Weil-Restriktion abelscher Varietäten

Diplomarbeit am Fachbereich 6 der
Universität GHS Essen

von

Niko Naumann

August 1999

Inhaltsverzeichnis

Kapitel 1

Einleitung

Das Ziel dieser Arbeit ist die Untersuchung arithmetischer Eigenschaften der Weil-Restriktion abelscher Varietäten.
Nach der Darstellung einiger grundlegender Sachverhalte im Bezug auf abelsche Varietäten (insbesondere über endlichen Definitionskörpern) in Kapitel 2 wird in Kapitel 3 zunächst der allgemeine Begriff der Weil-Restriktion unter besonderer Berücksichtigung von Konstruierbarkeitsfragen erläutert. Als nächstet wird gezeigt, daß Weil-Restriktion im Bezug auf eine Galois-Überlagerung ein spezieller Galois-descent ist, woraus sich bereits einfache arithmetische Aussagen ergeben. Für endliche Definitionskörper wird die Galois-Struktur der zu einer Weil-Restriktion gehörenden Tate-Moduln vollständig geklärt.
Als Beispiel für die Ergebnisse wird in Kapitel 4 ausführlich auf den Spezialfall einer elliptischen Kurve eingegangen, für die zunächst die Zerlegung der zugehörigen Weil-Restriktion in Isogeniefaktoren bestimmt wird. Im zweiten Teil des Kapitels werden explizite Gleichungen für den Fall einer Körpererweiterung vom Grad 3 hergeleitet, und mit ihrer Hilfe wird das Geschlecht von Kurven auf der Weil-Restriktion untersucht. Wir leiten auch Gleichungen für eine $\mathbb{F}_p$-einfache abelsche Fläche her, die ein Isogeniefaktor der Weil-Restriktion ist.
Im letzten Kapitel werden kryptographische Anwendungsmöglichkeiten diskutiert, die diese Arbeit eigentlich motiviert haben. Zum einen gibt es einen Vorschlag zum Angriff auf das DL-Problem auf elliptischen Kurven, der die Weil-Restriktion benutzt (vgl. [Fr1]), und zum anderen ein Konstruktionsverfahren für kryptographisch geeignete abelsche Flächen über Primkörpern.
Ich möchte mich bei meinem Diplomvater Herrn Prof. Dr. Dr. h.c. Gerhard

Frey für die Aufgabenstellung und die interessierte Betreuung bedanken.

Kapitel 2

Abelsche Varietäten

2.1 Allgemeines

Sei k ein vollkommener Körper mit algebraischem Abschluß $\bar{k}$.

Definition 1 *Eine* abelsche Varietät *A über $\bar{k}$ ist eine komplette, algebraische $\bar{k}$-Gruppenvarietät.*

Definition 2 *A heißt* über k definiert, *falls es ein k-Gruppenschema A_0 gibt, für das $A_0 \times_k \bar{k} = A$ gilt.*

Definition 3 *Ein* Morphismus *abelscher Varietäten ist ein mit der Gruppenstruktur verträglicher Morphismus von Varietäten.*

Definition 4 *Sind A und B über k definierte abelsche Varietäten und $\phi : A \to B$ ein Morphismus, so heißt ϕ* über k definiert, *falls ein Morphismus $\phi_0 : A_0 \to B_0$ existiert, dessen Basiserweiterung bzgl. $k \subset \bar{k}$ gerade ϕ ist. Die Menge aller dieser Morphismen wird mit* Hom_k(A,B) *bezeichnet.*

Definition 5 *Ein Morphismus ϕ abelscher Varietäten heißt eine* Isogenie, *falls ϕ surjektiv und $ker(\phi)$ ein endliches Gruppenschema ist.*

Prominente Beispiele abelscher Varietäten sind elliptische Kurven (siehe z.B. [Si1] und [Si2]).

Definition 6 *Eine* elliptische Kurve *ist eine Kurve vom Geschlecht 1 mit einem rationalen Punkt.*

Sie fügen sich zwanglos in die allgemeine Begrifflichkeit:

Satz 1 *Elliptische Kurven sind genau die abelschen Varietäten der Dimension 1.*

Beweis. Eine elliptische Kurve ist bekanntlich eine abelsche Varietät der Dimension 1 (vgl. [Si1]), sei also umgekehrt X eine solche. Dann ist X insbesondere eine nicht-singuläre Kurve, für deren Geschlecht nach dem Satz von Riemann-Roch ([H], V, Theorem 1.3) $g_X = l(K) = l(0) = 1$ gilt, weil der kanonische Divisor K auf jeder abelschen Varietät verschwindet. Damit ist X (nach Wahl eines Basispunktes) eine elliptische Kurve.

Eine abelsche Varietät ist durch ihren Funktionenkörper festgelegt:

Satz 2 *Seien A und A' abelsche Varietäten, die als Varietäten birational sind. Dann sind sie sogar als abelsche Varietäten isomorph.*

Beweis. Sei $\phi : A \cdots \to A'$ eine birationale Abbildung. Weil A' komplett ist, folgt aus einem Satz von Weil (vgl. [Si2], Proposition 6.2, b)), daß sich ϕ zu einem Morphismus fortsetzt. Das Gleiche gilt für ϕ^{-1}, und aus der Irreduzibilität von A und A' folgt, daß ϕ ein Isomorphismus (abstrakter) Varietäten ist. Also unterscheidet sich ϕ nach [M2], 4, Korollar 1 nur durch eine Translation von einem Isomorphismus abelscher Varietäten.

Definition 7 *Eine über k definierte abelsche Varietät heißt* k-einfach, *wenn sie außer* 0 *und A keine weiteren über k definierten abelschen Untervarietäten besitzt.*

Satz 3 (vollständiger Zerlegungssatz) *Sei A eine über k definierte abelsche Varietät. Dann ist A k-isogen zu einem Produkt $\prod A_i^{n_i}$ von paarweise nicht k-isogenen k-einfachen abelschen Varietäten A_i und die k-Isogenietypen der A_i sowie die Vielfachheiten n_i sind eindeutig bestimmt.*

Beweis. [M2], 19, Korollar 1.

2.2 Tate-Moduln

Fixiere eine von der Charakteristik von k verschiedene Primzahl l und eine über k definierte abelsche Varietät A der Dimension g. Für $n \geq 1$ setzt man $A[l^n]:=\{P \in A(\bar{k}) : l^n P = 0\}$.

Definition 8 *Der* l-adische Tate-Modul *von* A *ist der* $\mathbb{Z}_l$*-Modul*

$$T_l(A) := \lim_{\leftarrow} A[l^n].$$

Satz 4 $T_l(A) \cong \mathbb{Z}_l^{2g}$.

Beweis. [M2], 6, Proposition (3).

Sei A eine über k definierte abelsche Varietät. Dann operiert die absolute Galois-Gruppe G_k in verträglicher Weise auf allen $A[l^n]$ und damit wird $T_l(A)$ zu einem stetigen $\mathbb{Z}_l[G_k]$-Modul. Ein $\phi \in Hom_k(A,B)$ induziert auf natürliche Weise ein $\phi_l \in Hom_{\mathbb{Z}_l[G_k]}(T_l(A), T_l(B))$, denn ϕ respektiert die Galois-Struktur, weil es über k definiert ist. Durch lineare Fortsetzung erhält man die *l-adische Darstellung*

$$\Phi_l : Hom_k(A,B) \otimes_{\mathbb{Z}} \mathbb{Z}_l \longrightarrow Hom_{\mathbb{Z}_l[G_k]}(T_l(A), T_l(B))$$

über die Tate folgenden Satz bewiesen hat:

Satz 5 *Für einen endlichen Körper* k *ist* Φ_l *ein Isomorphismus.*

Beweis. [Ta]. Eine Ausarbeitung ist in [M2], Anhang 1 zu finden.

Der Satz bleibt gültig, wenn man k als Zahlkörper annimmt (vgl. [Fa]).Dieser Satz hat wichtige Konsequenzen für die Struktur abelscher Varietäten über endlichen Körpern bis auf Isogenie: Sind A und B über k definierte abelsche Varietäten, so gilt genau dann $A \sim_k B$, wenn für ein beliebieges $l \neq char(k)$ die Galois-Moduln $T_l(A)$ und $T_l(B)$ isomorph sind, und das wiederum ist äquivalent zu der Gleichheit der charateristischen Polynome des Frobenius in seiner Operation auf den Tate-Moduln. Also ist die Kenntnis der k-Isogenieklasse einer abelschen Varietät äquivalent zu der Kenntnis dieses charakteristischen Polynoms. Bezeichnet π den Frobenius, so gilt für die Menge der rationalen Punkte $A(k) = ker(1-\pi)$ und damit

$$|A(k)| = deg(1-\pi) = \chi(A)(1),$$

weil $1-\pi$ separabel ist. Hier bezeichnet natürlich χ das oben erwähnte charakteristische Polynom.

Kapitel 3

Weil-Restriktion

3.1 Allgemeines

Für eine endliche Körpererweiterung $k \subset K$ und eine Varietät X' über K möchte man gerne eine Varietät X über k haben, für die

$$X(k) = X'(K)$$

gilt. Nun ist natürlich $X(k) = Hom_k(k, X)$ und analog für X'. Also kann man das Problem auch wie im Folgenden formulieren, vgl. [BLR], 7.6.

Wir benutzen die abkürzende Notation $[A, B]_C := Hom_C(A, B)$ für die Morphismenmenge in einer Kategorie C. Sei ein Morphismus $h : S' \to S$ von Schemata gegeben. Für ein S'-Schema X' kann man dann den kontravarianten Funktor

$$\mathcal{R}_{S'|S}(X') : (Sch/S)^0 \longrightarrow Mengen$$

betrachten, der durch $T \mapsto [T \times_S S', X']_{S'}$ definiert ist. Ist dieser Funktor darstellbar, so ist ein darstellendes Objekt X nach Definition eine Weil-Restriktion von X' bezüglich h, d.h. X ist durch einen funktoriellen Isomorphismus

$$[T, X]_S \cong [T \times_S S', X']_{S'}$$

für alle S-Schemata T charakterisiert.
Da die Darstellbarkeit von $\mathcal{R}_{S'|S}(X')$ im folgenden der eigentlich nicht-triviale Punkt ist, arbeitet man besser in einem zunächst allgemeineren Kontext. Sei also ein Funktor

$$F' : (Sch/S')^0 \longrightarrow Mengen$$

gegeben. Dann definieren wir $h_*F'(T) := F'(T \times_S S')$, also einen Funktor

$$h_*F' : (Sch/S)^0 \longrightarrow Mengen.$$

Zunächst kommutiert diese Operation h_* mit Faserprodukten:

Proposition 1 *Seien $F', G', H' : (Sch/S')^0 \to$ Mengen Funktoren und $F' \to H'$, $G' \to H'$ Morphismen. Dann existiert ein funktorieller Isomorphismus*

$$h_*(F' \times_{H'} G') \cong (h_*F') \times_{(h_*H')} (h_*G').$$

Beweis. Für ein S-Schema T schreibe $T' := T \times_S S'$ und rechne

$$h_*(F' \times_{H'} G')(T) = (F' \times_{H'} G')(T') =$$

$$F'(T') \times_{H'(T')} G'(T') = (h_*F')(T) \times_{(h_*H')(T)} (h_*G')(T)$$
$$= (h_*F' \times_{h_*H'} h_*G')(T).$$

Sei nun wieder $F' = [\cdot, X']_{S'}$. Ist nun X' ein Gruppenschema, und exisiert die Weil-Restriktion X, so ist X auf natürliche Weise ein S-Gruppenschema.Zum Begriff des Gruppenschemas bzw. -funktors vergleiche [Si2], IV, 1. Aus dem in [BLR] gegebenen Existenzbeweis kann man folgendes Ergebnis ablesen, welches in bestimmten Fällen eine explizite Beschreibung der Weil-Restriktion liefert.

Proposition 2 *Sei $S' = Spec(R')$, $S = Spec(R)$ und R' ein freier R-Modul mit Basis $e_1, \ldots, e_n$. Ferner sei $X' \subset \mathbb{A}^N_{R'}$ ein abgeschlossenes Unterschema mit definierendem Ideal $I' = (f'_i) \subset R'[t_1, \ldots, t_N]$. Definiere neue Variablen durch*

$$t_i =: \sum_j t_{i,j} e_j$$

und entwickle damit

$$f'_i = \sum_j f_{i,j} e_j \,\text{mit}\, f_{i,j} \in R[t_{1,1}, \ldots, t_{N,n}].$$

Dann beschreiben die $f_{i,j}$ die Weil-Restriktion von X' als abgeschlossenes Unterschema von $\mathbb{A}^{Nn}_R$.

Beweis. Vergleiche [BLR], 7.6, Proposition 2 (ii) und Theorem 4.

