DIE HASSESCHRANKE

NICOLAS STALDER

ZUSAMMENFASSUNG. Presently, the topic which amuses me most is counting points on algebraic curves over finite fields. It is a kind of applied mathematics: you try to use any tool in algebraic geometry and number theory that you know of... and you don't quite succeed! – J.-P. Serre.

INHALTSVERZEICHNIS

1. EINFÜHRUNG

Sei k ein endlicher Körper der Ordnung $q = p^n$ (p prim, $p \neq 2, 3$). Wir betrachten eine kubische Gleichung

$$y^2 = x^3 + ax + b \tag{1.1}$$

in zwei Variablen, mit Koeffizienten $a, b \in k$. Nehmen wir ferner an, dass $4a^3 + 27b^2 \neq 0$ ist, was bedeutet, dass das Polynom $P = x^3 + ax + b$, die rechte Seite der Gleichung, keine doppelten Nullstellen besitzt. Wie viele Lösungen $(x, y) \in k^2$ dürfen wir erwarten?

In den 1930er Jahren hat Hasse gezeigt, dass ungefähr q Lösungen existieren. Genauer beweist er, dass die Abschätzung

$$\#\text{Lösungen} = q + \varepsilon, \quad |\varepsilon| \leq 2\sqrt{q}$$

gilt. Ziel dieser Semesterarbeit ist es, dieses Resultat zu erläutern, zu beweisen, und schliesslich etwas auf seine Relevanz einzugehen.

Wie sollen wir dabei vorgehen? Zunächst können wir uns davon überzeugen, dass diese Behauptung plausibel ist. Betrachten wir das Polynom $P =$

Datum: 7. Dezember 2001.

$x^3 + ax + b$ genauer: Falls $P(x)$ für ein $x \in k$ ein Quadrat in k^* ist, so gilt genau für die beiden Werte $y = \pm\sqrt{P(x)}$ die Gleichung (1). Unsere heuristische Annahme sei, dass die Werte $P(x)$ einigermassen gleichmässig über k verteilt sind. Da $[k^* : (k^*)^2] = 2$ ist, gilt unter Vernachlässigung der Sonderrolle der Nullstellen von P

$$\#\text{Lösungen} \approx 2 \cdot \frac{\#k}{2} = q.$$

Beispiel 1.1 (aus [8])**.** Man rechnet nach, dass über $\mathbb{F}_{23}$ auf den Kurven $E_a : y^2 = x^3 + x + a$ die folgenden Anzahlen von Punkten liegen:

a	0	1	2	3	4	5	6	7	8	9	10	11
$\#E_a(\mathbb{F}_{23})$	23	27	23	26	28	21	20	17	27	19	31	32
$\lvert\varepsilon\rvert$	0	4	0	3	5	2	0	6	4	4	8	9

a	12	13	14	15	16	17	18	19	20	21	22
$\#E_a(\mathbb{F}_{23})$	14	15	27	19	29	26	25	18	20	23	19
$\lvert\varepsilon\rvert$	9	8	4	4	6	3	2	5	3	0	4

In jedem Fall gilt also $|\varepsilon| \leq \lfloor 2\sqrt{23} \rfloor = 9$.

Die Heuristik ist zwar einigermassen plausibel, aber es bietet sich kein offensichtlicher Weg an, sie in einem Beweis zu formalisieren. Ich möchte deshalb kurz skizzieren, wie der Beweis der Abschätzung wirklich funktioniert. Das Paradigma der *arithmetischen Geometrie* ist es, die Methoden der algebraischen Geometrie auf die Arithmetik anzuwenden, manchmal natürlich auch umgekehrt. Algebraische Geometrie hingegen funktioniert am besten im projektiven Raum über algebraisch abgeschlossenen Körpern; wir brauchen dann aber eine Brücke, die uns zurück in unseren Grundkörper k bringt.

Wir werden also zunächst Lösungen der *homogenisierten* Gleichung

$$E: \quad Y^2Z = X^3 + aXZ^2 + bZ^3 \tag{1.2}$$

mit $(X, Y, Z) \neq (0, 0, 0)$ betrachten, wobei wir neu $X, Y, Z \in K = \overline{k}$ suchen, einem algebraischen Abschluss von k. Zweckmässigerweise fasst man skalare Vielfache von Lösungen zusammen, als sogenannte projektive Punkte

$$(X : Y : Z) \in \mathbb{P}^2 \cong \left\{\text{eindimensionale Unterräume von } K^3\right\}.$$

Die Gesamtheit dieser *K-wertigen Punkte* bezeichnen wir mit $E(K)$.

Wir können $E(K)$, wie wir sehen werden, eine natürliche Struktur als *abelsche* Gruppe geben. Die versprochene Brücke von $E(K)$ zurück zu

$$E(k) = \left\{P \in E(K) : \exists (X, Y, Z) \in k^3 \text{ mit } P = (X : Y : Z)\right\},$$

den k-wertigen Punkten von E, liefert uns dann die Abbildung

$$\text{Frob}_q : E(K) \longrightarrow E(K), \quad (X : Y : Z) \longmapsto (X^q : Y^q : Z^q),$$

der *Frobeniusmorphismus*. In Analogie zum Falle der Galoistheorie gilt nämlich $E(k) = \{\text{Fixpunkte von Frob}_q\} = \ker(\text{Frob}_q - \text{id})$. Die letzte Gleichung dürfen wir schreiben, da Frob_q ein Gruppenhomomorphismus der abelschen Gruppe $E(K)$ ist.

Es ist jetzt also wichtig, Gruppenhomomorphismen und ihre Kerne besser zu verstehen. Wir bezeichnen alle von Null verschiedenen Endomorphismen von E, die durch „algebraische Funktionen“ der Koordinaten gegeben sind,

als *Isogenien*. Unsere Frage ist, geometrisch ausgedrückt, wieviele Punkte unter einer Isogenie ψ auf das neutrale Element $O \in E(K)$ zu liegen kommen, und wir werden sehen, dass diese Anzahl Urbilder gleich ist für jeden beliebigen Punkt auf der Kurve. Damit bekommen wir eine Invariante $\deg_s(\psi)$, welche eng mit einer anderen Invariante $\deg(\psi)$ zusammenhängt. Diese letztere ist eine positiv-definite quadratische Form auf der Menge aller Isogenien, und darin liegt der mathematische Kern (sic!) der Abschätzung. Wir bekommen dann nämlich direkt eine Cauchy-Schwarz-Ungleichung

$$| \deg(\phi + \psi) - (\deg \phi + \deg \psi) | \leq 2\sqrt{\deg \phi \deg \psi},$$

mit $\phi = \mathrm{Frob}_q$, $\psi = -\mathrm{id}$, $\deg(\mathrm{Frob}_q - \mathrm{id}) = \deg_s(\mathrm{Frob}_q - \mathrm{id}) = \#E(k)$, $\deg \mathrm{Frob}_q = q$ und $\deg(-\mathrm{id}) = 1$ folgt also sofort

$$| \#E(k) - (q+1) | \leq 2\sqrt{q}.$$

Und das ist genau unsere gesuchte Abschätzung, zumal wenn wir bemerken, dass im Prozess der „Homogenisierung“ (1.1) $\rightsquigarrow$ (1.2) genau eine zusätzliche Lösung aufgetreten ist, nämlich $O = (0 : 1 : 0)$, die Identität des Gruppengesetzes auf E.

