Zur darstellungstheoretischen Beschreibung von elliptischen Kurven über lokalen Körpern der Charakteristik 2

Dissertation [1]
zur Erlangung des Grades
des Doktors der Naturwissenschaften
der Naturwissenschaftlich-Technischen Fakultät I
der Universität des Saarlandes

von
Jochen Frieden

Saarbrücken
2004

[1] Dies ist die Orginalversion, bei der einige Druckfehler bereits korrigiert wurden. Beim Auffinden weiterer Druckfehler bitte ich um Mitteilung über meine Emailadresse betyj@mexico.com unter dem Subject „Dissertation-Druckfehler“.

Tag des Kolloquiums:	13.07.2004
Dekan:	Prof. Dr. Jörg Eschmeier

Mitglieder des Prüfungsausschusses

Vorsitzender:	Prof. Dr. Joachim Weickert
Berichterstatter:	Prof. Dr. Ernst-Ulrich Gekeler
	Prof. Dr. Rainer Schulze-Pillot-Ziemen
Schriftführer:	Dr. Anselm Lambert

Inhaltsverzeichnis

Zusammenfassung

Ein wesentliches Problemfeld der heutigen algebraischen Zahlentheorie ist der Beweis und die Beschreibung der „Langlandskorrespondenz“. Diese postuliert einen allgemeinen Zusammenhang zwischen der Galoistheorie arithmetisch relevanter Körper (d. h. globale oder lokale Zahl- oder Funktionenkörper) und der Darstellungstheorie reduktiver algebraischer Gruppen über solchen Körpern (die „automorphe Seite“ der Korrespondenz).

Soweit diese Korrespondenz die Gruppen GL_n betrifft, sind die entsprechenden Vermutungen bewiesen für

- $n = 1$, wobei die Korrespondenz hier in expliziter Weise durch die Hauptsätze der abelschen Klassenkörpertheorie gegeben ist, die in den dreißiger bis fünfziger Jahren des letzten Jahrhunderts bewiesen wurden;
- $n \geq 2$ im lokalen Fall und im globalen Fall positiver Charakteristik (Laurent Lafforgue, Fields Medal 2002);

sowie in einigen weiteren Spezialfällen.

Leider ist diese Korrespondenz (soweit überhaupt) nur als Existenzaussage etabliert; ihre Auswirkung auf konkrete „Motive“ kann i. a. nicht explizit beschrieben werden. Dies gilt schon für die „einfache“ Situation eines lokalen Funktionenkörpers K mit $n = 2$, falls K die Charakteristik 2 hat. Hier liegen bisher weder über die „Galoisseite“ noch über die automorphe Seite hinreichend genaue Aussagen vor, um den Zusammenhang zu verstehen.

Das Anliegen dieser Arbeit ist das Studium solcher Darstellungen auf der Galoisseite, die sich von elliptischen Kurven $\mathcal{E}$ über K herleiten. In diesem Fall ist K ein Laurentreihenkörper über dem endlichen Körper mit 2^f Elementen. Diejenigen elliptischen Kurven über K, deren j-Invariante ungleich null ist, sind alle durch eine Weierstraßgleichung der Form

$$Y^2 + XY = X^3 + \alpha X^2 + \beta$$

mit $\alpha \in K$ und $\beta \in K^*$ gegeben. Zu jeder dieser elliptischen Kurven liefert der Tate-Modul eine zweidimensionale Darstellung $(\pi^K_{\alpha,\beta})'$ der Weil-Deligne-Gruppe $W'(K^{\mathrm{sep}}/K)$. Wenn β im Ganzheitsring von K liegt, läßt sich die Darstellung $\pi'_{\alpha,\beta}$ mit Hilfe der Tate-Theorie vollständig und zufriedenstellend beschreiben.

In der vorliegenden Arbeit betrachten wir den Fall, daß β nicht im Ganzheitsring von K liegt. In diesem Fall können wir $(\pi^K_{\alpha,\beta})'$ als Darstellung $\pi^K_{\alpha,\beta}$ der Weilgruppe $W(K^{\mathrm{sep}}/K)$, einer dichten Untergruppe der absoluten Galoisgruppe von K, auffassen. Wir bestimmen alle Fälle, in denen $\pi^K_{\alpha,\beta}$ irreduzibel ist, und geben jeweils eine Brauerzerlegung (Zerlegung in eine $\mathbb{Z}$-Linearkombination von Darstellungen, die von eindimensionalen Darstellungen induziert werden) an. Diese Charakterisierung von $\pi^K_{\alpha,\beta}$ ermöglicht es uns, die ϵ-Faktoren von allen Twists (Tensorierung mit eindimensionalen Darstellungen) von $\pi^K_{\alpha,\beta}$ zu bestimmen. Hierzu bemerken wir, daß die Kenntnis der ϵ-Faktoren aller Twists einer zweidimensionalen Darstellung von $W(K^{\mathrm{sep}}/K)$ diese zumindest in abstrakter Weise vollständig charakterisiert. Außerdem beschreiben wir vollständig das Verzweigungsverhalten von $\pi^K_{\alpha,\beta}$. Als Nebenprodukt erhalten wir ein Verfahren, mit dem wir den Führer von $\pi^K_{\alpha,\beta}$ explizit in Abhängigkeit von α und β berechnen können, ohne auf den Tate-Algorithmus zurückzugreifen. Der Tate-Algorithmus entspringt einer geometrischen Betrachtungsweise, während unser

Vorgehen rein darstellungstheoretischer Natur ist. Darüber hinaus bestimmen wir auch den minimalen Führer aller Twists von $\pi^K_{\alpha,\beta}$, (eine wichtige Invariante von $\pi^K_{\alpha,\beta}$) explizit in Abhängigkeit von β.

Abstract

One of the most important problems in recent algebraic number theory is to prove and describe the Langlands correspondence. This correspondence predicts a connection between the Galois theory of fields of arithmetic interest (global or local number or function fields) and the representation theory of reductive groups over such fields (the so-called automorphic side).

Concerning GL_n, the Langlands correspondence is proven in the cases

- $n = 1$, in this case the correspondence is given by local and global class field theory, established mainly between 1930 and 1950;
- $n \geq 2$, if the field is local or global of positive characteristic (Laurent Lafforgue, Fields Medal 2002)

and in some further special cases.

Unfortunately only the existence of these correspondences is well established. Their effect on concrete "motives" is unknown. Even in the situation where $n = 2$ and K is a local field, no explicit characterization is known, if K happens to have characteristic 2. Neither on the Galois nor on the automorphic side there are results which allow a satisfactory description of the correspondence.

The aim of the present thesis is to analyze those representations on the Galois side which occur in connection with elliptic curves. In this case the field K is the field of formal Laurent series over a finite field of 2^f elements. The elliptic curves with non-vanishing j-invariant are all given by a Weierstraß equation of the form

$$Y^2 + XY = X^3 + \alpha X^2 + \beta,$$

where $\alpha \in K$ and $\beta \in K^*$. To every elliptic curve of this form there is associated a two dimensional representation $(\pi^K_{\alpha,\beta})'$ of the Weil-Deligne group $W'(K^{\mathrm{sep}}/K)$. For β integral, Tate's uniformization theory yields a complete and satisfactory characterization of $(\pi^K_{\alpha,\beta})'$.

In this thesis we deal with the case where β ist not integral. Then we can consider $(\pi^K_{\alpha,\beta})'$ as a representation $\pi^K_{\alpha,\beta}$ of the Weil group, which is a dense subgroup of the absolute Galois group of K. We give necessary and sufficient conditions for the irreducibility of $\pi^K_{\alpha,\beta}$. In all cases where $\pi^K_{\alpha,\beta}$ is irreducible, we determine a Brauer decomposition, which means that $\pi^K_{\alpha,\beta}$ can be expressed as a $\mathbb{Z}$-linear combination of representations induced from one dimensional representations. That description of $\pi^K_{\alpha,\beta}$ enables us to calculate the ϵ-factors of all twists of $\pi^K_{\alpha,\beta}$ by one dimensional representations. We point out that knowledge of these ϵ-factors abstractly (but not explicitly) characterizes $\pi^K_{\alpha,\beta}$. We further determine the ramification properties of $\pi^K_{\alpha,\beta}$, including an explicit calculation of its conductor. Our calculation does not make use of the Tate algorithm; while Tate's algorithm is developed from a geometric point of view, we are working with purely representation theoretic methods. As a further important result we calculate explicitly and directly from β the minimal conductor of all twists of $\pi^K_{\alpha,\beta}$.

Einleitung

Ein wichtiges Problem der algebraischen Zahlentheorie ist die Beschreibung der absoluten Galoisgruppe von lokalen Körpern. Ein lokaler Körper K ist entweder isomorph zum Laurentreihenkörper $\mathbb{F}_q((T))$ über einem endlichen Körper mit q Elementen in einer Unbestimmten oder zu einer endlichen Erweiterung von $\mathbb{Q}_p$, der Vervollständigung von $\mathbb{Q}$ bzgl. des p-adischen Absolutbetrages. Diese Körper sind deshalb von Bedeutung, weil man ihre Galoistheorie als Annäherung an die Galoistheorie der globalen Körper auffassen kann. Unter einem globalen Körper verstehen wir entweder einen Funktionenkörper $\mathbb{F}_q(T)$ oder eine endliche Erweiterung von $\mathbb{Q}$.

Ein lokaler Körper K ist stets mit einer diskreten Bewertung $\nu_K : K^* \longrightarrow \mathbb{Z}$ versehen. Hierunter verstehen wir eine surjektive multiplikative Abbildung, die der strengen Dreiecksungleichung $\nu_K(x+y) \geq \min\{\nu_K(x), \nu_K(y)\}$ genügt. Die Elemente x von K mit $\nu_K(x) \geq 0$ bilden den sogenannten Ganzheitsring $\mathcal{O}_K$. Dieser Ganzheitsring besitzt ein eindeutig bestimmtes maximales Ideal $\mathfrak{p}_K$, das aus allen Elementen von K besteht, deren Bewertung echt größer als 0 ist. Alle weiteren Ideale sind von der Form $\mathfrak{p}_K^n$. Der Restklassenkörper $\mathcal{O}_K/\mathfrak{p}_K$ ist isomorph zu einem endlichen Körper $\mathbb{F}_q$. Der separable Abschluß K^{sep} weist eine ähnliche Struktur auf wie K selbst. Die Bewertung ν_K läßt sich zu einer multiplikativen Abbildung $(K^{\text{sep}})^* \longrightarrow \mathbb{Q}$ fortsetzen, die ebenfalls der strengen Dreiecksungleichung genügt. Auch K^{sep} besitzt einen Ganzheitsring $\mathcal{O}_{K^{\text{sep}}}$, der wiederum genau ein maximales Ideal $\mathfrak{p}_{K^{\text{sep}}}$ besitzt. Hierbei ist der Restklassenkörper von K^{sep} isomorph zum algebraischen Abschluß des Restklassenkörpers von K.

Eine erste Aussage über die Struktur der Galoisgruppe $G(K^{\text{sep}}/K)$ erhält man aus dem Studium ihrer Operation auf K^{sep}. Weil sowohl $\mathcal{O}_{K^{\text{sep}}}$ als auch $\mathfrak{p}_{K^{\text{sep}}}$ invariant bleiben, operiert $G(K^{\text{sep}}/K)$ auf dem Restklassenkörper $\mathbb{F}_q^{\text{alg}}$. Man erhält somit einen surjektiven Homomorphismus $G(K^{\text{sep}}/K) \longrightarrow G(\mathbb{F}_q^{\text{sep}}/\mathbb{F}_q)$. Seinen Kern bezeichnen wir mit $G_0(K^{\text{sep}}/K)$ und nennen ihn die Trägheitsgruppe von K. Wir erinnern daran, daß die Frobeniusabbildung $x \longmapsto x^q$ eine Untergruppe in $G(\mathbb{F}_q^{\text{sep}}/\mathbb{F}_q)$ erzeugt, die isomorph zur additiven Gruppe $\mathbb{Z}$ ist. Das Urbild dieser Untergruppe nennen wir die Weilgruppe $W(K^{\text{sep}}/K)$ von K. Wenn wir $G(K^{\text{sep}}/K)$ mit der Krulltopologie versehen, liegt $W(K^{\text{sep}}/K)$ dicht in $G(K^{\text{sep}}/K)$. Das bedeutet, daß $W(K^{\text{sep}}/K)$ annähernd die gleiche Information enthält wie $G(K^{\text{sep}}/K)$.

Die Struktur der Galoisgruppe $G(K^{\text{sep}}/K)$ können wir beschreiben, indem wir ihre Darstellungen klassifizieren. Genauer gesagt betrachtet man die endlichdimensionalen stetigen Darstellungen über $\mathbb{C}$. Diese stehen in enger Beziehung zu den Darstellungen von $W(K^{\text{sep}}/K)$. Alle Darstellungen von $G(K^{\text{sep}}/K)$ lassen sich auch als Darstellungen von $W(K^{\text{sep}}/K)$ auffassen. Umgekehrt können alle Darstellungen von $W(K^{\text{sep}}/K)$ nach leichter Abänderung auch als Darstellungen von $G(K^{\text{sep}}/K)$ angesehen werden. Somit gehen also keine wesentlichen Informationen verloren. Die lokale Klassenkörpertheorie liefert nun einen Isomorphismus $W(K^{\text{sep}}/K)^{ab} \longrightarrow K^*$, die sogenannte Artinabbildung. Hierbei bezeichnen wir mit $W(K^{\text{sep}}/K)^{ab}$ den maximalen abelschen Quotienten von $W(K^{\text{sep}}/K)$. Auf diese Weise entsprechen sich die eindimensionalen Darstellungen von $W(K^{\text{sep}}/K)$ und K^* eineindeutig.

Diese Korrespondenz wird durch die Langlandskorrespondenz verallgemeinert, nach der die n-dimensionalen Darstellungen von $W(K^{\text{sep}}/K)$ in Bijektion zu den irreduziblen zulässigen supercuspidalen Darstellungen von $Gl_n(K)$ stehen. Auf die Definition von zulässigen und supercuspidalen Darstellungen von $Gl_n(K)$ können wir an dieser Stelle nicht näher eingehen. Wir verraten nur

soviel, daß es sich hierbei um komplexe Darstellungen von $Gl_n(K)$ handelt, die i. a. unendlichdimensional sind und einer bestimmten topologischen Bedingung genügen. Für die Einzelheiten verweisen wir auf [8]. Um eine Korrespondenz mit allen zulässigen Darstellungen von $GL_n(K)$ zu bekommen, müssen wir $W(K^{\text{sep}}/K)$ durch die Weil-Deligne-Gruppe $W'(K^{\text{sep}}/K)$ ersetzen.

Die Weil-Deligne-Gruppe $W'(K^{\text{sep}}/K)$ können wir als ein semidirektes Produkt der Form $W(K^{\text{sep}}/K) \ltimes \mathbb{C}$ auffassen. Die n-dimensionalen Darstellungen von $W'(K^{\text{sep}}/K)$ fassen wir als Paare $\pi' = (\pi, N)$, bestehend aus einer nilpotenten n-reihigen quadratischen Matrix N über $\mathbb{C}$ und einer n-dimensionalen Darstellung π von $W(K^{\text{sep}}/K)$, auf. Für die technischen Details verweisen wir auf den Abschnitt 1.7. Wenn $N = 0$ ist, können wir (π, N) als Darstellung von $W(K^{\text{sep}}/K)$ ansehen. Auf diese Weise bilden die Darstellungen der Weilgruppe eine Teilmenge aller Darstellungen der Weil-Deligne-Gruppe. Die Langlandskorrespondenz setzt nun die n-dimensionalen Darstellungen von $W'(K^{\text{sep}}/K)$ („Galoisseite“) mit den irreduziblen zulässigen Darstellungen von $GL_n(K)$ („automorphe Seite“) auf natürliche Weise in Bijektion, wobei die n-dimensionalen Darstellungen auf die irreduziblen supercuspidalen Darstellungen von $GL_n(K)$ abgebildet werden. Hierzu ist zu bemerken, daß diese Langlandskorrespondenz im allgemeinen nicht in expliziter Weise vorliegt. Man weiß aber, daß gewisse Strukturmerkmale erhalten bleiben. Sowohl auf der Galoisseite als auch auf der automorphen Seite sind L- und ϵ-Faktoren von Darstellungen definiert. Auf die L- und ϵ-Faktoren von Darstellungen von $W'(K^{\text{sep}}/K)$ werden wir in Kapitel 1 eingehen. Für die Definition von L- und ϵ-Faktoren auf der automorphen Seite verweisen wir auf [8]. Diese L- und ϵ-Faktoren bleiben unter Langlandskorrespondenz erhalten. Wenn man also von einer gegebenen Darstellung von $W'(K^{\text{sep}}/K)$ die L- und ϵ-Faktoren kennt, liefert einem dies eine gewisse Information über die zugehörige Darstellung auf der automorphen Seite.

Für $n = 2$ ist die Langlandskorrespondenz noch weitgehend unverstanden, wenn K die Restcharakteristik 2 hat. Hierbei ist es interessant zu untersuchen, wie sich „natürlich vorkommende“ irreduzible zweidimensionale Darstellungen von $W'(K^{\text{sep}}/K)$ unter Langlandskorrespondenz verhalten. Solche Darstellungen treten z. B. im Zusammenhang mit elliptischen Kurven auf. Dazu fixieren wir eine elliptische Kurve $\mathcal{E}$ über K. Auf der Menge $\mathcal{E}(K^{\text{sep}})$ der K^{sep}-rationalen Punkte von $\mathcal{E}$ ist eine Operation erklärt, die mit der Operation von $G(K^{\text{sep}}/K)$ vertauscht und $\mathcal{E}(K^{\text{sep}})$ zu einer additiven Gruppe macht. Wir wählen eine Primzahl l, die verschieden ist von der Charakteristik des Restklassenkörpers, und betrachten die l^n-Torsionspunkte von $\mathcal{E}$. Diese bilden ein projektives System, dessen Limes einen $\mathbb{Z}_l$-Modul, den sogenannten Tate-Modul liefert. Durch Tensorieren mit $\mathbb{Q}_l$ erhalten wir einen $\mathbb{Q}_l$-Vektorraum und durch die Operation von $G(K^{\text{sep}}/K)$ eine zweidimensionale Darstellung von $G(K^{\text{sep}}/K)$ über $\mathbb{Q}_l$. Es gibt nun einen Mechanismus, der jeder Darstellung von $G(K^{\text{sep}}/K)$ über $\mathbb{Q}_l$ eine komplexe Darstellung von $W'(K^{\text{sep}}/K)$ zuordnet. Diesen werden wir im Abschnitt 1.9 noch genauer beschreiben. Somit können wir also jeder elliptischen Kurve $\mathcal{E}$ eine Darstellung $(\pi_{\mathcal{E}})'$ von $W'(K^{\text{sep}}/K)$ zuordnen.

Für elliptische Kurven existiert eine Einteilung in sogenannte Reduktionstypen. Jede elliptische Kurve $\mathcal{E}$ über K besitzt eine Weierstraßgleichung der Form

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

mit Koeffizienten a_1, a_2, a_3, a_4, a_6 aus dem Ganzheitsring $\mathcal{O}_K$. Indem wir nun die Koeffizienten als Elemente des Restklassenkörpers auffassen, erhalten wir eine reduzierte Kurve $\bar{\mathcal{E}}$. Um die Eindeutigkeit von $\bar{\mathcal{E}}$ zu gewährleisten, muß man noch fordern, daß die Bewertung der Diskriminante von $\mathcal{E}$ minimal ist. Die Diskriminante von $\mathcal{E}$ ist ein Element von K, das durch Einsetzen der Koeffizienten a_1, a_2, a_3, a_4, a_6 in ein bestimmtes Polynom ermittelt wird. Je nach Singularitätsverhalten von $\bar{\mathcal{E}}$ unterscheidet man zwischen guter, multiplikativer und additiver Reduktion, wobei wir hier nicht weiter auf die Einzelheiten eingehen wollen. Wichtig ist, daß gute und multiplikative Reduktion stabil unter endlicher Erweiterung des Grundkörpers K bleiben. Umgekehrt gibt es bei additiver Reduktion eine endliche Erweiterung M von K, so daß $\mathcal{E}$ als Kurve über M entweder multiplikative oder gute Reduktion hat. Man spricht dann von potentiell multiplikativer oder potentiell guter Reduktion. Diese beiden Reduktionstypen haben weitreichende Konsequenzen für die zugehörige Darstellung $(\pi_{\mathcal{E}})'$ von $W'(K^{\text{sep}}/K)$.

Wenn $\mathcal{E}$ potentiell multiplikative Reduktion hat, steht uns die sogenannte Tate-Theorie zur Verfügung, mit deren Hilfe wir den Tate-Modul und damit die Darstellung $(\pi_{\mathcal{E}})'$ vollständig beschreiben können. Um das Ergebnis zu formulieren, bezeichnen wir mit ω_K den Charakter von $W(K/K^{\text{sep}})$, der unter der Artinabbildung dem Betragscharakter $|x| := q^{-\nu_K(x)}$ entspricht. Weiter sei die Darstellung $\rho : W(K^{\text{sep}}/K) \longrightarrow GL(2,\mathbb{C})$ durch die Vorschrift

$$\sigma \longmapsto \begin{pmatrix} \omega_K(\sigma) & 0 \\ 0 & 1 \end{pmatrix}$$

gegeben. Das Ergebnis sieht so aus, daß es eine Erweiterung M von K gibt, die höchstens den Grad 2 hat, so daß $(\pi_{\mathcal{E}})'$ isomorph zur Darstellung $(\chi_M \otimes \rho, N)$ ist. Hierbei ist

$$N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

und χ_M der eindeutig bestimmte Charakter von $W(K^{\text{sep}}/K)$, dessen Kern $W(K^{\text{sep}}/M)$ ist. Es ist bekannt, daß $(\pi_{\mathcal{E}})'$ unter der Langlandskorrespondenz auf die Darstellung $(\chi_M \circ \det) \otimes \text{sp}(2)$ abgebildet wird. Das Symbol sp(2) steht für die spezielle Darstellung von $GL_2(K)$, die in zufriedenstellender Weise charakterisiert ist und die wir hier nicht näher beschreiben wollen. Mit $(\chi_M \circ \det)$ bezeichnen wir die Verkettung des Charakters χ_M, den wir mittels Artinabbildung als Charakter von K^* auffassen, mit der Determinantenabbildung $GL_2(K) \longrightarrow K^*$. Zusammenfassend können wir also sagen, daß vollständig bekannt ist, wie sich $(\pi_{\mathcal{E}})'$ im Fall potentiell multiplikativer Reduktion unter der Langlandskorrespondenz verhält.

Wenn $\mathcal{E}$ potentiell gute Reduktion hat, ist sehr viel weniger bekannt. Man weiß, daß $(\pi_{\mathcal{E}})'$ von der Form $(\pi_{\mathcal{E}}, 0)$ ist und somit als Darstellung von $W(K^{\text{sep}}/K)$ angesehen werden kann. Es kann sowohl der Fall auftreten, daß $\pi_{\mathcal{E}}$ in zwei Charaktere zerfällt, als auch der Fall, daß $\pi_{\mathcal{E}}$ irreduzibel ist. Hier interessieren wir uns hauptsächlich für den Fall, daß $\pi_{\mathcal{E}}$ irreduzibel ist. Wenn man $\pi_{\mathcal{E}}$ charakterisieren will, geht es zunächst darum, die „Komplexität“ zu kontrollieren. Diese läßt sich mittels einer natürlichen Zahl, dem sogenannten Führer $\text{cond}(\pi_{\mathcal{E}})$ von $\pi_{\mathcal{E}}$ messen. Hierzu muß man wissen, daß die Trägheitsgruppe $G_0(K^{\text{sep}}/K)$ durch eine absteigende Folge von Normalteilern $G_i(K^{\text{sep}}/K)$ für alle natürlichen Zahlen i filtriert ist. Diese Normalteiler nennen wir die höheren Verzweigungsgruppen. Aus der Stetigkeitsbedingung für $\pi_{\mathcal{E}}$ folgt, daß es ein $i \in \mathbb{N}$ gibt, so daß $\pi_{\mathcal{E}}$ auf $G_i(K^{\text{sep}}/K)$ trivial wird. Außerdem muß das Bild der Einschränkung von $\pi_{\mathcal{E}}$ auf $G_0(K^{\text{sep}}/K)$ endlich sein. Der Führer sammelt nun Informationen darüber, wie groß das kleinste solche i ist und wie komplex die Operation der Verzweigungsgruppen $G_k(K^{\text{sep}}/K)$ für $k < i$ auf dem Darstellungsraum ist. Je kleiner der Führer einer Darstellung von $W(K^{\text{sep}}/K)$ ist, desto leichter ist ihre Struktur zu beschreiben. Im Fall, daß die Charakteristik des Restklassenkörpers größer als 3 ist, kann nur der Fall $\text{cond}(\pi_{\mathcal{E}}) \leq 2$ auftreten, was bedeutet, daß $\pi_{\mathcal{E}}$ von einfacher Struktur ist. Wenn die Restcharakteristik dagegen 2 oder 3 ist, kann der Führer von $\pi_{\mathcal{E}}$ beliebig groß werden. Am interessantesten ist hierbei der Fall, daß der Restklassenkörper die Charakteristik 2 hat, weil hier die Theorie der zweidimensionalen Darstellungen von $W(K^{\text{sep}}/K)$ erheblich komplizierter ist.

In dieser Arbeit betrachten wir den Fall, daß $K = \mathbb{F}_{2^f}((T))$ ein Laurentreihenkörper über dem endlichen Körper mit 2^f Elementen ist. Die elliptischen Kurven, die wir betrachten, sollen nicht supersingulär sein, d. h. von der Form

$$\mathcal{E}_{\alpha,\beta} : Y^2 + XY = X^3 + \alpha X^2 + \beta$$

mit $\alpha, \beta \in K$ und $\beta \neq 0$. Die zugehörige Darstellung der Weil-Deligne-Gruppe bezeichnen wir mit $(\pi^K_{\alpha,\beta})'$. Wenn die Bewertung von β echt größer als 0 ist, hat $\mathcal{E}_{\alpha,\beta}$ potentiell multiplikative Reduktion. In diesem Fall ist $(\pi^K_{\alpha,\beta})'$ durch das vorher Gesagte schon bestimmt. Interessant ist der Fall, daß die Bewertung von β kleiner oder gleich 0 ist. In diesem Fall besitzt $\mathcal{E}$ potentiell gute Reduktion und es gilt $(\pi^K_{\alpha,\beta})' \cong (\pi^K_{\alpha,\beta}, 0)$, wobei die Darstellung $\pi^K_{\alpha,\beta}$ von $W(K^{\text{sep}}/K)$ noch zu bestimmen ist.

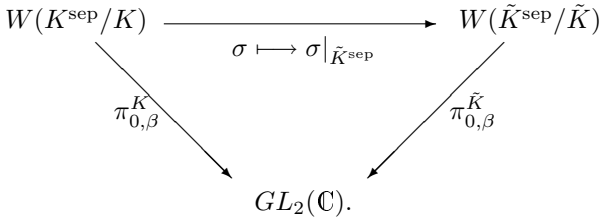
Wünschenswert wäre es, in allen Fällen, in denen $\pi^K_{\alpha,\beta}$ irreduzibel ist, explizit in Abhängigkeit von α und β die zu $\pi^K_{\alpha,\beta}$ korrespondierende Darstellung $\Pi_{\alpha,\beta}$ auf der automorphen Seite anzugeben.

In abstrakter Weise kann man $\Pi_{\alpha,\beta}$ charakterisieren, indem man für alle Twists von $\pi^K_{\alpha,\beta}$ die ϵ-Faktoren berechnet. Unter einem Twist von $\pi^K_{\alpha,\beta}$ verstehen wir die Tensorierung mit einem Charakter von $W(K^{\mathrm{sep}}/K)$. Beim Versuch einer expliziten Charakterisierung von $\Pi_{\alpha,\beta}$ ist es sinnvoll, zuerst einen Charakter χ von $W(K^{\mathrm{sep}}/K)$ zu suchen, so daß der Führer von $\chi \otimes \pi^K_{\alpha,\beta}$ minimal wird, und dann die Darstellung, die zu $\chi \otimes \pi^K_{\alpha,\beta}$ korrespondiert. Aus dieser kann man dann $\Pi_{\alpha,\beta}$ durch Twist auf der automorphen Seite konstruieren. Während es ein schwieriges Problem ist, einen solchen Charakter χ zu finden, stehen für die Berechnung von $\mathrm{cond}(\chi \otimes \pi^K_{\alpha,\beta})$ explizite Formeln zur Verfügung, wenn man die Darstellung $\pi^K_{\alpha,\beta}$ gut genug kennt.

Das erste Kapitel ist als Einleitung gedacht. In ihm stellen wir die wichtigsten Aussagen der Darstellungstheorie der Weilgruppe bzw. der Weil-Deligne-Gruppe von K zusammen. Ein besonderes Augenmerk legen wir dabei auf die irreduziblen zweidimensionalen Darstellungen von $W(K^{\mathrm{sep}}/K)$. Außerdem geben wir eine kurze Einführung in die Theorie der elliptischen Kurven über K. Insbesondere beschreiben wir die Konstruktion von $(\pi^K_{\alpha,\beta})'$.

Im zweiten Kapitel bestimmen wir den Körper L, der aus K durch Adjunktion der Koordinaten der 3-Torsionspunkte $\mathcal{E}_{\alpha,\beta}[3]$ entsteht, und liefern eine exakte Beschreibung der zugehörigen Operation von $G(L/K)$ auf $\mathcal{E}_{\alpha,\beta}[3]$. Weiter betrachten wir ausgewählte Zwischenkörper von L/K und nehmen anhand der Körpergrade dieser Zwischenerweiterungen eine Einteilung aller Fälle vor, in denen $G(L/K)$ nichtabelsch ist.

Im dritten Kapitel befassen wir uns zunächst mit der Darstellung $\pi^L_{\alpha,\beta}$, die zu dem Tate-Modul von $\mathcal{E}$ als elliptische Kurve über L gehört. A priori ist bekannt, daß $\mathcal{E}$ über L gute Reduktion hat. Wir geben explizit eine Transformation an, die zu einer minimalen Weierstraßgleichung führt (Beweis von 3.1.1). Hieraus ergibt sich die reduzierte Kurve, die stets die selbe ist und nicht von β abhängt. Mit Hilfe der Theorie der elliptischen Kurven über endlichen Körpern bestimmen wir $\pi^L_{\alpha,\beta}$ vollständig. Weiter definieren wir $\tilde{K} := \mathbb{F}_2((\beta^{-1}))$, d.h. den kleinsten lokalen Teilkörper von K, der β enthält. Im Fall $\alpha = 0$ können wir $\mathcal{E}$ auch als Kurve über $\tilde{K}$ auffassen. Wenn wir die jeweiligen Tate-Moduln identifizieren, erhalten wir das kommutative Diagramm



Im weiteren Verlauf des vierten Kapitels bestimmen wir $\pi^K_{0,\beta}$ im Fall $K = \mathbb{F}_2((T))$ und $\beta = T^{-1}$, womit wir eine vollständige Charakterisierung von $\pi^K_{0,\beta}$ erhalten (3.3.3). Im allgemeinen Fall $\alpha \neq 0$ unterscheiden sich $\pi^K_{\alpha,\beta}$ und $\pi^K_{0,\beta}$ nur um einen quadratischen Charakter, so daß wir auch eine vollständige Charakterisierung von $\pi^K_{\alpha,\beta}$ bekommen. Diese Beschreibung von $\pi^K_{\alpha,\beta}$ ist ähnlich zufriedenstellend wie im Fall potentiell multiplikativer Reduktion und stellt eines der Hauptergebnisse dieser Arbeit dar. Hieraus ergibt sich unter anderem die Aussage, daß $\pi^K_{\alpha,\beta}$ genau dann irreduzibel ist, wenn $G(L/K)$ nichtabelsch ist.

Im vierten Kapitel benutzen wir die Ergebnisse aus Kapitel 3, um das Verzweigungsverhalten von $\pi^K_{\alpha,\beta}$ durch die Differenten von bestimmten Zwischenerweiterungen von L/K zu beschreiben. Auf diese Weise erhalten wir auch eine Formel für den Führer von $\pi^K_{\alpha,\beta}$ (4.2.5). Im weiteren Verlauf entwickeln wir dann Methoden, mit denen wir diese Differenten explizit in Abhängigkeit von α und β durch Rechnungen im Grundkörper K bestimmen. Als Nebenprodukt erhalten wir ein Verfahren, mit dem wir den Führer von $\pi^K_{\alpha,\beta}$ berechnen können, ohne den Tate-Algorithmus zu verwenden.

In den Kapiteln 5 bis 10 behandeln wir die sechs Fälle, in denen $G(L/K)$ nichtabelsch ist, getrennt. In den Fällen, die in den Kapiteln 5-8 behandelt werden, gelingt es uns, eine quadratische

Erweiterung M/K und einen Charakter χ_M von $W(K^{\text{sep}}/K)$ zu bestimmen, der die Darstellung $\pi_{\alpha,\beta}$ induziert (vgl. 5.2.4, 6.2.3, 7.2.3 und 8.2.4). In diesen Fällen läßt sich die zu $\pi^K_{\alpha,\beta}$ gehörige Darstellung von $GL_2(K)$ explizit konstruieren. Dazu verweisen wir auf [9, Ch. 4].

Bei den Fällen, die wir in den Kapiteln 9 und 10 behandeln, gibt es keinen Charakter einer Untergruppe von $W(K^{\text{sep}}/K)$ vom Index 2, der $\pi^K_{\alpha,\beta}$ induziert. Hier gelingt es uns, eine Brauerzerlegung anzugeben (vgl. 9.2.5 und 10.1.5). Das bedeutet, daß wir $\pi^K_{\alpha,\beta}$ als $\mathbb{Z}$-Linearkombination von Darstellungen auffassen, die von eindimensionalen Darstellungen geeigneter Untergruppen von $W(K^{\text{sep}}/K)$ induziert werden.

In jedem der sechs Fälle, die wir in den Kapiteln 5 bis 10 behandeln, gelingt es uns, von allen Twists zumindest prinzipiell die ϵ-Faktoren zu berechnen (vgl. 5.4.2, 6.4.1, 7.4.5, 8.4.1, 9.4.2 und 10.3.2). Hierdurch erzielen wir eine abstrakte vollständige Charakterisierung sowohl von $\pi^K_{\alpha,\beta}$ als auch von $\Pi_{\alpha,\beta}$. In den Abschnitten 5.3, 6.3, 7.3, 8.3, 9.3 und 10.2 bestimmen wir jeweils den minimalen Führer unter allen Twists. Leider sind wir aber nicht in der Lage, allgemein einen Twist zu bestimmen, der den minimalen Führer realisiert. Wir verweisen aber darauf, daß die Bestimmung eines minimalen Twists ein endliches Problem ist, dessen Komplexität von der Größe des Führers abhängt. Deshalb erscheint uns zur weiteren Behandlung des Problems der folgende Ansatz vielversprechend: Man betrachte die Fälle, in denen $\pi^K_{\alpha,\beta}$ einen kleinen Führer hat. (Dies ist dann der Fall, wenn die Bewertung von β nicht zu klein ist.) Weiter bestimme man einen minimalen Twist von $\pi^K_{\alpha,\beta}$ und versuche so, die korrespondierende Darstellung $\Pi_{\alpha,\beta}$ von $GL_2(\mathbb{C})$ anhand ihrer ϵ-Faktoren zu identifizieren. Die explizite Berechnung von ϵ-Faktoren ist ebenfalls leicht, wenn der Führer klein ist. Außerdem stellt sich die Frage, was das oben abgebildete Diagramm (ein entscheidendes Strukturmerkmal der Darstellungen von $W(K^{\text{sep}}/K)$, die von elliptischen Kurven kommen) für die zu $\pi^K_{\alpha,\beta}$ korrespondierende Darstellung $\Pi_{\alpha,\beta}$ auf der automorphen Seite bedeutet. Auf diese Weise könnte man durch maschinelle Berechnung von konkreten Fällen zumindest zu einer Vermutung gelangen, wie sich $\Pi_{\alpha,\beta}$ in expliziter Weise charakterisieren läßt.

An dieser Stelle möchte ich mich bei allen Leuten bedanken, die mich beim Anfertigen dieser Arbeit unterstützt haben. An erster Stelle ist mein Doktorvater Herr Prof. Dr. E.-U. Gekeler zu nennen, dem ich das Thema zu verdanken habe und der mir in allen Phasen mit viel Geduld und Engagement zur Seite gestanden hat. Dies gilt ganz besonders für die langwierige und aufreibende Einarbeitungsphase. Allen Mitgliedern der Arbeitsgruppe danke ich für die hervorragende Zusammenarbeit und diverse Hilfen. Außerdem bedanke ich mich bei meinen Eltern und meiner lieben Frau Beatriz für den notwendigen Rückhalt.

Kapitel 1

Elliptische Kurven und Weildarstellungen

1.1 Die Weilgruppe und ihre Darstellungen

Sei $\mathbb{F}_q$ der endliche Körper der Charakteristik p mit $q = p^f$ Elementen und $\mathbb{F}_q^{\text{alg}}$ der algebraische Abschluß von $\mathbb{F}_q$. Unter der Weilgruppe $W(\mathbb{F}_q^{\text{alg}}/\mathbb{F}_q)$ von $\mathbb{F}_q$ verstehen wir die vom Frobeniusautomorphismus $x \longmapsto x^q$ erzeugte Untergruppe der absoluten Galoisgruppe $G(\mathbb{F}_q^{\text{alg}}/\mathbb{F}_q)$.

Wir betrachten nun einen nichtarchimedischen lokalen Körper K mit Restklassenkörper $\mathbb{F}_q$ und separablem Abschluß K^{sep}. Wir wählen eine Uniformisierende T und bezeichnen mit $\mathcal{O}_K$ den Bewertungsring sowie mit $\mathfrak{p}_K$ das maximale Ideal des Bewertungsrings von K. Weiter schreiben wir U_K^n für die Einseinheitengruppen $1 + \mathfrak{p}_K^n$. Ein Element von $G(K^{\text{sep}}/K)$, das unter dem Restklassenhomomorphismus $G(K^{\text{sep}}/K) \longrightarrow G(\mathbb{F}_q^{\text{alg}}/\mathbb{F}_q)$ auf den Frobeniusautomorphismus von $G(\mathbb{F}_q^{\text{alg}}/\mathbb{F}_q)$ abgebildet wird, nennen wir Frobeniuselement. Wir wählen ein festes Frobeniuselement Φ_K und definieren die Weilgruppe $W(K^{\text{sep}}/K)$ als die von der Trägheitsgruppe $G_0(K^{\text{sep}}/K)$ und von Φ_K erzeugte Untergruppe von $G(K^{\text{sep}}/K)$. Diese Definition ist unabhängig von der Wahl von Φ_K. Die Krulltopologie auf $G(K^{\text{sep}}/K)$ induziert eine Topologie auf $G_0(K^{\text{sep}}/K)$. Indem wir die Menge aller offenen Untergruppen von $G_0(K^{\text{sep}}/K)$ zu einem Fundamentalsystem offener Umgebungen des neutralen Elements erklären, machen wir $W(K^{\text{sep}}/K)$ zu einer topologischen Gruppe.

Unter einer Darstellung von $W(K^{\text{sep}}/K)$ verstehen wir einen stetigen Gruppenhomomorphismus $\pi : W(K^{\text{sep}}/K) \longrightarrow GL(V)$, wobei V ein endlichdimensionaler $\mathbb{C}$-Vektorraum ist. Eindimensionale Darstellungen bezeichnen wir auch als Charaktere. Manchmal ist es bequemer, statt der Darstellung π lediglich den Darstellungsraum V mit der zugehörigen Operation von $W(K^{\text{sep}}/K)$ zu betrachten. Diesen bezeichnen wir dann als $W(K^{\text{sep}}/K)$-Modul. Eine Darstellung, die trivial auf der Trägheitsgruppe ist, heißt unverzweigt. Bei einer unverzweigten Darstellung π von $W(K^{\text{sep}}/K)$ können wir nach dem Homomorphiesatz die Trägheitsgruppe herausteilen und erhalten so eine Darstellung

$$\bar{\pi} : W(\mathbb{F}_q^{\text{alg}}/\mathbb{F}_q) \longrightarrow GL(V),$$

die wir die Restdarstellung von π nennen. Im folgenden wollen wir auf den Zusammenhang der Darstellungen von $G(K^{\text{sep}}/K)$ und den Darstellungen von $W(K^{\text{sep}}/K)$ eingehen.

Dazu befassen wir uns zunächst mit der Frage, welche Bedeutung der Stetigkeitsforderung zukommt. Wir betrachten eine Darstellung $\pi : W(K^{\text{sep}}/K) \longrightarrow GL(V)$. Sei $\mathcal{U}$ eine offene Umgebung des neutralen Elements von $GL(V)$, die keine echte Untergruppe enthält. Dann muß $\pi^{-1}(\mathcal{U})$ ebenfalls eine offene Umgebung des neutralen Elements sein. Also gibt es eine offene Untergruppe U von $W(K^{\text{sep}}/K)$ mit $U \subset \pi^{-1}(\mathcal{U})$. Dabei muß $\pi(U)$ als Teilmenge von $\mathcal{U}$ trivial sein. Daraus folgt, daß Kern(π) als Vereinigung von Nebenklassen von U offen ist. Umgekehrt ist jeder Gruppenhomomorphismus $\pi : W(K^{\text{sep}}/K) \longrightarrow GL(V)$ mit offenem Kern auch stetig. Nun sind die offenen

Untergruppen von $G(K^{\text{sep}}/K)$ genau die Untergruppen, die zu endlichen Galoiserweiterungen korrespondieren. Dies motiviert die folgende Definition.

Definition 1.1.1 *Eine Darstellung $\pi : W(K^{\text{sep}}/K) \longrightarrow GL(V)$ ist vom Galois-Typ, wenn es eine endliche Galoiserweiterung M/K gibt mit* $\text{Kern}(\pi) = W(K^{\text{sep}}/M)$.

Unter den obigen Voraussetzungen kann man π als Darstellung der endlichen Galoisgruppe

$$G(M/K) = W(K^{\text{sep}}/M)/W(K^{\text{sep}}/K)$$

auffassen. Ein Beispiel einer Darstellung, die nicht vom Galois-Typ ist, liefert der Charakter

$$\omega_K : W(K^{\text{sep}}/K) \longrightarrow \mathbb{C}^*,$$

der durch die Bedingungen $\omega_K(G_0(K^{\text{sep}}/K)) = \{1\}$ und $\omega_K(\Phi_K) = q$ bestimmt ist. Eine Darstellung, die auf $G_0(K^{\text{sep}}/K)$ trivial wird, nennen wir unverzweigt. Jeder unverzweigte Charakter ist von der Form ω_K^s mit $s \in \mathbb{C}$.

Satz 1.1.2 *Sei π eine irreduzible Darstellung von $W(K^{\text{sep}}/K)$. Dann gibt es eine Darstellung π' von $W(K^{\text{sep}}/K)$ vom Galois-Typ und ein $s \in \mathbb{C}$ mit $\pi = \omega_K^s \otimes \pi'$.*

Beweis: Sei $I := \text{Kern}(\pi) \cap G_0(K^{\text{sep}}/K)$. Wegen der Stetigkeit von π muß I als Untergruppe $G_0(K^{\text{sep}}/K)$ endlichen Index haben. Unser fixiertes Frobeniuselement Φ_K operiert nun durch Konjugation auf der Faktorgruppe $G_0(K^{\text{sep}}/K)/I$. Weil diese Faktorgruppe endlich ist, gibt es ein $n \in \mathbb{N}$, so daß Φ_K^n trivial operiert. Man überzeugt sich leicht davon, daß $\pi(\Phi_K^n)$ ein Verkettungsoperator von π mit sich selbst ist. Nach dem Lemma von Schur ist $\pi(\Phi_K^n)$ ein Skalar. Man wählt nun $s \in \mathbb{C}$ mit $(q^{-n})^s = \pi(\Phi_K^n)$ und setzt $\pi' := \omega_K^{-s} \otimes \pi$. □

Dieser Satz gestattet es nun, den Satz von Brauer für Darstellungen von $W(K^{\text{sep}}/K)$ zu formulieren. Für eine Darstellung π von $W(K^{\text{sep}}/K)$ bezeichnen wir mit $\text{Tr}(\pi)$ ihre Spurabbildung. Ist M/K eine endliche separable Erweiterung, so schreiben wir Ind_M^K für die Induktion einer Darstellung von $W(K^{\text{sep}}/M)$ nach $W(K^{\text{sep}}/K)$ und Res_K^M für die Einschränkung von $W(K^{\text{sep}}/K)$ nach $W(K^{\text{sep}}/M)$.

