Elliptische Kurven über dem Körper $\mathbb{F}_4$ mit vier Elementen

Bachelorarbeit

Vorgelegt von

Luca Leon Happel

aus Mönchengladbach

Angefertigt am
Mathematischen Institut
der Mathematisch-Naturwissenschaftlichen Fakultät
der Heinrich-Heine-Universität Düsseldorf

04. April 2022

Betreuer: Prof. Dr. Stefan Schröer

Inhaltsverzeichnis

1 Einleitung **2**
1.1 Der Körper mit vier Elementen 6
1.2 Affiner Raum 7
1.3 Projektiver Raum 9
1.4 Projektive Kurven und ihre Morphismen 11

2 Elliptische Kurven **13**
2.1 Die allgemeine Weierstraßform 13
2.2 Das Gruppengesetz 14
2.3 Wichtige Konstanten 15
2.4 Zulässige Variablenänderungen 17

3 Isomorphe elliptische Kurven über $\mathbb{F}_4$ **18**
3.1 Nicht-singuläre Kurven in Charakteristik 2 18
3.2 Isomorphe elliptische Kurven in Charakteristik 2 21
3.3 Klassifikation der elliptischen Kurven über $\mathbb{F}_4$ 22
3.4 Abelsche Gruppen elliptischer Kurven auf $\mathbb{F}_4$ 24

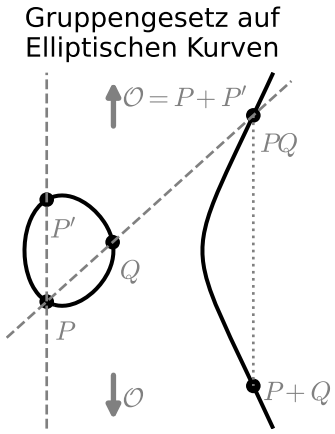
Literatur **28**

Erklärung **29**

1 Einleitung

In der Schulmathematik behandeln wir bereits einfachste polynomielle Gleichungen wie die quadratische Gleichung $ax^2 + bx + c = 0$ mit a, b, c und x als reelle Zahlen. Führen wir diesen Gedankengang weiter, gelangen wir in die abstrakte Algebra. Hier verwenden wir polynomielle Gleichungen wie $x^2 + 1 = 0$, um aus den reellen Zahlen die Komplexen zu gewinnen.

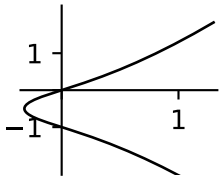
Elliptische Kurven entspringen derselben Grundidee. Sie sind die Lösungsmengen kubischer Gleichungen der Form $y^2 = x^3 + ux + v$, wobei u und v reelle Zahlen sind, sodass $4u^3 + 27v^2$ ungleich Null ist (ansonsten hätte die Kurve einen singulären Punkt). Trotz ihres Namens sind elliptische Kurven keine Ellipsen. Ihr Name stammt daher, dass sie bei der Berechnung der Bogenlänge von Ellipsen zum Tragen kommen.



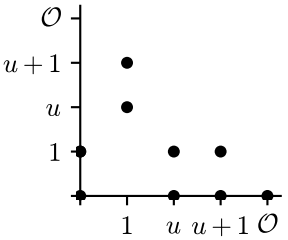
Erstaunlich ist, dass wir auf den Punkten einer elliptischen Kurve eine Addition erklären können. Wählen wir zwei Punkte P und Q, definieren wir ihre Summe durch das "Chord-Tangent group law": Wenn P und Q zwei verschiedene Punkte sind, so schneidet die Sekante welche durch P und Q geht, die elliptische Kurve in einem dritten Punkt PQ. Wenn wir PQ nun entlang der x-Achse spiegeln, erhalten wir den Punkt $P + Q$. Wenn P und Q gleich sind, betrachten wir einfach die Tangente, statt ihrer Sekante. Wenn die Gerade durch P und Q vertikal verläuft, ist der dritte Schnittpunkt ein Punkt im Unendlichen $\mathcal{O}$. Somit können wir elliptische Kurven nicht im gewohnten $\mathbb{R}^n$ betrachten und müssen in den projektiven Raum übergehen, in welchem $\mathcal{O}$ existiert.

Elliptische Kurven können jedoch nicht nur über dem Körper der reellen Zahlen definiert werden. So können wir auch einen endlichen Körper $\mathbb{F}_{p^d}$ mit p prim und d als natürliche Zahl wählen. Wir sehen rechts die elliptische Kurve zu der Gleichung $y^2 + y = x^3 + x^2 + x$ einmal für die reellen Zahlen und darunter für den endlichen Körper mit vier Elementen $\mathbb{F}_4$. Zu den acht Punkten der elliptischen Kurve über $\mathbb{F}_4$ kommt noch der Punkt im Unendlichen hinzu.

$y^2 + y = x^3 + x^2 + x$ über $\mathbb{R}$



$y^2 + y = x^3 + x^2 + x$ über $\mathbb{F}_4$



Der Beweis von Andrew Wiles des legendären "großen Satz von Fermat", welcher besagt, dass die Gleichung $a^n + b^n = c^n$ für $n > 2$ keine natür-

lichen Lösungen a, b und c hat, verwendet auch in einer zentralen Rolle die elliptischen Kurven.

Jedoch spielen die elliptischen Kurven nicht nur in der theoretischen Mathematik eine ausgesprochene Rolle. Besonders im Zusammenhang mit endlichen Körpern werden elliptische Kurven in der modernen Telekommunikation und im Internet verwendet. Angenommen wir verkaufen online ein Buch über Algebra, so wird der Käufer ein Formular mit seinen Bankdaten und anderen vertraulichen Informationen ausfüllen müssen. Damit jedoch keine Dritten diese Daten abgreifen können, müssen wir sicherstellen, dass seine Daten verschlüsselt an uns übermittelt werden. Wir betreten somit den Bereich der Kryptografie.

Bis 1975 waren alle kryptografischen Verfahren symmetrisch. Das bedeutet, ähnlich wie bei einem Ceasar-Cypher einigen sich Sender und Empfänger auf einen geheimen gemeinsamen Schlüssel, welcher das Verschlüsseln und Entschlüsseln von Nachrichten erlaubt. Diese Technik ist in unserem Fall jedoch nicht nützlich, da unser gesamter Verkehr über das Internet abgehört werden könnte (insbesondere auch der Austausch beim Einigen auf einen geheimen Schlüssel).

1976 wurde jedoch von den Amerikanern Whitefield Diffie, Matrin Hellman und Ralph Merkle die asymmetrische Kryptografie vorgeschlagen. Bei dieser gibt es einen privaten und einen öffentlichen Schlüssel. Jeder Absender kann seine Nachricht mit dem öffentlichen Schlüssel verschlüsseln, doch nur der Empfänger kann mit seinem privaten Schlüssel diese Nachrichten entschlüsseln. In unserem Fall würden wir unseren öffentlichen Schlüssel mit dem Formular verschicken, woraufhin der Käufer seine privaten Daten damit verschlüsselt an uns schickt und am Ende würden nur wir mit unserem privaten Schlüssel diese Daten entschlüsseln können.

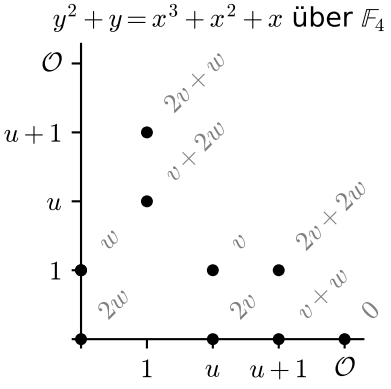
1978 wurde am MIT von Ronald Rivest, Adi Shamir und Leonard Adlermann ein Durchbruch erzielt und das RSA-Protokoll erfunden, welches die Ideen der asymmetrischen Kryptografie umsetzt. Dieses wandelt eine Nachricht zusammen mit einem öffentlichen Schlüssel injektiv in eine verschlüsselte Nachricht um. Jedoch ist, selbst wenn man den öffentlichen Schlüssel kennt, die Umkehrabbildung so schwer zu berechnen, dass selbst alle Rechner der Welt zusammen diese nicht in menschlicher Lebenszeit berechnen können, außer man besitzt den privaten Schlüssel.

RSA funktioniert in unserem Fall so: Wir einigen uns mit dem Käufer unseres Buches zuerst auf einen endlichen Körper mit t Elementen und wählen ein Element x daraus. Dieses Element soll durch wiederholtes multiplizieren auf sich selbst alle Elemente des Körpers durchlaufen – also eine primitive Einheitswurzel sein. Nun wählt der Käufer eine geheime Zahl a zwischen eins und $t-1$. Wir machen dasselbe und nennen diese Zahl b. Wir tauschen jetzt

gegenseitig unsere Werte für x^a, beziehungsweise x^b aus, woraufhin der Käufer $(x^b)^a$ berechnet und wir $(x^a)^b$. Diese Berechnungen sind äußerst effizient und nach den Potenzgesetzen haben wir beide am Ende $x^{ab} = x^{ba}$ berechnet.

Sollte indessen ein Betrüger die Kommunikation zu unserem Kunden belauscht haben, wüsste er x^a, x^b sowie x, doch der Wert x^{ab} ist ihm unbekannt! Somit kann unser Kunde nun seine privaten Daten mit unserem geheimen Wert x^{ab} als Passwort verschlüsseln und wir können es entschlüsseln.

Die einzige Möglichkeit des Betrügers wäre, aus seinen bekannten Werten x^{ab} effizient zu berechnen. Reichen würde dafür bereits aus x^a den Wert a zu bestimmen, was dem Logarithmus zur Basis x ähnelt. Dies ist das "Diskreter-Logarithmus-Problem", zu welchem es jedoch bisher noch keine effiziente Lösung gibt.



Für zusätzliche Sicherheit sollten wir t so wählen, dass es einen möglichst großen Primfaktor besitzt. Wir können es dem Betrüger bei weitem erschweren, indem wir komplexere algebraische Strukturen verwenden. Meist wird dazu die abelsche Gruppe einer elliptischen Kurve über einem endlichen Körper gewählt. Da diese Körper nur endlich viele Elemente besitzen, sind die Gruppen der Kurven auch endlich. Wählen wir unseren Körper oder unsere elliptische Kurve ungeschickt, kann das Diskrete-Logarithmus-Problem jedoch effizienter gelöst werden: So wird die Gruppe der elliptischen Kurve links von v und w erzeugt und sie ist isomorph zu $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. Egal welches x wir aus der Gruppe wählen, x^a, x^b und x^{ab} können maximal 3 verschiedene Werte sein.