Ich möchte abschliessend festhalten, dass der Begriff der elliptischen Kurve auch über einem Körper der Charakteristik 2 oder 3 definiert ist, s. Bemerkung 2.5. Die von Hasse angegebene Schranke gilt auch in diesen Fällen; der Beweis unterscheidet sich nicht grundlegend. Wir lassen ihn aber aus Bequemlichkeit weg.

2. Grundbegriffe und Topologie

Im folgenden sei k ein endlicher Körper, $K = \overline{k}$ ein fest gewählter algebraischer Abschluss. Viele der folgenden Konstruktionen funktionieren über einem beliebigen Körper k, aber das brauchen wir nicht. Um die Beweise einfacher zu halten, und keine Sonderfälle diskutieren zu müssen, beschränken wir uns auf die Charakteristiken $\mathrm{char}\, k > 3$.

Definition 2.1.

i) Die *projektive Ebene* $\mathbb{P}^2(K) =: \mathbb{P}^2$ ist die Menge

$$\mathbb{P}^2(K) := \big(K^3 \setminus \{(0,0,0)\}\big)/\sim,$$

wobei $(X,Y,Z) \sim (X',Y',Z') \iff \exists \lambda \in K^* : (X,Y,Z) = \lambda(X',Y',Z')$. Wir bezeichnen die Äquivalenzklasse von (X,Y,Z) mit $(X : Y : Z)$.

ii) Der $\mathbb{P}^2$ trägt die *Zariski-Topologie*, in der die abgeschlossen Mengen durch Mengen $I \subset K[X,Y,Z]$ von *homogenen* Polynomen gegeben sind:

$$V(I) = \left\{P \in \mathbb{P}^2 : F(P) = 0 \quad \forall F \in I \subset K[X,Y,Z]\right\}.$$

iii) Die *affine Ebene* $\mathbb{A}^2(K) =: \mathbb{A}^2$ ist die Menge K^2, versehen mit der durch die Inklusion

$$i : \mathbb{A}^2 \longrightarrow \mathbb{P}^2, \quad p = (x,y) \mapsto P = (x : y : 1)$$

induzierten Topologie. Die selbe Topologie ergibt sich, wenn für beliebige Teilmengen $J \subset K[x,y]$, die Mengen

$$V(J) = \left\{p = (x,y) \in \mathbb{A}^2 : f(p) = 0 \quad \forall f \in J\right\}$$

als abgeschlossen deklariert werden.

Bemerkung 2.2.

i) Die Gleichheit der beiden Topologien auf $\mathbb{A}^2$ ergibt sich durch *Homogenisierung*. Einem Polynom $f \in K[x,y]$ entspricht genau ein homogenisiertes Polynom $F = Z^{\deg f} f(X/Z, Y/Z) \in K[X,Y,Z]$. Man verwischt den Unterschied zwischen Polynomen in zwei und homogenen Polynomen in drei Variablen. Im folgenden steht dann auch oft ein Polynom, von dem die Homogenisierung gemeint ist.

ii) Es gilt $\mathbb{P}^2 \cong \mathbb{A}^2 \sqcup \mathbb{P}^1$, wo $\mathbb{P}^1 \cong \{(X:Y:Z) : Z = 0\}$. Die Punkte aus $\mathbb{P}^2 \setminus \mathbb{A}^2$ werden auch die *unendlich fernen Punkte* von $\mathbb{P}^2$ genannt.

Definition 2.3. Eine *Gerade* in $\mathbb{P}^2$ ist die Nullstellenmenge einer linearen Gleichung $aX + bY + cZ = 0$, mit $(0,0,0) \neq (a,b,c) \in K^3$.

Definition 2.4.

i) Eine *elliptische Kurve* E wird (in Charakteristik $\operatorname{char} k \neq 2,3$) gegeben durch eine Gleichung

$$E: \quad y^2 = x^3 + ax + b, \qquad a,b \in K,\ 4a^3 + 27b^2 \neq 0,$$

und ist die algebraische Menge $E(K) = V(F) \subset \mathbb{P}^2$, wo $F = Y^2Z - X^3 - aXZ^2 - bZ^3$. Ausgezeichnet ist $O_E = (0:1:0)$, der einzige unendlich ferne Punkt von E. Wir schreiben oft kurz E für $E(K)$.

ii) Eine *elliptische Kurve über* k ist eine elliptische Kurve, gegeben durch eine Gleichung der Form *i)*, aber mit $a,b \in k$.

Im folgenden bezeichnen E, E' etc. immer eine elliptische Kurve über k.

Bemerkung 2.5.

i) Die *Tangente von E in $P = (X:Y:Z) \in E$* ist die Nullstellenmenge der Gleichung

$$\frac{\partial F(P)}{\partial X} X + \frac{\partial F(P)}{\partial Y} Y + \frac{\partial F(P)}{\partial Z} Z = 0.$$

Die Bedingung $4a^3+27b^2 \neq 0$ stellt sicher, dass diese Gleichung nicht trivial ist, und daher tatsächlich eine Gerade definiert. Sie ist also eine geometrische Regularitätsbedingung. Sie ist ebenfalls gleichbedeutend damit, dass die rechte Seite der definierenden Gleichung F von E keine doppelten Nullstellen hat.

ii) In beliebiger Charakteristik möchte man eine elliptische Kurve definieren als das Nullstellengebilde eines beliebigen kubischen Polynoms in X, Y und Z, dessen Tangente in jedem Punkt eine Gerade bildet. Man zeigt in der algebraischen Geometrie, dass dann (über algebraisch abgeschlossenen Körpern) ein Wendepunkt existiert. Diesen legt man (durch lineare Koordinatentransformationen) auf $(0:1:0)$, und zwar so, dass die Tangente zur unendlich fernen Geraden $\mathbb{P}^2 \setminus \mathbb{A}^2$ wird. Man kann dann folgern (s. [4]), dass die Kurve von der Form

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

sein muss. Wir setzen im folgenden $\operatorname{char} k \neq 2, 3$ voraus, können also durch quadratisches Ergänzen der linken und kubisches Ergänzen der rechten Seite die Form $y^2 = x^3 + ax + b$ erreichen.

iii) Für beliebige Körper definiert man eine elliptische Kurve einfach als Kurve der Form (2.1), mit Koeffizienten in ebendiesem Körper, und der Regularitätsbedingung, welche ich hier nicht in expliziter Form angeben möchte. Die Resultate dieser Arbeit gelten in beliebiger Charakteristik, bloss der explizite Kalkül ändert sich ein wenig.

iv) Polynome der Form $F = Y^2Z - X^3 - aXZ - bZ^3$ mit $4a^3 + 27b^2$ sind stets irreduzibel.

Die induzierte Topologie von $E \subset \mathbb{P}^2$ ist besonders einfach:

Proposition 2.6. *E trägt die* kofinite Topologie*, d.h. abgeschlossen sind genau $\emptyset$, E, und alle endlichen Kollektionen von Punkten.*

Lemma 2.7 (Baby-Bézout)**.** *Seien $f, g \in K[x, y]$ teilerfremd. Dann ist $V(f, g) \subset \mathbb{A}^2$ eine endliche Menge.*

Beweis. Setze $R = K[x, y], n = \deg f, m = \deg g$. Wir zeigen

$$\#V(f, g) \leq \dim_K(R/(f, g)) \leq \deg(f) \deg(g).$$

Seien r verschiedene Punkte $P_1, \ldots, P_r$ aus $V(f, g)$ gegeben. Man konstruiere Polynome h_i mit $h_i(P_j) = \delta_{ij}$ als Produkte von linearen Polynomen. Die h_i sind in $R/(f, g)$ linear unabhängig nach Konstruktion, also folgt die erste Ungleichung.

