Elliptische Kurven in der Kryptographie, Teil I

Vortrag zum Seminar zur Funktionentheorie, 19.11.2007

Sebastian Kories

Das Ziel dieses Vortrages ist es, einen Überblick über verschiedene Verschlüsselungstechniken und Verfahren zu gewinnen und die Grundlagen für die beiden weiteren Vorträge über Elliptische Kurven in der Kryptographie zu schaffen.

§ 1 Kryptographie

Kryptographie bezeichnet im ursprünglichen Sinne die Lehre der Verschlüsselung von Informationen. Im Allgemeinen beschäftigt sie sich heute mit dem Schutz von Daten bei der Übertragung mittels sogenannter Schlüssel. Die Idee der Kryptographie ist zwar schon alt und hat eine lange Geschichte, jedoch gewann sie erst im 20. Jahrhundert an Bedeutung für die Allgemeinheit – zunächst im Krieg und dann mit der Erfindung des Internets.

Früher einigten sich Sender und Empfänger, die in der Kryptographie meist mit Alice und Bob bezeichnet werden, auf einen gemeinsamen geheimen Schlüssel. Dies musste im Rahmen eines persönlichen Treffens oder mittels eines versiegelten Briefes geschehen. Anschließend konnte die verschlüsselte Nachricht über eine nicht abhörsichere Verbindung (z. B. Radio, Funk) übertragen werden.

Diese Verschlüsselungstechnik bezeichnet man als *symmetrisches Verfahren*.

Im Zeitalter des Internets ist diese Art des geheimen Schlüsselaustausches nicht mehr praktikabel bei der Menge an Usern, die z. B. Onlinebanking betreiben, wobei die persönlichen Daten geheim gehalten werden müssen. Und so stellt sich die Frage: „Wie verschlüsselt man geheime Nachrichten, ohne vorher geheime Schlüssel ausgetauscht zu haben?“

Die Lösung für das Problem heißt *Public-Key-Kryptographie* (bzw. *asymmetrische Kryptographie*), welche auf den Ideen von Diffie und Hellman aus den 70er Jahren basiert:

Alice und Bob haben je einen sogenannten öffentlichen und einen privaten Schlüssel. Den öffentlichen Schlüssel kennt jeder Nutzer, den privaten nur die entsprechende Person selber. Diesen Schlüssel kann man sich als Funktion f vorstellen, die die Nachricht x verschlüsselt: $f : x \mapsto f(x)$. Dabei ist $f(x)$ zwar leicht berechenbar,

aber nur mittels des privaten Schlüssels effizient invertierbar. „Effizient“ heißt in diesem Zusammenhang „in Polynomialzeit“ berechenbar. Eine Funktion f mit dieser Eigenschaft nennt man in der Kryptographie Einwegfunktion. Ihre Existenz konnte bisher noch niemand beweisen.

(1.1) Definition (Polynomialzeit)
Ein Problem ist in *Polynomialzeit* lösbar, wenn die Rechenzeit einer Rechenmaschine mit der Problemgröße nicht stärker als mit Polynomfunktion wächst. In der Landau-Notation bedeutet das:

$$\exists k \in \mathbb{N} \text{ mit } m(n) \in \mathcal{O}(n^k)$$

wenn m die Rechenzeit und n die Problemgröße angeben. Die Bedeutung liegt darin, dass sie eine Grenze für die praktische Lösbarkeit von Problemen darstellt. ◇

(1.2) Definition
In der Landau-Notation gibt $f \in \mathcal{O}(g)$ folgende obere Schranke für den Rechenaufwand an:

$$f \in \mathcal{O}(g) :\Leftrightarrow \exists\, c > 0 \exists\, x_0 \,\forall\, x > x_0 : |f(x)| \leq c \cdot |g(x)|.$$

(1.3) Beispiel
Wählt man $n = 2^{512}$ als Problemgröße und benutzt den derzeit schnellsten Rechner der Welt („BlueGene/L“ (Stand 07.2007) mit einer Leistung von 280,6 TFLOPS, was $280,6 \cdot 10^{12}$ Rechenoperationen pro Sekunde entspricht), so bräuchte er

$$\frac{\sqrt{2^{512}}}{3600 \cdot 24 \cdot 365 \cdot 280,6 \cdot 10^{12}} \approx 1,3 \cdot 10^{55} \text{ Jahre}$$

für einen Algorithmus mit Komplexitätsklasse $\mathcal{O}(\sqrt{n})$. Steigt die Rechnerleistung, so kann man aber jederzeit noch n vergrößern. ◇

Privater und öffentlicher Schlüssel bilden ein von einander abhängiges Paar, da Bob nur die Nachricht mit seinem privaten Schlüssel entschlüsseln kann, die mit seinem öffentlichen Schlüssel verschlüsselt wurde.

— *Diskreter Logarithmus* —

Um elliptische Kurven in der Public-Key-Kryptographie nutzen zu können, definieren wir die Verschlüsselungsfunktion f mit Hilfe von endlichen abelschen Gruppen G, die wir additiv schreiben:

$$(P, Q) \mapsto P + Q$$

ist die Gruppenoperation.

Sei 0 das neutrale Element in G, P ein Element aus G und n die Ordnung der von P erzeugten zyklischen Untergruppe:

$$n := |\langle P \rangle| = |\{kP \mid k \in \mathbb{Z}\}|$$

d. h. $nP = 0$ und $\nexists k \in \mathbb{N}$ mit $kP = 0$ und $k < n$. Dann ist f die Funktion:

$$f : \mathbb{Z}/n\mathbb{Z} \to \langle P \rangle,$$
$$k + n\mathbb{Z} \mapsto kP.$$

Das Gruppenelement kP muss zu gegebenem k effizient, d. h. in Polynomialzeit berechenbar sein, andererseits darf die Umkehrung, k aus bekanntem kP zu bestimmen, gerade nicht in Polynomialzeit möglich sein.

(1.4) Definition (Problem des diskreten Logarithmus (DL-Problem))
Bestimme zu gegebenem G, $P \in G$, $n = \mathrm{ord}(P)$ und $Q \in \langle P \rangle$ das Element $k + n\mathbb{Z}$ in $\mathbb{Z}/n\mathbb{Z}$ mit

$$Q = kP.$$

◇

Die Namensgebung „Logarithmus“ liegt darin begründet, dass eine Umkehrfunktion zu $k \to kP$ gesucht wird und wir die endliche abelsche Gruppe additiv definiert hatten. Hätten wir die Verknüpfung in G multiplikativ geschrieben, also $(P, Q) \mapsto P \cdot Q$, so müssten wir nämlich die Umkehrfunktion zu der Exponentialfunktion $k \mapsto P^k$ bestimmen. Diskret kann man in diesem Zusammenhang etwa als ganzzahlig verstehen.

§ 2 Verfahren

— *Diffie-Hellman-Schlüsselaustausch* —

Dies ist ein Verfahren zum Austausch von geheimen Schlüsseln für ein symmetrisches Verschlüsselungsverfahren über einen öffentlichen Kanal – es seien also G, n, P öffentlich bekannt:

Algorithmus:

1) Alice wählt ein $d_A \in \{1, ..., n-1\}$ und schickt das Gruppenelement $d_A P$ an Bob.

2) Bob wählt ein $d_B \in \{1, ..., n-1\}$ und schickt das Gruppenelement $d_B P$ an Alice.