In allen uns interessierenden Fällen ist damit die explizite Beschreibung der Weil-Restriktion affiner Schemata möglich. Wir wollen jetzt kurz auf affine Atlanten für allgemeinere (nicht notwendigerweise affine) Schemata eingehen. Wir setzen $h : S' \longrightarrow S$ als endliche Körpererweiterung $k \subset K$ vom Grad n voraus. Dann garantiert [BLR], 7.6, Theorem 4 die Existenz der Weil-Restriktion für quasi-projektive K-Schemata X'.
Sei $(U_i)_{i\in I}$ ein System offener affiner Teilmengen von X'. Mit Proposition 2 erhält man (explizit) ein offenes Unterschema $Y \subset h_*(X') =: X$ der Weil-Restriktion, indem man die Restriktionen der einzelnen U_i berechnet und sie mit den induzierten Klebedaten verklebt.
Für eine Körpererweiterung $k \subset E$ ist $X(E) = X'(E \times_k K)$ und damit $Y(E) = \{\alpha : E \times_k K \longrightarrow X' | \exists i : \alpha \text{ faktorisiert über } U_i\}$. Sei jetzt $(U_i)_{i\in I}$ eine Überdeckung von X'. Für K und E *linear disjunkt* über k ist dann $X(E) = Y(E)$, weil dann $E \times_k K$ ein Körper, also ein reduziertes einpunktiges Schema ist. Für allgemeine algebraischen Punkte hat man (wegen $\bar{k} \times_k K = \bar{k}^n$):

$$(X - Y)(\bar{k}) = (X'^n - \bigcup_{i\in I} U_i{}^n)(\bar{k})$$

Im Allgemeinen ist also die Restriktion einer Überdeckung keine Überdeckung mehr, weil offenbar $\{U_i^n\}$ keine Überdeckung von X'^n sein muß.
Man kann leicht eine ganze Klasse von Beispielen angeben, wo dies so ist. Dazu braucht man die auch später wichtige Aussage:

Proposition 3 *Ist $X'|K$ eine eigentliche Varietät, dann ist die Weil-Restriktion X eine eigentliche Varietät über k.*

Beweis. Die Existenz von X ist klar. Genauer besagen die Voraussetzungen, daß X' ein eigentliches, separiertes und ganzes Schema von endlichem Typ über K ist (vgl. [H], II, 4). Diese Eigenschaften übertragen sich nach [BLR], 7.6, Proposition 5 b),c),f) und h) alle auf X.

Wählt man z.B. X' als eine Kurve über K, so ist X eine eigentliche Varietät der Dimension $n = [K : k]$ über k, die nicht mit weniger als $n + 1$ offenen affinen Teilemengen überdeckt werden kann. Das erkennt man aus der Betrachtung der kohomologischen Dimension von X und der Existenz nicht-trivialer top-Kohomologie auf X (vgl. [H], III, Übung 4.8.c

und Bemerkung 7.12.1).

Wir geben auch ein ganz explizites Beispiel dafür, wie bei der Restriktion „Punkte verlorengehen“ können:
Im folgenden sei $K = k(\alpha)$, $\alpha^2 = D \in k$, also K eine reine quadratische Erweiterung von k. Aus der offenen Einbettung

$$\mathbb{A}^1_K - 0 \longrightarrow \mathbb{A}^1_K$$

wird nach Restriktion eine offene Einbettung

$$X \longrightarrow \mathbb{A}^2_k - 0,$$

die schon deswegen nicht surjektiv sein kann, weil $A^2_k - 0$ nicht affin ist (vgl. [H], III, Übung 4.3). Aus $A^1_K - 0 \cong Spec(K[x,y]/(xy-1))$ berechnet man mit Proposition 2 ein Modell von $X \subset \mathbb{A}^4_k$:

$$\begin{aligned} x_1y_1 + Dx_2y_2 - 1 &= 0 \\ x_1y_2 + x_2y_1 &= 0 \end{aligned}$$

und daraus dann mit Substitution $X \cong \mathbb{A}^2_k - \{T_1^2 - DT_2^2 = 0\}$. Der fehlende Punkt wird also bei Restriktion zu einem fehlenden irreduziblen Unterschema der Kodimension 1.

Ein Beispiel zum Verkleben von Karten: Wir starten mit der elliptischen Kurve

$$E|K : y^2 = x^3 - x$$

und nehmen als zweite Karte $E - (0,0)$.Die beiden Karten sind isomorph und werden entlang $E - (0,0) - \infty$ durch die Translation mit $(0,0)$ verklebt:

$$(x,y) + (0,0) = (1/x, -y/x^2) =: \sigma((x,y))$$

Man erhält dann wie oben eine Karte X der Weil-Restriktion von E im $\mathbb{A}^4_k$:

$$\begin{aligned} y_1^2 + Dy_2^2 &= x_1^3 + 3Dx_1x_2^2 + x_1 \\ 2y_1y_2 &= 3x_1^2x_2 + Dx_2^3 + x_2. \end{aligned}$$

Diese wird entlang $X - \{x_1^2 - Dx_2^2 = 0\}$ mit dem Isomorphismus

$$\sigma'(x_1 \ldots y_2) = (x_1/\beta, -x_2/\beta, (2Dx_1x_2y_2 - y_1x_1^2 - Dy_1x_2^2)/\beta^2, (2x_1x_2y_1 - Dx_1^2y_2 - x_1^2y_2)/\beta^2)$$

mit sich selbst verklebt ($\beta := x_1^2 - Dx_2^2$). σ' erhält man aus σ durch Substitution. Dieser Atlas überdeckt dann die Restriktion bis auf die beiden Punkte, die $\infty \times 0$ und $0 \times \infty$ auf $E \times E$ entprechen.

Wir zeigen noch durch ein Beispiel, daß man Proposition 2 nicht auf *homogene* Koordinaten anwenden kann. Dazu betrachten wir die Weil-Restriktion W von $\mathbb{P}^1_K$. Nimmt man homogene Koordinaten für $\mathbb{P}^1_K$ und wendet formal Proposition 2 an, so erhält man 4 homogene Koordinaten ohne Relationen, d.h. einfach $\mathbb{P}^3_k$. W ist aber zwei-dimensional. Obwohl zwar die Restriktion von $\mathbb{A}^1_K$ der $\mathbb{A}^2_k$ ist, gilt die analoge Aussage für projektive Räume nicht. Nehmen wir nämlich $W \cong \mathbb{P}^2_k$ und $k = \mathbb{F}_q$ als endlichen Körper an. Zunächst hat man offensichtlich die Anzahlformel

$$|\mathbb{P}^n(\mathbb{F}_q)| = (q^{n+1} - 1)/(q - 1) = 1 + \ldots + q^n.$$

Aus der Definition der Weil-Restriktion bekommt man für ungerades n:

$$W(k_n) \cong \mathbb{P}^1_K(K \otimes_k k_n) \cong \mathbb{P}^1_K(K_n)$$

und damit die Anzahlaussage

$$|W(k_n)| = 1 + q^{2n}.$$

Nach der angenommen Isomorphie gilt andererseits

$$|W(k_n)| = |\mathbb{P}^2_k(k_n)| = 1 + q^n + q^{2n}$$

und daraus folgt $q = 0$, was Unsinn ist.

3.2 Weil-Restriktion und Galois-Überlagerungen

Zunächst soll das Abstiegsproblem („descent“) erläutert werden. Man fixiert eine Erweitrung $p : S' \to S$ und betrachtet den Funktor $F \mapsto p^*F$ von

der Kategorie der quasi-kohärenten S-Moduln in die Kategorie der quasi-kohärenten S'-Moduln. Gefragt ist dann nach dem wesentlichen Bild dieses Funktors. Setze $S'' := S' \times_S S'$ und $S''' := S'' \times_S S'$. Man hat kanonische Projektionen $p_1.p_2 : S'' \to S'$ und $p_{ij} : S''' \to S''$ $(1 \leq i < j \leq 3)$. Ein *Überlagerungdatum* eines quasi-kohärenten S'-Moduls F' ist ein S''-Isomorphismus

$$\phi : p_1^* F' \longrightarrow p_2^* F'.$$

ϕ ist ein *Abstiegsdatum*, falls die *Kozykelbedingung*

$$p_{13}^* \phi = p_{23}^* \phi \circ p_{12}^* \phi$$

erfüllt ist. Man beobachtet, daß jeder S' Modul der Form p^*F mit einem kanonischen Abstiegsdatum versehen ist. Ein Abstiegsdatum ϕ heißt *effektiv*, falls es einen S-Modul F gibt, für den

$$p^* F \cong (F', \phi)$$

gilt. Es gilt folgender

Satz 6 *(Grothendieck) Sei p treu-flach und quasi-kompakt. Dann ist der Funktor $F \mapsto p^*F$ von der Kategorie der S-Moduln in die Kategorie der S'-Moduln mit Abstiegsdaten eine Kategorienäquivalenz.*

Beweis. [BLR], Kapitel 6, Satz 4. Die wesentliche Aussage ist, daß unter den genachten Vorraussetzungen alle Abstiegsdaten effektiv sind.
Man kann anstelle von quasi-kohärenten Moduln auch Schemata über S bzw. S' betracheten. Die Begriffe Überlagerungsdatum und (effektives) Abstiegsdatum haben in diesem Fall offensichtliche Analogien. Sei in diesem Sinne

$$\phi : p_1^* X' \longrightarrow p_2^* X'$$

ein Abstiegsdatum des S'-Schemas X'. Eine offenes Unterschema $U' \subset X'$ heißt *ϕ-stabil*, falls $\phi | U'$ ein Abstiegsdatum für U' ist. Es gilt:

Satz 7 *Sei p treu-flach und quasi-kompakt.Dann gilt:*
1) Der Funktor $X \mapsto p^*X$ von der Kategorie der S-Schemata in die Kategorie der S'-Schemata ist treu-voll.
2) Sind S und S' affin, so ist ein Abstiegsdatum ϕ eines S'-Schemas X' genau dann effektiv, wenn X' eine offene, affine Überdeckung durch ϕ-stabile Mengen gestattet.

Beweis. [BLR], Kapitel 6, Satz 6.

p heißt *galoissch mit Gruppe* G, falls $G \subset Aut_S(S')$ und die Abbildung $(\sigma, x) \mapsto (\sigma x, x)$ ein Isomorphismus

$$G \times S' \longrightarrow S''$$

ist. In diesem Kontext ist ein Abstiegsdatum auf einem S'-Schema X' äquivalent zu einer Operation

$$G \times X' \longrightarrow X',$$

so daß für alle $\sigma \in G$ das Diagramm

$$\begin{array}{ccc} X' & \stackrel{\sigma}{\longrightarrow} & X' \\ \downarrow & & \downarrow \\ S' & \stackrel{\sigma}{\longrightarrow} & S' \end{array}$$

kommutiert.

Wir untersuchen nun Weil-Restriktionen bezüglich Galois-Überlagerungen und zeigen, daß in diesem Fall die Weil-Restriktion ein spezieller Galois-descent ist. Insbesondere folgt daraus, daß die Weil-Restriktion nach Basiserweiterung in das direkte Produkt der Konjugierten der Ausgangsvarietät zerfällt:

Satz 8 *Sei* $f : Spec(R') \to Spec(R)$ *treu-flach, endlich und galoissch mit Gruppe* G *und* $\alpha : X' \to R'$ *ein quasi-projektives Schema. Betrachte* $Y := \prod_{\sigma \in G} X'^{\sigma}$ *und die* G*-Operation* $(x_\sigma)^\tau_\sigma := (x_{\sigma\tau^{-1}})_\sigma$ *auf* Y*. Sie definiert ein effektives Abstiegsdatum* ϕ *auf* Y*, und das eindeutig bestimmte* R*-Schema* A *mit* $f^*(A) = (Y, \phi)$ *ist die Weilrestriktion von* X' *bzgl.* f*. Insbesondere gilt also*

$$A \times_R R' \cong \prod_\sigma X'^{\sigma}.$$

Beweis. Die hier über Galois-descent verwendeten Tatsachen stehen in [BLR], 6.2, Beispiel B. Betrachte die kanonischen Projektionen $p_1, p_2 : R'' := R' \times_R R' \stackrel{\to}{\to} R'$ und $q := f \circ p_1 = f \circ p_2$. Ein Abstiegsdatum für Y ist äquivalent zu einer G-Operation auf Y, so daß für alle $\tau \in G$

$$\begin{array}{ccc} Y & \stackrel{\tau}{\to} & Y \\ \downarrow \beta & & \downarrow \beta \\ R' & \stackrel{\tau}{\to} & R' \end{array}$$

kommutiert. Nach Definition ist $\beta((x_\sigma)_\sigma) = \rho(\alpha(x_\rho))$ für beliebiges $\rho \in G$. Damit rechnet man einerseits: $\beta(\tau((x_\sigma)_\sigma)) = \beta((x_{\sigma\tau^{-1}})_\sigma) \stackrel{\rho:=\tau}{=} \tau(\alpha(x_e))$ und andererseits: $\tau(\beta((x_\sigma)_\sigma)) \stackrel{\rho:=e}{=} \tau(\alpha(x_e))$. Das Abstiegsdatum ist genau dann effektiv, wenn jeder G-Orbit in einer offenen affinen Umgebung enthalten ist. Mit X' ist auch Y quasi-projektiv, also ist diese Bedingung erfüllt. Der Funktor $A \mapsto f^*(A)$ von R-Schemata in die Kategorie der R'-Schemata mit Überlagerungsdatum ist treu-voll. Deswegen ist A eindeutig bestimmt. Außerdem ist daher für jedes R-Schema T die kanonische Sequenz

$$Hom_R(T, A) \longrightarrow Hom_{R'}(f^*(T), f^*(A) = Y) \rightrightarrows Hom_{R''}(q^*(T), q^*(A))$$

exakt. Mit dem Isomorphismus $G \times R' \to R''$, $(\sigma, r) \mapsto (\sigma r, r)$ ergibt sich

$$Hom_R(T, A) \cong Hom_{R'}(f^*(T), Y)^G,$$

wobei G durch Komposition operiert. Nach Definition des Produktes ist $Hom_{R'}(f^*(T), Y) = \prod_\sigma Hom_{R'}(f^*(T), X'^\sigma)$, und die G-Operation wird zu $(\phi_\sigma)^\tau_\sigma = (\phi_{\sigma\tau^{-1}})_\sigma$. Damit ist dann

$$Hom_R(T, A) \cong Hom_{R'}(f^*(T), X'),$$

also ist nach Definition A eine Weilrestriktion von X' bzgl. f.