Wir betrachten für $d \geq n + m$ die Teilmenge $R_d \subset R$ aller Polynome von Grad $\leq d$ und setzen $I_d = (f, g) \cap R_d$. Man zeigt leicht die Gleichheit $I_d = R_{d-n}f + R_{d-m}g$. Mit Induktion folgt, dass $\dim_K R_d = \phi(d) := d(d + 1)/2$. Da R faktoriell ist, folgt aus der Tatsache, dass f und g teilerfremd sind, die Gleichheit $R_{d-n}f \cap R_{d-m}g = R_{d-n-m}fg$. Mit elementarer linearer Algebra folgt

$$\begin{aligned} \dim I_d &= \dim R_{d-n}f + \dim R_{d-m}g - \dim R_{d-n-m}fg \\ &= \phi(d - n) + \phi(d - m) - \phi(d - n - m); \end{aligned}$$

letztere Gleichung gilt, da für $h \neq 0$ die Vektorräume $R_{d-\deg h}$ und $R_{d-\deg h}h$ isomorph sind. Eine explizite Rechnung liefert $\dim(R_d/I_d) = \dim(R_d) - \dim(I_d) = nm$.

Seien schliesslich g_i mehr als nm Polynome. Für d genügend gross liegen die g_i in R_d, und sind aus Dimensionsgründen in R_d/I_d linear abhängig, folglich auch in R/I. Somit gilt $\dim R/(f, g) \leq nm$, die zweite Ungleichung. ∴

Beweis der Proposition. Jeder Punkt in $\mathbb{P}^2$ ist abgeschlossen, da er als Durchschnitt zweier Geraden geschrieben werden kann. Deshalb sind auch alle endlichen Teilmengen von E abgeschlossen.

Für die Umkehrung genügt es, die endlichen Punkte $E \cap \mathbb{A}^2$ zu betrachten. Sei $F \subsetneq E$ abgeschlossen, mit $F \cap \mathbb{A}^2 \neq \emptyset$. Dann gilt für ein $0 \neq f \in k[x, y]$ die Inklusion $F \cap \mathbb{A}^2 \subset V(f)$. Dieses f ist zum definierenden Polynom von E teilerfremd, da letzteres irreduzibel ist. Die Aussage folgt. ∴

3. Der Funktionenkörper

Sei E eine elliptische Kurve mit definierendem Polynom F. Sind G, H homogene Polynome gleichen Grades, und teilt F nicht H, so ist $P \longmapsto G(P)/H(P)$ eine wohldefinierte Funktion

$$E(K)\setminus\{\text{Nullstellen von } H\} \longrightarrow K.$$

Definition 3.1.

i) Der *homogene Koordinatenring von E* ist

$$S(E) := K[X,Y,Z]/(F) = \bigoplus_d S(E)_d.$$

Dabei besteht $S(E)_d$ aus den Elementen von $S(E)$, welche einen homogenen Repräsentanten in $K[X,Y,Z]$ von Grad d haben.

ii) Der *Funktionenkörper von E* ist

$$K(E) := \left\{ \frac{g}{h} : \exists d \text{ mit } g,h \in S(E)_d \right\}.$$

Nach der einführenden Bemerkung definiert f eine Funktion auf der Teilmenge von $E(K)$, wo h nicht verschwindet. Die Elemente des Funktionenkörpers heissen deshalb *rationale Funktionen*.

iii) Diejenigen Funktionen aus $K(E)$, welche in P definiert sind, bilden den *lokalen Ring* $\mathcal{O}_P$ von E in P.

Proposition 3.2. *Unter der Identifizierung $x = X/Z$, $y = Y/Z$ gilt $K(E) = K(x,y) = K(x)[y]/(F)$. Der Funktionenkörper $K(E)$ ist also eine endliche algebraische Erweiterung von Grad 2 des rationalen Funktionenkörpers $K(x)$.*

Beweis. Das ergibt sich aus der uns mittlerweile wohlvertrauten Homogenisierung respektive Dehomogenisierung von Polynomen. ∴

Wir können nun definieren, welche Abbildungen zwischen elliptischen Kurven wir zulassen wollen: nämlich diejenigen, welche durch rationale Funktionen in den Koordinaten gegeben werden können. Wir wollen also Abbildungen $\psi(P) = (f(P) : g(P) : h(P))$ zulassen, mit $f,g,h \in K(E)$. Da wir Nenner ausmultiplizieren können, definieren wir aber:

Definition 3.3.

i) Eine Abbildung $\psi : E \longrightarrow E'$ zwischen zwei elliptischen Kurven heisst *rational*, falls ein d und $f,g,h \in S(E)_d$ existieren, sodass $(f,g,h) \neq (0,0,0)$, und $\psi(P) = (f(P) : g(P) : h(P))$ überall dort gilt, wo $f(P)$, $g(P)$ und $h(P)$ nicht alle verschwinden. In solchen Punkten hat ψ eine *rationale Darstellung*.

ii) Eine rationale Abbildung heisst *regulär*, oder ein *Morphismus*, falls jedes $P \in E(K)$ eine rationale Darstellung zulässt.

Lemma 3.4. *Eine rationale Abbildung $\psi : E \longrightarrow E'$ zwischen elliptischen Kurven ist immer regulär.*

Beweis. Man beweist in der algebraischen Geometrie, dass $\mathcal{O}_P$ ein diskreter Bewertungsring ist. Sei t der Erzeuger des maximalen Ideals, und $\psi = (f_1 : f_2 : f_3)$ eine beliebige rationale Darstellung von ψ. Falls nun eines der f_i in P

einen Pol der Ordnung $n := -\operatorname{ord}_P(f_i)$ hat, ersetzt man die f_i durch $t^{-n}f_i$. Falls alle f_i in P eine gemeinsame Nullstelle der Ordnung $n = \operatorname{ord}_P(f_i)$ besitzen, macht man dieselbe Ersetzung. Somit ist ψ in P regulär. ∴

Proposition 3.5. *Ein Morphismus $\psi : E \longrightarrow E'$ zwischen elliptischen Kurven ist entweder konstant oder surjektiv.*

Beweis. Wir brauchen ein allgemeines Resultat der algebraischen Geometrie („Der projektive Raum ist eigentlich"), was in unserem Fall bedeutet, dass das Bild $\psi(E)$ von E in E' abgeschlossen ist. Ist es also eine echte Teilmenge von E', so muss es nach Proposition 2.6 endlich sein. Als Bild einer zusammenhängenden Menge unter einer stetigen Abbildung ist $\psi(E)$ auch zusammenhängend, folglich einpunktig. ∴

4. Dualität, I

Wir möchten in diesem Abschnitt einsehen, dass eine Dualität zwischen nicht-konstanten Morphismen von elliptischen Kurven und Einbettungen der zugehörigen Funktionenkörper über K besteht:

$$\psi : E \longrightarrow E' \quad \rightsquigarrow \quad \iota : K(E') \longrightarrow K(E)$$

Definition 4.1. Ein nicht-konstanter Morphismus $\psi : E \longrightarrow E'$ induziert eine Einbettung

$$\psi^* : K(E') \longrightarrow K(E)$$

der zugehörigen Funktionenkörper.