Im Folgenden möchten wir diese Problematik für den Körper $\mathbb{F}_4$ genauer untersuchen. Wir fragen uns, wie viele Gruppenstrukturen auf den elliptischen Kurven über diesem Körper existieren und welche für uns nützlicher als andere sind. Dabei werden wir Techniken aus der Analysis, Algebra und Geometrie verwenden und verknüpfen. Zudem werden wir mithilfe der Diskriminante und der j-Invarianten (welche in den letzten Jahren durch die Monstergruppe und die "moonshine theory" populär wurde) zu unserem Hauptresultat vordringen:

Theorem. *Über dem Körper $\mathbb{F}_4$ gibt es bis auf Isomorphie 13 elliptische Kurven:*

j-Invariante	*Repräsentant*	*Gruppe*
1	$E_1 : y^2 + xy = x^3 + 1$	$\mathbb{Z}/8\mathbb{Z}$
1	$E_2 : y^2 + xy = x^3 + ux^2 + 1$	$\mathbb{Z}/2\mathbb{Z}$
$u+1$	$E_3 : y^2 + xy = x^3 + u$	$\mathbb{Z}/4\mathbb{Z}$
$u+1$	$E_4 : y^2 + xy = x^3 + ux^2 + u$	$\mathbb{Z}/6\mathbb{Z}$
u	$E_5 : y^2 + xy = x^3 + (u+1)$	$\mathbb{Z}/4\mathbb{Z}$
u	$E_6 : y^2 + xy = x^3 + ux^2 + (u+1)$	$\mathbb{Z}/6\mathbb{Z}$
0	$E_7 : y^2 + y = x^3$	$\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$
0	$E_8 : y^2 + y = x^3 + u$	$\mathbb{Z}/3\mathbb{Z}$
0	$E_9 : y^2 + uy = x^3$	$\mathbb{Z}/7\mathbb{Z}$
0	$E_{10} : y^2 + uy = x^3 + u$	$\mathbb{Z}/3\mathbb{Z}$
0	$E_{11} : y^2 + (u+1)y = x^3$	$\mathbb{Z}/7\mathbb{Z}$
0	$E_{12} : y^2 + (u+1)y = x^3 + 1$	$\{0\}$
0	$E_{13} : y^2 + y = x^3 + x$	$\mathbb{Z}/8\mathbb{Z}$

Unser Plan ist dabei folgender: Zuerst möchten wir die Konstruktion des Körpers mit vier Elementen wiederholen. Wir möchten auch einen kleinen Einstieg in die Theorie der affinen Varietäten machen, um den projektiven Raum und seine Varietäten behandeln zu können.

Der darauf folgende Abschnitt handelt von elliptischen Kurven. Wir möchten deren Gruppengesetz genauer betrachten, die allgemeine Weierstraßform verwenden und wichtige Invarianten kennenlernen.

Der Höhepunkt wird im dritten und letzten Abschnitt erreicht. Hier werden wir alle elliptischen Kurven über dem Körper mit vier Elementen bis auf Isomorphie klassifizieren und ihre Gruppenstrukturen berechnen.

Außerdem würde ich diese Gelegenheit gerne nutzen, um meine Danksagungen an meine Familie – insbesondere meine Mutter Sonja G. C. Happel-Hermkes meinen Vater Ferdinand L. Happel – und meine Freunde kenntlich zu machen. Ohne Ihre Unterstützung wäre diese Arbeit nie zustande gekommen.

1.1 Der Körper mit vier Elementen

Zu jeder Primzahl p und natürlichen Zahl d existiert ein endlicher Körper $\mathbb{F}_{p^d}$. Nur für im Fall $d = 1$ ergibt $\mathbb{Z}/p\mathbb{Z}$ einen Körper mit p Elementen. Wenn $d > 1$ ist, müssen wir den Polynomring durch ein irreduzibles Polynom des Grades d teilen.

Definition 1.1. Der *Körper mit vier Elementen* ist $\mathbb{F}_4 = \mathbb{F}_2[X]/(f)$ wobei (f) das Ideal zu einem irreduziblen $f = X^2 + aX + b \in \mathbb{F}_2[X]$ ist.

Aus der abstrakten Algebra wissen wir, dass die obige Konstruktion eine Körpererweiterung des $\mathbb{F}_2$ darstellt und somit, dass $\mathbb{F}_4$ von Charakteristik 2 ist. Doch wie können wir dieses (f) wählen?

Proposition 1.2. *Der Körper $\mathbb{F}_4$ ist eindeutig und hat vier Elemente $\{0, 1, u, u+1\}$, wobei $u^2 = u + 1$, $u^2 + u + 1 = 0$, $u^3 = 1$, $(u + 1)^2 + (u + 1) + 1 = 1$.*

Beweis. Nach Definition 1.1 gilt $\mathbb{F}_4 = \mathbb{F}_2[X]/(f)$ für ein irreduzibles $f \in \mathbb{F}_2[X]$ von Grad zwei. Wir möchten die Eindeutigkeit von $\mathbb{F}_4$ durch die Eindeutigkeit von f schließen und folglich durch f die vier Gleichungen beweisen.

Sei $f_{ab} = X^2 + aX + b \in \mathbb{F}_2[X]$, so bilden $f_{00}, f_{01}, f_{10}, f_{11}$ alle möglichen Kandidaten für ein irreduzibles Polynom in $\mathbb{F}_2[X]$ von Grad zwei.

$f_{00} = X^2 = X \cdot X$	ist reduzibel
$f_{01} = X^2 + 1 = X^2 + 2X + 1 = (X + 1)(X + 1)$	ist reduzibel
$f_{10} = X^2 + X = X(X + 1)$	ist reduzibel
$f_{11} = X^2 + X + 1$	ist irreduzibel

Wobei wir die Irreduzibilität von f_{11} dadurch erkennen können, dass wir bereits sämtliche Kombinationen von Polynomen ersten Grades miteinander multipliziert haben, jedoch nicht f_{11} resultierte.

Somit ist $\mathbb{F}_4$ durch $\mathbb{F}_2/(f)$ mit $f = X^2 + X + 1$ eindeutig definiert und wir können $u = X$ und $v = X^2$ wählen, wodurch wir die Gleichungen erhalten. □

Basierend auf dieser Proposition können wir die Additions- und Multiplikationstabellen für $\mathbb{F}_4$ bestimmen:

$+$	0	1	u	$u+1$
0	0	1	u	$u+1$
1	1	0	$u+1$	u
u	u	$u+1$	0	1
$u+1$	$u+1$	u	1	0

$*$	0	1	u	$u+1$
0	0	0	0	0
1	0	1	u	$u+1$
u	0	u	$u+1$	1
$u+1$	0	$u+1$	1	u

Mit diesen Tabellen können wir direkt die folgende Proposition beweisen:

Proposition 1.3. *Der Körper $\mathbb{F}_4$ besitzt einen nicht-trivialen Automorphismus gegeben durch $u \mapsto u+1$.*

Beweis. Wir wissen, dass $\mathbb{F}_2$ keine nicht-trivialen Automorphismen besitzt. Somit ist $\mathrm{Aut}(\mathbb{F}_4) \cong \mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2)$ Wir haben nun nur zwei Abbildungen, welche Automorphismen sein können: id und $\varphi(u) = u+1$. Dabei ist id klarerweise ein Automorphismus. Auch φ ist ein Körperautomorphismus, da $\varphi(u+1) = u = \varphi(u) + \varphi(1) = u+1+1 = u$. Insgesamt gilt, dass φ bijektiv ist und die multiplikative, sowie additive Struktur erhält. □

1.2 Affiner Raum

Zu einem Körper k können wir den Vektorraum k^n bilden. Dieser ist auch als *affiner Raum* $\mathbb{A}^n(k)$ oder für $n=2$ als *affine Ebene* bekannt. Wählen wir ein Polynom f aus $k[T_1, \ldots, T_n]$, dann können wir es für Punkte im affinen Raum auswerten. Dies führt uns zu dem folgenden Begriff:

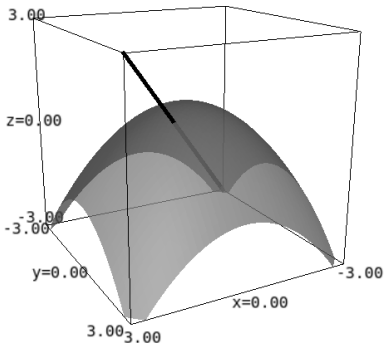
$$V(f) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n(k) \mid f(x_1, \ldots, x_n) = 0\}$$

ist die Nullstellenmenge zu f und wird auch eine *algebraische Varietät*, beziehungsweise *affine Varietät* wenn f irreduzibel ist, genannt. Analog ist $V(f_1, \ldots, f_r)$ die gemeinsame Nullstellenmenge zu f_1 bis f_r. Zu einer Teilmenge $X \subset \mathbb{A}^n(k)$ hat das Verschwindungsideal eine umgekehrte Bedeutung, da es die Menge aller Polynome ist, welche auf X verschwinden:

$$I(X) = \{f \in k[T_1, \ldots, T_n] \mid f(x_1, \ldots, x_n) = 0 \,\forall (x_1, \ldots, x_n) \in X\}$$

Proposition 1.4. *Die Menge $I(X)$ ist ein Ideal.*

Beweis. Seien $f, g \in I(X)$, $h \in k[T_1, \ldots, T_n]$. So gilt $f+g \in I(X)$ und $h \cdot f \in I(X)$. Insbesondere ist $h = -1$ möglich, wodurch $I(X)$ eine additive Gruppe mit Skalarmultiplikation aus $k[T_1, \ldots, T_n]$, also ein Ideal ist. □



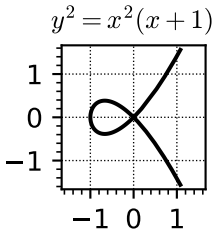
Rechts haben wir die affine Varietät $V_1 = V(\frac{1}{4}T_1^2 + \frac{1}{4}T_2^2 + T_3 - 1)$ in Grau und $V_2 = V(T_1 - T_2, T_1 - T_3)$ in Schwarz dargestellt, wobei wir erkennen, dass es einen Unterschied in der Dimension dieser gibt. Dieser Fakt scheint sich in der Anzahl der Parameter von V wieder zu spiegeln, jedoch gilt für jede Varietät über einem Körper, wenn f ein Polynom und $c \neq 0$ ist, dass $V(f) = V(c \cdot f)$ und somit insbesondere auch $V(f) = V(f, c \cdot f)$. Anhand der Parameterzahl von V können wir dessen Dimension somit nicht erschließen.