Bemerkung. Die Eindeutigkeit des Abstiegs gilt natürlich nur im Bezug auf ein fixiertes Abstiegsdatum, z.B. ist für $A_1 := \mathbb{Q}[x, y]/(xy)$ und $A_2 := \mathbb{Q}[x, y]/(x^2 - 2y^2)$ zwar $A_1 \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) \cong A_2 \otimes_{\mathbb{Q}} \mathbb{Q}(\sqrt{2})$, aber offenbar $A_1 \ncong A_2$. Die zugehörigen Abstiegsdaten sind also verschieden, genauer gilt für den nicht-trivialen Automorphismus σ in seiner Operation auf $\mathbb{Q}(\sqrt{2})[x, y]/(xy)$:

$$\sigma_1(x) = x \qquad \sigma_1(y) = y$$

in Bezug auf A_1 und

$$\sigma_1(x) = y \qquad \sigma_1(y) = x$$

in Bezug auf A_2.
Wir wollen noch einige einfache, affine Beispiele für Galois-descent bzw. Weil-Restriktion bezüglich Galois-Überlagerungen angeben. Dazu formulieren wir zunächst Aussagen, die eigentlich Spezialfälle der allgemeinen Theorie sind, die sich aber sehr elementar beweisen lassen.

Proposition 4 *Sei $k \subset K$ endlich galoissch und die Galoisgruppe G operiere auf dem K-Vektorraum V auf verträgliche Weise (d.h. für $v \in V$,$\alpha \in K$ und $\sigma \in G$ sei $(\alpha v)^\sigma = \alpha^\sigma v^\sigma$). Dann induziert die Inklusion einen Isomorphismus*

$$V^G \otimes_k K \cong V.$$

Beweis. Die Injektivität der natürlichen Abbildung ist klar, und die Surjektivität ist äquivalent zu $V \subset \langle V^G \rangle_K$. Sei $v \in V$ gegeben und $\alpha_1, \ldots, \alpha_n$ eine k-Basis von K. Dann gilt

$$w_i := \sum_\sigma (\alpha_i v)^\sigma = \sum_\sigma \alpha_i^\sigma v^\sigma \in V^G.$$

Aus $det(\alpha_i^\sigma) \neq 0$ und $v = v^e$ folgt die Behauptung.

Satz 9 *Sei $G := Gal(K|k)$ endlich und für eine K-Algebra B mit Strukturmorphismus $\alpha : K \to B$ werde für $\sigma \in G$ mit B^σ die K-Algebra B mit Strukturmorphismus $\alpha \circ \sigma$ bezeichnet. Die folgenden Aussagen sind äquivalent:*

1) Es gibt eine k-Algebra A mit $B \cong A \otimes_k K$.
2) G operiert auf der k-Algebra B und die natürliche Abbildung von K-Algebren $B^G \otimes_k K \to B$ ist ein Isomorphismus.
3) Für alle $\sigma \in G$ gibt es einen K-Algebrenisomorphismus $\alpha_\sigma : B \to B^\sigma$, so daß $\alpha_{\sigma\tau} = \alpha_\sigma \alpha_\tau$ gilt.(Beachte, daß $B \cong B^\sigma$ als k-Algebren via der Identität).

Beweis. $1 \Rightarrow 2$: Die Zuordnung $\sigma \mapsto 1 \otimes \sigma \in Aut_k(B = A \otimes_k K)$ hat die gewünschten Eigenschaften, denn $B^G = (A \otimes_k K)^G = A \otimes 1 \cong A$.
$2 \Rightarrow 1$: $A := B^G$.
$1 \Rightarrow 3$: Genau wie „ $1 \Rightarrow 2$“, da $1 \otimes \sigma : B \to B^\sigma$ K-linear ist.
$3 \Rightarrow 2$: Als Operation wählt man natürlich $\sigma \mapsto \alpha_\sigma$. Für $b \in B$,$\sigma \in G$ und $\lambda \in K$ ist dann $(\lambda b)^\sigma = \alpha_\sigma(\lambda b) = \lambda^\sigma \alpha_\sigma(b) = \lambda^\sigma b^\sigma$. Also folgt die Behauptung aus Proposition 4.

Es ist leicht, ein Beispiel für eine nicht induzierte Algebra anzugeben. Wähle $k = \mathbb{Q}, K = \mathbb{Q}(\alpha := \sqrt{2}), B := K[x]/(x^2 - \alpha) \cong K(\sqrt{\alpha})$. Dann ist $B^\sigma \cong K(\sqrt{-\alpha})$ und wegen $\alpha/-\alpha = -1 \notin K^{*2}$ ist $B \ncong B^\sigma$. Nach Punkt 3) von Satz 9 gibt es also keine $\mathbb{Q}$-Algebra A mit $B \cong A \otimes_{\mathbb{Q}} K$. Deswegen sollte man eine nicht-triviale Weil-Restriktion W von B bzgl. $k \subset K$ erwarten. Diese

soll jetzt berechnet werden, und der Isomorphismus aus Satz 8 soll verifiziert werden. Letzterer besagt im vorliegenden Fall

$$B \otimes_K B^\sigma \cong W \otimes_k K. \tag{3.1}$$

Weil B und B^σ über K linear disjunkt sind, ist

$$B \otimes_K B^\sigma \cong K(\beta := \sqrt{\alpha}, \gamma := \sqrt{-\alpha})$$

eine bi-quadratische Erweiterung von K. Schreibt man mit neuen Variablen x_1, x_2

$$(x_1 + \alpha x_2)^2 - \alpha = (x_1^2 + 2x_2^2) + \alpha(2x_1x_2 - 1),$$

so erhält man nach Proposition 2 eine Beschreibung der Weilrestriktion:

$$W \cong \mathbb{Q}[x_1, x_2]/(x_1^2 + 2x_2^2, 2x_1x_2 - 1)$$

und damit natürlich auch

$$W \otimes_k K \cong K[x_1, x_2]/(x_1^2 + 2x_2^2, 2x_1x_2 - 1).$$

Substituiert man nun $x_1 = 1/(2x_2)$ in die erste Gleichung, erhält man wegen $4 \in K^{*4}$:

$$W \otimes_k K \cong K[x_2]/(x_2^4 + 1/8) \cong K(\sqrt[4]{-2}).$$

Beide Erweiterungen haben Grad 4 über K. Will man also die oben behauptete Isomorphie (3.1) nachweisen, so reicht es $\sqrt[4]{-2} \in K(\beta, \gamma)$ zu zeigen. Wegen $\beta^2/\gamma^2 = -1$ gilt aber für das Element $\frac{\beta+\beta^2/\gamma}{\sqrt{2}} \in K(\beta, \gamma)$:

$$(\frac{\beta + \beta^2/\gamma}{\sqrt{2}})^4 = \beta^4(\frac{1 + \beta^2/\gamma^2 + 2\beta/\gamma}{2})^2 =$$
$$2(\beta/\gamma)^2 = -2.$$

3.3 Weil-Restriktion abelscher Varietäten und Tate-Moduln

Für das Weitere brauchen wir

Proposition 5 *Sei $k \subset K$ eine endliche Galoiserweiterung und A' eine abelsche Varietät über K. Dann ist auch die Weil-Restriktion A eine abelsche Varietät über k.*

Beweis. Nach Proposition 3 und der Bemerkung nach Proposition 1 ist A eine eigentliche Gruppen-Varietät über k. Wegen Satz 8 ist mit A' auch A geometrisch irreduzibel.
Bemerkung. Die Aussage gilt allgemeiner für endliche separabele Körpererweiterungen, auf die Separabilität kann aber nicht verzichtet verden, vgl. [Mi2].

Im Hinblick auf diese Proposition macht die Frage nach den Galois-Eigenschaften der Teilungspunkte der Weil-Restriktion einer abelschen Varietät Sinn, und darüber sollen nun einige einfache Ergebnisse bewiesen werden. Dazu zunächst einige Aussagen über induzierte Darstellungen.

Proposition 6 *Sei $H \subset G$ Normalteiler, Λ ein kommutativer Ring mit 1, V ein $\Lambda[H]$-Linksmodul und $W := \Lambda[G] \otimes_{\Lambda[H]} V$ der induzierte G-Modul. Dann ist*

$$W \cong \bigoplus_{\sigma} V^{\sigma} \qquad als \quad H - Moduln.$$

Dabei durchläuft σ ein Vertretersystem der Linksnebenklassen von G mod H und H operiert auf V^{σ} vermöge $hv = h^{\sigma}v = \sigma^{-1}h\sigma v$.

Beweis. $\{\sigma\}$ ist eine $\Lambda[H]$-Basis des $\Lambda[H]$-Rechtsmoduls $\Lambda[G]$. Damit schreibt sich jedes Element von W eindeutig in der Form $\sum_\sigma \sigma \otimes v_\sigma$ und die Zuordnung $\sum_\sigma \sigma \otimes v_\sigma \mapsto (v_\sigma)_\sigma$ ist ein Isomorphismus abelscher Gruppen. Die H-Operation auf der σ-Komponente der direkten Summe ist für $h \in H$ und $v \in V$ durch $h(\sigma \otimes v) = h\sigma \otimes v = \sigma h^{\sigma} \otimes v = \sigma \otimes h^{\sigma}v$ gegeben.

Jetzt noch ein etwas genaueres Ergebnis für den Fall einer zyklischen Faktorgruppe.

Lemma 1 *Sei $H \subset G$ ein Normalteiler mit zyklischer Faktorgruppe der Ordnung n, und $\pi \in G$ erzeuge G/H. Sei ferner Λ ein kommutativer Ring mit 1 und V ein $\Lambda[H]$-Linksmodul, frei von endlichem Rang als Λ-Modul. Betrachte die induzierte Darstellung $W := \Lambda[G] \otimes_{\Lambda[H]} V$ als G-Linksmodul. Dann gilt für die charakteristischen Polynome:*

$$\chi_{\pi|W}(t) = \chi_{\pi^n|V}(t^n).$$

Beweis. Nach Voraussetzung ist $\pi^n \in H$, also die rechte Seite der Gleichung sinnvoll. Sei $\mathcal{B} = \{v_1, \ldots, v_N\}$ eine Λ-Basis von V. Dann ist $\mathcal{B}' := \{\pi^i \otimes v_j\}$ eine Λ-Basis von W und für alle j gilt:

$$\pi(\pi^i \otimes v_j) = \begin{cases} \pi^{i+1} \otimes v_j & : \quad i = 0, \ldots, n-2 \\ 1 \otimes \pi^n v_j & : \quad i = n-1. \end{cases}$$

Damit ist die Darstellende von π bzgl. $\mathcal{B}'$ in Blockschreibweise:

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 \\ A & 0 & \cdots & 0 & 0 \end{pmatrix} \in M_n(M_N(\Lambda)),$$

wobei A die Darstellende von π^n bzgl $\mathcal{B}$ ist. Dann ist $\chi_{\pi|W}(t)$ die Determinante der Matrix

$$\begin{pmatrix} t & -1 & 0 & \cdots & 0 \\ 0 & t & -1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & t & -1 \\ -A & 0 & \cdots & 0 & t \end{pmatrix} \in M_n(M_N(\Lambda)).$$

Durch die (blockweisen) Zeilenumformungen $(k)' := (k) + t(k-1) \quad (k = 2, \ldots, n)$ erhält man

$$\begin{pmatrix} t & -1 & 0 & \cdots & 0 \\ t^2 & 0 & -1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ t^{n-1} & 0 & \cdots & 0 & -1 \\ t^n - A & 0 & \cdots & 0 & 0 \end{pmatrix} \in M_n(M_N(\Lambda)) \cong M_{nN}(\Lambda).$$

Dann kann man die Determinante nacheinander nach den Spalten $N+1, \ldots, Nn$ entwickeln, in denen jeweils nur der oberste Eintrag von 0 verschieden, nämlich -1, ist, und erhält:

$$\chi_{\pi|W}(t) = ((-1)(-1)^N)^{N(n-1)} det(t^n A - E) = \chi_{\pi^n|V}(t^n).$$

Nun kann zunächst ein allgemeines Ergebnis über die Galois-Darstellung auf den Tate-Moduln formuliert werden.

