Lemma 29, gilt*

$$j\big(a_0,\, b_0\big) = p^{c_\phi}.$$

Beweis. Wendet man Lemma 30 mit $L = k_\phi$, $K = k_{c_\phi}$, $\psi_L = \psi$ und $\theta = \chi$ auf die gaußschen Summen (3.10) an, so hat man

$$g(r) = \chi(c)^r p^{c_\phi}, \qquad \text{für } r = a_0,\, b_0,\, -a_0 - b_0.$$

Nun lässt sich (3.11) umformen

$$\begin{aligned} j(a_0, b_0) &= p^{-d_\phi} g(a_0)g(b_0)g(-a_0 - b_0) \\ &= p^{-d_\phi} \chi(c)^{a_0} \chi(c)^{b_0} \chi(c)^{-a_0-b_0} (p^{c_\phi})^3 \\ &= p^{-d_\phi + 3c_\phi} \chi(c^{a_0})\chi(c^{b_0})\chi(c^{-a_0-b_0}) = p^{c_\phi}\chi(c^{a_0+b_0-a_0-b_0}) \\ &= p^{c_\phi}\chi(1) = p^{c_\phi}. \end{aligned}$$

□

Dank dieses Lemmas können wir nun den Beweis von Satz 42 abschließen.

Beweis von Satz 42, 2. Teil. Da $\gamma, \delta \in k = \mathbb{F}_p$ nach Voraussetzung, und χ auf k_{c_ϕ} trivial ist, ergibt sich mit dem vorangegangenen Lemma aus (3.8)

$$L_\phi(U) = 1 + \chi\Big((\gamma^{-1}\delta)^{a_0}(-\delta)^{b_0}\Big)\, j(a_0, b_0)U^{d_\phi} = 1 + p^{c_\phi}U^{d_\phi}.$$

Die Produktzerlegung von $P_C(U)$ hat nun die behauptete Form

$$P_C(U) = \prod_\phi L_\phi = \prod_\phi \big(1 + p^{c_\phi}U^{d_\phi}\big).$$

□

Satz 43 (Folgerung)**.** *Ist C^F die über einem endlichen Körper $k = \mathbb{F}_p$ definierte Kurve aus (3.2), so hat die Zetafunktion $Z\big(C^F, U\big)$ die Form*

$$Z\big(C^F, U\big) = \frac{P_{C^F}(U)}{\big(1-p\big)\big(1-pU\big)} = \frac{\big(1+pU^2\big)^h R(U)}{\big(1-p\big)\big(1-pU\big)}, \tag{3.13}$$

wo h wie in Theorem 8 definiert und $R(U) \in \mathbb{Q}[U]$ ein zu $(1+pU^2)$ teilerfremder Rest ist.

Beweis. Nach den Definitionen von f, $F(t)$ und C^F in Theorem 8 ist in Satz 42 $e = 2$, und f ein Teiler von $p^n + 1$, mit n ungerade. Also teilt $m = \mathrm{kgV}(e, f)$ ebenfalls $p^n + 1$. Nach dem ersten Teil des Beweises von Satz 42 ist $d_\phi = 2\,\mathrm{ggT}(d_\phi, n)$. Damit folgt, da n ungerade, dass $c_\phi = d_\phi/2$ ebenfalls ungerade ist. Dann ist aber jeder der Faktoren in (3.6) durch $1+pU^2$ teilbar,

$$\begin{aligned} P_{C^F}(U) = \quad \prod_\phi L_\phi(U) \qquad\qquad\qquad &= \prod_\phi \big(1 + (pU^2)^{c_\phi}\big) \\ = \prod_\phi \big(1+pU^2\big) \sum_{i=0}^{c_\phi - 1} (-1)^i p^i U^{2i} \quad &= \big(1+pU^2\big)^{\sharp\{\phi\}} R(U), \end{aligned}$$

mit einem zu $1+pU^2$ teilerfremden Rest $R(U)$. Betrachten wir nun die Bedingungen aus (3.5). Da $e = 2$ ist, führt $\phi(\xi)^e = 1$ zu $\phi(\xi) = -1$. $\phi(\eta)$ wiederum ist ungleich 1 und erfüllt $\phi(\eta)^f = 1$. Damit ist für ein ungerades f die Anzahl der ϕ, die (3.5) erfüllen, gleich derjenigen der über k irreduziblen Teiler g von $t^f - 1$, die ungleich $t - 1$ sind. Die weitere Bedingung $\phi(\xi\eta) = -\phi(\eta) \neq -1$ impliziert noch $g \neq t + 1$. Für ungerades f ist dies bereits erfüllt, wegen $\phi(\eta)^f = 1$, für gerades f muss es jedoch zusätzlich berücksichtigt werden. Damit ist $\sharp\{\phi\} = h$ mit h aus Theorem 8. □

3.1.5 Der Rang von E^F

Es gelten die Bezeichnungen aus Theorem 8:

Es ist $k = \mathbb{F}_p$, $p \neq 2$, E eine supersinguläre elliptische Kurve über k,

$$E \,:\, y^2 = x^3 + ax^2 + bx + c, \text{ mit } a, b, c \in k.$$

Zu f mit $f \geq 2$, $f \mid p^n + 1$ für ein ungerades n, ist

$$\begin{aligned} C^F \,:\, s^2 &= F(t), \qquad \text{mit} \\ F(t) &= \gamma t^f + \delta, \qquad \gamma, \delta \in k^\times, \end{aligned}$$

als eine geometrisch irreduzible, nichtsinguläre, projekive hyperelliptische (oder elliptische) Kurve über k definiert. Als Twist von E mit $F(t)$ bezüglich $k(C)$ haben wir die elliptische Kurve E^F über $k(t)$ erhalten,

$$E^F \,:\, y^2 = x^3 + aF(t)x^2 + bF(t)^2x + cF(t)^3. \tag{3.14}$$

Wir wollen den Rang von $E^F\big(k(t)\big)$ ermitteln, und somit den Beweis des Theorems abschließen. Dazu wissen wir bereits

$$\begin{aligned} \operatorname{Rang} E^F\big(k(t)\big) &= \operatorname{Rang} E\big(k(C^F)\big) \quad \text{(Satz 37)} \\ \operatorname{Rang} E\big(k(C^F)\big) &= \operatorname{Rang} \operatorname{Hom}_k\big(J(C^F),\, E\big) \quad \text{(Satz 39).} \end{aligned}$$