Beweis. Das ist ein Korollar der vorangehenden Proposition 3.5. Man bekommt zunächst eine Abbildung $S(E') \longrightarrow S(E)$ durch Komposition mit ψ. Diese ist injektiv, da ψ surjektiv ist. Somit wird auch die gewünschte Körpererweiterung induziert. ∴

Proposition 4.2. *Sei ψ ein nicht-konstanter Morphismus.*
Dann ist $K(E)/\psi^*(K(E'))$ eine endliche Erweiterung von Körpern.

Beweis. Beide Körper haben Transzendenzgrad 1 über K, also folgt aus der Additivität des Transzendenzgrades, dass die Erweiterung algebraisch ist. Der Körper $K(E)$ ist endlich erzeugt über K, also auch über seinem Oberkörper $\psi^*(K(E'))$. Somit ist die Körpererweiterung endlich erzeugt und algebraisch, also endlich. ∴

Proposition 4.3. *Sei $\iota : K(E') \longrightarrow K(E)$ eine Körpererweiterung, welche auf K die Identität ist. Dann existiert genau ein nicht-konstanter Morphismus $\psi : E \longrightarrow E'$ mit $\psi^* = \iota$.*

Beweis. Man nutzt aus, dass einerseits $K(E)$ durch x, y erzeugt wird, anderseits, dass eine Abbildung gerade durch die Koordinaten x, y des Bildpunktes festgelegt wird. Für $x, y \in K(x, y) = K(E')$ setzt man also $\psi(P) := \big(\iota(x)(P) : \iota(y)(P) : 1\big)$. ∴

Definition 4.4. Sei $\psi : E \longrightarrow E'$ ein nicht-konstanter Morphismus. Wir definieren den *Grad* von ψ

$$\deg(\psi) := [K(E) : \psi^*(K(E'))]$$

als den Grad der zugehörigen Körpererweiterung. Der *separable* und *inseparable* Grad $\deg_s(\psi)$ und $\deg_i(\psi)$ von ψ sind analog definiert.

Ist ψ konstant, setzen wir $\deg(\psi) = \deg_s(\psi) = \deg_i(\psi) = 0$.

Auf die Bedeutung der Separabilität oder Inseparabilität gehen wir in Abschnitt 7 und 8 noch genauer ein, insbesondere werden wir mit Proposition 8.3 ein (geometrisches) Separabilitätskriterium erhalten.

5. Der Frobeniusmorphismus

Für eine elliptische Kurve E über einem endlichen Körper k mit definierender Gleichung $y^2 = x^3 + ax + b$ gilt, für $q = \#k$, dass $(y^q)^2 = (x^3 + ax + b)^q = (x^q)^3 + ax^q + b$ ist, was die folgende Definition nahelegt:

Definition 5.1. Für E, k wie oben, und $q = (\#k)^r$, mit $r > 0$, definieren wir die Frobenius-Morphismen

$$\mathrm{Frob}_q : E \longrightarrow E, \qquad (X : Y : Z) \longmapsto (X^q : Y^q : Z^q).$$

Sie sind nach der obigen Bemerkung wohldefiniert.

Der Spezialfall $q = \#k$ heisst „der“ Frobenius(morphismus) von E, wir bezeichnen ihn mit Frob_k.

Proposition 5.2. *Die k-rationalen Punkte einer über k definierten elliptischen Kurve sind genau die Fixpunkte von* Frob_k.

Beweis. Bekanntlich gilt $k = \{x \in K : x^q = x\}$. Die Inklusion $E(k) \subset E(K)^{\mathrm{Frob}_k}$ ist also klar. Sei umgekehrt ein Fixpunkt $P = (X : Y : Z) \in E(K)$ des Frobenius gegeben, und sei ohne Beschränkung der Allgemeinheit $Z \neq 0$. Dann gilt also $(X/Z)^q = X/Z$, und analog $(Y/Z)^q = (Y/Z)$, also sind X/Z und Y/Z in k, und somit $P = (X/Z : Y/Z : 1) \in E(k)$. $\therefore$

Für die zwei nachfolgenden Aussagen brauchen wir etwas mehr Allgemeinheit. Falls $q = (\mathrm{char}\, k)^r$ keine Potenz von $\#k$ ist, ist der Bildbereich von Frob_q nicht mehr E, sondern die Kurve $E^{(q)}$, die entsteht, indem man alle Koeffizienten im definierenden Polynom von E zur q-ten Potenz erhebt. Man sieht leicht ein, dass $E^{(q)}$ wieder eine elliptische Kurve ist.

Proposition 5.3. *Sei $q = (\mathrm{char}\, k)^r$, mit $r > 0$.*

i) $\mathrm{Frob}_q^* K(E^{(q)}) = K(E)^q = \{f^q : f \in K(E)\}$.
ii) *Der Frobenius* Frob_q *ist rein inseparabel,*
iii) $\deg(\mathrm{Frob}_q) = \deg_i(\mathrm{Frob}_q) = q$.

Beweis. Nach (3.2) ist $K(E^{(q)}) = K(x, y)$. Somit ist

$$\mathrm{Frob}_q^* K(E^{(q)}) = \mathrm{Frob}_q^* K(x, y) = K(x^q, y^q) = K(E)^q,$$

woraus *i)* und dann auch *ii)* folgen.

iii): Sei $t \in K(E)$ der Erzeuger des maximalen Ideals eines lokalen Rings $\mathcal{O}_P$, wie im Beweis von Lemma (3.4). Man weiss, oder liest in [6] nach, dass $K(E)$ über $K(t)$ endlich separabel ist. Wir haben folglich eine separable Körpererweiterung $K(E)/K(t)$, und eine rein inseparable $K(E)/K(E)^q$. Der Körper $K(E)^q(t) \subset K(E)$ umfasst sowohl $K(t)$ als auch $K(E)^q$, und ist damit separabel und rein inseparabel. Folglich gilt $K(E) = K(E)^q(t)$.

Nach i) ist $\deg \mathrm{Frob}_q = [K(E)^q(t) : K(E)^q]$. Da t^q in $K(C)^q$ liegt, müssen wir bloss noch zeigen, dass $t^{q/p} \neq K(E)^q$; dann ist nämlich $\deg \mathrm{Frob}_q = q$ offensichtlich.

Aber falls $t^{q/p} = f^q$ für ein $f \in K(E)$, so gilt $q/p = \mathrm{ord}_P(t^{q/p}) = q\,\mathrm{ord}_P(f)$, was absurd ist. ∴

Korollar 5.4. *Jeder Morphismus $\psi : E \longrightarrow E'$ faktorisiert als*

$$E \xrightarrow{\mathrm{Frob}_q} E^{(q)} \xrightarrow{\phi} E', \qquad \psi = \phi \circ \mathrm{Frob}_q,$$

wobei ϕ separabel ist und $q = \deg_i(\phi)$.

Beweis. Sei L der separable Abschluss von $\psi^* K(E')$ in $K(E)$. Wir erhalten einen Turm $K(E)/L/\psi^* K(E')$ von Körpererweiterungen, wobei die obere rein inseparabel vom Grad $q = \deg_i(\psi)$ ist. Also gilt $L \supset K(E)^q = \mathrm{Frob}_q^*(K(E^{(q)}))$. Da aber auch $K(E)/\mathrm{Frob}_q^*(K(E^{(q)}))$ vom Grad q ist, gilt sogar Gleichheit. Also ist unser Turm isomorph zu

$$K(E)/\mathrm{Frob}_q^*(K(E^{(q)}))/\psi^* K(E'),$$

was mit der vorangehenden Proposition die gesuchte Zerlegung von ψ liefert. ∴

Proposition 5.5. *Jeder Frobeniusmorphismus ist bijektiv.*

Beweis. Falls $\mathrm{Frob}_q(P) = (X^q : Y^q : Z^q) = (0 : 1 : 0)$ ist, folgt $X = Z = 0$, und somit ist $P = O_E$. Der Frobenius ist also injektiv.