Korollar 1.1.3 *Sei π eine irreduzible Darstellung von $W(K^{\text{sep}}/K)$. Dann besitzt die Spurabbildung von π eine Zerlegung der Form*

$$\text{Tr}(\pi) = \sum_{i=1}^{n} c_i \text{Tr}(\text{Ind}_{M_i}^K(\chi_i))$$

mit endlichen separablen Erweiterungen M_i/K, Charakteren χ_i von $W(K^{\text{sep}}/M_i)$ und ganzen Zahlen c_i.

Beweis: Wir schreiben π in der Form $\omega_K^s \otimes \pi'$ mit π' vom Galois-Typ. Dabei können wir π' als Darstellung der Galoisgruppe $G(M/K)$ einer endlichen Galoiserweiterung M von K auffassen. Der Satz von Brauer liefert eine Zerlegung der Form

$$\text{Tr}(\pi') = \sum_{i=1}^{n} \text{Ind}_{M_i}^K(\chi_i')$$

mit Zwischenerweiterungen M_i von M/K, Charakteren χ_i' von $W(K^{\text{sep}}/M_i)$ und ganzen Koeffizienten c_i. Beachten wir nun noch, daß die Induktion mit dem Tensorprodukt vertauscht (siehe [14, Lemma 2.3]), so erhalten wir

$$\text{Tr}(\pi) = \sum_{i=1}^{n} c_i \text{Ind}_{M_i}^K(\text{Res}_K^{M_i}(\omega_K^s)\chi_i').$$

□

Wir weisen an dieser Stelle darauf hin, daß wir jeden Charakter von $W(K^{\text{sep}}/K)$ sowohl mit Hilfe der klassischen als auch mit Hilfe der modifizierten Artinabbildung

$$K^* \longrightarrow W(K^{\text{sep}}/K)^{ab}$$

als Charakter der multiplikativen Gruppe K^* auffassen können. Unter der modifizierten Artinabbindung verstehen wir die klassische Artinabbildung verkettet mit der Inversenbildung $x \longmapsto x^{-1}$ auf K^*. Die klassische Artinabbildung wird z. B. in [15] explizit beschrieben und hat die Eigenschaft, daß sie Uniformisierende modulo der Kommutatorgruppe $[W(K^{\text{sep}}/K), W(K^{\text{sep}}/K)]$ auf Frobeniuselemente abbildet. Bei der modifizierten Artinabbildung werden Uniformisierende modulo $[W(K^{\text{sep}}/K), W(K^{\text{sep}}/K)]$ auf inverse Frobeniuselemente abbgebildet. Wir werden für die gesamte Arbeit die Gruppen K^* und $W(K^{\text{sep}}/K)^{ab}$ sowie auch die Charaktere von K^* und $W(K^{\text{sep}}/K)$ stets mit der modifizierten Artinabbildung identifizieren. Insbesondere ist dann $\omega_K : K^* \longrightarrow \mathbb{C}$ der Betragscharakter, der durch die Vorschrift $x \longmapsto q^{-\nu_K(x)}$ gegeben ist.

1.2 Zur Klassifizierung von Weildarstellungen

Die Ergebnisse des vorigen Abschnitts legen es nahe, eine Darstellung π von $W(K^{\text{sep}}/K)$ aufgrund ihrer Brauerzerlegung zu charakterisieren.

Definition 1.2.1 *Die Darstellung π heißt induziert, wenn es eine endliche separable Erweiterung M von K und eine eindimensionale Darstellung χ von $W(K^{\text{sep}}/M)$ gibt mit $\pi \cong \text{Ind}_M^K(\chi)$. Ansonsten nennen wir π primitiv. Ist π induziert und können wir M so wählen, daß M/K unverzweigt ist, so nennen wir π unverzweigt induziert. Ist π induziert und können wir M nicht so wählen, daß M/K unverzweigt ist, so nennen wir π verzweigt induziert.*

Eine andere Möglichkeit, Informationen über π zu gewinnen, bietet die Untersuchung der zugehörigen projektiven Darstellung

$$\tilde{\pi} : W(K^{\text{sep}}/K) \longrightarrow PGL(V),$$

die sich aus π durch Verkettung mit der kanonischen Projektion $GL(V) \longrightarrow PGL(V)$ ergibt. Aus 1.1.2 folgt, daß Bild$(\tilde{\pi})$ endlich sein muß. Folglich gibt es eine endliche Galoiserweiterung P/K mit $W(K^{\text{sep}}/P) = \text{Kern}(\tilde{\pi})$. Diesen Körper P nennen wir den projektiven Kernkörper von π. Die Galoisgruppe $G(P/K)$ ist isomorph zu Bild$(\tilde{\pi})$.

Definition 1.2.2 *Unter dem projektiven Typ von π verstehen wir den Isomorphietyp der Galoisgruppe $G(P/K)$.*

Lemma 1.2.3 *Für zwei Darstellungen $\pi_1, \pi_2 : W(K^{\text{sep}}/K) \longrightarrow GL(V)$ gilt genau dann $\tilde{\pi_1} = \tilde{\pi_2}$, wenn es eine eindimensionale Darstellung χ von $W(K^{\text{sep}}/K)$ gibt mit $\pi_1 = \chi \otimes \pi_2$.*

Beweis: Für alle $g \in W(K^{\text{sep}}/K)$ definieren wir $\chi_(g) := \pi_1(g)(\pi_2(g))^{-1}$. Dann läßt sich $\chi(g)$ als Skalar auffassen. Auf diese Weise erhalten wir eine Abbildung $\chi : W(K^{\text{sep}}/K) \longrightarrow \mathbb{C}^*$ mit $\pi_1(g) = \chi(g)\pi_2(g)$ für alle $g \in W(K^{\text{sep}}/K)$. Wir müssen nun nur noch zeigen, daß χ multiplikativ ist. Dazu seien $g, h \in W(K^{\text{sep}}/K)$. Dann gilt

$$\chi(gh) = \pi_1(g)\pi_1(h)(\pi_2(h))^{-1}(\pi_2(g))^{-1} = \pi_1(g)\chi(h)(\pi_2(g))^{-1} = \chi(g)\chi(h).$$

□

Eine Darstellung der Form $\chi \otimes \pi$ mit einer eindimensionalen Darstellung χ von $W(K^{\text{sep}}/K)$ nennen wir Twist von π.

1.3 Der Führer

In diesem Abschnitt greifen wir auf die Ergebnisse von [21, Chap. VI] zurück. Wir betrachten eine Darstellung

$$\pi : W(K^{\text{sep}}/K) \longrightarrow GL(V).$$

Wegen der Stetigkeit von π gibt es eine endliche Galoiserweiterung R von K, so daß π auf $G_0(K^{\text{sep}}/R)$ trivial wird. Die Darstellung π definiert eine Operation der Trägheitsgruppe

$$G_0(R/K) = G_0(K^{\text{sep}}/K)/G_0(K^{\text{sep}}/R)$$

auf V. Diese Operation untersuchen wir nun genauer. Wie in [21, Chap. IV] definieren wir für alle natürlichen Zahlen i die höheren Verzweigungsgruppen

$$G_i(R/K) := \{\sigma \in G(R/K) \mid \nu_R(\sigma(T_R) - T_R) \geq i + 1\}.$$

Hierbei soll ν_R die Bewertung und T_R eine Uniformisierende von R sein. Schließlich bezeichnen wir noch mit $V^{G_i(R/K)}$ den Raum der Fixpunkte von V unter der Operation von $G_i(R/K)$.

Definition 1.3.1 *Unter den obigen Voraussetzungen heißt*

$$\text{cond}(\pi) := \sum_{i=0}^{\infty} \frac{\#G_i(R/K)}{\#G_0(R/K)} \dim(V/V^{G_i(R/K)})$$

der Führer von π.

In [21, Chap. VI, §2] wird gezeigt, daß sich $\text{cond}(\pi)$ als die Verkettungszahl von π mit einer Darstellung, der sogenannten Artin-Darstellung von $G(R/K)$, auffassen läßt. Außerdem wird gezeigt, daß $\text{cond}(\pi)$ unabhängig von der Wahl von R ist ([21, Chap. VI, Prop. 3, Cor.]). Weil sich die Verkettungszahl mit einer festen Darstellung additiv unter kurzen exakten Sequenzen verhält, liefert die Vorschrift $\pi \longmapsto \text{cond}(\pi)$ einen Homomorphismus von der Grothendieckgruppe der virtuellen Darstellungen von $W(K^{\text{sep}}/K)$ nach $\mathbb{Z}$.

Satz 1.3.2 *Sei M/K eine endliche separable Körpererweiterung und ρ eine Darstellung von $W(K^{\text{sep}}/M)$. Weiter sei $\text{d}(M/K)$ der Diskriminatenexponent und $\text{f}(M/K)$ der Trägheitsgrad von M/K. Dann gilt*

$$\text{cond}(\text{Ind}_M^K(\rho)) = \dim(\rho)\text{d}(M/K) + \text{f}(M/K)\text{cond}(\rho).$$

Beweis: Diese Aussage folgt aus [21, Chap. VI, Prop. 4, Cor.]. □

Bei eindimensionalen Darstellungen kommt dem Führer eine weitere Bedeutung zu, wie der folgende Satz zeigt.

Satz 1.3.3 *Sei χ eine eindimensionale Darstellung von $W(K^{\text{sep}}/K)$. Vermöge der modifizierten Artinabbildung fassen wir χ als Darstellung von K^* auf. Dann gilt*

$$\text{cond}(\chi) = \begin{cases} 0, & \text{falls } \chi \text{ unverzweigt ist} \\ \min\{m \in \mathbb{N} \mid \text{Kern}(\chi) \subset U_K^n\}, & \text{sonst.} \end{cases}$$

Beweis: Ohne Einschränkung können wir annehmen, daß χ vom Galois-Typ ist. Dann reicht es aus, in [21, Chap. V, Prop. 5, Cor] anzuwenden und auf die Bemerkung auf S. 228, loc. cit. zu verweisen. □

Definition 1.3.4 *Für eine Darstellung π von $W(K^{\text{sep}}/K)$ heißt*

$$\text{cond}_{\min}(\pi) := \min\{\text{cond}(\rho) \mid \rho \text{ ist Twist von } \pi\}$$

der minimale Führer von π.

Im allgemeinen ist es ein schwieriges Problem, einen Twist zu finden, dessen Führer minimal ist.

1.4 Der L-Faktor

In diesem Abschnitt betrachten wir wiederum eine Darstellung

$$\pi : W(K^{\text{sep}}/K) \longrightarrow GL(V).$$

Zunächst interessieren wir uns für die Operation eines inversen Frobeniuselements Φ_K^{-1} der Weilgruppe $W(K^{\text{sep}}/K)$ auf der Menge

$$V_0 := \{v \in V \mid \pi(\sigma)v = v \text{ für alle } \sigma \in G_0(K^{\text{sep}}/K)\}.$$

Offensichtlich hängt die Einschränkung $\pi(\Phi_K^{-1}) \mid_{V_0}$ von $\pi(\Phi_K^{-1})$ auf V_0 nicht von der Wahl von Φ_K ab.

Definition 1.4.1 *Unter den obigen Voraussetzungen heißt die meromorphe Funktion*

$$L(\pi, s) := \frac{1}{\det(1 - \omega_K^s(\Phi_K^{-1}) \otimes \pi(\Phi_K^{-1}) \mid_{V_0})}$$

der zu π gehörige L-Faktor. Für den Fall, daß $V_0 = 0$ ist, soll $L(\pi, s) = 1$ sein.

Sei $\pi' : W(K^{\text{sep}}/K) \longrightarrow GL(V')$ eine weitere Darstellung, so daß V' ein $W(K^{\text{sep}}/K)$-Untermodul von V ist. Bezeichnen wir die zum Faktormodul V/V' gehörige Darstellung mit π'', so erhalten wir

$$L(\pi, s) = L(\pi', s)L(\pi'', s).$$

Also wird durch die Vorschrift $\pi \longmapsto L(\pi, s)$ ein Homomorphismus von der Grothendieckgruppe der virtuellen Darstellungen in die multiplikative Gruppe der meromorphen Funktionen über $\mathbb{C}$ definiert.

Satz 1.4.2 *Sei M/K eine endliche separable Körpererweiterung und ρ eine Darstellung von $W(K^{\text{sep}}/K)$. Dann gilt*

$$L(\text{Ind}_M^K(\rho), s) = L(\rho, s).$$

Beweis: Für $s = 0$ siehe [5, Prop. 3.8 (ii)]. Für beliebige $s \in \mathbb{C}$ folgt

$$\begin{aligned} L(\text{Ind}_M^K(\rho), s) &= L(\omega_K^s \otimes \text{Ind}_M^K(\rho), 0) \\ &= L(\text{Ind}_M^K(\text{Res}_K^M(\omega_K^s) \otimes \rho), 0) \\ &= L(\text{Res}_K^M(\omega_K^s) \otimes \rho, 0) \\ &= L(\omega_M^s \otimes \rho, 0) \\ &= L(\rho, s). \end{aligned}$$

□

Lemma 1.4.3 *Wenn π irreduzibel und $\dim(\pi) > 1$ ist, gilt $L(\pi, s) = 1$.*

Beweis: Sei $\sigma \in W(K^{\text{sep}}/K)$ und $v \in V_0$. Weil $G_0(K^{\text{sep}}/K)$ ein Normalteiler von $W(K^{\text{sep}}/K)$ ist, gibt es für alle $g \in G_0(K^{\text{sep}}/K)$ ein $g' \in G_0(K^{\text{sep}}/K)$ mit $g\sigma = \sigma g'$. Daraus folgt

$$g(\sigma(v)) = \sigma(g(v)) = \sigma(v).$$

und damit $\sigma(v) \in V_0$. Also ist V_0 ein $W(K^{\text{sep}}/K)$-invarianter Unterraum von V. Somit gilt $V_0 = 0$ oder $V_0 = V$.

Wäre $V_0 = V$ so würde die Darstellung π über $G_0(K^{\text{sep}}/K)$ faktorisieren. Wegen

$$W(K^{\text{sep}}/K)/G_0(K^{\text{sep}}/K) \cong \mathbb{Z}$$

ergäbe sich ein Widerspruch zur Irreduzibilität von π. Also gilt $V_0 = 0$ und somit $L(\pi, s) = 1$. □

1.5 Der ϵ-Faktor

Unter einem additiven Charakter von K verstehen wir einen stetigen nichttrivialen Homomorphismus $\psi : K^+ \longrightarrow \mathbb{C}^*$, der unitär ist, d.h. der nur Werte vom Betrag 1 annimmt. Aus der Stetigkeit folgt, daß es ein $n \in \mathbb{Z}$ gibt mit $\psi(\mathfrak{p}^n) = \{1\}$. Das kleinste n mit dieser Eigenschaft nennen wir den Führer von ψ und bezeichnen es mit $\mathrm{cond}(\psi)$. Falls ψ nichttrivial ist, sind alle anderen additiven Charaktere von der Form

$$\psi_a : K^+ \longrightarrow \mathbb{C}, x \longmapsto \psi(ax)$$

mit einem geeigneten $a \in K$ (s. [10, Satz 7.7.1]).

Für die Ausführung späterer Rechnungen ist es sinnvoll, einen additiven Charakter zu fixieren. Wir tun dies nur für den Fall, daß K ein Laurentreihenkörper ist. Für den Fall, daß K eine endliche Erweiterung von $\mathbb{Q}_p$ ist, verweisen wir auf [18, §11].

Bezeichnung 1.5.1 *Im Fall $K = \mathbb{F}_q((T))$ ist ψ_K der additive Charakter von K, der durch die Vorschrift*

$$\sum_{i=n}^{\infty} a_i T^i \longmapsto e^{\frac{2\pi i}{p}\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_p}(a_{-1})}$$

definiert ist. Hierbei fassen wir $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_p}(a_{-1})$ als natürliche Zahl zwischen 0 und $p-1$ auf. Für jede endliche separable Erweiterung M von K setzen wir

$$\psi_M := \psi_K \circ \mathrm{Tr}_M^K.$$

Weil K^+ lokalkompakt ist, gibt es ein bis auf eine positive multiplikative Konstante eindeutig bestimmtes positives Integral von K^+ (s. [10, Satz C.3.1]). Dieses bezeichnen wir als additives Haarsches Maß von K. Der folgende Satz geht auf Langlands [14] und Deligne [5] zurück.

Satz 1.5.2 *Für jede endliche separable Erweiterung M/K und jedes Tripel (π, ψ, dx), das aus einer Darstellung π von $W(K^{\mathrm{sep}}/M)$, einem additiven Charakter ψ von M und einem Haarschen Maß dx von M besteht, gibt es eine eindeutig bestimmte Zahl $\epsilon(\pi, \psi, dx)$, so daß die folgenden Bedingungen erfüllt sind:*

(i) Sei $0 \longrightarrow V \longrightarrow V' \longrightarrow V'' \longrightarrow 0$ eine kurze exakte Sequenz von $W(K^{\mathrm{sep}}/K)$-Moduln mit den zugehörigen Darstellungen π, π' und π''. Dann gilt

$$\epsilon(\pi, \psi, dx) = \epsilon(\pi', \psi, dx)\epsilon(\pi'', \psi, dx)$$

für alle additiven Charaktere ψ und Haarschen Maße dx von K.

(ii) Sei M/K eine endliche separable Erweiterung und ρ eine Darstellung von $W(K^{\mathrm{sep}}/M)$. Für alle Haarschen Maße dx von K und $d_M x$ von M sowie alle additiven Charaktere ψ von K gilt

$$\epsilon(\mathrm{Ind}_M^K(\rho), \psi, dx) = \epsilon(\rho, \psi \circ \mathrm{Tr}_M^K, d_M x)\lambda(M/K, \psi, dx, d_M x)^{\dim(\rho)}.$$

Dabei ist

$$\lambda(M/K, \psi, dx, d_M x) := \frac{\epsilon(\mathrm{Ind}_M^K(1_M), \psi, dx)}{\epsilon(1_M, \psi \circ \mathrm{Tr}_M^K, d_M x)}$$

und 1_M die triviale Darstellung von $W(K^{\mathrm{sep}}/M)$.

(iii) Sei $r \in \mathbb{R}_{>0}$ eine positive Konstante. Für jede Darstellung $\pi : W(K^{\mathrm{sep}}/K) \longrightarrow GL(V)$, jeden additiven Charakter ψ und jedes Haarsche Maß dx von K gilt die Gleichung

$$\epsilon(\pi, \psi, rdx) = r^{\dim(V)}\epsilon(\pi, \psi, dx).$$

(iv) Sei M/K eine endliche separable Erweiterung von K, ψ ein additiver Charakter und $d_M x$ ein Haarsches Maß von M sowie χ eine eindimensionale Darstellung von $W(K^{\mathrm{sep}}/M)$. Vermöge der modifizierten Artinabbildung fassen wir χ als Darstellung von M^* auf und wählen ein $c \in M$ mit Bewertung $\mathrm{cond}(\chi) - \mathrm{cond}(\psi)$. Dann gilt

$$\epsilon(\chi, \psi, dx) = \begin{cases} \int\limits_{c^{-1}\mathcal{O}_M^*} \chi^{-1}(x)\psi(x)\, d_M x, & \text{falls } \chi \text{ verzweigt} \\ \chi\omega_M^{-1}(c) \int\limits_{\mathcal{O}_M} 1\, d_M x, & \text{falls } \chi \text{ unverzweigt.} \end{cases}$$

Mit dem additiven Charakter ψ von K kann man für jede lokalkonstante Funktion $f : K^* \longrightarrow \mathbb{C}$ mit kompaktem Träger eine Fourier-Transformierte

$$\hat{f}(y) = \int_K f(x)\psi(-xy)\, dx$$

definieren. Gilt nun für alle lokalkonstanten Funktionen mit kompaktem Träger die Bedingung

$$f(-x) = \hat{\hat{f}}(x),$$

so nennen wir das Haarsche Maß dx selbstdual und bezeichnen es mit $d_\psi x$. Nach [10, S. 207] ist dx genau dann selbstdual, wenn

$$\int_{\mathcal{O}_K} 1\, dx = q^{\frac{1}{2}\mathrm{cond}\psi}$$

ist. Insbesondere ist $d_\psi x$ in Abhängigkeit von ψ eindeutig bestimmt. Die Bedingung (iv) besagt nun nichts anderes, als daß

$$\epsilon(\chi, \psi, d_\psi x) = \rho(\chi, \psi)\frac{L(\chi^{-1}, 1)}{L(\chi, 0)}$$

gilt, wobei $\rho(\chi, \psi)$ den ρ-Faktor in der Funktionalgleichung von Tate bezeichnet. Dabei fassen wir wieder χ als Charakter von K^* auf. Entsprechende Rechnungen hierzu finden sich in [26] und [10].

Wir beschreiben nun, wie man für eine gegebene Weildarstellung π den ϵ-Faktor $\epsilon(\pi, \psi, dx)$ zumindest prinzipiell berechnen kann. Zunächst bestimmen wir eine Zerlegung der Form

$$\mathrm{Tr}(\pi) = \sum_{i=1}^{n} c_i(\mathrm{Ind}_{M_i}^K(\chi_i))$$

mit endlichen separablen Erweiterungen M_i/K, Charakteren χ_i von $W(K^{\mathrm{sep}}/M_i)$ und ganzen Zahlen c_i. Kennen wir nun für vorgegebene Haarsche Maße $d_{M_i}x$ die λ-Faktoren $\lambda(M_i/K, \psi, dx, d_{M_i}x)$, so erhalten wir

$$\epsilon(\pi, \psi, dx) = \prod_{i=1}^{n} \left(\lambda(M_i/K, \psi, dx, d_{M_i}x)\epsilon(\chi_i, \psi \circ \mathrm{Tr}_{M_i}^K, d_{M_i})\right)^{c_i}.$$

Hierbei lassen sich die ϵ-Faktoren $\epsilon(\chi_i, \psi \circ \mathrm{Tr}_{M_i}^K, d_{M_i})$ durch Integrale ausdrücken. Bei der Berechnung der λ-Faktoren ist das folgende Lemma nützlich.

Lemma 1.5.3 *Sei ψ ein additiver Charakter von K und M/K eine endliche separable Erweiterung. Dann gilt*

$$\mathrm{cond}(\psi \circ \mathrm{Tr}_M^K) = \mathrm{cond}(\psi) - \mathrm{d}(M/K).$$

Beweis: Zunächst ist klar, daß $\mathrm{Tr}_M^K(\mathfrak{p}_M^{\mathrm{cond}(\psi)-\mathrm{d}(M/K)})$ ein gebrochenes Ideal von K ist. Nach [21, Chap. III, Prop. 7] gilt

$$\mathrm{Tr}_M^K(\mathfrak{p}_M^{\mathrm{cond}(\psi)-\mathrm{d}(M/K)}) \subset \mathfrak{p}_K^{\mathrm{cond}(\psi)}$$

und

$$\mathrm{Tr}_M^K(\mathfrak{p}_M^{\mathrm{cond}(\psi)-\mathrm{d}(M/K)-1}) \not\subset \mathfrak{p}_K^{\mathrm{cond}(\psi)}.$$

Daraus folgt $\mathrm{cond}(\psi \circ \mathrm{Tr}_M^K) = \mathrm{cond}(\psi) - \mathrm{d}(M/K)$. □

Der folgende Satz beschreibt den Einfluß, den die Wahl des additiven Charakters ψ und das Tensorieren von π mit einem unverzweigten Charakter auf den ϵ-Faktor $\epsilon(\pi, \psi, dx)$ hat.

Satz 1.5.4 *Sei π eine Darstellung von $W(K^{\mathrm{sep}}/K)$ sowie ψ ein additiver Charakter und dx ein Haarsches Maß auf K.*

(i) Faßt man die Abbildung $\det \circ \pi$ *vermöge der modifizierten Artinabbildung als Charakter von K^* auf, so gilt für alle $a \in K^*$ die Gleichung*

$$\epsilon(\pi, \psi_a, dx) = \det \circ \pi(a) \omega_K(a)^{-\dim(\pi)} \epsilon(\pi, \psi, dx).$$

(ii) Für alle $s \in \mathbb{C}$ gilt

$$\epsilon(\omega_K^s \otimes \pi, \psi, dx) = \epsilon(\pi, \psi, dx) q^{-s(\mathrm{cond}(\psi)\dim(\pi) + \mathrm{cond}(\pi))}.$$

Beweis: Siehe [18, §11, Prop.]. □

Der nächste Satz beschreibt den Zusammenhang zwischen dem ϵ-Faktor und dem Führer einer Darstellung.

Satz 1.5.5 *Sei π eine Darstellung von $W(K^{\mathrm{sep}}/K)$ vom Galois-Typ. Dann gilt*

$$\mid \epsilon(\pi, \psi, d_\psi x) \mid = q^{\frac{1}{2}(-\mathrm{cond}(\psi)\dim(\pi) + \mathrm{cond}(\pi))}.$$

Beweis: Weil π als Darstellung vom Galois-Typ endlich faktorisiert, muß π unitär sein. Damit läßt sich [18, §12, Prop. (i)] anwenden, wodurch wir das gewünschte Resultat erhalten. □

Die Tatsache, daß der Betrag des ϵ-Faktors im wesentlichen durch den Führer festgelegt ist, motiviert die folgende Definition.

Definition 1.5.6 *Sei π eine Darstellung, ψ ein additiver Charakter und dx ein Haarsches Maß von K. Dann heißt*

$$W(\pi, \psi) = \frac{\epsilon(\pi, \psi, dx)}{\mid \epsilon(\pi, \psi, dx) \mid}$$

die Wurzelzahl von π und ψ.

Wir weisen darauf hin, daß die Wurzelzahl $W(\pi, \psi)$ wegen 1.5.2 (iii) nicht von der Wahl des Haarschen Maßes dx abhängt.

1.6 Zweidimensionale Weildarstellungen

In diesem Abschnitt sei $\pi : W(K^{\mathrm{sep}}/K) \longrightarrow GL(V)$ eine irreduzible zweidimensionale Darstellung von $W(K^{\mathrm{sep}}/K)$. Wir betrachten die zugehörige projektive Darstellung

$$\tilde{\pi} : W(K^{\mathrm{sep}}/K) \longrightarrow PGL(V).$$

Das Bild von $\tilde{\pi}$ läßt sich als endliche Untergruppe von $PGL_2(\mathbb{C})$ auffassen.

Satz 1.6.1 *Für* $\mathrm{Bild}(\tilde{\pi})$ *kommen nur die folgenden Isomorphietypen in Frage:*

- *eine Diedergruppe D_n der Ordnung $2n$,*
- *A_4 oder*

- S_4.

Beweis: Wie allgemein bekannt ist, sind alle endlichen Untergruppen von $PGL_2(\mathbb{C})$ isomorph zu A_4, S_4, A_5, zu einer zyklischen Gruppe oder zu einer Diedergruppe. Aus der Irreduzibilität von π folgt, daß Bild(π) nichtabelsch ist und deshalb auch nicht zyklisch sein kann. Außerdem scheidet der Fall Bild$(\tilde{\pi}) \cong A_5$ aus, weil sonst die Galoisgruppe des projektiven Kernkörpers nicht auflösbar wäre, was im Widerspruch zu [21, Chap. IV, Cor. 5] steht. □

Anhand des projektiven Typs können wir entscheiden, ob π primitiv oder induziert ist.

Satz 1.6.2 *Die Darstellung π ist genau dann induziert, wenn ihr projektiver Typ einer Diedergruppe entspricht.*

Beweis: Weil Twist und Induktion vertauschen, können wir annehmen, daß π vom Galois-Typ ist, und π als injektive Darstellung einer endlichen Galoisgruppe $G(M/K)$ auffassen. Weiter können wir $\tilde{\pi}$ als injektiven Homomorphismus von der Galoisgruppe $G(P/K)$ des projektiven Kernkörpers P von π nach $PGL_2(\mathbb{C})$ auffassen.

Zunächst nehmen wir an, daß π vom Diedertyp ist. Dann gibt es eine quadratische Galoiserweiterung N/K, so daß $G(P/N)$ zyklisch ist. Folglich gibt es ein $\sigma \in G(M/N)$, so daß $G(M/N)$ von $G(M/P)$ und σ erzeugt wird. Weil $G(M/P)$ zum Zentrum von $G(M/K)$ gehört, muß $G(M/N)$ abelsch sein. Somit ist $\mathrm{Res}^N_K(\pi)$ reduzibel, und es gibt Charaktere χ_1, χ_2 von $G(M/N)$ mit $\mathrm{Res}^N_K(\pi) \cong \chi_1 \oplus \chi_2$. Aufgrund der Irreduzibilität von π und der Frobeniusreziprozität folgt $\pi = \mathrm{Ind}^K_N(\chi_1)$.

Nun nehmen wir an, daß π induziert ist, d.h. es gibt eine quadratische Galoiserweiterung N/K und einen Charakter χ von $G(M/N)$ mit $\pi = \mathrm{Ind}^K_N(\chi)$. Für ein $\sigma \in G(M/K) \setminus G(M/N)$ sei χ^σ der Charakter von $G(M/N)$, der durch die Vorschrift $g \longmapsto \chi(\sigma^{-1} g \sigma)$ gegeben ist. Nach [22, Chap. 7, Prop. 22] gilt für alle $\sigma \in G(M/K) \setminus G(M/N)$ die Isomorphie $\mathrm{Res}^N_K(\pi) \cong \chi \oplus \chi^\sigma$. Hierbei gilt stets $\sigma \notin G(M/P)$, weil sonst $\chi = \chi^\sigma$ und damit Bild$(\tilde{\pi})$ abelsch wäre. Daraus folgt $G(M/P) \subset G(M/N)$. Wir betrachten nun den Charakter $\theta := \chi^{-1}\chi^\sigma$ von $G(M/N)$. Wegen $\mathrm{Kern}(\tilde{\pi}) = G(M/P)$ folgt $\mathrm{Kern}(\theta) = G(M/P)$. Somit läßt sich θ als injektiver Charakter von $G(P/N)$ auffassen. Folglich ist $G(P/N)$ eine zyklische Untergruppe von $G(P/K)$ vom Index 2. Daraus folgt $G(P/K) \ncong S_4, A_4$. (Die einzige Untergruppe von S_4 vom Index 2 ist A_4, während A_4 selbst keine Untergruppe vom Index 2 besitzt.) □

Es stellt sich nun heraus, daß primitive irreduzible zweidimensionale Darstellungen der Weilgruppe $W(K^{\mathrm{sep}}/K)$ nur unter ganz besonderen Bedingungen auftreten können.

Satz 1.6.3 *Die Darstellung π kann nur dann primitiv sein, wenn die Restcharakteristik von K gerade ist.*

Beweis: Siehe [2, Prop. 4.9.3]. □

Eine systematische Untersuchung der primitiven zweidimensionalen Darstellungen der Weilgruppe $W(K^{\mathrm{sep}}/K)$ findet sich unter anderem in [11]. Wir stellen nun einige Aussagen über den minimalen Führer von π zusammen.

Um den minimalen Führer im Fall, daß π induziert ist, berechnen zu können, betrachten wir eine beliebige separable Erweiterung M von K vom Grad 2. Weiter wählen wir ein $\sigma \in W(K^{\mathrm{sep}}/K) \setminus W(K^{\mathrm{sep}}/M)$. Für einen beliebigen Charakter $\rho : W(K^{\mathrm{sep}}/M) \longrightarrow \mathbb{C}^*$ sei ρ^σ der Charakter von $W(K^{\mathrm{sep}}/M)$, der durch die Vorschrift

$$\rho^\sigma(g) = \rho(\sigma^{-1} g \sigma)$$

gegeben ist. Wir bemerken, daß $\rho^\sigma(g)$ nicht von der Wahl von σ abhängt.

Definition 1.6.4 *Die Zahl* $\mathrm{cond}_{M/K}(\rho) := \mathrm{cond}(\rho(\rho^\sigma)^{-1})$ *heißt der relative Führer von ρ.*

Satz 1.6.5 *Wir nehmen an, daß $\pi = \mathrm{Ind}_M^K(\rho)$ ist. Wenn π unverzweigt induziert ist, soll die quadratische Erweiterung M/K unverzweigt sein. Dann gilt*

$$\mathrm{cond}_{\min}(\pi) = \begin{cases} 2\mathrm{cond}_{M/K}(\rho), & \text{falls } M/K \text{ unverzweigt ist} \\ 2\mathrm{d}(M/K) + \mathrm{cond}_{M/K}(\rho) - 1, & \text{falls } M/K \text{ verzweigt ist.} \end{cases}$$

Beweis: Sei χ eine beliebige eindimensionale Darstellung von $W(K^{\mathrm{sep}}/K)$. Nach 1.3.2 gilt

$$\mathrm{cond}(\chi \otimes \pi) = \mathrm{d}(M/K) + \mathrm{f}(M/K)\mathrm{cond}(\mathrm{Res}_K^M(\chi)\rho).$$

Also wird der Führer von $\chi \otimes \pi$ genau dann minimal, wenn der Führer von $\mathrm{Res}_K^M(\chi)\rho$ minimal ist. Um die Ergebnisse von [7] anwenden zu können, fassen wir mit Hilfe der modifizierten Artinabbildung ρ und $\mathrm{Res}_K^M(\chi)\rho$ als Charaktere von M^* und χ als Charakter von K^* auf. Aufgrund der Funktorialitätseigenschaften gilt dann $\mathrm{Res}_K^M(\chi)\rho = \chi \circ \mathrm{N}_M^K\rho$ und $\rho^\sigma = \rho \circ \sigma$. Im Fall M/K unverzweigt erhält man die gesuchte Gleichung unter Anwendung der Ergebnisse von [7, §3.2].

Wir betrachten nun den Fall, daß M/K verzweigt ist. Nach [12, Th. 1.3] muß $\mathrm{cond}_{\min}(\pi)$ ungerade sein. Wenn wir nun χ so wählen, daß der Führer von $\chi \otimes \pi$ minimal ist, muß also $\mathrm{cond}(\mathrm{Res}_K^M(\chi)\rho) - \mathrm{d}(M/K)$ ungerade sein. Die Anwendung von [7, §5.2, Lemme (c)] liefert

$$\mathrm{cond}(\mathrm{Res}_K^M(\chi)\rho) = \mathrm{cond}_{M/K}(\mathrm{Res}_K^M(\chi)\rho) + \mathrm{d}(M/K) - 1 = \mathrm{cond}_{M/K}(\rho) + \mathrm{d}(M/K) - 1.$$

Hieraus erhält man die gesuchte Gleichung. □

Leider scheint keine explizite Formel zur Berechnung eines Charakters χ, der den Führer von $\chi \otimes \pi$ minimiert, bekannt zu sein. Wir wenden uns nun dem Fall zu, daß π primitiv ist. Sei P der projektive Kernkörper von π und P_0 die maximale unverzweigte Erweiterung sowie P_1 die maximale zahm verzweigte Zwischenerweiterung von P/K. Außerdem sei t die größte natürliche Zahl mit $G_t(P/K) \neq \{\mathrm{id}_P\}$.

Satz 1.6.6 *Wenn π primitiv ist, gilt*

$$\mathrm{cond}_{\min}(\pi) = 2 + \frac{3}{[P_1 : P_0]}t.$$

Beweis: Siehe [1, Th. 2]. □

Leider scheint auch hier nicht bekannt zu sein, wie man einen Twist findet, dessen Führer minimal ist.

Wir beenden diesen Abschnitt, indem wir die besondere Bedeutung hervorheben, die den ϵ-Faktoren bei zweidimensionalen Darstellungen zukommt.

Satz 1.6.7 *Zwei irreduzible zweidimensionale Darstellungen π und π' von $W(K^{\mathrm{sep}}/K)$ sind genau dann isomorph, wenn*

$$\det \circ \pi = \det \circ \pi'$$

ist und für jeden Charakter χ von $W(K^{\mathrm{sep}}/K)$ die Identität

$$\epsilon(\chi \otimes \pi, \psi, dx) = \epsilon(\chi \otimes \pi', \psi, dx)$$

gilt.

Beweis: Diese Aussage ergibt sich aus [9, Cor. 2.19] zusammen mit dem Beweis der Langlandskorrespondenz für GL_2 in [11]. □

Das bedeutet, daß die ϵ-Faktoren aller Twists zusammen mit dem Determinantencharakter eine irreduzible zweidimensionale Darstellung von $W(K^{\mathrm{sep}}/K)$ vollständig charakterisieren.

1.7 Die Weil-Deligne-Gruppe und ihre Darstellungen

Wir definieren das semidirekte Produkt

$$W'(K^{\text{sep}}/K) := W(K^{\text{sep}}/K) \ltimes \mathbb{C},$$

indem wir auf $\mathbb{C}$ für alle $g \in W(K^{\text{sep}}/K)$ und $z \in \mathbb{C}$ die Operation

$$gzg^{-1} := \omega_K(g)z$$

erklären. Ferner versehen wir $W'(K^{\text{sep}}/K)$ mit der Produktopologie des unterliegenden kartesischen Produktes $W(K^{\text{sep}}/K) \times \mathbb{C}$. Hierdurch erhalten wir eine topologische Gruppe $W'(K^{\text{sep}}/K)$, die wir die Weil-Deligne-Gruppe von K nennen.

Unter einer Darstellung von $W'(K^{\text{sep}}/K)$ verstehen wir einen stetigen Homomorphismus

$$\pi' : W(K^{\text{sep}}/K) \longrightarrow GL(V),$$

wobei V ein endlichdimensionaler $\mathbb{C}$-Vektorraum und die Einschränkung von π auf $\mathbb{C}$ komplex analytisch ist.

Sei (π, N) ein Paar, das aus einer Darstellung

$$\pi : W(K^{\text{sep}}/K) \longrightarrow GL(V)$$

und einem nilpotenten Endomorphismus N auf V besteht, so daß für alle $g \in W(K^{\text{sep}}/K)$ die Verträglichkeitsbedingung

$$\pi(g)N\pi(g)^{-1} = \omega_K(g)N$$

erfüllt ist. Durch dieses Paar erhalten wir eine Abbildung $\pi' : W'(K^{\text{sep}}/K) \longrightarrow GL(V)$, indem wir

$$\pi'(gz) := \pi(g)\exp(zN)$$

für alle $g \in W(K^{\text{sep}}/K)$ und $z \in \mathbb{C}$ setzen. Man überzeugt sich leicht davon, daß π' eine Darstellung von $W'(K^{\text{sep}}/K)$ ist. In [18, §3] wird gezeigt, daß die Vorschrift $(\pi, N) \longmapsto \pi'$ eine bijektive Abbildung der Menge aller Paare mit den oben beschriebenen Eigenschaften in die Menge aller Darstellungen von $W'(K^{\text{sep}}/K)$ definiert. Deshalb erlauben wir uns, Darstellungen mit solchen Paaren zu identifizieren, und schreiben $\pi' = (\pi, N)$. Für die Frage, wie man aus einer gegebenen Darstellung π' von $W'(K^{\text{sep}}/K)$ das zugehörige Paar erhält, verweisen wir auf [18, §3]. Dort wird auch gesagt, wie man einige Standardoperationen von Darstellungen wie z. B. Induktion, Tensorierung oder die Bildung von direkten Summen mit Hilfe dieser Paare beschreiben kann.

1.8 Invarianten von Darstellungen der Weil-Deligne-Gruppe

In diesem Abschnitt geht es darum, den Führer sowie L- und ϵ-Faktoren für Darstellungen

$$\pi' = (\pi, N) : W'(K^{\text{sep}}/K) \longrightarrow GL(V)$$

der Weil-Deligne-Gruppe zu definieren. Für die folgenden Betrachtungen sei

$$V_0 := \{v \in V \mid \pi(\sigma)(v) = v \text{ für alle } \sigma \in G_0(K^{\text{sep}}/K)\}$$

und

$$V_0^N := \{v \in V_0 \mid Nv = 0\}.$$

Definition 1.8.1 *Die Zahl*

$$\text{cond}(\pi') := \dim V_0/V_0^N + \text{cond}(\pi)$$

heißt Führer von π'.

Den L-Faktor von π' können wir definieren, indem wir einfach V_0 durch V_0^N ersetzen.

Definition 1.8.2 *Die meromorphe Funktion*

$$L(\pi', s) := \frac{1}{\det(1 - \omega_K^s(\Phi_K^{-1}) \otimes \pi(\Phi_K^{-1})|_{V_0^N})}$$

heißt der zu π' gehörige L-Faktor. Im Fall $V_0^N = 0$ soll $L(\pi', s) = 1$ sein.

Um nun den ϵ-Faktor von π' zu definieren, betrachten wir die Operation eines inversen Frobeniuselements $\pi(\Phi_K^{-1})|_{V_0}$ auf V_0. Für alle $v \in V_0^N$ gilt

$$N\pi(\Phi_K^{-1})(v) = \pi(\Phi_K^{-1})\pi(\Phi_K)N\pi(\Phi_K^{-1})(v) = \pi(\Phi_K)\omega_K(\Phi_K^{-1})Nv = 0.$$

Also operiert das Bild $\pi(\Phi_K^{-1})$ auf dem Faktorraum V_0/V_0^N. Diese Operation bezeichnen wir mit $\pi(\Phi_K^{-1})|_{V_0/V_0^N}$.

Definition 1.8.3 *Für einen additiven Charakter $\psi : K^+ \longrightarrow \mathbb{C}$ und ein Haarsches Maß dx von K heißt die Funktion*

$$\epsilon(\pi', \psi, dx) := \epsilon(\pi, \psi, dx) \begin{cases} \det(-\pi(\Phi_K^{-1})|_{V_0/V_0^N}), & \text{falls } V_0 \neq V_0^N \\ 1, & \text{falls } V_0 = V_0^N \end{cases}$$

der ϵ-Faktor von (π', ψ, dx).

Diese Definitionen sind mit den Definitionen aus den Abschnitten 3-5 verträglich, d. h. im Fall $N = 0$ gilt $\mathrm{cond}(\pi') = \mathrm{cond}(\pi)$, $L(\pi', s) = L(\pi', s)$ und $\epsilon(\pi', \psi, dx) = \epsilon(\pi, \psi, dx)$. Außerdem verhalten sich $\mathrm{cond}(\pi')$, $L(\pi', s)$ und $\epsilon(\pi', \psi, dx)$ unter Induktion und kurzen exakten Sequenzen ähnlich wie $\mathrm{cond}(\pi)$, $L(\pi, s)$ und $\epsilon(\pi, \psi, dx)$. Für die Einzelheiten verweisen wir auf [18, §8-11].

1.9 l-adische Galoisdarstellungen

Für die folgenden Betrachtungen sei l eine von der Restcharakteristik p von K verschiedene Primzahl. Unter einer l-adischen Galoisdarstellung verstehen wir einen stetigen Homomorphismus $\pi_l' : G(K^{\mathrm{sep}}/K) \longrightarrow GL(V_l)$, wobei V_l ein endlichdimensionaler $\mathbb{Q}_l$-Vektorraum ist. Wir beschreiben nun, wie man mit Hilfe einer Konstruktion, die auf Deligne und Grothendieck zurückgeht, aus einer solchen l-adischen Darstellung eine Darstellung der Weil-Deligne-Gruppe erhält. Dazu wählen wir einen nichttrivialen stetigen Homomorphismus

$$t_l : G_0(K^{\mathrm{sep}}/K) \longrightarrow \mathbb{Q}_l$$

und fixieren ein Frobeniuselement $\Phi_K \in W(K^{\mathrm{sep}}/K)$. In [18, §4] wird das folgende Resultat gezeigt.

Satz 1.9.1 *Sei $\pi_l' : G(K^{\mathrm{sep}}/K) \longrightarrow GL(V_l)$ eine l-adische Darstellung. Dann gilt:*

(i) Es gibt eine offene Untergruppe H von $G_0(K^{\mathrm{sep}}/K)$ und einen eindeutig bestimmten nilpotenten Endomorphismus N_l von V_l, so daß

$$\pi'(h) = \exp(t_l(h)N_l)$$

für alle $h \in H$ gilt.