Nach Satz 41 benötigen wir die Zähler der Zetafunktionen von C und E, um $\operatorname{Rang} \operatorname{Hom}_k\big(J(C^F),\, E\big)$ zu berechnen. Für C^F wurde dieser schon bestimmt:

$$P_{C^F}(U) = (1 + pU^2)^h R(U), \quad \text{mit } \operatorname{ggT}\big((1 + pU^2), R(U)\big) = 1 \text{ (Satz 43)},$$

mit h wie in Theorem 8. Da E per Definition supersingulär ist, haben wir

$$P_E(U) = 1 + pU^2,$$

nach Korollar 7 auf Seite 32. Also $P_{C^F}(U) = P_E(U)^h R(U)$, damit ist

$$\operatorname{Rang} \operatorname{Hom}_k\big(J(C^F),\, E\big) = 2h,$$

nach Satz 41, denn $1 + pU^2$ irreduzibel über $\mathbb{Q}$. Es ergibt sich

$$\operatorname{Rang} E^F\big(k(t)\big) = 2h,$$

wo h die Anzahl der irreduziblen, normierten Teiler von $t^f - 1$ ist, die ungleich $t - 1$ und für gerades f zusätzlich ungleich $t^f + 1$ sind. Damit ist der Beweis von Theorem 8 abgeschlossen.

3.1.6 Die normierten irreduziblen Teiler des Polynoms $t^f - 1$

In dem Beweis des sich an Theorem 8 anschließenden Korollars 15 wurde folgende Aussage benötigt:
Ist n eine ungerade Primzahl, so gilt

$$f = p^n + 1 \implies h = \frac{p^n - p}{2n} + \frac{p-1}{2}.$$

Dies ergibt sich unmittelbar aus dem nachfolgenden Lemma.

Lemma 32. *Sind p und n ungerade Primzahlen, so hat das Polynom*

$$F(t) = t^{p^n+1} - 1$$

genau

$$\frac{p^n - p}{2n} + \frac{p-1}{2} + 2$$

normierte irreduzible Teiler. Davon sind genau

- $\frac{p^n-p}{2n}$ *vom Grad* $2n$,
- $\frac{p-1}{2}$ *vom Grad* 2,
- 2 *vom Grad 1, nämlich* $t-1$ *und* $t+1$.

Für den Beweis brauchen wir zunächst ein weiteres, allgemeineres Lemma.

Lemma. *Ist $F(t)$ ein normiertes, separables Polynom aus $\mathbb{F}_p[t]$, so ist die Anzahl der normierten, irreduziblen Teiler vom Grad d von $F(t)$ genau*

$$\frac{1}{d} \sharp \left\{ \alpha \in \overline{\mathbb{F}}_p \,:\, F(\alpha) = 0, \alpha \in \mathbb{F}_{p^d},\ \textit{aber } \alpha \notin \mathbb{F}_{p^m} \textit{ für } m < d \right\}$$

Beweis. Ist $\alpha \in \overline{\mathbb{F}}_p$, schreiben wir

$$G = \mathrm{Gal}\big(\mathbb{F}_p(\alpha) \mid \mathbb{F}_p\big)$$

sowie

$$B(\alpha) = \{\alpha^\sigma \,:\, \sigma \in G\}$$

für die Bahn von α unter G. Da G durch den Frobenius-Automorphismus $x \mapsto x^p$ erzeugt wird, gilt $B(\alpha) = \{\alpha^{p^i} \,:\, i = 0, 1, \dots\}$. Dann ist

$$\prod_{\sigma \in G} \big(t - \alpha^\sigma\big) = \prod_i \big(t - \alpha^{p^i}\big)$$

ein normiertes, über $\mathbb{F}_p$ irreduzibles Polynom aus $\mathbb{F}_p[t]$.

Hat man umgekehrt ein irreduzibles normiertes Polynom $g(t) \in \mathbb{F}_p[t]$, mit einer Nullstelle $\alpha \in \overline{\mathbb{F}}_p$, so gilt

$$g(t) = \prod_{\beta \in B(\alpha)} \big(t - \beta\big).$$

Für $d = \operatorname{grad} g(t)$ gilt

$$d = \sharp B(\alpha) = \big[\mathbb{F}_p(\alpha) : \mathbb{F}_p\big], \qquad \text{also } \mathbb{F}_p(\alpha) = \mathbb{F}_{p^d}.$$

Wir definieren nun

$$L = \big\{\alpha \in \overline{\mathbb{F}}_p \,:\, F(\alpha) = 0\big\}.$$

Da $F(x)$ als separabel vorausgesetzt wurde, gilt

$$F(t) = \prod_{\alpha \in L} \big(t - \alpha\big).$$

Haben wir eine Zerlegung von $F(t)$ in normierte irreduzible Faktoren $F_i(t)$,

$$F(t) = F_1(t)F_2(t)F_3(t) \cdots F_r(t),$$

und ist $\alpha_i \in \overline{\mathbb{F}}_p$ eine Nullstelle von $F_i(t)$, so gilt

$$F_i(t) = \prod_{\alpha \in B(\alpha_i)} \big(t - \alpha\big) \qquad \text{und } d_i = \operatorname{grad} F_i(t) = \big[\mathbb{F}_p(\alpha_i) \,:\, \mathbb{F}_p\big].$$

Außerdem ist $B(\alpha_i) \subset \mathbb{F}_p(\alpha_i)$, aber $B(\alpha_i) \cap \mathbb{F}_{p^m} = \emptyset$ für jedes $m < d_i$.