Proposition 7 *Sei $k \subset K$ endlich galoissch, $\sigma \in Gal(K|k)$ und $\mathcal{A}/K$ eine abelsche Varietät. Dann gilt für den Tate-Modul der konjugierten Varietät:*

$$T_l(\mathcal{A})^\sigma \cong T_l(\mathcal{A}^\sigma) \text{ als } G_K - Moduln,$$

wobei die Modulstruktur der linken Seite wie in Proposition 6 ist.

Beweis Die Abbildung $P \mapsto P^\sigma$ ist wohldefiniert, denn ist $P \in \mathcal{A}[l^n]$ so gilt $[l^n]_{\mathcal{A}^\sigma}(P^\sigma) = ([l^n]_{\mathcal{A}})^\sigma(P^\sigma) = ([l^n]_{\mathcal{A}}(P))^\sigma = 0^\sigma_{\mathcal{A}} = 0_{\mathcal{A}^\sigma}$. Sie ist offensichtlich bijektiv, und für $h \in G_K$ ist $h(P^\sigma) = P^{\sigma h} = P^{h^\sigma \sigma} = (h(P))^\sigma$, nach Definition der Modulstruktur von $T_l(\mathcal{A})^\sigma$.

Satz 10 *Mit den Voraussetzungen von Proposition 7 gilt für die Weil-Restriktion $\mathcal{W}$ von $\mathcal{A}$:*

$$T_l(\mathcal{W}) \cong \mathbb{Z}_l[G_k] \otimes_{\mathbb{Z}_l[G_K]} T_l(\mathcal{A}) \qquad \text{als Moduln über } G_K.$$

Beweis. Das folgt aus $\mathcal{W} \times_k K \cong \prod_\sigma \mathcal{A}^\sigma$ (Satz 8), Proposition 7 und Proposition 6.

Das ist allerdings nicht besonders interessant, denn die Restriktion ist über k definiert, und dieses Ergebnis spiegelt nur das Verhalten der Restriktion nach der Basiserweiterung $k \subset K$ wieder. Im Falle eines endlichen Definitionskörpers zumindestens kann man das obige Ergebnis verbessern.

Satz 11 *Sei $k \subset K$ eine endliche Erweiterung endlicher Körper vom Grad n, $\mathcal{A}/K$ eine abelsche Varietät und $\mathcal{W}$ ihre Weilrestriktion bzgl. $k \subset K$. Sei ferner l eine Primzahl $\neq char(k)$. Dann ist*

$$T_l(\mathcal{W}) \cong \mathbb{Z}_l[G_k] \otimes_{\mathbb{Z}_l[G_K]} T_l(\mathcal{A}) \text{ als } G_k\text{-Moduln.}$$

Insbesondere gilt für die charakteristische Polynome der l-adischen Darstellung des Frobenius:

$$\chi_{\pi_k|\mathcal{W}}(t) = \chi_{\pi_K|\mathcal{A}}(t^n).$$

Beweis. Nach [Ta] ist $T_l(\mathcal{W})$ halbeinfacher G_k-Modul und G_k ist topologisch zyklisch, erzeugt vom Frobenius π_k. Daher ist $T_l(\mathcal{W})$ schon durch das charakteristische Polynom des Frobenius bestimmt. Mit Lemma 1 sieht man,

daß die erste Aussage aus der zweiten folgt. Wegen der Isomorphieaussage in Satz 8 hat man

$$T_l(\mathcal{W}) \cong \bigoplus_{i=0}^{i=n-1} T_l(\mathcal{A}^{\pi^i}) \text{ als } G_K\text{-Moduln.}$$

Ausserdem ist $\pi_k : \mathcal{A}^{\pi^i} \to \mathcal{A}^{\pi^{i+1}}$ eine Isogenie vom Grad $|k|$ (vgl. [M2], II, 4, Korollar 1), die wegen $l \neq char(k)$ einen Isomorphismus

$$\pi_l : T_l(\mathcal{A}^{\pi^i}) \longrightarrow T_l(\mathcal{A}^{\pi^{i+1}})$$

von $\mathbb{Z}_l$-Moduln induziert.
Wählt man nun eine $\mathbb{Z}_l$-Basis $\{v_i^{(0)}\}$ von $T_l(\mathcal{A})$ und definiert induktiv $v_i^{(k+1)} := \pi_l(v_i^{(k)}) \in T_l(\mathcal{A}^{\pi^{k+1}})$, so erhält man eine $\mathbb{Z}_l$-Basis von $T_l(\mathcal{W})$ bezüglich der die darstellende Matrix von π_l

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 \\ A & 0 & 0 & \cdots & 0 \end{pmatrix}$$

ist, wobei A die Darstellende von π_K bzgl. $\{v_i^{(0)}\}$ ist. Daraus folgt die Formel für die charakteristischen Polynome (vgl. Lemma 1).

Bemerkung. Die erste Aussage von Satz 11 wird allgemeiner für endliche separable Körpererweiterungen $k \subset K$ in [Mi2] gemacht, der Beweis jedoch nicht ausgeführt.

Kapitel 4

Beispiele

4.1 Zerlegung der Weil-Restriktion in Isogeniefaktoren

Mit Hilfe von Satz 11 soll jetzt angegeben werden, wie sich die Weil-Restriktion einer elliptischen Kurve über einem endlichen Körper in Isogeniefaktoren zerlegt.

Satz 12 *Sei $k = \mathbb{F}_q$ ein endlicher Körper, $E|k$ eine elliptische Kurve, $[K : k] = n$ und W die Weil-Restriktion von $E \times_k K$ bzgl. $k \subset K$. E sei nicht supersingulär und habe Weilzahl α. Betrachte*

$$I := \{d|n : \alpha \in \mathbb{Q}(\zeta_d)\}$$

$$J := \{d|n : \alpha \notin \mathbb{Q}(\zeta_d)\}.$$

Die Zerlegung von W in k-einfache Isogeniefaktoren besteht aus $2|I| + |J|$ Faktoren der Vielfachheit 1, für deren Dimension gilt:

$$dim\, W_d = \begin{cases} \phi(d) & : \quad d \in J \\ \frac{1}{2}\phi(d) & : \quad d \in I \end{cases} .$$

Außerdem ist $W_1 \sim E$.

Für spätere kryptographische Betrachtungen notieren wir noch eine einfache Folgerung:

Korollar 1 *Unter den Vorraussetzungen des Satzes sei außerdem n prim und es gelte entweder $n \equiv 1 \bmod 4$ oder sowohl $n \equiv 3 \bmod 4$ als auch $Disc(Mipo(\alpha)) \not\equiv -n \bmod \mathbb{Q}^{*2}$. Dann hat die Zerlegung die Form*

$$W \sim E \times A,$$

wobei $\dim A = n - 1$. *Für allgemeines n ist die Anzahl der Isogeniefaktoren von W mindestens gleich der Anzahl der Teiler von n.*

Bemerkung. Will man für eine gegebene Weil-Zahl α die Mengen I und J ausrechnen, so braucht man eine Liste aller quadratischen Teilkörper eines vorgegebenen Kreisteilungskörpers, vgl. Satz 14.

Beweis. *(des Korollars)* Die letzte Behauptung ist offensichtlich, denn $|I|+|J|$ ist die Anzahl der Teiler von n. Für $n \neq 2$ prim ist $\mathbb{Q}(\sqrt{(\frac{-1}{n})n}) \subset \mathbb{Q}(\zeta_n)$ der einzige quadratische Teilkörper. Unter den gemachten Voraussetzungen liegt α nicht in diesem Teilkörper, also ist $I = \emptyset$ und $J = \{1, n\}$, und die Aussage damit klar.

Beweis. *(des Satzes)* Wir schreiben „χ“ für das charakteristische Polynom des Frobenius in seiner Operation auf einer abelschen Varietät. Wir haben

$$\chi_{E|k} = (T - \alpha)(T - \bar{\alpha})$$

und damit

$$\chi_{E|K} = (T - \alpha^n)(T - \bar{\alpha}^n).$$

Aus Satz 11 folgt dann

$$\chi_{W|k} = (T^n - \alpha^n)(T^n - \bar{\alpha}^n) = \prod_{i=0}^{n-1}(T - \alpha\zeta^i)(T - \bar{\alpha}\zeta^i) \tag{4.1}$$

mit einer primitiven n-ten Einheitswurzel ζ. Man hat zunächst

$$\chi_{W|k} = \begin{cases} (\prod_i (T - \alpha\zeta^i))^2 & : \quad (\alpha/\bar{\alpha})^n = 1 \\ separabel & : \quad sonst \end{cases}$$

Das ist leicht einzusehen, denn die Punkte $\{\alpha\zeta^i\}$ bzw. $\{\bar{\alpha}\zeta^i\}$ bilden jeweils ein demselben Kreis einbeschriebenes regelmäßiges n-Eck. Zwei solche Polygone

können offenbar nur gleich sein (erster Fall) oder überhaupt keine gemeinsame Ecke besitzen (separabler Fall). Zwei Ecken fallen genau dann zusammen, wenn eine Gleichung der Form $\alpha\zeta^i = \bar{\alpha}\zeta^j$ besteht, und das ist äquivalent zu $(\alpha/\bar{\alpha})^n = 1$. Der inseparable Fall kann unter den gemachten Vorraussetzungen nicht eintreten, denn aus $\alpha^n = \bar{\alpha}^n$ folgt natürlich auch $\alpha^{2n} = \bar{\alpha}^{2n}$, aber auch $|\alpha^{2n}| = q^n \in \mathbb{Z}$. Damit ist das charakteristische Polynom von E über dem Erweiterungskörper vom Grad $2n$ von k das Quadrat eines linearen Polynoms, und aus [Ta], Theorem 1,$d1 \Leftrightarrow d5$ folgt, daß E supersingulär ist, im Widerspruch zu Voraussetzung. Schreiben wir π für den Frobenius von k auf W, so folgt wegen der Separabilität von $\chi_{W|k}$ aus [Ta], Theorem 2, $c2 \Leftrightarrow c3$

$$F := \mathbb{Q}(\pi) = E := End_k(W) \otimes \mathbb{Q}.$$

Insbesondere ist E kommutativ. Sei

$$W \sim \prod A_i^{n_i} \tag{4.2}$$

die nach Satz 3 eindeutige Zerlegung von W in k-einfache Isogeniefaktoren. Dann ist also $E \cong \oplus M_{n_i}(End_k(A_i) \otimes \mathbb{Q})$ kommutativ, und damit sind alle $n_i = 1$. Die Zerlegung (4.2) entspricht der Zerlegung der halbeinfachen Algebra E in ihre einfachen Komponenten, wegen der Kommutativität also der Zerlegung in eine direkte Summe von Körpern. Da π halbeinfach operiert und separables charakteristisches Polynom hat, ist dieses Polynom zugleich das Minimalpolynom von π. Damit entspricht also die Zerlegung (4.2) der Zerlegung von $\chi_{W|k}$ über $\mathbb{Q}$.
Um sie zu berechnen betrachten wir die Konjugationsbahnen über $\mathbb{Q}$ der aus (1) ersichtlichen Nullstellen von $\chi_{W|k}$. Sei also $\alpha\zeta^i$ fixiert und schreibe $\xi := \zeta^i$ und $d := ord(\xi)$ $(d|n)$. Ist nun $\alpha \notin \mathbb{Q}(\xi)$ so gilt für die Konjugationsbahn:

$$G_{\mathbb{Q}}(\alpha\xi) = \{\alpha\xi^j, \bar{\alpha}\xi^j : (j,d) = 1\},$$

denn dann sind $\mathbb{Q}(\alpha)$ und $\mathbb{Q}(\xi)$ linear disjunkt über $\mathbb{Q}$. Ist $\alpha \in \mathbb{Q}(\xi)$ so gilt

$$\#G_{\mathbb{Q}}(\alpha\xi) = \phi(d).$$

Zunächst operiert nämlich $G_{\mathbb{Q}}$ über $G := Gal(\mathbb{Q}(\xi)|\mathbb{Q})$ auf $\alpha\xi$. Dem Erweiterungsturm

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\xi)$$

entspricht eine Zerlegung

$$G = U \cup \sigma U$$

mit $U = Gal(\mathbb{Q}(\xi)|\mathbb{Q}(\alpha))$. Setze $\xi' := \xi^\sigma$. Dann hat man als Konjugierte von $\alpha\xi$ zunächst für $\tau \in U : (\alpha\xi)^\tau = \alpha\xi^\tau$, und diese sind offensichtlich paarweise verschieden. Hinzu kommen Elemente der Form $(\alpha\xi)^{\sigma\tau} = \bar{\alpha}\xi'^\tau$, die ebenfalls paarweise verschieden sind. Außerdem schneiden sich diese beiden Bahnen nicht, denn aus $\alpha\xi^{\tau_1} = \bar{\alpha}\xi'^{\tau_2}$ folgt $(\alpha/\bar{\alpha})^d = 1$ und damit auch $(\alpha/\bar{\alpha})^n = 1$, im Widerspruch zu oben.
Damit hat man folgende Zerlegung von $\chi_{W|k}$ über $\mathbb{Q}$:

$$\chi_{W|k} = \prod_{d\in J} G_d \prod_{d\in I} F_{d,1}F_{d,2} \tag{4.3}$$

mit $deg(G_d) = 2\phi(d)$ und $deg(F_{d,i}) = \phi(d)$ $(i = 1, 2)$. Daraus folgt die Aussage über die Anzahl der Isogeniefaktoren, und die Dimensionsaussage ist ein Spezialfall einer Formel aus [Ta], die in der anschließenden Bemerkung erläutert wird. Offenbar ist $1 \in J$ und $G_1 = \chi_{E|k}$. Deswegen folgt $W_1 \sim E$ aus [Ta], Theorem 1, b1⇔b3.