Anderseits ist K algebraisch abgeschlossen, weswegen der Frobenius sich als surjektiv erweist. ∴

6. Elliptische Addition

Punkte auf elliptischen Kurven können *addiert* werden. Man kann beweisen, dass die Abschätzung in Lemma 2.7 zur Gleichheit wird, wenn man die Punkte mit geeigneten Multiplizitäten zählt (tangentiale Schnittpunkte zählen doppelt, etc.) und unendlich ferne Punkte mitzählt. Das ist dann der wirkliche Satz von Bézout. Deshalb schneidet jede Gerade eine elliptische Kurve in genau drei Punkten, und wir setzen

$$P_1 + P_2 + P_3 = 0$$

falls die P_i diese drei Punkte sind. Wir brauchen den allgemeinen Satz aber nicht, denn wir können rechnen. Die geometrische Definition liefert folgende Formeln, wo $P = (x, y)$, und $P_i = (x_i, y_i)$ sind:

$$\begin{aligned} -(x,y) &= (x,-y) \\ (x,y) + (x,-y) &= O_E \\ (x_1,y_1) + (x_2,y_2) &= (\lambda^2 - x_1 - x_2, -\lambda(\lambda^2 - x_1 - x_2) - \mu) \end{aligned}$$

wobei

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}, & \text{falls } x_1 \neq x_2 \\ \frac{3x_1^2 + a}{2y_1}, & \text{falls } x_1 = x_2 \text{ falls } y_1 \neq -y_2 \end{cases}$$

und $\mu = y_1 - \lambda x_1$ sind. (Die Gerade durch die beiden Punkte hat die Gleichung $y = \lambda x + \mu$).

Theorem 6.1. *Dieses Gruppengesetz macht E zu einer abelschen Gruppe. Dabei sind die Addition $E \times E \longrightarrow E$ und die Inversenbildung $E \longrightarrow E$ Morphismen.*

Korollar 6.2. *Aus zwei Morphismen $\phi, \psi : E \longrightarrow E$ entsteht durch punktweise Addition $(\phi + \psi)(P) := \phi(P) + \psi(P)$ wieder ein Morphismus.*

Beweis. Wir beweisen fast nichts (s. [1], [4], [5], [6], [7], [8],. . .). Die Kommutativität der Operation ist aus der geometrischen Definition klar; was Mühe bereitet, ist die Assoziativität. Um das elementar zu zeigen, nimmt man sich die Konfiguration aller beteiligten Punkte und Geraden, und wendet dann ein Lemma an, welches besagt, dass zwei ebene projektive Kurven von Grad 3, welche in 8 Punkten übereinstimmen, dies auch im neunten tun. ∴

Definition 6.3. Für jedes $T \in E$ bezeichnet $\tau_T : E \longrightarrow E$ den Morphismus $P \mapsto P + T$.

Definition 6.4.

i) Ein Morphismus $E \longrightarrow E'$ heisst *Homomorphismus*, wenn er O_E auf $O_{E'}$ abbildet.
ii) Ein Homomorphismus $E \longrightarrow E$ ist ein *Endomorphismus*, und wir bezeichnen die Menge aller Endomorphismen mit $\mathrm{End}(E)$. Sie wird zum Ring durch punktweise Addition und Komposition.
iii) Der einzige konstante Homomorphismus ist die Nullabbildung. Jeder nichtkonstante Homomorphismus heisst *Isogenie*.

Beispiel 6.5. Der Frobenius ist eine Isogenie, ebenso die Identität.

Der Grund für diese Definition von Endomorphismen ist das folgende Theorem:

Theorem 6.6. *Jeder Endomorphismus ist ein Gruppenhomomorphismus.*

Beweis. siehe [6], Theorem 4.8. Für id_E ist das allerdings klar, und für Frob_k folgt direkt aus dem Additionsgesetz, dass $\mathrm{Frob}_k\big((x_1, y_1)+(x_2, y_2)\big) = (\lambda^{2q} - x_1^q - x_2^q, -\lambda^q(\lambda^{2q} - x_1^q - x_2^q) - \mu^q) = \mathrm{Frob}_k(x_1, y_1) + \mathrm{Frob}_k(x_2, y_2)$. ∴

Proposition 6.7.

i) $\mathrm{End}(E)$ *ist eine nullteilerfreier Ring.*
ii) *Die Abbildung* $\mathbb{Z} \longrightarrow \mathrm{End}(E), \quad m \mapsto m \cdot \mathrm{id}_E$, *ist injektiv.*

Beweis. *i*) Seien $\phi, \psi \in \mathrm{End}(E)$. Aus $\phi \circ \psi = 0$ folgt mit der Multiplikativität des Grades, dass $0 = \deg(\phi\psi) = \deg(\phi)\deg(\psi)$ ist. Nach Definition hat nur aber nur die Nullabbildung Grad 0, also ist $\mathrm{End}(E)$ nullteilerfrei.

ii) Die Abbildung ist gegeben durch $m \longmapsto m \cdot \mathrm{id}$. Das sind nach Korollar (6.2) Morphismen. Da -1 ein Isomorphismus ist, genügt es, positive m zu betrachten. Wegen *i*) genügt es sogar, $m = 2$ und ungerade m zu betrachten.

Fall $m = 2$: Ein Punkt $(x, y) = P \in E \setminus \{O\}$ hat Ordnung 2 genau dann, wenn $y = 0$, also wenn $x^3 + ax + b = 0$. Diese Gleichung besitzt nur endlich viele Lösungen, und somit ist $2 \neq 0$ in $\mathrm{End}(E)$.

Fall m ungerade, positiv: Für irgendeine Nullstelle x_0 von $x^3 + ax + b$ ist $P = (x_0, 0)$ ein nicht-trivialer Punkt der Ordnung 2. Für ihn gilt $mP = P \neq O$, also ist auch $m \neq 0$ in $\mathrm{End}(E)$. ∴

Wir identifizieren im folgenden $\mathbb{Z}$ mit seinem Bild in $\mathrm{End}(E)$.

7. Der separable Grad

Die geometrische Bedeutung des separablen Grades $\deg_s(\psi)$ einer Isogenie $\psi : E \longrightarrow E'$ ist die folgende:

Proposition 7.1. *Für alle $Q \in E'$ gilt $\#\psi^{-1}(Q) = \deg_s(\psi)$.*

Korollar 7.2. *Sei $\phi : E \longrightarrow E'$ eine separable Isogenie. Dann gilt*

$$\#\ker\phi = \deg(\phi).$$

Zunächst eine heuristische Analogie: Da Frob_k bijektiv ist, (5.5), genügt es nach der Zerlegung (5.4), separable Isogenien zu betrachten. Der Analogieschluss sagt uns, dass die separable Isogenie ψ einem separablen Polynom von Grad $\deg\psi$ entspricht, welches wiederum genau $\deg\psi$ verschiedene Nullstellen besitzt. Zur strengen Herleitung können wir uns auf das folgende Resultat der allgemeinen Kurventheorie berufen:

Proposition 7.3. *Sei $\phi : C \longrightarrow C'$ ein nicht-konstanter Morphismus glatter irreduzibler projektiver Kurven. Dann gilt für fast alle $Q \in C'$, dass $\#\phi^{-1}(Q) = \deg_s(\phi)$.*