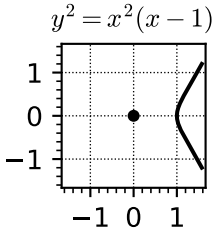
Stattdessen betrachten wir den *Koordinatenring* $k[V_1]$, beziehungsweise $k[V_2]$. Dieser ist definiert für eine beliebige Varietät $X \subset \mathbb{A}^n(k)$ als

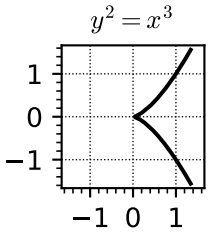
$$k[X] = k[T_1, \ldots, T_n]/I(X).$$

Die Dimension von X ist die *Krull-Dimension* dieses Ringes; also der größte Wert r für den eine Primidealkette $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_r$ in $k[X]$ existiert.

Für V_2 gilt $k[V_2] = k[T_1, T_2, T_3]/(T_1 - T_2, T_1 - T_3) \cong k[T_1]$. Hier finden wir als größte Primidealkette $(0) \subsetneq (T_1)$ und die Dimension von V_2 ist 1, so wie wir es auch geometrisch von einer Geraden erwarten.







Links sehen wir Beispiele für *Singularitäten*. Grob gesagt sind dies Punkte, an denen die Dimension lokal anders ist, als die Dimension der Varietät, auf denen sie liegen. Wir möchten diese nun rigoros definieren.

Definition 1.5. Zu einem Punkt $p = (p_1, \ldots, p_n)$ der Varietät $V(f)$ mit $f \in k[T_1, \ldots, T_n]$ ist der *Zariski-Tangentialraum* definiert als die Lösungsmenge $T_pV(f)$ des linearen Gleichungssystems

$$\sum_{i=1}^{n} \frac{\partial f}{\partial T_i}(p)(T_i - p_i).$$

Es ist klar, dass $T_pV(f)$ ein Vektorraum ist, für den stets $\dim(T_pV(f)) \geq \dim(V(f))$ gilt.

Definition 1.6. Eine *Singularität* ist ein Punkt p auf einer Varietät V mit $\dim(T_pV) > \dim(V)$

Für Kurven auf der affinen Ebene folgt daraus direkt:

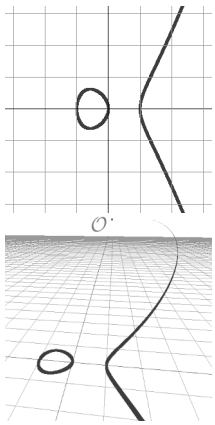
Proposition 1.7. *Sei $V(f)$ eine Kurve. Ein $p \in V(f)$ ist eine Singularität, genau dann wenn*

$$f(p) = \left.\frac{\partial f}{\partial x}\right|_p = \left.\frac{\partial f}{\partial y}\right|_p = 0.$$

Der Punkt $(0,0)$ in den drei Beispielen stellt alle möglichen Singularitäten von Kurven in der affinen Ebene dar. Das sind der Reihe nach: Ein *Doppelpunkt*, ein *isolierter Punkt* und eine *Spitze*. Man nennt nicht-singuläre Varietäten auch *glatt*.

1.3 Projektiver Raum

In der Einleitung haben wir bereits über einen Punkt im Unendlichen $\mathcal{O}$ gesprochen, welcher nicht im affinen Raum vorhanden ist und nur im *projektiven Raum* $\mathbb{P}^n$ existiert. Der $\mathbb{P}^n$ ist so konstruiert, dass die Defekte des affinen Raumes behoben werden. So sind Sätze wie "Zwei verschiedene Geraden schneiden sich stets in einem Punkt" wahr im projektiven Raum. Für die reelle projektive Ebene $\mathbb{P}^2(\mathbb{R})$ können wir uns vorstellen, dass wir für jede Schar von parallelen Geraden einen "unendlich weit entfernten Punkt", worauf all diese gemeinsam zulaufen und welcher nur am Horizont sichtbar ist, hinzufügen. Rechts ist dazu ein Beispiel, mit einer elliptischen Kurve, welche auch einen Punkt im Unendlichen $\mathcal{O}$ beinhaltet.



Definition 1.8. Der *projektive Raum* $\mathbb{P}^n(k)$ zu einem Körper k ist definiert als $(k^{n+1} \setminus \mathbf{0})/k^*$. Seine Elemente werden mit $(x_1 : \cdots : x_{n+1})$ bezeichnet.

Diese Konstruktion korrespondiert dazu, dass wir die eindimensionalen Untervektorräume von k^{n+1} als Punkte in einem neuen Raum $\mathbb{P}^n(k)$ betrachten. Die Bahnen der obigen Äquivalenzrelation zusammen mit $\mathbf{0}$ sind dabei genau diese Untervektorräume. Wie wir in unseren Darstellungen der reellen projektiven Ebene schon sehen konnten, gibt es auch eine Verbindung des projektiven n-Raumes mit dem affinen n-Raum:

Proposition 1.9. *Der $\mathbb{P}^n(k)$ ist eine n-dimensionale k-Mannigfaltigkeit.*

Beweis. Wir möchten zeigen, dass $X = \mathbb{P}^n(k)$ eine n-dimensionale k - Mannigfaltigkeit ist. Es ist bereits klar, dass X zweitabzählbar und hausdorff'sch ist. Wir zeigen nur noch, dass X lokal homöomorph zu $\mathbb{A}^n(k)$ ist. Mit Hinblick auf den kommenden Abschnitt verwenden wir dabei V_+, welches wir dort definieren werden. Dazu wählen wir die Karten $U_i = X \setminus V_+(T_i)$ mit

$X_i \in k[T_1, \ldots, T_{n+1}]$ für $1 \leq 1 \leq n+1$ zusammen mit der Kartenabbildung $\phi_i : U_i \to \mathbb{A}^n(k)$ (auch *Dehomogenisierung* genannt, beziehungsweise ϕ^{-1} *Homogenisierung*) definiert durch:

$$(p_1 : \cdots : p_{i-1} : p_i : p_{i+1} : \cdots : p_{n+1}) = \left(\frac{p_1}{p_i}, \ldots, \frac{p_{i-1}}{p_i}, \frac{p_{i+1}}{p_i}, \ldots, \frac{p_{n+1}}{p_i}\right)$$

Die ϕ_i sind somit auch *rationale Funktionen.* □

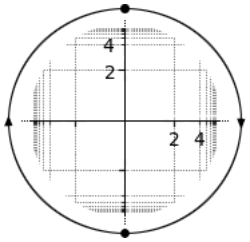
In diesem Beweis verwenden wir projektive Varietäten $V_+(T_i)$, welche wir noch genau definieren müssen. Dazu betrachten wir den graduierten Ring $R = k[T_1, \ldots, T_{n+1}]$ Ein *graduierter Ring* R ist ein Ring, welcher als direkte Summe additiver Gruppen $\bigoplus_{i=0}^{\infty} R_i$ mit $R_m R_n \subseteq R_m R_n$ zerlegt werden kann. Der Polynomring $k[T_1, \ldots, T_{n+1}]$ erhält seine Graduierung kanonisch durch den Grad deg. Ein Element f, welches in genau einem R_i liegt, nennen wir *homogen.* Für $k[T_1, \ldots, T_{n+1}]$ ist das äquivalent dazu, dass $f(\lambda x) = \lambda^d f(x)$ für alle $\lambda \in k$ und eine natürliche Zahl d, welche wir den *Grad* von f nennen, gilt.

Insbesondere gilt, wenn $x \in k^{n+1}$ und $f \in k[T_1, \ldots, T_{n+1}]$ ein homogenes Polynom mit $f(x) = 0$ ist, so wird auch $f(\lambda x) = 0$ sein. Somit können wir einem Punkt $p \in \mathbb{P}^n(k)$ eindeutig zuordnen, ob dieser eine Nullstelle des homogenen Polynoms f ist. Dies führt uns zu dem Begriff der projektiven Varietät:

$$V_+(f) = \{(x_1 : \cdots : x_{n+1}) \in \mathbb{P}^n(k) \mid f((x_1, \ldots, x_{n+1})) = 0\}$$

Indem wir nun die *homogene Zerlegung* $f = f_0 + \cdots + f_r$ für ein Element f in einem graduierten Ring $R = \bigoplus_{i=0}^{\infty} R_i$ in *homogene Komponenten* f_i betrachten, können wir *homogene Ideale* $\mathfrak{a}$ als Ideale definieren, welche zu jedem $f \in \mathfrak{a}$ auch alle homogenen Komponenten von f in $\mathfrak{a}$ haben. Diese treten beim *homogenen Verschwindungsideal* $I_+(X)$ auf, welches analog zum Verschwindungsideal im affinen Fall, für ein $X \subset \mathbb{P}^n(k)$ als homogenes Ideal aller homogenen Polynome in $k[T_1, \ldots, T_{n+1}]$, welche auf X verschwinden, definiert ist.

Gerade im Unendlichen des $\mathbb{P}^2(\mathbb{R})$



Analog können wir auch den Koordinatenring $k[V_+]$ für projektive Varietäten $V_+ \subset \mathbb{P}^n(k)$ definieren, was uns erlaubt, die Dimension und den Tangentialraum einer projektiven Varietät zu bestimmen.

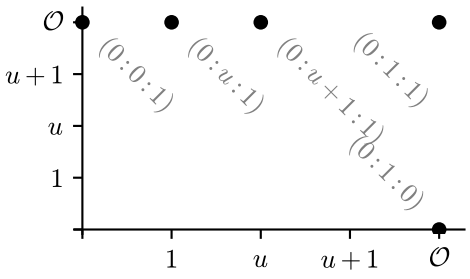
So können wir die Dimension der Geraden im Unendlichen der projektiven Ebene bestimmen. Diese ist eine *projektive Hyperebene*, das bedeutet sie ist von der Dimension genau um eins kleiner, als die des Raumes in welchem sie liegt. Die Gerade im Unendlichen ist

die Menge aller Punkte, welche wir der affinen Ebene hinzufügen müssen, um die projektive Ebene zu erhalten. Wie wir bereits in 1.9 gesehen haben, können wir die projektive Ebene zu dem affinen Raum dehomogenisieren. Dehomogenisieren wir also mittels ϕ_1 zur ersten Koordinate von $\mathbb{P}^2(k)$, so wird $\mathbb{P}^2(k) \setminus U_1$ nicht in $\mathbb{A}^2(k)$ abgebildet. Unsere Gerade im Unendlichen ist $\mathbb{P}^2(k) \setminus U_1 \cong \mathbb{P}^1(k)$, welche für den reellen Fall auch links als Kreis abgebildet ist, da $\mathbb{P}^1(R) = \mathbb{A}^1 \dot{\cup} \{\infty\}$ mit ∞ zu dem Punkt $(0:1)$ korrespondiert.