Bemerkung. Wenn E supersingulär ist, hängt die Zerlegung der Weil-Restriktion davon ab, über welcher Erweiterung der volle Endomorphismenring von E definiert ist, und wie diese Erweiterung zur Körpererweiterung bzgl. derer man die Restriktion betrachtet liegt. Wir betrachten ein einfaches Beispiel und schreiben stets $F := \mathbb{Q}(\pi_k) \subset E := End_k(\cdot) \otimes \mathbb{Q}$. Nach [Ta], Theorem 2,a) ist F das Zentrum von E. Welche Varietäten bzw. Grundkörper gemeint sind, sollte sich aus dem Zusammenhang erklären.
Sei $E|\mathbb{F}_p$ eine elliptische Kurve mit charakteristischem Polynom T^2+p. Dann hat man für die oben definierten E und F folgende Liste:

	F	E
$E\|\mathbb{F}_p$	$\mathbb{Q}(\sqrt{-p})$	$\mathbb{Q}(\sqrt{-p})$
$E\|\mathbb{F}_{p^2}$	$\mathbb{Q}$	D_p
$W\|\mathbb{F}_p$	$\mathbb{Q}(\sqrt{-p})$	$M_2(\mathbb{Q}(\sqrt{-p}))$

Dabei ist D_p die definite Quaternionenalgebra über $\mathbb{Q}$, die genau an den Stellen p und ∞ nicht zerfällt, und W ist die Weilrestriktion von E bzgl. $\mathbb{F}_p \subset \mathbb{F}_{p^2}$. Insbesondere hat die Restriktion einen nicht-kommutativen Endomorphismenring, obwohl der Endomorphismenring der Ausgangskurve kommutativ ist. Das liegt daran, daß E zwar supersingulär ist, der volle Endomorphismenring aber erst nach der quadratischen Erweiterung definiert ist. Diese Endomorphismen „vererben“ sich dann auf die Restriktion über $\mathbb{F}_p$. Die erste Zeile der Tabelle folgt aus der Irreduzibilität von T^2+p mit den bereits im

Beweis des Satzes verwendeten Ergebnissen. Das charakteristische Polynom von E über $\mathbb{F}_{p^2}$ ist $(T+p)^2$, damit folgt die zweite Zeile aus [Ta], Theorem 2,d2$\Leftrightarrow$d5. Das charakteristische Polynom von W über $\mathbb{F}_p$ ist $(T^2+p)^2$. Damit ist W isogen zur Potenz einer $\mathbb{F}_p$-einfachen abelschen Varietät A ([Ta], Theorem 2,e)) der Dimension

$$g = \frac{1}{2} m\, deg(\pi)\, (= m).$$

Dabei ist m die Ordnung von E in $Br(F)$, der Brauer-Gruppe von F (vgl. [Ta], Seite 142 ff.). Zu ihrer Berechnung reicht die Kenntnis von $||\pi||_v$ an allen reellen und p teilenden Stellen v von $F = \mathbb{Q}(\pi)$ aus. Im vorliegenden Fall hat F keine reellen Stellen, und weil $T^2 + p$ über $\mathbb{Q}_p$ irreduzibel, da Eisenstein, ist, hat man $||\pi||_v = p^{-1}$ für die einzige Stelle v von F, die p teilt. Damit erhält man $m = 1$, also ist $W \sim E \times E$ über $\mathbb{F}_p$, woraus sich die letzte Zeile der Tabelle ergibt.

Für die Gültigkeit von Satz 12 ist natürlich entscheidend, daß E bereits über k definiert ist. Insbesondere ist in diesem Fall E stets ein Isogeniefaktor der Weil-Restriktion, diese also nicht k-einfach. Man hat eine Art Umkehrung dazu. Dazu zunächst

Proposition 8 *Sei k ein endlicher Körper und A eine k- einfache abelsche Varietät. Sei ferner $l \neq char(k)$ eine Primzahl und K das Zenrum von $End_k^0(A) := End_k(A) \otimes \mathbb{Q}$. Dann ist $T_l(A)$ genau dann ein einfacher G_k-Modul, wenn l in K unzerlegt ist. Insbesondere existieren unendlich viele solche l.*

Beweis. Nach [Ta] ist

$$End_k^0(A) \otimes_{\mathbb{Q}} \mathbb{Q}_l \cong End_{G_k}(V_l(A)),$$

und V_l ist halb-einfach. Also ist V_l genau dann einfach, wenn das Zentrum der rechten Seite des Isomorphismus unzerlegt, d.h. ein Körper ist. Dieses Zentrum ist aber gerade $K \otimes \mathbb{Q}_l \cong \sum_{w|l} K_w$. Das ist offenbar genau dann ein Körper, wenn l in K unzerlegt ist. Die letzte Aussage ist aus der algebraischen Zahlentheorie wohlbekannt.

Satz 13 *Sei $k \subset K$ endliche Erweiterung endlicher Körper und $A|K$ eine K-einfache abelsche Varietät. Ist dann die Weil-Restriktion W nicht k einfach, so existiert ein echter Teilkörper $K' \subset K$ und eine abelsche Varietät $A'|K'$, so daß gilt:*

$$A' \times_{K'} K \sim_K A.$$

Beweis. Nach Proposition 8 existiert eine Primzahl l, verschieden von $char(k)$, so daß $V_l(A) = T_l(A) \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ G_K-einfach ist. Da W nicht k-einafch ist, besitzt der Ring $End_k^0(W)$ eine nicht-triviale Zerlegung. Das gleiche gilt dann für

$$\mathbb{Q}_l \otimes End_k^0(W) \cong End_{G_k}(V_l(W)).$$

Damit ist also $V_l(W)$ nicht G_k-einafch. Da $V_l(W)$ von $V_l(A)$ induziert wird, folgt aus dem Kriterium von Mackey ([Se], 7.4, Korollar zu Proposition 23) die Existenz eines $1 \neq \sigma \in Gal(K|k)$, für das $A^\sigma \sim_K A$ gilt. Der Fixkörper von $H := \{\sigma \in Gal(K|k) : A^\sigma \sim_K A\}$ erfüllt dann die Behauptung des Satzes.

Wir leiten jetzt noch die Liste aller quadratischen Teilkörper eines Kreisteilungskörpers ab.

Proposition 9 *Sei $G = \prod C_{n_i}$ endliches Produkt endlicher zyklischer Gruppen der Ordnungen n_i und $k := \#\{i : n_i \text{ ist gerade}\}$. Dann ist*

$$\#\{U \subset G : [G : U] = 2\} = 2^k - 1.$$

Beweis. Sei allgemeiner A eine abelsche Gruppe und p eine Primzahl, so daß $\nu := dim_{\mathbb{F}_p}(A/pA)$ endlich ist. Dann stehen die Untergruppen $U \subset A$ vom Index p in kanonischer Bijektion zu den 1-kodimensionalen $\mathbb{F}_p$-Untervektorräumen von A/pA. Deren Anzahl ist $\#\mathbb{P}^{\nu-1}_{\mathbb{F}_p} = (p^\nu - 1)/(p-1)$. Für G ist offenbar $\#2G = 2^{-k}\#G$, woraus die Behauptung folgt.

Satz 14 *Sei n eine natürliche Zahl mit Primfaktorzerlegung $n = 2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$ $(\alpha \geq 0, \alpha_i > 0)$. Dann sind genau die folgenden quadratischen Zahlkörper in $\mathbb{Q}(\zeta_n)$ enthalten:*

$$\mathbb{Q}(\sqrt{(\frac{-1}{k})}) \quad , falls \quad \alpha = 0, 1,$$

$$\mathbb{Q}(\sqrt{\pm k}), \mathbb{Q}(i) \quad , falls \quad \alpha = 2,$$
$$\mathbb{Q}(\sqrt{\pm k}), \mathbb{Q}(\sqrt{\pm 2k}), \mathbb{Q}(\sqrt{\pm 2}), \mathbb{Q}(i) \quad , falls \quad \alpha \geq 3,$$

Wobei stets $1 \neq k | p_1 \dots p_r$.

Beweis. Zunächst ist $Gal(\mathbb{Q}(\zeta_n)|\mathbb{Q}) \cong (\mathbb{Z}/n)^* \cong \prod(\mathbb{Z}/p_i^{\alpha_i})^* \times (\mathbb{Z}/2^\alpha)^* \cong \prod C_{(p_i-1)p_i^{\alpha_i-1}} \times A$, wobei $A = 1, C_2, C_2 \times C_{2^{\alpha-2}}$ je nach dem, ob $\alpha = 0, 1; 2 \, oder \geq 3$ ist (vgl. [L], Kapitel 9). Definiert man in Abhängigkeit davon $\nu := 0, 1$ oder 2, so folgt aus Proposition 9 und Galoistheorie, daß die Anzahl der gesuchten Teilkörper gleich $2^{r+\nu} - 1$ ist. Nach Kummertheorie und Restriktion an k sind die aufgelisteten Körper paarweise verschieden und in der richtigen Anzahl. Es bleibt also nur zu zeigen, daß alle aufgelisteten Körper tatsächlich in $\mathbb{Q}(\zeta_n)$ enthalten sind. Für eine Einheitswurzel ζ der primen Ordnung $p \neq 2$ ist $(\sum_{l=0}^{p-1}(\frac{l}{p})\zeta^l)^2 = (\frac{-1}{p})p$, offenbar ist $i \in \mathbb{Q}(\zeta_4)$ und schließlich berechnet man mit einer primitiven achten Einheitswurzel ζ: $(\zeta+\zeta^3)^2 = -2$. Wegen $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{2^\alpha}) \dots \mathbb{Q}(\zeta_{p_r^{\alpha_r}})$ ist die Aussage bewiesen.

4.2 der Fall n=3

Wir spezialisieren jetzt auf den Fall einer Erweiterung vom Grad 3 eines Primkörpers und wollen die Weil-Restriktion W einer elliptischen Kurve E untersuchen, die über dem Primkörper definiert ist. Nach Korollar 1 besteht die Zerlegung von W in Isogeniefaktoren fast immer aus E und einer $\mathbb{F}_p$-einfachen abelschen Fläche $\mathcal{A}$. Wir geben explizite Gleichungen für W und $\mathcal{A}$ an und untersuchen das Geschlecht von Kurven auf diesen Varietäten.