(ii) Für alle $g = \Phi_K^m g_0 \in W(K^{\mathrm{sep}}/K)$ mit $m \in \mathbb{Z}$ und $g_0 \in G_0(K^{\mathrm{sep}}/K)$ setze man

$$\pi_l(g) := \pi_l'(g)\exp(-t_l(g_0)N_l).$$

Dann ist

$$\begin{aligned} \pi_l : W(K^{\mathrm{sep}}/K) &\longrightarrow GL(V), \\ g &\longmapsto \pi_l(g) \end{aligned}$$

ein Homomorphismus, der auf einer offenen Untergruppe von $G_0(K^{\mathrm{sep}}/K)$ trivial wird.

(iii) Für alle $g \in W(K^{\text{sep}}/K)$ *gilt* $\pi_l(g)N_l\pi_l(g)^{-1} = \omega_K(g)N_l$.

Wir können also einer l-adischen Galoisdarstellung ein Paar (N_l, π_l) zuordnen, das der Verträglichkeitsbedingung

$$\pi_l(g)N_l\pi_l(g)^{-1} = \omega_K(g)N_l$$

genügt. Aus diesem Paar wollen wir nun eine Darstellung der Weil-Deligne-Gruppe konstruieren. Dazu fixieren wir eine Einbettung $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$. Wir definieren $\pi'_{l,\iota} := (\pi_{l,\iota}, N_{l,\iota})$, wobei $N_{l,\iota}$ das Bild von N_l unter der Einbettung $\text{End}(V_l) \hookrightarrow \text{End}(V_l \otimes_\iota \mathbb{C})$ und $\pi_{l,\iota}$ die Verkettung von π_l mit der Einbettung $GL(V_l) \hookrightarrow GL(V_l \otimes_\iota \mathbb{C})$ sein soll. In [18, §4, Prop. (iv)] wird gezeigt, daß die Isomorphieklasse von $\pi'_{l,\iota}$ unabhängig von der Wahl von t_l und der Wahl des Frobeniuselements Φ_K ist.

1.10 Elliptische Kurven und l-adische Darstellungen

Unter einer elliptischen Kurve $(\mathcal{E}, O)$ über K verstehen wir eine nichtsinguläre projektive eindimensionale Varietät $\mathcal{E}$ über K vom Geschlecht 1 zusammen mit einem ausgezeichneten K-rationalen Punkt O. Zwei elliptische Kurven $(\mathcal{E}_1, O_1)$ und $(\mathcal{E}_2, O_2)$ bezeichnen wir als isomorph, wenn es einen Isomorphismus $\phi : \mathcal{E}_1 \longrightarrow \mathcal{E}_2$ gibt mit $\phi(O_1) = O_2$. Bekanntlich ist jede elliptische Kurve isomorph zu einer elliptischen Kurve $(\mathcal{E}, O)$, wobei $\mathcal{E}$ in der projektiven Ebene durch eine Gleichung der Form

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

mit Koeffizienten $a_1, a_2, a_3, a_4, a_6 \in K$ gegeben und $O = [(0, 1, 0)]$ der ausgezeichnete Punkt ist (Siehe dazu [24, Prop. III.3.1]). Es ist leicht einzusehen, daß O der einzige Punkt „im Unendlichen“ ist, d. h. alle anderen Punkte von $\mathcal{E}$ von der Form $[(x, y, 1)]$ sind. Deshalb verwenden wir die dehomogenisierte Gleichung

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

und geben die von O verschiedenen Punkte P in der affinen Schreibweise $P = (x, y)$ an. Eine Gleichung dieser Form nennen wir Weierstraßgleichung. Wenn immer wir eine elliptische Kurve durch eine solche Gleichung angeben, meinen wir die zu der homogenen Gleichung gehörige Kurve mit dem ausgezeichneten Punkt $O = [(0, 1, 0)]$.

Wir befassen uns nun mit der Frage, inwiefern Weierstraßgleichungen elliptische Kurven definieren und inwiefern eine Weierstraßgleichung einer elliptischen Kurve eindeutig bestimmt ist. Dazu führen folgende weitere Konstanten ein:

$$\begin{aligned}
b_2 &:= a_1 + 4a_2,\\
b_4 &:= 2a_4 + a_1a_3,\\
b_6 &:= a_3^2 + 4a_6,\\
b_8 &:= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &:= b_2^2 - 24b_4,\\
c_6 &:= -b_3^2 + 36b_2b_4 - 216b_6,\\
\Delta &:= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &:= \frac{c_4^3}{\Delta}.
\end{aligned}$$

Gewöhnlich nennt man Δ die Diskriminante von $\mathcal{E}$. Eine Weierstraßgleichung obiger Form definiert genau dann eine elliptische Kurve mit ausgezeichnetem Punkt $O = [(0, 1, 0)]$, wenn $\Delta \neq 0$ ist ([24, Prop. III.1.4 (a)]). Die Konstante j nennt man die j-Invariante von $\mathcal{E}$. Sie gibt den Isomorphietyp der Kurve über dem algebraischen Abschluß von K an ([24, Prop. III.1.4 (b)]).

Die einzigen Koordinatenwechsel, die die Weierstraß-Form erhalten und den ausgezeichneten Punkt O invariant lassen, lauten

$$\begin{aligned} X &= u^2X' + r, \\ Y &= u^3Y' + u^2sX' + t, \end{aligned}$$

wobei $u, r, s, t \in K^{\text{sep}}$ sind mit $u \neq 0$. Die Konstanten a_1, a_2, a_3, a_4, a_6 gehen dabei in Konstanten $a_1', a_2', a_3', a_4', a_6'$ über. Diese berechnen sich wie folgt:

$$\begin{aligned} a_1' &= u^{-1}(a_1 + s), \\ a_2' &= u^{-2}(a_2 - sa_1 + 3r - s^2), \\ a_3' &= u^{-3}(a_3 + ra_1 + 2t), \\ a_4' &= u^{-4}(a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st), \\ a_6' &= u^{-6}(a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1). \end{aligned}$$

Für die Diskriminante Δ' und die j-Invariante j' der transformierten Kurve erhält man

$$\Delta' = \tfrac{\Delta}{u^{12}} \text{ und } j' = j.$$

Wir gehen nun auf den Fall ein, daß die durch die obige Weierstraßgleichung gegebene Kurve einen singulären Punkt besitzt. Es stellt sich heraus, daß dieser Punkt P eindeutig bestimmt und von O verschieden ist. Also ist P von der Form $P = [(x_0, y_0, 1)]$, wobei (x_0, y_0) eine Nullstelle des Polynoms

$$\mathrm{f}(x, y) := y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

ist. Weil P singulär ist, müssen die partiellen Ableitungen $\frac{\partial f}{\partial x}$ und $\frac{\partial f}{\partial y}$ an der Stelle (x_0, y_0) verschwinden. Durch Taylorentwicklung erhält man eindeutig bestimmte $\alpha, \beta \in K^{\text{sep}}$ mit

$$\mathrm{f}(x, y) - \mathrm{f}(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))\,((y - y_0) - \beta(x - x_0)) - (x - x_0)^3.$$

Falls $\alpha \neq \beta$ ist, so nennen wir P einen Knoten und α, β die Tangentensteigungen im Punkt P. Falls $\alpha = \beta$ ist, nennen wir P eine Spitze.

Man sieht leicht, daß jede Weierstraßgleichung durch eine Transformation der Form

$$\begin{aligned} X &= u^2X', \\ Y &= u^3Y' \end{aligned}$$

mit geeignetem $u \in K$ in eine Weierstraßgleichung mit ganzen Koeffizienten $a_1', a_2', a_3', a_4', a_6' \in \mathcal{O}_K$ übergeht. Hierbei können wir die Koeffizienten modulo dem maximalen Ideal $\mathfrak{p}_K$ von $\mathcal{O}_K$ reduzieren und erhalten so eine Kurve über dem Restkörper $\mathbb{F}_q$. Damit der Isomorphietyp dieser Kurve eindeutig bestimmt ist, muß man eine Minimalitäts-Forderung an die Koeffizienten der Weierstraßgleichung stellen. Eine Weierstraßgleichung mit ganzen Koeffizienten heißt minimal, wenn die Bewertung der Diskriminante $\nu_K(\Delta)$ minimal ist. Eine minimale Weierstraßgleichung geht durch eine Koordinatentransformation der Form

$$\begin{aligned} X &= u^2X' + r, \\ Y &= u^3Y' + u^2sX' + t \end{aligned}$$

genau dann in eine andere minimale Weierstraßgleichung über, wenn $u \in \mathcal{O}_K^*$ und $r, s, t \in \mathcal{O}_K$ gilt ([24, Prop. VII.1.3]). Hieraus ergibt sich, daß der Isomorphietyp der reduzierten Kurve $\overline{\mathcal{E}}$ eindeutig bestimmt ist.

Wenn $\overline{\mathcal{E}}$ keine Singularität besitzt, spricht man von guter Reduktion. Besitzt $\overline{\mathcal{E}}$ einen Knoten, spricht man von multiplikativer Reduktion. Wenn $\overline{\mathcal{E}}$ eine Spitze besitzt, spricht man von additiver Reduktion. Im Fall von multiplikativer Reduktion unterscheidet man zwischen zerfallend und nicht zerfallend multiplikativer Reduktion, je nachdem, ob die Steigungen der Tangenten an den

singulären Punkt in K liegen oder nicht. Wir bemerken, daß gute und multiplikative Reduktion stabil unter endlichen Erweiterungen des Grundkörpers K sind. Dies bedeutet, daß gute und multiplikative Reduktion einer elliptischen Kurve $\mathcal{E}$ erhalten bleiben, wenn man $\mathcal{E}$ als elliptische Kurve über einer endlichen Erweiterung M von K auffaßt ([24, Prop. VII.5.4 (b)]). Umgekehrt gibt es bei elliptischen Kurven mit additiver Reduktion eine endliche Erweiterung M von K, so daß $\mathcal{E}$ als Kurve über M betrachtet entweder gute oder multiplikative Reduktion hat. ([24, Prop. VII.5.4 (c)]). In diesem Fall spricht man von potentiell guter bzw. potentiell multiplikativer Reduktion. Ob potentiell gute oder potentiell multiplikative Reduktion vorliegt, läßt sich leicht mit dem folgenden Kriterium entscheiden:

Satz 1.10.1 *Eine elliptische Kurve über einem lokalen Körper hat genau dann potentiell gute Reduktion, wenn die j-Invariante ganz ist.*

Beweis: Siehe [24, Prop. VII.5.5.]. □

Auf den Punkten einer elliptischen Kurve $\mathcal{E}$ ist nun eine Operation $+ : \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$ definiert, die $(\mathcal{E}, +)$ zu einer abelschen Gruppe macht. Sei nun l eine von p verschiedene Primzahl. Dann bilden die l^n-Torsionspunkte von $(\mathcal{E}, +)$ in natürlicher Weise ein projektives System. Der zugehörige projektive Limes heißt Tate-Modul und wird mit $T_l(K)$ bezeichnet. Dabei hat $T_l(K)$ die Struktur eines $\mathbb{Z}_l$-Moduls der Dimension 2. Durch Tensorieren erhalten wir einen zweidimensionalen $\mathbb{Q}_l$-Vektorraum $V_l(\mathcal{E}) := T_l \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$. Das koordinatenweise Auswerten definiert eine Operation der Galoisgruppe $G(K^{\text{sep}}/K)$ auf den Punkten von $\mathcal{E}$. Diese Operation vertauscht mit der Gruppenstruktur von $(\mathcal{E}, +)$ und liefert eine zweidimensionale l-adische Darstellung

$$\pi_l : G(K^{\text{sep}}/K) \longrightarrow GL(V_l(\mathcal{E})).$$

Wir bemerken, daß isomorphe elliptische Kurven isomorphe Darstellungen liefern.

Dieser l-adischen Galoisdarstellung π_l läßt sich nun wie im letzten Abschnitt beschrieben ein Paar (π_l, N_l) zu ordnen. Für eine fixierte Einbettung $\iota : \mathbb{Q}_l \hookrightarrow \mathbb{C}$ erhält man eine Darstellung $\pi'_{\mathcal{E}} = (\pi_{\mathcal{E}}, N_{\mathcal{E}})$ der Weil-Deligne-Gruppe $W'(K^{\text{sep}}/K)$. Hierbei soll $N_{\mathcal{E}}$ das Bild von N_l unter der Einbettung $\text{End}(V_l(\mathcal{E})) \hookrightarrow \text{End}(V_l(\mathcal{E}) \otimes_\iota \mathbb{C})$ und $\pi_{\mathcal{E}}$ die Verkettung von π_l mit der Einbettung $GL(V_l(\mathcal{E})) \hookrightarrow GL(V_l(\mathcal{E}) \otimes_\iota \mathbb{C})$ sein. In [18, §14-15] wird gezeigt, daß der Isomorphietyp dieser Darstellung weder von der Wahl von l noch von der Wahl von ι abhängt. Außerdem werden die folgenden Ergebnisse gezeigt, die eine nähere Beschreibung von $\pi'_{\mathcal{E}}$ in Abhängigkeit vom Reduktionstyp von $\mathcal{E}$ liefern.

Wir betrachten zuerst den Fall, daß $\mathcal{E}$ potentiell multiplikative Reduktion hat. Falls $\mathcal{E}$ nicht schon zerfallend multiplikative Reduktion hat, gibt es eine separable quadratische Erweiterung M, so daß $\mathcal{E}$ über M zerfallend multiplikative Reduktion hat. Falls $\mathcal{E}$ schon zerfallend multiplikative Reduktion über K hat, setzen wir $M = K$. Wir definieren $\chi : W(K^{\text{sep}}/K) \longrightarrow \mathbb{C}^*$ als den eindeutig bestimmten Charakter mit $\text{Kern}(\chi) = W(K^{\text{sep}}/M)$. In [18, §15] wird das folgende Ergebnis gezeigt:

Satz 1.10.2 *Falls $\mathcal{E}$ potentiell multiplikative Reduktion hat, ist $\pi'_{\mathcal{E}}$ isomorph zu $(\chi \otimes \rho, N)$, wobei die Darstellung $\rho : W(K^{\text{sep}}/K) \longrightarrow GL(2, \mathbb{C})$ durch die Vorschrift*

$$g \longmapsto \begin{pmatrix} \omega(g) & 0 \\ 0 & 1 \end{pmatrix}$$

gegeben ist und

$$N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

gilt.

Damit ist $\pi'_{\mathcal{E}}$ vollständig beschrieben.

Nun betrachten wir den Fall, daß $\mathcal{E}$ potentiell gute Reduktion hat.

Satz 1.10.3 *Falls $\mathcal{E}$ potentiell gute Reduktion hat, gilt $N_{\mathcal{E}} = 0$, und $\pi_{\mathcal{E}}$ ist halbeinfach.*

Beweis: Siehe [18, §14, Prop.]. □

Sei nun M eine endliche separable Erweiterung, so daß $\mathcal{E}$ über M gute Reduktion besitzt. Dann besagt das bekannte Kriterium von Neron-Ogg-Shafarevich, daß die Einschränkung $\mathrm{Res}_K^M(\pi_{\mathcal{E}})$ unverzweigt ist und die Restdarstellung $\overline{\mathrm{Res}_K^M(\pi_{\mathcal{E}})}$ durch den Tate-Modul der reduzierten Kurve $\overline{\mathcal{E}}$ über dem Restklassenkörper von M gegeben ist. Diese Aussage, verallgemeinert auf beliebige abelsche Varietäten, wird in [23, §1] gezeigt. Die Theorie der elliptischen Kurven über endlichen Körpern liefert eine Methode, die die vollständige Charakterisierung von $\overline{\mathrm{Res}_K^M(\pi_{\mathcal{E}})}$ durch das Zählen rationaler Punkte erlaubt (vgl. [24, Chap. V]). Dadurch läßt sich $\mathrm{Res}_K^M(\pi_{\mathcal{E}})$ zufriedenstellend beschreiben. Die gesuchte Erweiterung M erhält man, indem man für eine von 2 und der Restcharakteristik p verschiedene Primzahl l an K die affinen Koordinaten aller l-Torsionspunkte adjungiert (siehe dazu [23, §2, Cor. 2(b)]). Wir tragen nun noch einige Ergebnisse über die Invarianten der Darstellung $\pi_{\mathcal{E}}$ zusammen.

Satz 1.10.4 *Für der Führer von $\pi_{\mathcal{E}}$ gilt die Abschätzung*

$$\mathrm{cond}(\pi_{\mathcal{E}}) \leq 2 + 3\nu_K(3) + 6\nu_K(2).$$

Beweis: Für den Fall $\mathrm{char}(K) = 0$ und $p < 5$ siehe [3, Th. 6.2]. Der Fall $p \geq 5$ ist durch [18, §18, Prop. (iii)] abgedeckt. □

Im Fall $\mathrm{char}(K) \geq 5$ erhält man $\mathrm{cond}(\pi_{\mathcal{E}}) \leq 2$. Für den Fall, daß K die Charakteristik 2 oder 3 hat, wird die Aussage dieses Satzes trivial. In der Tat kann man zeigen, daß in diesem Fall der Führer von $\pi_{\mathcal{E}}$ beliebig groß werden kann.

Satz 1.10.5 *Die Wurzelzahl $W(\pi_{\mathcal{E}}, \psi)$ hängt nicht von der Wahl des additiven Charakters ψ ab und ist entweder 1 oder -1.*

Beweis: Siehe [18, §19]. □

Satz 1.10.6 *Für den Determinantencharakter von $\pi_{\mathcal{E}}$ gilt*

$$\det \circ \pi_{\mathcal{E}} = \omega_K.$$

Beweis: Siehe [18, §16, Prop.]. □

1.11 Besonderheiten in Charakteristik 2

Ab nun soll K die Charakteristik 2 haben. Dann läßt sich K als der Laurentreihenkörper $\mathbb{F}_{2^f}((T))$ über dem Körper $\mathbb{F}_{2^f}$ mit 2^f Elementen auffassen. Wir gehen von einer elliptischen Kurve $\mathcal{E}$ aus, die durch die Weierstraßgleichung

$$Y^2 + a_1XY + a_3Y = X^3 + a_2x^2 + a_4X + a_6$$

gegeben ist. Dann erhält man für die j-Invariante

$$j = \frac{a_1^{12}}{\Delta}.$$

Nehmen wir nun an, daß $j \neq 0$ ist, so ist auch $a_1 \neq 0$, und wir können die Transformation

$$X = a_1^2 X' + \frac{a_3}{a_1},$$
$$Y = a_1^3 Y' + \frac{a_1^2 a_4 + a_3^2}{a_1^3}$$

ausführen. Indem wir X, Y für X', Y' schreiben, erhalten eine Weierstraßgleichung der Form

$$Y^2 + XY = X^3 + \alpha X^2 + \beta$$

mit $\alpha \in K$ und $\beta \in K$. Wir bemerken, daß eine Gleichung der obigen Form genau dann eine elliptische Kurve ohne Singularität beschreibt, wenn $\beta \neq 0$ ist. In diesem Fall berechnen sich j-Invariante und Diskriminante wie folgt:

$$j = \beta^{-1},$$
$$\Delta = \beta.$$

Für alle $\alpha \in K$ und $\beta \in K^*$ definiert die obige Gleichung also eine elliptische Kurve $\mathcal{E}_{\alpha,\beta}$. Die zugehörige Darstellung der Weil-Deligne-Gruppe bezeichnen wir mit $(\pi^K_{\alpha,\beta})'$. Es stellt sich nun das interessante Problem, diese Darstellung näher zu beschreiben.

Die Charakterisierung von $(\pi^K_{\alpha,\beta})'$ ist einfach im Fall $\nu_K(\beta) > 0$. Wir definieren dazu die separable Erweiterung $M := K(s)$ mit $s \in K^{\mathrm{sep}}$, so daß $s^2 + s = \alpha$ ist. Indem wir von der obigen Gleichung ausgehend die Transformation

$$X = X',$$
$$Y = Y' + sX'$$

ausführen, erhalten wir die Gleichung

$$Y'^2 + X'Y' = X'^3 + \beta.$$

Also sind $\mathcal{E}_{\alpha,\beta}$ und $\mathcal{E}_{0,\beta}$ über M isomorph. Man überzeugt sich nun leicht davon, daß $\mathcal{E}_{0,\beta}$ zerfallend multiplikative Reduktion hat. Wir definieren χ_α als den eindeutig bestimmten Charakter von $W(K^{\mathrm{sep}}/K)$ mit $\mathrm{Kern}(\chi_\alpha) = W(K^{\mathrm{sep}}/M)$. Nach 1.10.2 erhält man das folgende Ergebnis.

Satz 1.11.1 *Die Darstellung $(\pi^K_{\alpha,\beta})'$ ist isomorph zu $(\chi_\alpha \otimes \rho, N)$, wobei die Darstellung $\rho : W(K^{\mathrm{sep}}/K) \longrightarrow GL(2,\mathbb{C})$ durch die Vorschrift*

$$g \longmapsto \begin{pmatrix} \omega(g) & 0 \\ 0 & 1 \end{pmatrix}$$

gegeben ist und

$$N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

gilt.

Nun betrachten wir den Fall $\nu_K(\beta) \leq 0$. Dann hat $\mathcal{E}_{\alpha,\beta}$ potentiell gute Reduktion und die zugehörige Darstellung ist von der Form $(\pi^K_{\alpha,\beta})' = (\pi^K_{\alpha,\beta}, 0)$. Zuerst wollen wir beschreiben, wie $\pi^K_{\alpha,\beta}$ von α abhängt. Für alle $\alpha' \in K$ wählen wir ein $r \in K^{\mathrm{sep}}$ mit $r + r^2 = \alpha + \alpha'$. Wir betrachten die Transformation

$$\psi : \mathcal{E}_{\alpha,\beta} \longrightarrow \mathcal{E}_{\alpha',\beta}$$
$$(X, Y) \longmapsto (X, Y + rX),$$

mittels der wir die Punkte von $\mathcal{E}_{\alpha,\beta}$ mit den Punkten von $\mathcal{E}_{\alpha',\beta}$ identifizieren können. Wir bemerken, daß diese Transformation über $K(r)$ ein Isomorphismus ist. Folglich sind $\pi_{\alpha,\beta}$ und $\pi_{\alpha',\beta}$

auf $W(K^{\mathrm{sep}}/K(r))$ isomorph. Um zu beschreiben, wie $\pi_{\alpha,\beta}$ und $\pi_{\alpha',\beta}$ auf $W(K^{\mathrm{sep}}/K)$ zusammenhängen, definieren wir $\chi_{\alpha+\alpha'} : W(K^{\mathrm{sep}}/K) \longrightarrow \mathbb{C}^*$ als den eindeutig bestimmten Charakter mit $\mathrm{Kern}(\chi) = W(K^{\mathrm{sep}}/K(r))$. Sei $P = (x, y)$ ein Punkt von $\mathcal{E}_{0,\beta}$. Für alle $\sigma \in W(K^{\mathrm{sep}}/K)$ mit $\sigma(r) = r$ gilt

$$\sigma(\psi(P)) = (\sigma(x), \sigma(y) + r\sigma(x)) = \psi(\sigma(P)).$$

Ist dagegen $\sigma \in W(K^{\mathrm{sep}}/K)$ mit $\sigma(r) = r + 1$, so erhält man

$$\sigma(\psi(P)) = (\sigma(x), \sigma(y) + (r+1)\sigma(x)) = -\psi(\sigma(P))$$

nach [24, III.2.3]. Insgesamt erhält man also

$$\sigma(\psi(P)) = \chi_{\alpha+\alpha'}(\sigma)(\sigma(P)).$$

Hieraus ergibt sich der folgende Satz.

Satz 1.11.2 *Für alle $\alpha' \in K$ gilt*

$$\pi^K_{\alpha,\beta} \cong \chi_{\alpha+\alpha'} \otimes \pi^K_{\alpha',\beta}.$$

Im Fall $\nu_K(\beta) = 0$ gilt $\pi^K_{\alpha,\beta} \cong \chi_\alpha \otimes \pi^K_{0,\beta}$, wobei $\pi^K_{0,\beta}$ zur elliptischen Kurve $\mathcal{E}_{0,\beta}$ mit der Gleichung

$$Y^2 + XY = X^3 + \beta$$

gehört. Diese Kurve besitzt gute Reduktion. Nach dem Kriterium von Neron-Ogg-Shafarevich ist $\pi^K_{0,\beta}$ unverzweigt, wobei die Darstellung $\bar{\pi}^K_{0,\beta} : W(\mathbb{F}_2^{\mathrm{alg}}/\mathbb{F}_{2^f}) \longrightarrow GL_2(\mathbb{C})$ durch die reduzierte Kurve gegeben ist. Wegen $W(\mathbb{F}_2^{\mathrm{alg}}/\mathbb{F}_{2^f}) \cong \mathbb{Z}$ ist $\bar{\pi}^K_{0,\beta}$ eindeutig bestimmt durch das Bild des Frobeniuselements in $W(\mathbb{F}_2^{\mathrm{alg}}/\mathbb{F}_{2^f})$. Wie man dieses Bild berechnet, ist in [24, Chap. V] beschrieben. Wegen der Kommutativität von $W(\mathbb{F}_2^{\mathrm{alg}}/\mathbb{F}_{2^f})$ und der Halbeinfachheit von $\pi^K_{0,\beta}$ folgt, daß $\pi^K_{0,\beta}$ und damit auch $\pi^K_{\alpha,\beta}$ in zwei eindimensionale Darstellungen zerfällt. Der Fall, daß $\pi^K_{\alpha,\beta}$ irreduzibel ist, kann also nur auftreten, wenn $\nu_K(\beta) < 0$ ist.

Kapitel 2

Berechnung der 3-Torsionspunkte

2.1 Einleitung

Für den gesamten Rest dieser Arbeit sei $K = \mathbb{F}_{2^f}((T))$ ein lokaler Körper der Charakteristik 2 und $\alpha, \beta \in K$ mit $\beta \neq 0$. Weiter sei $\mathcal{E}_{\alpha,\beta}$ die elliptische Kurve, die durch die Weierstraßgleichung

$$Y^2 + XY = X^3 + \alpha X^2 + \beta$$

gegeben ist. In diesem Kapitel werden wir den Körper L, der aus K durch Adjunktion der affinen Koordinaten der 3-Torsionspunkte von $\mathcal{E}_{\alpha,\beta}$ entsteht, beschreiben. Außerdem werden wir die Operation der Galoisgruppe $G(K^{\text{sep}}/K)$ auf der Gruppe der 3-Torsionspunkte $\mathcal{E}_{\alpha,\beta}[3]$ explizit beschreiben.

Für die folgenden Betrachtungen wählen wir ein für allemal:

- eine primitive dritte Einheitswurzel $\varphi \in K^{\text{sep}}$,
- ein Element $\gamma \in K^{\text{sep}}$ mit $\gamma^3 = \beta$,
- ein Element $D \in K^{\text{sep}}$ mit $D + D^2 = \gamma$,
- ein Element $E \in K^{\text{sep}}$ mit $E + E^2 = D$ und
- ein Element $F_\alpha \in K^{\text{sep}}$ mit $F_\alpha + F_\alpha^2 = (D+1)E + \alpha$.

Diese Bezeichnungen bleiben für den gesamten Rest dieser Arbeit in Kraft.

Bemerkung 2.1.1 *Die Menge $\{0, 1, \varphi, \varphi+1\}$ ist ein Körper mit 4 Elementen. Bezüglich der Multiplikation gilt die folgende Verknüpfungstabelle:*

$\bullet$	0	1	φ	$\varphi+1$
0	0	0	0	0
1	0	1	φ	$\varphi+1$
φ	0	φ	$\varphi+1$	1
$\varphi+1$	0	$\varphi+1$	1	φ

2.2 Der Körper der 3-Torsionspunkte

Satz 2.2.1 *Ein Punkt $P := (x, y)$ ist genau dann ein 3-Torsionspunkt von $\mathcal{E}_{\alpha,\beta}$, wenn die Koordinaten x, y dem folgenden Gleichungssystem genügen:*

$$0 = x^4 + x^3 + \beta$$
$$0 = y^2 + xy + x^3 + \alpha x^2 + \beta.$$

Beweis: Sei P ein 3-Torsionspunkt von $\mathcal{E}_{\alpha,\beta}$. Dann müssen x, y der Gleichung

$$y^2 + xy + x^3 + \alpha x^2 + \beta = 0$$

genügen. Nach [24, III.2.3] gilt $-P = (x, y+x)$, und die x-Koordinate von $2P$ berechnet sich nach der Verdopplungsformel

$$\frac{x^4 + b_4 x^2 + b_8}{b_2 x^2 + b_6},$$

wobei $b_2 = 1$, $b_4 = 0$, $b_6 = 0$ und $b_8 = \beta$ ist. Damit $3P = O$ bzw. $2P = -P$ ist, muß also die Gleichung

$$\frac{x^4 + \beta}{x^2} = x$$

gelten. Daraus folgt $x^4 + x^3 + \beta = 0$. Also gilt für jeden 3-Torsionspunkt das obige Gleichungssystem. Weil nun $\mathcal{E}_{\alpha,\beta}$ genau acht von O verschiedene 3-Torsionspunkte besitzt (vgl. [24, III.6.4]) und das obige Gleichungssystem höchstens acht Lösungen haben kann, folgt die Aussage des Satzes. □

Wir benennen nun spezielle Elemente von K^{sep}, die im weiteren Verlauf dieser Arbeit eine wichtige Rolle spielen werden.

Bezeichnung 2.2.2 *Wir setzen*

$$\begin{aligned} x_1 &:= (D+1)E, \quad & x_2 &:= (D+1)(E+1), \\ x_3 &:= (E+\varphi)D, \quad & x_4 &:= (E+\varphi+1)D. \end{aligned}$$

Satz 2.2.3 *Die Menge aller Nullstellen des Polynoms*

$$f := X^4 + X^3 + \beta$$

lautet

$$\{x_1, x_2, x_3, x_4\}.$$

Beweis: Es gilt

$$\begin{aligned} f &= X^4 + X^3 + \gamma^3 \\ &= X^4 + X^3 + D^3(D+1)^3 \\ &= (X^2 + (D+1)X + (D+1)^2 D)(X^2 + DX + (D+1)D^2) \\ &= (X^2 + (D+1)X + (D+1)^2(E^2+E))(X^2 + DX + (E^2+E+\varphi^2+\varphi)D^2) \\ &= (X + (D+1)E)(X + (D+1)(E+1))(X + (E+\varphi)D)(X + (E+\varphi+1)D) \\ &= (X+x_1)(X+x_2)(X+x_3)(X+x_4). \end{aligned}$$

□

Korollar 2.2.4 *Der Körper $K(E, \varphi)$ ist der Zerfällungskörper des Polynoms*

$$f := X^4 + X^3 + \beta$$

über K. Insbesondere hängt $K(\varphi, E)$ nicht von der Wahl der Erzeuger φ, γ, D und E ab.

Beweis: Nach 2.2.3 ist $K(x_1, x_2, x_3, x_4)$ der Zerfällungskörper von f über K. Offensichtlich gilt $K(x_1, x_2, x_3, x_4) \subset K(E, \varphi)$. Wegen

$$E = \frac{x_1}{x_1 + x_2} \in K(x_1, x_2, x_3, x_4)$$

und

$$\varphi = \frac{x_3}{E + E^2} + E \in K(x_1, x_2, x_3, x_4)$$

erhält man die Gleichheit $K(x_1, x_2, x_3, x_4) = K(E, \varphi)$. □

Im folgenden benötigen wir weitere Abkürzungen.

Bezeichnung 2.2.5 *Wir setzen*

$$\begin{array}{ll} y_{11} := x_1(x_1 + F_\alpha), & y_{12} := x_1(x_1 + F_\alpha + 1), \\ y_{21} := x_2(x_2 + F_\alpha + E + \varphi), & y_{22} := x_2(x_2 + F_\alpha + E + \varphi + 1), \\ y_{31} := x_3(x_3 + F_\alpha + (\varphi + 1)E), & y_{32} := x_3(x_3 + F_\alpha + (\varphi + 1)E + 1), \\ y_{41} := x_4(x_4 + F_\alpha + \varphi E), & y_{42} := x_4(x_4 + F_\alpha + \varphi E + 1) \end{array}$$

und

$$\begin{array}{llll} P_{11} := (x_1, y_{11}), & P_{12} := (x_1, y_{12}), & P_{21} := (x_2, y_{21}), & P_{22} := (x_2, y_{22}), \\ P_{31} := (x_3, y_{31}), & P_{32} := (x_3, y_{32}), & P_{41} := (x_4, y_{41}), & P_{42} := (x_4, y_{42}). \end{array}$$

Satz 2.2.6 *Es gilt* $\mathcal{E}_{\alpha,\beta}[3] \setminus \{O\} = \{P_{11}, P_{12}, P_{21}, P_{22}, P_{31}, P_{32}, P_{41}, P_{42}\}$.

Beweis: Nach 2.2.1 und 2.2.3 ist lediglich

$$y_{ij}^2 + x_i y_{ij} = x_i^3 + \alpha x_i^2 + \beta$$

für alle $i = 1, \ldots, 4$ und $j = 1, 2$ zu zeigen. Dies geschieht im folgenden durch einfache Rechnungen.

(i) Für $i = 1$ und $j = 1$ gilt

$$\begin{aligned} y_{11}^2 + x_1 y_{11} &= (x_1(x_1 + F_\alpha))^2 + x_1(x_1(x_1 + F_\alpha)) \\ &= x_1^2(F_\alpha^2 + F_\alpha) + x_1^4 + x_1^3 \\ &= x_1^2((D+1)E + \alpha) + \beta \\ &= x_1^2(x_1 + \alpha) + \beta \\ &= x_1^3 + \alpha x_1^2 + \beta. \end{aligned}$$

(ii) Für $i = 1$ und $j = 2$ gilt

$$\begin{aligned} y_{12}^2 + x_1 y_{12} &= (x_1(x_1 + F_\alpha + 1))^2 + x_1(x_1(x_1 + F_\alpha + 1)) \\ &= x_1^2(F_\alpha^2 + F_\alpha) + x_1^4 + x_1^3 \\ &= x_1^3 + \alpha x_1^2 + \beta. \end{aligned}$$

(iii) Für $i = 2$ und $j = 1$ gilt

$$\begin{aligned} y_{21}^2 + x_2 y_{21} &= (x_2(x_2 + F_\alpha + E + \varphi))^2 + x_2(x_2(x_2 + F_\alpha + E + \varphi)) \\ &= x_2^2(F_\alpha^2 + F_\alpha + E^2 + E + \varphi^2 + \varphi) + x_2^4 + x_2^3 \\ &= x_2^2((D+1)E + \alpha + D + 1) + \beta \\ &= x_2^2((D+1)(E+1) + \alpha) + \beta \\ &= x_2^2(x_2 + \alpha) + \beta \\ &= x_2^3 + \alpha x_2^2 + \beta. \end{aligned}$$

(iv) Für $i = 2$ und $j = 2$ gilt

$$\begin{aligned} y_{22}^2 + x_2 y_{22} &= (x_2(x_2 + F_\alpha + E + \varphi + 1))^2 + x_2(x_2(x_2 + F_\alpha + E + \varphi + 1)) \\ &= x_2^2(F_\alpha^2 + F_\alpha + E^2 + E + \varphi^2 + \varphi) + x_2^4 + x_2^3 \\ &= x_2^3 + \alpha x_2^2 + \beta. \end{aligned}$$

(v) Für $i = 3$ und $j = 1$ gilt

$$\begin{aligned} y_{31}^2 + x_3 y_{31} &= (x_3(x_3 + F_\alpha + (\varphi+1)E))^2 + x_3(x_3(x_3 + F_\alpha + (\varphi+1)E)) \\ &= x_3^2(F_\alpha^2 + F_\alpha + (\varphi^2+1)E^2 + (\varphi+1)E) + x_3^4 + x_3^3 \\ &= x_3^2((D+1)E + \alpha + \varphi E^2 + (\varphi+1)E) + \beta \\ &= x_3^2(DE + \alpha + \varphi(E^2+E)) + \beta \\ &= x_3^2(DE + \alpha + \varphi D) + \beta \\ &= x_3^2((E+\varphi)D + \alpha) + \beta \\ &= x_3^2(x_3 + \alpha) + \beta \\ &= x_3^3 + \alpha x_3^2 + \beta. \end{aligned}$$

(vi) Für $i = 3$ und $j = 2$ gilt

$$\begin{aligned} y_{32}^2 + x_3 y_{32} &= (x_3(x_3 + F_\alpha + (\varphi+1)E + 1))^2 + x_3(x_3(x_3 + F_\alpha + (\varphi+1)E + 1)) \\ &= x_3^2(F_\alpha^2 + F_\alpha + (\varphi^2+1)E^2 + (\varphi+1)E) + x_3^4 + x_3^3 \\ &= x_3^3 + \alpha x_3^2 + \beta. \end{aligned}$$

(vii) Für $i = 4$ und $j = 1$ gilt

$$\begin{aligned} y_{41}^2 + x_4 y_{41} &= (x_4(x_4 + F_\alpha + \varphi E))^2 + x_4(x_4(x_4 + F_\alpha + \varphi E)) \\ &= x_4^2(F_\alpha^2 + F_\alpha + \varphi^2 E^2 + \varphi E) + x_4^4 + x_4^3 \\ &= x_4^2((D+1)E + \alpha + (\varphi+1)E^2 + \varphi E) + \beta \\ &= x_4^2(DE + (\varphi+1)(E^2+E) + \alpha) + \beta \\ &= x_4^2(DE + (\varphi+1)D + \alpha) + \beta \\ &= x_4^2((E+\varphi+1)D + \alpha) + \beta \\ &= x_4^2(x_4 + \alpha) + \beta \\ &= x_4^3 + \alpha x_4^2 + \beta. \end{aligned}$$

(viii) Für $i = 4$ und $j = 2$ gilt

$$\begin{aligned} y_{42}^2 + x_4 y_{42} &= (x_4(x_4 + F_\alpha + \varphi E + 1))^2 + x_4(x_4(x_4 + F_\alpha + \varphi E + 1)) \\ &= x_4^2(x_4 + F_\alpha^2 + F_\alpha + \varphi^2 E^2 + \varphi E) + x_4^4 + x_4^3 \\ &= x_4^3 + \alpha x_4^2 + \beta. \end{aligned}$$

□

Korollar 2.2.7 *Es gilt* $L = K(\varphi, E, F_\alpha)$.

Beweis: Nach 2.2.6 gilt

$$L = K(x_1, x_2, x_3, x_4, y_{11}, y_{12}, y_{21}, y_{22}, y_{31}, y_{32}, y_{41}, y_{42}).$$

Daraus folgt $L \subset K(\varphi, E, F_\alpha)$. Wegen

$$E = \frac{x_1}{x_1 + x_2}$$

und

$$F_\alpha = \frac{y_{11}}{x_1} + x_1$$

müssen E und F_α in L liegen. Außerdem gilt

$$\varphi = \frac{x_3}{E^2 + E} + E$$

Somit ist auch $\varphi \in L$. Insgesamt erhält man $L = K(\varphi, E, F_\alpha)$. □

Damit ist die Körpererweiterung L/K zufriedenstellend beschrieben. Als nächstes nehmen wir die Galoisgruppe $G(L/K)$ unter die Lupe und beschreiben deren Operation auf den Erzeugern φ, E, F_α.

Satz 2.2.8 *Sei $\sigma \in G(L/K)$. Dann kann das Tripel $(\sigma(\varphi), \sigma(E), \sigma(F_\alpha))$ nur die Werte der 1-3. Spalte bzw. der 4-6. Spalte der folgenden Tabelle annehmen:*

$\sigma(\varphi)$	$\sigma(E)$	$\sigma(F_\alpha)$	$\sigma(\varphi)$	$\sigma(E)$	$\sigma(F_\alpha)$
φ	E	F_α	φ	E	$F_\alpha + 1$
φ	$E + 1$	$F_\alpha + E + \varphi$	φ	$E + 1$	$F_\alpha + E + \varphi + 1$
φ	$E + \varphi$	$F_\alpha + (\varphi + 1)E$	φ	$E + \varphi$	$F_\alpha + (\varphi + 1)E + 1$
φ	$E + \varphi + 1$	$F_\alpha + \varphi E$	φ	$E + \varphi + 1$	$F_\alpha + \varphi E + 1$
φ	φE	$F_\alpha + (\varphi + 1)E$	φ	φE	$F_\alpha + (\varphi + 1)E + 1$
φ	$\varphi E + 1$	$F_\alpha + E + \varphi$	φ	$\varphi E + 1$	$F_\alpha + E + \varphi + 1$
φ	$\varphi E + \varphi$	$F_\alpha + \varphi E$	φ	$\varphi E + \varphi$	$F_\alpha + \varphi E + 1$
φ	$\varphi E + \varphi + 1$	F_α	φ	$\varphi E + \varphi + 1$	$F_\alpha + 1$
φ	$(\varphi + 1)E$	$F_\alpha + \varphi E$	φ	$(\varphi + 1)E$	$F_\alpha + \varphi E + 1$
φ	$(\varphi + 1)E + 1$	$F_\alpha + E + \varphi$	φ	$(\varphi + 1)E + 1$	$F_\alpha + E + \varphi + 1$
φ	$(\varphi + 1)E + \varphi$	F_α	φ	$(\varphi + 1)E + \varphi$	$F_\alpha + 1$
φ	$(\varphi + 1)E + \varphi + 1$	$F_\alpha + (\varphi + 1)E$	φ	$(\varphi + 1)E + \varphi + 1$	$F_\alpha + (\varphi + 1)E + 1$
$\varphi + 1$	E	F_α	$\varphi + 1$	E	$F_\alpha + 1$
$\varphi + 1$	$E + 1$	$F_\alpha + E + \varphi$	$\varphi + 1$	$E + 1$	$F_\alpha + E + \varphi + 1$
$\varphi + 1$	$E + \varphi$	$F_\alpha + (\varphi + 1)E$	$\varphi + 1$	$E + \varphi$	$F_\alpha + (\varphi + 1)E + 1$
$\varphi + 1$	$E + \varphi + 1$	$F_\alpha + \varphi E$	$\varphi + 1$	$E + \varphi + 1$	$F_\alpha + \varphi E + 1$
$\varphi + 1$	φE	$F_\alpha + (\varphi + 1)E$	$\varphi + 1$	φE	$F_\alpha + (\varphi + 1)E + 1$
$\varphi + 1$	$\varphi E + 1$	$F_\alpha + E + \varphi$	$\varphi + 1$	$\varphi E + 1$	$F_\alpha + E + \varphi + 1$
$\varphi + 1$	$\varphi E + \varphi$	$F_\alpha + \varphi E$	$\varphi + 1$	$\varphi E + \varphi$	$F_\alpha + \varphi E + 1$
$\varphi + 1$	$\varphi E + \varphi + 1$	F_α	$\varphi + 1$	$\varphi E + \varphi + 1$	$F_\alpha + 1$
$\varphi + 1$	$(\varphi + 1)E$	$F_\alpha + \varphi E$	$\varphi + 1$	$(\varphi + 1)E$	$F_\alpha + \varphi E + 1$
$\varphi + 1$	$(\varphi + 1)E + 1$	$F_\alpha + E + \varphi$	$\varphi + 1$	$(\varphi + 1)E + 1$	$F_\alpha + E + \varphi + 1$
$\varphi + 1$	$(\varphi + 1)E + \varphi$	F_α	$\varphi + 1$	$(\varphi + 1)E + \varphi$	$F_\alpha + 1$
$\varphi + 1$	$(\varphi + 1)E + \varphi + 1$	$F_\alpha + (\varphi + 1)E$	$\varphi + 1$	$(\varphi + 1)E + \varphi + 1$	$F_\alpha + (\varphi + 1)E + 1$

Beweis: Wir zeigen, daß $\sigma(\varphi)$, $\sigma(E)$ und $\sigma(F_\alpha)$ nur ganz bestimmte Werte annehmen können, so daß sich das Tripel $(\sigma(\varphi), \sigma(E), \sigma(F_\alpha))$ leicht in der Tabelle auffinden läßt. Wegen

$$(X + \varphi)(X + \varphi + 1) = X^2 + X + 1 \in K[X]$$

gilt $\sigma(\varphi) = \varphi$ oder $\sigma(\varphi) = \varphi + 1$. Man betrachte das Polynom

$$f := ((X^2 + X)^2 + (X^2 + X))^3 + \beta = (X^4 + X)^3 + \beta \in K[X].$$

Für alle $a, b \in \{0, 1, \varphi, \varphi + 1\}$ mit $b \neq 0$ gilt

$$\begin{aligned} f(aE + b) &= ((aE + b)^4 + aE + b)^3 + \beta \\ &= (aE^4 + b + aE + b)^3 + \beta \\ &= a^3(E^4 + E)^3 + \beta \\ &= (E^4 + E)^3 + \beta \\ &= 0. \end{aligned}$$

Wegen

$$\deg(f) = 12 = \#\{aE + b \mid a, b \in \{0, 1, \varphi, \varphi + 1\}, b \neq 0\}$$

muß $\sigma(E)$ von der Form $aE + b$ sein mit $a, b \in \{0, 1, \varphi, \varphi + 1\}$ und $b \neq 0$.