3) Alice und Bob können jetzt jeweils $d_A(d_B P) = d_A d_B P = d_B(d_A P)$ berechnen, ohne den privaten Schlüssel d_A bzw. d_B des anderen zu kennen.

Ein Hacker, der in der Kryptographie meist mit Eve bezeichnet wird, versucht nun an $d_A d_B P$ zu gelangen, kennt aber nur die öffentlichen Daten: $G, P \in G, d_A P, d_B P$. Will Sie daraus das Elment $d_A d_B P$ berechnen, so muss sie ein sogenanntes Diffie-Hellman-Problem lösen:

(2.1) Definition (Diffie-Hellman-Problem)
Berechne zu $kP, lP \in \langle P \rangle$ das Element $klP \in \langle P \rangle$. ◇

Kann Eve das DL-Problem für klP in G lösen, so kann sie auch das Diffie-Hellman-Problem lösen. Ob auch die Umkehrung gilt, d. h. ob eine Gruppe, in der das DL-Problem schwer zu lösen ist auch die Eigenschaft hat, dass das Diffie-Hellman-Problem schwer zu lösen ist, ist nicht bekannt.

Ein Schwachpunkt des Diffie-Hellman-Schlüsselaustausches wird bei einer sogenannten „Man in the middle Attacke“ ausgenutzt. Dabei gibt sich Eve gegenüber Alice als Bob aus und gegenüber Bob als Alice. Mit beiden erzeugt sie je ein Schlüsselpaar, so dass sie die von Alice verschlüsselte Nachricht mit ihrem eigenen privaten Schlüssel entschlüsseln kann. Anschließend verschlüsselt sie die Nachricht wieder mit Bobs öffentlichem Schlüssel und schickt diese an ihn weiter. Alice und Bob können eine solche Attacke nur verhindern, wenn sie sicher sein können, wirklich mit dem richtigen Schlüsselpartner zu kommunizieren.

— *Elgamal-Verschlüsselung* —

Die Elgamal-Verschlüsselung wurde 1985 von Taher Elgamal entwickelt. Dabei geht man wieder von dem grundsätzlichen Anliegen aus, dass Alice eine geheime Nachricht an Bob schicken möchte. Dazu sei die Nachricht mit $m \in G$ identifiziert.

Algorithmus:

1) Alice wählt ein $k \in \{1, ..., n-1\}$.

2) Sie berechnet damit $Q := kP$ und mit Bobs öffentlichem Schlüssel $d_B P$

$$R := k(d_B P) + m.$$

3) Sie schickt das Paar (Q, R) an Bob.

4) Bob berechnet $d_B Q = d_B kP$ mit seinem privaten Schlüssel d_B.

5) Er erhält die entschlüsselte Nachricht m, indem er folgendes berechnet:

$$R - d_B Q = kd_B P + m - d_B kP = m.$$

Bei diesem Verfahren kennt Eve $G, n, P, d_B P$ und das Paar (Q, R). Eve kann nun m genau dann berechnen, wenn sie $kd_B P$ berechnen kann (da $R = kd_B P + m$). Dazu muss sie wieder ein Diffie-Hellman Problem lösen.

Um die Sicherheit für dieses Verfahren zu erhöhen, sollte Alice bei jeder Verschlüsselung ein neues k wählen, denn wenn Eve ein m_1 heraus bekommt, so kann sie ganz einfach mittels

$$R_1 - R_2 = m_1 - m_2$$

auch m_2 bestimmen.

— *Elgamal-Signatur* —

Diesmal möchte Alice gerne eine Nachricht an Bob digital signieren, d. h. eine digitale Unterschrift mitsenden, so dass man ihr die Nachricht eindeutig zuordnen kann. Sei $\mathcal{M}$ die Menge aller möglichen Nachrichten und h eine Hashfunktion

$$h : \mathcal{M} \to \{0, 1, ..., n-1\}$$

die folgende Anforderungen erfüllt:

i) zu gegebenem $x \in \{0, 1, ..., n-1\}$ lässt sich kein $m \in \mathcal{M}$ effizient bestimmen, so dass $h(m) = x$ (Urbild nicht bestimmbar)

ii) zu $m \in \mathcal{M}$ lässt sich kein $m' \in \mathcal{M}$ effizient bestimmen, so dass $h(m) = h(m')$

(2.2) Bezeichnung (Hashfunktion)
Eine *Hashfunktion* bezeichnet eine Abbildung, unter der ein relativ großer Definitionsbereich auf einen relativ kleinen Zielbereich abgebildet wird. Eine gute Hashfunktion zeichnet sich dadurch aus, dass sie wenige Kollisionen erzeugt, d.h. es gilt meistens $h(m) \neq h(m')$ für $m \neq m'$. Dadurch können die meisten Eingaben anhand ihres Hashwertes $h(m)$ unterschieden werden. ◇

Sei $\psi : \langle P \rangle \to \{0, 1, ..., n-1\}$ eine effektiv (also in Polynomialzeit) berechenbare Bijektion. (In der Praxis genügt es, wenn die Urbildmenge zu jedem Element aus $\{0, 1, ..., n-1\}$ hinreichend klein ist.)

Algorithmus:

1) Alice wählt ein $k \in \{1, ..., n-1\}$ mit: $\nexists\, a \in \mathbb{N}, a \neq 1$ mit $a \mid k$ und $a \mid n$ (d. h. k, n sind teilerfremd).

2) Sie berechnet damit $r := kP$ und das Inverse k^{-1} von k in $\mathbb{Z}/n\mathbb{Z}$.

3) Sie berechnet damit nun

$$s := k^{-1}(h(m) - \psi(r)d_A) \text{ in } \mathbb{Z}/n\mathbb{Z}.$$

4) Sie schickt m und das Paar (r, s) an Bob.

Die Authentifizierung der Signatur erfolgt dann durch Bob wie folgt:

Er berechnet mittels Alices öffentlichem Schlüssel $d_A P$ den Wert

$$Q := \psi(r)d_A P + sr \in G$$

und den Hashwert $h(m)$. Gilt nun

$$Q = h(m)P,$$

so ist die Signatur echt.

Beweis

$$\begin{aligned} Q = h(m)P &\Leftrightarrow \psi(r)d_A P + sr = h(m)P \\ &\Leftrightarrow \psi(r)d_A P + skP = h(m)P \\ &\Leftrightarrow \psi(r)d_A + sk \equiv h(m) \bmod n \end{aligned}$$

und gerade so war s in 3) gewählt worden. □

Möchte Eve nun die Signatur von Alice fälschen, so muss sie r und s bestimmen, so dass $\psi(r)d_A P + sr = h(m)P$ gilt. Wählt sich Eve also zunächst ein beliebiges k und versucht, zu $r = kP$ ein geeignetes s zu finden, so muss sie ein DL-Problem in $\langle P \rangle$ lösen, da ihr der private Schlüssel d_A im Schritt 3) fehlt.