Proposition 1.10. *Die projektive Ebene über dem endlichen Körper mit vier Elementen besteht aus* 21 *Punkten.*

Beweis. Da $\mathbb{F}_4$ ein Körper ist, sind alle von Null verschiedenen Elemente invertierbar, also $\mathbb{F}_4^* = \mathbb{F}_4^\times$. Außerdem gilt $\mathbb{F}_4^\times \cong \mathbb{Z}/3\mathbb{Z}$, da u ein primitives Element ist. Da $\mathbb{F}_4^*$ frei auf $\mathbb{F}_4^3$ wirkt, gilt, dass die Länge jeder Bahn drei ist. Somit gilt $|(\mathbb{F}_4^3 \setminus \mathbf{0})/\mathbb{F}_4^*| = (4^3 - 1)/3 = 21$ □

Insbesondere haben wir, wenn wir die projektive Ebene über dem Körper mit vier Elementen nach der ersten Koordinate dehomogenisieren, eine Gerade im Unendlichen bestehend aus 5 Punkten, da $\mathbb{A}^2(\mathbb{F}_4)$ aus $4^2 = 16$ Punkten besteht und somit 5 Punkte übrig bleiben:



Die Gerade im Unendlichen des $\mathbb{P}^2(\mathbb{F}_4)$

1.4 Projektive Kurven und ihre Morphismen

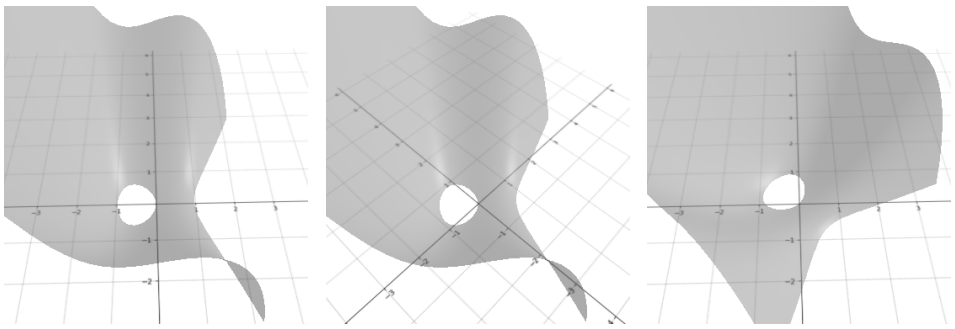
Wir bezeichnen mit dem Grad einer Kurve $V_+(f)$ über dem Körper k den Grad d des homogenen Polynoms f. Im Fall $d = 1$ nennen wir $V_+(f)$ eine Gerade und für $d = 2$ einen Kegelschnitt. Ein *K-rationaler Punkt* für eine Körpererweiterung $K \supset k$ ist ein Punkt aus $V_+(f) \subset \mathbb{P}^2(K)$. Um einfacher

über die K-rationalen Punkte einer Kurve zu reden, führen wir die Notation $C_f = V_+(f) \subset \mathbb{P}^2(k)$ ein. Wir bezeichnen die Menge aller K-rationalen Punkte der Kurve C_f als $C_f(K)$.

Es ist nun klar, sollte man einen Hintergrund in Kategorientheorie und Funktoren haben, dass C_f ein Unterfunktor des Funktors $\mathbb{P}^2 : (k-\text{Körper}) \to (\text{Set})$ von der Kategorie der Körper über k in die Kategorie der Mengen ist (Siehe [6, Kapitel 2, Absatz 2]). Und diesen Fakt möchten wir nutzen, um *projektive Transformationen* einzuführen. Ist $M : \mathbb{A}^3(k) \to \mathbb{A}^3(k)$ eine nichtsinguläre lineare Transformationen, also eine Matrix mit vollem Rang, so besitzt diese eine Inverse M^{-1} und wir können dazu assoziierte projektive Transformationen $\mathbb{P}^2(M), \mathbb{P}^2(M^{-1}) : \mathbb{P}^2(K) \to \mathbb{P}^2(K)$ bilden. Diese sind wohldefiniert, da Matrizen Geraden auf Geraden abbilden. Als Bijektionen, welche Geraden auf Geraden abbilden nennen wir die Abbildungen $\mathbb{P}^2(M)$ und $\mathbb{P}^2(M)^{-1}$ auch *Kolineationen*. Hierbei ist zu beachten, dass jedoch nicht alle Kolineationen auch projektive Transformationen sind. Über dem Körper $\mathbb{F}_4$, welcher nach Proposition 1.3 nicht-triviale Automorphismen besitzt, wirken diese als Kolineationen, jedoch nicht als projektive Transformationen auf $\mathbb{P}^2(\mathbb{F}_4)$.

Wichtig ist, dass wenn $f \in k[x, y, z]_d$ ein homogenes Polynom von Grad d ist, dass auch $f \circ M$ ein homogenes Polynom von Grad d ist und $C_{f\circ M}(K) = M^{-1}C_f(K)$. Der Grund dafür ist, dass $(f \circ M)(M^{-1}(x, y, z)) = 0$ genau dann gilt, wenn $f(x, y, z) = 0$, doch wir können dies auch direkt visuell an einem zwei-dimensionalen Beispiel erkennen, indem wir den Schnitt des Graphen von f mit der Ebene $z = 0$ betrachten:

$$f(x, y) = y^2 - x^3 + x, \quad M = \begin{pmatrix} \cos(\frac{\pi}{4}) & \sin(\frac{\pi}{4}) \\ -\sin(\frac{\pi}{4}) & \cos(\frac{\pi}{4}) \end{pmatrix}$$



(a) C_f (b) $C_{(f\circ M)}$ (c) $M^{-1}C_f$

Abbildung 3: Darstellung von $C_{f\circ M}(\mathbb{R}) = M^{-1}C_f(\mathbb{R})$ als Schnitt von Graphen mit der $Z = 0$ Ebene

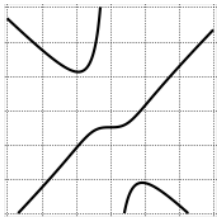
In beiden Fällen 3b und 3c sind die Schnittmengen der Graphen mit der Ebene $z = 0$ identisch. Somit bilden projektive Transformationen algebraische Kurven auf algebraische Kurven ab und erhalten dabei Grad und Irreduzibilität, da eine Abbildung M wie oben als Gruppenautomorphismus auf $k[T_1, T_2, T_3]_d$ für jeden Grad $d \in \mathbb{N}$ wirkt. Sie stellen also die Morphismen zwischen algebraischen Kurven da. Eine wichtige Folgerung daraus ist:

Proposition 1.11. *Sei C_f eine nicht-singuläre projektive kubische Kurve. Eine projektive Transformation ändert nicht die Anzahl der Singularitäten von C_f.*

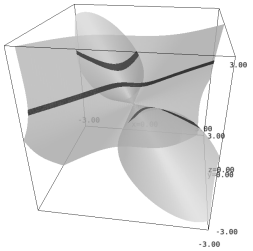
Beweis. Betrachten wir die projektive Transformation $\mathbb{P}^2(M)$ für eine nicht-singuläre Matrix M. Angenommen für die nicht-singuläre kubische Kurve C_f würde $C_{f \circ M}$ eine Singularität besitzen. Da $C_{f \circ M} = M^{-1} C_f$ ist, müsste bereits C_f eine Singularität besitzen, da M^{-1} nicht-singulär ist, da M nicht singulär ist. Dies ist ein Widerspruch. □

2 Elliptische Kurven

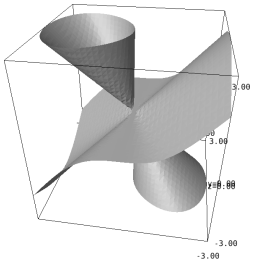
2.1 Die allgemeine Weierstraßform



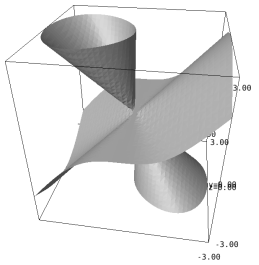
Somit kommen wir auch zum Kernthema dieser Bachelorarbeit. Die *elliptischen Kurven* sind nicht-singuläre kubische projektive Kurven. Diese haben immer einen *Inflektionspunkt*, also einen nicht-singulären Punkt, dessen Tangente seine Kurve nur ein mal schneidet. Wenden wir auf eine elliptische Kurve eine projektive Transformation an, wodurch wir ihren Inflektionspunkt zum Punkt im Unendlichen $\mathcal{O} = (0 : 1 : 0)$ verschieben, sodass die Tangente der elliptischen Kurve bei $\mathcal{O}$ die Gerade im Unendlichen ist, so erhalten wir als definierende Gleichung dieser transformierten elliptischen Kurve folgendes:

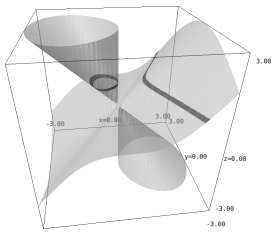


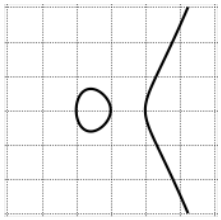
$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$



Diese Gleichung nennen wir auch *projektive allgemeine Weierstraßgleichung*. Rechts sehen wir am Beispiel der homogenisierten Gleichung von $-x^3 + \frac{1}{4}x(2y+z)^2 + \frac{1}{2}(2y+z)z^2$, wie der oben genannte Prozess zu der allgemeinen Weierstraßgleichung $Y^2Z - X^3 + XZ^2$ führt. Dabei verwenden wir $\mathbb{P}^2(M)$ mit $M = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -0.5 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.







Standardmäßig werden wir diese jedoch dehomogenisiert nach der Z-Koordinate in der affinen Ebene behandel. So erhalten wir mit der Konvention $\phi_3(X) = x$ und $\phi_3(Y) = y$ die *affine allgemeine Weierstraßgleichung*, beziehungsweise *affine allgemeine Weierstraßform*:

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

welche wir fortan benutzen werden, um elliptische Kurven aufzuschreiben. Dabei steht E für die Lösungsmenge der Gleichung. Links sehen wir, wie aus der allgemeinen Weierstraßform die affine allgemeine Weierstraßform gewonnen wird. Wäre die Charakteristik des Körpers über dem wir diese Gleichung betrachten ungleich 2, so könnten wir noch eine kürzere Gleichung - die *kurze Weierstraßgleichung* - konstruieren. Doch da wir uns für den Körper mit vier Elementen interessieren, ist dies nicht relevant für uns.