Damit wir nun entscheiden können, ob $(\sigma(\varphi), \sigma(E), \sigma(F_\alpha))$ in der Tabelle steht, müssen wir nur noch die möglichen Werte von $\sigma(F_\alpha)$ in Abhängigkeit von $\sigma(E)$ bestimmen. Dazu wählen wir $a, b \in \{0, 1, \varphi, \varphi + 1\}$ mit $a \neq 0$, so daß $\sigma(E) = aE + b$ gilt. Zunächst betrachten wir den Fall $b = 1$. Es gilt

$$\begin{aligned} &(\sigma(F_\alpha) + F_\alpha + E + \varphi)(\sigma(F_\alpha) + F_\alpha + E + \varphi + 1) \\ &\quad = \sigma(F_\alpha)^2 + \sigma(F_\alpha) + F_\alpha^2 + F_\alpha + E^2 + E + \varphi^2 + \varphi \\ &\quad = \sigma(F_\alpha^2 + F_\alpha) + (D + 1)E + \alpha + E^2 + E + 1 \\ &\quad = \sigma((D + 1)E + \alpha) + (E^2 + E + 1)E + \alpha + E^2 + E + 1 \\ &\quad = \sigma((E^2 + E + 1)E + \alpha) + E^3 + \alpha + 1 \\ &\quad = \sigma(E^3 + E^2 + E) + E^3 + 1 \\ &\quad = (aE + 1)^3 + (aE + 1)^2 + aE + 1 + E^3 + 1 \\ &\quad = a^3E^3 + E^3 \\ &\quad = 0. \end{aligned}$$

Daraus folgt $\sigma(F_\alpha) = F_\alpha + E + \varphi$ oder $\sigma(F_\alpha) = F_\alpha + E + \varphi + 1$. Nun können wir es verantworten, den Leser das Tripel $(\sigma(\varphi), \varphi(E), \sigma(F_\alpha))$ in der Tabelle auffinden zu lassen. Wir wenden uns nun dem Fall $b \neq 1$ zu. Es gilt

$$\begin{aligned} &(\sigma(F_\alpha) + F_\alpha + (ab^2 + a + 1)E)(\sigma(F_\alpha) + F_\alpha + (ab^2 + a + 1)E + 1) \\ &\quad = \sigma(F_\alpha)^2 + \sigma(F_\alpha) + F_\alpha^2 + F_\alpha + (ab^2 + a + 1)^2E^2 + (ab^2 + a + 1)E \\ &\quad = \sigma(F_\alpha^2 + F_\alpha) + (D + 1)E + \alpha + (a^2b + a^2 + 1)E^2 + (ab^2 + a + 1)E \\ &\quad = \sigma((D + 1)E + \alpha) + DE + \alpha + (a^2b + a^2 + 1)E^2 + (ab^2 + a)E \\ &\quad = \sigma((D + 1)E) + DE + (a^2b + a^2 + 1)E^2 + (ab^2 + a)E \\ &\quad = \sigma((E^2 + E + 1)E) + (E^2 + E)E + (a^2b + a^2 + 1)E^2 + (ab^2 + a)E \\ &\quad = \sigma(E^3 + E^2 + E) + E^3 + (a^2b + a^2)E^2 + (ab^2 + a)E \\ &\quad = (aE + b)^3 + (aE + b)^2 + aE + b + E^3 + (a^2b + a^2)E^2 + (ab^2 + a)E \\ &\quad = (a^3 + 1)E^3 + b + b^2 + b^3 \\ &\quad = 0. \end{aligned}$$

Daraus folgt $\sigma(F_\alpha) = F_\alpha + (ab^2 + a + 1)E$ oder $\sigma(F_\alpha) = F_\alpha + (ab^2 + a + 1)E + 1$. Auch an dieser Stelle muten wir es dem Leser wieder zu, zu verifizieren, daß das Tripel $(\sigma(\varphi), \sigma(E), \sigma(F_\alpha))$ in der Tabelle enthalten ist. □

2.3 Die Operation von $G(L/K)$ auf den 3-Torsionspunkten

Satz 2.3.1 *Die Gruppenoperation $+$ auf $\mathcal{E}_{\alpha,\beta}[3]$ hat die folgende Verknüpfungstabelle:*

$+$	O	P_{11}	P_{12}	P_{21}	P_{22}	P_{31}	P_{32}	P_{41}	P_{42}
O	O	P_{11}	P_{12}	P_{21}	P_{22}	P_{31}	P_{32}	P_{41}	P_{42}
P_{11}	P_{11}	P_{12}	O	P_{31}	P_{41}	P_{42}	P_{22}	P_{32}	P_{21}
P_{12}	P_{12}	O	P_{11}	P_{42}	P_{32}	P_{21}	P_{41}	P_{22}	P_{31}
P_{21}	P_{21}	P_{31}	P_{42}	P_{22}	O	P_{41}	P_{12}	P_{11}	P_{32}
P_{22}	P_{22}	P_{41}	P_{32}	O	P_{21}	P_{11}	P_{42}	P_{31}	P_{12}
P_{31}	P_{31}	P_{42}	P_{21}	P_{41}	P_{11}	P_{32}	O	P_{12}	P_{22}
P_{32}	P_{32}	P_{22}	P_{41}	P_{12}	P_{42}	O	P_{31}	P_{21}	P_{11}
P_{41}	P_{41}	P_{32}	P_{22}	P_{11}	P_{31}	P_{12}	P_{21}	P_{42}	O
P_{42}	P_{42}	P_{21}	P_{31}	P_{32}	P_{12}	P_{22}	P_{11}	O	P_{41}

Beweis: Wegen $2P_{11} = -P_{11}$ muß $2P_{11}$ die selbe x-Koordinate haben wie P_{11}. Weil nun x_1,x_2,x_3 und x_4 nach 2.2.3 als Nullstellen eines separablen Polynoms paarweise verschieden sind, kann nur noch $2P_{11} = P_{12}$ gelten. Mit der selben Überlegung zeigt man $2P_{21} = P_{22}$, $2P_{31} = P_{32}$ und $2P_{41} = P_{42}$.

Nach [24, III.2.3] ist $P_{11} + P_{21} = (x, y)$ mit

$$\begin{aligned} x &= \lambda^2 + \lambda + \alpha + x_1 + x_2, \\ y &= (\lambda + 1)x + \nu \end{aligned}$$

und

$$\begin{aligned} \lambda &= \frac{y_{21} + y_{11}}{x_2 + x_1}, \\ \nu &= \frac{y_{11}x_2 + y_{21}x_1}{x_2 + x_1}. \end{aligned}$$

Durch Einsetzen erhält man

$$\begin{aligned} \lambda &= \frac{x_2(x_2 + F_\alpha + E + \varphi) + x_1(x_1 + F_\alpha)}{x_2 + x_1} \\ &= \frac{(x_2 + x_1)(x_2 + x_1 + F_\alpha) + x_2(E + \varphi)}{x_2 + x_1} \\ &= x_2 + x_1 + F_\alpha + \frac{x_2(E + \varphi)}{x_2 + x_1} \\ &= (D + 1)(E + 1) + (D + 1)E + F_\alpha + \frac{(D + 1)(E + 1)(E + \varphi)}{(D + 1)(E + 1) + (D + 1)E} \\ &= D + 1 + F_\alpha + (E + 1)(E + \varphi) \\ &= F_\alpha + \varphi E + \varphi + 1 \end{aligned}$$

und

$$\begin{aligned} \nu &= \frac{x_1(x_1 + F_\alpha)x_2 + x_2(x_2 + F_\alpha + E + \varphi)x_1}{x_2 + x_1} \\ &= \frac{x_1x_2(x_1 + x_2 + E + \varphi)}{x_2 + x_1} \\ &= \frac{(D + 1)E(D + 1)(E + 1)((D + 1)E + (D + 1)(E + 1) + E + \varphi)}{(D + 1)(E + 1) + (D + 1)E} \\ &= \frac{(D + 1)^2(E^2 + E)(D + 1 + E + \varphi)}{D + 1} \\ &= (D + 1)D(E + E^2 + 1 + E + \varphi) \\ &= (D + 1)(E + \varphi)D(E + \varphi) \\ &= (D + 1)(E + \varphi)x_3. \end{aligned}$$

Daraus folgt

$$\begin{aligned}
x &= (F_\alpha + \varphi E + \varphi + 1)^2 + F_\alpha + \varphi E + \varphi + 1 + \alpha + x_1 + x_2 \\
&= F_\alpha^2 + F_\alpha + \varphi^2 E^2 + \varphi E + \varphi^2 + \varphi + \alpha + x_1 + x_2 \\
&= x_1 + \alpha + (\varphi + 1)E^2 + \varphi E + 1 + \alpha + x_1 + x_2 \\
&= (\varphi + 1)E^2 + \varphi E + x_2 + 1 \\
&= \varphi(E^2 + E) + E^2 + (D + 1)(E + 1) + 1 \\
&= \varphi D + E^2 + DE + D + E \\
&= (E + \varphi)D \\
&= x_3
\end{aligned}$$

und

$$\begin{aligned}
y &= (F_\alpha + \varphi E + \varphi + 1 + 1)x_3 + (D + 1)(E + \varphi)x_3 \\
&= x_3(F_\alpha + \varphi E + \varphi + D(E + \varphi) + E + \varphi) \\
&= x_3(F_\alpha + (\varphi + 1)E + x_3) \\
&= y_{31}.
\end{aligned}$$

Damit erhält man $P_{11} + P_{21} = P_{31}$.

Nun berechnen wir auf ähnliche Weise $P_{11} + P_{22}$. Es gilt $P_{11} + P_{22} = (x, y)$ mit

$$\begin{aligned}
x &= \lambda^2 + \lambda + \alpha + x_1 + x_2, \\
y &= (\lambda + 1)x + \nu
\end{aligned}$$

und

$$\begin{aligned}
\lambda &= \frac{y_{22} + y_{11}}{x_2 + x_1}, \\
\nu &= \frac{y_{11}x_2 + y_{22}x_1}{x_2 + x_1}.
\end{aligned}$$

Durch Einsetzen erhält man

$$\begin{aligned}
\lambda &= \frac{x_2(x_2 + F_\alpha + E + \varphi + 1) + x_1(x_1 + F_\alpha)}{x_2 + x_1} \\
&= \frac{(x_2 + x_1)(x_2 + x_1 + F_\alpha) + x_2(E + \varphi + 1)}{x_2 + x_1} \\
&= x_2 + x_1 + F_\alpha + \frac{x_2(E + \varphi + 1)}{x_2 + x_1} \\
&= (D + 1)(E + 1) + (D + 1)E + F_\alpha + \frac{(D + 1)(E + 1)(E + \varphi + 1)}{(D + 1)(E + 1) + (D + 1)E} \\
&= D + 1 + F_\alpha + (E + 1)(E + \varphi + 1) \\
&= F_\alpha + (\varphi + 1)E + \varphi
\end{aligned}$$

und

$$\begin{aligned}
\nu &= \frac{x_1(x_1+F_\alpha)x_2 + x_2(x_2+F_\alpha+E+\varphi+1)x_1}{x_2+x_1} \\
&= \frac{x_1x_2(x_1+x_2+E+\varphi+1)}{x_2+x_1} \\
&= \frac{(D+1)E(D+1)(E+1)((D+1)E+(D+1)(E+1)+E+\varphi+1)}{(D+1)(E+1)+(D+1)E} \\
&= \frac{(D+1)^2(E^2+E)(D+1+E+\varphi+1)}{D+1} \\
&= (D+1)D(E+E^2+1+E+\varphi+1) \\
&= (D+1)(E+\varphi+1)D(E+\varphi+1) \\
&= (D+1)(E+\varphi+1)x_4.
\end{aligned}$$

Daraus folgt

$$\begin{aligned}
x &= (F_\alpha+(\varphi+1)E+\varphi)^2 + F_\alpha + (\varphi+1)E + \varphi + \alpha + x_1 + x_2 \\
&= F_\alpha^2 + F_\alpha + (\varphi+1)^2E^2 + (\varphi+1)E + \varphi^2 + \varphi + \alpha + x_1 + x_2 \\
&= x_1 + \alpha + \varphi E^2 + (\varphi+1)E + 1 + \alpha + x_1 + x_2 \\
&= \varphi(E^2+E) + E + x_2 + 1 \\
&= \varphi D + E + (D+1)(E+1) + 1 \\
&= (E+\varphi+1)D \\
&= x_4
\end{aligned}$$

und

$$\begin{aligned}
y &= (F_\alpha+(\varphi+1)E+\varphi+1)x_4 + (D+1)(E+\varphi+1)x_4 \\
&= x_4(F_\alpha+(\varphi+1)E+\varphi+1+D(E+\varphi+1)+E+\varphi+1) \\
&= x_4(F_\alpha+\varphi E+x_4) \\
&= y_{41}.
\end{aligned}$$

Damit erhält man $P_{11}+P_{22}=P_{41}$.

Aus dem, was wir bis jetzt gezeigt haben, erhalten wir

$$\begin{aligned}
P_{21} &= 2P_{11} \\
P_{22} &= 2P_{21} \\
P_{31} &= P_{11}+P_{21} \\
P_{32} &= 2P_{31} \\
&= 2P_{11}+2P_{21} \\
P_{41} &= P_{11}+2P_{21} \\
P_{42} &= 2P_{41} \\
&= 2P_{11}+P_{21}.
\end{aligned}$$

Damit haben wir es geschafft, alle Elemente von $\mathcal{E}_{\alpha,\beta}[3]$ als Linearkombination von P_{11} und P_{21} darzustellen. Hiermit läßt sich nun leicht die angegebene Verknüpfungstabelle verifizieren. □

Das nächste Korollar ist eine unmittelbare Folgerung.

Korollar 2.3.2 *Das Paar (P_{11}, P_{21}) ist eine Basis von $\mathcal{E}_{\alpha,\beta}[3]$ als $\mathbb{F}_3$-Vektorraum.*

Mit Hilfe dieser Basis können wir nun vollständig die Operation von $G(L/K)$ auf $\mathcal{E}_{\alpha,\beta}[3]$ beschreiben.

Satz 2.3.3 *Für alle $\sigma \in G(L/K)$ sei $\pi(\sigma) \in GL_2(\mathbb{F}_3)$ die Matrix, die die Operation von σ auf dem $\mathbb{F}_3$- Vektorraum $\mathcal{E}_{\alpha,\beta}[3]$ bzgl. der Basis (P_{11}, P_{21}) beschreibt. Dann erhält man $\pi(\sigma)$ in Abhängigkeit von $\sigma(\varphi)$, $\sigma(E)$ und $\sigma(F_\alpha)$ gemäß der folgenden Tabelle:*

$\sigma(\varphi)$	$\sigma(E)$	$\sigma(F_\alpha)$	$\pi(\sigma)$
φ	E	F_α	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
φ	E	$F_\alpha + 1$	$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$
φ	$E + 1$	$F_\alpha + E + \varphi$	$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
φ	$E + 1$	$F_\alpha + E + \varphi + 1$	$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$
φ	$E + \varphi$	$F_\alpha + (\varphi + 1)E$	$\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$
φ	$E + \varphi$	$F_\alpha + (\varphi + 1)E + 1$	$\begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}$
φ	$E + \varphi + 1$	$F_\alpha + \varphi E$	$\begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$
φ	$E + \varphi + 1$	$F_\alpha + \varphi E + 1$	$\begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}$
φ	φE	$F_\alpha + (\varphi + 1)E$	$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$
φ	φE	$F_\alpha + (\varphi + 1)E + 1$	$\begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}$
φ	$\varphi E + 1$	$F_\alpha + E + \varphi$	$\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$
φ	$\varphi E + 1$	$F_\alpha + E + \varphi + 1$	$\begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$
φ	$\varphi E + \varphi$	$F_\alpha + \varphi E$	$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}$
φ	$\varphi E + \varphi$	$F_\alpha + \varphi E + 1$	$\begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$
φ	$\varphi E + \varphi + 1$	F_α	$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$
φ	$\varphi E + \varphi + 1$	$F_\alpha + 1$	$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$
φ	$(\varphi + 1)E$	$F_\alpha + \varphi E$	$\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$
φ	$(\varphi + 1)E$	$F_\alpha + \varphi E + 1$	$\begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}$
φ	$(\varphi + 1)E + 1$	$F_\alpha + E + \varphi$	$\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$
φ	$(\varphi + 1)E + 1$	$F_\alpha + E + \varphi + 1$	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$
φ	$(\varphi + 1)E + \varphi$	F_α	$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$
φ	$(\varphi + 1)E + \varphi$	$F_\alpha + 1$	$\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$
φ	$(\varphi + 1)E + \varphi + 1$	$F_\alpha + (\varphi + 1)E$	$\begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$
φ	$(\varphi + 1)E + \varphi + 1$	$F_\alpha + (\varphi + 1)E + 1$	$\begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$

$\varphi+1$	E	F_α	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$
$\varphi+1$	E	$F_\alpha+1$	$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$
$\varphi+1$	$E+1$	$F_\alpha+E+\varphi$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\varphi+1$	$E+1$	$F_\alpha+E+\varphi+1$	$\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$
$\varphi+1$	$E+\varphi$	$F_\alpha+(\varphi+1)E$	$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$
$\varphi+1$	$E+\varphi$	$F_\alpha+(\varphi+1)E+1$	$\begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}$
$\varphi+1$	$E+\varphi+1$	$F_\alpha+\varphi E$	$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$
$\varphi+1$	$E+\varphi+1$	$F_\alpha+\varphi E+1$	$\begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}$
$\varphi+1$	φE	$F_\alpha+(\varphi+1)E$	$\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}$
$\varphi+1$	φE	$F_\alpha+(\varphi+1)E+1$	$\begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}$
$\varphi+1$	$\varphi E+1$	$F_\alpha+E+\varphi$	$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$
$\varphi+1$	$\varphi E+1$	$F_\alpha+E+\varphi+1$	$\begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}$
$\varphi+1$	$\varphi E+\varphi$	$F_\alpha+\varphi E$	$\begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}$
$\varphi+1$	$\varphi E+\varphi$	$F_\alpha+\varphi E+1$	$\begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}$
$\varphi+1$	$\varphi E+\varphi+1$	F_α	$\begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}$
$\varphi+1$	$\varphi E+\varphi+1$	$F_\alpha+1$	$\begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}$
$\varphi+1$	$(\varphi+1)E$	$F_\alpha+\varphi E$	$\begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}$
$\varphi+1$	$(\varphi+1)E$	$F_\alpha+\varphi E+1$	$\begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}$
$\varphi+1$	$(\varphi+1)E+1$	$F_\alpha+E+\varphi$	$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$
$\varphi+1$	$(\varphi+1)E+1$	$F_\alpha+E+\varphi+1$	$\begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}$
$\varphi+1$	$(\varphi+1)E+\varphi$	F_α	$\begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}$
$\varphi+1$	$(\varphi+1)E+\varphi$	$F_\alpha+1$	$\begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}$
$\varphi+1$	$(\varphi+1)E+\varphi+1$	$F_\alpha+(\varphi+1)E$	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
$\varphi+1$	$(\varphi+1)E+\varphi+1$	$F_\alpha+(\varphi+1)E+1$	$\begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}$

Beweis: Um die nachfolgenden Rechnungen etwas übersichtlicher zu machen, leiten wir als erstes

alternative Formeln für x_1, x_2, x_3, x_4 her. Es gilt

$$\begin{aligned}
x_1 &= (D+1)E = (E^2+E+1)E = (E+1)^3+1,\\
x_2 &= (D+1)(E+1) = (E^2+E+1)(E+1) = E^3+1,\\
x_3 &= (E+\varphi)D = (E+\varphi)(E^2+E) = (E+\varphi+1)^3+1,\\
x_4 &= (E+\varphi+1)D = (E+\varphi+1)(E^2+E) = (E+\varphi)^3+1.
\end{aligned}$$

Zunächst müssen wir $\sigma(x_1)$ und $\sigma(x_2)$ in Abhängigkeit von $\sigma(E)$ berechnen. Hierzu sind zwölf Fälle zu unterscheiden. Für jeden dieser zwölf Fälle können noch einmal vier mögliche Werte für $(\sigma(\varphi), \sigma(F_\alpha))$ auftreten, in deren Abhängigkeit dann $\sigma(y_{11})$ und $\sigma(y_{21})$ zu bestimmen sind. Hieraus erhalten wir jeweils $\sigma(P_{11})$ und $\sigma(P_{21})$ und damit auch die gesuchte Matrix. Aus Platzgründen behandeln wir nur die Fälle, in denen $\sigma(E) = E$ und $\sigma(E) = E+1$ ist. Die übrigen Rechnungen überlassen wir dem Leser.

(i) Im Fall $\sigma(E) = E$ gilt

$$\sigma(x_1) = (E+1)^3+1 = x_1$$

und

$$\sigma(x_2) = E^3+1 = x_2.$$

(a) Gilt zusätzlich $\sigma(\varphi) = \varphi$ und $\sigma(F_\alpha) = F_\alpha$, so erhält man

$$\sigma(y_{11}) = x_1(x_1+F_\alpha) = y_{11}$$

und

$$\sigma(y_{21}) = x_2(x_2+F_\alpha+E+\varphi) = y_{21}.$$

Daraus folgt $\sigma(P_{11}) = P_{11}$ und $\sigma(P_{21}) = P_{21}$. Also gilt $\pi(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(b) Gilt zusätzlich $\sigma(\varphi) = \varphi$ und $\sigma(F_\alpha) = F_\alpha+1$, so erhält man

$$\sigma(y_{11}) = x_1(x_1+F_\alpha+1) = y_{12}$$

und

$$\sigma(y_{21}) = x_2(x_2+F_\alpha+1+E+\varphi) = y_{22}.$$

Daraus folgt $\sigma(P_{11}) = -P_{11}$ und $\sigma(P_{12}) = -P_{21}$. Also gilt $\pi(\sigma) = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$.

(c) Gilt zusätzlich $\sigma(\varphi) = \varphi+1$ und $\sigma(F_\alpha) = F_\alpha$, so erhält man

$$\sigma(y_{11}) = x_1(x_1+F_\alpha) = y_{11}$$

und

$$\sigma(y_{21}) = x_2(x_2+F_\alpha+E+\phi+1) = y_{22}.$$

Daraus folgt $\sigma(P_{11}) = P_{11}$ und $\sigma(P_{21}) = -P_{21}$. Also gilt $\pi(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$.

(d) Gilt zusätzlich $\sigma(\varphi) = \varphi+1$ und $\sigma(F_\alpha) = F_\alpha+1$, so erhält man

$$\sigma(y_{11}) = x_1(x_1+F_\alpha+1) = y_{12}$$

und

$$\sigma(y_{21}) = x_2(x_2+F_\alpha+1+E+\varphi+1) = y_{21}.$$

Daraus folgt $\sigma(P_{11}) = -P_{11}$ und $\sigma(P_{21}) = P_{21}$. Also gilt $\pi(\sigma) = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$.

(ii) Im Fall $\sigma(E) = E + 1$ gilt

$$\sigma(x_1) = (E + 1 + 1)^3 + 1 = x_2$$

und

$$\sigma(x_2) = (E + 1)^3 + 1 = x_1.$$

(a) Gilt zusätzlich $\sigma(\varphi) = \varphi$ und $\sigma(F_\alpha) = F_\alpha + E + \varphi$, so erhält man

$$\sigma(y_{11}) = x_2(x_2 + F_\alpha + E + \varphi) = y_{21}$$

und

$$\sigma(y_{21}) = x_1(x_1 + F_\alpha + E + \varphi + E + 1 + \varphi) = y_{12}.$$

Daraus folgt $\sigma(P_{11}) = P_{21}$ und $\sigma(P_{21}) = -P_{11}$. Also gilt $\pi(\sigma) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

(b) Gilt zusätzlich $\sigma(\varphi) = \varphi$ und $\sigma(F_\alpha) = F_\alpha + E + \varphi + 1$, so erhält man

$$\sigma(y_{11}) = x_2(x_2 + F_\alpha + E + \varphi + 1) = y_{22}$$

und

$$\sigma(y_{21}) = x_2(x_2 + F_\alpha + E + \varphi + 1 + E + 1 + \varphi) = y_{12}.$$

Daraus folgt $\sigma(P_{11}) = -P_{21}$ und $\sigma(P_{21}) = -P_{11}$. Also gilt $\pi(\sigma) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$.

(c) Gilt zusätzlich $\sigma(\varphi) = \varphi + 1$ und $\sigma(F_\alpha) = F_\alpha + E + \varphi$, so erhält man

$$\sigma(y_{11}) = x_2(x_2 + F_\alpha + E + \varphi) = y_{21}$$

und

$$\sigma(y_{21}) = x_1(x_1 + F_\alpha + E + \varphi + E + 1 + \varphi + 1) = y_{11}.$$

Daraus folgt $\sigma(P_{11}) = P_{21}$ und $\sigma(P_{21}) = -P_{11}$. Also gilt $\pi(\sigma) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

(d) Gilt zusätzlich $\sigma(\varphi) = \varphi + 1$ und $\sigma(F_\alpha) = F_\alpha + E + \varphi + 1$, so erhält man

$$\sigma(y_{11}) = x_2(x_2 + F_\alpha + E + \varphi + 1) = y_{22}$$

und

$$\sigma(y_{21}) = x_1(x_1 + F_\alpha + E + \varphi + 1 + E + 1 + \varphi + 1) = y_{11}.$$

Daraus folgt $\sigma(P_{11}) = -P_{21}$ und $\sigma(P_{21}) = -P_{11}$. Also gilt $\pi(\sigma) = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$.

□

Korollar 2.3.4 *Sei $\sigma \in G(L/K)$. Dann ist die Matrix, die σ nach der Tabelle von 2.3.3 zugeordnet wird, genau dann eine obere Dreiecksmatrix, wenn $\sigma \in G(L/K(x_1))$ ist.*

Beweis: Die besagte Matrix ist genau dann eine obere Dreiecksmatrix, wenn $\sigma(P_{11}) = P_{11}$, oder $-P_{11}$ gilt. Dies ist genau dann der Fall, wenn $\sigma(x_1) = x_1$ ist. □

2.4 Eine erste Beschreibung des Verhaltens der Erweiterung L/K

Die Körpererweiterung L/K untergliedert sich in die Zwischenerweiterungen

$$K \subset K(\varphi) \subset K(\varphi,\gamma) \subset K(\varphi,D) \subset K(\varphi,E) \subset L.$$

Im folgenden befassen wir uns mit der Frage, welche Grade die einzelnen Zwischenerweiterungen haben können. Zunächst ist klar, daß die Körpererweiterungen $K(\varphi)/K$, $K(\varphi,D)/K(\varphi,\gamma)$, $K(\varphi,E)/K(\varphi,D)$ und $L/K(\varphi,E)$ nur den Grad 1 oder 2 haben können. Außerdem kann die Erweiterung $K(\varphi,\gamma)/K(\varphi)$ als Kummererweiterung eines Körpers, der die dritten Einheitswurzeln enthält, nur den Grad 1 oder 3 haben. Für die Körpergrade der fünf Zwischenerweiterungen

$$K(\varphi)/K, K(\varphi,\gamma)/K(\varphi), K(\varphi,D)/K(\varphi,\gamma), K(\varphi,E)/K(\varphi,D), L/K(\varphi,E)$$

können also a priori $2^5 = 32$ Fälle auftreten. Wir werden nun zeigen, daß einige dieser Fälle unmöglich sind.

Lemma 2.4.1 *Falls $E \notin K(\varphi,D)$ ist, so gilt $F_\alpha \notin K(\varphi,E)$.*

Beweis: Wäre $F_\alpha \in K(\varphi,E)$, so gäbe es $A,B \in K(\varphi,D)$ mit $F_\alpha = AE+B$. Damit erhielte man

$$\begin{aligned}(D+1)E+\alpha &= AE+B+(AE+B)^2\\ &= AE+B+A^2(D+E)+B^2\\ &= (A+A^2)E+A^2D+B+B^2.\end{aligned}$$

Daraus folgte $A+A^2 = D+1$ bzw. $(A+\varphi)+(A+\varphi)^2 = D$. Also wäre $A+\varphi = E$ oder $A+\varphi+1 = E$, was beides im Widerspruch zu $E \notin K(\varphi,D)$ steht. □

Lemma 2.4.2 *Falls $[K(\varphi,\gamma):K(\varphi)] = 3$ und $E \notin K(\varphi,D)$ ist, so muß auch $D \notin K(\varphi,\gamma)$ sein.*

Beweis: Wäre $D \in K(\varphi,\gamma)$, so gäbe es $A,B,C \in K(\varphi)$ mit $D = A+B\gamma+C\gamma^2$. Damit erhält man

$$\begin{aligned}\gamma &= A+B\gamma+C\gamma^2+(A+B\gamma+C\gamma^2)^2\\ &= A+B\gamma+C\gamma^2+A^2+B^2\gamma^2+C^2\beta\gamma\\ &= A+A^2+(B+C^2\beta)\gamma+(C+B^2)\gamma^2.\end{aligned}$$

Der Koeffizientenvergleich liefert $1 = B+C^2\beta$ und $C+B^2 = 0$ bzw. $C = B^2$. Daraus folgt $1 = B+B^4\beta$. Durch Multiplikation mit γ erhält man

$$\gamma = B\gamma+B^4\beta\gamma = B\gamma+(B\gamma)^4.$$

Hieraus ergibt sich $B\gamma = E, E+1, E+\varphi$ oder $E+\varphi+1$. Daraus folgt $E \in K(\varphi,\gamma)$, was im Widerspruch zu Voraussetzung steht. □

Mit dem folgenden Satz ist es möglich, bestimmte Einschränkungen für die Wahl der Erzeuger $\varphi,\gamma,D,E,F_\alpha$ von L vorzunehmen, die es gestatten, noch mehr Fälle auszuschließen.

Satz 2.4.3 *Die Wahl der Erzeuger $\varphi,\gamma,D,E,F_\alpha$ von L kann so vorgenommen werden, daß nicht gleichzeitig $D \notin K(\varphi,\gamma)$ und $E \in K(\varphi,D)$ gilt.*

Beweis: Wir nehmen an, daß $D \notin K(\varphi,\gamma)$ und $E \in K(\varphi,D)$ ist. Dann gibt es $A, B \in K(\varphi,\gamma)$ mit $E = AD + B$. Damit erhält man

$$\begin{aligned} D &= AD + B + (AD+B)^2 \\ &= AD + B + A^2(\gamma + D) + B^2 \\ &= (A^2 + A)D + A^2\gamma + B + B^2. \end{aligned}$$

Der Koeffizientenvergleich liefert $A^2 + A = 1$ und $A^2\gamma + B + B^2 = 0$. Daraus folgt $A = \varphi$ oder $A = \varphi + 1$. Wir setzen nun $\gamma' := \gamma A^2$, $E' := EA^2$, $D' := E' + E'^2$ und wählen $F'_\alpha \in K^{\text{sep}}$ mit $F'_\alpha + F'^2_\alpha = (D'+1)E' + 1$. Dann gilt

$$\gamma'^3 = (\gamma A^2)^3 = \beta$$

und

$$\begin{aligned} D + D'^2 &= E' + E'^2 + (E' + E'^2)^2 \\ &= EA^2 + (EA^2)^4 \\ &= A^2(E + E^4) \\ &= A^2\gamma \\ &= \gamma'. \end{aligned}$$

Wegen $B + B^2 + A^2\gamma = 0$ bzw. $B + B^2 = \gamma'$ muß $B = D'$ oder $B = D' + 1$ sein. Daraus folgt $D' \in K(\varphi,\gamma')$. Indem man nun $(\varphi,\gamma,D,E,F_\alpha)$ durch $(\varphi,\gamma',D',E',F'_\alpha)$ ersetzt, erhält man die Aussage des Satzes. □

Vereinbarung 2.4.4 *Ab jetzt sollen die Erzeuger $\varphi,\gamma,D,E,F_\alpha$ so gewählt sein, daß nicht gleichzeitig $D \notin K(\varphi,\gamma)$ und $E \in K(\varphi,D)$ gilt.*

Durch diese Vereinbarung erreichen wir, daß der Grad der Erweiterung $K(\varphi,E)/K(\varphi,\gamma)$ die Körpergrade von $K(\varphi,E)/K(\varphi,D)$ und $K(\varphi,D)/K(\varphi,\gamma)$ vollständig bestimmt.

Satz 2.4.5 *Für die Grade der Körpererweiterungen $K(\varphi)/K$, $K(\varphi,\gamma)/K(\varphi)$, $K(\varphi,E)/K(\varphi,\gamma)$ und $L/K(\varphi,E)$ können höchstens die folgenden Fälle auftreten.*

$K(\varphi)/K$	$K(\varphi,\gamma)/K(\varphi)$	$K(\varphi,E)/K(\varphi,\gamma)$	$L/K(\varphi,E)$
1	1	1	1
1	1	1	2
1	1	2	2
1	1	4	2
1	3	1	1
1	3	1	2
1	3	4	2
2	1	1	1
2	1	1	2
2	1	2	2
2	1	4	2
2	3	1	1
2	3	1	2
2	3	4	2

Beweis: Alle anderen Fälle scheiden wegen 2.4.1 und 2.4.2 aus. □

Korollar 2.4.6 *Wenn $G(L/K)$ nichtabelsch ist, können für die Körpergrade der Erweiterungen $K(\varphi)/K$, $K(\varphi,\gamma)/K(\varphi)$, $K(\varphi,E)/K(\varphi,\gamma)$ und $L/K(\varphi,E)$ nur die folgenden Fälle auftreten:*

$K(\varphi)/K$	$K(\varphi,\gamma)/K(\varphi)$	$K(\varphi,E)/K(\varphi,\gamma)$	$L/K(\varphi,E)$
1	1	4	2
1	3	4	2
2	1	2	2
2	1	4	2
2	3	1	1
2	3	1	2
2	3	4	2

Beweis: Zunächst nehmen wir an, daß die Bedingungen $[K(\varphi):K]=1$, $[K(\varphi,\gamma):K(\varphi)]=3$, $[K(\varphi,E):K(\varphi,\gamma)]=1$ und $[L:K(\varphi,E)]=2$ gelten. Dann muß es einen Automorphismus $\sigma\in G(L/K)$ geben, der trivial auf $K(\varphi,E)$, aber nicht trivial auf L ist. Daraus folgt $\sigma(\varphi)=\varphi$, $\sigma(E)=E$ und $\sigma(F_\alpha)=F_\alpha+1$. Nach 2.3.3 entspricht die Operation von σ auf $\mathcal{E}_{\alpha,\beta}[3]$ bzgl. der Basis (P_{11},P_{21}) der Matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Weil diese Matrix im Zentrum von $GL_2(\mathbb{F}_3)$ liegt, muß σ mit allen anderen Elementen von $G(L/K)$ vertauschen. Wir wählen nun ein $\rho\in G(L/K)\setminus <\sigma>$. Wegen $\#G(L/K)=6$ gilt die Identität $G(L/K)=<\rho,\sigma>$. Daraus folgt, daß $G(L/K)$ abelsch ist. In allen anderen Fällen, die unter 2.4.5 aufgelistet sind und unter 2.4.6 fehlen, gilt $[L:K]<6$, woraus die Kommutativität von $G(L/K)$ folgt. □

Zum Schluß dieses Kapitels verweisen wir darauf, daß wir bis jetzt keinen Gebrauch davon gemacht haben, daß K ein lokaler Körper ist. Wir haben nur verwendet, daß K die Charakteristik 2 hat. Insofern stellt dieses Kapitel einen ganz allgemeinen Beitrag zur Theorie der elliptischen Kurven über einem Körper der Charakteristik 2 dar.

Kapitel 3

Beschreibung des Tate-Moduls

3.1 Bestimmung der Deligne-Zerlegung

Für den Rest der gesamten Arbeit nehmen wir an, daß $\nu_K(\beta) < 0$ ist, wenn nicht ausdrücklich etwas anders vereinbart ist. Dies wird nur in 4.2 der Fall sein. Insbesondere soll $\nu_K(\beta) < 0$ für den gesamten Rest dieses Kapitels gelten. Zunächst befassen wir uns mit dem Isomorphietyp, den unsere elliptische Kurve $\mathcal{E}_{\alpha,\beta} : Y^2 + XY = X^3 + \alpha X^2 + \beta$ als Kurve über dem Körper $L = K(\varphi, E, F_\alpha)$ hat.

Satz 3.1.1 *Die Kurve $\mathcal{E}_{\alpha,\beta}$ ist über dem Körper L isomorph zur elliptischen Kurve $\mathcal{E}$, die durch die Gleichung*

$$Y^2 + E^{-1}XY + Y = X^3 + E^{-3} + 1$$

gegeben ist. Diese Gleichung ist minimal. Darüber hinaus hat $\mathcal{E}$ gute Reduktion, wobei die reduzierte Kurve $\bar{\mathcal{E}}$ durch die Gleichung

$$Y^2 + Y = X^3 + 1$$

gegeben ist.

Beweis: Indem wir die Transformation $(X, Y) \longmapsto (X, Y + (E + F_\alpha))$ ausführen, erhalten wir die Gleichung

$$Y^2 + XY = X^3 + (F_\alpha + F_\alpha^2 + E + E^2)X^2 + \alpha + \beta.$$

Unter Verwendung der Identitäten

$$F_\alpha + F_\alpha^2 = (D + 1)E + \alpha = E^3 + E^2 + E + \alpha$$

und

$$\beta = \gamma^3 = (E + E^4)^3 = E^3 + E^6 + E^9 + E^{12}$$

lautet diese Gleichung

$$Y^2 + XY = X^3 + E^3X^2 + E^3 + E^6 + E^9 + E^{12}.$$

Wir bemerken, daß die auftretenden Koeffizienten nicht mehr von α abhängen. Nun führen wir die Transformation $(X, Y) \longmapsto (X + E^3, Y + E^6)$ durch, mit der wir die deutlich vereinfachte Gleichung

$$Y^2 + XY + E^3Y = X^3 + E^3 + E^6$$

bekommen. Zuletzt erhalten wir durch die Transformation $(X, Y) \longmapsto (E^2X, E^3Y)$ die Gleichung

$$Y^2 + E^{-1}XY + Y = X^3 + E^{-3} + 1.$$

Weil sich alle Transformationen über L ausführen lassen, folgt die Isomorphie von $\mathcal{E}_{\alpha,\beta}$ und $\mathcal{E}$ über L. Die Diskriminante dieser Gleichung lautet

$$\Delta = (E^{-2})^2(E^{-2}(E^{-3} + 1)) + 1 + E^{-2}E^{-1} = 1 + E^{-3} + E^{-6} + E^{-9}$$

Wegen $\nu_K(\beta) < 0$ muß auch $\nu_L(E) < 0$ sein. Daraus folgt $\nu_L(\Delta) = 0$. Hieraus ergeben sich die übrigen Aussagen. □

Das Bemerkenswerte an diesem Ergebnis ist, daß der Isomorphietyp von $\bar{\mathcal{E}}$ nicht von β abhängt. Dieser Umstand gestattet es uns, im folgenden die Einschränkung der zu $\mathcal{E}_{\alpha,\beta}$ gehörigen Weildarstellung $\pi^K_{\alpha,\beta}$ auf die Untergruppe $W(K^{\text{sep}}/L)$ einheitlich zu beschreiben. Nach dem Kriterium von Neron-Ogg-Shafarevich ist diese Darstellung unverzweigt. Wir betrachten die Darstellung

$$\bar{\pi} : W(K^{\text{sep}}/L)/G_0(K^{\text{sep}}/L) \longrightarrow GL_2(\mathbb{C}),$$

die wir aus $\text{Res}^L_K \pi^K_{\alpha,\beta}$ durch Herausteilen von $G_0(K^{\text{sep}}/L)$ erhalten. Wenn wir den Restklassenkörper von L mit $\mathbb{F}_{2^g}$ bezeichnen, können wir $W(K^{\text{sep}}/L)/G_0(K^{\text{sep}}/L)$ mit $W(\mathbb{F}_2^{\text{alg}}/\mathbb{F}_{2^g})$ identifizieren. Dann ist die Darstellung $\bar{\pi}$ durch den Tate-Modul der Kurve $\bar{\mathcal{E}}$ bestimmt, die durch die Gleichung

$$Y^2 + Y = X^3 + 1$$

gegeben ist. Weil nun $W(\mathbb{F}_2^{\text{alg}}/\mathbb{F}_{2^g})$ zyklisch ist, reicht es aus, $\bar{\pi}(\Phi_{\mathbb{F}_{2^g}})$ zu bestimmen, wobei $\Phi_{\mathbb{F}_{2^g}}$ der Frobeniusautomorphismus $x \longmapsto x^{2^g}$ sein soll. Da wir außerdem wissen, daß $\pi^K_{\alpha,\beta}$ halbeinfach ist, genügt es, die Eigenwerte von $\bar{\pi}(\Phi_{\mathbb{F}_{2^g}})$ zu ermitteln.

Lemma 3.1.2 *Die Matrix $\bar{\pi}(\Phi_{\mathbb{F}_{2^g}}) \in GL_2(\mathbb{C})$ hat die Eigenwerte $(\sqrt{2}i)^g$ und $(-\sqrt{2}i)^g$.*

Beweis: Zunächst fassen wir $\bar{\mathcal{E}}$ als elliptische Kurve über $\mathbb{F}_2$ auf. Die elliptische Kurve $\bar{\mathcal{E}}$ hat über $\mathbb{F}_2$ genau 3 Punkte, nämlich O, $(1,0)$ und $(1,1)$. Nach [24, p. 136] gilt für die gesuchten Eigenwerte λ_1 und λ_2 die Gleichung

$$3 = 1 - \lambda_1 - \lambda_2 + 2.$$

Außerdem müssen λ_1 und λ_2 zueinander komplex konjugiert sein und den Absolutbetrag $\sqrt{2}$ haben. Hierfür kommen nur noch die Werte $\sqrt{2}i$ und $-\sqrt{2}i$ in Frage. Wegen $\Phi_{\mathbb{F}_{2^g}} = \Phi^g_{\mathbb{F}_2}$ folgt die Aussage des Lemmas. □

Nun können wir eine Zerlegung von $\pi^K_{\alpha,\beta}$ im Sinne von 1.1.2 angeben. Dazu benennen wir einen ganz speziellen unverzweigten Charakter von $W(K^{\text{sep}}/K)$.

Bezeichnung 3.1.3 *Wir setzen $\Omega_K = \omega_K^{-\frac{1}{2} + i\frac{\pi}{2\ln(2)}}$.*

Satz 3.1.4 *Die Darstellung*

$$\Omega_K \otimes \pi^K_{\alpha,\beta} : W(K^{\text{sep}}/K) \longrightarrow GL_2(\mathbb{C})$$

ist trivial auf $W(K^{\text{sep}}/L)$.