Hier sei ebenso darauf hingewiesen, dass Alice für jede Signatur ein neues k aus der Menge $\{1, ..., n-1\}$ wählen muss, da sonst mit (r_1, s_1) für m_1 und (r_2, s_2) für m_2 gilt:

$$\begin{aligned} r_1 = r_2 \Rightarrow s_1 - s_2 &\equiv k^{-1}(h(m_1) - \psi(r_1)d_A) - k^{-1}(h(m_2) - \psi(r_2)d_A) \bmod n \\ &\equiv k^{-1}(h(m_1) - \psi(r_1)d_A - h(m_2) + \psi(r_2)d_A) \bmod n \\ &\equiv k^{-1}(h(m_1) - h(m_2)) \bmod n. \end{aligned}$$

Nimmt man nun an, dass $h(m_1) - h(m_2)$ und $\psi(r_1)$ invertierbar sind in $\mathbb{Z}/n\mathbb{Z}$, so kann Eve k mod n bestimmen und den privaten Schlüssel d_A folgenderweise bestimmen:

$$\begin{aligned} & s_1 \equiv k^{-1}(h(m_1) - \psi(r_1)d_A) \bmod n \\ \Rightarrow\ & \psi(r_1)\, d_A \equiv h(m_1) - s_1 k \bmod n \\ \Rightarrow\ & d_A \equiv \psi(r_1)^{-1}(h(m_1) - s_1 k) \bmod n. \end{aligned}$$

Die Kollisionsfreiheit der Hashfunktion ist bei diesem Verfahren besonders wichtig, da so das Schlüsselpaar (r, s) eindeutig der Nachricht m zugeordnet wird. Ansonsten könnte Eve eine andere Nachricht m' mit der Unterschrift zu der Nachricht m von Alice signieren.

— *Geeignete Gruppen* —

Um diese gerade eben vorgestellten Verschlüsselungsverfahren anwenden zu können, benötigen wir also stets geeignete endliche abelsche Gruppen, in denen das DL-Problem schwer zu lösen ist. Das bedeutet insbesondere auch, dass die Ordnung n von P groß sein muss, da sich sonst alle Möglichkeiten $1P, 2P, 3P, ...$ durchprobieren ließen. Jeder endliche Körper $\mathbb{F}_q$ mit q Elementen liefert uns eine endliche abelsche multiplikative und eine endliche abelsche additive Gruppe.

Für die additive Gruppe ließe sich dabei der diskrete Logarithmus zu $P \in G, k \in \{1, ..., n-1\}, Q := kP$ in der von P erzeugten zyklischen Untergruppe $\langle P \rangle$ leicht bestimmen, da nur die Fälle $P = Q = 0$ oder $k = Q/P$ möglich sind.

Bei geeignet gewähltem q bieten sich die multiplikativen Gruppen an, aber am besten geeignet sind die „Punktegruppen“ $E(\mathbb{F}_q)$ zu elliptischen Kurven über $\mathbb{F}_q$.

Es gibt bereits Algorithmen, die das DL-Problem für multiplikative Gruppen lösen, die sich aber (noch) nicht auf solche Gruppen $E(\mathbb{F}_q)$ übertragen lassen. Als Beispiele sind hier die Babystep-Giantstep- $(\mathcal{O}(\sqrt{n}))$, Pohlig-Hellman- $(\mathcal{O}(\sqrt{p})$ wobei p der größte Primfaktor von n ist), Index-Calculus- $(\mathcal{O}(exp(\sqrt{2ln(p)ln(ln(p))})))$ und Pollard-Reno-Algorithmen $(\mathcal{O}(\sqrt{n}))$ zu nennen.

§ 3 Affine und projektive Kurven

— Affine Kurven —

Seit 1985 werden die Anwendungsmöglichkeiten der elliptischen Kurven in der Public-Key-Kryptographie untersucht. Dazu betrachten wir hier nun elliptische Kurven und die dadurch gegebene Gruppenstruktur. Im Folgenden sei F zwecks kryptographischer Anwendung immer $F = \mathbb{F}_q$. Unsere Untersuchungen und Ergebnisse gelten jedoch für jeden Körper.

(3.1) Definition (affine ebene Kurve)
Es sei f ein Polynom in zwei Variablen x und y mit Koeffizienten in F:

$$f(x,y) = \sum_{i,j\geq 0} a_{i,j} x^i y^j$$

mit $a_{i,j} \in F$, von denen nur endlich viele ungleich Null sind. Unter der Annahme, dass $f \neq 0$ ist, bezeichnen wir die Menge der Nullstellen von f in $F \times F$ als $C_f(F)$:

$$C(F) := C_f(F) := \{(a,b) \in F \times F \mid f(a,b) = 0\}.$$

Jede solche Nullstellenmenge $C_f(F)$ nennen wir eine *affine ebene Kurve*.

Statt $F \times F = \{(a,b) \mid a,b \in F\}$ schreiben wir auch $\mathbb{A}^2(F)$ und nennen diese Menge den *zweidimensionalen affinen Raum*. ◇

(3.2) Beispiel
Es sei f das Polynom

$$f(x,y) = y^2 - x^3 - x$$

und $F = \mathbb{F}_p$, wobei p eine Primzahl ist. Dann ist

$$C_f(\mathbb{F}_p) = \{(a,b) \in \mathbb{F}_p \times \mathbb{F}_p \mid b^2 = a^3 + a\}$$

die zugehörige affine Kurve.

Wählt man z. B. $p = 3$ so berechnet man

$a = 0 \Rightarrow a^3 + a = 0^3 + 0 = 0$, $\quad b = 0 \Rightarrow b^2 = 0^2 = 0$,

$a = 1 \Rightarrow a^3 + a = 1^3 + 1 = 2$, $\quad b = 1 \Rightarrow b^2 = 1^2 = 1$,

$a = 2 \Rightarrow a^3 + a = 2^3 + 2 = 10 \equiv 1 \bmod 3$, $\quad b = 2 \Rightarrow b^2 = 2^2 = 4 \equiv 1 \bmod 3$,

◇

und es ergibt sich

$$C_f(\mathbb{F}_3) = \{(0,0),(2,1),(2,2)\}.$$

(3.3) Bemerkung
Betrachtet man das Polynom $f(x,y) = \sum_{i,j\geq 0} a_{i,j}x^i y^j \in F[X,Y]$ als Polynom über dem Körper K, der F als Teilkörper enthält, so gilt offensichtlich:

$$C_f(F) \subseteq C_f(K)$$

Dies gilt insbesondere, wenn K der algebraische Abschluss von F ist, den wir im Hinblick auf den zweiten Teil der Vortragsreihe „Elliptische Kurven in der Kryptographie“ hier schon einmal einführen. ◇

Zunächst rufen wir uns ein paar Definitionen aus der Algebra in Erinnerung:

(3.4) Definition (algebraischer Abschluss)
Sei $x \in F$. Dann heißt x *algebraisch über* F, wenn ein $0 \neq f \in F[X]$ existiert mit $f(x) = 0$.

Ein Körper F heißt *algebraisch abgeschlossen*, wenn jedes nicht konstante Polynom in einer Variablen mit Koeffizienten in F eine Nullstelle in F hat.

Ein Körper K heißt *Erweiterungskörper* von F, wenn $F \leq K$ (Teilring).

Ein Erweiterungskörper $\overline{F}$ von F heißt *algebraischer Abschluss von* F, wenn jedes $x \in \overline{F}$ algebraisch über F ist und zusätzlich $\overline{F}$ algebraisch abgeschlossen ist. ◇

Für die von uns betrachteten endlichen Körper $\mathbb{F}_q$ ist der algebraische Abschluss ein abzählbar unendlicher Körper der Charakteristik q, und enthält für jede natürliche Zahl n einen Teilkörper der Ordnung q^n (er besteht sogar aus der Vereinigung dieser Teilkörper).