Zur Vereinfachung der Rechnung nehmen wir an, daß die Erweiterung $\mathbb{F}_p \subset \mathbb{F}_{p^3}$ von einer neunten Einheitswurzel ζ erzeugt wird und schreiben $\zeta^3 =: \mu \in \mathbb{F}_p$. Diese Annahme ist äquivalent zur Kongruenzbedingung $p \equiv 4, 7 \ (9)$. E sei durch die Gleichung

$$Y^2 = X^3 + AX + B \tag{4.4}$$

gegeben ($A, B \in \mathbb{F}_p$). Nach Proposition 2 führen wir die Substitutionen

$$\begin{aligned} X &= x_0 + x_1\zeta + x_2\zeta^2 \\ Y &= y_0 + y_1\zeta + y_2\zeta^2 \end{aligned} \tag{4.5}$$

ein und erhalten als Modell eines affinen Teils von W im $\mathbb{A}_k^6$ mit den Koordinaten $x_0, \ldots, y_2$:

$$\begin{aligned} y_0^2 + 2\mu y_1 y_2 &= x_0^3 + \mu x_1^3 + \mu^2 x_2^3 + 6\mu x_0 x_1 x_2 + A x_0 + B \\ \mu y_2^2 + 2 y_0 y_1 &= 3x_0^2 x_1 + 3\mu x_0 x_2^2 + 3\mu x_1^2 x_2 + A x_1 \\ y_1^2 + 2 y_0 y_2 &= 3x_0^2 x_2 + 3 x_0 x_1^2 + 3\mu x_1 x_2^2 + A x_2. \end{aligned} \tag{4.6}$$

Die Zerlegung

$$W \sim \mathcal{A} \times E$$

in Isogeniefaktoren entspricht der Faktorisierung

$$0 = \sigma^3 - 1 = (\sigma - 1)(\sigma^2 + \sigma + 1),$$

wobei σ ein Erzeugendes der Galois-Gruppe ist. Um die Gleichungen für $\mathcal{A}$ zu erhalten, muß man also $Spur(P) = 0$ für $P \in E(\mathbb{F}_{p^3})$ in den neuen Kordinaten entwickeln. $Spur(P) = 0$ ist äquivalent zu

$$P + P^\sigma = -P^{\sigma^2}. \tag{4.7}$$

Mit der üblichen Additionsformel erhält man aus (4.7), indem man nur die X-Koordinate beachtet:

$$\left(\frac{Y^\sigma - Y}{X^\sigma - X}\right)^2 = X + X^\sigma + X^{\sigma^2}. \tag{4.8}$$

Offenbar gilt für die Galois-Aktion

$$(x_0 + x_1\zeta + x_2\zeta^2)^\sigma = x_0 + x_1\mu\zeta + x_2\mu^2\zeta^2 \tag{4.9}$$

und analog für die y_i. Setzt man (4.9) in (4.8) ein, so erhält man leicht

$$(y_1(\mu - 1)\zeta + y_2(\mu^2 - a)\zeta^2)^2 = 3x_0(x_1(\mu - 1)\zeta + x_2(\mu^2 - 1)\zeta^2)^2 \tag{4.10}$$

und nach Ausmultiplizieren und Koeffizientenvergleich

$$\begin{aligned} y_1 y_2 &= 3 x_0 x_1 x_2 \\ y_2^2 &= 3 x_0 x_2^2 \\ y_1^2 &= 3 x_0 x_1^2. \end{aligned} \tag{4.11}$$

Wir definieren jetzt s durch

$$s^2 = 3x_0. \tag{4.12}$$

Damit berechnen wir nun also nicht mehr die Spur 0-Fläche $\mathcal{A}$, sondern eine quadratische Unterlagerung $\mathcal{A}'$. Aus (4.11) und (4.12) erhält man

$$\begin{aligned} y_1 &= sx_1 \\ y_2 &= sx_2. \end{aligned} \tag{4.13}$$

Substituiert man (4.13) in (4.6), so vereinfachen sich die erste und dritte Gleichung zu

$$\begin{aligned} y_0^2 &= x_0^3 + \mu x_1^3 + \mu^2 x_2^3 + Ax_0 + B \\ 2y_0y_2 &= 3x_0^2x_2 + 3\mu x_1x_2^2 + Ax_2. \end{aligned} \tag{4.14}$$

Nochmaliges Einsetzen von (4.13) in (4.14) und Kürzung der zweiten Gleichung mit x_2 liefert

$$\begin{aligned} y_0^2 &= x_0^3 + \mu x_1^3 + \mu^2 x_2^3 + Ax_0 + B \\ 2y_0s &= 3x_0^2 + 3\mu x_1x_2 + A. \end{aligned} \tag{4.15}$$

Quadrieren der zweiten Gleichung, Multiplikation der ersten mit $12x_0$ und Gleichsetzen der linken Seiten führt schließlich zu

$$(3x_0^2 + 3\mu x_1x_2 + A)^2 = 12x_0(x_0^3 + \mu x_1^3 + \mu^2 x_2^3 + Ax_0 + B). \tag{4.16}$$

Die Gleichung (4.16) beschreibt $\mathcal{A}'$ im $\mathbb{A}_k^3$. Diese Fläche wird jetzt durch Faserung über $\mathbb{A}_k^1$ mit der Koordinatenfunktion x_0 auf Kurven untersucht. Aus (4.12) erkennt man, daß die folgenden Resultate über Kurven auf $\mathcal{A}'$ auch für die eigentlich interessierende Fläche $\mathcal{A}$ gelten. Fixiere also x_0 und betrachte die ebene, affine Kurve C, die durch Gleichung (4.16) in den Koordinaten x_1, x_2 gegeben wird.

1.) Homogenisiert man (4.16) mit x_3 und setzt $x_3 = 0$, so erhält man $9\mu^2x_1^2x_2^2 = 0$, das heißt, C hat die beiden unendlichen Punkte $P_1 = [0:1:0]$ und $P_2 = [1:0:0]$.

2.) Ableiten nach x_3 und einsetzen von P_i ergibt $-12\mu^2x_0 = 0$ bzw. $-12\mu x_0 = 0$. Im Folgenden sei $x_0 \neq 0$. Dann sind also die unendlichen Punkte auf C nicht-singulär.

3.) Die Galois-Operation induziert einen wieder mit σ bezeichneten Automorphismus der Ordnung 3 von C durch $(x_1, x_2)^\sigma = (\mu x_1, \mu^2 x_2)$.

Dieser hat als einzigen Fixpunkt $(0,0)$, und $(0,0) \in C$ gilt genau dann, wenn $(3x_0^2 + A)^2 - 12x_0(x_0^3 + Ax_0 + B) = 0$ ist. Diese Gleichung ergibt ausmultipliziert $3x_0^4 + 6Ax_0 + 12Bx_0 - A^2 = 0$, und das ist das dritte Teilungspolynom von E. Schließt man also für x_0 die x-Koordinaten rationaler 3-Teilungspunkte von E aus, so tauchen Singularitäten von C im Endlichen notwendigerweise in Tripeln auf. C ist eine ebene Kurve vom Grad 4, hat also arithmetisches Geschlecht 3. Weil das geometrische Geschlecht der Normalisierung von C nicht-negativ ist, ist C entweder nicht-singulär oder hat genau 3 singuläre Punkte. In letzterem Fall wäre C eine rationale Kurve. Solche können aber nicht auf einer abelschen Fläche liegen (vgl. [M1]).

Man hat also folgende

Proposition 10 *Auf $\mathcal{A}$ liegt eine Einparameterfamilie von nicht-singulären Kurven vom Geschlecht 3, die alle eine Automorphismus der Ordnung 3 besitzen.*

Wir haben keine über $\mathbb{F}_p$ definierte Kurve vom Geschlecht 1 auf $\mathcal{A}$, weil $\mathcal{A}$ $\mathbb{F}_p$-einfach ist. Die Existenz einer solchen Kurve vom Geschlecht 2 ist gleichbedeutend damit, daß $\mathcal{A}$ isogen zur Jacobischen einer über $\mathbb{F}_p$ definierten Kurve ist. Das halten wir für einen Ausnahmefall, aber beweisen können wir nichts. In diesem Sinne ist das minimale Geschlecht einer Kurve auf $\mathcal{A}$ mindestens 2, wahrscheinlich aber 3.

Man hat einen Projektionsoperator

$$\pi : W \longrightarrow \mathcal{A}$$

von der Weil-Restriktion auf die Spur 0-Fläche, der durch die Abbildung $P \mapsto P^\sigma - P$ induziert wird. Die explizite Formel für π in den gewählten Koordinaten ist sehr lang und leider wenig aufschlußreich. Wenigstens kann man sehen, das im Allgemeinen eine Kurve C' auf W vermöge π eine Kurve C auf $\mathcal{A}$ vom Grad 7 überlagert. Damit liefert die Hurwitz-Geschlechtsformel als untere Abschätzung für das minimale Geschlecht einer Kurve auf W die Schranke $g \geq 15$. Bei zahlreich durchgeführten Experimenten (wählen zufälliger Hyperschnitte und Berechnung des Geschlechts des enstehenden Funktionenkörpers mit MAPLE) konnte diese Schranke auch nicht unterschritten werden.

Kapitel 5

Kryptographische Anwendungen

5.1 Das DL-Problem auf elliptischen Kurven

Von G. Frey wurde 1998 ein möglicher Angriff auf **spezielle Klassen** des DL-Problems auf elliptischen Kurven vorgeschlagen, der die Weil-Restriktion benutzt ([Fr1]). Wir geben nur eine kurze Beschreibung der Idee, etwas ausführlicher ist sie in [GS] beschrieben.

Sei k ein (kleiner) endlicher Körper und $k \subset K$ eine Erweiterung von Primzahlgrad n sowie $E|k$ eine elliptische Kurve. Ferner sei ein $P \in E(K)$ von Primzahlordnung gegeben und gefragt ist nach dem DL-Problem in der von P erzeugten Gruppe. Ist W die Weil-Restriktion von E bzgl. $k \subset K$ so hat man einen im wesentlichen durch Substitution gegebenen Isomorphismus

$$E(K) \cong W(k).$$

Wir wissen, daß die Zerlegung von W in k-einfache Isogeniefaktoren fast immer die Gestalt

$$W \sim E \times A$$

hat, wobei A eine k-einfache abelsche Varietät der Dimension $n-1$ ist (vgl. Korollar 1). Da bei kryptographischen Anwendungen die Ordnung von P stets groß ist, folgt, daß P unter dem obigen Isomorphismus einem $P' \in A(k)$ entspricht. Sei nun C eine über k definierte Kurve auf A vom Geschlecht g,

die einen k- rationalen Punkt besitzt. Dann erhält man aus der universellen Eigenschaft der Jacobischen J_C einen Morphismus abelscher Varietäten

$$f : J_C \longrightarrow A,$$

der wegen der Einfachheit von A surjektiv ist. Man bestimmt nun ein Urbild D von P' unter f. Damit hat man das DL-Problem in die Jacobische „zurückgezogen". Ist nun C hyperelliptisch, so gibt es für dieses Problem einen Algorithmus, der subexponentiell in g ist ([AMH]). Aus der Surjektivität von f folgt sofort, daß das Geschlecht einer solchen Kurve C mindestens $n-1$ sein muß. Die Frage ist also, ob man auf A Kurven vom Geschlecht der Größenordung n finden kann. Denn es gilt ja

$$|J_C(k)| \sim |k|^g$$

und

$$|E(K)| \sim |k|^n.$$

Ist also $g \gg n$, so verlagert man das DL-Problem in eine wesentlich größere Gruppe und kann sich keinen Gewinn erhoffen.

Die Existenz solcher Kurven C ist völlig unklar, wir können nur einige wenige Fakten zusammenfassen:

Für den Fall $n = 3$ haben wir in Kapitel 4 auf A eine 1-Parameterfamilie von ebenen, nicht-singulären Kurven vom Grad 4 und Geschlecht 3 gefunden. Das Geschlecht ist zwar fast kleinstmöglich, aber andererseits sind ebene Kurven vom Grad 4 genau die kanonischen Kurven vom Geschlecht 3 (vgl. [H], V, Beispiel 5.2.1), d.h. keine dieser Kurven ist hyperelliptisch. Ferner haben wir gesehen,daß das minimale Geschlecht einer Kurve auf der gesamten Weil-Restriktion 15 ist. Das scheint zumindest zu suggerieren, daß das minimale Geschlecht auf A wesentlich kleiner ist als das auf W. Das hieße, daß die oben betrachteten Kurven E, die bereits über dem Grundkörper k definiert sind, anfälliger gegen diesen Angriff sind als Kurven, die echt über K definiert sind. Denn in diesem Fall ist die Weil-Restriktion einfach, und man wird schwieriger Kurven kleinen Geschlechtes finden. Insbsondere sollten die Angriffsmöglichekeiten für zusammengesetzte Körpergerade besser sein, weil dann nach Satz 12 in der Weil-Restriktion Isogeniefaktoren kleiner Dimension auftauchen.

Für allgemeines n können wir zur Existenz der fraglichen Kurven nicht viel mehr sagen, als das direkte Anwendung von Eliminationstheorie Kurven vom Geschlecht $\sim exp(n)$ liefert, was uninteressant ist. Eine letzte Bemerkung zum allgemeinen Fall wäre, daß die hier als Weil-Restriktionen auftretenden abelschen Varietäten von recht spezieller Natur sind: Aus Proposition 2 folgt sofort, das sie alle lokal vollständige Durchschnitte von Hyperflächen vom Grad 3 in einem $\mathbb{P}^{2n}$ ($n=$ Dimension der Weil-Restriktion) sind, was wesentlich mehr ist, als man von allgemeinen abelschen Varietäten erwarten kann (vgl. [M3]). Es scheint sehr unwahrscheinlich, daß durch Weil-Restriktion ein Angriff auf allgemeine elliptische Kurven möglich ist. Es ist jedoch durchaus denkbar, daß spezielle Klassen elliptischer Kurven Weil-Restriktionen besitzen, die im Bezug auf die Frage nach Kurven, die auf ihnen ligen, wesentlich einfacher zu behandeln sind. Solche elliptischen Kurven hätten dann möglicherweise ein Sicherheitsproblem.