Wir möchten bei der allgemeinen Weierstraßform nur einen Punkt im Unendlichen haben, welcher ein Inflektionspunkt ist und als Tangente die Gerade im Unendlichen hat, damit wir die folgende Gruppenstruktur später einfacher anwenden können.

2.2 Das Gruppengesetz

Das *Chord-Tangent group law*, welches in der Einführung bereits kurz erwähnt wurde und ein Gruppengesetz auf den elliptischen Kurven definiert, entspringt folgendermaßen: Sei C_f eine elliptische Kurve. Wählen wir eine Gerade $L \subset \mathbb{P}^2$ aus, so schneidet sie die elliptische Kurve 3 mal nach Bezout's Theorem, da C_f eine kubische Kurve ist. Dabei ist wichtig, sollte L eine Tangente von C_f am Punkt P sein, so wird P doppelt gezählt.

Definition 2.1. Wir definieren auf der elliptischen Kurve C_f eine binäre Operation durch

$$+ : C_f \times C_f \longrightarrow C_f, \quad P + Q = (PQ)\mathcal{O}$$

Dabei bezeichnet PQ den dritten Schnittpunkt der Geraden L durch P und Q, beziehungsweise der Tangente an P, sollte $P = Q$ sein, mit der elliptischen Kurve C_f.

Proposition 2.2. *Durch die oben definierte Operation wird C_f zu einer abelschen Gruppe.*

Beweis. 1. Die Kommutativität folgt daraus, dass die Gerade PQ durch P und Q dieselbe ist wie QP durch Q und P.

2. Dazu funktioniert $\mathcal{O}$ als das neutrale Element, denn für einen Punkt $P \in C_f$ geht die Gerade durch P und $\mathcal{O}$ nur noch durch einen dritten Punkt $P\mathcal{O}$. Wenn wir nun die Gerade durch $P\mathcal{O}$ und $\mathcal{O}$ betrachten, so muss diese ihren dritten Schnittpunkt wieder bei P haben. Also gilt $P + \mathcal{O} = (P\mathcal{O})\mathcal{O} = P$

3. Zu einem $P \in C_f$ existiert auch ein inverses $-P$ mit der Eigenschaft $P + (-P) = \mathcal{O}$. Wählen wir $-P$ als $P\mathcal{O}$, so sehen wir durch die Kommutativität von $+$ und dadurch, dass $\mathcal{O}$ das neutrale Element ist, dass $\mathcal{O} = (P + \mathcal{O}) + PQ = P + (-P)$.

4. Zuletzt ist der Beweis der Assoziativität in [1, Kapitel 7] zu finden.

□

Diese Gruppe ist zudem immer von Rang 1, also zyklisch, oder Rang 2, also das Produkt zweier zyklischer Gruppen. Eine sehr einfache Folgerung, deren Beweis direkt aus den obigen Sätzen folgt, ist:

Korollar 2.3. *Sind $P, Q, R \in C_f$ Punkte auf einer Geraden, so gilt: $P+Q+R = \mathcal{O}$*

Nun können wir auch erklären, warum wir die allgemeine Weierstraßform einer elliptischen Kurve E so gewählt haben, dass ihr Inflektionspunkt der Punkt im Unendlichen $\mathcal{O}$ und seine Tangente die Gerade im Unendlichen ist. Rechts sehen wir am Beispiel der elliptischen Kurve mit Weierstraßform $y^2 = x^3 - x$ im Reellen wieso: Dadurch, dass der Inflektionspunkt und seine Tangente im Unendlichen liegen, können wir unter der Dekomposition $\mathbb{P}^2 = \mathbb{A}^2 \dot\cup \mathbb{P}^1$ sehen, dass alle Punkte welche nicht trivial auf E wirken in $\mathbb{A}^2$ liegen. Lediglich das neutrale Element $\mathcal{O}$ liegt fernab auf der projektiven Gerade.

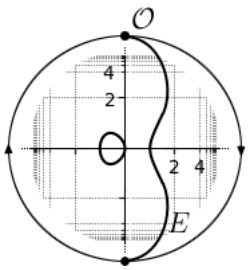


Abbildung 4: $E : y^2 = x^3 - x \subset \mathbb{P}^2 = \mathbb{A}^2 \dot\cup \mathbb{P}^1$

2.3 Wichtige Konstanten

Nun stellt sich uns die Frage, ob unter einer projektiven Transformation die Gruppenstruktur erhalten bleibt? Erstaunlicherweise ist die Antwort ja, was daran liegt, dass projektive Transformationen auch Kolineationen sind.

Jedoch muss eine projektive Transformation nicht den Punkt im Unendlichen der elliptischen Kurve bei $\mathcal{O} = (0 : 1 : 0)$, oder als Inflektionspunkt belassen.

Wir fragen uns jedoch, welche projektiven Transformationen den Punkt im Unendlichen unverändert lassen und ihn als Inflektionspunkt mit der Geraden im Unendlichen als Tangente beibehalten. Werden diese Eigenschaften nämlich erhalten, so wird auch die transformierte elliptische Kurve in allgemeiner Weierstraßform sein.

Definieren wir dafür zuerst ein paar nützliche Konstanten zu einer frei wählbaren kubischen Kurve E in affiner allgemeiner Weierstraßform, welche durch quadratische Ergänzung auftreten:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \end{aligned}$$

Diese Werte stehen dabei durch $4b_8 = b_2b_6 - b_4^2$ in Relation und führen uns zu dem Begriff der Diskriminanten:

Definition 2.4. Sei E eine projektive kubische Kurve in allgemeiner Weierstraßform. Wir definieren zu E die Diskriminante Δ durch:

$$\Delta = \Delta(E) = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

Die Diskriminante ist, wie wir noch sehen werden, dadurch für uns von Bedeutung, dass sie uns ein einfaches Kriterium liefert, welches uns entscheiden lässt, ob eine kubische Kurve nicht-singulär (also eine elliptische Kurve) ist, oder nicht. Darauf werden wir im nächsten Abschnitt beim Untersuchen der Bedingungen für Glätte einer kubischen Kurve eingehen und dies speziell für den Körper mit vier Elementen beweisen. Außerdem definieren wir jetzt noch die Konstanten, welche durch kubische Ergänzung auftreten:

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 21b_6 \end{aligned}$$

mit der Relation $12^3\Delta = c_4^3 - c_6^2$. Diese führen uns – sollte $\Delta(E)$ invertierbar sein – zu der j-Invarianten.

Definition 2.5. Zu einer projektiven kubischen Kurve mit invertierbarer Diskriminante definieren wir die j-Invariante als:

$$j = j(E) = \frac{c_4^3}{\Delta} = 12^3\frac{c_4^3}{c_4^3 - c_6^2}$$

Doch wieso nennen wir diese Konstante eine Invariante? Wir haben bereits die projektiven Transformationen als Morphismen der projektiven Varietäten und insbesondere der elliptischen Kurven beschrieben. Somit sind zwei elliptische Kurven C_f und C_g isomorph, wenn diese isomorph als projektive Varietäten sind, also Morphismen $\varphi : C_f \to C_g$ und $\psi : C_g \to C_f$ existieren, sodass deren Kompositionen $\varphi \circ \psi$ und $\psi \circ \varphi$ die Identitäten auf C_f, beziehungsweise C_g sind. Wir können somit bei einer Isomorphie von zwei elliptischen Kurven diese umkehrbar eindeutig aufeinander durch eine projektive Transformation abbilden. Die j-Invariante ist nun genau zu diesen Isomorphien invariant. Das bedeutet, alle isomorphen Kurven haben dieselbe j-Invariante. Sollte der zugrunde liegende Ring dieser Kurven zudem algebraisch abgeschlossen sein, so gilt sogar die Rückrichtung [3] und zwei elliptische Kurven sind isomorph, genau dann, wenn ihre j-Invariante gleich ist. Ein Beweis dazu folgt im kommenden Abschnitt. Außerdem gilt, sind zwei elliptische Kurven isomorph, so sind auch deren abelschen Gruppen isomorph. Wie wir auch noch sehen werden, können wir jedoch nicht durch isomorphe abelsche Gruppen elliptischer Kurven darauf schließen, dass diese elliptischen Kurven isomorph sind[8].

2.4 Zulässige Variablenänderungen

Angenommen wir haben eine elliptische Kurve E, welche ihren Inflektionspunkt im Punkt im Unendlichen $\mathcal{O} = (0 : 1 : 0)$ hat und dessen Tangente die Gerade im Unendlichen ist. Betrachten wir die affine Weierstraßform dieser Kurve, so fragen wir uns, welche projektiven Transformationen diese Eigenschaften beibehalten. Dazu betrachten wir Folgendes:

Definition 2.6. Eine *zulässige Variablenänderung* in der affinen Weierstraßgleichung einer elliptischen Kurve C_f mit $f \in k[x, y]$ hat die Form:

$$x = u^2\bar{x} + r, \quad y = u^3\bar{y} + su^2\bar{x} + t$$

mit u, r, s und t in k und u invertierbar.

Dabei ist die Betrachtung $x \mapsto u^2\bar{x} + r$ und $y \mapsto u^3\bar{y} + su^2\bar{x} + t$ als "Variablenänderung" eine äquivalente Sichtweise zu der, dass dies eine projektive Transformation ist. Die wichtigste Eigenschaft dieser Variablenänderungen, welche sie "zulässig" macht, ist folgende:

Proposition 2.7. *Substitution durch eine zulässige Variablenänderung der Variablen wie in 2.6 einer elliptischen Kurve in affiner allgemeiner Weierstraßgleichung:*

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

führt zu der neuen elliptischen Kurve in affinen allgemeinen Weierstraßgleichung:

$$\bar{y}^2 + \bar{a}_1\bar{x}\bar{y} + \bar{a}_3\bar{y} = \bar{x}^3 + \bar{a}_2\bar{x}^2 + \bar{a}_4\bar{x} + \bar{a}_6$$

mit den Relationen:

$$\begin{aligned}
u\bar{a}_1 &= a_1 + 2s \\
u^2\bar{a}_2 &= a_2 - sa_1 + 3r - s^2 \\
u^3\bar{a}_3 &= a_3 + ra_1 + 2t \\
u^4\bar{a}_4 &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st \\
u^6\bar{a}_6 &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - rta_1 - t^2
\end{aligned}$$

Beweis. Da die Länge des Beweises durch seine langwierigen Rechnungen den Rahmen dieser Arbeit sprengen würde, verweisen wir auf [1, Kapitel III Absatz 1] □

Direkt daraus folgt auch, dass $u^3\bar{c}_4 = c_4$, $u^6\bar{c}_6 = c_6$, $u^{12}\bar{\Delta} = \Delta$ und insbesondere $\bar{j} = j$, was die Invarianz der j-Invarianten unter zulässigen Variablenänderungen, beweist.