Beweis der Proposition 7.1. Wir wissen, dass die Aussage $\#\phi^{-1}(Q_0) = \deg_s(\phi)$ für ein $Q_0 \in E'$ gilt. Sei $Q \in E'$ beliebig. Da ϕ nach Proposition 3.5 surjektiv ist, können wir ein $R \in E$ wählen mit $\phi(R) = Q - Q_0$. Da ϕ ein Homomorphismus von Grupen ist, erhalten wir durch

$$P \longmapsto P + R$$

eine Bijektion $\phi^{-1}(Q_0) \longrightarrow \phi^{-1}(Q)$, also folgt die Behauptung. ∴

8. Ein Separabilitätkriterium

Definition 8.1. Die Raum der *Differentiale* von E ist der $K(E)$- Vektorraums

$$\Omega_E = \Big(\bigoplus_{t \in K(E)} K(E) \cdot dt \Big) / \sim,$$

wobei $\sim$ von den folgenden Relationen Relationen erzeugt ist:

i) $d(s+t) = ds + dt$ für $s, t \in K(E)$
ii) $d(st) = s \cdot dt + t \cdot ds$
iii) $da = 0$ für $a \in K$

Ein nicht-konstanter Morphismus $\psi : E \longrightarrow E'$ induziert auf den Differentialen eine Abbildung $\psi^* : \Omega_{E'} \longrightarrow \Omega_E$ via

$$\psi^*\Big(\sum f_i dt_i\Big) := \sum (\psi^* f_i) d(\psi^* t_i).$$

Theorem 8.2.

i) *Ω_E ist ein 1-dimensionaler $K(E)$-Vektorraum.*
ii) *Sei $t \in K(E)$. Dann ist dt eine Basis von Ω_E genau dann, wenn $K(E)/K(t)$ endlich separabel ist.*

Beweis. Siehe [3], 27.A und 27.B. Das sind Standardresultate der algebraischen Theorie der Differentiale für beliebige Körpererweiterungen. ∴

Proposition 8.3. *Ein nichtkonstanter Morphismus $\psi : E \longrightarrow E'$ ist separabel genau dann, wenn ψ^* auf den Differentialen injektiv ist.*

Beweis. Sei $t \in K(E')$ so, dass $\Omega_{E'} = K(E')dt$ und $K(E')/K(t)$ endlich separabel ist. Dann ist natürlich $\psi^*K(E')$ separabel über $\psi^*K(t) = K(\psi^*t)$.

Es folgt: ψ^* injektiv $\iff$ $\psi^*dt = d(\psi^*t) \neq 0$ $\iff$ $d(\psi^*t)$ ist Basis von Ω_E $\iff$ $K(E)/K(\psi^*t) = \psi^*(K(t))$ separabel $\iff$ $K(E)/\psi^*K(E')$ separabel. Für die letzte Äquivalenz betrachtet man

$$K(E)/\psi^*K(E')/K(\psi^*y).$$

$\therefore$

Definition 8.4. Ein Differential $\omega \in \Omega_E$ heisst *invariant*, falls es unter der natürlichen Operation von E auf Ω_E invariant ist, d.h., falls für alle $T \in E$ die Gleichheit $\tau_T^*\omega = \omega$ gilt.

Proposition 8.5. *Das Differential $\omega = \frac{dx}{2y}$ ist invariant.*

Beweis. Mann schreibe $x(P+T)$ und $y(P+T)$ mit der Additionsformel explizit aus, und wende in längerer Rechnung die Differentiationsregeln an.

$\therefore$

Wir nennen $\omega = \frac{dx}{2y}$ im folgenden *das* invariante Differential.

Rechenregel 8.6. *Für das invariante Differential ω gelten:*

i) $(\phi + \psi)^*\omega = \phi^*\omega + \psi^*\omega$, *und*
ii) $(-\mathrm{id})^*\omega = -\omega$.

Beweis. i): Seien (x_1, y_1) und (x_2, y_2) unabhängige Koordinaten auf E (genauer gesagt, seien $([x_1, y_1, 1], [x_2, y_2, 1])$ Koordinaten für $E \times E \subset \mathbb{P}^1 \times \mathbb{P}^2$). Sei $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$, wobei die Additionsregel in E verwendet wird. Es ist klar, dass durch Anwenden der Differentiationsregeln eine Gleichung der Form

$$\omega(x_3, y_3) = f(x_1, y_1, x_2, y_2)\omega(x_1, y_1) + g(x_1, y_1, x_2, y_2)\omega(x_2, y_2)$$

entsteht, wo f, g rationale Funktionen sind. Nun sind f und g eindeutig, also wie die ω *invariant*. Deshalb sind sie Konstanten; durch Einsetzen von $(x_i, y_i) = 0$ wird klar, dass $f = g = 1$. Man könnte diese letzte Aussage natürlich auch durch krampfhaftes Rechnen verifizieren.

ii): Wegen $-(x, y) = (x, -y)$ gilt $(-1)^*\left(\frac{dx}{2y}\right) = \frac{dx}{2(-y)} = -\frac{dx}{2y}$. $\therefore$

Proposition 8.7. *Die Abbildung* $\mathrm{Frob}_q - \mathrm{id}$ *ist separabel.*

Beweis. Da der Frobenius inseparabel ist (Proposition 5.3), folgt für das invariante Differential ω die Gleichungskette $(\mathrm{Frob}_q - \mathrm{id})^*\omega = \mathrm{Frob}_q^*\,\omega - \mathrm{id}^*\,\omega = -\omega \neq 0$, also auch die Behauptung. $\therefore$

9. Dualität, II

In diesem zweiten Abschnitt über Dualität auf elliptischen Kurven beschäftigen uns die sogenannten *dualen Isogenien*.

Definition 9.1. Sei $\psi : E \to E'$ eine Isogenie. Eine Isogenie $\widehat{\psi} : E' \longrightarrow E$ heisst die *duale Isogenie* von ψ, falls gilt $\widehat{\psi}\psi = \deg(\psi) \in \mathbb{Z} \cap \mathrm{End}(E)$.

Wir setzen $\widehat{0} = 0$.

Wir werden zeigen, dass die duale Isogenie existiert und eindeutig ist. Dazu brauchen wir etwas mehr Galoistheorie für unsere Funktionenkörper.

Proposition 9.2. *Sei $\phi : E \longrightarrow E$ eine Isogenie.*

i) $\iota_\phi : \ker\phi \longrightarrow \mathrm{Aut}(K(E)/\phi^*K(E)), T \mapsto \tau_T^*$ *ist ein Isomorphismus.*

ii) Für separables ϕ ist $K(E)/\phi^*K(E)$ Galoissch, mit Galoisgruppe $\Gamma \cong \ker\phi$.

Beweis. i): Für $T \in \ker\phi$ und $f \in K(E)$ folgt $\tau_T^*(\phi^* f) = (\phi \circ \tau_T)^* f = \phi^* f$, also fixiert τ_T^* den Körper $\phi^*K(E)$, und ι_ϕ ist somit wohldefiniert.

Da $\tau_S \circ \tau_T = \tau_{S+T}$ ist, folgt dass ι_ϕ ein Homomorphismus ist.