Beweis: Wegen der Unverzweigtheit des Charakters Ω_K können wir die Eischränkung des Twists $\Omega_K \otimes \pi^K_{\alpha,\beta}$ auf $W(K^{\text{sep}}/K)$ auch als Darstellung von $W(\mathbb{F}_2^{\text{alg}}/\mathbb{F}_{2^g})$ auffassen und müssen dann nur noch zeigen, daß $\Omega_K \otimes \pi^K_{\alpha,\beta}(\Phi_{\mathbb{F}_{2^g}})$ trivial ist. Wegen $\varphi \in L$ muß der Restklassenkörper $\mathbb{F}_{2^g}$ von L den Körper $\mathbb{F}_4 = \{0, 1, \varphi, \varphi + 1\}$ enthalten. Also ist g gerade. Nach 3.1.2 hat $\pi_{\alpha,\beta}(\Phi_{\mathbb{F}_{2^g}})$ zweimal den Eigenwert $(\sqrt{2}i)^g$. Weil $\pi^K_{\alpha,\beta}$ halbeinfach ist, können wir $\pi^K_{\alpha,\beta}(\Phi_{\mathbb{F}_{2^g}})$ als den Skalar $(\sqrt{2}i)^g$ auffassen. Hieraus folgt

$$\begin{aligned}
\Omega_K \otimes \pi^K_{\alpha,\beta}(\Phi_{\mathbb{F}_{2^g}}) &= \Omega_K(\Phi_{\mathbb{F}_{2^g}})\pi^K_{\alpha,\beta}(\Phi_{\mathbb{F}_{2^g}}) \\
&= (2^g)^{-\frac{1}{2} + i\frac{\pi}{2\ln(2)}} (\sqrt{2}i)^g \\
&= (2^g)^{i\frac{\pi}{2\ln(2)}} i^g \\
&= e^{i\frac{\pi}{2}g} i^g \\
&= (-1)^g \\
&= 1.
\end{aligned}$$

□

Korollar 3.1.5 *Es gilt*

$$\mathrm{Kern}(\Omega_K \otimes \pi^K_{\alpha,\beta}) = W(K^{\mathrm{sep}}/L).$$

Beweis: Sei $\sigma \in \mathrm{Kern}(\Omega_K \otimes \pi^K_{\alpha,\beta})$. Dann ist $\pi^K_{\alpha,\beta}(\sigma)$ ein Skalar. Folglich muß σ auch als Skalar auf den 3-Torsionspunkten von $\mathcal{E}_{\alpha,\beta}$ operieren. Nach der Tabelle von Satz 2.3.3 erhält man $\sigma(\varphi) = \varphi$, $\sigma(E) = E$ und $\sigma(F_\alpha) \in \{F_\alpha, F_\alpha + 1\}$. Also ist $\sigma \in W(K^{\mathrm{sep}}/K(\varphi, E))$. Hieraus folgt

$$\mathrm{Kern}(\Omega_K \otimes \pi_{\alpha,\beta}) \subset W(K^{\mathrm{sep}}/K(\varphi, E)).$$

Weil nach 3.1.4 $\mathrm{Kern}(\Omega_K \otimes \pi_{\alpha,\beta}) \supset W(K^{\mathrm{sep}}/L)$ gilt, müssen wir nur noch den Fall $L \neq K(\varphi, E)$ betrachten und zeigen, daß die Einschränkung

$$\mathrm{Res}^{K(\varphi,E)}_K \left(\Omega_K \otimes \pi^K_{\alpha,\beta}\right) \cong \Omega_{K(\varphi,E)} \otimes \pi^{K(\varphi,E)}_{\alpha,\beta}$$

nicht trivial ist. Dazu sei $\chi : W(K^{\mathrm{sep}}/K(\varphi, E)) \longrightarrow \mathbb{C}^*$ der eindeutig bestimmte Charakter mit $\mathrm{Kern}(\chi) = W(K^{\mathrm{sep}}/L)$. Nach 1.11.2 gilt die Isomorphie

$$\pi^{K(\varphi,E)}_{\alpha,\beta} \cong \chi \otimes \pi^{K(\varphi,E)}_{E^3,\beta}.$$

Wegen

$$F_{E^3} + (F_{E^3})^2 = (D+1)E + E^3 = D$$

gilt $K(F_{E^3}, E, \varphi) = K(E, \varphi)$. Nach 3.1.4 folgt, daß $\Omega_{K(\varphi,E)} \otimes \pi^{K(\varphi,E)}_{E^3,\beta}$ trivial ist. Damit erhalten wir die Nichttrivialität von

$$\Omega_{K(\varphi,E)} \otimes \pi^{K(\varphi,E)}_{\alpha,\beta} \cong \chi \oplus \chi.$$

□

Damit haben wir das Problem der Beschreibung von $\pi^K_{\alpha,\beta}$ auf das Problem der Beschreibung einer Darstellung vom Galois-Typ zurückgeführt. Dieser Darstellung, die wir nun weiter untersuchen werden, geben wir einen speziellen Namen.

Vereinbarung 3.1.6 *Die Darstellung $\Omega_K \otimes \pi^K_{\alpha,\beta}$ bezeichnen wir mit $\rho^K_{\alpha,\beta}$ und fassen sie als injektive Darstellung von*

$$W(K^{\mathrm{sep}}/K)/W(K^{\mathrm{sep}}/L) \cong G(L/K)$$

auf.

Korollar 3.1.7 *Die Darstellung $\pi^K_{\alpha,\beta}$ ist genau dann reduzibel, wenn $G(L/K)$ abelsch ist.*

Beweis: Offensichtlich ist $\pi^K_{\alpha,\beta}$ genau dann reduzibel, wenn $\rho^K_{\alpha,\beta}$ es ist. Damit folgt die Aussage aus der Injektivität von $\rho^K_{\alpha,\beta}$. □

3.2 Reduktion auf den Fall $K = \mathbb{F}_2((T))$ und $\beta = T^{-1}$

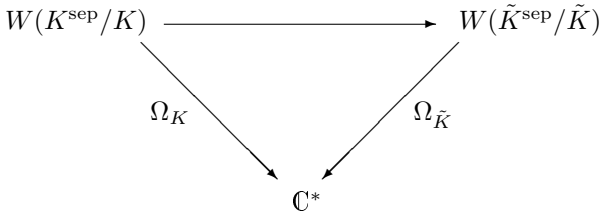
Im letzten Abschnitt haben wir Informationen über $\pi^K_{\alpha,\beta}$ gewonnen, indem wir die Einschränkung auf $W(K^{\mathrm{sep}}/L)$ studiert haben. In diesem Abschnitt wollen wir den umgekehrten Weg gehen: Wir verkleinern den Grundkörper K. Dazu müssen wir uns auf den Fall $\alpha = 0$ beschränken. Wir verweisen darauf, daß die Beschränkung auf den Fall $\alpha = 0$ unproblematisch ist, da wir mittels 1.11.2 zufriedenstellend beschreiben können, wie $\pi^K_{\alpha,\beta}$ von α abhängt. Wir definieren

$$\tilde{K} := \mathbb{F}_2((\beta^{-1})).$$

Dies ist der kleinste lokale Teilkörper von K, über dem sich die Kurve $\mathcal{E}_{0,\beta}$ definieren läßt. Außerdem betrachten wir die injektive Einbettung

$$W(K^{\mathrm{sep}}/K) \longrightarrow W(\tilde{K}^{\mathrm{sep}}/\tilde{K}), \quad \sigma \longmapsto \sigma|_{\tilde{K}^{\mathrm{sep}}}.$$

Lemma 3.2.1 *Das folgende Diagramm ist kommutativ:*

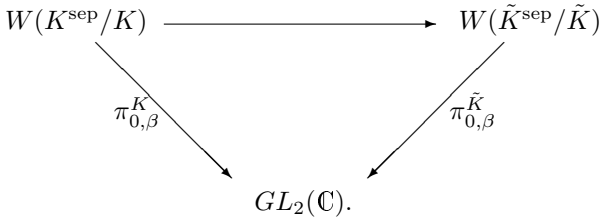


Beweis: Zunächst bemerken wir, daß die Vorschrift $\sigma \longmapsto \sigma|_{\tilde{K}^{\mathrm{sep}}}$ die Trägheitsgruppe $G_0(K^{\mathrm{sep}}/K)$ auf Trägheitsgruppe $G_0(K^{\mathrm{sep}}/\tilde{K})$ abbildet. Des weiteren sind Ω_K und $\Omega_{\tilde{K}}$ unverzweigt. Schließlich gilt für ein Frobeniuselement Φ_K von $W(K^{\mathrm{sep}}/K)$ die Identität

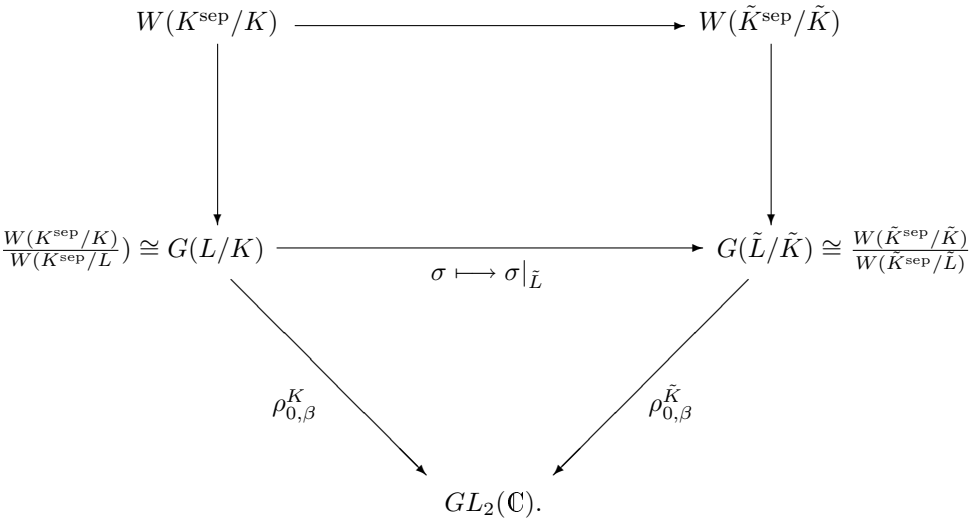
$$\Omega_{\tilde{K}}(\Phi_K|_{\tilde{K}^{\mathrm{sep}}}) = \Omega_{\tilde{K}}(\Phi_{\tilde{K}}^f) = (2^f)^{-\frac{1}{2}+i\frac{\pi}{2\ln(2)}} = \Omega_K(\Phi_K).$$

□

Wir können nun alle Punkte von $\mathcal{E}_{0,\beta}$ über $\tilde{K}$ auch als Punkte von $\mathcal{E}_{0,\beta}$ über K auffassen. Entsprechend lassen sich auch die Tate-Moduln identifizieren. Damit erhalten wir das kommutative Diagramm



Dieses Diagramm können wir mit dem Diagramm aus 3.2.1 „tensorieren“. Weiter definieren wir $\tilde{L} := \tilde{K}(\varphi, E, F_0)$. Dann bildet die Vorschrift $\sigma \longmapsto \sigma|_{\tilde{K}^{\mathrm{sep}}}$ die Weilgruppe $W(K^{\mathrm{sep}}/L)$ auf die Weilgruppe $W(\tilde{K}^{\mathrm{sep}}/\tilde{L})$ ab. Damit erhalten wir das kommutative Diagramm



Somit können wir das Ergebnis diese Abschnittes folgendermaßen formulieren:

Satz 3.2.2 *Für alle $\sigma \in G(L/K)$ gilt*

$$\mathrm{Tr}(\rho^K_{0,\beta}(\sigma)) = \mathrm{Tr}(\rho^{\tilde{K}}_{0,\beta}(\sigma|_{\tilde{L}})).$$

Dies bedeutet, daß wir nur noch die Darstellung $\rho^K_{0,T^{-1}}$ im Fall $K = \mathbb{F}_2((T))$ zu beschreiben brauchen, um die Darstellung $\rho^K_{\alpha,\beta}$ im allgemeinen Fall zu charakterisieren.

3.3 Der Spezialfall $K = \mathbb{F}_2((T))$ und $\beta = T^{-1}$

In diesem Abschnitt nehmen wir an, daß $K = \mathbb{F}_2((T))$ und $\beta = T^{-1}$ ist. Zunächst bestimmen wir den Verzweigungsgrad und den Trägheitsgrad von L/K.

Lemma 3.3.1 *Es gilt* $\mathrm{f}(L/K) = 2$ *und* $\mathrm{e}(L/K) = 24$.

Beweis: Zunächst erinnern wir daran, daß L/K höchstens den Grad 48 haben kann. Also brauchen wir lediglich $\mathrm{f}(L/K) \geq 2$ und $\mathrm{e}(L/K) \geq 24$ zu zeigen. Wegen $\varphi \notin K = \mathbb{F}_2((T))$ und $\varphi + \varphi^2 = 1$ erhält man $\mathrm{f}(L/K) \geq 2$. Weiter gilt

$$T^{-1} = \beta = (E + E^4)^3 = E^3 + E^6 + E^9 + E^{12}.$$

Hieraus folgt $\nu_K(E) = -\frac{1}{12}$. Ferner ist

$$F_0 + F_0^2 = (D + 1)E = E^3 + E^2 + E,$$

woraus sich $\nu_K(F_0) = -\frac{1}{24}$ ergibt. Damit erhält man $\mathrm{e}(L/K) \geq 24$. □

Wegen $\#GL_2(\mathbb{F}_3) = 48$ erhalten wir das nachfolgende Korollar.

Korollar 3.3.2 *Es gilt* $G(L/K) \cong GL_2(\mathbb{F}_3)$.

Für die folgenden Betrachtungen identifizieren wir $G(L/K)$ mit $GL_2(\mathbb{F}_3)$ gemäß der Tabelle von 2.3.3. Somit fassen wir $\rho^K_{0,T^{-1}}$ als irreduzible zweidimensionale Darstellung von $GL_2(\mathbb{F}_3)$ auf, deren Isomorphieklasse wir nun bestimmen werden. Dabei greifen auf die Ergebnisse von [17] zurück, wo die Isomorphieklassen irreduzibler Darstellungen von $GL_2(F)$ für alle endlichen Körper F klassifiziert sind. Nach der Tabelle auf Seite 70, loc. cit. sind alle zweidimensionalen irreduziblen Darstellungen von $GL_2(\mathbb{F}_3)$ cuspidal. Die cuspidalen Darstellungen ρ_μ von $GL_2(\mathbb{F}_3)$ sind parametrisiert durch die regulären Charaktere μ von $\mathbb{F}_9^*$. Einen Charakter $\mu : \mathbb{F}_9^* \longrightarrow \mathbb{C}^*$ nennen wir regulär, wenn er von seinem konjugierten Charakter $\bar{\mu}$ verschieden ist. Hierbei soll $\bar{\mu} : \mathbb{F}_9^* \longrightarrow \mathbb{C}^*$ durch die Vorschrift $x \longmapsto \mu(\bar{x})$ definiert sein. Mit $\bar{x} \in \mathbb{F}_9^*$ ist das zu x über $\mathbb{F}_3^*$ konjugierte Element gemeint. Für zwei reguläre Charaktere μ, μ' von $\mathbb{F}_9^*$ gilt genau dann $\rho_\mu = \rho_{\mu'}$, wenn $\bar{\mu} = \mu'$ oder $\mu = \mu'$ ist. Für die genaue Konstruktion von ρ_μ verweisen wir auf [17, Chap. 2, §10-14].

Zunächst wollen wir uns einen Überblick über die regulären Charaktere von $\mathbb{F}_9^*$ verschaffen. Dazu wählen wir einen Erzeuger $\zeta := 1 + \sqrt{-1}$ von $\mathbb{F}_9^*$ und die primitive 8-te Einheitswurzel $\xi := e^{\frac{2\pi}{8}i}$. Für alle $k = 0, 1, \ldots, 7$ gibt es nun einen eindeutig bestimmten Charakter $\mu_k : \mathbb{F}_9^* \longrightarrow \mathbb{C}^*$ mit $\mu_k(\zeta) = \xi^k$. Wegen $\zeta^3 = \bar{\zeta}$ gilt $\bar{\mu}_k = \mu_k^3$ für alle $k = 0, 1, \ldots 7$. Daraus folgt $\bar{\mu}_1 = \mu_3$, $\bar{\mu}_2 = \mu_6$ und $\bar{\mu}_5 = \mu_7$, während μ_0 und μ_4 nicht regulär sind. Damit kommt als Isomorphieklasse von $\rho^K_{0,T^{-1}}$ nur noch ρ_{μ_1}, ρ_{μ_2} oder ρ_{μ_5} in Frage.

Satz 3.3.3 *Es gilt* $\mathrm{Tr}(\rho^K_{0,T^{-1}}) = \mathrm{Tr}(\rho_{\mu_5})$.

Beweis: Wäre $\mathrm{Tr}(\rho^K_{0,T^{-1}}) = \mathrm{Tr}(\rho_{\mu_2})$, so müßte nach [17, S. 70]

$$\mathrm{Tr}(\rho^K_{0,T^{-1}}) \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = 2\mu_2(-1) = 2$$

sein. Dies steht aber im Widerspruch zur Injektivität von $\rho^K_{0,T^{-1}}$. Also gilt

$$\mathrm{Tr}(\rho^K_{0,T^{-1}}) \neq \mathrm{Tr}(\rho_{\mu_2}).$$

Wir nehmen nun $\mathrm{Tr}(\rho^K_{0,T^{-1}}) = \mathrm{Tr}(\rho_{\mu_1})$ an und zeigen, daß diese Annahme im Widerspruch zu unseren bisherigen Ergebnissen steht. Sei dazu $\sigma \in G(L/K)$ mit $\sigma(\varphi) = \varphi+1$, $\sigma(E) = (\varphi+1)E+1$ und $\sigma(F_0) = F_0 + E + \varphi$. Dann entspricht σ der Matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -\zeta\bar{\zeta} \\ 1 & \zeta+\bar{\zeta} \end{pmatrix}.$$

Weiter betrachten wir eine Fortsetzung $\tilde{\sigma} \in W(K^{\mathrm{sep}}/K)$ von σ. Wir wählen nun ein $j \in \mathbb{Z}$ und ein $\sigma_0 \in G_0(L/K)$, so daß $\tilde{\sigma} = \Phi_K^j \sigma_0$ bezüglich eines fest gewählten Frobeniuselements $\Phi_K \in W(K^{\mathrm{sep}}/K)$ gilt. Damit erhält man

$$\varphi^2 = \sigma(\varphi) = \Phi_K^j(\sigma_0(\varphi)) = \Phi_K^j(\varphi) = \varphi^{2j}.$$

Daraus folgt, daß j ungerade ist. Weiter setzen wir $\sigma^* := \Phi_L^{\frac{1-j}{2}} \tilde{\sigma}$ für ein fest gewähltes Frobeniuselement $\Phi_L \in W(K^{\mathrm{sep}}/K)$. Dann gilt $\sigma^*|_L = \sigma$. Wegen $\mathrm{f}(L/K) = 2$ erhält man

$$\omega_K(\sigma^*) = \omega_K(\Phi_L^{\frac{1-j}{2}} \Phi_K^j) = \omega_K(\Phi_K) = 2.$$

Nach [17, S. 70] folgt

$$\begin{aligned}
\mathrm{Tr}(\pi^K_{0,T^{-1}}(\sigma^*)) &= \mathrm{Tr}\big(\big(\Omega_K^{-1}(\sigma^*)\big)\rho^K_{0,T^{-1}}(\sigma)\big) \\
&= \mathrm{Tr}(2^{\frac{1}{2}-i\frac{\pi}{2\ln(2)}} \rho_{\mu_1} \begin{pmatrix} 0 & -\zeta\bar{\zeta} \\ 1 & \zeta+\bar{\zeta} \end{pmatrix}). \\
&= -i\sqrt{2}(-\mu_1(\zeta) - \mu_1(\bar{\zeta})) \\
&= -i\sqrt{2}(-\xi - \xi^3) \\
&= -i\sqrt{2}(-(\cos(\frac{\pi}{4}) + i\sin(\frac{\pi}{4})) - (\cos(\frac{3\pi}{4}) + i\sin(\frac{3\pi}{4}))) \\
&= -2.
\end{aligned}$$

Wir zeigen nun, daß dieses Ergebnis im Widerspruch zur Operation von σ^* auf den 3-Torsionspunkten steht. Dazu fassen wir $\mathrm{Tr}(\pi^K_{0,T^{-1}}(\sigma^*))$ als Element von $\mathbb{Z}_3$ auf. Die Reduktion modulo $3\mathbb{Z}_3$ liefert

$$\begin{aligned}
\mathrm{Tr}(\pi^K_{0,T^{-1}}(\sigma^*)) &\equiv \mathrm{Tr}(\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}) \mod 3\mathbb{Z}_3 \\
&\equiv 2 \mod 3\mathbb{Z}_3.
\end{aligned}$$

Folglich muß die Annahme $\mathrm{Tr}(\pi^K_{0,T^{-1}}) = \mathrm{Tr}(\rho_{\mu_1})$ falsch gewesen sein. Damit folgt die Aussage des Satzes. □

Zum Ende dieses Abschnittes wollen wir noch darauf hinweisen, daß die Spurabbildungen $\mathrm{Tr}(\rho_{\mu_1})$ und $\mathrm{Tr}(\rho_{\mu_5})$ bis auf komplexe Konjugation identisch sind. Wenn wir ein $\rho \in \{\rho_{\mu_1}, \rho_{\mu_5}\}$ haben, müssen wir, um festzustellen, ob $\rho = \rho_{\mu_1}$ oder $\rho = \rho_{\mu_5}$ gilt, erst verbindlich den Erzeuger i von $\mathbb{C}$ festlegen. Für die Wahl von i gibt es ja bekanntlich zwei Möglichkeiten. Im zurückliegenden Beweis konnten wir die Identität $\rho^K_{0,T^{-1}} = \rho_{\mu_5}$ nur deshalb zeigen, weil Ω_K und damit auch $\rho^K_{0,T^{-1}}$ ebenfalls von der Wahl des Erzeugers i abhängt.

3.4 Folgerungen

In diesem Abschnitt wollen wir $\rho^K_{\alpha,\beta}$ im allgemeinen Fall $K = \mathbb{F}_{2^f}((T))$ sowie $\alpha \in K$ beliebig und $\nu_K(\beta) < 0$ betrachten. Dazu setzen wir $L_0 := K(\varphi, E, F_0)$. Gemäß der Tabelle von 2.3.3 identifizieren wir sowohl $G(L/K)$ als auch $G(L_0/K)$ mit einer Untergruppe von $GL_2(\mathbb{F}_3)$. Weiter sei K_α der Zerfällungskörper des Polynoms $X^2 + X + \alpha$ über K und $\chi_\alpha : W(K^{\text{sep}}/K) \longrightarrow \mathbb{C}^*$ der eindeutig bestimmte Charakter mit $\text{Kern}(\chi_\alpha) = W(K^{\text{sep}}/K_\alpha)$. Weil χ_α nur die Werte 1 und -1 annehmen kann und sich $\mathbb{F}_3^*$ mit der Untergruppe $\{1, -1\}$ von $\mathbb{C}^*$ identifizieren läßt, können wir χ_α auch als Homomorphismus von $W(K^{\text{sep}}/K)$ nach $\mathbb{F}_3^*$ auffassen.

Lemma 3.4.1 *Für alle $\sigma \in W(K^{\text{sep}}/K)$ gilt*

$$\sigma|_L = \chi_\alpha(\sigma)\sigma|_{L_0}.$$

Beweis: Wir setzen $r := F_\alpha + F_0$. Dann ist $r + r^2 = \alpha$. Für alle $\sigma \in W(K^{\text{sep}}/K)$ gelten die Bedingungen $\sigma|_L(\varphi) = \sigma|_{L_0}(\varphi)$ und $\sigma|_L(E) = \sigma|_{L_0}(E)$. Außerdem gilt

$$\sigma|_L(F_\alpha) = \sigma|_{L_0}(F_0) + \begin{cases} 0, & \text{falls } \chi_\alpha(\sigma) = 1 \\ 1, & \text{falls } \chi_\alpha(\sigma) = -1. \end{cases}$$

Dies reicht aus, um die gewünschte Aussage anhand der Tabelle von 2.3.3 zu verifizieren. □

Satz 3.4.2 *Es gilt*

$$\rho^K_{\alpha,\beta} \cong \rho_{\mu_5}|_{G(L/K)}.$$

Beweis: Unmittelbar aus 3.3.3 und 3.2.2 folgt $\rho^K_{0,\beta} \cong \rho_{\mu_5}|_{G(L_0/K)}$. Sei nun $\sigma \in G(L/K)$ und $\tilde{\sigma} \in W(K^{\text{sep}}/K)$ eine Fortsetzung von σ. Dann gilt

$$\begin{aligned}
\text{Tr}(\rho^K_{\alpha,\beta}(\sigma)) &= \text{Tr}(\Omega_K^{-1}(\tilde{\sigma})\pi^K_{\alpha,\beta}(\tilde{\sigma})) \\
&= \text{Tr}(\Omega_K^{-1}(\tilde{\sigma})\chi_\alpha(\tilde{\sigma})\pi^K_{0,\beta}(\tilde{\sigma})) \\
&= \text{Tr}(\chi_\alpha(\tilde{\sigma})\rho^K_{0,\beta}(\tilde{\sigma}|_{L_0})) \\
&= \text{Tr}(\chi_\alpha(\tilde{\sigma})\rho_{\mu_5}(\tilde{\sigma}|_{L_0})) \\
&= \text{Tr}(\rho_{\mu_5}(\chi_\alpha(\tilde{\sigma})(\tilde{\sigma}|_{L_0}))) \\
&= \text{Tr}(\rho_{\mu_5}(\sigma)).
\end{aligned}$$

Daraus folgt $\rho^K_{\alpha,\beta} \cong \rho_{\mu_5}|_{G(L/K)}$. □

Damit sind wir nun in der Lage, die Spurabbildung $\text{Tr}(\rho^K_{\alpha,\beta})$ explizit zu beschreiben.

Korollar 3.4.3 *Sei $\sigma \in G(L/K)$. Dann erhält man $\text{Tr}(\rho^K_{\alpha,\beta}(\sigma))$ in Abhängigkeit von $\sigma(\varphi)$, $\sigma(E)$ und $\sigma(F_\alpha)$ gemäß der folgenden Tabelle:*

$\sigma(\varphi)$	$\sigma(E)$	$\sigma(F_\alpha)$	$\text{Tr}(\rho^K_{\alpha,\beta}(\sigma))$
φ	E	F_α	2
φ	E	$F_\alpha + 1$	-2
φ	$E + 1$	$F_\alpha + E + \varphi$	0
φ	$E + 1$	$F_\alpha + E + \varphi + 1$	0
φ	$E + \varphi$	$F_\alpha + (\varphi + 1)E$	0
φ	$E + \varphi$	$F_\alpha + (\varphi + 1)E + 1$	0
φ	$E + \varphi + 1$	$F_\alpha + \varphi E$	0
φ	$E + \varphi + 1$	$F_\alpha + \varphi E + 1$	0
φ	φE	$F_\alpha + (\varphi + 1)E$	-1

φ	φE	$F_\alpha + (\varphi+1)E + 1$	1
φ	$\varphi E + 1$	$F_\alpha + E + \varphi$	-1
φ	$\varphi E + 1$	$F_\alpha + E + \varphi + 1$	1
φ	$\varphi E + \varphi$	$F_\alpha + \varphi E$	1
φ	$\varphi E + \varphi$	$F_\alpha + \varphi E + 1$	-1
φ	$\varphi E + \varphi + 1$	F_α	-1
φ	$\varphi E + \varphi + 1$	$F_\alpha + 1$	1
φ	$(\varphi+1)E$	$F_\alpha + \varphi E$	-1
φ	$(\varphi+1)E$	$F_\alpha + \varphi E + 1$	1
φ	$(\varphi+1)E + 1$	$F_\alpha + E + \varphi$	1
φ	$(\varphi+1)E + 1$	$F_\alpha + E + \varphi + 1$	-1
φ	$(\varphi+1)E + \varphi$	F_α	-1
φ	$(\varphi+1)E + \varphi$	$F_\alpha + 1$	1
φ	$(\varphi+1)E + \varphi + 1$	$F_\alpha + (\varphi+1)E$	1
φ	$(\varphi+1)E + \varphi + 1$	$F_\alpha + (\varphi+1)E + 1$	-1
$\varphi+1$	E	F_α	0
$\varphi+1$	E	$F_\alpha + 1$	0
$\varphi+1$	$E + 1$	$F_\alpha + E + \varphi$	0
$\varphi+1$	$E + 1$	$F_\alpha + E + \varphi + 1$	0
$\varphi+1$	$E + \varphi$	$F_\alpha + (\varphi+1)E$	$\sqrt{2}i$
$\varphi+1$	$E + \varphi$	$F_\alpha + (\varphi+1)E + 1$	$-\sqrt{2}i$
$\varphi+1$	$E + \varphi + 1$	$F_\alpha + \varphi E$	$\sqrt{2}i$
$\varphi+1$	$E + \varphi + 1$	$F_\alpha + \varphi E + 1$	$-\sqrt{2}i$
$\varphi+1$	φE	$F_\alpha + (\varphi+1)E$	0
$\varphi+1$	φE	$F_\alpha + (\varphi+1)E + 1$	0
$\varphi+1$	$\varphi E + 1$	$F_\alpha + E + \varphi$	$-\sqrt{2}i$
$\varphi+1$	$\varphi E + 1$	$F_\alpha + E + \varphi + 1$	$\sqrt{2}i$
$\varphi+1$	$\varphi E + \varphi$	$F_\alpha + \varphi E$	$-\sqrt{2}i$
$\varphi+1$	$\varphi E + \varphi$	$F_\alpha + \varphi E + 1$	$\sqrt{2}i$
$\varphi+1$	$\varphi E + \varphi + 1$	F_α	0
$\varphi+1$	$\varphi E + \varphi + 1$	$F_\alpha + 1$	0
$\varphi+1$	$(\varphi+1)E$	$F_\alpha + \varphi E$	0
$\varphi+1$	$(\varphi+1)E$	$F_\alpha + \varphi E + 1$	0
$\varphi+1$	$(\varphi+1)E + 1$	$F_\alpha + E + \varphi$	$\sqrt{2}i$
$\varphi+1$	$(\varphi+1)E + 1$	$F_\alpha + E + \varphi + 1$	$-\sqrt{2}i$
$\varphi+1$	$(\varphi+1)E + \varphi$	F_α	0
$\varphi+1$	$(\varphi+1)E + \varphi$	$F_\alpha + 1$	0
$\varphi+1$	$(\varphi+1)E + \varphi + 1$	$F_\alpha + (\varphi+1)E$	$-\sqrt{2}i$
$\varphi+1$	$(\varphi+1)E + \varphi + 1$	$F_\alpha + (\varphi+1)E + 1$	$\sqrt{2}i$

Beweis: Diese Aussage folgt aus 3.4.2 in Verbindung mit der Beschreibung von $\mathrm{Tr}(\rho_{\mu_5})$ im Anhang. □

Korollar 3.4.4 *Der Körper $K(\varphi, E)$ ist der projektive Kernkörper von $\pi^K_{\alpha,\beta}$.*

Beweis: Sei P der projektive Kernkörper von $\pi^K_{\alpha,\beta}$. Zunächst ist klar, daß $P \subset L$ gilt. Für alle $\sigma \in G(L/K)$ ist $\rho^K_{\alpha,\beta}(\sigma)$ genau dann ein Skalar, wenn $\mathrm{Tr}(\rho^K_{\alpha,\beta}(\sigma))$ den Betrag 2 hat. Dies wiederum ist genau dann der Fall, wenn $\sigma(\varphi) = \varphi$ und $\sigma(E) = E$, d.h. σ trivial auf $K(\varphi, E)$ ist. Also gilt $P = K(\varphi, E)$. □

Kapitel 4

Berechnung des Verzweigungsverhaltens

Wir erinnern zunächst an unsere Voraussetzungen, daß $K = \mathbb{F}_{2^f}((T))$ und $\nu_K(\beta) < 0$ ist. In diesem Kapitel werden wir uns für alle $i \in \mathbb{N}_0$ der Bestimmung der i-ten Verzweigungsgruppen $G_i(L/K)$ zuwenden. Für eine genaue Definition von $G_i(L/K)$ verweisen wir auf [21, Chap. IV, §1]. Die Bestimmung aller $G_i(L/K)$ ist äquivalent zur Berechnung der Zahlen

$$\mathrm{i}_{L/K}(\sigma) = \min\{i \in \mathbb{N}_0 \mid \sigma \notin G_i(L/K)\}$$

für alle $\sigma \in G(L/K) \setminus \{\mathrm{id}_L\}$. Im ersten Abschnitt dieses Kapitels werden wir Formeln herleiten, die die Berechnung von $\mathrm{i}_{L/K}(\sigma)$ aus den Differentenexponenten gewisser Zwischenerweiterungen von L/K gestatten. Im zweiten Abschnitt geben wir eine Formel für den Führer von $\pi^K_{\alpha,\beta}$ an. Im dritten Abschnitt werden wir uns dann allgemein mit der Berechnung von Differentenexponenten quadratischer Erweiterungen befassen, um dann in den letzten drei Abschnitten mit diesem Wissen die Differentenexponenten, die im ersten Abschnitt auftreten, explizit zu berechnen.

4.1 Charakterisierung der höheren Verzweigungsgruppen

Zunächst müssen wir ein paar Vereinbarungen treffen, die für den gesamten Rest dieser Arbeit gültig sein sollen. Für eine beliebige endliche Erweiterung K'/K bezeichnen wir mit $\nu_{K'}$ die eindeutig bestimmte Bewertung auf K', die jeder Uniformisierenden von K' die Zahl 1 zuordnet. Diese Bewertung besitzt eine eindeutig bestimmte Fortsetzung nach K^{sep}, die wir ebenfalls mit $\nu_{K'}$ bezeichnen. Mit $\mathrm{d}(K'/K)$ bezeichnen wir den Differentenexponenten von K'/K.

Lemma 4.1.1 *Sei $\sigma \in G(L/K)$ mit $\sigma(\varphi) = \varphi + 1$. Dann gilt $\mathrm{i}_{L/K}(\sigma) = 0$.*

Beweis: Wegen $\varphi^2 + \varphi + 1 = 0$ ist $K(\varphi)/K$ unverzweigt und folglich in der maximalen unverzweigten Zwischenerweiterung K_0 von L/K enthalten. Wegen $\sigma(\varphi) \neq \varphi$ folgt $\sigma \notin G_0(L/K) = G(L/K_0)$ und damit $\mathrm{i}_{L/K}(\sigma) = 0$. □

Lemma 4.1.2 *Sei $\sigma \in G(L/K)$ mit $\sigma(\varphi) = \varphi$ und $\sigma(E) \notin \{E, E+1, E+\varphi, E+\varphi+1\}$. Dann gilt $\mathrm{i}_{L/K}(\sigma) \leq 1$.*

Beweis: Zunächst zeigen wir $\sigma(\gamma) \neq \gamma$. Anderenfalls wäre

$$\gamma = \sigma(\gamma) = \sigma(E)^4 + \sigma(E).$$

Damit müßte $\sigma(E)$ eine Nullstelle des Polynoms $f := X^4 + X + \gamma$ sein. Weil aber f die Nullstellen $E, E+1, E+\varphi$ und $E+\varphi+1$ hat, kann dies nicht sein. Also gilt $\sigma(\gamma) \neq \gamma$.

Weil $K(\varphi,\gamma)/K(\varphi)$ den Grad 1 oder 3 hat, muß diese Erweiterung zahm sein. Wegen der Unverzweigtheit von $K(\varphi)/K$ folgt, daß auch $K(\varphi,\gamma)/K$ zahm ist und somit in der maximalen zahmen Zwischenerweiterung von L/K liegt. Wegen $\sigma(\gamma) \neq \gamma$ erhält man $\sigma \notin G_1(L/K)$ und damit $\mathrm{i}_{L/K}(\sigma) \leq 1$. □

Damit haben wir herausgefunden, welche Elemente von $G(L/K)$ auf keinen Fall der wilden Verzweigungsgruppe $G_1(L/K)$ angehören. Mit diesem Wissen können wir eine Aussage über ihren Isomorphietyp machen.

Satz 4.1.3 *(i) Es gilt* $\#G_1(L/K) = 1, 2, 4$ *oder* 8.

(ii) Im Fall $\#G_1(L/K) = 8$ *ist* $G_1(L/K)$ *isomorph zu* $[SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$.

(iii) Im Fall $\#G_1(L/K) = 4$ *gilt* $G_1(L/K) \cong \mathbb{Z}/4\mathbb{Z}$.

Beweis: Zunächst verweisen wir auf die explizite Berechnung von $[SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$ im Anhang. Wenn wir $G_1(L/K)$ gemäß der Tabelle von 2.3.3 mit einer Untergruppe von $GL_2(\mathbb{F}_3)$ identifizieren, so können wir mit 4.1.2 leicht überprüfen, daß $G_1(L/K)$ einer Untergruppe von $[SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$ entspricht. Hieraus ergibt sich (i) und (ii). Die Aussage (iii) folgt aus der Tatsache, daß jede echte Untergruppe von $[SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$ zyklisch ist, was ebenfalls im Anhang gezeigt wird. □

Wir werden nun $\mathrm{i}_{L/K}(\sigma)$ für alle $\sigma \in G_1(L/K)$ bestimmen.

Satz 4.1.4 *(i) Falls es ein* $\sigma \in G(L/K)$ *gibt mit* $\sigma(\varphi) = \varphi$, $\sigma(E) = E$ *und* $\sigma(F_\alpha) = F_\alpha + 1$, *so gilt* $\mathrm{i}_{L/K}(\sigma) = \mathrm{d}(L/K(\varphi, E))$.

(ii) Falls $\mathrm{d}(L/K(\varphi, E)) > 0$ *ist, gibt es ein* $\sigma \in G_1(L/K)$ *mit* $\sigma(\varphi) = \varphi$, $\sigma(E) = E$ *und* $\sigma(F_\alpha) = F_\alpha + 1$.

Beweis: Zu (i): Wegen $[L : K(\varphi, E)] \leq 2$ ist σ das eindeutig bestimmte nichttriviale Element von $G(L/K(\varphi, E))$. Nach [21, Chap. IV, Prop. 2 und 4] gilt

$$\mathrm{i}_{L/K}(\sigma) = \mathrm{i}_{L/K(\varphi,E)}(\sigma) = \mathrm{d}(L/K(\varphi, E)).$$

Zu (ii): Wegen $\mathrm{d}(L/K(\varphi, E)) > 0$ muß $L/K(\varphi, E)$ wild verzweigt vom Grad 2 sein. Folglich enthält $G_1(L/K(\varphi, E)) \subset G_1(L/K)$ einen nichttrivialen Automorphismus σ. Für diesen Automorphismus muß $\sigma(\varphi) = \varphi$, $\sigma(E) = E$ und $\sigma(F_\alpha) = F_\alpha + 1$ gelten. □

Das folgende Lemma werden wir ohne explizite Nennung benutzen.

Lemma 4.1.5 *Sei* M/K *eine separable Erweiterung und* K'/K *eine unverzweigte Erweiterung. Dann gilt* $\mathrm{d}(MK'/K') = \mathrm{d}(M/K)$.

Beweis: Wegen der Transitivität der Differente gilt

$$\mathrm{d}(MK'/K) = \mathrm{d}(MK'/K') + \mathrm{e}(MK'/K')\mathrm{d}(K'/K) = \mathrm{d}(MK'/K')$$

und

$$\mathrm{d}(MK'/K) = \mathrm{d}(MK'/M) + \mathrm{e}(MK'/M)\mathrm{d}(M/K) = \mathrm{d}(M/K).$$

Daraus folgt $\mathrm{d}(MK'/K') = \mathrm{d}(M/K)$. □

Satz 4.1.6 *(i) Falls es ein* $\sigma \in G(L/K)$ *gibt mit* $\sigma(\varphi) = \varphi$ *und* $\sigma(E) = E + 1$, *so gilt*

$$\mathrm{i}_{L/K}(\sigma) = \mathrm{d}(K(E)/K(D)).$$

(ii) Falls $\mathrm{d}(K(E)/K(D)) > 0$ *ist, so gibt es ein* $\sigma \in G_1(L/K)$ *mit* $\sigma(\varphi) = \varphi$ *und* $\sigma(E) = E + 1$.

Beweis: Zu (i): Wegen $\sigma(D) = (E+1)^2 + E + 1 = E^2 + E = D$ muß $\sigma \in G(L/K(\varphi, D))$ sein. Nach der Tabelle von 2.3.3 entspricht die Operation von σ auf $\mathcal{E}_{\alpha,\beta}[3]$ bzgl. der Basis (P_{11}, P_{21}) entweder der Matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ oder } \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Weil beide Matrizen die Ordnung 4 haben, folgt $\mathrm{ord}(\sigma) = 4$. Wegen $[L : K(\varphi, D)] \leq 4$ erhält man $G(L/K(\varphi, D)) = \{\sigma, \sigma^2, \sigma^3, \mathrm{id}_L\}$. Hierbei muß $\sigma^2 \in G(L/K(\varphi, E))$ sein und die Identität $\mathrm{i}_{L/K(\varphi,D)}(\sigma) = \mathrm{i}_{L/K(\varphi,D)}(\sigma^3)$ gelten. Die Anwendung von [21, Chap. IV, Prop. 2 und 4] liefert das Ergebnis

$$\begin{aligned} \mathrm{d}(L/K(\varphi, D)) &= \mathrm{i}_{L/K(\varphi,D)}(\sigma) + \mathrm{i}_{L/K(\varphi,D)}(\sigma^2) + \mathrm{i}_{L/K(\varphi,D)}(\sigma^3) \\ &= 2\mathrm{i}_{L/K(\varphi,D)}(\sigma) + \mathrm{i}_{L/K(\varphi,D)}(\sigma^2) \\ &= 2\mathrm{i}_{L/K}(\sigma) + \mathrm{i}_{L/K}(\sigma^2). \end{aligned}$$

Durch Auflösen nach $\mathrm{i}_{L/K}(\sigma)$ und Anwendung von 4.1.4 erhalten wir

$$\begin{aligned} \mathrm{i}_{L/K}(\sigma) &= \frac{1}{2}\left(\mathrm{d}(L/K(\varphi, D)) - \mathrm{i}_{L/K}(\sigma^2)\right) \\ &= \frac{1}{2}\left(\mathrm{d}(L/K(\varphi, D)) - \mathrm{d}(L/K(\varphi, E))\right). \end{aligned}$$

Wegen der Transitivität der Differente gilt

$$\mathrm{d}(L/K(\varphi, D)) = \mathrm{d}(L/K(\varphi, E)) + \mathrm{e}(L/K(\varphi, E))\mathrm{d}(K(\varphi, E)/K(\varphi, D)).$$

Damit ergibt sich

$$\begin{aligned} \mathrm{i}_{L/K}(\sigma) &= \frac{1}{2}\mathrm{e}(L/K(\varphi, E))\mathrm{d}(K(\varphi, E)/K(\varphi, D)). \\ &= \frac{1}{2}\mathrm{e}(L/K(\varphi, E))\mathrm{d}(K(E)/K(D)). \end{aligned}$$

Wenn $L/K(\varphi, E)$ verzweigt ist, erhält man die gewünschte Aussage. Im Fall, daß $L/K(\varphi, E)$ unverzweigt ist, muß die maximale unverzweigte Zwischenerweiterung von $L/K(\varphi, D)$ mindestens den Grad 2 haben. Damit muß diese den Körper $K(\varphi, E)$ enthalten. Daraus folgt

$$\mathrm{d}(K(E)/K(D)) = \mathrm{d}(K(\varphi, E)/K(\varphi, D)) = 0,$$

woraus sich ebenfalls die gewünschte Aussage ergibt.