Die zulässigen Variablenänderungen sind somit die projektiven Transformationen, welche den Punkt im Unendlichen erhalten und auch die Tangente dessen, als Gerade im Unendlichen beibehalten. Man nennt solche projektiven Transformationen elliptischer Kurven, welche den Punkt im Unendlichen und seine Tangente, sowie die Gruppenstruktur unverändert lassen auch *Isogenien*. Die Kompositionen und das Inverse zulässiger Variablenänderungen sind auch wieder zulässige Variablenänderungen, da diese projektive Transformationen sind. Insbesondere gilt, dass eine zulässige Variablenänderung $\varphi : E \to \bar{E}$ auch eine affine lineare Transformation ist, wodurch für P und Q auf E gilt, dass $\varphi(P + Q) = \varphi(P) + \varphi(Q)$, wodurch zulässige Variablenänderung Gruppenisomorphismen sind.

Aufgrund dessen bezeichnen wir die zulässigen Variablenänderungen im folgenden als Isomorphismen elliptischer Kurven in affiner Weierstraßform.

3 Isomorphe elliptische Kurven über $\mathbb{F}_4$

3.1 Nicht-singuläre Kurven in Charakteristik 2

Wir haben bereits gesehen, dass zu jeder elliptischen Kurve eine affine allgemeine Weierstraßform mit Punkt im Unendlichen $\mathcal{O} = (0 : 1 : 0)$ existiert, welcher nicht in der affinen Ebene liegt. Nun möchten wir wissen, zu welcher affinen Weierstraßform eine elliptische Kurve mit Punkt im Unendlichen wie gerade beschrieben gehört.

Proposition 3.1. *Zu jeder affinen allgemeinen Weierstraßgleichung f ist der einzige Punkt im Unendlichen, welcher auf der korrespondierenden Kurve C_f liegt der Punkt* $(0:1:0)$.

Beweis. Betrachte die affine allgemeine Weierstraßgleichung $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ und homogenisiere sie zur projektiven allgemeinen Weierstraßgleichung $Y^2Z+a_1XYZ+a_3YZ^2 = X^3+a_2X^2Z+a_4XZ^2+a_6Z^3$. Nachrechnen ergibt, dass $(0:1:0)$ eine Lösung ist. Es kann keine weitere Lösung auf der Geraden im Unendlichen $Z=0$ existieren, da wenn wir $Z=0$ einsetzen, nur $0=X^3$ übrig bleibt. Somit muss für einen Punkt im Unendlichen die X-Koordinate Null sein. Auch kann die Y-Koordinate nicht Null sein, da $(0:0:0)$ nicht in der projektiven Ebene liegt. Somit ist der einzige Punkt im Unendlichen einer allgemeinen Weierstraßgleichung $\mathcal{O} = (0:1:0)$. □

Jedoch muss die kubische Kurve C_f, welche zu der allgemeinen Weierstraßgleichung f korrespondiert auch nicht-singulär sein, damit C_f eine elliptische Kurve ist. Wir schränken nun unsere Sicht auf einen Körper k mit Charakteristik 2 – wie den Körper mit vier Elementen – ein, wo uns folgende Proposition hilft:

Proposition 3.2. *Die Kurve korrespondierend zu einer allgemeinen Weierstraßgleichung über einem Körper k mit Charakteristik 2 ist nicht-singulär, wenn ihre Diskriminante nicht Null ist.*

Beweis. Sei $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$ eine affine allgemeine Weierstraßgleichung konstruiert zu der Kurve E. Nach Proposition 1.11 reicht es aus diese auf Singularitäten zu prüfen.

1. Fall $j \neq 0$: Dieser Fall tritt genau dann ein, wenn $a_1 \neq 0$ ist. Das liegt daran, weil in Charakteristik 2 die ausgegrauten Terme wegfallen:

$$\begin{aligned} j &= \frac{c_4^3}{\Delta} \\ c_4 &= b_2^2 - 24b_4 \\ b_2 &= a_1^2 + 4a_2 \end{aligned}$$

   Wir wählen nun eine Konstante $c \in k$ und wenden die zulässige Variablenänderung $x \mapsto x+c,\ y \mapsto y$ an. Dadurch wird:

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

   zu

$$\bar{y}^2+a_1\bar{x}\bar{y}+(a_1c+a_3)\bar{y} = \bar{x}^3+a_2\bar{x}^2+a_4\bar{x}+a_6.$$

Wenn a_1 ungleich Null ist können wir also durch eine passende Wahl von c als a_3/a_1 eine zulässige Variablenänderung finden, welche unsere allgemeine Weierstraßform so umformt, dass kein a_3y Term mehr vorhanden ist:

$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x + a_6.$$

Wenden wir jetzt die zulässige Variablenänderung $x \mapsto a_1^3x$, $y \mapsto a_1^3y$ an, so können wir diese resultierende Gleichung durch $a_1 = 1$ normalisieren. So erhalten wir:

$$y^2 + xy = x^3 + a_2x^2 + a_4x + a_6.$$

Indem wir indessen $s = -a_4$ in einer zulässigen Variablenänderung wählen, erhalten wir eine isomorphe Kurve mit allgemeiner Weierstraßform:

$$y^2 + xy = x^3 + a_2x^2 + a_6.$$

Hieraus folgt $b_2 = a_1^2 = 1, b_4 = 0a_1+2a_4 = 0 = 0^2+4a_6 = b_6$ und $b_8 = a_4^2$ durch die Definition der b_2, b_4, b_6 und b_8. Außerdem vereinfacht sich Δ zu a_6, da $c_4 = 1$ ist. Nach Proposition 1.7 existiert eine Singularität, wenn $\frac{\partial f}{\partial x} = y + x^2$, $\frac{\partial f}{\partial y} = x$ und $f = y^2 + xy - x^3 - a_2x^2 - a_6$ eine gemeinsame Nullstelle besitzen. Die Terme $y + x^2$ und x teilen sich nur bei $(0, 0)$ eine Nullstelle. Diese ist auch eine Nullstelle von f, wenn ihr konstanter Term a_6 Null ist.

Somit ist eine kubische Kurve in allgemeiner Weierstraßform mit $j \neq 0$ genau dann glatt, wenn Δ ungleich Null ist und dieser Fall stimmt.

2. Fall $j = 0$: Analog zum obigen Fall wissen wir, dass $a_1 = 0$ sein muss. Außerdem erhalten wir durch kubische Ergänzung:

$$y^2 + a_3y = x^3 + a_4x + a_6$$

Hieraus folgt $b_2 = b_4 = 0, b_6 = a_3^2$ und $b_8 = a_4^2$, woraus folgt, dass $c_4 = 1$ und $\Delta = a_3^4$ sowie $j = 0$. Berechnen wir wieder wie im obigen Fall $\frac{\partial f}{\partial x} = x^2 + a_4$, $\frac{\partial f}{\partial y} = a_3$ sehen wir direkt, dass die Kurve genau dann nicht-singulär ist, wenn $a_3 \neq 0$, beziehungsweise weil k als Körper keine nilpotenten Elemente besitzt, wenn $\Delta \neq 0$ ist. Somit stimmt auch dieser Fall.

□

Korollar 3.3. *Die affine allgemeine Weierstrassform einer elliptischen Kurve E vereinfacht sich für $j(E) \neq 0$ zu $y^2 + xy = x^3 + a_2x^2 + a_6$ und für $j = 0$ zu: $y^2 + a_3y = x^3 + a_4x + a_6$.*

3.2 Isomorphe elliptische Kurven in Charakteristik 2

Wann sind zwei elliptische Kurven E und $\bar{E}$ isomorph über einem Körper k mit Charakteristik 2? Auf jeden Fall muss $j(E) = j(\bar{E})$ gelten, da j invariant unter Isomorphismen elliptischer Kurven ist. Nun vereinfacht sich die Frage auf die Fälle $j \neq 0$ und $j = 0$:

Fall $j \neq 0$: Wie wir bereits aus Proposition 3.2 wissen, ist dieser Fall gleichbedeutend mit $a_1 \neq 0$. Dank 3.3 wissen wir, dass E und $\bar{E}$ bis auf Isomorphie folgendermaßen beschrieben werden können:

$$E : y^2 + xy = x^3 + a_2x^2 + a_6$$
$$\bar{E} : y^2 + xy = x^3 + \bar{a}_2x^2 + \bar{a}_6$$

Somit sind E und $\bar{E}$ isomorph, sollte es eine zulässige Variablenänderung $f : E \to \bar{E}$ geben. Angenommen $f(x) = u^2x + r$ so würde sich die Gleichung von E unter f zu

$$y^2 + u^2xy + ry = \left(r + u^2x\right)^3 + a_2\left(r + u^2x\right)^2 + a_6$$

ändern. Insbesondere sehen wir einen ry Term. Da dieser Null sein muss, gilt somit $r = 0$. Auch muss das x auf der linken Seite der Gleichung normiert bleiben, wodurch $u = 1$ gelten muss. Somit muss $f(x) = x$.

Betrachten wir nun $f(y) = u^3y + su^2x + t = y + sx + t$, so ändert sich E unter f zu:

$$(sx + t + y)^2 + x(sx + t + y) = x^3 + a_2x^2 + a_6$$

was nach Ausklammern zu

$$y^2 + t^2 + tx + xy + (s^2 + s)x^2 = x^3 + a_2x^2 + a_6$$

wird. Wir sehen, dass ein tx Term vorkommt, welcher nicht in der Gleichung von $\bar{E}$ erscheint. Somit muss $t = 0$ gelten, wodurch wir folgendes nach einer Umformung erhalten:

$$y^2 + xy = x^3 + (a_2 - (s^2 + s))x^2 + a_6.$$

Daraus folgt, dass $f(y) = y + sx$ gilt. Aus diesen Ergebnissen folgern wir direkt:

Lemma 3.4. *Es existiert ein Isomorphismus $f : E \to \bar{E}$ für $j(E) = j(\bar{E}) \neq 0$ mit affiner allgemeiner Weierstraßform wie oben genau dann, wenn es ein $s \in k$ gibt, für welches $a_2 - (s^2 + s) = \bar{a}_2$, beziehungsweise $s^2 + s = \bar{a}_2 - a_2$ gilt.*

Natürlicherweise folgt daraus, dass in einer Körpererweiterung $K \supset k$ in welcher diese Bedingungen gilt, auch E und $\bar{E}$ isomorph werden, sollten sie es nicht bereits in E gewesen sein. Hierbei erinnern wir noch einmal daran, dass sollte k algebraisch abgeschlossen sein, so folgt aus der gleichen j-Invarianten zweier elliptischer Kurven ihre Isomorphie.