Nach Korollar (7.2) ist $\#\ker\phi = \deg_s\phi$, und mit elementarer Galoistheorie ist $\#\,\mathrm{Aut}(K(E)/\phi^*K(E)) \leq \deg_s\phi$, also brauchen wir bloss zu zeigen, dass ι_ϕ injektiv ist. Aber falls τ_T^* den Funktionenkörper $K(E)$ fixiert, nehmen insbesondere die Koordinatenfunktionen auf T und O dieselben Werte an, d.h. $T = O$.

ii): Falls ϕ separabel ist, so gilt nach *i)* und (7.2) die Gleichungskette

$$\#\,\mathrm{Aut}(K(E)/\phi^*K(E)) = \#\ker\phi = \deg_s\phi = \deg\phi = [K(E) : \phi^*K(E)].$$

Die Körpererweiterung $K(E)/\phi^*K(E)$ ist also normal, und somit Galoissch.

$\therefore$

Proposition 9.3.

i) Jede Isogenie besitzt genau eine duale Isogenie.

ii) Es gilt auch $\psi\widehat{\psi} = \deg(\psi)$.

Beweis (für den Fall $E = E'$). Seien ψ, ϕ, ϕ' Isogenien mit $\phi\psi = \phi'\psi = \deg(\psi)$. Da $\mathrm{End}(E)$ nullteilerfrei ist, folgt $\phi = \phi'$.

Wir betrachten $(\psi\widehat{\psi})\psi = \psi(\widehat{\psi}\psi) = \psi m = m\psi$ und kürzen ψ.

Es bleibt noch zu zeigen, dass zu jeder Isogenie ψ eine duale überhaupt existiert. Mit Rechenregel 9.5.ii und der Zerlegung $\psi = \phi\circ\mathrm{Frob}^r$ aus Korollar 5.4 genügt es, den Frobenius und separable Isogenien zu behandeln.

Für $\psi = \mathrm{Frob}$ gilt $\deg(\mathrm{Frob}) = p$. Ferner ist $p^*\omega = p\omega = 0$, da $\mathrm{char}\,K = p$, also ist p nicht separabel. Folglich muss in der Zerlegung $p = \phi \circ \mathrm{Frob}^e$ der Frobenius wirklich auftreten, also $e \geq 1$. Somit ist

$$\widehat{\mathrm{Frob}} := \phi \circ \mathrm{Frob}^{e-1}$$

eine zu Frob duale Isogenie.

Sei ϕ eine separable Isogenie, mit $\deg\phi = m$. Nach Korollar (7.2) gilt $\#\ker\phi = m$, also gilt die Inklusion $\ker\phi \subseteq \ker m$. Die Existenz und Eindeutigkeit von $\widehat{\phi}$ ist eine Korollar des folgenden Lemmas. $\therefore$

Lemma 9.4. *Seien $\phi, \psi : E \longrightarrow E$ Isogenien, wobei ϕ separabel sei, und $\ker\phi \subset \ker\psi$ gelte. Dann existiert genau eine Isogenie $\lambda : E \longrightarrow E$ mit $\psi = \lambda \circ \phi$.*

Beweis. Wegen der Separabilität von ϕ ist $K(E)/\phi^*K(E)$ Galoissch mit Galoisgruppe $\Gamma \cong \ker\phi$. Diese Isomorphie ist mit der Isomorphie $\mathrm{Aut}(K(E)/\psi^*K(E) \cong \ker\psi$ verträglich, also erhalten wir mit elementarer Galoistheorie die Inklusionen

$$\psi^*K(E) \subset \phi^*K(E) \subset K(E).$$

Unsere Proposition (4.3) liefert die Existenz und Eindeutigkeit eines Morphismus $\lambda : E \longrightarrow E$ mit $\phi^*\lambda^*K(E) = \psi^*K(E)$, was wiederum zu $\lambda\phi = \psi$ äquivalent ist.

Ferner ist $\lambda(O) = \lambda(\phi(O)) = \psi(O) = O$, also ist λ eine Isogenie. $\therefore$

Rechenregel 9.5. *Es gelten die Rechenregeln*

i) $\widehat{\varphi + \psi} = \widehat{\varphi} + \widehat{\psi}$.
ii) $\widehat{\varphi\psi} = \widehat{\psi}\widehat{\varphi}$.

Beweis. Die zweite Aussage folgt direkt aus den Definitionen, für die erste siehe [6], Theorem 6.2. $\therefore$

Proposition 9.6. *Für $\psi \in \mathrm{End}(E)$ liegt*

$$\mathrm{tr}(\psi) := \psi + \widehat{\psi} \in \mathbb{Z} \subset \mathrm{End}(E).$$

Beweis. Es gilt $\deg(\mathrm{id} + \psi) = (\mathrm{id} + \psi)(\widehat{\mathrm{id}} + \widehat{\psi}) = 1 + \deg(\psi) + \mathrm{tr}(\psi)$. Folglich muss $\mathrm{tr}(\psi)$ eine ganze Zahl sein. $\therefore$

Definition 9.7. Die Zahl $\mathrm{tr}(\psi)$ heisst die *Spur* von ψ.

10. Der Abbildungsgrad als quadratische Form

Definition 10.1. Sei A eine abelsche Gruppe. Eine Abbildung

$$q : A \longrightarrow \mathbb{Z}$$

heisst *quadratische Form* auf A, falls gilt:

i) $q(a) = q(-a)$ für alle $a \in A$, und
ii) die Abbildung

$$\begin{array}{rcl} B : A \times A & \longrightarrow & \mathbb{Z} \\ (a, b) & \longmapsto & q(a+b) - q(a) - q(b) \end{array}$$

ist $\mathbb{Z}$-bilinear.

Sie heisst *positiv definit*, falls $q \geq 0$, und $q(a) = 0$ genau für $a = 0$.

Lemma 10.2 (Cauchy-Schwarz-Ungleichung)**.** *Sei A eine abelsche Gruppe, und $q : A \longrightarrow \mathbb{Z}$ eine positiv definite quadratische Form. Für alle $a, b \in A$ gilt dann*

$$|q(a+b) - (q(a) + q(b))| \leq 2\sqrt{q(a)q(b)}.$$

Beweis. Betrachte die assoziierte Bilinearform B. Für $m, n \in \mathbb{Z}$ gilt

$$0 \leq q(ma + nb) = m^2 q(a) + mnB(a, b) + n^2 q(b).$$

Indem wir $m = -B(a, b)$ und $n = 2q(a)$ setzen, erhalten wir

$$0 \leq q(a)\left(4q(a)q(b) - B(a, b)^2\right).$$

Damit folgt die Behauptung, ausser wenn $q(a) = 0$. In diesem Fall ist allerdings $a = 0$, und die Ungleichung ist sowieso klar. $\therefore$

Für den Beweis der Hasseschranke auf elliptischen Kurven fehlt uns nur noch das

Theorem 10.3. *Sei E eine elliptische Kurve. Die Abbildung*

$$\deg : \mathrm{End}(E) \longrightarrow \mathbb{Z}$$

ist eine positiv definite quadratische Form.