5.2 Konstruktion kryptographisch geeigneter abelscher Varietäten

In diesem Abschnitt soll die Möglichkeit diskutiert werden, mit Hilfe der Ergebnisse aus Kapitel 4 kryptographisch geeignete abelsche Flächen über einem Primkörper zu konstruieren. Sei dazu $E|\mathbb{F}_p$ eine elliptische Kurve über einem Primkörper (man stelle sich $p \sim 10^{20}$ vor). Es sei daran erinnert, daß wir $p \equiv 4,7 \bmod (9)$ voraussetzen mußten. Wir wissen, daß die Weil-Restriktion fast immer eine $\mathbb{F}_p$-einfache Fläche als Faktor besitzt. Dies sei im Folgenden der Fall. Die Eignung der Fläche $\mathcal{A}$ soll anhand folgender Punkte untersucht werden, wobei wir die Ergebnisse stets mit der Situation vergleichen, daß man entweder in $E'(\mathbb{F}_{p'})$ ($p' \sim p^2$) oder in $E'(\mathbb{F}_{p^2})$ rechnet (Fälle 2 und 3), wobei bei letzterem vorausgesetzt sei, daß E' nicht bereits über $\mathbb{F}_p$ definiert ist:

1.) Man muß auf den fraglichen Varietäten (möglichst) schnell rechnen können.
2.) Man muß die (Ordnung der) Mordell-Weil Gruppe bestimmen können und wissen, daß mit vernünftig hoher Wahrscheinlichkeit große zyklische Untergruppen von Primzahlordnung auftauchen.

3.) Die Schlüssellänge (d.h. die zur Darstellung eines Punktes auf der Varietät benötigte Bitanzahl) sollte mit der Sicherheit (d.h. der Ordnung der zyklischen Gruppe, in der man rechnet) vergleichbar sein.
4.) Man muß einen Basispunkt großer Ordnung finden können.

5.2.1 Rechnen auf $\mathcal{A}$

Wir benutzen die Bezeichnungen aus Kapitel 4. Man hat einen Isomorphismus

$$\begin{array}{rcl} \mathcal{W}(\mathbb{F}_p) & \stackrel{\cong}{\longrightarrow} & E(\mathbb{F}_{p^3}) \\ (x_0, \ldots, y_2) & \mapsto & (x_0 + x_1\zeta + x_2\zeta^2, y_0 + y_1\zeta + y_2\zeta^2), \end{array}$$

der

$$\mathcal{A}(\mathbb{F}_p) \cong A := \{P \in E(\mathbb{F}_{p^3}) : Spur(P) = 0\}$$

identifiziert.
Damit ist das Rechnen auf $\mathcal{A}$ zunächst äquivalent zum Rechnen auf E über $\mathbb{F}_{p^3}$. Für kleine n (n=2,3) braucht eine elliptische Addition über einem Körper mit $\sim p^n$ Elementen etwa $n^2\, log(p)^2$ elementare Operationen. Das heißt, eine elliptische Addition auf $\mathcal{A}$ kostet etwa $9\, log(p)^2$ elementare Operationen, während der Preis in den Fällen 2 und 3 jeweils nur etwa $4\, log(p)^2$ beträgt. Man kann jedoch die Arithmetik auf $\mathcal{A}$ folgendermaßen zu beschleunigen versuchen:
Bezeichnet π den vom Frobenius induzierten Endomorphismus von A, so gilt nach Definition von A:

$$\pi^2 + \pi + 1 = 0.$$

Außerdem erfüllt π natürlich sein charakteristisches Polynom

$$\pi^2 - a\pi + p = 0,$$

wobei nach Hasse-Weil $|a| \leq 2\sqrt{p}$ gilt. Man erhält unschwer die in $End(A)$ gültige Relation

$$(1 + a)\pi = p - 1.$$

Aus Kapitel 4 erkennt man, daß die Anwendung des Frobenius auf einen Punkt vernachlässigbare Zeitkomplexität hat (man braucht 4 bzw. bei Beschränkung auf die X-Koordinate 2 Multiplikationen in $\mathbb{F}_p$). Man kann ohne

Einschränkung davon ausgehen, daß $1 + a \in Aut(A)$ gilt, denn eigentlich ist man nur am Rechnen in einer zyklischen Untergruppe von A großer Primordnung interessiert. Sei also ein $P \in \mathcal{A}(\mathbb{F}_p)$ mit $ord(P) = q$ prim in der Größenordnung $q \sim p^2$ gegeben. Setze

$$C := min\{\frac{q}{a+p}, \frac{p-1}{(p-1, a+1)}\},$$

wobei $(\cdot, \cdot)$ den größten gemeinsamen Teiler bezeichnet. Betrachte

$$\phi : \mathbb{Z}^2 \longrightarrow End(< P >)$$

definiert durch $(\lambda_1, \lambda_2) \mapsto \lambda_1 + \lambda_2\pi$ und setze $X := \{(\lambda_1, \lambda_2) : 0 \leq \lambda_i < C\} \subset \mathbb{Z}^2$. Dann hat man

Proposition 11 *Die Einschränkung von ϕ auf X ist injektiv.*

Beweis. Hat man $(\lambda_1, \lambda_2), (\lambda_1', \lambda_2') \in X$ mit

$$\lambda_1 + \lambda_2\pi = \lambda_1' + \lambda_2'\pi \quad \text{in } End(< P >),$$

so gilt für $\alpha_i := \lambda_i - \lambda_i'$:

$$\alpha_1 + \alpha_2\pi = 0 \quad und\, |\alpha_i| < C.$$

Durch Multiplikation mit $a + 1$ folgt

$$(a+1)\alpha_1 + (p-1)\alpha_2 = 0 \quad \text{in } End(< P >),$$

wegen der Wahl von C also auch

$$(a+1)\alpha_1 + (p-1)\alpha_2 = 0 \quad \text{in } \mathbb{Z}.$$

Wieder wegen der Wahl von C folgt $\alpha_1 = \alpha_2 = 0$.

Man kann also mindestens C^2 Endomorphismen von $< P >$ in der Form

$$\lambda_1 + \lambda_2\pi \quad \text{mit } 0 \leq \lambda_i < p$$

darstellen. Der Verlust der Schlüssellänge gegenüber $q \sim p^2$ hängt also im Wesentlichen von $(p-1, a+1)$ ab. Die Endomorphismen dieser speziellen

Form können folgendermaßen schnell implementiert werden:
Man berechnet zunächst

$$(2^i P, \pi 2^i P, -\pi^2 2^i P) \quad \text{für} \, 0 \leq i < log(p).$$

Da π und -1 praktisch kostenfrei sind, braucht man dazu $log(p)$ elliptische Additionen. Dann entwichelt man die λ_i 2-adisch und summiert über i. Bei jedem Schritt hat man einen Punkt der Form

$$0, 2^i P, \pi 2^i P \quad \text{oder} \, 2^i P + \pi 2^i P = -\pi^2 2^i P$$

zu addieren. Wegen der gemachten Vorrausberechnung hat man $\frac{3}{4}log(p)$, gesamt also $\frac{7}{4}log(p)$, elliptische Additionen und damit $\frac{7}{4}log(p).3log(p) = \frac{21}{4}log(p)^2$ elementare Operationen zur Berechnung von kP zu erwarten.
In den Fällen 2 und 3 muß man $k \sim p^2$ 2-adisch entwickeln ($2log(p) + log(p) = 3log(p)$ elliptische Additionen) und braucht zur Berechnung von kP etwa $3log(p).2log(p) = 6log(p)^2$ elementare Operationen.
Die speziellen Multiplikationen in $Im(\phi)$ sind also sogar schneller als in den Fällen 2 und 3, man muß aber eine geeignete Kurve finden (d.h. $(p-1, a+1)$ klein), um bei der Schlüssellänge keine großen Einbußen zu erleiden, vgl. den Anhang. Eine minimale Änderung des Protokolls besteht bei dem beschriebenen Verfahren darin, die übliche Zahl k durch das Tupel (λ_1, λ_2) zu ersetzen.

5.2.2 Die (Ordnung der) Mordell-Weil Gruppe

Aus der Kenntnis von $|E(\mathbb{F}_p)|$ berechnet man zunächst

$$a_p := Spur(\pi) = 1 + p - |E(\mathbb{F}_p)|.$$

Vergleiche [Si1], Kapitel V). Und daraus dann die Weil-Zahl α von $E|\mathbb{F}_p$ mit Hilfe von

$$\alpha^2 - a_p \alpha + p = 0.$$

Wegen $\mathcal{W} \sim E \times \mathcal{A}$ und $\mathcal{W}(\mathbb{F}_p) \cong E(\mathbb{F}_{p^3})$ erhält man

$$|\mathcal{A}(\mathbb{F}_p)| = \frac{|\mathcal{W}(\mathbb{F}_p)|}{|E(\mathbb{F}_p)|} = \frac{(1-\alpha^3)(1-\bar{\alpha}^3)}{(1-\alpha)(1-\bar{\alpha})}.$$

Damit ist die Konstruktion von Flächen mit geeigneter Gruppenordnung ziemlich einfach, vergleiche die Beispiele im Anhang.

Die Chance auf große zyklische Untergruppen dürften für $\mathcal{A}(\mathbb{F}_p)$ genausogut wie in den Fällen 2 und 3 sein, denn es ist $A \subset E(\mathbb{F}_{p^3})$. *MAPLE* hat etwa eine halbe Stunde gebraucht, um aus 20 zufällig gewählten elliptischen Kurven die folgenden beiden interessanten Fälle herauszusuchen. Wir wählen

$$p = 31415926535897932333$$

und haben als erstes Beispiel

$$a_p = 7405961513$$

$$|\mathcal{A}(\mathbb{F}_p)| = 9869604403416010014831924339426684010 68$$

$$= 2^2\, 3^2\, 27415567787266694485644234276185233363.$$

Und als zweites Beispiel

$$a_p = 5062396712$$

$$|\mathcal{A}(\mathbb{F}_p)| = 9869604402679757418336397713336573873 09$$

$$= 3^2\, 10966227114088619353707108570373970970 1.$$

5.2.3 Vergleich von Schlüssellänge und Sicherheit

In den Fällen 2 und 3 ist dieser Vergleich leicht zu erbringen. Wir betrachten nur den zweiten Fall, d.h. wir rechnen in $E(\mathbb{F}_p)$. Der Satz von Hasse-Weil besagt, daß $|E(\mathbb{F}_p)| \sim p$. Damit ist die Sicherheit $\sim p$. Einen Punkt auf der elliptischen Kurve übergibt man üblicherweise durch seine X-Koordinate plus einem weiteren Bit zur Bestimmung des Vorzeichens von Y. Damit beträgt die Schlüssellänge also $2p$. Der Grund für dieses nahezu optimale Verhältnis liegt natürlich an der besonderen Form

$$Y^2 = f(X)$$

der Gleichung für E. Insbesondere hat E Irrationalitätsgrad 2. Aus Satz 8 folgt, daß $\mathcal{A}$ geometrisch isomorph zu $E \times E$ ist, also Irrationalitätsgrad 4 hat. Schreibt man die Gleichung für $\mathcal{A}'$ aus Kapitel 4 als Polynom in x_0, so erhält man

$$F := 3x_0^4 + (6A - 18\mu x_1 x_2)x_0^2 + (12B + 12(\mu x_1^3 + \mu^2 x_2^3))x_0 - (A + 3\mu x_1 x_2)^2 = 0.$$

Die obigen Überlegungen zeigen, daß dieses Polynom irreduzibel über $\mathbb{F}_p(x_1, x_2)$ ist.
Die ökonomischste Kodierung eines Punktes $P \in \mathcal{A}(\mathbb{F}_p)$ bestünde also in der Übergabe eines Vektors

$$(x_1, x_2, \nu, s),$$

wobei $1 \leq \nu \leq 4$ anzeigt, die wievielteste Nullstelle von F x_0 ist (im Bezug auf eine festgewählte Anordnung von $\mathbb{F}_p$), und s wie üblich das Vorzeichen von Y ist. Die so erreichte Schlüssellänge ist $8p^2$ und im Vergleich zur Sicherheit von $\sim p^2$ sehr gut. Die beschriebene Umrechnung

$$P = (X, Y) \in \mathcal{A}(\mathbb{F}_p) \leftrightarrow (x_1, x_2, \nu, s)$$

ist leider extrem aufwendig, denn in beiden Richtungen muß man ein Polynom vom Grad 4 über $\mathbb{F}_p$ faktorisieren. In der Anwendung wird man diese Umrechnung jedoch nicht allzuoft vornehmen müssen.

Eine Idee wäre es vielleicht, die Erweiterung $\mathbb{F}_p(x_1, x_2) \subset \mathbb{F}_p(x_1, x_2)(x_0)$ statt durch F durch eine reine Gleichung in x_0 zu beschreiben.

5.2.4 Berechnung eines Basispunktes

In den Fällen 2 und 3 läßt man zum Auffinden eines rationalen Punktes auf E bekanntermaßen X variieren und muß nicht lange warten, bis die Auswertung des quadratischen Residuums $(\frac{f(X)}{p}) = 1$ ergibt. Um ein $Q \in \mathcal{A}(\mathbb{F}_p)$ zu finden, muß man nur wenig mehr tun:
Hat man $P \in E(\mathbb{F}_{p^3} - \mathbb{F}_p)$ (man kann natürlich von Anfang an die Suche auf nicht-rationale Punkte von E beschränken), so hat

$$Q := P - P^\pi$$

die gewünschten Eigenschaften, denn offenbar ist $Spur(Q) = 0$ und $Q \neq 0$, weil P nicht rational ist. Die Chancen, eine hohe Ordnung zu haben, sind

für P und Q wohl gleichgut.