Nun definieren wir, wann eine affine ebene Kurve als singulär bezeichnet wird:

(3.5) Definition
Die ebene affine Kurve $C_f(F)$ heißt *singulär in dem Punkt* $(a,b) \in C_f(F)$, falls beide Ableitungen von f in (a,b) verschwinden. Für einen Punkt $(a,b) \in \mathbb{A}^2(F)$ muss also folgendes gelten:

$$f(a,b) = 0,\ \frac{\partial f}{\partial x}(a,b) = 0,\ \frac{\partial f}{\partial y}(a,b) = 0.$$

$C_f(F)$ heißt *nicht-singulär*, falls die Kurve $C_f(\overline{F})$ in keinem Punkt (a,b) singulär ist.◇

(3.6) Bemerkung
Bei der Ableitung in (3.5) handelt es sich um die formale Ableitung für $f(x,y) = \sum_{i,j\geq 0} a_{i,j}x^i y^j \in F[X,Y]$

$$\text{nach } x, \text{ also} \quad \frac{\partial f}{\partial x}(x,y) = \sum_{j\geq 0, i>1} a_{i,j} i x^{i-1} y^j \text{ , und}$$

$$\text{nach } y, \text{ also} \quad \frac{\partial f}{\partial y}(x,y) = \sum_{i\geq 0, j>1} a_{i,j} j x^i y^{j-1}.$$

◇

(3.7) Beispiel

i) Als Beispiel einer Kurve, die weder singulär noch nicht-singulär ist, betrachten wir $C_f(\mathbb{R})$ gegeben durch $f(x,y) = y^2 - x^4 - 2x^2 - 1$. Hier gilt

$$\frac{\partial f}{\partial x}(x,y) = -4x(x^2+1) \quad \text{und} \quad \frac{\partial f}{\partial y}(x,y) = 2y$$

haben als einzige gemeinsame reelle Nullstelle $(0,0)$. Dies ist aber wiederum keine Nullstelle von $f(x,y)$, woraus folgt, dass $C_f(\mathbb{R})$ keine singulären Punkte enthält.

Allerdings sind $(i,0)$ und $(-i,0)$ singuläre Punkte in $C_f(\mathbb{C})$, wobei $\mathbb{C}$ der algebraische Abschluss von $\mathbb{R}$ ist, so dass $C_f(\mathbb{R})$ auch keine nicht-singuläre Kurve ist.

ii) Wir betrachten das Polynom

$$f(x,y) = y^2 - x^3 - x$$

über dem Körper $\mathbb{F}_p$ mit $p \geq 3$. Wir berechnen also die Ableitungen

$$\frac{\partial f}{\partial x}(x,y) = -3x^2 - 1 \quad \text{und} \quad \frac{\partial f}{\partial y}(x,y) = 2y.$$

Die singulären Punkte in $C_f(\overline{\mathbb{F}}_p)$ sind gerade die Punkte $(a,b) \in \overline{\mathbb{F}}_p \times \overline{\mathbb{F}}_p$ mit

$$f(a,b) = 0, \quad \frac{\partial f}{\partial x}(a,b) = 0 \quad \text{und} \quad \frac{\partial f}{\partial y}(a,b) = 0.$$

Für einen solchen Punkt gilt also

1) $b^2 = a^3 + a$,

2) $-3a^2 - 1 = 0$,

3) $2b = 0$.

Da $p \neq 2$ folgt aus $2b = 0$ sofort $b = 0$. Betrachten wir also 1) so gilt: $0 = a^3 + a = a(a^2 + 1) = a(3a^2 + 3) = a(-1 + 3) = 2a$. Daraus folgt $a = 0$, was aber im Widerspruch zu 2) steht. Für $p \neq 2$ gibt es also keine singulären Punkte auf $C_f(\overline{\mathbb{F}}_p)$, d. h. die Kurve $C_f(\mathbb{F}_p)$ ist nicht singulär. ◇

— *Projektive Kurven* —

Wir betrachten noch einmal die Kurve $C_f(F)$ gegeben durch

$$f(x, y) = y^2 - x^3 - x.$$

Wie wir festgestellt hatten, ist $C_f(F)$ die Menge aller Lösungen $(a, b) \in \mathbb{A}^2(F)$ von

$$y^2 = x^3 + x \tag{1}$$

Für eine solche Lösung (a, b) gilt offenbar:

$$b^2 = a^3 + a.$$

Wir definieren $a' := ac$ und $b' := bc$ mit $c \in F$ und $c \neq 0$. Mit dieser Wahl gilt:

$$\left(\frac{b'}{c}\right)^2 = \left(\frac{a'}{c}\right)^3 + \frac{a'}{c}$$

$$\Leftrightarrow b'^2 c = a'^3 + a' c^2$$

Demnach ist $(a', b', c') \in F \times F \times F$ eine Lösung folgender Gleichung in drei Variablen

$$Y^2 Z = X^3 + XZ^2 \tag{2}$$

Der Grund, die Gleichung auf diese Form zu bringen, liegt darin, dass (2) noch weitere wichtige Lösungen hat, die nicht von (1) kommen. Für Lösungen $(a, b, c) \in F \times F \times F$ von (2) gelten folgende Fälle:

1. Fall: $c \neq 0$. Dann ist $\left(\frac{a}{c}, \frac{b}{c}\right)$ ist Lösung von (1), also $\left(\frac{a}{c}, \frac{b}{c}\right) \in C_f(F)$

2. Fall: $c = 0$. Dann ist $a^3 = 0$ also auch $a = 0$ und $b \in F$ beliebig

   (So nicht aus der Gleichung (1) zu gewinnen.)

(3.8) Bemerkung
Sei (a, b, c) eine Lösung von (2) mit $c \neq 0$ (1. Fall). Mit

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \left(\frac{at}{ct}, \frac{bt}{ct}\right),$$

wobei $t \neq 0$ und $t \in F$, ist auch (ta, tb, tc) eine Lösung von (2). Das heißt, alle Vielfachen geben dieselbe Lösung von (1). ◇

Dies motiviert uns, solche Vielfachen zu identifizieren:

(3.9) Definition (projektiver Raum)

i) Wir nennen (a, b, c) und $(a', b', c') \in F \times F \times F$ *äquivalent* und schreiben dafür $(a, b, c) \sim (a', b', c')$, falls es ein $t \in F \setminus \{0\}$ gibt mit:

$$a = ta', b = tb', c = tc'.$$

ii) Wir definieren den *zweidimensionalen projektiven Raum* $\mathbb{P}^2(F)$ als den Quotienten von $F \times F \times F \setminus \{(0,0,0)\}$ nach der Äquivalenzrelation $\sim$:

$$\mathbb{P}^2(F) = (F \times F \times F \setminus \{(0,0,0)\})/\sim .$$

Der zweidimensionale projektive Raum ist also die Menge der Äquivalenzklassen von $\sim$, und jedes von $(0,0,0)$ verschiedene Tripel (a, b, c) gibt uns einen Punkt aus $\mathbb{P}^2(F)$, nämlich die Äquivalenzklasse $[a : b : c] := [(a : b : c)]_\sim$, in der (a, b, c) liegt. ◇

Zwei Punkte $[a : b : c]$ und $[a' : b' : c']$ sind genau dann gleich, wenn ein $t \in F$ existiert, so dass $a = ta', b = tb', c = tc'$.