Beweis. Nach Definition ist der Grad einer Isogenie eine nicht-negative ganze Zahl. Ebenfalls aus den Definitionen und daraus, dass 0 der einzige Endomorphismus von Grad 0 ist, folgt die positive Definitheit. Da $\deg(-1) = 1$ ist, folgt auch, dass der Grad eine gerade Abbildung ist. Zu prüfen bleibt die Bilinearität. Aber

$$\deg(\phi+\psi) - \deg(\phi) - \deg(\psi) = \widehat{(\phi+\psi)}(\phi+\psi) - \widehat{\phi}\phi - \widehat{\psi}\psi = \widehat{\phi}\psi + \widehat{\psi}\phi,$$

und der letzte Ausdruck ist nach Rechenregel (9.5) bilinear. ∴

11. Beweis der Hasseschranke

Theorem 11.1. *Sei E eine elliptische Kurve über k. Dann gilt*

$$\#E(k) = q + 1 + \varepsilon \qquad \textit{mit } \mid \varepsilon \mid \leq 2\sqrt{q}.$$

Beweis. $E(k)$ ist die Menge der Fixpunkte von Frob_q, also gleich dem Kern von $\mathrm{Frob}_q - \mathrm{id}$. Letztere Abbildung ist separabel. Die Kardinalität von $E(k)$ ist also gleich $\deg(\mathrm{Frob}_q - \mathrm{id})$. Die Behauptung folgt mit der Cauchy-Schwarz-Ungleichung aus $\deg(\mathrm{Frob}_q) = q$ und $\deg(\mathrm{id}) = 1$. ∴

12. Ausblick

Es gibt eine wunderbare Uminterpretation der Hasseschranke, die sogenannte Riemannsche Vermutung für elliptische Funktionenkörper. Sie bildet Teil der sogenannten Weil-Vermutungen, welche von Weil selbst für Kurven und abelsche Varietäten 1949 bewiesen wurden. Der allgemeine Beweis wurde erst 1973 von Deligne nachgeliefert.

Ich nehme in diesem Abschnitt an, dass der Leser sich unter einer glatten irreduzible projektiven Varietät über einem endlichen Körper etwas vorstellen kann.

Definition 12.1. Sei X eine glatte irreduzible projektive Varietät der Dimension n über einem endlichen Körper k der Kardinalität q. Wir bezeichnen einen Erweiterungskörper von k vom Grad r mit k_r. Die *Zetafunktion* von X ist die formale Potenzreihe

$$Z(X,t) := \exp\Big(\sum_{r=1}^{\infty} \frac{\#X(k_r)}{r} t^r\Big) \in \mathbb{Q}[[t]].$$

Die Definition ist ähnlich vielen Definitionen der Kombinatorik, wo abzählbar viel Information als Koeffizienten in eine formale Potenzreihe gesteckt wird. Die etwas naheliegendere Definition als $\sum_{r\geq 1} \#X(k_r)t^r$ bekommt man durch Multiplikation der logarithmischen Ableitung der Zetafunktion mit t.

Weil-Vermutungen 12.2.

i) Rationalität: $Z(X,t) \in \mathbb{Q}(t)$, ist also eine rationale Funktion.

ii) *Funktionalgleichung:*

$$Z(X, \frac{1}{q^n t}) = \pm q^{n\chi/2} t^\chi Z(X,t).$$

Zur Definition von χ siehe [1]. *Für elliptische Kurven ist $\chi = 0$.*

iii) *Analogon der Riemannschen Vermutung:*

$$Z(X,t) = \frac{P_1(t)P_3(t)\cdots P_{n-1}(t)}{(1-t)P_2(t)P_4(t)\cdots P_{2n-2}(t)(1-q^n t)}$$

wobei die $P_i(t) \in \mathbb{Z}[t]$ liegen, und als $P_i(t) = \prod(1-\alpha_{ij}t)$ geschrieben werden können, wobei $|\alpha_{ij}| = q^{i/2}$.

Die Analogie zur Riemannschen Vermutung erklärt sich für Kurven (unter anderem) folgendermassen: Man setzt $\zeta(X,s) := Z(X, q^{-s})$. Dann bedeutet (iii), dass die Nullstellen von $\zeta(X,s)$ Realteil $\frac{1}{2}$ besitzen.

Proposition 12.3. *Sei E eine elliptische Kurve über k. Dann ist*

$$Z(E,t) = \frac{1 - \varepsilon t + qt^2}{(1-t)(1-qt)},$$

dabei ist ε der Fehlerterm aus der Hasseschranke.

Beweis. Als erstes bemerken wir, dass $\varepsilon = \mathrm{tr}(\mathrm{Frob}_k)$ ist (s. auch unten). Es gilt $0 = (\mathrm{Frob}_k - \mathrm{Frob}_k)(\mathrm{Frob}_k - \widehat{\mathrm{Frob}_k}) = \mathrm{Frob}_k^2 - \mathrm{tr}(\mathrm{Frob}_k)\,\mathrm{Frob}_k + q$, also löst Frob_k die Gleichung $X^2 - \varepsilon X + q$. Die Hasseschranke $|\varepsilon| \leq 2\sqrt{q}$ ist genau die Bedingung, dass obiges Polynom über $\mathbb{C}$ zwei komplex-konjugierte Nullstellen besitzt, also

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

wobei $|\alpha| = \sqrt{q}$. Somit erhalten wir durch $\alpha \mapsto \mathrm{Frob}_k$ einen natürlichen Isomorphismus

$$\mathbb{Z}[\alpha] \longrightarrow \mathbb{Z}[\mathrm{Frob}_k] \subset \mathrm{End}(E).$$

Für alle $r \geq 1$ gilt also

$$\begin{aligned} \#E(k_r) &= \deg(\mathrm{id} - \mathrm{Frob}_{k_r}) \\ &= \deg(\mathrm{id} - \mathrm{Frob}_k^r) \\ &= q^r + 1 - \mathrm{tr}(\mathrm{Frob}_k^r) \\ &= q^r + 1 - \alpha^r - \overline{\alpha}. \end{aligned}$$

Wir können jetzt rechnen:

$$\begin{aligned} Z(E,t) &= \exp\left(\sum_{r\geq 1} \frac{\#E(k_r)}{r} t^r\right) \\ &= \exp\left(\sum_{r\geq 1} \frac{(qt)^r}{r} + \sum_{r\geq 1} \frac{t^r}{r} - \sum_{r\geq 1} \frac{(\alpha t)^r}{r} - \sum_{r\geq 1} \frac{(\overline{\alpha}t)^r}{r}\right) \\ &= \exp\Big(\log\frac{1}{1-qt} + \log\frac{1}{1-t} - \log\frac{1}{1-\alpha t} - \log\frac{1}{1-\overline{\alpha}t}\Big) \\ &= \frac{(1-\alpha t)(1-\overline{\alpha}t)}{(1-t)(1-qt)} = \frac{1-\varepsilon t + qt^2}{(1-t)(1-qt)} \end{aligned}$$

$\therefore$

Wir haben somit Teile *i*) und *iii*) der Weil-Vermutungen für elliptische Kurven beweisen können. Die Funktionalgleichung folgt im Fall der elliptischen Kurven durch einfaches Einsetzen, sie lautet

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

Literatur

[1] R. Hartshorne: Algebraic geometry. GTM 52. Springer, 1977.
[2] S. Lang: Algebra, 3rd ed. Addison-Wesley, 1993.
[3] H. Matsumura: Commutative algebra. Benjamin, 1970.
[4] J. Milne: Elliptic curves. http://www.jmilne.org/math/CourseNotes/math679.ps.gz, 1996.
[5] I. Shafarevich: Basic algebraic geometry, vol. 1, 2nd ed. Springer, 1994.
[6] J. Silverman: The arithmetic of elliptic curves. GTM 106. Springer, 1991.
[7] J. Silverman, J. Tate: Rational points on elliptic curves. UTM. Springer, 1992.
[8] M. Stoll: Elliptische Kurven I. http://www.math.uni-duesseldorf.de/~stoll/vorlesungen/Elliptische-Kurven-SS2000.pdf, 2000.