Wir definieren jetzt für $d \in \mathbb{N}$

$$L(d) = \big\{\alpha \in L \,:\, \alpha \in \mathbb{F}_{p^d},\, \alpha \notin \mathbb{F}_{p^m} \text{ für } m < d\big\}.$$

Nach dem bisher Gesagten ist klar, dass $L(d)$ genau aus den Nullstellen der Polynome $F_i(x)$ mit $d_i = d$ besteht, also

$$L_d = \bigcup \{B(\alpha_i) \,:\, \operatorname{grad} F_i(t) = d\}.$$

Folglich gilt

$$\sharp L(d) = d \cdot \sharp \,\{i \,:\, \operatorname{grad} F_i(t) = d\},$$

also $\sharp L(d)$ ist die Anzahl der irreduziblen Teiler von $F(t)$ vom Grad d. $\square$

Beweis von Lemma 32. Das Polynom $F(t)$ ist separabel, wie man sofort an $F'(t) = t^{p^n}$ sieht. Wie im vorangegangen Beweis definieren wir

$$L = \left\{\alpha \in \overline{\mathbb{F}}_p \,:\, F(\alpha) = 0\right\} = \left\{\alpha \in \overline{\mathbb{F}}_p \,:\, \alpha^{p^{n+1}} = 1\right\}.$$

Für ein $\alpha \in L$ gilt

$$\alpha^{p^{2n}} = \alpha \cdot \alpha^{p^{2n}-1} = \alpha \cdot \left(\alpha^{p^n+1}\right)^{p^n-1} = \alpha \cdot 1 = \alpha,$$

es ergibt sich also $\alpha \in \mathbb{F}_{p^{2n}}$ und somit $L \subset \mathbb{F}_{p^{2n}}$.

Nach Voraussetzung ist n eine ungerade Primzahl, das heißt, die einzigen Teiler von $2n$ sind $1, 2, n$ und $2n$, also hat $\mathbb{F}_{p^{2n}}$ genau die folgenden Teilkörper:

$$\mathbb{F}_p,\ \mathbb{F}_{p^2},\ \mathbb{F}_{p^n},\ \mathbb{F}_{p^{2n}}.$$

Da eine Bijektion zwischen den Bahnen $B(\alpha)$ von $\alpha \in L$ unter Galois-Operation und den normierten irreduziblen Teilern von $F(t)$ besteht, müssen wir jetzt untersuchen, wie sich die Elemente von L auf die Teilkörper von $\mathbb{F}_{p^{2n}}$ verteilen:

- Was ist $\mathbb{F}_p \cap L$?
  Für $\alpha \in \overline{\mathbb{F}}_p$ gilt:

  $$\begin{aligned} \alpha \in \mathbb{F}_p \cap L &\iff \alpha^p = \alpha \text{ und } \alpha^{p^n+1} = 1 \\ &\iff \alpha^p = \alpha \text{ und } \alpha^2 = 1 \\ &\iff \alpha = \pm 1 \end{aligned}$$

  Also ist

  $$\mathbb{F}_p \cap L = \left\{-1,\, +1\right\}$$

  und somit sind $t+1$ und $t-1$ die einzigen Teiler von $F(t)$ vom Grad 1.

- $L \cap \mathbb{F}_{p^2}$:
  Für $\alpha \in \overline{\mathbb{F}}_p$, so gilt:

  $$\begin{aligned} \alpha \in \mathbb{F}_{p^2} \cap L &\iff \alpha^{p^2} = \alpha \text{ und } \alpha^{p^n+1} = 1 \\ &\iff \alpha^{p^2-1} = 1 \text{ und } \alpha^{p^n+1} = 1 \\ &\iff \alpha^{\mathrm{ggT}(p^2-1,\, p^n+1)} = 1 \iff \alpha^{p+1} = 1, \end{aligned}$$

  wobei die Hilfsaussage $\mathrm{ggT}(p^2-1,\, p^n+1) = p+1$ angewendet wurde, die wir im Anschluss beweisen werden. Damit ist

  $$L \cap \mathbb{F}_{p^2} = \left\{\alpha \,:\, \alpha^{p+1}\right\}$$

und es ergibt sich

$$\sharp\,(L \cap \mathbb{F}_{p^2}) = p+2 \implies \sharp\,(L \cap \mathbb{F}_{p^2} \backslash \mathbb{F}_p) = p-1,$$

da $+1, -1$ schon in $\mathbb{F}_p$ liegen. Mit dem vorangegangen Lemma gibt es also genau $\frac{p-1}{2}$ irreduzible normierte quadratische Teiler von $F(t)$.

- $L \cap \mathbb{F}_{p^n}$:
  Für $\alpha \in \overline{\mathbb{F}}_p$ hat man:

$$\begin{aligned} \alpha \in \mathbb{F}_{p^n} \cap L &\iff \alpha^{p^n} = \alpha \text{ und } \alpha^{p^n+1} = 1 \\ &\iff \alpha^{p^n} = \alpha \text{ und } \alpha^2 = 1 \\ &\iff \alpha = \pm 1. \end{aligned}$$

  Also ist $L \cap \mathbb{F}_{p^n} = \{\pm 1\}$ und

$$L \cap \big(\mathbb{F}_{p^n} \backslash \mathbb{F}_p\big) = \emptyset.$$

- Wir können L folgendermaßen zerlegen:

$$\begin{aligned} L = L \cap \mathbb{F}_{p^{2n}} = \Big(L \cap \mathbb{F}_p\Big) &\cup \Big(L \cap \big(\mathbb{F}_{p^2} \backslash \mathbb{F}_p\big)\Big) \\ &\cup \Big(L \cap \big(\mathbb{F}_{p^n} \backslash \mathbb{F}_p\big)\Big) \cup \Big(L \cap \big(\mathbb{F}_{p^{2n}} \backslash \big(\mathbb{F}_{p^2} \cup \mathbb{F}_{p^n}\big)\big)\Big). \end{aligned}$$

  Die Menge L hat p^n+1 Elemente, da sie über die Bedingung $\alpha^{p^n+1} = 1$ definiert ist. Setzt man dies mit den bisherigen Ergebnissen zusammen, so folgt

$$\sharp\, L \cap \big(\mathbb{F}_{p^{2n}} \backslash \big(\mathbb{F}_{p^2} \cup \mathbb{F}_{p^n}\big)\big) = \big(p^n+1\big) - \big(p+1\big).$$

  Eine Konjugationsklasse unter der Operation von $\mathrm{Gal}(\mathbb{F}_{p^{2n}} \mid \mathbb{F}_p)$ umfasst $2n$ Elemente, und somit gibt es genau

$$\frac{p^n - p}{2n}$$

  normierte irreduzible Teiler von $t^{p^n+1} - 1$ vom Grad $2n$.