Nun wollen wir den zweidimensionalen affinen Raum $\mathbb{A}^2(F)$ in den zweidimensionalen projektiven Raum $\mathbb{P}^2(F)$ einbetten:

(3.10) Lemma
Die Abbildung

$$\begin{aligned} i : \mathbb{A}^2(F) &\to \mathbb{P}^2(F) \\ (a, b) &\mapsto [a : b : 1] \end{aligned}$$

ist injektiv. ◇

Beweis
Seien $(a,b),(a',b') \in F \times F$, so dass $i(a,b) = i(a',b')$. Dann gilt

$$\begin{aligned} i(a,b) = i(a',b') &\Rightarrow [a:b:1] = [a':b':1] \\ &\Rightarrow a = ta', b = tb', \text{ und } 1 = t \cdot 1 \text{ für ein } t \in F \\ &\Rightarrow t = 1, a = ta', b = tb' \\ &\Rightarrow (a,b) = (a',b'). \end{aligned}$$

Die Abbildung i ist also injektiv. □

(3.11) Bemerkung
Mit der Abbildung $i : \mathbb{A}^2(F) \to \mathbb{P}^2(F)$; $(a,b) \mapsto [a:b:1]$ lässt sich jeder Punkt $[a:b:c] \in \mathbb{P}^2(F), c \neq 0$ wie folgt darstellen:

$$[a:b:c] = \left[\frac{a}{c} : \frac{b}{c} : 1\right] = i\left(\frac{a}{c}, \frac{b}{c}\right)$$

Offensichtlich lässt sich auf diese Weise aber kein Punkt $[a:b:0] \in \mathbb{P}^2(F)$ darstellen, denn nehmen wir an, es gelte

$$[a:b:0] = [a':b':1] = i(a',b'),$$

so würde folgen

$$\exists t \in F, t \neq 0, \text{ mit } a't = a, b't = b \text{ und } 1t = 0$$

als Widerspruch. ◇

Deswegen definieren wir eine weitere Abbildung und stellen fest:

(3.12) Lemma
Die Abbildung

$$\begin{aligned} j : F &\to \mathbb{P}^2(F) \\ a &\mapsto [a:1:0] \end{aligned}$$

ist injektiv. ◇

Beweis
Analog zu (3.10) □

Mit der Abbildung j lassen sich also alle Punkte $[a : b : 0]$ mit $b \neq 0$ darstellen. Der letzte in $\mathbb{P}^2(F)$ verbliebene Punkt, der weder im Bild von i noch in dem Bild von j liegt, ist der Punkt $[1 : 0 : 0]$, denn offenbar gilt $[a : 0 : 0] = [1 : 0 : 0]$ für $a \neq 0$.

So lässt sich $\mathbb{A}^2(F)$ nun als Vereinigung wie folgt in $\mathbb{P}^2(F)$ einbetten:

$$\mathbb{P}^2(F) = i(\mathbb{A}^2(F)) \dot{\cup} j(F) \dot{\cup} \{[1 : 0 : 0]\}.$$

Im Folgenden wollen wir Nullstellenmengen von Polynomen in $\mathbb{P}^2(F)$ betrachten. Da wir die Punkte (a, b, c) und (ta, tb, tc) identifizieren, ist es nur sinnvoll, Polynome zu betrachten, bei denen die Vielfachen der Nullstellen wieder Nullstellen sind. Eine Klasse von solchen Polynomen wird in der folgenden Definition eingeführt.

(3.13) Definition (homogen)
Es sei $g \in F[X, Y, Z]$ ein Polynom. Dann heißt g *homogen vom Grad d*, falls gilt:

$$g(X, Y, Z) = \sum_{i,j,k \geq 0} a_{i,j,k} X^i Y^j Z^k$$

mit mindestens einem Koeffizienten $a_{i,j,k} \neq 0$ und so, dass gilt:

$$i + j + k = d \text{ falls } a_{i,j,k} \neq 0.$$

◇

(3.14) Beispiel
Das Polynom $g(X, Y, Z) = Y^2Z - X^3 - XZ^2$ ist homogen vom Grad 3. ◇

(3.15) Lemma
Ist $g \in F[X, Y, Z]$ ein homogenes Polynom vom Grad d, so gilt für alle a, b, c aus F und $t \in F \setminus \{0\}$:

$$g(a, b, c) = 0 \Leftrightarrow g(ta, tb, tc) = 0.$$

Beweis

$$\begin{aligned} g(ta, tb, tc) &= \sum_{i,j,k \geq 0} a_{i,j,k} (ta)^i (tb)^j (tc)^k \\ &= \sum_{i,j,k \geq 0} a_{i,j,k} t^{i+j+k} a^i b^j c^k \\ &= t^d g(a, b, c) \end{aligned}$$

□

Nun definieren wir die Nullstellenmenge eines homogenen Polynomes als *projektive ebene Kurve*:

(3.16) Definition (projektive ebene Kurve)
Sei g erneut ein homogenes Polynom in $F[X,Y,Z]$. Dann bezeichnen wir die Menge der Nullstellen von g in $\mathbb{P}^2(F)$ als $C_g(F)$:

$$C_g(F) = \{[a:b:c] \in \mathbb{P}^2(F) \mid g(a,b,c) = 0\}.$$

Jede solche Nullstellenmenge $C_g(F)$ nennen wir eine *projektive ebene Kurve*. ◇

Betrachten wir projektive Kurven, so kennzeichnen wir die Variablen durch große Buchstaben (X,Y,Z) und bei affinen Kurven durch kleine Buchstaben (x,y,z).

(3.17) Beispiel
Betrachten wir die Polynome $f(x,y) = y^2 - x^3 - x$ und $g(X,Y,Z) = Y^2Z - X^3 - XZ^2$ die wir durch Umstellen aus den Gleichungen (1) und (2) gewinnen, so gilt nun: Ist $(a,b) \in C_f(F)$, so ist $[a:b:1] \in C_g(F)$ ◇

(3.18) Bemerkung
Die Abbildung $(a,b) \mapsto [a:b:1]$ haben wir gerade mit $i : \mathbb{A}^2(F) \to \mathbb{P}^2(F)$ bezeichnet, und da diese injektiv ist, lässt sich unsere affine Kurve $C_f(F)$ folgendermaßen in $C_g(F)$ einbetten:

$$C_g(F) = i(C_f(F)) \dot\cup \{[0:1:0]\}$$

Von diesem zusätzlichen Punkt $[0:1:0]$ sagt man auch, er läge „im Unendlichen“.◇

(3.19) Proposition
Sei $0 \neq f \in F[x,y]$ ein beliebiges Polynom, also $f(x,y) = \sum_{i,j\geq 0} a_{i,j}x^iy^j$. Wenn d der Grad von f ist, das heißt d ist der größte, der in f vorkommenden Exponenten $(d := \max\{i,j\})$, so ist

$$g(X,Y,Z) = \sum_{i,j\geq 0, i+j\leq d} a_{i,j}X^iY^jZ^{d-i-j}$$

homogen vom Grad d und erfüllt $g(a,b,1) = f(a,b)$ für alle $(a,b) \in \mathbb{A}^2(F)$.