Zu (ii): Wenn $\mathrm{d}(K(E)/K(D)) = \mathrm{d}(K(\varphi, E)/K(\varphi, D)) > 0$ ist, muß $K(\varphi, E)/K(\varphi, D)$ den Grad 2 haben. Sei $\tilde{\sigma}$ das eindeutig bestimmte nichttriviale Element von $G(K(\varphi, E)/K(\varphi, D))$. Dann gilt $\tilde{\sigma}(\varphi) = \varphi$ und $\tilde{\sigma}(E) = E + 1$. Sei nun $\sigma \in G(L/K(\varphi, D))$ eine Fortsetzung von $\tilde{\sigma}$. Wir zeigen, daß $L/K(\varphi, D)$ vollständig wild verzweigt ist. Dazu bezeichnen wir die maximale zahm verzweigte Zwischenerweiterung von $L/K(\varphi, D)$ mit K'. Wegen der Wildverzweigtheit von $K(\varphi, E)/K(\varphi, D)$ folgt $[K'(\varphi, E) : K'(\varphi, D)] = 2$. Nach 2.4.1 muß auch $L/K'(\varphi, E)$ den Grad 2 haben. Daraus folgt $[L : K'] = 4$. Hieraus erhalten wir $\sigma \in G_1(L/K(\varphi, D)) \subset G_1(L/K)$. □

Bemerkung 4.1.7 *Wir verweisen darauf, daß beim Beweis von 4.1.6 kein Gebrauch von der Vereinbarung 2.4.4 gemacht wurde. Also gilt 4.1.6 auch dann, wenn man auf die Vereinbarung 2.4.4 verzichtet.*

Die folgenden Bezeichnungen brauchen wir, um geschlossene Formeln für $\mathrm{i}_{L/K}(\sigma)$ im Fall $\sigma(E) = E + \varphi$ bzw. $\sigma(E) = E + \varphi + 1$ angeben zu können. Sie sollen für den gesamten Rest dieser Arbeit in Kraft bleiben.

Bezeichnung 4.1.8 *Wir setzen* $D_\varphi := \varphi E + (\varphi E)^2$ *und* $D_{\varphi^2} := \varphi^2 E + \left(\varphi^2 E\right)^2$.

Lemma 4.1.9 *Es gilt* $D_\varphi + D_\varphi^2 = \varphi\gamma$ *und* $D_{\varphi^2} + D_{\varphi^2}^2 = \varphi^2\gamma$.

Beweis: Durch eine elementare Rechnung erhalten wir

$$D_\varphi + D_\varphi^2 = \varphi E + (\varphi E)^2 + (\varphi E + (\varphi E)^2)^2 = \varphi E + (\varphi E)^4 = \varphi(E + E^4) = \varphi\gamma.$$

Indem wir φ durch φ^2 ersetzen, verifizieren wir auch die Identität $D_{\varphi^2} + D_{\varphi^2}^2 = \varphi^2\gamma$.

Satz 4.1.10 *(i) Falls es ein* $\sigma \in G(L/K)$ *gibt mit* $\sigma(\varphi) = \varphi$ *und* $\sigma(E) = E + \varphi$, *so gilt*

$$\mathrm{i}_{L/K}(\sigma) = \mathrm{d}(K(E)/K(D_{\varphi^2})).$$

(ii) Falls $\mathrm{d}(K(E)/K(D_{\varphi^2})) > 0$ *ist, so gibt es ein* $\sigma \in G_1(L/K)$ *mit* $\sigma(\varphi) = \varphi$ *und* $\sigma(E) = E+\varphi$.

Beweis: Wir setzen $\tilde{F_\alpha} := F_\alpha + \varphi E$, $\tilde{E} := \varphi^2 E$ und $\tilde{\gamma} := \varphi^2\gamma$. Damit erhalten wir $\tilde{\gamma}^3 = \beta$ sowie $D_{\varphi^2} + D_{\varphi^2}^2 = \tilde{\gamma}$ und $\tilde{E} + \tilde{E}^2 = D_{\varphi^2}$. Außerdem gilt

$$\begin{aligned}
\tilde{F_\alpha} + \tilde{F_\alpha}^2 &= Fa + F_\alpha^2 + \varphi E + \varphi^2 E^2 \\
&= (D+1)E + \alpha + \varphi E + \varphi^2 E^2 \\
&= E^3 + E^2 + E + \varphi E + \varphi^2 E^2 + \alpha \\
&= (\varphi^2 E)^3 + (\varphi^2 E)^2 + \varphi^2 E + \alpha \\
&= (D_{\varphi^2} + 1)\tilde{E} + \alpha.
\end{aligned}$$

Für alle $\sigma \in G(L/K)$ mit $\sigma(\varphi) = \varphi$ ist die Bedingung $\sigma(E) = E + \varphi$ äquivalent zu

$$\sigma(\tilde{E}) = \varphi^2(E + \varphi) = \tilde{E} + 1.$$

Wir ersetzen nun $(\varphi, \gamma, D, E, F_\alpha)$ durch $(\varphi, \tilde{\gamma}, D_{\varphi^2}, \tilde{E}, \tilde{F_\alpha})$ und wenden 4.1.6 an. Nach 4.1.7 können hierbei keine Probleme auftreten. □

Satz 4.1.11 *(i) Falls es ein* $\sigma \in G(L/K)$ *gibt mit* $\sigma(\varphi) = \varphi$ *und* $\sigma(E) = E + \varphi + 1$, *so gilt*

$$\mathrm{i}_{L/K}(\sigma) = \mathrm{d}(K(E)/K(D_\varphi)).$$

(ii) Falls $\mathrm{d}(K(E)/K(D_\varphi)) > 0$ *ist, gibt ein* $\sigma \in G_1(L/K)$ *mit* $\sigma(\varphi) = \varphi$ *und* $\sigma(E) = E + \varphi + 1$.

Beweis: Wir ersetzen φ durch $\varphi^2 = \varphi + 1$ und wenden 4.1.10 an. □

Nun können wir den Isomorphietyp aller höheren Verzweigungsgruppen $G_i(L/K)$ bestimmen.

Satz 4.1.12 *Wir setzen*

$$r := \min\{\mathrm{d}(K(E)/K(D)), \mathrm{d}(K(E)/K(D_\varphi)), \mathrm{d}(K(E)/K(D_{\varphi^2}))\},$$

$$s := \max\{\mathrm{d}(K(E)/K(D)), \mathrm{d}(K(E)/K(D_\varphi)), \mathrm{d}(K(E)/K(D_{\varphi^2}))\}$$

und

$$t := \mathrm{d}(L/K(\varphi, E)).$$

Für alle $i \in \mathbb{N}$ *gilt dann*

$$G_i(L/K) \cong \begin{cases} [SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)], & \text{falls } i < r \\ \mathbb{Z}/4\mathbb{Z}, & \text{falls } r \le i < s \\ \mathbb{Z}/2\mathbb{Z}, & \text{falls } s \le i < t \\ \{1\}, & \text{falls } t \le i. \end{cases}$$

Beweis: Aus 4.1.3 folgt, daß $G_i(L/K)$ als Untergruppe von $G_1(L/K)$ nur die Isomorphietypen $[SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ oder $\{1\}$ haben kann.

Als erstes betrachten wir den Fall $i < r$. Nach 4.1.6 enthält $G_i(L/K)$ einen Automorphismus σ mit $\sigma(\varphi) = \varphi$ und $\sigma(E) = E + 1$. Indem wir $G(L/K)$ gemäß 2.3.3 mit einer Untergruppe von $GL_2(\mathbb{F}_3)$ identifizieren, überzeugen wir uns leicht davon, daß σ die Ordnung 4 hat. Hiebei ist $\sigma^2(E) = E$ und $\sigma^3(E) = E+1$. Außerdem gibt es nach 4.1.10 ein $\sigma' \in G_i(L/K)$ mit $\sigma'(E) = E+\varphi$. Damit hat $G_i(L/K)$ mehr als 4 Elemente und ist isomorph zu $[SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$.

Im Fall $r \leq i < s$ erhält man durch Anwendung von 4.1.6 oder 4.1.10 oder 4.1.11, daß es ein $\sigma \in G_i(L/K)$ gibt mit $\sigma(E) = E + 1$ oder $\sigma(E) = E + \varphi$ oder $\sigma(E) = E + \varphi + 1$. Unter Zuhilfenahme von 2.3.3 verifizieren wir leicht, daß dieses σ die Ordnung 4 hat. Also hat $G_i(L/K)$ mindestens vier Elemente. Weiter erhält man ebenfalls durch 4.1.6 oder 4.1.10 oder 4.1.11, daß es entweder kein $\sigma \in G_i(L/K)$ mit $\sigma(E) = E + 1$ oder kein $\sigma \in G_i(L/K)$ mit $\sigma(E) = E + \varphi$ oder kein $\sigma \in G_i(L/K)$ mit $\sigma(E) = E + \varphi + 1$ gibt. Hieraus ergibt sich $\#G_i(L/K) < 8$ und damit $G_i(L/K) \cong \mathbb{Z}/4\mathbb{Z}$.

Wir betrachten nun den Fall $s \leq i < t$. Nach 4.1.4 gibt es ein $\sigma \in G_i(L/K)$ mit $\sigma(\varphi) = \varphi$, $\sigma(E) = E$ und $F_\alpha + 1$. Damit hat $G_i(L/K)$ mindestens zwei Elemente. Gäbe es noch mehr Elemente, so müßte es ein $\sigma \in G_i(L/K)$ geben, so daß $\sigma(E) = E + 1$, $\sigma(E) = E + \varphi$ oder $\sigma(E) = E + \varphi + 1$ gilt, was aber die Sätze 4.1.6, 4.1.10 und 4.1.11 nicht zulassen.

Im Fall $t \leq i$ erhält man nach 4.1.4, daß es kein $\sigma \in G_i(L/K)$ gibt mit $\sigma(\varphi) = \varphi$, $\sigma(E) = E$ und $\sigma(F_\alpha) = F_\alpha + 1$. Daraus folgt $G_i(L/K) = \{1\}$. □

4.2 Der Führer von $\pi^K_{\alpha,\beta}$

In diesem Abschnitt soll die Voraussetzung $\nu_K(\beta) < 0$ nicht gelten. Für die folgenden Betrachtungen bezeichnen wir mit V den Darstellungsraum von $\rho^K_{\alpha,\beta}$ bzw. $\pi^K_{\alpha,\beta}$ und mit $V^{G_i(L/K)}$ den Fixpunkteraum der zugehörigen Operation der i-ten Verzweigungsgruppe. Zunächst behandeln wir die trivialen Fälle. Dabei setzen wir die Ergebnisse von 1.11 als bekannt voraus. Mit K_α bezeichnen wir den Zerfällungskörper des quadratischen Polynoms $X^2 + X + \alpha$ über K und mit χ_α den eindeutig bestimmten Charakter von $W(K^{\mathrm{sep}}/K)$ mit $\mathrm{Kern}(\chi_\alpha) = W(K^{\mathrm{sep}}/K_\alpha)$.

Lemma 4.2.1 *Es gilt* $\mathrm{cond}(\chi_\alpha) = \mathrm{d}(K_\alpha/K)$.

Beweis: Sei σ das eindeutig bestimmte nichttriviale Element von $G(K_\alpha/K)$. Der Rückgriff auf die Definition des Führers und die Anwendung von [21, Chap. IV, Prop. 4] liefert

$$\begin{aligned}\mathrm{cond}(\chi_\alpha) &= \sum_{i=0}^{\infty} \frac{\#G_i(K_\alpha/K)}{\#G_0(K_\alpha/K)} \dim \mathbb{C}/\mathbb{C}^{G_i(K_\alpha/K)} \\ &= \sum_{i=0}^{\mathrm{i}_{K_\alpha/K}(\sigma)-1} 1 \\ &= \mathrm{d}(K_\alpha/K).\end{aligned}$$

□

Satz 4.2.2 *Im Fall* $\nu_K(\beta) > 0$ *gilt* $\mathrm{cond}(\pi^K_{\alpha,\beta}) = 2\mathrm{d}(K_\alpha/K)$ *und*

$$\mathrm{cond}((\pi^K_{\alpha,\beta})') = \begin{cases} 1, & \textit{falls } K_\alpha/K \textit{ unverzweigt} \\ 2\mathrm{d}(K_\alpha/K), & \textit{falls } K_\alpha/K \textit{ verzweigt.} \end{cases}$$

Beweis: Es gilt die Isomorphie $(\pi^K_{\alpha,\beta})' \cong (\chi_\alpha \otimes \pi, N)$, mit $\pi = \omega_K \oplus 1$ und

$$N = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Daraus folgt

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = \mathrm{cond}(\chi_\alpha\omega^{-1}) + \mathrm{cond}(\chi_\alpha) = 2\mathrm{cond}(\chi_\alpha) = 2\mathrm{d}(K_\alpha/K).$$

Falls K_α/K unverzweigt ist, erhält man $\mathrm{cond}(\pi^K_{\alpha,\beta}) = 0$. Außerdem operiert die Trägheitsgruppe $G_0(K^{\mathrm{sep}}/K)$ trivial auf V, und es gilt $\dim(\mathrm{Kern}(N)) = 1$. Daraus folgt $\mathrm{cond}((\pi^K_{\alpha,\beta})') = 1$.

Für den Fall, daß K_α/K verzweigt ist, sei σ das nichttriviale Element von $G_0(K_\alpha/K)$. Die Formel für $\mathrm{cond}((\pi^K_{\alpha,\beta})')$ erhält man, wenn man beachtet, daß jede Fortsetzung von σ nach K^{sep} in $G_0(K^{\mathrm{sep}}/K)$ liegt und als Skalar -1 auf V operiert und deshalb $V^{G_0(K^{\mathrm{sep}}/K)} = 0$ gilt. □

Satz 4.2.3 *Im Fall* $\nu_K(\beta) = 0$ *gilt*

$$\mathrm{cond}((\pi^K_{\alpha,\beta})') = \mathrm{cond}(\pi^K_{\alpha,\beta}) = 2\mathrm{d}(K_\alpha/K).$$

Beweis: Weil $\mathcal{E}_{\alpha,\beta}$ potentiell gute Reduktion hat, gilt $(\pi^K_{\alpha,\beta})' = (\pi^K_{\alpha,\beta}, 0)$. Daraus folgt

$$\mathrm{cond}((\pi^K_{\alpha,\beta})') = \mathrm{cond}(\pi^K_{\alpha,\beta}).$$

Außerdem gilt $\pi^K_{\alpha,\beta} \cong \chi_\alpha \otimes \pi^K_{0,\beta}$. Weil $\mathcal{E}_{0,\beta}$ gute Reduktion hat, ist $\pi^K_{0,\beta}$ nach dem Kriterium von Neron-Ogg-Shafarevich unverzweigt. Dies hat zur Folge, daß $\pi^K_{0,\beta}$ Summe von zwei unverzweigten eindimensionalen Darstellungen ρ_1 und ρ_2 ist. Daraus folgt

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = \mathrm{cond}(\chi_\alpha \otimes (\rho_1 \oplus \rho_2)) = \mathrm{cond}(\chi_\alpha\rho_1 \oplus \chi_\alpha\rho_2) = 2\mathrm{cond}(\chi_\alpha).$$

Wegen $\mathrm{cond}(\chi_\alpha) = \mathrm{d}(K_\alpha/K)$ erhält man die gewünschte Aussage. □

Satz 4.2.4 *Im Fall* $\nu_K(\beta) < 0$ *und* $\mathrm{e}(L/K(\varphi,\gamma)) = 1$ *gilt*

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = \begin{cases} 0, & \textit{falls } K(\varphi,\gamma)/K(\varphi) \textit{ unverzweigt} \\ 2, & \textit{falls } K(\varphi,\gamma)/K(\varphi) \textit{ verzweigt.} \end{cases}$$

Beweis: Im Fall $K(\varphi,\gamma)/K(\varphi)$ unverzweigt ist L/K unverzweigt. Daraus folgt $\mathrm{cond}(\pi^K_{\alpha,\beta}) = 0$. Wir nehmen nun an, daß $K(\varphi,\gamma)/K(\varphi)$ verzweigt ist. Dann ist L/K zahm verzweigt vom Grad 3. Daraus folgt

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = \mathrm{cond}(\rho^K_{\alpha,\beta}) = \frac{\#G_0(L/K)}{\#G_0(L/K)} \dim V/V^{G_0(L/K)} = 2 - \dim V^{G_0(L/K)}.$$

Sei nun K_0 die maximale unverzweigte Zwischenerweiterung von L/K. Dann ist die Galoisgruppe $G_0(L/K) = G(L/K_0)$ zyklisch der Ordnung 3. Wir fixieren einen Erzeuger σ. Wäre nun $\dim V^{G(L/K_0)} \neq 0$, so müßte es einen Charakter χ_0 von $G(L/K_0)$ geben mit $\rho^{K_0}_{\alpha,\beta} \cong 1 \oplus \chi_0$. Wegen der Injektivität von $\rho^{K_0}_{\alpha,\beta}$ müßte $\chi_0(\sigma)$ eine primitive dritte Einheitswurzel sein. Dies ist aber nicht möglich, da

$$\mathrm{Tr}(\rho^{K_0}_{\alpha,\beta}(\sigma)) = 1 + \chi_0(\sigma)$$

nach 3.4.3 nur die Werte 0,1,-1,$\sqrt{2}i$ oder $-\sqrt{2}i$ annehmen kann. Also folgt $\dim V^{G(L/K_0)} = 0$ und damit $\mathrm{cond}(\pi^K_{\alpha,\beta}) = 2$. □

Nun behandeln wir den wichtigsten Fall, daß $L/K(\varphi,\gamma)$ verzweigt ist.

Satz 4.2.5 *Wir nehmen $\nu_K(\beta) < 0$ und $\mathrm{e}(L/K(\varphi,\gamma)) > 1$ an. Außerdem setzen wir*

$$r' := \min\{\mathrm{d}(K(E)/K(D)), \mathrm{d}(K(E)/K(D_\varphi)), \mathrm{d}(K(E)/K(D_{\varphi^2}))\},$$

$$s' := \max\{\mathrm{d}(K(E)/K(D)), \mathrm{d}(K(E)/K(D_\varphi)), \mathrm{d}(K(E)/K(D_{\varphi^2}))\}$$

sowie

$$t := \mathrm{d}(L/K(\varphi, E))$$

und definieren $r := \max\{r', 1\}$, $s := \max\{s', 1\}$. Dann gilt

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = 2 + \frac{8r + 4(s+t) - 16}{\mathrm{e}(L/K)}.$$

Beweis: Es gilt

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = \mathrm{cond}(\rho^K_{\alpha,\beta}) = \sum_{i=0}^{\infty} \frac{\#G_i(L/K)}{\#G_0(L/K)} \dim(V/V^{G_i(L/K)}).$$

Für alle $i \in \mathbb{N}_0$ mit $i \geq t$ wird $G_i(L/K)$ nach 4.1.12 trivial. Daraus folgt $V^{G_i(L/K)} = V$. Sei nun $i < t$. Nach 4.1.4 gibt es ein $\sigma \in G_i(L/K)$ mit $\sigma(\varphi) = \varphi$, $\sigma(E) = E$ und $\sigma(F_\alpha) = F_\alpha + 1$. Nach 3.4.3 gilt $\mathrm{Tr}(\rho^K_{\alpha,\beta}(\sigma)) = -2$. Dies läßt nur den Schluß zu, daß σ auf V als Skalar -1 operiert. Also gilt $V^{G_i(L/K)} = 0$. Unter Anwendung von 4.1.12 erhält man

$$\begin{aligned}
\mathrm{cond}(\pi^K_{\alpha,\beta}) &= \frac{2}{\mathrm{e}(L/K)} \sum_{i=0}^{t-1} \#G_i(L/K) \\
&= 2 + \frac{2}{\mathrm{e}(L/K)} \left(\sum_{i=1}^{r-1} \#G_i(L/K) + \sum_{i=r}^{s-1} \#G_i(L/K) + \sum_{i=s}^{t-1} \#G_i(L/K) \right) \\
&= 2 + \frac{2}{\mathrm{e}(L/K)} \left((r-1)8 + (s-r)4 + (t-s)2 \right) \\
&= 2 + \frac{8r + 4(s+t) - 16}{\mathrm{e}(L/K)}.
\end{aligned}$$

□

4.3 Differenten quadratischer Erweiterungen

Ab jetzt soll wieder die Voraussetzung $\nu_K(\beta) < 0$ gelten. Wir erinnern daran, daß alle separablen quadratischen Erweiterungen unseres Körpers K Artin-Schreier-Erweiterungen sind. Das bedeutet, daß sich diese Erweiterungen als Zerfällungskörper K_a eines Polynoms der Form $X^2 + X + a$ mit geeignetem $a \in K$ realisieren lassen. Hierbei gilt genau dann $K_a = K$, wenn a von der Form $a = x^2 + x$ mit $x \in K$ ist. Zwei Elemente a, a' von K liefern genau dann die selbe quadratische Erweiterung, wenn sie sich um ein Element der Form $x^2 + x$ mit $x \in K$ unterscheiden. Die Menge aller Elemente dieser Form bilden eine additive Untergruppe $Q(K)$ von K. Die Elemente der Faktorgruppe $K/Q(K)$ entsprechen dann eineindeutig den separablen quadratischen Erweiterungen von K. Es stellt sich nun die Frage, wie man für ein beliebiges $a \in K$ einen geeigneten Repräsentanten von $a + Q(K)$ wählt, so daß man den Differentenexponenten $\mathrm{d}(K_a/K)$ leicht berechnen kann.

Weil wir uns nur für die verzweigten Erweiterungen interessieren, wollen wir im folgenden die Faktorgruppe $K^{\mathrm{unv}}/Q(K^{\mathrm{unv}})$ der maximalen unverzweigten Erweiterung K^{unv} betrachten. Wir erinnern daran, daß jede Uniformisierende T von K auch eine Uniformisierende von K^{unv} ist und man K^{unv} aus K durch algebraischen Abschluß des Restklassenkörpers erhält, d. h. $K^{\mathrm{unv}} = \mathbb{F}_2^{\mathrm{alg}}((T))$. Für die folgenden Betrachtungen verwenden wir das Zeichen $\sum'$, wenn eine Summation nur über ungerade Indices erfolgen soll.

Definition 4.3.1 *In Abhängigkeit von einer Uniformisierenden T von K^{unv} definieren wir die Menge*

$$R_T(K^{\mathrm{unv}}) := \{ \sum_{i=-k}^{-1}{}' a_i T^i \mid k \in \mathbb{N} \text{ ungerade und } a_{-1}, a_{-3}, \ldots, a_{-k} \in \mathbb{F}_2^{\mathrm{alg}} \}.$$

Satz 4.3.2 *Die Menge $R_T(K^{\mathrm{unv}})$ ist ein additiv abgeschlossenes Repräsentantensystem der Faktorgruppe $K^{\mathrm{unv}}/Q(K^{\mathrm{unv}})$.*

Beweis: Daß $R_T(K^{\mathrm{alg}})$ additiv abgeschlossen ist, folgt aus der additiven Abgeschlossenheit des Restklassenkörpers $\mathbb{F}_2^{\mathrm{alg}}$ von K^{unv}. Sei $b = \sum_{i=m}^{\infty} b_i T^i \in K^{\mathrm{unv}}$ beliebig. Mit $b_- := \sum_{i=m}^{-1} b_i T^i$ und $b_+ := \sum_{i=0}^{i=\infty} b_i T^i$ erhalten wir

$$b = b_- + b_+.$$

Nach dem Lemma von Hensel gibt es ein $x \in K^{\mathrm{unv}}$, das die Gleichung $x^2 + x = b_+$ erfüllt. Damit erhält man

$$b \equiv b_- \mod Q(K^{\mathrm{unv}}).$$

Für alle $i = -m, -m+2, \ldots, -1$ wählen wir $i', s \in \mathbb{N}$ mit $i = -i'2^s$ und i' ungerade sowie $a_i \in \mathbb{F}_2^{\mathrm{alg}}$ mit $b_i = a_i^{2^s}$. Dann gilt

$$\begin{aligned} b_i T^i &\equiv b_i T^i + \sum_{j=0}^{s-1} a_i^{2^j} T^{-i'2^j} + \left(\sum_{j=0}^{s-1} a_i^{2^j} T^{-i'2^j} \right)^2 \mod Q(K^{\mathrm{unv}}) \\ &= b_i T^i + a_i T^{-i'} + a_i^{2^s} T^{-i'2^s} \\ &= a_i T^{-i'}. \end{aligned}$$

Damit erhält man

$$b \equiv \sum_{i=m}^{-1} a_i T^{-i'} \mod Q(K^{\mathrm{unv}})$$

mit $\sum_{i=m}^{-1} a_i T^{-i'} \in R_T(K^{\mathrm{unv}})$.

Seien nun $a, b \in R_T(K^{\mathrm{unv}})$ mit $a \equiv b \mod Q(K^{\mathrm{unv}})$. Dann gilt $a + b \in R_T(K^{\mathrm{unv}})$, und es gibt ein $x \in K$ mit $a + b = x + x^2$. Wäre nun $\nu_{K^{\mathrm{unv}}}(x) < 0$, so wäre $\nu_{K^{\mathrm{unv}}}(a + b) = 2\nu_{K^{\mathrm{unv}}}(x)$ gerade und echt kleiner als 0. Weil $R_T(K^{\mathrm{unv}})$ aber kein Element mit dieser Eigenschaft besitzt, muß $\nu_{K^{\mathrm{unv}}}(x) \geq 0$ sein. Folglich gilt $\nu_{K^{\mathrm{unv}}}(a+b) \geq 0$, woraus wir $a+b = 0$ bzw. $a = b$ erhalten. □

Wir nehmen an, daß wir eine Uniformisierende T von K ausgezeichnet haben.

Definition 4.3.3 *Für ein beliebiges $a \in K^{\mathrm{unv}}$ bezeichnen wir mit a' das eindeutig bestimmte Element $a' \in R_T(K^{\mathrm{unv}})$, für das*

$$a \equiv a' \mod Q(K^{\mathrm{unv}})$$

gilt. Wir nennen a' den Rest von a bzgl. T.

Korollar 4.3.4 *Sei $a \in K$ und $b \in K^{\mathrm{unv}}$ mit $a = a' + b + b^2$. Dann ist $a' \in K$, und b liegt in der eindeutig bestimmten unverzweigten quadratischen Erweiterung $\mathbb{F}_{q^2}((T))$ von K. Hierbei ist b von der Form $b = b_0 + b_1$ mit $b_0 \in \mathbb{F}_{q^2}$ und $b_1 \in K$.*

Beweis: Die Aussage $a' \in K$ ergibt sich aus dem Beweis von Satz 4.3.2. Wegen $a + a' = b + b^2$ und $b \in K^{\mathrm{unv}}$ folgt $b \in \mathbb{F}_{q^2}((T))$. Weil $\mathbb{F}_{q^2}/\mathbb{F}_q$ eine Artin-Schreier-Erweiterung ist, gibt es ein $\psi \in \mathbb{F}_{q^2}$ mit $\psi + \psi^2 \in \mathbb{F}_q$. Wir wählen nun $c_0, c_1 \in K$ mit $b = c_0 + c_1\psi$. Dann gilt

$$a + a' = c_0 + c_1\psi + (c_0 + c_1\psi)^2 = c_0 + c_0^2 + c_1^2(\psi + \psi^2) + (c_1 + c_1^2)\psi.$$

Wegen $a + a' \in K$ muß $c_1 + c_1^2 = 0$ bzw. $c_1 = 0$ oder 1 sein. Mit $b_0 := c_1\psi$ und $b_1 := c_0$ erhalten wir die Aussage des Korollars. □

Satz 4.3.5 *Sei $a \in K$ beliebig. Dann gilt*

$$\mathrm{d}(K_a/K) = \begin{cases} 0, & \text{falls } a' = 0 \\ 1 - v_K(a'), & \text{falls } a \neq 0. \end{cases}$$

Beweis: Im Fall $a' = 0$ ist K_a/K unverzweigt nach 4.3.4, und man erhält die gewünschte Aussage. Im Fall $a' \neq 0$ sei K' die eindeutig bestimmte unverzweigte quadratische Erweiterung von K. Weiter sei $z \in K'_a$ mit $z^2 + z = a'$. Dann gilt

$$\nu_{K'_a}(z) = \frac{1}{2}\nu_{K'_a}(a') = \nu'_K(a').$$

Weiter wählen wir ein $m \in \mathbb{N}$ mit $\nu'_K(a') = -2m + 1$ und setzen $\tau := zT^m$. Dann ist τ eine Uniformisierende von K'_a. Wir setzen $f = X^2 + T^m X + T^{2m} a'$. Wegen

$$f(\tau) = z^2 T^{2m} + T^m z T^m + T^{2m} a' = 0$$

ist f das Minimalpolynom von τ. Nach [21, Chap. III, Prop. 11, Cor.] wird die Differente von K'_a/K' von $f'(\tau) = T^m$ erzeugt. Daraus folgt

$$\mathrm{d}(K'_a/K') = \nu_{K'_a}(T^m) = 2m = 1 - \nu_{K'}(a).$$

Wegen $\mathrm{d}(K_a/K) = \mathrm{d}(K'_a/K')$ erhält man die gewünschte Aussage. □

Im Fall $\nu_K(a') < 0$ haben wir lediglich davon Gebrauch gemacht, daß $\nu_K(a')$ ungerade und kleiner als 0 ist. Deshalb erhalten wir das folgende Korollar.

Korollar 4.3.6 *Sei $a \in K$ mit $\nu_K(a)$ ungerade und kleiner als 0. Dann gilt*

$$\mathrm{d}(K_a/K) = 1 - \nu_K(a).$$

Insgesamt haben wir nun das Problem der Berechnung der Differentenexponenten zufriedenstellend gelöst, **wenn wir eine Uniformisierende T ausgezeichnet haben**. Wenn wir aber in den Zwischenerweiterungen von L/K rechnen, haben wir das Problem, daß a priori keine Uniformisierende ausgezeichnet ist. Das folgende Lemma hilft uns bei der Lösung von Problemen, die in diesem Zusammenhang auftreten.

Lemma 4.3.7 *Sei $a \in K$. Dann gilt $\nu_K(a') = \max\{\nu_K(a + x + x^2) \mid x \in K^{\mathrm{unv}}\}$.*

Beweis: Wäre $\nu(a') < \max\{\nu_K(a + x + x^2) \mid x \in K\}$, so gäbe es ein $x \in K$ mit

$$\nu_K(a') < \nu_K(a' + x + x^2).$$

Dies ist nur im Fall $a' \neq 0$ bzw. $\nu_K(a') < 0$ möglich. Ist aber $\nu_K(a') < 0$, so muß auch $\nu_K(x) < 0$ sein. Hieraus folgt $\nu_K(a') = \nu_K(x^2)$, was aber nicht geht, da a' als Element von $R_T(a)$ ungerade Bewertung haben muß. □

Zum Schluß schauen wir uns noch an, was passiert, wenn wir die Uniformisierende „geringfügig“ abändern.

Lemma 4.3.8 *Sei $c \in \mathbb{F}_{2^f}$ und $T^* := cT$. Für alle $a \in K$ bezeichnen wir mit a^* den Rest von a bezüglich der Uniformisierden T^*. Dann gilt $a' = a^*$.*

Beweis: Es gilt $a^* \in R_T(K)$. □

4.4 Der Rest in der zahmen Erweiterung $K(\varphi,\gamma)$

Zuerst wollen wir eine Uniformisierende in $K(\varphi,\gamma)$ auszeichnen. Dazu ist es notwendig, das Element $\beta \in K^*$ zu zerlegen.

Lemma 4.4.1 *Es gibt ein $i \in \{0,1,2\}$, ein $\beta_0 \in \mathbb{F}_{2^f}$ und ein $\tilde{\gamma} \in K$ mit*

$$\beta = \beta_0 T^i \tilde{\gamma}^3.$$

Beweis: Zuerst setzen wir $n := \nu_K(\beta)$. Sei $i \in \{0,1,2\}$ das eindeutig bestimmte Element mit $n \equiv i \mod 3$. Weiter sei $\beta_0 \in \mathbb{F}^*_{2^f}$ das eindeutig bestimmte Element mit $\nu_K(T^{-n}\beta + \beta_0^{-1}) \geq 1$. Nach dem Lemma von Hensel gibt es ein $\gamma^* \in K$ mit $\beta_0 T^{-n}\beta = {\gamma^*}^3$. Indem wir $\tilde{\gamma} = T^{\frac{n-i}{3}}\gamma^*$ setzen, erhalten wir die gewünschte Zerlegung. □

Damit können wir nun eine Uniformisierende von $K(\varphi,\gamma)$ auszeichnen. Dazu seien $i \in \{0,1,2\}$ und $\beta_0 \in \mathbb{F}^*{}_{2^f}$ sowie $\tilde{\gamma} \in K$ mit $\beta = \beta_0 T^i \tilde{\gamma}^3$. Wir wählen

$$\tau := \begin{cases} \mathrm{T}, & \text{falls } i = 0 \\ \text{eine dritte Wurzel von } \beta_0 T, & \text{falls } i = 1 \\ \text{eine dritte Wurzel von } \sqrt{\beta_0} T, & \text{falls } i = 2. \end{cases}$$

Lemma 4.4.2 *Das Element τ ist eine Uniformisierende von $K(\varphi,\gamma)$.*

Beweis: Im Fall $i = 0$ liegt γ in der unverzweigten Erweiterung von K, die durch Adjungieren einer dritten Wurzel von β_0 entsteht. Also ist $K(\varphi,\gamma)/K$ unverzweigt. Folglich ist $\tau = T$ eine Uniformisierende von $K(\varphi,\gamma)$. Im Fall $i = 1$ oder $i = 2$ sind die Erweiterungen $K(\varphi,\gamma)/K(\varphi)$ und $K(\varphi,\tau)/K(\varphi)$ beide voll verzweigt vom Grad 3, wobei τ eine Uniformisierende von $K(\varphi,\tau)$ ist. Wegen $(\tau^i\tilde{\gamma})^3 = \beta_0 T^i \tilde{\gamma}^3 = \beta$ gilt $\gamma \in \{\tau^i\tilde{\gamma}, \varphi\tau^i\tilde{\gamma}, \varphi^2\tau^i\tilde{\gamma}\} \subset K(\varphi,\tau)$. Daraus folgt $K(\varphi,\tau) = K(\varphi,\gamma)$. Somit ist τ auch eine Uniformisierende von $K(\varphi,\gamma)$. □

Definition 4.4.3 *Für alle $a \in K(\varphi,\gamma)$ definieren wir a' als den Rest von a bzgl. τ.*

Anmerkung zur Wohldefiniertheit: Eine andere Wahl von β_0 und der dritten Wurzel von $\beta_0 T$ bewirkt lediglich eine Änderung von τ um einen Faktor aus dem Restklassenkörper von $K(\varphi,\gamma)$. Wegen 4.3.8 folgt die Eindeutigkeit von a'. □

Jetzt haben wir einen Konflikt von Notationen herbeigeführt, den wir unverzüglich ausräumen müssen.

Bemerkung 4.4.4 *Sei $a \in K$. Dann ist das a' von 4.3.3 mit dem von 4.4.3 identisch.*

Beweis: Man überzeugt sich leicht davon, daß a' im Sinne von 4.3.3 in $R_\tau(K(\varphi,\gamma))$ liegt. □

4.5 Die Differenten von $K(E)$ über $K(D)$, $K(D_\varphi)$ und $K(D_{\varphi^2})$

Wir erinnern daran, daß $K(\varphi,E)$ als Erweiterung von $K(\varphi,D)$, $K(\varphi,D_\varphi)$ und $K(\varphi,D_{\varphi^2})$ jeweils höchstens vom Grad 2 ist. Die Grade von $K(\varphi,D)$, $K(\varphi,D_\varphi)$ und $K(\varphi,D_{\varphi^2})$ als Erweiterungen von $K(\varphi,\gamma)$ sind ebenfalls kleiner oder gleich 2. Im vorhergehenden Abschnitt haben wir die Uniformisierdende τ von $K(\varphi,\gamma)$ ausgezeichnet und damit den Rest in $K(\varphi,\gamma)$ definiert. Nun verwenden wir die Ergebnisse des vorletzten Abschnitts, um die Differentenexponenten $\mathrm{d}(K(\varphi,E)/K(\varphi,D))$, $\mathrm{d}(K(\varphi,E)/K(\varphi,D_\varphi))$ und $\mathrm{d}(K(\varphi,E)/K(\varphi,D_{\varphi^2}))$ zu berechnen, welche mit den Differentenexponenten von $K(E)/K(D)$, $K(E)/K(D_\varphi)$ und $K(E)/K(D_{\varphi^2})$ identisch sind.

Für die folgenden Betrachtungen seien δ, ϵ Elemente der maximalen unverzweigten Erweiterung von $K(\varphi, \gamma)$ mit

$$\gamma = \gamma' + \delta + \delta^2$$

und

$$\delta = \delta' + \epsilon + \epsilon^2.$$

Nach 4.3.4 liegt δ in der unverzweigten quadratischen Erweiterung von $K(\varphi, \gamma)$ und ϵ in der unverzweigten Erweiterung vom Grad 4 von $K(\varphi, \gamma)$. Diese Bezeichnungen sollen für den gesamten Rest dieser Arbeit in Kraft bleiben.

Satz 4.5.1 *Im Fall $\gamma' = 0$ gilt*

$$\mathrm{d}(K(E)/K(D)) = \begin{cases} 0, & \text{falls } \delta' = 0 \\ 1 - \nu_{K(\varphi,\gamma)}(\delta'), & \text{falls } \delta' \neq 0. \end{cases}$$

Beweis: Aus $\gamma' = 0$ folgt $D = \delta$ oder $\delta + 1$ und $K(\varphi, E) = K(\varphi, D)_\delta$. Die Anwendung von 4.3.5 liefert die Formel

$$\mathrm{d}(K(E, \varphi)/K(D, \varphi)) = \begin{cases} 0, & \text{falls } \delta' = 0 \\ 1 - \nu_{K(\varphi,D)}(\delta'), & \text{falls } \delta' \neq 0. \end{cases}$$

Weiter gilt $\mathrm{d}(K(E, \varphi)/K(D, \varphi)) = \mathrm{d}(K(E)/K(D))$. Außerdem folgt aus $\gamma' = 0$ die Unverzweigtheit von $K(\varphi, D)/K(\varphi, \gamma)$ und damit $\nu_{K(\varphi,D)}(\delta') = \nu_{K(\varphi,\gamma)}(\delta')$. Hieraus ergibt sich die gewünschte Aussage. □

Satz 4.5.2 *Im Fall $\gamma' \neq 0$ gilt*

$$\mathrm{d}(K(E)/K(D)) = \begin{cases} 0, & \text{falls } \gamma'^2 + \delta'\gamma' + \delta'^2 = 0 \\ 1 - \nu_{K(\varphi,\gamma)}\left(\frac{\gamma'^2 + \delta'\gamma' + \delta'^2}{\gamma'}\right), & \text{falls } \gamma'^2 + \delta'\gamma' + \delta'^2 \neq 0. \end{cases}$$

Beweis: Für $\tilde{D} := D + \delta$ gilt

$$\tilde{D} + \tilde{D}^2 = D + D^2 + \delta + \delta^2 = \gamma + \delta + \delta^2 = \gamma'.$$

Daraus folgt, daß $\nu_{K(\varphi,D)}(\tilde{D}) = \nu_{K(\varphi,\gamma)}(\gamma')$ ungerade und kleiner als 0 ist. Damit wir 4.3.6 anwenden können, müssen wir $a, b \in K(\varphi, \gamma)$ so wählen, daß

$$\begin{aligned} D + a\tilde{D} + b + (a\tilde{D} + b)^2 &= D + a\tilde{D} + b + a^2\tilde{D}^2 + b^2 \\ &= \tilde{D} + \delta + a\tilde{D} + b + a^2(\tilde{D} + \gamma') + b^2 \\ &= (1 + a + a^2)\tilde{D} + a^2\gamma' + b + b^2 + \delta \end{aligned}$$

eine möglichst große Bewertung hat. Dazu setzen wir $b := \epsilon$. Weiter verweisen wir darauf, daß sich γ' und δ' als ungerade Polynome in der inversen Uniformisierenden τ^{-1} auffassen lassen. Folglich enthält die Laurentreihenentwicklung von $\frac{\delta'}{\gamma'}$ nur Koeffizienten gerader Ordnung, weshalb $\frac{\delta'}{\gamma'}$ ein Quadrat ist. Wir setzen nun

$$a := \sqrt{\frac{\delta'}{\gamma'}}.$$

Damit erhalten wir

$$\begin{aligned} D + a\tilde{D} + b + (a\tilde{D} + b)^2 &= (1 + \sqrt{\frac{\delta'}{\gamma'}} + \frac{\delta'}{\gamma'})\tilde{D} + \frac{\delta'}{\gamma'}\gamma' + \epsilon + \epsilon^2 + \delta \\ &= \sqrt{1 + \frac{\delta'}{\gamma'} + \frac{\delta'^2}{\gamma'^2}}\tilde{D} + \delta' + \epsilon + \epsilon^2 + \delta \\ &= \frac{\sqrt{\gamma'^2 + \delta'\gamma' + \delta'^2}}{\gamma'}\tilde{D}. \end{aligned}$$

Im Fall ${\gamma'}^2+\delta'\gamma'+{\delta'}^2 = 0$ muß $E = a\tilde{D}+b$ oder $E = a\tilde{D}+b+1$ sein und somit in einer unverzweigten Erweiterung von $K(\varphi, D)$ liegen. Daraus folgt $\mathrm{d}(K(\varphi, E)/K(\varphi, D)) = 0$. Wir betrachten nun den Fall ${\gamma'}^2 + \delta'\gamma' + {\delta'}^2 \neq 0$. Dann gilt

$$\begin{aligned}\nu_{K(\varphi,D)}\left(\frac{\sqrt{{\gamma'}^2+\delta'\gamma'+{\delta'}^2}}{\gamma'}\tilde{D}\right) &= \nu_{K(\varphi,D)}\left(\frac{\sqrt{{\gamma'}^2+\delta'\gamma'+{\delta'}^2}}{\gamma'}\right)+\nu_{K(\varphi,D)}(\tilde{D})\\ &= 2\nu_{K(\varphi,\gamma)}\left(\frac{\sqrt{{\gamma'}^2+\delta'\gamma'+{\delta'}^2}}{\gamma'}\right)+\nu_{K(\varphi,\gamma)}(\gamma')\\ &= \nu_{K(\varphi,\gamma)}\left(\frac{{\gamma'}^2+\delta'\gamma'+{\delta'}^2}{\gamma'}\right).\end{aligned}$$

Wenn wir jetzt nur noch zeigen können, daß diese Zahl ungerade und kleiner als 0 ist, erhalten wir die gewünschte Formel für $\mathrm{d}(K(\varphi, E)/K(\varphi, D)) = \mathrm{d}(K(E)/K(D))$ aus 4.3.6.

Daß

$$\begin{aligned}\nu_{K(\varphi,\gamma)}\left(\frac{{\gamma'}^2+\delta'\gamma'+{\delta'}^2}{\gamma'}\right) &= \nu_{K(\varphi,\gamma)}\left(\frac{(\varphi\gamma'+\delta')(\varphi^2\gamma'+\delta')}{\gamma'}\right)\\ &= \nu_{K(\varphi,\gamma)}(\varphi\gamma'+\delta')+\nu_{K(\varphi,\gamma)}(\varphi^2\gamma'+\delta')-\nu_{K(\varphi,\gamma)}(\gamma')\end{aligned}$$

ungerade ist, folgt daraus, daß sowohl $\nu_{K(\varphi,\gamma)}(\varphi\gamma' + \delta')$ als auch $\nu_{K(\varphi,\gamma)}(\varphi^2\gamma' + \delta')$ als auch $\nu_{K(\varphi,\gamma)}(\gamma')$ ungerade sind.

Falls nun $\nu_{K(\varphi,\gamma)}(\gamma') > \nu_{K(\varphi,\gamma)}(\delta')$ ist, erhalten wir $\nu_{K(\varphi,\gamma)}(\varphi\gamma' + \delta') = \nu_{K(\varphi,\gamma)}(\gamma')$ und $\nu_{K(\varphi,\gamma)}(\varphi^2\gamma' + \delta') = \nu_{K(\varphi,\gamma)}(\gamma')$. Daraus folgt

$$\nu_{K(\varphi,\gamma)}\left(\frac{{\gamma'}^2+\delta'\gamma'+{\delta'}^2}{\gamma'}\right) = \nu_{K(\varphi,\gamma)}(\gamma') < 0.$$

Im Fall $\nu_{K(\varphi,\gamma)}(\gamma') < \nu_{K(\varphi,\gamma)}(\delta')$ erhalten wir die Bedingungen $\nu_{K(\varphi,\gamma)}(\varphi\gamma' + \delta') = \nu_{K(\varphi,\gamma)}(\delta')$ und $\nu_{K(\varphi,\gamma)}(\varphi^2\gamma' + \delta') = \nu_{K(\varphi,\gamma)}(\delta')$. Hieraus ergibt sich

$$\nu_{K(\varphi,\gamma)}\left(\frac{{\gamma'}^2+\delta'\gamma'+{\delta'}^2}{\gamma'}\right) = 2\nu_{K(\varphi,\gamma)}(\delta') - \nu_{K(\varphi,\gamma)}(\gamma') < 0.$$

Wir betrachten nun den Fall $\nu_{K(\varphi,\gamma)}(\gamma') = \nu_{K(\varphi,\gamma)}(\delta')$. Dann gilt $\nu_{K(\varphi,\gamma)}(\varphi\gamma' + \delta') = \nu_{K(\varphi,\gamma)}(\gamma')$ oder $\nu_{K(\varphi,\gamma)}(\varphi^2\gamma' + \delta') = \nu_{K(\varphi,\gamma)}(\gamma')$. Weil $\nu_{K(\varphi,\gamma)}(\varphi\gamma' + \delta')$ und $\nu_{K(\varphi,\gamma)}(\varphi^2\gamma' + \delta')$ echt kleiner als 0 sein müssen, erhält man wiederum

$$\nu_{K(\varphi,\gamma)}\left(\frac{{\gamma'}^2+\delta'\gamma'+{\delta'}^2}{\gamma'}\right) < 0.$$

□

Wir versuchen nun, die letzten beiden Sätze übersichtlich in einer Aussage zusammenzufassen. Dazu benötigen wir eine Hilfsaussage.