Hilfsaussage: Sind p, n ungerade Primzahlen, so gilt

$$\mathrm{ggT}\big(p^2-1,\, p^n+1\big) = p+1.$$

Beweis: Bekanntlich ist

$$\begin{aligned} p^2 - 1 &= \big(p+1\big)\big(p-1\big), \\ p^n + 1 &= \big(p+1\big)\big((-p)^{n-1} + (-p)^{n-2} + \ldots + (-p) + 1\big), \end{aligned}$$

also

$$\begin{aligned}\operatorname{ggT}\big(p^2-1,\, p^n+1\big) = \\ \big(p+1\big)\operatorname{ggT}\big(p-1,\, (-p)^{n-1}+(-p)^{n-2}+\ldots+(-p)+1\big).\end{aligned}$$

Dies ist gerade gleich $p+1$, denn aus $d \mid p-1$ folgt $p \equiv 1 \bmod d$, was aber wegen n ungerade

$$0 \not\equiv (-p)^{n-1}+\ldots+(-p)+1 \equiv (-1)^{n-1}+\ldots+(-1)+1 \equiv 1 \bmod d$$

impliziert. □

3.2 Konstruktionen mit nicht konstanter j-Invariante

Ein Grundmerkmal der in Abschnitt 3.1 dargestellten Konstruktion von Tate und Shafarevich ist die Verwendung quadratischer Twists. Eine Folge daraus ist, dass die so gewonnen Kurven E^F alle dieselbe j-Invariante wie die Ausgangskurve E aufweisen. Insbesondere ist $j \in \mathbb{F}_p$, und die so gebildeten Kurven sind alle isotrivial, vgl. Lemma 25, auf Seite 69 sowie Bemerkung 20. Man kann nun die Frage stellen: Ist es auch möglich, Familien von elliptischen Kurven asymptotisch beliebig hohen Ranges über $\mathbb{F}_p(t)$ zu konstruieren, deren j-Invarianten nicht in $\mathbb{F}_p$ liegen, also keine Konstanten sind?

3.2.1 Die Konstruktion von Shioda

Eine erste Annäherung an diese Frage geschieht durch Tetsui Shioda in [Shi86]. Wie bereits aus dem Titel „An explicit algorithm for computing the Picard number of certain algebraic surfaces“ ersichtlich, liegt Shiodas Interesse hier nicht unmittelbar auf den elliptischen Kurven sondern auf der Theorie algebraischer Flächen. Die elliptischen Kurven dienen ihm nur als Beispiel für die Anwendung seiner allgemeineren Resultate. Entsprechend sind seine Methoden sehr verschieden von den bislang von uns behandelten, und eine detaillierte Darstellung würde den gegebenen Rahmen dieser Diplomarbeit übersteigen. Wir werden uns deshalb auf einige Bemerkungen und das Zitieren seiner wesentlichen Ergebnisse beschränken.

Picard- und Lefschetz-Zahl Sei X eine nichtsinguläre projektive Varietät über einem algebraisch abgeschlossenen Körper k. Die *Picard-Zahl*, die

wir mit $\rho(X)$ bezeichnen wollen, stellt eine wichtige geometrische Invariante von X dar. Sie lässt sich definieren durch

$$\rho\big(X\big) = \operatorname{Rang} \mathrm{NS}(X) = \operatorname{Rang}\left(Pic(X)/Pic^0(X)\right), \tag{3.15}$$

wo $\mathrm{NS}(X)$ die sogenannte *Néron-Severi Gruppe* von X durch $Pic(X)/Pic^0(X)$ definiert ist, siehe z.B. [Har77], S. 140. Für die Theorie algebraischer Flächen ist es von großem Interesse, deren Picard-Zahlen berechnen zu können.

Die *Lefschetz-Zahl*, $\lambda(X)$, einer Fläche X ist, im Gegensatz etwa zu $\rho(X)$, eine birationale Invariante der Fläche, für die immer $\lambda(X) \geq 0$ gilt. Sie ist eng mit der Picard-Zahl verbunden, genauer gilt die Beziehung

$$\lambda(X) = b_2(X) - \rho(X), \tag{3.16}$$

mit der 2ten Betti-Zahl $b_2(X)$, welche ebenfalls keine birationale Invariante ist. Als birationale Invariante ist $\lambda(X)$ invariant unter Aufblasungen und kann somit auch für Flächen betrachtet werden, welche nicht als minimales, nichtsinguläres Modell vorliegen. Zum Zusammenhang zwischen $\lambda(X)$ und $\rho(X)$ in Charakteristik p, siehe etwa [Zar71], S. 122.

Shiodas wichtigstes Ergebnis in [Shi86] stellt ein Verfahren dar, durch das die Lefschetz- und damit mittels (3.16) auch die Picard-Zahl von sogenannten Delsarte-Flächen berechnet werden kann.

Delsarte-Flächen

Definition 27. Eine *Delsarte-Fläche* im Sinne Shiodas ist eine algebraische Fläche $X_A \subset \mathbb{P}^3_k$, welche durch eine Gleichung der Form

$$X_A : \sum_{i=0}^{3} b_i x_0^{a_{i0}} x_1^{a_{i1}} x_2^{a_{i2}} x_3^{a_{i3}} = 0, \tag{3.17}$$

mit Koeffizienten $b_i \in k^\times$, $i = 0, \ldots, 3$, gegeben ist, wobei die Exponenten a_{ij}, $i, j = 0, \ldots, 3$, eine Matrix $A \in \mathrm{Mat}(4 \times 4, \mathbb{Z})$ bilden, die den folgenden Bedingungen genügt:

$$\begin{gathered} \det(A) \neq 0 \text{ in } k \\ \sum_{j=0}^{3} a_{0j} = \cdots = \sum_{j=0}^{3} a_{3j} \\ \text{für jedes } j \text{ gibt es ein } i \text{ mit } a_{ij} = 0. \end{gathered} \tag{3.18}$$

Bemerkung 23. Der Name Delsarte-Fläche rührt daher, dass J. Delsarte 1951, in [Del51], für einen recht allgemeinen Typ von Varietäten Bedingungen aufgestellt hatte, welche für Flächen in $\mathbb{P}^3_k$ zu (3.18) äquivalent sind, unter denen sich der Beweis der Weil-Vermutungen auf ein, im allgemeinen jedoch kaum zugängliches, kombinatorisches Problem reduzieren lässt.