Unter der Abbildung $i : \mathbb{A}^2(F) \to \mathbb{P}^2(F)$ wird $C_f(F)$ nach $C_g(F)$ abgebildet, und wenn ein Punkt $[a:b:c] \in \mathbb{P}^2(F)$ sich als $i(r,s)$ für ein $(r,s) \in \mathbb{A}^2(F)$ schreiben lässt, so liegt (r,s) bereits in $C_f(F)$. ◇

(3.20) Bemerkung
a) Wir werden die Abbildung i in Zukunft öfters weglassen und einfach schreiben

$$C_g(F) \cap \mathbb{A}^2(F) = C_f(F)$$

b) Andere Einbettungen $i_1(a,b) = [1 : a : b]$ und $i_2(a,b) = [a : 1 : b]$ von $\mathbb{A}^2(F)$ nach $\mathbb{R}^2(F)$ „überlappen“ sich, da z. B.

$$\begin{aligned} i(a,b) &= [a : b : 1] \\ &= \left[1 : \frac{b}{a} : \frac{1}{a}\right] = i_1\left(\frac{b}{a}, \frac{1}{a}\right) \end{aligned}$$

oder auch

$$\begin{aligned} i(a,b) &= [a : b : 1] \\ &= \left[\frac{a}{b} : 1 : \frac{1}{b}\right] = i_2\left(\frac{a}{b}, \frac{1}{b}\right) \end{aligned}$$

für $a, b \neq 0$ gilt. ◇

Als Nächstes wollen wir definieren, wann eine projektive Kurve nicht-singulär ist:

(3.21) Definition
Sei g ein homogenes Polynom in $F[X,Y,Z]$ vom Grad d. Die projektive ebene Kurve $C_g(F)$ heißt *singulär in dem Punkt* $P = [a : b : c] \in C_g(F)$, falls alle Ableitungen von g in P verschwinden, d. h.

$$\frac{\partial g}{\partial X}(a,b,c) = \frac{\partial g}{\partial Y}(a,b,c) = \frac{\partial g}{\partial Z}(a,b,c) = 0.$$

Die Kurve $C_g(F)$ heißt *nicht-singulär*, falls $C_g(\overline{F})$ in keinem Punkt singulär ist. ◇

Diese Definition passt auch zu der alten Definition für affine Kurven, denn es gilt:

(3.22) Lemma
Sei g mit

$$g(X,Y,Z) = \sum_{i,j,k \geq 0} a_{i,j,k} X^i Y^j Z^k$$

ein homogenes Polynom in $F[X,Y,Z]$ vom Grad d und f sei das Polynom

$$f(x,y) = \sum_{i,j \geq 0, i+j \leq d} a_{i,j,d-i-j} x^i y^j.$$

Für jeden Punkt $P \in C_g(F)$ gilt: Falls ein $Q \in \mathbb{A}^2(F)$ existiert, so dass $P = i(Q)$, so gilt:

$$\begin{aligned} &\text{projektive ebene Kurve } C_g(F) \text{ ist singulär in } P \\ \Leftrightarrow\ &\text{ebene affine Kurve } C_f(F) \text{ ist singulär in } Q. \end{aligned}$$

◇

Beweis
Aus (3.19) folgt, dass Q in der affinen Kurve $C_f(F)$ liegt. Ist $Q = (a, b)$, so ist $P = i(Q) = [a : b : 1]$. Mit diesen Erkenntnissen gilt nun:

Da

$$\frac{\partial g}{\partial X}(X, Y, Z) = \sum_{i>0,j,k\geq 0} a_{i,j,k} i X^{i-1} Y^j Z^k$$

und

$$\frac{\partial f}{\partial x}(x, y) = \sum_{i>0,j\geq 0,i+j\leq d} a_{i,j,d-i-j} i x^{i-1} y^j,$$

gilt offenbar $\frac{\partial g}{\partial X}(a, b, 1) = \frac{\partial f}{\partial x}(a, b)$. Völlig analog folgt $\frac{\partial g}{\partial Y}(a, b, 1) = \frac{\partial f}{\partial y}(a, b)$. Außerdem gilt

$$\frac{\partial g}{\partial Z}(X, Y, Z) = \sum_{i,j\geq 0,k>0} a_{i,j,k} k X^i Y^j Z^{k-1},$$

so dass

$$\begin{aligned}
\frac{\partial g}{\partial Z}(a, b, 1) &= \sum_{i,j,k\geq 0} a_{i,j,k} k a^i b^j \\
&= \sum_{i,j\geq 0,i+j\leq d} a_{i,j,d-i-j} (d - i - j) a^i b^j \\
&= \sum_{i,j\geq 0,i+j\leq d} a_{i,j,d-i-j} (d a^i b^j - i a^i b^j - j a^i b^j) \\
&= d f(a, b) - a \frac{\partial f}{\partial x}(a, b) - b \frac{\partial f}{\partial y}(a, b)
\end{aligned}$$

gilt, da $i + j + k = d$ ist. Aus dem Vergleich der Ableitungen von g und f folgt sofort die Behauptung. □

§ 4 Elliptische Kurven

Nun sind wir so weit, dass wir elliptische Kurven definieren können. Elliptische Kurven sind spezielle projektive Kurven, auf denen man ein Gruppengesetz definieren kann und wir wollen nun die Grundlagen schaffen, um die Gruppenaxiome nachweisen zu können. Dabei handelt es sich dann um eine Gruppe, in der das DL-Problem schwer zu lösen ist, und sie eignet sich daher sehr gut für die Kryptographie.

(4.1) Definition (elliptische Kurve)
Eine *elliptische Kurve* ist eine nicht-singuläre projektive ebene Kurve $C_g(F)$, wobei g ein homogenes Polynom vom Grad drei der folgenden Gestalt ist:

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

mit $a_1, a_2, a_3, a_4, a_6 \in F$. ◇

(4.2) Bemerkung (Weierstraßgleichung)
Betrachtet man folgende Umformungen:

$$g(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0 \quad (3)$$

$$\Leftrightarrow Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \quad (4)$$

so spricht man bei der Gleichung (4) auch von der *Weierstraßgleichung*, deren Lösung gerade Punkte auf der elliptischen Kurve sind. Bei einem Polynom der Form (3) sprechen wir von dem *Weierstraßpolynom*. Die eigenartige Numerierung der Koeffizienten a_i hat historischen Ursprung. ◇

(4.3) Satz
Der einzige Punkt in $C_g(F)$, der nicht im affinen Raum $i(\mathbb{A}^2(F))$ liegt, ist $[0:1:0]$. Dieser Punkt wird auch mit O bezeichnet. ◇

Beweis
Alle Punkte der Form $[a:b:c]$ mit $c \neq 0$ liegen im affinen Raum $i(\mathbb{A}^2(F))$. Also bleibt $P := [a:b:0] \in \mathbb{P}^2(F)$ zu betrachten. Setzt man P in die Weierstraßgleichung ein, so ergibt sich

$$0 = a^3$$

$$\Rightarrow a = 0 \text{ und } b \text{ beliebig}$$

Daraus folgt $P = [0:b:0] = [0:1:0]$. □

(4.4) Bemerkung
Da

$$\frac{\partial g}{\partial Z}(X,Y,Z) = Y^2 + a_1XY + 2a_3YZ - a_2X^2 - 2a_4XZ - 3a_6Z^2$$

gilt, folgt

$$\frac{\partial g}{\partial Z}(0,1,0) = 1,$$

d. h. O ist nicht singulär, egal welche a_i man wählt, um g zu definieren. ◇

Hat man also ein Polynom der Form

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

gegeben und will nun untersuchen, ob $C_g(F)$ eine elliptische Kurve ist, so muss man nur noch untersuchen, ob die Punkte in $C_g(F) \cap i(\mathbb{A}^2(F))$ nicht-singulär sind. Nach (3.22) genügt es dafür zu zeigen, dass die affine Kurve $C_f(F)$ für

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

nicht-singulär ist.