Lemma 4.5.3 *Es gilt*

$$(\varphi\gamma)' = \varphi\gamma' + \delta'$$

und

$$(\varphi^2\gamma)' = \varphi^2\gamma' + \delta'.$$

Beweis: Es gilt

$$\begin{aligned}\varphi\gamma &= \varphi(\gamma' + \delta + \delta^2)\\ &= \varphi(\gamma' + (\delta' + \epsilon + \epsilon^2) + (\delta' + \epsilon + \epsilon^2)^2)\\ &= \varphi\gamma' + \varphi\delta' + \varphi\delta'^2 + \varphi\epsilon + \varphi\epsilon^4\\ &= \varphi\gamma' + \delta' + (\varphi^2\delta' + \varphi\epsilon + (\varphi\epsilon)^2) + (\varphi^2\delta' + \varphi\epsilon + (\varphi\epsilon)^2)^2.\end{aligned}$$

Daraus folgt $(\varphi\gamma)' = \varphi\gamma' + \delta'$. Hieraus erhalten wir

$$(\varphi^2\gamma)' = (\varphi\gamma)' + \gamma' = \varphi^2\gamma' + \delta'.$$

□

Satz 4.5.4 *Es gilt*

$$\mathrm{d}(K(E)/K(D)) = \begin{cases} 0, & \textit{falls } (\varphi\gamma)' = 0 \textit{ oder } (\varphi^2\gamma)' = 0\\ 1 - \nu_{K(\varphi,\gamma)}((\varphi\gamma)'), & \textit{falls } (\varphi\gamma)' = (\varphi^2\gamma)' \neq 0\\ 1 - \nu_{K(\varphi,\gamma)}\left(\frac{(\varphi\gamma)'(\varphi^2\gamma)'}{\gamma'}\right), & \textit{sonst.}\end{cases}$$

Beweis: Wir betrachten zunächst den Fall $(\varphi\gamma)' = 0$ oder $(\varphi^2\gamma)' = 0$. Gilt zusätzlich $\gamma' = 0$, so erhält man $\delta' = 0$ nach 4.5.3. Daraus folgt $\mathrm{d}(K(E)/K(D)) = 0$ nach 4.5.1. Ist dagegen $\gamma' \neq 0$, so gilt

$$\gamma'^2 + \delta'\gamma' + \delta'^2 = (\varphi\gamma' + \delta')(\varphi^2\gamma' + \delta') = (\varphi\gamma)'(\varphi^2\gamma)' = 0.$$

Hieraus erhalten wir $\mathrm{d}(K(E)/K(D)) = 0$ nach 4.5.2.

Sei nun $(\varphi\gamma)' = (\varphi^2\gamma)' \neq 0$. Dann erhalten wir $\gamma' = 0$ und $\delta' = (\varphi\gamma)'$ aus 4.5.3. Die Anwendung von 4.5.1 liefert uns

$$\mathrm{d}(K(E)/K(D)) = 1 - \nu_{K(\varphi,\gamma)}((\varphi\gamma)').$$

In allen anderen Fällen folgt schließlich

$$\gamma'^2 + \delta'\gamma' + \delta'^2 = (\varphi\gamma)'(\varphi^2\gamma)' \neq 0$$

und

$$\gamma' = (\varphi\gamma)' + (\varphi^2\gamma)' \neq 0.$$

Die Anwendung von 4.5.2 liefert die gewünschte Aussage. □

Damit haben wir eine einigermaßen geschlossene Formel zur Berechnung des Differentenexponenten von $K(E)/K(D)$ gefunden. Indem wir nun bei allen Rechnungen die Elemente (γ, D, E) durch $(\varphi\gamma, D_\varphi, \varphi E)$ bzw. $(\varphi^2\gamma, D_{\varphi^2}, \varphi^2 E)$ ersetzen, erhalten wir die folgenden beiden Sätze:

Satz 4.5.5 *Es gilt*

$$\mathrm{d}(K(E)/K(D_\varphi)) = \begin{cases} 0, & \textit{falls } \gamma' = 0 \textit{ oder } (\varphi^2\gamma)' = 0\\ 1 - \nu_{K(\varphi,\gamma)}(\gamma'), & \textit{falls } \gamma' = (\varphi^2\gamma)' \neq 0\\ 1 - \nu_{K(\varphi,\gamma)}\left(\frac{\gamma'(\varphi^2\gamma)'}{(\varphi\gamma)'}\right), & \textit{sonst.}\end{cases}$$

Satz 4.5.6 *Es gilt*

$$\mathrm{d}(K(E)/K(D_{\varphi^2})) = \begin{cases} 0, & \textit{falls } \gamma' = 0 \textit{ oder } (\varphi\gamma)' = 0\\ 1 - \nu_{K(\varphi,\gamma)}(\gamma'), & \textit{falls } \gamma' = (\varphi\gamma)' \neq 0\\ 1 - \nu_{K(\varphi,\gamma)}\left(\frac{\gamma'(\varphi\gamma)'}{(\varphi^2\gamma)'}\right), & \textit{sonst.}\end{cases}$$

Um eine Aussage über den größten und den kleinsten Differentenexponenten der drei Körpererweiterungen $K(E)/K(D)$, $K(E)/K(D_\varphi)$ und $K(E)/K(D_{\varphi^2})$ machen zu können, verschärfen wir 2.4.4, indem wir gegebenenfalls γ durch $\varphi\gamma$ oder $\varphi^2\gamma$ ersetzen und D, E sowie F_α entsprechend abändern.

Vereinbarung 4.5.7 *Wir nehmen an, daß*

$$\nu_{K(\varphi,\gamma)}(\gamma') \geq \nu_{K(\varphi,\gamma)}((\varphi\gamma)'), \nu_{K(\varphi,\gamma)}((\varphi\gamma^2)')$$

ist.

Korollar 4.5.8 *Es gilt* $\nu_{K(\varphi,\gamma)}((\varphi\gamma)') = \nu_{K(\varphi,\gamma)}((\varphi\gamma^2)')$.

Beweis: Wegen $(\varphi\gamma)' = (\varphi^2\gamma)'+\gamma'$ folgt $\nu_{K(\varphi,\gamma)}((\varphi\gamma)') \geq \nu_{K(\varphi,\gamma)}((\varphi\gamma^2)')$. Aus $(\varphi^2\gamma)' = (\varphi\gamma)'+\gamma'$ erhalten wir $\nu_{K(\varphi,\gamma)}((\varphi\gamma)') \leq \nu_{K(\varphi,\gamma)}((\varphi\gamma^2)')$. □

Satz 4.5.9 *Es gilt*

$$\mathrm{d}(K(E)/K(D)) \geq \mathrm{d}(K(E)/K(D_\varphi)) = \mathrm{d}(K(E)/K(D_{\varphi^2}))$$

sowie

$$\mathrm{d}(K(E)/K(D)) = \begin{cases} 0, & \text{falls } \gamma' = 0 \text{ und } (\varphi\gamma)' = 0 \\ 1 - \nu_{K(\varphi,\gamma)'}((\varphi\gamma)'), & \text{falls } \gamma' = 0 \text{ und } (\varphi\gamma)' \neq 0 \\ 1 - 2\nu_{K(\varphi,\gamma)}((\varphi\gamma)') + \nu_{K(\varphi,\gamma)}(\gamma'), & \text{falls } \gamma' \neq 0 \end{cases}$$

und

$$\mathrm{d}(K(E)/K(D_\varphi)) = \begin{cases} 0, & \text{falls } \gamma' = 0 \\ 1 - \nu_{K(\varphi,\gamma)}(\gamma'), & \text{falls } \gamma' \neq 0. \end{cases}$$

Beweis: Wir wenden die letzten drei Sätze an und nützen 4.5.8 aus. Im Fall $\gamma' = 0$ und $(\varphi\gamma)' = 0$ erhalten wir

$$0 = \mathrm{d}(K(E)/K(D)) = \mathrm{d}(K(E)/K(D_\varphi)) = \mathrm{d}(K(E)/K(D_{\varphi^2})).$$

Im Fall $\gamma' = 0$ und $(\varphi\gamma)' \neq 0$ erhalten wir

$$\mathrm{d}(K(E)/K(D)) = 1 - \nu_{K(\varphi,\gamma)}((\varphi\gamma)') > 0 = \mathrm{d}(K(E)/K(D_\varphi)) = \mathrm{d}(K(E)/K(D_{\varphi^2})).$$

Falls $\gamma' \neq 0$ ist, muß auch $(\varphi\gamma)' \neq 0$ und $(\varphi^2\gamma)' \neq 0$ sein. Wegen $(\varphi^2\gamma)' = \gamma' + (\varphi\gamma)'$ folgt $\gamma' \neq (\varphi\gamma)'$ und $\gamma' \neq (\varphi^2\gamma)'$. Insgesamt ergibt sich die Ungleichung

$$\begin{aligned} \mathrm{d}(K(E)/K(D)) &= 1 - 2\nu_{K(\varphi,\gamma)}((\varphi\gamma)') + \nu_{K(\varphi,\gamma)}(\gamma') \\ &\geq 1 - \nu_{K(\varphi,\gamma)}((\varphi\gamma)') \\ &= \mathrm{d}(K(E)/K(D_\varphi)) \\ &= \mathrm{d}(K(E)/K(D_{\varphi^2})). \end{aligned}$$

□

Wir können jetzt die Formel für den Führer in 4.2.5 vereinfachen.

Korollar 4.5.10 *Wir nehmen* $\nu_K(\beta) < 0$ *und* $\mathrm{e}(L/K(\varphi,\gamma)) > 1$ *an.*

(i) Im Fall $\gamma' = 0$ *und* $(\varphi\gamma)' = 0$ *gilt*

$$\mathrm{cond}(\pi_{\alpha,\beta}) = 2 + \frac{4(\mathrm{d}(L/K(\varphi,E)) - 1)}{\mathrm{e}(L/K)}.$$

(ii) Im Fall $\gamma' = 0$ und $(\varphi\gamma)' \neq 0$ gilt

$$\mathrm{cond}(\pi_{\alpha,\beta}) = 2 + \frac{4(\mathrm{d}(L/K(\varphi,E)) - \nu_{K(\varphi\gamma)}(\gamma') - 1)}{\mathrm{e}(L/K)}.$$

(iii) Im Fall $\gamma' \neq 0$ gilt

$$\mathrm{cond}(\pi_{\alpha,\beta}) = 2 + \frac{4(\mathrm{d}(L/K(\varphi,E)) - \nu_{K(\varphi,\gamma)}(\gamma') - 2\nu_{K(\varphi,\gamma)}((\varphi\gamma)') - 1)}{\mathrm{e}(L/K)}.$$

Beweis: Wir benutzen die Ergebnisse des letzten Satzes und wenden 4.2.5 an. Im Fall $\gamma' = 0$ und $(\varphi\gamma)' = 0$ erhalten wir

$$\mathrm{cond}(\pi_{\alpha,\beta}) = 2 + \frac{8 + 4(1 + \mathrm{d}(L/K(\varphi,E))) - 16}{\mathrm{e}(L/K)} = 2 + \frac{4(\mathrm{d}(L/K(\varphi,E)) - 1)}{\mathrm{e}(L/K)}.$$

Im Fall $\gamma' = 0$ und $(\varphi\gamma)' \neq 0$ erhalten wir

$$\begin{aligned}\mathrm{cond}(\pi_{\alpha,\beta}) &= 2 + \frac{8 + 4(1 - \nu_{K(\varphi\gamma)}(\gamma') + \mathrm{d}(L/K(\varphi,E))) - 16}{\mathrm{e}(L/K)} \\ &= 2 + \frac{4(\mathrm{d}(L/K(\varphi,E)) - \nu_{K(\varphi\gamma)}(\gamma') - 1)}{\mathrm{e}(L/K)}\end{aligned}$$

Für den Fall $\gamma' \neq 0$ erhalten wir

$$\begin{aligned}&\mathrm{cond}(\pi_{\alpha,\beta}) \\ &\quad = 2 + \frac{8(1 - \nu_{K(\varphi,\gamma)}(\gamma')) + 4(1 - 2\nu_{K(\varphi,\gamma)}((\varphi\gamma)') + \nu_{K(\varphi,\gamma)}(\gamma') + \mathrm{d}(L/K(\varphi,E))) - 16}{\mathrm{e}(L/K)} \\ &\quad = 2 + \frac{4(\mathrm{d}(L/K(\varphi,E)) - \nu_{K(\varphi,\gamma)}(\gamma') - 2\nu_{K(\varphi,\gamma)}((\varphi\gamma)') - 1)}{\mathrm{e}(L/K)}.\end{aligned}$$

□

4.6 Berechnung der Differente von $L/K(\varphi, E)$

Für die folgenden Betrachtungen wählen wir

- ein η in K^{sep} mit
$$\gamma'\delta' = (\gamma'\delta')' + \eta + \eta^2$$
- ein ϑ in K^{sep} mit
$$\eta + \alpha + (\delta+1)\epsilon = (\eta + \alpha + (\delta+1)\epsilon)' + \vartheta + \vartheta^2$$
- ein μ in K^{sep} mit
$$\gamma'\epsilon + \delta\eta + \gamma'(\eta + \alpha + (\delta+1)\epsilon)' = \left(\gamma'\epsilon + \delta\eta + \gamma'(\eta + \alpha + (\delta+1)\epsilon)'\right) + \mu + \mu^2.$$

Satz 4.6.1 *Im Fall $\gamma' = 0$ und $\delta' = 0$ gilt*

$$\mathrm{d}(L/K(\varphi,E)) = \begin{cases} 0, & \text{falls } ((\delta+1)\epsilon + \alpha)' = 0 \\ 1 - \nu_{K(\varphi,\gamma)}(((\delta+1)\epsilon + \alpha)'), & \text{sonst.} \end{cases}$$

Beweis: Aus den Bedingungen $\gamma' = 0$ und $\delta' = 0$ folgt, daß $K(\varphi, E)/K(\varphi, \gamma)$ unverzweigt ist. Hieraus ergibt sich $\nu_{K(\varphi,E)} = \nu_{K(\varphi,\gamma)}$. Weiter erhält man $\gamma = \epsilon + \epsilon^4$. Also können wir ohne Einschränkung annehmen, daß $E = \epsilon$ ist. Damit erhält man die gewünschte Aussage nach 4.3.5. □

Satz 4.6.2 *Im Fall $\gamma' = 0$ und $\delta' \neq 0$ gilt*

$$\mathrm{d}(L/K(\varphi, E)) = 1 - 2\nu_{K(\varphi,\gamma)}\left((\delta^2 + 1)\delta' + a + a^2\right) - \nu_{K(\varphi,\gamma)}(\delta')$$

mit

$$a := \sqrt{\frac{((\delta + 1)\epsilon + \alpha)'}{\delta'}}.$$

Beweis: Aus $\gamma' = 0$ folgt $D = \delta$ oder $D = \delta + 1$. Ohne Einschränkung nehmen wir $D = \delta$ an. Mit $\tilde{E} := E + \epsilon$ erhalten wir

$$\tilde{E} + \tilde{E}^2 = E + E^2 + \epsilon + \epsilon^2 = \delta + \epsilon + \epsilon^2 = \delta'.$$

Hieraus folgt $\nu_{K(\varphi,E)}(\tilde{E}) = \nu_{K(\varphi,\gamma)}(\delta')$. Weiter wählen wir $b \in K^{\mathrm{sep}}$ mit

$$(\delta + 1)\epsilon + \alpha = ((\delta + 1)\epsilon + \alpha)' + b + b^2.$$

Dann gilt

$$\begin{aligned}(D + 1)E + \alpha + (a\tilde{E} + b) + (a\tilde{E} + b)^2 &= (\delta + 1)\tilde{E} + (\delta + 1)\epsilon + \alpha + a\tilde{E} + b + a^2\tilde{E}^2 + b^2 \\ &= (\delta + 1 + a + a^2)\tilde{E} + a^2\delta' + (\delta + 1)\epsilon + \alpha + b + b^2 \\ &= (\delta + 1 + a + a^2)\tilde{E} \\ &= (\delta + (\varphi + a) + (\varphi + a)^2)\tilde{E}.\end{aligned}$$

Daraus folgt, daß

$$\nu_{K(\varphi,E)}((D + 1)E + \alpha + (a\tilde{E} + b) + (a\tilde{E} + b)^2) = 2\nu_{K(\varphi,\gamma)}(\delta + 1 + a + a^2) + \nu_{K(\varphi,\gamma)}(\delta')$$

ungerade und echt kleiner als 0 ist. Die Anwendung von 4.3.6 liefert die Gleichung

$$\mathrm{d}(L/K(\varphi, E)) = 1 - 2\nu_{K(\varphi,\gamma)}(\delta + 1 + a + a^2) - \nu_{K(\varphi,\gamma)}(\delta').$$

□

Lemma 4.6.3 *Wir nehmen an, daß $\gamma' \neq 0$ ist, und setzen $\tilde{D} := D + \delta$, $e := \frac{\eta}{\gamma'}\tilde{D} + \epsilon$, $f := \frac{\vartheta}{\gamma'}\tilde{D} + \mu$ sowie*

$$g := \frac{(D + 1)e + \alpha + f + f^2}{D + e + e^2}.$$

Dann gilt:

(i) Die Bewertung $\nu_{K(\varphi,D)}(D + e + e^2)$ ist ungerade.

(ii) Das Element g ist ein Quadrat in $K(\varphi, D)$.

Beweis: Wegen

$$\tilde{D} + \tilde{D}^2 = D + D^2 + \delta + \delta^2 = \gamma + \delta + \delta^2 = \gamma'$$

erhalten wir

$$\begin{aligned}
D+e+e^2 &= D+\frac{\eta}{\gamma'}\tilde{D}+\epsilon+\left(\frac{\eta}{\gamma'}\tilde{D}+\epsilon\right)^2\\
&= D+\epsilon+\epsilon^2+\frac{\eta}{\gamma'}\tilde{D}+\frac{\eta^2}{\gamma'^2}\tilde{D}^2\\
&= \tilde{D}+\delta+\epsilon+\epsilon^2+\frac{\eta}{\gamma'}\tilde{D}+\frac{\eta^2}{\gamma'^2}\tilde{D}^2\\
&= \left(1+\frac{\delta'}{\gamma'}\right)\tilde{D}+\delta'+\frac{\eta}{\gamma'}\tilde{D}+\frac{\eta^2}{\gamma'^2}\tilde{D}^2+\frac{\delta'}{\gamma'}\tilde{D}\\
&= \left(1+\frac{\delta'+(\gamma'\delta')'+\gamma'\delta'+\eta+\eta^2}{\gamma'}\right)\tilde{D}+\frac{\eta}{\gamma'}\tilde{D}+\frac{\eta^2}{\gamma'^2}\tilde{D}^2+\frac{\delta'}{\gamma'}(\gamma'+\tilde{D})\\
&= \left(1+\frac{\delta'+(\gamma'\delta')'+\gamma'\delta'+\eta^2}{\gamma'}\right)\tilde{D}+\left(\frac{\eta^2}{\gamma'^2}+\frac{\delta'}{\gamma'}\right)\tilde{D}^2\\
&= \left(1+\frac{\delta'+(\gamma'\delta')'}{\gamma'}\right)\tilde{D}+\left(\frac{\eta^2}{\gamma'^2}+\frac{\delta'}{\gamma'}\right)\left(\gamma'+\tilde{D}\right)\tilde{D}\\
&= \left(1+\frac{(\delta'+\gamma'\delta')'}{\gamma'}\right)\tilde{D}+\left(\frac{\eta^2}{\gamma'^2}+\frac{\delta'}{\gamma'}\right)\tilde{D}^3.
\end{aligned}$$

Folglich ist

$$\frac{D+e+e^2}{\tilde{D}} = 1+\frac{(\delta'+\gamma'\delta')'}{\gamma'}+\left(\frac{\eta^2}{\gamma'^2}+\frac{\delta'}{\gamma'}\right)\tilde{D}^2$$

ein Quadrat. Außerdem muß

$$\nu_{K(\varphi,D)}(\tilde{D}) = \frac{1}{2}\nu_{K(\varphi,D)}(\gamma') = \nu_{K(\varphi,\gamma)}(\gamma')$$

ungerade sein. Daraus folgt, daß

$$\nu_{K(\varphi,D)}(D+e+e^2) = \nu_{K(\varphi,D)}(\frac{D+e+e^2}{\tilde{D}})+\nu_{K(\varphi,D)}(\tilde{D})$$

ebenfalls ungerade ist, wenn wir zeigen können, daß $D+e+e^2 \neq 0$ ist.

Wäre $0 = D+e+e^2$, so könnten wir $a, b \in K(\varphi,\gamma)^{\mathrm{unv}}$ wählen mit $e = aD+b$ und erhielten

$$\begin{aligned}
0 &= D+(aD+b)+(aD+b)^2\\
&= (1+a+a^2)D+a^2\gamma+b+b^2.
\end{aligned}$$

Daraus folgte $(1+a+a^2) = 0$, woraus wir $a = \varphi$ oder $a = \varphi^2$ und $0 = a^2\gamma+b+b^2$ erhielten. Aus der letzten Gleichung ergäbe sich dann $(\varphi\gamma)' = 0$ oder $(\varphi^2\gamma)' = 0$, was aber wegen $\gamma' \neq 0$ und

$$\nu_{K(\varphi,\gamma)}(\gamma') \leq \nu_{K(\varphi,\gamma)}((\varphi\gamma)'), \nu_{K(\varphi,\gamma)}((\varphi^2\gamma)')$$

nicht sein kann. Also gilt $D+e+e^2 \neq 0$, und wir erhalten die Aussage (i).

Weiter gilt

$$
\begin{aligned}
&(D+1)e+\alpha+f+f^2\\
&\quad=(\tilde{D}+\delta+1)e+\alpha+f+f^2\\
&\quad=(\tilde{D}+\delta+1)\left(\frac{\eta}{\gamma'}\tilde{D}+\epsilon\right)+\alpha+\frac{\vartheta}{\gamma'}\tilde{D}+\mu+\left(\frac{\vartheta}{\gamma'}\tilde{D}+\mu\right)^2\\
&\quad=\left(\frac{\eta}{\gamma'}+\frac{\vartheta^2}{\gamma'^2}\right)\tilde{D}^2+\left(\epsilon+\frac{(\delta+1)\eta+\vartheta}{\gamma'}\right)\tilde{D}+\alpha+(\delta+1)\epsilon+\mu+\mu^2\\
&\quad=\left(\frac{\eta}{\gamma'}+\frac{\vartheta^2}{\gamma'^2}\right)(\tilde{D}+\gamma')+\left(\epsilon+\frac{(\delta+1)\eta+\vartheta}{\gamma'}\right)\tilde{D}+\alpha+(\delta+1)\epsilon+\mu+\mu^2\\
&\quad=\left(\epsilon+\frac{\delta\eta+\vartheta}{\gamma'}+\frac{\vartheta^2}{\gamma'^2}\right)\tilde{D}+\frac{\vartheta^2}{\gamma'}+\eta+\alpha+(\delta+1)\epsilon+\mu+\mu^2\\
&\quad=\left(\epsilon+\frac{\delta\eta+\vartheta}{\gamma'}+\frac{\vartheta^2}{\gamma'^2}\right)\tilde{D}+\frac{\vartheta^2}{\gamma'}+(\eta+\alpha+(\delta+1)\epsilon)'\\
&\quad=\left(\epsilon+\frac{\delta\eta+\vartheta}{\gamma'}+\frac{\vartheta^2}{\gamma'^2}\right)\tilde{D}+\left(\frac{\vartheta^2}{\gamma'}+(\eta+\alpha+(\delta+1)\epsilon)'\right)\frac{\tilde{D}^2+\tilde{D}}{\gamma'}\\
&\quad=\left(\epsilon+\frac{\delta\eta+\vartheta}{\gamma'}+\frac{\vartheta^2}{\gamma'^2}\right)\tilde{D}+\left(\frac{\vartheta^2}{\gamma'}+(\eta+\alpha+(\delta+1)\epsilon)'\right)\frac{\tilde{D}(\gamma'+\tilde{D}^2)+\tilde{D}}{\gamma'}\\
&\quad=\left(\frac{(\eta+\alpha+(\delta+1)\epsilon)'}{\gamma'}+\frac{\gamma'\epsilon+\delta\eta+\gamma'(\alpha+\eta+(\delta+1)\epsilon)'+\vartheta+\vartheta^2}{\gamma'}\right)\tilde{D}\\
&\qquad+\left(\frac{\vartheta^2}{\gamma'^2}+\frac{(\eta+\alpha+(\delta+1)\epsilon)'}{\gamma'}\right)\tilde{D}^3\\
&\quad=\left(\frac{(\eta+\alpha+(\delta+1)\epsilon)'}{\gamma'}+\frac{(\gamma'\epsilon+\delta\eta+\gamma'(\alpha+\eta+(\delta+1)\epsilon)')'}{\gamma'}\right)\tilde{D}\\
&\qquad+\left(\frac{\vartheta^2}{\gamma'^2}+\frac{(\eta+\alpha+(\delta+1)\epsilon)'}{\gamma'}\right)\tilde{D}^3.
\end{aligned}
$$

Hieraus folgt, daß

$$
\begin{aligned}
\frac{(D+1)e+\alpha+f+f^2}{\tilde{D}}&=\frac{(\eta+\alpha+(\delta+1)\epsilon)'}{\gamma'}+\frac{(\gamma'\epsilon+\delta\eta+\gamma'(\alpha+\eta+(\delta+1)\epsilon)')'}{\gamma'}\\
&\quad+\left(\frac{\vartheta^2}{\gamma'^2}+\frac{(\eta+\alpha+(\delta+1)\epsilon)'}{\gamma'}\right)\tilde{D}^2
\end{aligned}
$$

ein Quadrat ist. Insgesamt erhalten wir die Aussage, daß auch

$$g=\left(\frac{(D+1)e+\alpha+f+f^2}{\tilde{D}}\right)\left(\frac{D+e+e^2}{\tilde{D}}\right)^{-1}$$

ein Quadrat ist. Damit ist (ii) gezeigt. □

Korollar 4.6.4 *Wir nehmen an, daß $\gamma\neq 0$ ist, und setzen $\tilde{D}:=D+\delta$ sowie $e:=\frac{\eta}{\gamma'}\tilde{D}+\epsilon$. Dann gilt*

$$\nu_{K(\varphi,D)}(D+e+e^2)=\nu_{K(\varphi,\gamma)}(\frac{(\varphi\gamma)'(\varphi^2\gamma)'}{\gamma'}).$$

Beweis: Nach 4.3.6 und 4.5.4 gilt

$$1-\nu_{K(\varphi,D)}(D+e+e^2)=\mathrm{d}(K(\varphi,E)/K(\varphi,D))=1-\nu_{K(\varphi,\gamma)}(\frac{(\varphi\gamma)'(\varphi^2\gamma)'}{\gamma'}).$$

Hieraus ergibt sich die behauptete Gleichung. □

Jetzt können wir das Hauptergebnis dieses Abschnittes formulieren.

Satz 4.6.5 *Wir nehmen an, daß $\gamma' \neq 0$ ist, und setzen $\tilde{D} := D + \delta$, $e := \frac{\eta}{\gamma'}\tilde{D} + \epsilon$, $f := \frac{\vartheta}{\gamma'}\tilde{D} + \mu$ und*

$$g := \frac{(D+1)e + \alpha + f + f^2}{D + e + e^2}.$$

Dann gilt

$$\mathrm{d}(L/K(\varphi, E)) = 1 - 2\nu_{K(\varphi,D)}(D + 1 + \sqrt{g} + g) - \nu_{K(\varphi,D)}(D + e + e^2).$$

Beweis: Wir setzen $h := \sqrt{g}(E + e) + f$. Dann gilt

$$\begin{aligned}(D+1)E + \alpha + h + h^2 &= (D+1)E + \alpha + \sqrt{g}(E+e) + f + g(E^2 + e^2) + f^2 \\ &= (D + 1 + \sqrt{g} + g)(E + e) + (D+1)e + \alpha + f + f^2 + g(D + e + e^2) \\ &= (D + 1 + \sqrt{g} + g)(E + e).\end{aligned}$$

Wegen

$$(E + e) + (E + e)^2 = E + E^2 + e + e^2 = D + e + e^2$$

erhält man, daß

$$\nu_{K(\varphi,E)}(E + e) = \frac{1}{2}\nu_{K(\varphi,E)}(D + e + e^2) = \nu_{K(\varphi,D)}(D + e + e^2)$$

ungerade und kleiner als 0 ist. Folglich muß auch

$$\nu_{K(\varphi,E)}((D + 1 + \sqrt{g} + g)(E + e))$$

ungerade und kleiner als 0 sein. Nach 4.3.6 folgt

$$\begin{aligned}\mathrm{d}(L/K(\varphi, E)) &= 1 - \nu_{K(\varphi,E)}((D + 1 + \sqrt{g} + g)(E + e)) \\ &= 1 - 2\nu_{K(\varphi,D)}(D + 1 + \sqrt{g} + g) - \nu_{K(\varphi,D)}(D + e + e^2).\end{aligned}$$

□

Korollar 4.6.6 *Im Fall $\gamma' \neq 0$ gilt*

$$\mathrm{d}(L/K(\varphi, E)) \geq 1 - 6\nu_{K(\varphi,\gamma)}((\varphi\gamma)') + 3\nu_{K(\varphi,\gamma)}(\gamma').$$

Beweis: Mit den Bezeichnungen von 4.6.5 erhält man unter Anwendung von 4.6.4 die Ungleichung

$$\begin{aligned}\mathrm{d}(L/K(\varphi, E)) &\geq 1 - 3\nu_{K(\varphi,D)}(D + e + e^2) \\ &= 1 - 3\nu_{K(\varphi,\gamma)}(\frac{(\varphi\gamma)'(\varphi^2\gamma)'}{\gamma'}) \\ &= 1 - 6\nu_{K(\varphi,\gamma)}((\varphi\gamma)') + 3\nu_{K(\varphi,\gamma)}(\gamma').\end{aligned}$$

□

Kapitel 5

Zahm verzweigte elliptische Kurven vom D_3-Typ

In diesem Kapitel betrachten wir ausschließlich den Fall, daß $[K(\varphi) : K] = 2$, $[K(\varphi, \gamma) : K(\varphi)] = 3$ und $[K(\varphi, E) : K(\varphi, \gamma)] = 1$ ist.

5.1 Charakterisierung von β

Wir beginnen mit zwei einfachen Beobachtungen.

Beobachtung 5.1.1 *Die Bedingung $[K(\varphi) : K] = 1$ gilt genau dann, wenn f gerade ist.*

Beobachtung 5.1.2 *Im Fall f ungerade ist jedes Element von $\mathbb{F}_{2^f}$ eine dritte Potenz.*

Satz 5.1.3 *Die Bedingung $[K(\varphi) : K] = 2$ und $[K(\varphi, \gamma) : K(\varphi)] = 3$ gilt genau dann, wenn f ungerade und $\nu_K(\beta)$ nicht durch 3 teilbar ist. In diesem Fall gilt $K(\varphi, \gamma) = \mathbb{F}_{2^{2f}}((\tau))$, wobei τ eine beliebige dritte Wurzel von T ist.*

Beweis: Sei f ungerade und $\nu_K(\beta)$ nicht durch 3 teilbar. Dann gilt $[K(\varphi) : K] = 2$. Außerdem kann β keine dritte Potenz eines Elements von $K(\varphi)$ sein. Daraus folgt $[K(\varphi, \gamma) : K(\varphi)] = 3$.

Wir nehmen nun an, daß $[K(\varphi) : K] = 2$ und $[K(\varphi, \gamma) : K(\varphi)] = 3$ ist. Dann ist f ungerade. Wäre $\nu_K(\beta)$ durch 3 teilbar, gäbe es ein $l \in \mathbb{Z}$ mit $\nu_K(\beta T^{3l}) = 0$. Sei $\beta_0 \in \mathbb{F}_{2^f}^*$ mit

$$\beta T^{3l} \equiv \beta_0 \mod (T).$$

Wir wählen $\gamma_0 \in \mathbb{F}_{2^f}^*$ mit $\beta_0 = \gamma_0^3$. Nach dem Lemma von Hensel folgt, daß βT^{3l} und damit auch β selbst eine dritte Potenz in K ist. Dies ist ein Widerspruch zur Annahme $[K(\varphi, \gamma) : K(\varphi)] = 3$. Also kann $\nu_K(\beta)$ nicht durch 3 teilbar sein. Damit ist die erste Aussage bewiesen.

Für den Fall $[K(\varphi) : K] = 2$ und $[K(\varphi, \gamma) : K(\varphi)] = 3$ wählen wir eine beliebige dritte Wurzel τ von T. Dann gilt zunächst $\varphi \in \mathbb{F}_4 \subset \mathbb{F}_{2^{2f}}((\tau))$. Um zu zeigen, daß γ ebenfalls in $\mathbb{F}_{2^{2f}}((\tau))$ liegt, wählen wir $m \in \mathbb{Z}$ so, daß βT^m als Element von K die Bewertung 0 hat. Nach dem Lemma von Hensel ist $\beta T^m = (\gamma \tau^m)^3$ eine dritte Potenz in K. Also liegt $\gamma \tau^m$ oder $\varphi \gamma \tau^m$ oder $\varphi^2 \gamma \tau^m$ in $\mathbb{F}_{2^{2f}}((\tau))$. Wegen $\tau, \varphi \in \mathbb{F}_{2^{2f}}((\tau))$ erhält man in allen drei Fällen $\gamma \in \mathbb{F}_{2^{2f}}((\tau))$. Wegen $[\mathbb{F}_{2^{2f}}((\tau)) : K] = 6$ folgt $K(\varphi, \gamma) = \mathbb{F}_{2^{2f}}((\tau))$. □

Satz 5.1.4 *Wir nehmen den Fall $[K(\varphi) : K] = 2$ und $[K(\varphi, \gamma) : K(\varphi)] = 3$ an. Dann gilt $[K(\varphi, E) : K(\varphi, \gamma)] = 1$ genau dann, wenn es ein ein $\tilde{\alpha} \in K$ gibt mit*

$$\beta = \tilde{\alpha} + \tilde{\alpha}^2 + \tilde{\alpha}^3 + \tilde{\alpha}^4.$$

Beweis: Sei $[K(\varphi,E):K(\varphi,\gamma)]=1$. Dann gibt es $a,b,c\in K(\varphi)$ mit $E=a+b\gamma+c\gamma^2$. Weiter gilt

$$\begin{aligned}\gamma &= E+E^4\\ &= a+b\gamma+c\gamma^2+a^4+b^4\gamma^4+c^4\gamma^8\\ &= a+a^4+(b+b^4\beta)\gamma+(c+c^4\beta^2)\gamma^2.\end{aligned}$$

Der Koeffizientenvergleich liefert $0=a+a^4$, $1=b+b^4\beta$ und $0=c+c^4\beta^2$. Aus der letzten Gleichung folgt $c=0$. Sonst wäre nämlich $c^3=\beta^{-2}$, woraus sich $(c\beta)^3=\beta$ ergäbe, was im Widerspruch zu $[K(\varphi,\gamma):K(\varphi)]=3$ steht. Wir setzen nun $\tilde{E}:=a+E$ und $\tilde{\alpha}:=\tilde{E}^3$. Dann gilt

$$\begin{aligned}\tilde{\alpha}+\tilde{\alpha}^2+\tilde{\alpha}^3+\tilde{\alpha}^4 &= \tilde{E}^3+\tilde{E}^6+\tilde{E}^9+\tilde{E}^{12}\\ &= \left(\tilde{E}+\tilde{E}^4\right)^3\\ &= \left(a+E+a^4+E^4\right)^3\\ &= \left(E+E^4\right)^3\\ &= \gamma^3\\ &= \beta.\end{aligned}$$

Wir wählen weiter $b_0,b_1\in K$ mit $b=b_0+b_1\varphi$. Damit erhalten wir

$$\begin{aligned}1 &= b+b^4\beta\\ &= b_0+b_1\varphi+(b_0+b_1\varphi)^4\beta\\ &= b_0+b_0^4\beta+(b_1+b_1^4\beta)\varphi.\end{aligned}$$

Daraus folgt $b_1=b_1^4\beta$. Wäre nun $b_1\neq 0$, so folgte $b_1^3=\beta^{-1}$ und damit $b_1\in\{\gamma^{-1},\varphi\gamma^{-1},\varphi^2\gamma^{-1}\}$. Dies ist ein Widerspruch zu $b_1\in K$. Also gilt $b_1=0$. Daraus ergibt sich die Aussage, daß $\tilde{\alpha}=(b\gamma)^3=b_0^3\beta$ in K liegt.

Wir nehmen nun an, daß es ein $\tilde{\alpha}\in K$ gibt mit $\beta=\tilde{\alpha}+\tilde{\alpha}^2+\tilde{\alpha}^3+\tilde{\alpha}^4$. Sei $\tilde{E}$ eine dritte Wurzel von $\tilde{\alpha}$. Dann gilt

$$\begin{aligned}\left(\tilde{E}+\tilde{E}^4\right)^3 &= \tilde{E}^3+\tilde{E}^6+\tilde{E}^9+\tilde{E}^{12}\\ &= \tilde{\alpha}+\tilde{\alpha}^2+\tilde{\alpha}^3+\tilde{\alpha}^4\\ &= \beta.\end{aligned}$$

Nach 2.2.4 folgt $K(\varphi,E)=K(\varphi,\tilde{E})$. Damit erhalten wir $[K(\varphi,E):K]\leq 6$. Hieraus folgt $[K(\varphi,E):K(\varphi,\gamma)]=1$. □

Insgesamt haben wir nun eine einigermaßen zufriedenstellende Parametrisierung aller Fälle, in denen die Bedingungen $[K(\varphi):K]=2$, $[K(\varphi,\gamma):K(\varphi)]=3$ und $[K(\varphi,E):K(\varphi,\gamma)]=1$ erfüllt sind.

5.2 Die Brauerzerlegung von $\pi^K_{\alpha,\beta}$

Für den gesamten Rest dieses Kapitels nehmen wir $[K(\varphi):K]=2$, $[K(\varphi,\gamma):K(\varphi)]=3$ und $[K(\varphi,E):K(\varphi,\gamma)]=1$ an. Wir fixieren darüber hinaus ein $\tilde{\alpha}\in K$ mit $\beta=\tilde{\alpha}+\tilde{\alpha}^2+\tilde{\alpha}^3+\tilde{\alpha}^4$.

Lemma 5.2.1 *Die Darstellung $\pi^K_{\alpha,\beta}$ ist irreduzibel und besitzt den projektiven Typ D_3.*

Beweis: Weil $K(\varphi,\gamma)$ der Zerfällungskörper des Polynoms $X^3+\beta$ über K ist, muß $K(\varphi,\gamma)/K$ eine Galoiserweiterung sein, deren Galoisgruppe isomorph zu einer Untergruppe von S_3 ist. Wegen $[K(\varphi,\gamma):K]=6$ folgt, daß $G(K(\varphi,\gamma)/K)\cong S_3\cong D_3$ nichtabelsch ist. Somit kann auch $G(L/K)$ nicht abelsch sein. Nach 3.1.7 folgt die Irreduzibilität von $\pi^K_{\alpha,\beta}$. □

Satz 5.2.2 *Falls $\tilde{\alpha} = \alpha$ ist, so gilt $L = K(\varphi, \gamma)$.*

Beweis: Wir wählen $\tilde{E} \in K^{\text{sep}}$ mit $\tilde{E}^3 = \alpha$. Dann gilt

$$\beta = (\tilde{E} + \tilde{E}^4)^3.$$

Also gibt es ein $i \in \{0, 1, 2\}$ mit $\gamma = \varphi^i(\tilde{E} + \tilde{E}^4)$. Wir setzen nun $E^* := \varphi^i \tilde{E}$. Dann gilt $(E^*)^3 = \alpha$ und

$$E^* + (E^*)^4 = \varphi^i \tilde{E} + \varphi^i \tilde{E}^4 = \varphi^i(\tilde{E} + \tilde{E}^4) = \gamma.$$

Daraus folgt $E = E^* + a$ mit $a \in \{0, 1, \varphi, \varphi + 1\}$. Im Fall $a \neq 1$ setzen wir $b := \varphi$. Ansonsten soll $b := 0$ sein. Damit erhalten wir

$$\begin{aligned} F_\alpha + F_\alpha^2 &= (D+1)E + \alpha \\ &= E^3 + E^2 + E + \alpha \\ &= (E^* + a)^3 + (E^* + a)^2 + E^* + a + (E^*)^3 \\ &= (a+1)(E^*)^2 + (a^2+1)E^* + a^3 + a^2 + a \\ &= (a^2+1)E^* + a + b + ((a^2+1)(E^*) + a + b)^2. \end{aligned}$$

Daraus folgt $F_\alpha \in K(\varphi, \gamma)$. Somit ist $L = K(\varphi, E) = K(\varphi, \gamma)$. □

Wir wählen nun einen nichttrivialen Charakter $\chi_{K(\varphi)}$ von $G(K(\varphi, \gamma)/K(\varphi))$, den wir auch als Charakter von $W(K^{\text{sep}}/K(\varphi))$ auffassen.

Satz 5.2.3 *Im Fall $\tilde{\alpha} = \alpha$ gilt $\rho^K_{\alpha,\beta} \cong \text{Ind}^K_{K(\varphi)}(\chi_{K(\varphi)})$.*

Beweis: Weil $L = K(\varphi, \gamma)$ der Zerfällungskörper des Polynoms $X^3 + \beta$ über K und $[L : K] = 6$ ist, gilt $G(L/K) \cong S_3 \cong D_3$. Die Diedergruppe D_3 besitzt genau eine irreduzible zweidimensionale Darstellung, die von einem beliebigen nichttrivialen Charakter der eindeutig bestimmten Untergruppe der Ordnung 3 induziert wird (siehe [22, Chap. 5.3]). □

Im allgemeinen Fall, daß α und $\tilde{\alpha}$ nicht notwendigerweise identisch sind, liefert 1.11.2 die Brauerzerlegung von $\pi^K_{\alpha,\beta}$.