Shiodas Algorithmus für die Picard-Zahl

Im Folgenden sei k ein algebraisch abgeschlossener Körper und X_A eine Delsartefläche mit Exponentenmatrix $A = (a_{ij})$. Um das Hauptergebnis Shiodas formulieren zu können, müssen wir etwas Notation festlegen:

Wir bezeichnen mit A^* die komplementäre Matrix zu A, also die Matrix mit $A \cdot A^* = \det(A)\,\mathbf{1}_4$. Seien nun δ, d und B definiert durch

$$\delta = \mathrm{ggT}(a^*_{ij}),\ d = \frac{|\det(A)|}{\delta} \ \text{ und } \ B = dA^{-1} = \pm\delta^{-1}A^*,$$

und weiterhin seien M_d und $L_A \subset M_d$ die $(\mathbb{Z}/d\mathbb{Z})$-Moduln

$$M_d = \big\{(a_0,a_1,a_2,a_3) \in (\mathbb{Z}/d\mathbb{Z}) \,:\, a_0 + \cdots + a_3 \equiv 0 \bmod d\big\},$$
$$L_A = \big\{(a_0,a_1,a_2,a_3)B \,:\, (a_0,a_1,a_2,a_3) \in M_d\big\}.$$

Wir definieren nun die Mengen $\mathfrak{U}^n_m$, $\mathfrak{B}^n_m(p)$, für $n, m \in \mathbb{Z}$, m prim zu $char(k)$, $p = char(k) \geq 0$, welche in der Theorie der Fermatflächen eine wichtige Rolle spielen:

$$\mathfrak{U}^n_m = \Big\{(a_0,\ldots,a_{n+2}) \in \mathbb{Z}^{n+2} \,:\, 0 < a_i < m, \sum_{i=0}^{n+1} a_i \equiv 0 \bmod m\Big\}$$

$$\mathfrak{B}^n_m(0) = \Big\{(a_0,\ldots,a_{n+2}) \in \mathfrak{U}^n_m \,:\, \sum_{i=0}^{n+1}\Big\langle\frac{ta_i}{m}\Big\rangle = \frac{n}{2}+1,\ \forall t,\ \mathrm{ggT}(t,m)=1\Big\}$$

$$\mathfrak{B}^n_m(p) = \Big\{(a_i) \in \mathfrak{U}^n_m \,:\, \sum_{i=0}^{n+1}\sum_{j=0}^{f-1}\Big\langle\frac{tp^j a_i}{m}\Big\rangle = (\frac{n}{2}+1)f,\ \forall t,\ \mathrm{ggT}(t,m)=1\Big\},$$

wo $f = \mathrm{ord}_{(\mathbb{Z}/d\mathbb{Z})^\times}(p)$ gesetzt wurde, und $\langle x\rangle = x - \lfloor x\rfloor$ den gebrochenen Anteil einer rationalen Zahl x bezeichnet.

Im Folgenden benötigen wir die Mengen $\mathfrak{U}^n_m$, $\mathfrak{B}^n_m$ nur für $n = 2$, in diesem Fall bezeichnet man die Elemente von $\mathfrak{B}^2_m$ als *Fermatquadrupel*, und sonst, im allgemeinen, die von $\mathfrak{B}^{k-2}_m$ als *Fermat-k-tupel*. Wir führen noch eine weitere Bezeichnung ein,

$$\mathfrak{T}^2_d(p) = \mathfrak{U}^2_d - \mathfrak{B}^2_d(p), \ \text{ für } p = 0 \text{ oder } p \text{ prim},$$

und können nun das Hauptergebnis Shiodas formulieren:

Satz 44. *Für die Lefschetz-Zahl der Delsarte-Fläche X_A über dem Grundkörper k, mit $p = char(k) \geq 0$, gilt:*

$$\lambda(X_A) = \sharp\big(\mathfrak{T}^2_d(p) \cap L_A\big). \tag{3.19}$$

Haben wir ein nichtsinguläres projektives Modell X von X_A vorliegen, so ist die Picard-Zahl $\rho(X)$ definiert, und wir erhalten aus (3.16):

Korollar 17. *Ist $b_2(X)$ die 2.te Betti-Zahl von X, so gilt für die Picard-Zahl $\rho(X)$:*

$$\rho(X) = b_2(X) - \sharp\big(\mathfrak{T}_d^2(p) \cap L_A\big).$$

Bemerkung 24. Die Methode hinter dem Beweis von SHIODAS Hauptsatz besteht darin, die Kohomologiegruppen der Delsartefläche X_A mit denen einer Fermatfläche X_d,

$$X_d \,:\, x_0^d + x_1^d + x_2^d + x_3^d = 0,$$

mit d wie oben aus A berechnet, in Beziehung zu setzen, wobei für $char(k) = 0$ die klassischen Kohomologiegruppen über $\mathbb{C}$, und für $char(k) > 0$ die l-adischen Kohomologiegruppen zu eine Primzahl $l \neq char(k)$ zur Anwendung kommen. Die Geometrie der Fermatflächen wiederum war zu diesem Zeitpunkt bereits sehr intensiv studiert worden.

Für die Anwendung auf elliptische Kurven von Funktionenkörpern in Charakteristik $\neq 0$ ist das folgende Korollar entscheidend

Korollar 18. *Ist X_A eine Delsarte-Fläche über dem Körper k mit $char(k) = p > 0$ und ist $p^\nu \equiv -1 \bmod d$ für ein ganzzahliges $\nu > 0$, so gilt*

$$\lambda(X_A) = 0. \tag{3.20}$$

Bemerkung 25. Eine Fläche X, für die $\lambda(X) = 0$, wird auch als *supersingulär* bezeichnet, was nicht mit dem Begriff "supersingulär" als Gegenteil von "gewöhnlich" für elliptische Kurven nach Definition 13 auf Seite 17 verwechselt werden sollte.