(4.5) Beispiel
Ruft man sich das Polynom g aus (3.7)(ii) in Erinnerung, so sieht man, dass es die gewünschte Gestalt einer elliptischen Kurve mit $a_1 = a_2 = a_3 = a_6 = 0$ und $a_4 = 1$ hat. Da wir bereits gezeigt haben, dass die affine Kurve $C_g(F) \cap \mathbb{A}^2(F)$ nicht-singulär ist falls $F = \mathbb{F}_p$ mit $p \geq 3$, folgt schon, dass es sich bei $C_g(F)$ um eine elliptische Kurve handelt. ◇

Bevor wir zu dem nächsten Satz kommen, erinnern wir an folgenden Satz aus der Analysis II:

(4.6) Satz
Seien $U \subset \mathbb{R}^n$ offen, $V \subset \mathbb{R}^m$ offen, $F : U \to \mathbb{R}^m$ total differenzierbar in $a \in U$ mit $F(U) \subset V$ sowie $G : V \to \mathbb{R}^p$ total differenzierbar in $b = F(a)$. Dann ist $H := G \circ F : U \to \mathbb{R}^p$ total differenzierbar in a mit

$$(D(G \circ F))(a) = (DG)(F(a)) \cdot (DF)(a),$$

d. h.

$$\frac{\partial H_i}{\partial x_j}(a) = \sum_{k=1}^{m} \frac{\partial G_i}{\partial y_k}(F(a)) \cdot \frac{\partial F_k}{\partial x_j}(a), \qquad 1 \leq i \leq p, 1 \leq j \leq n.$$

Beweis
Siehe Aloys Krieg, Analysis II, Kapitel X (2.9) □

Wir betrachten nun zwei Fälle, in denen man die Weierstraßgleichung vereinfachen kann. Diese Umformungen sind elementar für den zweiten Teil des Vortrages.

(4.7) Satz
Es sei $C_g(F)$ eine elliptische Kurve, also g von der Form $g(X,Y,Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$

i) Falls $\text{char}(F) \neq 2$, so ist die Abbildung

$$\begin{aligned} \Phi : \mathbb{P}^2(F) &\to \mathbb{P}^2(F) \\ [r:s:t] &\mapsto \left[r : s + \frac{a_1}{2}r + \frac{a_3}{2}t : t\right] \end{aligned}$$

bijektiv und es gilt

$$\Phi(C_g(F)) = C_{h_1}(F)$$

mit $h_1(X,Y,Z) = Y^2Z - X^3 - \frac{1}{4}b_2X^2Z - \frac{1}{2}b_4XZ^2 - \frac{1}{4}b_6Z^3$, wobei $b_2 = a_1^2 + 4a_2, b_4 = 2a_4 + a_1a_3$ und $b_6 = a_3^2 + 4a_6$. Die Kurve $C_{h_1}(F)$ ist ebenfalls eine elliptische Kurve.

ii) Falls $\text{char}(F) \neq 2$ und $\text{char}(F) \neq 3$, so ist die Abbildung

$$\begin{aligned} \Psi : \mathbb{P}^2(F) &\to \mathbb{P}^2(F) \\ [r:s:t] &\mapsto [36r + 3b_2t : 216s : t] \end{aligned}$$

bijektiv und es gilt

$$\Psi(C_{h_1}(F)) = C_{h_2}(F)$$

mit $h_2(X,Y,Z) = Y^2Z - X^3 + 27c_4XZ^2 + 54c_6Z^3$, wobei $c_4 = b_2^2 - 24b_4$ und $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. Die Kurve $C_{h_2}(F)$ ist ebenfalls eine elliptische Kurve.

Es gibt noch eine weitere Erkenntnis für den Fall, dass $\text{char}(F) = 2$ und $a_1 \neq 0$, die hier aber nicht weiter von Interesse ist. ◇

Beweis

i) Die Abbildung Φ ist wohldefiniert, da $\text{char}(F) \neq 2$ ist, man also die 2 invertieren kann. Zum Beweis der Bijektivität geben wir die zugehörige Umkehrabbildung Φ^{-1} an:

$$\Phi^{-1}([r:s:t]) = \left[r : s - \frac{a_1}{2}r - \frac{a_3}{2}t : t\right]$$

Aus Gründen der Analogie bezeichnen wir auch folgende beiden Abbildungen mit Φ und Φ^{-1}:

$$\begin{aligned} \Phi : F \times F \times F &\to F \times F \times F & \qquad \Phi^{-1} : F \times F \times F &\to F \times F \times F \\ (r,s,t) &\mapsto \left(r, s + \frac{a_1}{2}r + \frac{a_3}{2}t, t\right) & (r,s,t) &\mapsto \left(r, s - \frac{a_1}{2}r - \frac{a_3}{2}t, t\right) \end{aligned}$$

Des Weiteren gilt $h_1(X,Y,Z) = g(X, Y - \frac{a_1}{2}X - \frac{a_3}{2}Z, Z)$, wie wir nachrechnen:

$$\begin{aligned}
g(\Phi^{-1}(X,Y,Z)) &= g(X, Y - \frac{a_1}{2}X - \frac{a_3}{2}Z, Z) \\
&= \left(Y - \frac{a_1}{2}X - \frac{a_3}{2}Z\right)^2 Z + a_1 X \left(Y - \frac{a_1}{2}X - \frac{a_3}{2}Z\right) Z \\
&\quad + a_3 \left(Y - \frac{a_1}{2}X - \frac{a_3}{2}Z\right) Z^2 - X^3 - a_2 X^2 Z - a_4 X Z^2 - a_6 Z^3 \\
&= \left[Y^2 - 2Y\left(\frac{a_1}{2}X + \frac{a_3}{2}Z\right) + \left(\frac{a_1^2}{4}X^2 + 2\frac{a_1 a_3}{4}XZ + \frac{a_3^2}{4}Z^2\right)\right] Z \\
&\quad + a_1 XYZ - \frac{a_1^2}{2}X^2 Z - \frac{a_1 a_3}{2}XZ^2 + a_3 YZ^2 - \frac{a_1 a_3}{2}XZ^2 - \frac{a_3^2}{2}Z^3 \\
&\quad - X^3 - a_2 X^2 Z - a_4 X Z^2 - a_6 Z^3 \\
&= Y^2 Z - X^3 + \left(-\frac{a_1^2}{4} - a_2\right) X^2 Z + \left(-\frac{a_1 a_3}{2} - a_4\right) XZ^2 \\
&\quad + \left(-\frac{a_3^2}{4} - a_6\right) Z^3 \\
&= Y^2 Z - X^3 - \frac{1}{4}b_2 X^2 Z - \frac{1}{2}b_4 XZ^2 - \frac{1}{4}b_6 Z^3 \\
&= h_1(X,Y,Z)
\end{aligned}$$

Wie man sieht, gilt also $h_1(r,s,t) = g(\Phi^{-1}(r,s,t))$. Somit gilt:

$$\begin{aligned}
(g(r,s,t) = 0 \quad &\Leftrightarrow h_1(\Phi(r,s,t)) = 0) \\
\Rightarrow ((r,s,t) \in C_g(F) &\Leftrightarrow \Phi(r,s,t) \in C_{h_1}(F))
\end{aligned}$$