5.2.5 Zusammenfassung

Der beschriebene Angriff auf das DL-Problem auf elliptischen Kurven steckt bestenfalls in den Kinderschuhen, nichtsdestotrotz gibt es Hinweise wie die spezielle Gestalt der auftauchenden abelschen Varietäten, die Motivation für weitere Untersuchungen in dieser Richtung sein könnten. Es hat sich zum Beispiel im Laufe dieser Arbeit der Verdacht ergeben, daß Weil-Restriktionen bestimmter elliptischer Kurven die Jacobischen von Fermat-Kurven sein könnten.
Das beschriebene Konstruktionsverfahren für kryptographisch geeignete Flächen scheint in allen Bereichen mit gängigen Verfahren vergleichbar zu sein, bzw. bei der Bestimmung der Gruppenordnung sogar Vorteile zu haben. Man sollte auch einen Sicherheitsbonus nicht außer acht lassen, den diese Konstruktion hat: Die Fläche, auf der man rechnet, ist $\mathbb{F}_p$-einfach, d.h. insbesondere, daß sie die zur Konstruktion verwendete elliptische Kurve nicht enthält, die man dann wohl „versteckt“ hat.

Anhang A

Numerische Beispiele

In diesem Anhang sollen einige Beispiele für die in Kapitel 5 erwähnten Konstruktionsmöglichkeiten gegeben werden. Wir betrachten zunächst die folgenden elliptischen Kurven über $\mathbb{Q}$, die den angegebenen Endomorphismenring haben. Das habe ich in [Si2], Anhang A abgeschrieben.

$$E_1 : Y^2 = X^3 + 4X^2 + 2X \quad ; \quad \mathbb{Z}[\sqrt{-2}]$$

$$E_2 : Y^2 + XY = X^3 - X^2 - 2X - 1 \quad ; \quad \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$$

Dies sind global minimale Weiserstrass-Gleichungen, die wir für unsere Zwecke zunächst in die kurze Weierstrass-Form überführen:

$$E_1 : Y^2 = X^3 - \frac{10}{3}X + \frac{56}{27}$$

$$E_2 : Y^2 = X^3 - \frac{35}{16}X - \frac{49}{32}.$$

Nun sucht man rationale Primzahlen $p \sim 10^{25}$, die in dem Endomorphismenring zerlegt sind und der zusätzlichen Kongruenzbedingung $p \equiv 4, 7 \bmod (9)$ gehorchen. Dann löst man in dem Endomorphismenring die Norm-Gleichung $N(\alpha) = p$ und erhält, weil die Einheitengruppen der gewählten Endomorphismenringe $\{+1, -1\}$ sind, zwei Lösungen $\alpha_{1,2}$, die sich um ein Vorzeichen unterscheiden (natürlich erhält man 4 Lösungen, aber Konjugierte sind als gleich anzusehen). Eine der beiden Lösungen ist die Weil-Zahl der bei p reduzierten Kurve, die andere ist die Weil-Zahl eines quadratischen Twists. Das

kann man leicht zuordnen, indem man die durch die Weil-Zahl bestimmte Ordnung der Punktegruppe berechnet, und einen zufällig gewählten Punkt auf der elliptischen Kurve mit dieser Ordnung multipliziert.
Die folgenden beiden Tabellen wurden so erstellt: Ab 10^{25} wurden alle „geeigneten“ Primzahlen p erzeugt (s.o.) und dann, wie in Kapitel 5 beschrieben, zunächst die Weil-Zahl der reduzierten Kurve und aus ihr dann die Punkteordnung der Fläche $\mathcal{A}$ berechnet. Letztere wurde faktorisiert, und die Ordnungen mit großen Primfaktoren kamen dann in die Liste . In Kapitel 5 wurde erläutert, daß der ggT(Spur der Weil-Zahl+1, p-1) klein sein sollte. Obwohl die aufgelisteten Beispiele erst im Nachhinein darauf untersucht wurden, ist in keinem der Beispiele dieser ggT größer als 5.

Beispiele für die Kurve E_1

Es bezeichnet $z := \sqrt{2}$ und α die Weil-Zahl.

p	10000000000000000000001113
α	$2747855356501 + 1106637009084 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.18433.602783654918744504765922832859161088670518137$
p	10000000000000000000002217
α	$2943895426765 + 816541400136 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.855787.1298350069715671434709021762892988143215881 1$
p	10000000000000000000003009
α	$680388315041 + 2183697751608 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	163.61349693251542090654209197455038675505068670505 9
p	10000000000000000000010857
α	$1356586233073 + 2019860613042 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.28387.391415475785187788325949661469862419465852019$
p	10000000000000000000011649
α	$1622005665329 + 1919517858948 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	433.499.462819403240811600631005940396310178001360451
p	10000000000000000000012633
α	$2460576803099 + 1404557189304 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	1000000000000492115363146542177528779694348843007 93
p	10000000000000000000013953
α	$924571727435 + 2138360016558 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	67.163.915667063455896817460193694893613613131369897
p	10000000000000000000018249
α	$2486291691299 + 1381729645368 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	16921.590981620471897203677034304867239451801989921 7
p	10000000000000000000020739
α	$271655568241 + 2227801971927 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.163.681663258350411950318879\ 279449127486664184267 61$
p	10000000000000000000021273
α	$2328646766071 + 1512845702454 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.19.241.24265366043058060453700927347160501713370081\ 39$

p	10000000000000000000024411
α	$3065431760323 + 549148487571 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.43.2583979328166958879475315\ 44153714879727408088217$
p	10000000000000000000024627
α	$1948441439185 + 1761189364899 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.409.2716653083402308308320 46\ 3058562789016726116 5123$
p	10000000000000000000027993
α	$3118944931099 + 368905487064 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.11111111111180420999090965456966 7\ 8615119223926897$
p	10000000000000000000032691
α	$2746602408863 + 1108191140469 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$43.139.167308014053965086245 32\ 5581688638696791015314 67$
p	10000000000000000000033393
α	$2389300526041 + 1464794012184 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.43.2583979328166609457653454\ 5952203662670749851 3747$
p	10000000000000000000037113
α	$2613752056345 + 1258630245138 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.11111111111116919449096575258533 27\ 1356050359416713$
p	10000000000000000000038739
α	$779091372367 + 2167142892555 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.19.5847953216375180223872638\ 1536803231784083530 0569$
p	10000000000000000000041217
α	$2467433629237 + 1398529814718 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.11111111111116594297045454928101 67\ 3573783675932209$
p	10000000000000000000042369
α	$2869352889781 + 939897333198 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$3^2.19.5847953216377624974189650\ 4639031735396063047 9787$

Beispiele für die Kurve E_2

Es bezeichnet $z := \sqrt{7}$ und α die Weil-Zahl.

p	1000000000000000000000001821
α	$2906938089039 + 470518095370 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	7039.142065634323139847651395402473584635055739121 39
p	1000000000000000000000003009
α	$2407532541879 + 774945810068 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	1033.968054211036284130211982315439029770752966762 49
p	1000000000000000000000003333
α	$2136161033165 + 881299044462 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	1000000000000427232207299682527358526941626999186 77
p	1000000000000000000000003729
α	$2820852672273 + 540210303140 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	127.787401574803593835067087101014482013562689141767
p	1000000000000000000000004191
α	$497125030928 + 1180367176749 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	1000000000000099425007023709885331896685561030253 79
p	1000000000000000000000005181
α	$454565028209 + 1182815686350 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	1000000000000090913006677908265174641937078421863 81
p	1000000000000000000000011409
α	$2672518722647 + 638932555920 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	7.37.3861003861005924724891163651 32 916419235086578011
p	1000000000000000000000012633
α	$2218957583571 + 851572263716 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	127.787401574803499048440347162953473124548237619687

p	10000000000000000000013089
α	$741933280071 + 1161866417692 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	7.43.79.42053913116621741312024556205837077981187243 63

p	10000000000000000000014883
α	$2884546993774 + 489808802451 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	3^2.11111111111175212155747959202717247810753679117 27

p	10000000000000000000020739
α	$675373968858 + 1167651489235 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	79.499.15817.160379275945872596560046933238182692030747

p	10000000000000000000021477
α	$2402526936483 + 777161898878 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	7.127.11248593925764685100017909233806841991957706461 3

p	10000000000000000000030693
α	$1447197037875 + 1062720278582 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	757.13210039630122713862796744831904511 8331875087401

p	10000000000000000000070251
α	$3156565832626 + 71805435825 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	3^2.111111111111181257 02006396650625762924180140737 751

p	10000000000000000000150249
α	$246815365557 + 1191582511700 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	2251.4442470013327629334087788105005391953273304849 9

p	10000000000000000000150267
α	$2564671769262 + 699230057783 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	227371.43980982623136324965976574105829638333000646 1

p	10000000000000000000150303
α	$3116662358204 + 202278360171 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	10000000000006233325017016885433795707653439025200 3

p	10000000000000000000070887
α	$2160716057912 + 872705654607 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	2767.361402240694048 47966236352972452417062803831 813

p	10000000000000000000032241
α	$108133281273 + 1194529626104 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	43.232558139534888750386675046620398216 3914662303723

Noch eine kleine Bemerkung: Man kann **nicht** die über $\mathbb{Q}$ definierte elliptische Kurve mit Endomorphismenring $\mathbb{Q}(\sqrt{-3})$ verwenden, weil aus Satz 12 folgt, daß in diesem Fall die Fläche $\mathcal{A}$ über $\mathbb{F}_p$ in zwei elliptische Kurven zerfällt. Das spiegelt sich natürlich in der Zerlegung der Gruppenordnung in Primfaktoren wieder. Wir geben auch in diesem Fall die Liste der Daten zu den ersten 5 „geeigneten“ Primzahlen $> 10^{25}$ ($z := \sqrt{-3}$):

p	1000000000000000000000000561
2α	$1460788713059 + 3552749936589 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$2^4.3^2.5^2.7^2.19.2113.11329.219522091.3376987039.1681315124691551731$
p	1000000000000000000000000609
2α	$5431307509453 + 1870908757597 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$2^2.7.13.307.739.1291.284659.16308738337.285327229657.708110536051$
p	1000000000000000000000001113
2α	$1507417475287 + 3546251192231 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$2^6.7.13.3319039.33109014353269\ 039.1562500000000948919\ 61361$
p	1000000000000000000000001371
2α	$3748240973441 + 2941127312501 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$2^2.3^3.733.919.66090031177.68807980867.302260911619099438141$
p	1000000000000000000000001527
2α	$4621656141365 + 2492675571281 * z$
$\lvert\mathcal{A}(\mathbb{F}_p)\rvert$	$2^2.3^3.7^2.907.6271.76207.83036262493453.525017063054474290687$

Literaturverzeichnis

[A-M] M.F. Atiyah, I.G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, 1969.

[AMH] Adleman, DeMarris, Huang, *A subexponential algorithm for discrete logarithms [...]*, Algorithmic number theory (Ithaca, NY, 1944), 28-40, Lecture Notes in Comp. Sci., **877**, Springer, Berlin, 1994.

[BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Springer, NY, 1980.

[E] D. Eisenbud, *Commutative Algebra with a View toward Algebraic Geometry*, Springer, NY, 1995.

[E-H] D. Eisenbud, J. Harris, *Schemes: the language of modern algebraic geometry*, Wadsworth & Brooks/Cole Advanced Books, 1992.

[Fa] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent.math., **73**, 349-366, 1983.

[Fr1] G.Frey, *How to disguise an elliptic curve*, Vortrag in Waterloo (ECC 98), 1998.

[GS] S. Galbraith, N. Smart, *A cryptographic application of weil descent*, Preprint, 1999.

[H] R. Hartshorne, *Algebraic Geometry*, Springer, NY, 1997.

[K] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer, NY, 1994.

[L] F. Lorenz, *Einführung in die Algebra I*, Spektrum Akademischer Verlag, 1996.

[Ma] Y. Matsumura, *Commutative ring theory*, Cambridge University Press, 1986.

[M1] D. Mumford, *Lectures on curves on an algebraic surface*, Princeton Univerity Press, 1966.

[M2] D.Mumford, *Abelian Varieties*, Oxford University Press, 1974.

[M3] D.Mumford, *On the equations defining Abelian Varieties*, Inv.math., **1**, 1966.

[Mi1] J.S. Milne, *Lectures on Étale Cohomology*, Vorlesungsskript, 1998.

[Mi2] J.S. Milne, *On the Arithmetic of Abelian Varieties*, Invent. math., **17**, 1972.

[Sh] I.R. Shafarevich, *Basic algebraic geometry*, Springer, Berlin, 1994.

[Se] J.P. Serre, *Linear Representation of Finite Groups*, GTM 42, Springer, NY, 1977.

[Si1] J.H. Silverman, *The Arithmectic of Elliptic Curves*, Springer, NY, 1986.

[Si2] J.H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, NY, 1994.

[Ta] J. Tate, *Endomorphisms of abelian varieties over finite fields*, Inventiones math., **2**, 134-144, 1966.

[W] A. Weil, *Foundations of Algebraic Geometry*, Am.Math.Soc., 1975.