Beweis zu Korollar 18. Es gelte $p^\nu \equiv 1 \bmod d$, und sei $f = \mathrm{ord}_{(\mathbb{Z}/d\mathbb{Z})^\times}(p)$. Ohne Einschränkung gilt $\nu < f$, sonst betrachte $\nu \bmod f$. Sei t teilerfremd zu f und $a \not\equiv 0 \bmod d$. Dann

$$0 \not\equiv p^j at \equiv -p^{j+\nu} at \mod d \;\Rightarrow\; 0 \neq p^j at + p^{j+v} at \equiv 0 \mod d$$
$$\Rightarrow \langle \frac{p^j at}{d} \rangle + \langle \frac{p^{j+\nu} at}{d} \rangle = 1.$$

Aus $p^{2\nu} \equiv p^f \equiv 1 \bmod d$ ergibt sich $2\nu = f$, damit erhält man

$$\sum_{i=0}^{3} \sum_{j=1}^{f} \langle \frac{p^j a_i t}{d} \rangle = \sum_{i=0}^{3} \sum_{j=1}^{f/2} \langle \frac{p^j a_i t}{d} \rangle + \sum_{j=1}^{f/2} \langle \frac{p^{j+\nu} a_i t}{d} \rangle = \sum_{i=0}^{3} \sum_{j=1}^{f/2} 1 = 2f,$$

für alle t mit $\mathrm{ggT}(t, d) = 1$ und alle $(a_0, \ldots, a_3) \in \mathfrak{U}_d^2$. Also $\mathfrak{B}_d^2 = \mathfrak{U}_d^2$ nach Definition, woraus die Behauptung folgt. □

Anwendung auf elliptische Kurven

SHIODA wendet nun seine Methode auf eine Reihe von Beispielen an. Die für uns wichtigsten sind die, in denen er sich mit elliptischen Flächen befasst. Wir geben kurz eine Definition dieses Begriffs (vgl. [Sil94], S. 202):

Definition 28. Sei C eine nichtsinguläre projektive Kurve über einem Körper k. Eine elliptische Fläche über C besteht aus

1. einer Fläche $\mathcal{E}$,
2. einem Morphismus $\pi : \mathcal{E} \to C$, so, dass die Faser $\mathcal{E}_t = \pi^{-1}(t)$ für alle bis auf endlich viele Punkte $t \in C(\bar{k})$ eine nichtsinguläre Kurve vom Geschlecht 1 ist,
3. einem Schnitt von π, $\sigma_0 : C \to \mathcal{E}$.

Wir wollen die Theorie elliptischer Flächen nicht vertiefen, die nötigen Grundlagen vermittelt z.B. [Sil94] in Chapter III, ab Seite 187, insbesondere wird dort auch der Algorithmus von TATE behandelt, der es ermöglicht, ein minimales Modell einer elliptischen Fläche zu erhalten, das *Néron-Modell* oder auch *Néron-Kodaira Modell*.

Wir begnügen uns mit der Feststellung, dass jeder elliptischen Kurve über einem Funktionenkörper $k(t)$ eine elliptische Fläche $\mathcal{E}$ über der Kurve $C = \mathbb{P}^1_k$ über k, zugeordnet werden kann, deren generische Faser wieder E über $k(t)$ ist.

SHIODA studiert nun elliptische Kurven, welche durch eine affine Weierstraßgleichung der folgenden Form, über $k(t)$ gegeben sind:

$$E : y^2 = x^2 + at^n x + bt^m, \qquad a, b \in k,\ ab \neq 0,\ n, m \in \mathbb{Z}, \tag{3.21}$$

wobei vorausgesetzt ist, dass k algebraisch abgeschlossen ist. Für das minimale Modell $\tilde{\mathcal{E}}$ der dieser Kurve zugeordneten elliptischen Fläche über $\mathbb{P}^1_k$, benutzt er Methoden, welche man beispielsweise in [Sil86] Ch. X, S. 358f bzw. in [Sil94], Ch. III nachlesen kann, um die geometrischen Invarianten der Fläche zu untersuchen. Er wendet dann noch die sogenannte *Shioda-Tate Formel*,

$$\operatorname{Rang} E\big(\bar{k}(t)\big) = \lambda(\tilde{\mathcal{E}}) - 2 - \sum_{\nu}(n_\nu - 1),$$

an, welche einen Zusammenhang herstellt zwischen dem Rang der elliptischen Kurve, der Lefschetz-Zahl der zugehörigen elliptischen Fläche sowie der Anzahl der Komponenten n_ν der Fasern der endlich vielen Punkte t_ν, für die $\tilde{\mathcal{E}}_t$ aus der obigen Definition keine nichtsinguläre Kurve ist, siehe [Shi72],

[Tat66b], ein recht lesbarer Beweis findet sich auch in [MP86]. Schließlich erhält er dann:

$$\lambda(\tilde{\mathcal{E}}) = D - \operatorname{Rang} E\big(\bar{k}(t)\big) - \begin{cases} 4 & \text{falls } \epsilon_0 = \epsilon_\infty = 0 \\ 2 & \text{falls } \epsilon_0 + \epsilon_\infty > 0,\ \epsilon_0\epsilon_\infty = 0 \\ 0 & \text{falls } \epsilon_0,\ \epsilon_\infty > 0, \end{cases} \tag{3.22}$$

wobei $D = |2m-3n|$, ϵ_0 der kleinste nichtnegative Rest $\bmod 12$ von $\min(2m, 2n)$ und ϵ_∞ der kleinste nichtnegative Rest von $-\max(2m, 2n) \bmod 12$ sind. (Diese Größen hatten sich aus der Betrachtung der singulären Fasern von $\tilde{\mathcal{E}}$ ergeben.)

Theorem 9. *Sei $k = \mathbb{F}_p$, mit $p \equiv -1 \bmod 4$, und $\bar{k}$ der algebraische Abschluss von k. Bezeichne E_N für $N \in \mathbb{N}$, N ungerade und > 0, die elliptische Kurve über $k(t)$ mit der (affinen) Weierstraßgleichung*

$$E_N \,:\, y^2 = x^3 + c + t^{\frac{p^N+1}{2}},$$

so hat diese über $\bar{k}$ den Rang

$$\operatorname{Rang} E_N\big(\bar{k}(t)\big) = p^N - \begin{cases} 1 \\ 3 \end{cases}, \qquad p \equiv \begin{cases} 1 \\ -1 \end{cases} \mod 3.$$

Insbesondere wird also der Rang über $\bar{k}(t)$ in der Familie $\{E_N \,:\, N = 1, 3, \dots\}$ asymptotisch beliebig hoch.

Bemerkung 26. Laut Ulmer, [Ul02], S. 297, ist

$$E_N\big(\mathbb{F}_{p^{2N}}(t)\big) = E_N\big(\bar{k}(t)\big),$$

mit anderen Worten, E_N erreicht bereits nach einer endlichen algebraischen Körpererweiterung maximalen Rang. Es lässt sich sogar zeigen, dass der Rang von $E_N\big(k(t)\big)$ mit $N \to \infty$ ebenfalls gegen unendlich strebt.