Hinsichtlich des Körpers $\mathbb{F}_4$ ist das Bild der Funktion $s \mapsto s^2 + s$ nur $\{0, 1\}$. Daher gilt trivialerweise:

Proposition 3.5. *In dem Körper $\mathbb{F}_4$ existiert ein Isomorphismus zwischen zwei elliptischen Kurven E und $\bar{E}$ mit $j(E) = j(\bar{E}) \neq 0$ nur, wenn $\bar{a}_2 - a_2$ gleich 1 oder 0 ist.*

Aus obigem Lemma folgt auch direkt, dass in einem Körper, welcher die quadratische Gleichung $s^2 + s = \bar{a}_2 - a_2$ erfüllt, die Automorphismengruppe $\mathrm{Aut}(E)$ isomorph zu $\mathbb{Z}/2\mathbb{Z}$ ist.

Fall $j = 0$: Wie im vorherigen Fall ist dieser Fall äquivalent zu $a_1 = 0$ und gehen wir analog vor, erkennen wir, dass $f(x) = u^2x$ und $f(y) = u^3y + su^2x + t$ gilt. Dazu muss es $u, r, s, t \in k$ wie in 2.6 geben, für welche die folgenden Gleichungen stimmen:

$$\begin{aligned} u^3\bar{a}_3 &= a_3 \\ u^4\bar{a}_4 &= a_4 + sa_3 + s^4 \\ u^6\bar{a}_6 &= a_6 + s^2a_4 + ta_3 + s^6 + r^2 \end{aligned}$$

Somit erhalten wir die Schlüsselaussage:

Lemma 3.6. *Es existiert ein Isomorphismus $f : E \to \bar{E}$ für $j(E) = j(\bar{E}) = 0$ mit affiner allgemeiner Weierstraßform wie oben genau dann, wenn $u^3 = \frac{a_3}{\bar{a}_3}$ eine Kubikwurzel in k besitzt, sowie die separable Gleichung vierten Grades $s^4 + a_3t + a_4 + u^4\bar{a}_4 = 0$ eine Lösung in s besitzt und die quadratische Gleichung $t^2 + a_3t + (s^6 + s^2a_4 + a_6 + u^6\bar{a}_6) = 0$ eine Lösung in t besitzt.*

Interessant mit Blick auf den Körper $\mathbb{F}_4$ ist hierbei, dass, wie wir es bereits im Beweis von 1.10 gesehen haben, jedes Element sich selbst als Kubikwurzel hat.

Betrachten wir nun eine Körpererweiterung $K \supset k$ in welcher stets die Lösungen, welche in 3.6 gefordert sind, vorhanden sind. Dort gilt somit $\mathrm{Aut}(E) \cong Q_8$, wobei $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ die Einheitengruppe der ganzzahligen Quaternionen ist.

3.3 Klassifikation der elliptischen Kurven über $\mathbb{F}_4$

Wir möchten nun alle elliptischen Kurven über dem Körper mit vier Elementen klassifizieren. Das Resultat dessen ist das Hauptresultat dieser Bachelorarbeit:

Theorem 3.7. *Über dem Körper $\mathbb{F}_4$ gibt es bis auf Isomorphie 13 elliptische Kurven:*

j-Invariante	*Repräsentant*
1	$E_1 : y^2 + xy = x^3 + 1$
1	$E_2 : y^2 + xy = x^3 + ux^2 + 1$
$u+1$	$E_3 : y^2 + xy = x^3 + u$
$u+1$	$E_4 : y^2 + xy = x^3 + ux^2 + u$
u	$E_5 : y^2 + xy = x^3 + (u+1)$
u	$E_6 : y^2 + xy = x^3 + ux^2 + (u+1)$
0	$E_7 : y^2 + y = x^3$
0	$E_8 : y^2 + y = x^3 + u$
0	$E_9 : y^2 + uy = x^3$
0	$E_{10} : y^2 + uy = x^3 + u$
0	$E_{11} : y^2 + (u+1)y = x^3$
0	$E_{12} : y^2 + (u+1)y = x^3 + 1$
0	$E_{13} : y^2 + y = x^3 + x$

Beweis. Wir betrachten wieder zwei Fälle, je nachdem, ob die j-Invariante einer elliptischen Kurve E über dem Körper mit vier Elementen $\mathbb{F}_4$ null oder nicht-null ist.

1. Fall $j \neq 0$: Nach 3.3 können wir annehmen, dass E bis auf Isomorphie die Form $y^2 + xy = x^3 + a_2x^2 + a_6$ hat. Nach 3.2 muss dabei a_6 ungleich Null sein.

   Wählen wir $a_2 = 0$ und $a_6 = 1$ erhalten wir $E_1 : y^2 + xy = x^3 + 1$. Aus 3.5 folgt, dass $E_1 \cong E_1' : y^2 + xy = x^3 + x^2 + 1$ jedoch die elliptische Kurve $E_2 : y^2 + xy = x^3 + ux^2 + 1$ mit $E_2 \cong E_2' : y^2 + xy = x^3 + (u+1)x^2 + 1$ nicht isomorph zu E_1 ist.

   Wählen wir nun $a_2 = 0$ und $a_6 = u$, so erhalten wir $E_3 : y^2 + xy = x^3 + u$. Da sich die j-Invariante einer Kurve unter einer zulässigen Variablenänderung nicht ändert, ist diese Kurve nicht isomorph zu E_1 oder E_2 und analog wie im obigen Fall erhalten wir die nicht-isomorphe Kurve $E_4 : y^2 + xy = x^3 + ux^2 + u$

   Zu guter Letzt wählen wir noch $a_2 = 0$ und $a_6 = (u+1)$, wodurch wir $E_5 : y^2 + xy = x^3 + (u+1)$ erhalten, wobei diese Kurve wiederum nicht-isomorph zu der elliptischen Kurve $E_6 : y^2 + xy = x^3 + ux^2 + (u+1)$ nach denselben Gründen wie oben ist.

   Wir finden die j-Invarianten der jeweiligen elliptischen Kurven durch simples Ausrechnen mittels ihrer Formel aus 2.5.

2. Fall $j = 0$: Nach 3.3 muss die affine allgemeine Weierstraßform von E bis auf Isomorphie $y^2 + a_3y = x^3 + a_4x + a_6$ sein. Dazu gilt nach 3.2, dass $a_3 \neq 0$ ist, da $a_3^3 = \Delta \neq 0$.

   Wählen wir daher $a_3 = 1$, $a_4 = 0$ und $a_6 = 0$, was uns die elliptische Kurve $E_7 : y^2+y = x^3$ liefert. Mittels 3.6 können wir herausfinden, welche Variablenänderungen zulässig sind. Indem wir alle nicht-zulässigen Variablenänderungen betrachten, finden wir alle nicht-isomorphen Kurven. Insbesondere nutzen wir dabei, dass $x \mapsto x^4$ die Identität auf $\mathbb{F}_4$ ist, sowie dass die Abbildung $x \mapsto x^6$ genau wie $x \mapsto x^3$ in $\mathbb{F}_4$ jedes Element außer 0 auf 1 schickt. Somit existiert eine zulässige Variablenänderung $y \mapsto vy + sv^2x + t$ genau dann, wenn es $v, r, s, t \in k$ mit $v \neq 0$ gibt, sodass $s + a_3t + a_4 + v\bar{a}_4 = 0$ eine Lösung in s, sowie $t^2 + a_3t + (s^6 + s^2a_4 + a_6 + \bar{a}_6) = 0$ eine Lösung in t besitzt.

   Für unsere Wahl $a_3 = 1$, $a_4 = 0$ und $a_6 = 0$ bedeutet das, $t + v\bar{a}_4 = s$ und $t^2 + t + (s^6 + \bar{a}_6) = 0$. Wählen wir $\bar{a}_4 = 0$ so erhalten wir $t = s$ und die Gleichung $t^2 + t + t^6 = \bar{a}_6$ hat nur für $\bar{a}_6 = 0$ oder $\bar{a}_6 = 1$ eine Lösung. Somit ist die Kurve $E_8 : y^2 + y = x^3 + u \cong y^2 + y = x^3 + u$ nicht isomorph zu E_7.

   Da nach 3.6 $u^3\bar{a}_3 = a_3$ für eine zulässige Variablenänderung gelten muss, wobei sich das in $\mathbb{F}_4$ zu $\bar{a}_3 = a_3$ vereinfacht, können wir nun $\bar{a}_3 \neq a_3$ betrachten, um nicht-isomorphe elliptische Kurven zu erhalten.

   So kann es zu der elliptischen Kurve mit $a_3 = u$, $a_4 = 0$ und $a_6 = 0$, also $E_9 : y^2 + uy = x^3$ keinen Isomorphismus von E_7 oder E_8 geben. Gehen wir analog wie im vorherigen Fall vor, erhalten wir $E_{10} : y^2+uy = x^3+u$, wobei E_{10} nicht isomorph zu E_9, E_8 und $_7$ sein kann.

   Analog finden wir für $a_3 = u + 1$ die nicht-isomorphen elliptischen Kurven $E_{11} : y^2 + (u + 1)y = x^3$ und $E_{12} : y^2 + (u + 1)y = x^3 + 1$

   Zuletzt erkennen wir, würde man bei einer der Kurven E_7, E_8, E_9, E_{10}, E_{11}, E_{12} für eine zulässige Variablenänderung $\bar{a}_4 \neq 0$ wählen, so erhalten wir zu der Gleichung $t^2 + a_3t + (s^6 + s^2a_4 + a_6 + \bar{a}_6) = 0$ mit $t = \bar{a}_4 + s$ keine Lösung. Dies liefert uns $E_{13} : y^2 + y = x^3 + x$ eine neue Isomorphieklasse elliptischer Kurven und wir haben alle möglichen nicht-zulässigen Variablenänderungen in $\mathbb{F}_4$ ausprobiert.

   □

3.4 Abelsche Gruppen elliptischer Kurven auf $\mathbb{F}_4$

Zuletzt können wir noch die Isomorphieklassen der elliptischen Kurven darstellen. Interessant ist dies für uns unter Betrachtung des RSA-Verfahrens,

welches wir in der Einleitung kennengelernt haben. Angenommen es wird dieses angewandt und zwei Personen einigen sich auf eine elliptische Kurve über dem Körper $\mathbb{F}_4$, sowie einen Punkt P darauf. Nun werden aP und bP mit a und b als natürliche Zahlen, von den verschiedenen Personen generiert und ausgetauscht. Aus der Einleitung wissen wir, dass diese zwei Personen nun das Geheimnis abP teilen. Möchten wir dieses als Angreifer herausfinden, wäre es sehr nützlich zu wissen, welche Werte xP für ein natürliches x auftreten können und wie diese zusammenhängen. Dazu wählen wir zu jeder Isomorphieklasse einen Repräsentanten und konstruieren zu diesem, genauso wie in der Einleitung, eine Grafik, welche die Gruppenstruktur darstellt. Außerdem können wir, da wir wissen, dass die auftretenden Gruppen stets zyklisch von maximal Rang zwei sind, durch Ausprobieren einen, beziehungsweise zwei Erzeuger finden.