Daraus folgt $\Phi(C_g(F)) = C_{h_1}(F)$, was die zweite Behauptung war. Bleibt noch zu zeigen, dass es sich bei $C_{h_1}(F)$ wirklich um eine elliptische Kurve handelt. Das Polynom h_1 hat schon die in der Definition (4.1) geforderte Form. Wir berechnen mit Hilfe von (4.6) folgende Ableitungen:

$$\begin{aligned}
\frac{\partial h_1}{\partial X}(r,s,t) &= \frac{\partial g \circ \Phi^{-1}}{\partial X}(r,s,t) \\
&= \frac{\partial g}{\partial X}(\Phi^{-1}(r,s,t)) \underbrace{\frac{\partial r}{\partial r}}_{=1} + \frac{\partial g}{\partial Y}(\Phi^{-1}(r,s,t)) \underbrace{\frac{\partial (s - \frac{a_1}{2}r - \frac{a_3}{2}t)}{\partial r}}_{=-\frac{a_1}{2}} \\
&\quad + \frac{\partial g}{\partial Z}(\Phi^{-1}(r,s,t)) \underbrace{\frac{\partial t}{\partial r}}_{=0} \\
&= \frac{\partial g}{\partial X}(\Phi^{-1}(r,s,t)) - \frac{a_1}{2}\frac{\partial g}{\partial Y}(\Phi^{-1}(r,s,t))
\end{aligned}$$

$$\begin{aligned}
\frac{\partial h_1}{\partial Y}(r,s,t) &= \frac{\partial g \circ \Phi^{-1}}{\partial Y}(r,s,t) \\
&= \frac{\partial g}{\partial X}(\Phi^{-1}(r,s,t)) \underbrace{\frac{\partial r}{\partial s}}_{=0} + \frac{\partial g}{\partial Y}(\Phi^{-1}(r,s,t)) \underbrace{\frac{\partial (s - \frac{a_1}{2}r - \frac{a_3}{2}t)}{\partial s}}_{=1} \\
&\quad + \frac{\partial g}{\partial Z}(\Phi^{-1}(r,s,t)) \underbrace{\frac{\partial t}{\partial s}}_{=0} \\
&= \frac{\partial g}{\partial Y}(\Phi^{-1}(r,s,t))
\end{aligned}$$

$$\begin{aligned}
\frac{\partial h_1}{\partial Z}(r,s,t) &= \frac{\partial g \circ \Phi^{-1}}{\partial Z}(r,s,t) \\
&= \frac{\partial g}{\partial X}(\Phi^{-1}(r,s,t)) \underbrace{\frac{\partial r}{\partial t}}_{=0} + \frac{\partial g}{\partial Y}(\Phi^{-1}(r,s,t)) \underbrace{\frac{\partial (s - \frac{a_1}{2}r - \frac{a_3}{2}t)}{\partial t}}_{=-\frac{a_3}{2}} \\
&\quad + \frac{\partial g}{\partial Z}(\Phi^{-1}(r,s,t)) \underbrace{\frac{\partial t}{\partial t}}_{=1} \\
&= -\frac{a_3}{2}\frac{\partial g}{\partial Y}(\Phi^{-1}(r,s,t)) - \frac{\partial g}{\partial Z}(\Phi^{-1}(r,s,t))
\end{aligned}$$

Sei nun $P = [r : s : t]$ ein Punkt in $C_{h_1}(\overline{F})$. Dann ist $\Phi^{-1}([r : s : t])$ ein Punkt in $C_g(\overline{F})$, d. h. nicht singulär. Die drei Ableitungen von g in diesem Punkt

$\Phi^{-1}([r:s:t])$ sind also nicht alle gleichzeitig 0. Dann können auch nicht alle drei Ableitungen von h_1 in (r,s,t) gleich 0 sein, d. h. P ist ein nicht-singulärer Punkt auf $C_{h_1}(\overline{F})$, also folgt die Behauptung.

ii) Zum Beweis der Bijektivität geben wir einfach wieder die zugehörige Umkehrabbildung Ψ^{-1} an:

$$\Psi^{-1}([r:s:t]) = \left[\frac{1}{36}r - \frac{b_2}{12}t : \frac{1}{216}s : t\right]$$

Der gemeinsame Nenner der Brüche ist $216 = 2^3 3^3$, also ist auch die Abbildung Ψ^{-1} wohldefiniert, da $\mathrm{char}(F) \neq 2$ und $\mathrm{char}(F) \neq 3$.

Des Weiteren gilt $h_2(X,Y,Z) = 2^6 3^6 h_1(\frac{1}{36}X - \frac{b_2}{12}Z, \frac{1}{216}Y, Z)$ wie wir nachrechnen:

$$\begin{aligned}
2^6 3^6 h_1\left(\frac{1}{36}X - \frac{b_2}{12}Z, \frac{1}{216}Y, Z\right) &= 2^6 3^6 \left[\left(\frac{1}{216}Y\right)^2 Z - \left(\frac{1}{36}X - \frac{b_2}{12}Z\right)^3 \right.\\
&\qquad -\frac{1}{4}b_2\left(\frac{1}{36}X - \frac{b_2}{12}Z\right)^2 Z\\
&\qquad \left. -\frac{1}{2}b_4\left(\frac{1}{36}X - \frac{b_2}{12}Z\right)Z^2 - \frac{1}{4}b_6 Z^3\right]\\
&= Y^2Z - X^3 + 9b_2X^2Z - 27b_2^2XZ^2 + 27b_2^3Z^3\\
&\quad -9b_2X^2Z + 54b_2^2XZ^2 - 81b_2^3Z^3 - 648b_4XZ^2\\
&\quad +1944b_2b_4Z^3 - 11664b_6Z^3\\
&= Y^2Z - X^3 + (9b_2 - 9b_2)X^2Z\\
&\quad +27(-b_2^2 + 2b_2^2 - 24b_4)XZ^2\\
&\quad +(27b_2^3 - 81b_2^3 + 1944b_2b_4 - 11664b_6)Z^3\\
&= Y^2Z - X^3 + 27(b_2^2 - 24b_4)XZ^2\\
&\quad +54(-b_2^3 + 36b_2b_4 - 216b_6)Z^3\\
&= Y^2Z - X^3 + 27c_4XZ^2 + 54c_6Z^3\\
&= h_2(X,Y,Z)
\end{aligned}$$

Wie man sieht, gilt also:

$$\begin{aligned} (h_1(r,s,t) = 0 \quad &\Leftrightarrow h_2(\Psi(r,s,t)) = 0) \\ \Rightarrow ((r,s,t) \in C_{h_1}(F) &\Leftrightarrow \Psi(r,s,t) \in C_{h_2}(F)) \end{aligned}$$

Daraus folgt $\Phi(C_g(F)) = C_{h_1}(F)$, was die zweite Behauptung war. Bleibt noch zu zeigen, dass es sich bei $C_{h_2}(F)$ wirklich um eine elliptische Kurve handelt. Das Polynom h_2 hat schon die in der Definition (4.1) geforderte Form. Analog zu i) berechnet man die drei Ableitungen von h_2 und argumentiert so, dass mit $C_{h_1}(F)$ auch $C_{h_2}(F)$ nicht-singulär ist, woraus auch die letzte Behauptung folgt. □

Aus den beiden Resultaten folgt, dass man im Fall $\text{char}(F) \neq 2$ immer zu einer Weierstraßgleichung der Form

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

mit neuen Koeffizienten a_i mit $a_1 = a_3 = 0$ übergehen kann.

Im Fall $\text{char}(F) \neq 2$ und $\text{char}(F) \neq 3$ ist sogar eine Transformation in eine Weierstraßgleichung der Form

$$Y^2Z = X^3 + a_4XZ^2 + a_6Z^3$$

möglich.