Beweis. Wir setzen $m = \frac{p^N+1}{2}$. Die projektive Form der Gleichung von E_N, aufgefasst als Fläche $\mathcal{E}_N$ über k, ist

$$Z^{m-2}Y^2 - Z^{m-3}X^3 - XZ^{m-1} - T^m = 0,$$

mit den projektiven Koordinaten

$$\big(Z \,:\, X \,:\, Y \,:\, T\big) = \big(x_0 : x_1 : x_2 : x_3\big).$$

Man sieht, dass $\mathcal{E}_N$ sich somit als Delsarte-Fläche zur Matrix

$$A = \begin{pmatrix} m-2 & 0 & 2 & 0 \\ m-3 & 3 & 0 & 0 \\ m-1 & 1 & 0 & 0 \\ 0 & 0 & 0 & m \end{pmatrix}$$

auffassen lässt. Wir wollen die Lefschetz-Zahl dieser Fläche bestimmen, wozu wir das Néron-Modell von $\mathcal{E}_N$ nicht zu kennen brauchen. Man berechnet leicht

$$A^* = \begin{pmatrix} 0 & 0 & -2m^2 & 0 \\ -2m & 2m(m-1) & m(m-2) & 0 \\ -6m & -2m(m-3) & 3m(m-2) & 0 \\ 0 & 0 & 0 & -4m \end{pmatrix},$$

$$\delta = \mathrm{ggT}(a_{ij}^*) = m,\ \det(A) = -4m,\ d = \delta^{-1}\,|\det(A)| = 4.$$

Da nach Voraussetzung $p \equiv -1 \bmod 4$, also $p \equiv -1 \bmod d$, folgt nach Korollar 18, dass $\lambda(\mathcal{E}_N) = 0$. Sei nun $\tilde{\mathcal{E}}_N$ das Néron-Modell von $\mathcal{E}_N$. Da die Weierstraßgleichung von E_N vom obigen Typ (3.21) ist, mit $a = b = 1$, $n = 0$ und $m = m$, können wir (3.22) anwenden. Wir müssen dazu lediglich noch ϵ_0, ϵ_∞ berechnen:

$$\begin{aligned} \epsilon_0 &= \min(2m, 0) \bmod 12 = 0 \\ \epsilon_\infty &= -\max(2m, 0) \bmod 12 = -(p^N + 1) \bmod 12. \end{aligned}$$

Somit erhalten wir

$$\mathrm{Rang}\, E_N\big(\bar{k}(t)\big) = p^N + 1 - \begin{cases} 4 & p \equiv -1 \bmod 3 \\ 2 & p \equiv 1 \bmod 3 \end{cases}.$$

□

Mit Ausnahme von Korollar 18 war die gesamte Theorie in diesem Abschnitt, einschließlich der hier nur angedeuteten Untersuchung elliptischer Flächen, so aufgebaut, dass immer auch $char(k) = 0$ zugelassen war. Die Hoffnung, eventuell in der Familie E_N oder einer anderen Familie elliptischer Kurven des Typs (3.21) ein Beispiel für das Auftreten beliebig hohen Ranges in Charakteristik 0 zu finden, scheint sich jedoch nicht zu bewahrheiten, zumindest gilt:

Satz 45 (vgl. [Shi86], Cor. 9)**.** *Sei k ein algebraisch abgeschlossener Körper mit $char(k) = 0$, E eine elliptische Kurve über $k(t)$, mit einer Weierstraßgleichung des Typs*

$$E\ :\ y^2 = x^3 + at^n x + bt^m,$$
$$a, b \in k, ab \neq 0,\ n, m \in \mathbb{Z}\ \textit{und}\ 2m \neq 3n.$$

Dann ist

$$\operatorname{Rang} E\big(\bar{k}(t)\big) \leq 56,$$

mit Gleichheit genau dann, wenn $m \equiv 0 \bmod 2$ *und* $2m \equiv 3n \bmod 2^3 \cdot 3^2 \cdot 5 \cdot 7$.

3.2.2 Die Konstruktion von Ulmer

Die Ideen Shiodas liefern, zumindest in der ursprünglichen Form, nur über $\overline{\mathbb{F}}_p(t)$ Familien elliptischer Kurven mit asymptotisch beliebig hohem Rang, und auch dies nur für $p \equiv -1 \bmod 4$. In [Ul02] baut jedoch Douglas Ulmer die Methode Shiodas aus, eine Beziehung zwischen einer elliptischen Fläche und einer geeigneten Fermatfläche auszunutzen, um zu einer Konstruktion zu gelangen, die für jedes p, sogar für $p = 2$, eine Familie elliptischer Kurven liefert, deren Rang bereits über $\mathbb{F}_p(t)$ asymptotisch unbeschränkt ist.

Sein Hauptresultat ist der folgende Satz:

Theorem 10. *Sei* $k = \mathbb{F}_p$*, mit* p *einer beliebigen Primzahl, und* $\bar{k}$ *dessen algebraischer Abschluss, sowie* $k(t)$ *der rationale Funktionenkörper in einer Variablen über* k*. Sei weiterhin* E *die über* $k(t)$ *durch die Weierstraßgleichung*

$$E : y^2 + xy = x^3 - t^d, \text{ wo } d = p^n + 1,\ n > 0,$$

definierte elliptische Kurve, dann gilt:

1. *Die* j*-Invariante* $j(E)$ *ist nicht konstant, genauer*

$$j(E) = t^{-d}\big(1 - 2^4 \cdot 3^3 \cdot t^d\big)^{-1} \big(\notin k\big).$$

2. *Für den Rang der Mordell-Weil-Gruppe von* E *über* $k(t)$ *gilt*

$$\operatorname{Rang} E\big(k(t)\big) \geq \frac{p^n - 1}{2n},$$

und

$$\operatorname{Rang} E\big(k(t)\big) \leq \operatorname{Rang} E\big(\mathbb{F}_{p^{2n}}(t)\big) = \operatorname{Rang} E\big(\bar{k}(t)\big) = \begin{cases} p^n & : 6 \nmid d \\ p^n - 2 & : 6 \mid d. \end{cases}$$

Bemerkung 27. Ulmer zeigt außerdem, dass die Vermutung von Birch und Swinnerton-Dyer für E gilt, und zwar über jedem $\mathbb{F}_q(t)$ für $q = p^m$, $m \geq 1$.