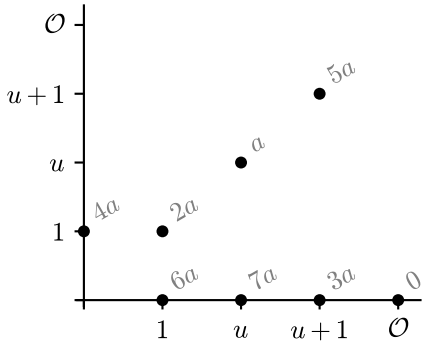
Die Anzahl der rationalen Punkte auf einer elliptischen Kurve E über $\mathbb{F}_{q^p}$ ist durch folgendes Theorem eingeschränkt:

Theorem 3.8 (Riemann-Hypothese für elliptische Kurven (Hasse, 1934))**.** *Sei E eine elliptische Kurve über $\mathbb{F}_q$. Dann gilt*

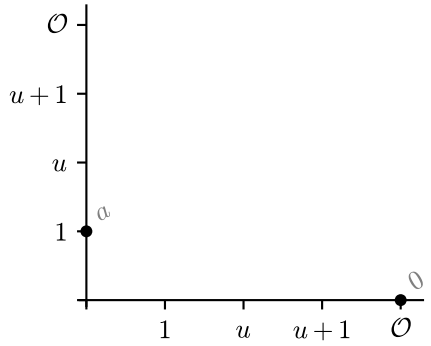
$$|\#E(\mathbb{F}_{q^n}) - 1 - q^n| \leq 2q^{n/2}, \quad \forall n \geq 1.$$

Somit können wir nach maximal 9 gefundenen rationalen Punkten unsere Suche einstellen. Dies gibt uns folgende Klassifikation aller elliptischen Kurven über dem Körper $\mathbb{F}_4$ bis auf Isomorphie:

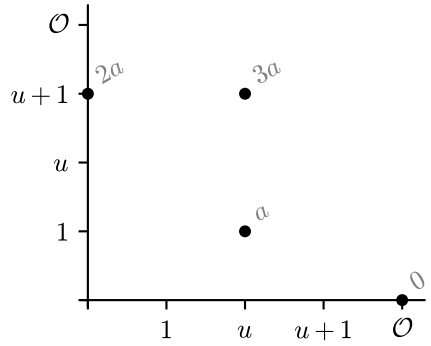
$E_1 : y^2 + xy = x^3 + 1$
$\mathbb{Z}/8\mathbb{Z}$



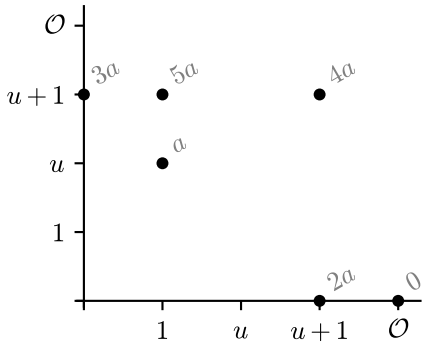
$E_2 : y^2 + xy = x^3 + ux^2 + 1$
$\mathbb{Z}/2\mathbb{Z}$



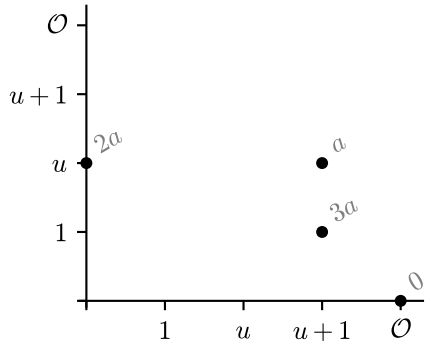
$E_3 : y^2 + xy = x^3 + u$
$\mathbb{Z}/4\mathbb{Z}$



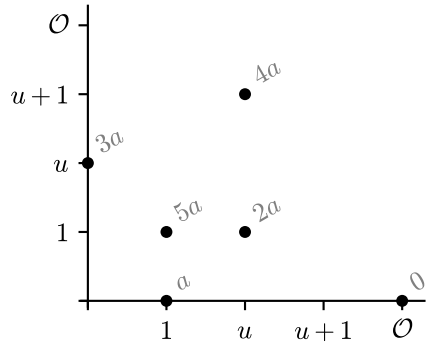
$E_4 : y^2 + xy = x^3 + ux^2 + u$
$\mathbb{Z}/6\mathbb{Z}$



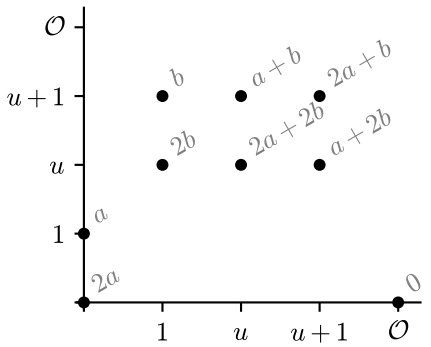
$E_5 : y^2 + xy = x^3 + (u+1)$
$\mathbb{Z}/4\mathbb{Z}$



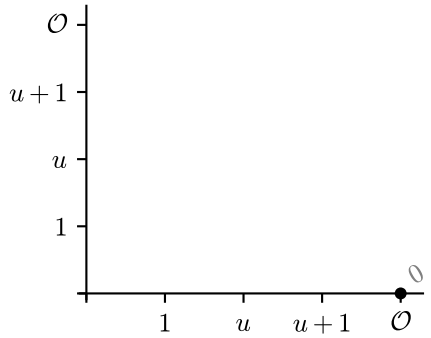
$E_6 : y^2 + xy = x^3 + ux^2 + (u+1)$
$\mathbb{Z}/6\mathbb{Z}$



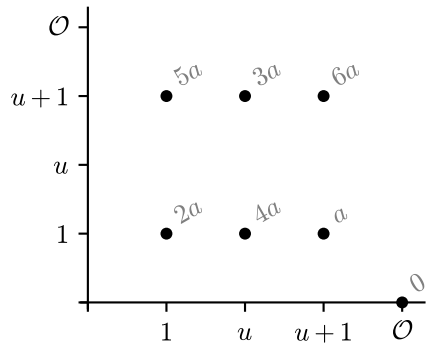
$E_7 : y^2 + y = x^3$
$\mathbb{Z}/3 + \mathbb{Z}/3\mathbb{Z}$



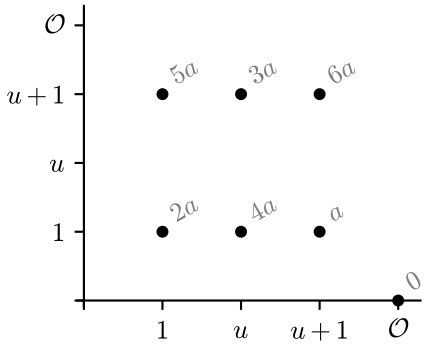
$E_8 : y^2 + y = x^3 + u$
$\{0\}$



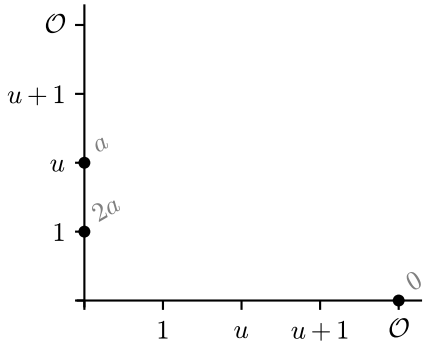
$E_9 : y^2 + uy = x^3$
$\mathbb{Z}/7\mathbb{Z}$



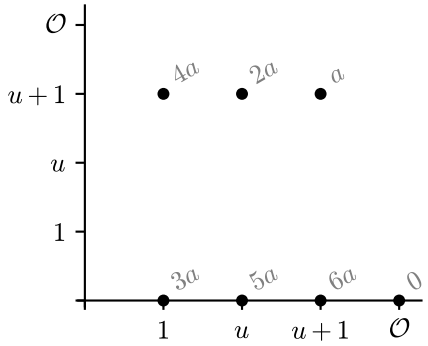
$E_{10} : y^2 + uy = x^3 + u$
$\mathbb{Z}/7\mathbb{Z}$



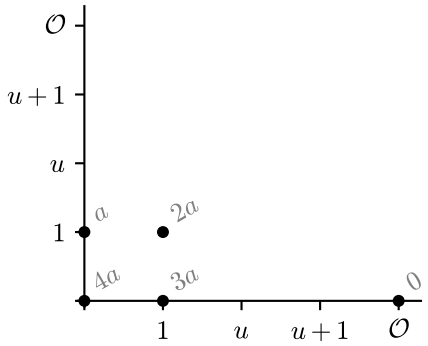
$E_{11} : y^2 + (u+1)y = x^3 + u$
$\mathbb{Z}/3\mathbb{Z}$



$E_{12} : y^2 + (u+1)y = x^3 + 1$
$\mathbb{Z}/7\mathbb{Z}$



$E_{13} : y^2 + y = x^3 + x$
$\mathbb{Z}/5\mathbb{Z}$



Literatur

[1] J. Silverman: The Arithmetic of Elliptic Curves. Springer, New York, 2009.

[2] J. Silverman: Rational Points on Elliptic Curves. Springer, New York, 1992.

[3] I. Shparlinski: Finite Fields: Theory and Computation. Springer Science+Business Media, Dordrecht, 1999.

[4] R. Hartshorne: Algebraic geometry. Springer, New York, 2006.

[5] I. Shafarevich: Basic Algebraic Geometry 1. Springer, Heidelberg, 2013.

[6] D. Husemöller: Elliptic Curves. Springer, New York, 2 ed., 2004.

[7] N. Koblitz: A course in number theory and cryptography. Springer, New York, 1987.

[8] A. Menezes, T. Okamoto, S. Vanstone: Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field. IEEE Trans. Inform. Theory 39 (1993), 1639-1646.

Erklärung

Hiermit versichere ich, dass ich die Bachelorarbeit selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Düsseldorf, den 04. April 2022

(Luca Leon Happel)