Korollar 19. *Für die Familie elliptischer Kurven* $\{E_n : n = 1, 2, 3, \dots\}$, *über* $\mathbb{F}_p(t)$, *mit*

$$E_n : y^2 + yx = x^3 - t^{p^n+1},$$

gilt

$$\lim_{n\to\infty} \operatorname{Rang} E_n\big(\mathbb{F}_p(t)\big) \to \infty.$$

Ähnlich wie schon vorher, Satz 45, stellt sich auch in diesem Fall heraus, dass der Rang von Kurven des Typs E_n über $\mathbb{Q}(t)$ und sogar über $\overline{\mathbb{Q}}(t)$ absolut beschränkt ist, vgl. [Ul02], Rem. 1.6.

Literaturverzeichnis

[BDS04] I. Bouw, C. Diem, J. Scholten. *Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j-invariant*, Manuscripta Mathematica **114**, (2004), 487-501

[DS05] C. Diem, J. Scholten. *Ordinary elliptic curves of high rank over $\overline{\mathbb{F}}_p(x)$ with constant j-invariant II*, preprint (2005)

[DH35] H. Davenport, H. Hasse. J. Reine Angew. Mathematik, vol. **172** (1935), 151-182

[Deu41] Max Deuring. *Die Typen der Multiplikatorringe elliptischer Funktionenkörper*. Abh. Math. Sem. Hamburg **14** (1941), 197-272

[Del51] J. Delsarte. *Nombres des solutions des équation polynomiales sur un corps fini*, Sem. Bourbaki No. **39**, (1951) 1-9

[Fal83] Gerd Faltings. *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*. Invent. Math. **73** (1983), 349-366; Erratum, ibid. (1984), **75**, 381

[Har77] Robin Hartshorne. *Algebraic Geometry*. Springer, New York, 1977

[Hus] D. Husemöller, *Elliptic Curves*, GTM 111, Springer

[IR82] K. Ireland, M. Rosen. *A Classical Introduction to modern Number Theory*, Springer, 1982

[Kr05] Wolfgang Kroworsch. *Konstruktion elliptischer Kurven hohen Ranges*. Diplomarbeit. (2005)

[La] Serge Lang. *Abelian Varieties*, Springer, 1983

[LEM] Lang ed. *Encyclopedia of Mathematical Sciences*. Vol **60**, *Number Theory III*, Springer, 1991.

[MilAV] J. S. Milne. *Abelian Varieties* in Cornell, Silverman eds. *Arithmetic Geometry*, Springer, 103-150. Auch verfügbar unter `www.jmilne.org/math/`

[MilAb] J. S. Milne. *Abelian Varieties*. Verfügbar unter `www.jmilne.org/math/`

[MilJV] J. S. Milne *Jacobian Varieties* in Cornell, Silverman eds. *Arithmetic Geometry*, Springer, 167-212. Auch verfügbar unter `www.jmilne.org/math/`

[Mil96] J. S. Milne. *Elliptic Curves*. Verfügbar unter `www.jmilne.org/math/`

[Mor22] I. J. Mordell. *On the rational solutions of the indeterminate equations of third and fourth degrees*. Proc. Camb. Philos. Soc. **21** (1922), 179-192

[MP86] I. Morrison, U. Persson. *Numerical Sections on Elliptic Surfaces*. Compositio Math. **59** (1986), 323-337

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie*. Springer, 1992

[RS01] Karl Rubin, Alice Silverberg. *Rank frequencies for quadratic twists of elliptic curves*, Experimental. Math. **10** (2001), 559-569

[RS02] Karl Rubin, Alice Silverberg. *Ranks of elliptic curves*, Bull. Amer. Math. Soc. **39** (2002), 455-474

[RS04] Karl Rubin, Alice Silverberg. *Twists of elliptic curves of rank at least four*, preprint (2004)

[Sb00] Alice Silverberg. *Open Questions in Arithmetic Algebraic Geometry*, LAS / Park City Mathematics Series, 2000

[Sb04] Alice Silverberg. *The distribution of Ranks in families of quadratic twists of elliptic curves*, preprint (2004)

[Shi72] Tetsui Shioda. *On elliptic modular surfaces*, J. Math. Soc. Japan, **24** (1972), 20-59

[Shi86] Tetsui Shioda. *An explicit algorithm for computing the Picard number of certain algebraic surfaces*, Amer J. Math., **108** (1986), 415-432

[Sil86] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986

[Sil94] Joseph H. Silverman. *Advanced Topics in the Arithmetic of elliptic curves*. Springer, 1994.

[SK79] Tetsui Shioda, Toshiyuki Katsura. *On Fermat Varieties*. Tohoku Math. Journ. **31** (1979), 97-115

[Sto00] Michael Stoll. *Elliptische Kurven I, Vorlesung im Sommersemester 2000*. Vorlesungsskript

[TS67] J. Tate, J. R. Shafarevich. *The Rank of Elliptic Curves*. Soviet Math. Dokl., vol. **8** (1967), Nr. 4, 917-920

[Ta66] John Tate. *Endomorphisms of Abelian Varieties over Finite Fields*. Inventiones math. **2** (1966), 132-144

[Tat66b] John Tate. *On the Conjectures of Birch and Swinnerton-Dyer and a Geometric Analog*. Séminaire Bourbaki, **9**. Soc. Math. France, Paris, (1966), Exp. No. 306, 415-440

[Ul02] Douglas Ulmer. *Elliptic curves with large rank over function fields*. Ann. of Math. (2) **155**, 295-315 (2002)

[Ul04] Douglas Ulmer. *Elliptic curves and analogies between number fields and function Fields*. in *Heegner points and Rankin L-series*. MSRI Publications **49** (2004), 285-315

[Wei48] André Weil. *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*. Hermann, Paris (1948)

[Wei49] André Weil. *Number of Solutions of Equations in Finite Fields*. Bull. Amer. Math. Soc. vol. **55** (1949), 497-508

[Wei52] André Weil. *Jacobi Sums as "Grössencharaktere"*. Trans. Amer. Math. Soc. **73** (1952), 487-495

[Zh74] Yu. G. Zarhin. *Isogenies of abelian varieties over fields of finite characteristics*. Math. USSR Sbornik **24**, 451-461 (1974)

[Zh75] Yu. G. Zarhin. *A remark on endomorphisms of abelian varieties over function fields of finite characteristics*. Izv. Akad. Nauk. SSSR Ser. Mat. **39** (1975), no 2. 272-277

[Zar71] O. Zariski. *Algebraic Surfaces*, 2nd Edition, Springer 1971