Korollar 5.2.4 *Es gilt $\pi^K_{\alpha,\beta} \cong \text{Ind}^K_{K(\varphi)} \left(\text{Res}^{K(\varphi)}_K(\chi_{\alpha+\tilde{\alpha}}) \Omega^{-1}_{K(\varphi)} \chi_{K(\varphi)} \right)$.*

Beweis: Wegen der Vertauschbarkeit von Twist und Induktion erhalten wir

$$\pi^K_{\alpha,\beta} \cong \chi_{\alpha+\tilde{\alpha}} \Omega_K^{-1} \otimes \text{Ind}^K_{K(\varphi)}(\chi_{K(\varphi)}) \cong \text{Ind}^K_{K(\varphi)} \left(\text{Res}^{K(\varphi)}_K(\chi_{\alpha+\tilde{\alpha}}) \Omega^{-1}_{K(\varphi)} \chi_{K(\varphi)} \right).$$

□

5.3 Führer und minimale Twists

Satz 5.3.1 *Es gilt*

$$\text{cond}(\pi^K_{\alpha,\beta}) = \begin{cases} 2, & \text{falls } \tilde{\alpha}' = \alpha' \\ 2 - 2\nu_K((\tilde{\alpha} + \alpha)'), & \text{sonst.} \end{cases}$$

Beweis: Wir wählen ein $\tilde{\epsilon} \in K^{\text{sep}}$ mit $\tilde{\alpha} = \tilde{\epsilon}^3$. Dann gilt $\beta = (\tilde{\epsilon} + \tilde{\epsilon}^4)^3$. Wir setzen $\tilde{\gamma} := \tilde{\epsilon} + \tilde{\epsilon}^4$ und $\tilde{\delta} := \tilde{\epsilon} + \tilde{\epsilon}^2$. Dann gilt $\tilde{\gamma}^3 = \beta$ und $\tilde{\gamma} = \tilde{\delta} + \tilde{\delta}^2$. Außerdem ist $\tilde{\gamma}' = 0$ und $\tilde{\delta}' = 0$. Beachten wir nun noch die Gleichheit

$$((\tilde{\delta} + 1)\tilde{\epsilon} + \alpha)' = (\tilde{\epsilon}^3 + \tilde{\epsilon}^2 + \tilde{\epsilon} + \alpha)' = (\tilde{\alpha} + \alpha)',$$

so erhalten wir unter Anwendung von 4.6.1 die Aussage

$$\mathrm{d}(L/K(\varphi,\gamma)) = \begin{cases} 0, & \text{falls } (\tilde{\alpha} + \alpha)' = 0 \\ 1 - \nu_{K(\varphi,\gamma)}((\tilde{\alpha} + \alpha)'), & \text{sonst.} \end{cases}$$

Im Fall $\tilde{\alpha}' = \alpha'$ erhalten wir $\mathrm{cond}(\pi^K_{\alpha,\beta}) = 2$ nach 4.2.4. Im Fall $\tilde{\alpha}' \neq \alpha'$ gilt nach 4.5.10 die Gleichung

$$\begin{aligned} \mathrm{cond}(\pi^K_{\alpha,\beta}) &= 2 + \frac{4(\mathrm{d}(L/K(\varphi,\gamma)) - 1)}{\mathrm{e}(L/K)} \\ &= 2 + \frac{4\mathrm{d}(L/K(\varphi,\gamma)) - 4}{6} \\ &= 2 + \frac{4(1 - \nu_{K(\varphi,\gamma)}((\tilde{\alpha} + \alpha)')) - 4}{6} \\ &= 2 - 2\nu_K((\tilde{\alpha} + \alpha)'). \end{aligned}$$

□

Korollar 5.3.2 *Es gilt* $\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 2$.

Beweis: Wegen

$$\mathrm{cond}(\chi_{\tilde{\alpha}+\alpha} \otimes \pi^K_{\alpha,\beta}) = \mathrm{cond}(\pi^K_{\tilde{\alpha},\beta}) = 2$$

gilt $\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) \leq 2$. Weil $\pi^K_{\alpha,\beta}$ unverzweigt induziert ist, muß der minimale Führer gerade sein. Wäre $\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 0$, so müßte es einen Charakter χ von $W(K^{\text{sep}}/K)$ geben, so daß $\chi \otimes \pi^K_{\alpha,\beta}$ unverzweigt ist. Hierbei können wir annehmen, daß $\chi \otimes \pi^K_{\alpha,\beta}$ vom Galois-Typ ist und damit über die Galoisgruppe einer endlichen unverzweigten Erweiterung faktorisiert. Dies steht im Widerspruch zur Irreduzibilität von $\pi^K_{\alpha,\beta}$, weil jede unverzweigte Erweiterung zyklisch und damit abelsch ist. Also folgt $\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 2$. □

Bemerkung 5.3.3 *(i) Wie wir gesehen haben, wird hier der minimale Führer durch Tensorieren mit dem quadratischen Charakter $\chi_{\alpha+\tilde{\alpha}}$ realisiert. Daß bedeutet, daß der Führer von $\pi^K_{\alpha,\beta}$ in Abhängigkeit von α für $\alpha = \tilde{\alpha}$ minimal ist und nicht mehr durch Twist verringert werden kann. Wir werden später sehen, daß es Fälle gibt, in denen zwar* $\mathrm{cond}(\pi_{\alpha,\beta})$ *in Abhängigkeit von α minimal ist, aber trotzdem* $\mathrm{cond}(\pi_{\alpha,\beta}) > \mathrm{cond}_{\min}(\pi_{\alpha,\beta})$ *gilt.*

(ii) In [6, Remark 4.5(b)] wird die Frage angeschnitten, ob für ein gegebenes β der Führer von $\pi^K_{\alpha,\beta}$ stets bei $\alpha = 0$ minimal ist. Dies würde bedeuten, daß die elliptische Kurve $\mathcal{E}_{0,\beta}$ unter den $\mathcal{E}_{\alpha,\beta}$ ausgezeichnet wäre. Hierzu ist zu bemerken, daß sich β ziemlich stark variieren läßt, ohne die Bedingungen $[K(\varphi) : K] = 2$, $[K(\varphi,\gamma) : K(\varphi)] = 3$ und $[K(\varphi, E) : K(\varphi,\gamma)] = 1$ zu verletzen. Somit erhalten wir aus unseren Ergebnissen viele Beispiele von elliptischen Kurven $\mathcal{E}_{\alpha,\beta}$, deren Führer nicht bei $\alpha = 0$ minimal wird. Man kann sich sogar überlegen, daß für ein vorgegebenes α mit $\nu_K(\alpha) < 0$ die Kurve $\mathcal{E}_{\alpha,\alpha^4+\alpha^3+\alpha^2+\alpha}$ stets den Führer 0 hat. Somit findet man also für jedes $\alpha \in K$ ein β, so daß die Kurve $\mathcal{E}_{\alpha,\beta}$ in Abhängigkeit von α minimalen Führer hat.

5.4 Berechnung von ϵ-Faktoren

Im folgenden verwenden wir die Bezeichnungen von Kapitel 1.5. Aus Bequemlichkeitsgründen identifizieren wir die Charaktere von $W(K^{\mathrm{sep}}/K)$ mit Charakteren von K^*.

Satz 5.4.1 *Sei N/M eine unverzweigte quadratische Erweiterung lokaler Körper der Charakteristik 2. Dann gilt*

$$\lambda(N/M, \psi_M, d_{\psi_M}x, d_{\psi_N}x) = 1.$$

Beweis: Zunächst haben wir die Gleichung

$$\lambda(N/M, \psi_M, d_{\psi_M}x, d_{\psi_N}x) = \frac{\epsilon(\mathrm{Ind}_N^M(1_N), \psi_M, d_{\psi_M}x)}{\epsilon(1_N, \psi_N, d_{\psi_N}x)}.$$

Weil N/M unverzweigt ist, gilt $\mathrm{cond}(\psi_N) = \mathrm{cond}(\psi_M) = 0$. Damit erhalten wir

$$\epsilon(1_N, \psi_N, d_{\psi_N}x) = \omega_N^{-1}(1)\int_{\mathcal{O}_N} 1\, d_{\psi_N}x = (q^2)^{\frac{1}{2}\mathrm{cond}(\psi_N)} = 1.$$

Weiter gilt $\mathrm{Ind}_N^M(1_N) \cong 1_M \oplus \chi$, wobei χ der eindeutig bestimmte Charakter von $W(M^{\mathrm{sep}}/M)$ ist mit $\mathrm{Kern}(\chi) = W(M^{\mathrm{sep}}/N)$. Somit ergibt sich

$$\lambda(N/M, \psi_M, d_{\psi_M}x, d_{\psi_N}x) = \epsilon(1_M, \psi_M, d_{\psi_M}x)\epsilon(\chi, \psi_M, d_{\psi_M}x).$$

Hierbei ist

$$\epsilon(1_M, \psi_M, d_{\psi_M}x) = \omega_M^{-1}(1)\int_{\mathcal{O}_M} 1\, d_{\psi_M}x = q^{\frac{1}{2}\mathrm{cond}(\psi_M)} = 1$$

und

$$\epsilon(\chi, \psi_M, d_{\psi_M}x) = \chi\omega_M^{-1}(1)\int_{\mathcal{O}_M} 1\, d_{\psi_M}x = q^{\frac{1}{2}\mathrm{cond}(\psi_M)} = 1.$$

□

Die Anwendung von 5.2.4 und 1.5.2 liefert das folgende Korollar.

Korollar 5.4.2 *Für jeden Charakter χ von $W(K^{\mathrm{sep}}/K)$ gilt*

$$\epsilon(\chi \otimes \pi^K_{\alpha,\beta}, \psi_K, d_{\psi_K}x) = \epsilon(\mathrm{Res}_K^{K(\varphi)}(\chi\chi_{\tilde{\alpha}+\alpha})\Omega^{-1}_{K(\varphi)}\chi_{K(\varphi)}, \psi_{K(\varphi)}, d_{\psi_{K(\varphi)}}x).$$

Kapitel 6

Unverzweigt induzierte elliptische Kurven vom D_2-Typ

In diesem Kapitel betrachten wir ausschließlich den Fall $[K(\varphi) : K] = 2$, $[K(\varphi, \gamma) : K(\varphi)] = 1$ und $[K(\varphi, E) : K(\varphi, \gamma)] = 2$.

6.1 Charakterisierung von β

Satz 6.1.1 *Die Bedingung* $[K(\varphi) : K] = 2$, $[K(\varphi, \gamma) : K(\varphi)] = 1$, $[K(\varphi, E) : K(\varphi, \gamma)] = 2$ *und* $G(L/K)$ *nichtabelsch gilt genau dann, wenn* f *ungerade ist und* $D \in K$ *sowie* $D' \neq 0$ *gilt.*

Beweis: Zunächst nehmen wir an, daß f ungerade ist und $D \in K$ sowie $D' \neq 0$ gilt. Dann gilt $[K(\varphi) : K] = 2$ und $[K(\varphi, \gamma) : K(\varphi)] = 1$ sowie $[K(\varphi, E) : K(\varphi, \gamma)] \leq 2$. Wegen $K(\varphi, E) = K(\varphi)_D$ erhalten wir $[K(\varphi, E) : K(\varphi, \gamma)] = 2$. Nach 2.4.1 gilt nun $[L : K(\varphi, E)] = 2$, womit man $[L : K] = 8$ erhält. Für alle $\sigma \in G(L/K)$ muß nun $\sigma(E) = E$ oder $\sigma(E) = E+1$ gelten. Nach 2.2.8 gibt es genau acht Automorphismen mit dieser Eigenschaft. Wir identifizieren nun gemäß der Tabelle von 2.3.3 die Galoisgruppe $G(L/K)$ mit einer Untergruppe von $GL_2(\mathbb{F}_3)$. Dann enthält diese Untergruppe die Matrizen

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ und } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Weil diese beiden Matrizen offensichtlich nicht kommutieren, kann $G(L/K)$ nicht abelsch sein.

Wir nehmen nun an, daß $[K(\varphi) : K] = 2$, $[K(\varphi, \gamma) : K(\varphi)] = 1$, $[K(\varphi, E) : K(\varphi, \gamma)] = 2$ und $G(L/K)$ nichtabelsch ist. Dann muß f ungerade sein. Wegen 2.4.4 folgt $D \in K(\varphi)$. Weil $G(L/K)$ nichtabelsch ist, muß $\pi^K_{\alpha,\beta}$ nach 3.1.7 irreduzibel sein. Dies wiederum hat zur Folge, daß die Galoisgruppe des projektiven Kernkörpers $G(K(\varphi, E)/K)$ nach 1.6.1 nicht zyklisch sein kann und folglich isomorph zur Kleinschen Vierergruppe ist. Wir wählen nun ein beliebiges $\sigma \in G(K(\varphi, E)/K)$. Aus der Tabelle von 2.2.8 entnimmt man, daß es $a, b \in \mathbb{F}_4$ gibt mit $a \neq 0$ und $\sigma(E) = aE + b$. Damit

$$\sigma(D) = \sigma(E) + \sigma(E)^2 = aE + b + a^2E^2 + b^2 = a^2D + (a + 1)E + b + b^2$$

in $K(\varphi)$ liegt, muß $a = 1$ sein. Also gilt $\sigma(E) = E$, $E + 1$, $E + \varphi$ oder $E + \varphi + 1$. Wäre nun $\sigma(E) = E + \varphi$, so hätte man $\sigma(D) = E + \varphi + (E + \varphi)^2 = D + 1$ und folglich auch $\sigma(\varphi) = \varphi + 1$. Andererseits muß auch

$$E = \sigma^2(E) = \sigma(E + \varphi) = E + \varphi + \varphi + 1$$

gelten, was ein Widerspruch ist. Also gilt $\sigma(E) \neq E + \varphi$. Ebenso zeigt man $\sigma(E) \neq E + \varphi + 1$. Somit muß also $\sigma(E) = E$ oder $E + 1$ gelten. Daraus folgt $\sigma(D) = D$. Insgesamt erhalten wir die Aussage $D \in K$. Wäre nun $D' = 0$, so müßte $K(\varphi, E)/K$ unverzweigt sein, was im Widerspruch dazu steht, daß $G(K(\varphi, E)/K)$ isomorph zur Kleinschen Vierergruppe ist. □

6.2 Die Brauerzerlegung von $\pi^K_{\alpha,\beta}$

Für den gesamten Rest dieses Kapitels nehmen wir an, daß $G(L/K)$ nichtabelsch ist und die Gleichungen $[K(\varphi) : K] = 2$, $[K(\varphi,\gamma) : K(\varphi)] = 1$ sowie $[K(\varphi,E) : K(\varphi,\gamma)] = 2$ gelten, was gleichbedeutend ist mit der Bedingung f ungerade, $D \in K$ und $D' \neq 0$. Weiter wählen wir einen injektiven Charakter $\chi_{K(\varphi)}$ von $G(L/K(\varphi))$.

Lemma 6.2.1 *Die Darstellung $\pi^K_{\alpha,\beta}$ ist irreduzibel und besitzt den projektiven Typ D_2.*

Beweis: Weil $G(L/K)$ nichtabelsch ist, muß $\pi^K_{\alpha,\beta}$ irreduzibel sein. Außerdem darf die Galoisgruppe $G(K(\varphi,E)/K)$ nach 1.6.1 nicht zyklisch sein, womit als Isomorphietyp nur noch die Kleinsche Vierergruppe D_2 in Betracht kommt. □

Satz 6.2.2 *Es gilt $G(L/K) \cong D_4$ und $G(L/K(\varphi)) \cong \mathbb{Z}/4\mathbb{Z}$. Außerdem gilt*

$$\rho^K_{\alpha,\beta} \cong \mathrm{Ind}^K_{K(\varphi)}(\chi_{K(\varphi)}).$$

Beweis: Wir wissen, daß $G(L/K)$ die Ordnung 8 besitzt. Wegen $D \in K$ gilt $\sigma(E) = E$ oder $E+1$ für alle $\sigma \in G(L/K)$. Nach 2.2.8 gibt es $\sigma_1, \sigma_2 \in G(L/K)$ mit $\sigma_1(\varphi) = \varphi + 1$, $\sigma_1(E) = E$ und $\sigma_1(F_\alpha) = F_\alpha$ sowie $\sigma_2(\varphi) = \varphi$, $\sigma_2(E) = E+1$ und $\sigma_2(F_\alpha) = F_\alpha + E + \varphi$. Wenn wir $G(L/K)$ gemäß 2.3.3 mit einer Untergruppe von $GL_2(\mathbb{F}_3)$ identifizieren, so entsprechen σ_1 und σ_2 den Matrizen

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ und } \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

Damit lassen sich leicht die Relationen $\mathrm{ord}(\sigma_1) = 2$, $\mathrm{ord}(\sigma_2) = 4$ und $\sigma_1\sigma_2\sigma_1 = \sigma_2^{-1}$ verifizieren. Daraus folgt $G(L/K) \cong D_4$ und $G(L/K(\varphi)) \cong \mathbb{Z}/4\mathbb{Z}$. Nach [22, S. 37] gibt es (bis auf Isomorphie) nur eine irreduzible zweidimensionale Darstellung von $G(L/K)$, wobei diese von den beiden injektiven Charakteren von $G(L/K(\varphi))$ induziert wird. □

Wenn wir nun $\chi_{K(\varphi)}$ als Charakter von $W(K^{\mathrm{sep}}/K(\varphi))$ auffassen und beachten, daß Twist und Induktion vertauschen, erhalten wir das folgende Korollar.

Korollar 6.2.3 *Es gilt $\pi^K_{\alpha,\beta} \cong \mathrm{Ind}^K_{K(\varphi)}(\Omega^{-1}_{K(\varphi)}\chi_{K(\varphi)})$.*

6.3 Führer und minimale Twists

Für die folgenden Betrachtungen verwenden wir die in 4.5 definierten Elemente ϵ und δ der unverzweigten Erweiterung von $K(\varphi,\gamma)$ vom Grad 4. Wegen $D \in K$ gilt $\gamma' = 0$, und wir können $\delta = D$ annehmen.

Satz 6.3.1 *Wir setzen*

$$a := \sqrt{\frac{((\delta+1)\epsilon+\alpha)'}{\delta'}}.$$

Dann gilt

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = 2 - 2\nu_K((\delta+1) + a + a^2) - 2\nu_K(\delta').$$

Beweis: Nach 4.5.10 gilt

$$\begin{aligned}\mathrm{cond}(\pi^K_{\alpha,\beta}) &= 2 + \frac{4(\mathrm{d}(L/K(\varphi,E)) - \nu_{K(\varphi)}((\varphi\gamma)') - 1)}{\mathrm{e}(L/K)} \\ &= 1 + \mathrm{d}(L/K(\varphi,E)) - \nu_{K(\varphi)}((\varphi\gamma)').\end{aligned}$$

Die Anwendung von 4.5.3 und 4.6.2 liefert

$$\nu_{K(\varphi)}((\varphi\gamma)') = \nu_K(\delta')$$

und

$$\mathrm{d}(L/K(\varphi)) = 1 - 2\nu_K(\delta + 1 + a + a^2) - \nu_K(\delta').$$

Daraus folgt

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = 2 - 2\nu_K(\delta + 1 + a + a^2) - 2\nu_K(\delta').$$

□

Korollar 6.3.2 *Es gilt* $\mathrm{cond}(\pi^K_{\alpha,\beta}) \geq 2 - 4\nu_K((\varphi\gamma)')$.

Beweis: Wegen

$$\nu_K(\delta + 1 + a + a^2) = \nu_K(\delta + (a + \varphi) + (a + \varphi)^2) \leq \nu_K(\delta')$$

folgt

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) \geq 2 - 4\nu_K(\delta').$$

Beachtet man nun noch, daß nach 4.5.3 die Identität $(\varphi\gamma)' = \delta'$ gilt, so erhält man die gewünschte Ungleichung. □

Satz 6.3.3 *Für den minimalen Führer gilt*

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 2 - 2\nu_K((\varphi\gamma)').$$

Beweis: Nach 1.6.5 gilt $\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 2\mathrm{cond}_{K(\varphi)/K}(\chi_{K(\varphi)})$. Um den relativen Führer zu berechnen, betrachten wir den konjugierten Charakter $\chi^\sigma_{K(\varphi)} : G(L/K(\varphi)) \longrightarrow \mathbb{C}^*$. Weil $\chi_{K(\varphi)}$ injektiv ist, muß auch $\chi^\sigma_{K(\varphi)}$ injektiv sein. Weil $G(L/K)$ nicht abelsch ist, muß außerdem $\chi_{K(\varphi)} \neq \chi^\sigma_{K(\varphi)}$ gelten. Bei einer zyklischen Gruppe der Ordnung 4 unterscheiden sich die beiden injektiven Charaktere gerade um den Charakter, dessen Kern die eindeutig bestimmten Untergruppe der Ordnung 2 ist. Daraus folgt $\mathrm{Kern}(\chi_{K(\varphi)}(\chi^\sigma_{K(\varphi)})^{-1}) = G(L/K(\varphi, E))$. Wir können also $\chi_{K(\varphi)}(\chi^\sigma_{K(\varphi)})^{-1}$ als Charakter von $G(K(\varphi, E)/K(\varphi))$ auffassen. Nach 4.2.1 und 4.3.5 folgt

$$\mathrm{cond}_{K(\varphi)/K}(\chi_{K(\varphi)}) = \mathrm{d}(K(\varphi, E)/K(\varphi)) = 1 - \nu_K(\delta').$$

Hieraus erhält man wegen $(\varphi\gamma') = \delta'$ die gewünschte Formel. □

Das folgende Korollar ist eine unmittelbare Folgerung.

Korollar 6.3.4 *Es gilt* $\mathrm{cond}(\pi^K_{\alpha,\beta}) > \mathrm{cond}_{\min}(\pi^K_{\alpha,\beta})$.

Der minimale Führer kann also nicht durch quadratischen Twist realisiert werden.

6.4 Berechnung von ϵ-Faktoren

Satz 6.4.1 *Für jeden Charakter* χ *von* $W(K^{\mathrm{sep}}/K)$ *gilt*

$$\epsilon(\chi \otimes \pi^K_{\alpha,\beta}, \psi_K, d_{\psi_K}) = \epsilon(\mathrm{Res}^{K(\varphi)}_K(\chi)\Omega^{-1}_{K(\varphi)}\chi_{K(\varphi)}, \psi_{K(\varphi)}, d_{\psi_{K(\varphi)}}x).$$

Beweis: Nach 5.4.1 gilt

$$\lambda(K(\varphi)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(\varphi)}}x) = 1.$$

Durch Anwendung von 1.5.2 und 6.2.3 erhalten wir

$$\begin{aligned}\epsilon(\chi \otimes \pi^K_{\alpha,\beta}, \psi_K, d_{\psi_K}x) &= \epsilon(\chi \otimes \mathrm{Ind}^K_{K(\varphi)}(\Omega^{-1}_{K(\varphi)}\chi_{K(\varphi)}), \psi_K, d_{\psi_K}x) \\ &= \epsilon(\mathrm{Res}^{K(\varphi)}_K(\chi)\Omega^{-1}_{K(\varphi)}\chi_{K(\varphi)}, \psi_{K(\varphi)}, d_{\psi_{K(\varphi)}}x).\end{aligned}$$

□

Kapitel 7

Verzweigt induzierte elliptische Kurven vom D_2-Typ

In diesem gesamten Kapitel nehmen wir an, daß $[K(\varphi) : K] = 1$ und $[K(\varphi, \gamma) : K(\varphi)] = 1$ ist. Dies ist gleichbedeutend damit, daß f gerade ist und γ in K liegt.

7.1 Charakterisierung von β

Satz 7.1.1 *Wir nehmen $D \notin K$ an. Dann gibt es $\sigma_1, \sigma_2 \in G(L/K)$ mit $\sigma_1(\varphi) = \varphi$, $\sigma_1(E) = E+1$ und $\sigma_1(F_\alpha) = F_\alpha + E + \varphi$ sowie $\sigma_2(\varphi) = \varphi$, $\sigma_2(E) = E + \varphi$ und $\sigma_2(F_\alpha) = F_\alpha + (\varphi + 1)E$. Es gelten die Relationen $\mathrm{ord}(\sigma_1) = 4$, $\mathrm{ord}(\sigma_2) = 4$ und $\sigma_2\sigma_1\sigma_2^{-1} = \sigma_1^3$.*

Beweis: Es gilt $E \notin K(D)$ nach 2.4.4. Gemäß 2.4.1 folgt $F_\alpha \notin K(E)$. Also ist $[L : K] = 8$. Für alle $\sigma \in G(L/K)$ gilt $\sigma(\varphi) = \varphi$ und $\sigma(\gamma) = \gamma$. Aus letzterem folgt $\sigma(E) = E$, $E + 1$, $E + \varphi$ oder $E+\varphi+1$. Mit der Tabelle von 2.2.8 lassen sich leicht die acht Automorphismen auffinden, die diesen Bedingungen genügen. Hierunter befinden sich offensichtlich auch die gesuchten Automorphismen σ_1 und σ_2. Wenn wir $G(L/K)$ gemäß 2.3.3 mit einer Untergruppe von $GL_2(\mathbb{F}_3)$ identifizieren, so entsprechen die Automorphismen σ_1 und σ_2 den Matrizen

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ und } \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}.$$

Hiermit lassen sich die angegebenen Relationen leicht nachprüfen. □

Korollar 7.1.2 *Die Galoisgruppe $G(L/K)$ ist genau dann nichtabelsch, wenn $D \notin K$ gilt. In diesem Fall gelten die Isomorphien $G(K(E)/K) \cong D_2$ und $G(L/K(D)) \cong \mathbb{Z}/4\mathbb{Z}$*

Beweis: Damit $G(L/K)$ nichtabelsch sein kann, muß L/K den maximalen Grad 8 haben. Dies geht nur, wenn $D \notin K$ ist. Damit erhält man die Äquivalenz der Bedingungen $G(L/K)$ nichtabelsch und $D \notin K$. Wir nehmen nun $D \notin K$ an und wählen σ_1, σ_2 wie im obigen Satz. Dann gilt

$$\sigma_1(D) = E + 1 + (E + 1)^2 = D.$$

Daraus folgt $G(L/K(D)) =< \sigma_1 > \cong \mathbb{Z}/4\mathbb{Z}$. Weil $K(E)/K$ neben $K(D)/K$ auch noch die Zwischenerweiterungen $K(D_\varphi)/K$ und $K(D_{\varphi^2})/K$ besitzt, kann $G(K(E)/K)$ nicht zyklisch sein. Daraus folgt $G(K(E)/K) \cong D_2$. □

7.2 Die Brauerzerlegung von $\pi^K_{\alpha,\beta}$

Wir nehmen nun den Fall $D \notin K$ für den Rest dieses Kapitels an, so daß $G(L/K)$ nichtabelsch der Ordnung 8 ist. Weiter wählen wir einen injektiven Charakter $\chi_{K(D)}$ von $G(L/K(D))$. Schließlich sei $\sigma \in G(L/K)$ ein Automorphismus, dessen Einschränkung auf $K(D)$ nicht trivial ist. Für die folgenden Betrachtungen benötigen wir den konjugierten Charakter

$$\begin{aligned} \chi^\sigma_{K(D)} : G(L/K(D)) &\longrightarrow \mathbb{C}^* \\ g &\longmapsto \chi_{K(D)}(\sigma^{-1} g \sigma). \end{aligned}$$

Lemma 7.2.1 *Es gilt* $\mathrm{Kern}(\chi_{K(D)}(\chi^\sigma_{K(D)})^{-1}) = G(L/K(E))$.

Beweis: Wir bemerken zunächst, daß $G(L/K(E))$ die eindeutig bestimmte Untergruppe von $G(L/K(D))$ der Ordnung 2 ist. Weil $\chi_{K(D)}$ injektiv ist, muß auch $\chi^\sigma_{K(D)}$ injektiv sein. Wäre nun $\chi^\sigma_{K(D)} = \chi_{K(D)}$, so müßte σ wegen der Injektivität von $\chi_{K(D)}$ mit allen $g \in G(L/K(D))$ kommutieren. Dies steht im Widerspruch dazu, daß $G(L/K)$ nichtabelsch ist. Also gilt $\chi^\sigma_{K(D)} \neq \chi_{K(D)}$. Weil nun die beiden injektiven Charaktere von $\mathbb{Z}/4\mathbb{Z}$ auf der eindeutig bestimmten Untergruppe der Ordnung 2 übereinstimmen, folgt die Aussage des Lemmas. □

Korollar 7.2.2 *Es gilt* $\rho^K_{\alpha,\beta} \cong \mathrm{Ind}^K_{K(D)}(\chi_{K(D)})$.

Beweis: Nach dem Kriterium von Mackey folgt die Irreduzibilität von $\mathrm{Ind}^K_{K(D)}(\chi_{K(D)})$. Weil eine Gruppe der Ordnung 8 bis auf Isomorphie höchstens eine irreduzible zweidimensionale Darstellung haben kann, folgt die gewünschte Isomorphie. □

Wenn wir $\chi_{K(D)}$ als Charakter von $W(K^{\mathrm{sep}}/K(D))$ auffassen und beachten, daß Twist und Induktion vertauschen, erhalten wir das folgende Korollar.

Korollar 7.2.3 *Es gilt* $\pi^K_{\alpha,\beta} \cong \mathrm{Ind}^K_{K(D)}(\Omega^{-1}_{K(D)}\chi_{K(D)})$.

Korollar 7.2.4 *Die Darstellung* $\pi^K_{\alpha,\beta}$ *ist genau dann unverzweigt induziert, wenn* $\gamma' = 0$ *ist.*

Beweis: Wenn $\gamma' = 0$ ist, so ist $K(D)/K$ unverzweigt und $\pi^K_{\alpha,\beta}$ unverzweigt induziert. Im Fall $\gamma' \neq 0$ ist $K(D)/K$ verzweigt. Nach 4.5.9 muß $K(E)/K(D)$ verzweigt sein. Die Anwendung von 4.6.5 liefert die Verzweigtheit von $L/K(E)$. Somit ist L/K voll verzweigt, was zur Folge hat, daß $\pi^K_{\alpha,\beta}$ nicht unverzweigt induziert sein kann. □

7.3 Führer und minimale Twists

Für die folgenden Betrachtungen verwenden wir die in 4.5 definierten Elemente ϵ und δ der unverzweigten Erweiterung von $K(\varphi,\gamma)$ vom Grad 4.

Lemma 7.3.1 *Im Fall* $\gamma' = 0$ *gilt* $\delta' \neq 0$.

Beweis: Wäre $\delta' = 0$, so müßte $K(E)/K$ unverzweigt vom Grad 4 sein. Damit wäre $G(K(E)/K)$ isomorph zu $\mathbb{Z}/4\mathbb{Z}$, was im Widerspruch zu 7.1.2 steht. □

Im Spezialfall $\gamma' = 0$ können wir bei der Berechnung des Führers genauso vorgehen wie unter 6.3. Wir beschränken uns darauf, die Ergebnisse anzugeben.

Satz 7.3.2 *Wir nehmen $\gamma' = 0$ an und setzen*

$$a := \sqrt{\frac{((\delta+1)\epsilon+\alpha)'}{\delta'}}.$$

Dann gilt

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = 2 - 2\nu_K((\delta+1)+a+a^2) - 2\nu_K(\delta').$$

Korollar 7.3.3 *Im Fall $\gamma' = 0$ gilt* $\mathrm{cond}(\pi^K_{\alpha,\beta}) \geq 2 - 4\nu_K((\varphi\gamma)')$.

Satz 7.3.4 *Im Fall $\gamma' \neq 0$ gilt*

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = 1 - \nu_K((\varphi\gamma)') + \frac{\mathrm{d}(L/K(E)) - \nu_K(\gamma') + 1}{2}.$$

Beweis: Nach 4.5.10 gilt

$$\begin{aligned}\mathrm{cond}(\pi^K_{\alpha,\beta}) &= 2 + \frac{4(\mathrm{d}(L/K(E)) - \nu_K(\gamma') - 2\nu_K((\varphi\gamma)') - 1)}{\mathrm{e}(L/K)} \\ &= 2 + \frac{4(\mathrm{d}(L/K(E)) - \nu_K(\gamma') - 2\nu_K((\varphi\gamma)') - 1)}{8} \\ &= 1 - \nu_K((\varphi\gamma)') + \frac{\mathrm{d}(L/K(E)) - \nu_K(\gamma') + 1}{2}.\end{aligned}$$

Korollar 7.3.5 *Im Fall $\gamma' \neq 0$ gilt*

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) \geq 2 - 4\nu_K((\varphi\gamma)') + \nu_K(\gamma').$$

Beweis: Durch Anwendung von 4.6.6 erhält man

$$\begin{aligned}\mathrm{cond}(\pi^K_{\alpha,\beta}) &\geq 1 - \nu_K((\varphi\gamma)') + \frac{1 - 3\nu_K(\frac{(\varphi\gamma)'(\varphi^2\gamma)'}{\gamma'}) - \nu_K(\gamma') + 1}{2} \\ &= 2 - \nu_K((\varphi\gamma)') + \frac{-6\nu_K((\varphi\gamma)') + 2\nu_K(\gamma')}{2} \\ &= 2 - 4\nu_K((\varphi\gamma)') + \nu_K(\gamma').\end{aligned}$$

Satz 7.3.6 *Für den minimalen Führer gilt*

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = \begin{cases} 2 - 2\nu_K((\varphi\gamma)'), & \textit{falls } \gamma' = 0 \\ 2 - \nu_K(\gamma') - 2\nu_K((\varphi\gamma)'), & \textit{falls } \gamma' \neq 0. \end{cases}$$

Beweis: Wir bestimmen zunächst den relativen Führer von $\chi_{K(D)}$. Nach 7.2.1 hat der Charakter $\chi_{K(D)}(\chi^\sigma_{K(D)})^{-1}$ den Kern $G(L/K(E))$. Damit können wir $\chi_{K(D)}(\chi^\sigma_{K(D)})^{-1}$ auch als Charakter von $G(K(E)/K(D))$ auffassen. Nach 4.2.1 und gilt

$$\mathrm{cond}_{K(D)/K}(\chi_{K(D)}) = \mathrm{d}(K(E)/K(D)).$$

Unter Anwendung von 7.2.4 und 1.6.5 erhalten wir

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = \begin{cases} 2\mathrm{d}(K(E)/K(D)), & \text{falls } \gamma' = 0 \\ 2\mathrm{d}(K(D)/K) + \mathrm{d}(K(E)/K(D)) - 1, & \text{falls } \gamma' \neq 0. \end{cases}$$

Im Fall $\gamma' = 0$ liefern 4.5.1 und 4.5.3 das Ergebnis

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 2 - 2\nu_K(\delta') = 2 - \nu_K((\varphi\gamma)').$$

Im Fall $\gamma' \neq 0$ erhalten wir

$$\begin{aligned}\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) &= 2(1 - \nu_K(\gamma')) + 1 - \nu_K(\frac{(\varphi\gamma)'(\varphi^2\gamma)'}{\gamma'}) - 1 \\ &= 2 - \nu_K(\gamma') - 2\nu_K((\varphi\gamma)').\end{aligned}$$

□

Hier sehen wir, daß im Fall $\gamma' = 0$ der minimale Führer nicht durch quadratischen Twist realisiert werden kann. Im Fall $\gamma' \neq 0$ und $\nu_K(\gamma') > \nu_K((\varphi\gamma)')$ erhalten wir

$$\begin{aligned}\mathrm{cond}(\pi^K_{\alpha,\beta}) - \mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) &= 2 - 4\nu_K((\varphi\gamma)') + \nu_K(\gamma') - (2 - \nu_K(\gamma') - 2\nu_K((\varphi\gamma)')) \\ &= 2\nu_K(\gamma') - 2\nu_K((\varphi\gamma)') \\ &> 0.\end{aligned}$$

Also kann der minimale Führer in diesem Fall ebenfalls nicht durch quadratischen Twist realisiert werden.

7.4 Berechnung von ϵ-Faktoren

Im Spezialfall $\gamma' = 0$ können wir bei der Berechnung von $\epsilon(\pi^K_{\alpha,\beta}, \psi_K, d_{\psi_K})$ genauso vergehen wie unter 6.4, wenn wir nur $K(\varphi)$ durch $K(D)$ ersetzen. Wir geben nur das Ergebnis an.

Satz 7.4.1 *Im Fall $\gamma' = 0$ gilt für jeden Charakter χ von $W(K^{\mathrm{sep}}/K)$ die Gleichung*

$$\epsilon(\chi \otimes \pi^K_{\alpha,\beta}, \psi_K, d_{\psi_K}) = \epsilon(\mathrm{Res}^{K(D)}_K(\chi)\Omega^{-1}_{K(D)}\chi_{K(D)}, \psi_{K(D)}, d_{\psi_{K(D)}}x).$$

Um nun den allgemeinen Fall $\gamma' \neq 0$ zu behandeln, müssen wir uns mit der Berechnung von λ-Faktoren beliebiger quadratischer Erweiterungen befassen.

Satz 7.4.2 *Sei $M := \mathbb{F}_r((T))$ ein lokaler Körper der Charakteristik 2, dessen Restkörper r Elemente hat. Weiter sei $a \in M$ mit $a' \neq 0$ und χ_a der eindeutig bestimmte Charakter von $W(M^{\mathrm{sep}}/M)$ mit $\mathrm{Kern}(\chi_a) = W(K^{\mathrm{sep}}/M_a)$. Wir setzen $n := \frac{1}{2}(1-\nu_M(a'))$. Wenn wir χ_a vermöge der modifizierten Artinabbildung als Charakter von M^* auffassen, so gilt*

$$\chi_a(1+x) = \psi_M(\frac{a'}{T}x)$$

für alle $x \in \mathfrak{p}^n_M$.

Beweis: Für alle $x \in M^*$ ist

$$\chi_a(x) = \begin{cases} 1, & \text{falls } x \in \mathrm{N}^M_{M_a}(M_a^*) \\ -1, & \text{Falls } x \notin \mathrm{N}^M_{M_a}(M_a^*). \end{cases}$$

Damit erhalten wir $\chi_a(x) = (-1)^{\{a,x\}}$, wobei $\{\cdot,\cdot\}$ das spezielle Normenrestsymbol im Sinne von [20, §3] ist, dessen Wert wir als die Zahl 0 oder 1 auffassen. Nach 4.3.4 gibt es $b_0 \in \mathbb{F}_{r^2}$ und $b_1 \in M$ mit $a = a' + b_0 + b_1 + (b_0 + b_1)^2$.Wir setzen nun $a^* := a' + b_0 + b_0^2$. Dann gilt $a = a^* + b_1 + b_1^2$ und damit $M_a = M_{a^*}$. Hieraus ergibt sich

$$\chi_a(x) = (-1)^{\{a^*,x\}}$$

für alle $x \in M^*$. Nach [20] gilt die Formel

$$\{a^*, x\} = \mathrm{Tr}^{\mathbb{F}_2}_{\mathbb{F}_r}\left(\mathrm{res}(a^*\frac{\mathrm{d}x}{x})\right),$$

wobei $\mathrm{res}(a^*\frac{\mathrm{d}x}{x})$ das Residuum des Differntials $a^*\frac{\mathrm{d}x}{x}$ bezeichnet. Sei nun $x = \sum_{i=n}^{\infty} x_i T^i \in \mathfrak{p}_M$ mit $x_n, x_{n+1}, \cdots \in \mathbb{F}_r$. Wir setzen

$$x_u := \sum_{i=n}^{\infty}{}' x_i T^i,$$

wobei das Zeichen $\sum'$ bedeutet, daß nur über ungerade Indizes summiert werden soll. Dann gilt

$$\mathrm{d}(1+x) = \sum_{i=n}^{\infty} x_i i T^{i-1} \mathrm{d}T = \sum_{i=n}^{\infty}{}' x_i T^{i-1} \mathrm{d}T = \frac{x_u}{T}\mathrm{d}T.$$

Daraus folgt

$$\begin{aligned}
\chi_a(1+x) &= (-1)^{\mathrm{Tr}_{\mathbb{F}_r}^{\mathbb{F}_2}\left(\mathrm{res}(a^* \frac{x_u}{T(1+x)}\mathrm{d}T)\right)} \\
&= \psi_M(a^* \frac{x_u}{T(1+x)}) \\
&= \psi_M(a' \frac{x_u}{T(1+x)} + (b_0 + b_0^2)\frac{x_u}{T(1+x)}) \\
&= \psi_M(a' \frac{x_u}{T(1+x)}).
\end{aligned}$$

Wegen

$$\nu_M(a'\frac{x_u}{T}) = \nu_M(a') + \nu_M(x_u) - 1 = -2n + \nu_M(x_u) \geq -n$$

gilt

$$a' \frac{x_u}{T(1+x)} \equiv a' \frac{x_u}{T} \mod \mathfrak{p}_M^0.$$

Hieraus ergibt sich

$$\chi_a(1+x) = \psi_M(a'\frac{x_u}{T}).$$

Bei der Laurententwicklung von $a' \frac{x_u+x}{T}$ in T verschwinden alle ungeraden Koeffizienten. Damit erhalten wir

$$\chi_a(1+x) = \psi_M(a'\frac{x_u}{T} + a'\frac{x_u+x}{T}) = \psi_M(a'\frac{x}{T}).$$

□

Korollar 7.4.3 *Sei $M := \mathbb{F}_r((T))$ ein lokaler Körper der Charakteristik 2, dessen Restkörper r Elemente hat. Weiter sei $a \in M$ mit $a' \neq 0$ und χ_a der eindeutig bestimmte Charakter von $W(M^{\mathrm{sep}}/M)$ mit $\mathrm{Kern}(\chi_a) = W(M^{\mathrm{sep}}/M_a)$. Wir setzen $n := \frac{1}{2}(1 - \nu_M(a'))$. Dann gilt*

$$\epsilon(\chi_a, \psi_M, d_{\psi_M} x) = r^n.$$

Beweis: Zunächst bemerken wir, daß $\mathrm{cond}(\chi_a) = 2n$ und $\mathrm{cond}(\psi_M) = 0$ gilt. Nach 1.5.5 erhalten wir

$$\mid \epsilon(\chi_a, \psi_M, d_{\psi_M} x) \mid = r^n.$$

Wir bestimmen nun die Wurzelzahl. Nach 1.5.2 gilt

$$\epsilon(\chi_a, \psi_M, d_{\psi_M} x) = \int_{T^{-2n}\mathcal{O}_M^*} \chi_a^{-1}(x)\psi_M(x)\, d_{\psi_M} x.$$

Nach [10, Kap 7.7] gilt

$$\begin{aligned}
\int_{T^{-2n}\mathcal{O}_M^*} \chi_a^{-1}(x)\psi_M(x)\, d_{\psi_M} x &= \omega_M(T^{-2n}) \int_{\mathcal{O}_M^*} \chi_a^{-1}(\frac{x}{T^{2n}})\psi_M(\frac{x}{T^{2n}})\, d_{\psi_M} x \\
&= r^{2n} \int_{\mathcal{O}_M^*} \chi_a^{-1}(x)\psi_M(\frac{x}{T^{2n}})\, d_{\psi_M} x.
\end{aligned}$$

Damit erhalten wir für die Wurzelzahl die Gleichung

$$W(\chi_a, \psi_M) = \frac{\int_{\mathcal{O}_M^*} \chi_a^{-1}(x)\psi_M(\frac{x}{T^{2n}})\, d_{\psi_M} x}{\left|\int_{\mathcal{O}_M^*} \chi_a^{-1}(x)\psi_M(\frac{x}{T^{2n}})\, d_{\psi_M} x\right|}.$$

Die Anwendung von 7.4.2 und [14, Lemma 8.1] liefert

$$\begin{aligned} W(\chi_a, \psi_M) &= \psi_M(\frac{a'T^{2n-1}}{T^{2n}})\chi_a^{-1}(a'T^{2n-1}) \\ &= \psi_M(\frac{a'}{T})\chi_a^{-1}(\frac{a'}{T}). \end{aligned}$$

Man beachte nun, daß bei der Laurentententwicklung von $\frac{a'}{T}$ alle ungeraden Koeffizienten verschwinden. Daraus folgt $\psi_M(\frac{a'}{T}) = 1$. Weil $\frac{a'}{T}$ ein Quadrat ist, muß auch $\chi_a(\frac{a'}{T}) = 1$ sein. Insgesamt erhalten wir so die Aussage des Korollars. □

Korollar 7.4.4 *Sei $M := \mathbb{F}_r((T))$ ein lokaler Körper der Charakteristik 2, dessen Restkörper r Elemente hat. Weiter sei $a \in M$ mit $a' \neq 0$. Dann gilt*

$$\lambda(M_a/M, \psi_M, d_{\psi_M}, d_{\psi_{M_a}}) = r^{1-\nu_M(a')}.$$

Beweis: Wir setzen $n := \frac{1}{2}(1 - \nu_M(a'))$. Weiter sei χ_a der eindeutig bestimmte Charakter von $W(M^{\text{sep}}/M)$ mit $\text{Kern}(\chi_a) = W(M^{\text{sep}}/M_a)$. Dann gilt

$$\begin{aligned} \lambda(M_a/M, \psi_M, d_{\psi_M}, d_{\psi_{M_a}}) &= \frac{\epsilon(\text{Ind}_{M_a}^M(1_{M_a}), \psi_M, d_{\psi_M}x)}{\epsilon(1_{M_a}, \psi_{M_a}, d_{\psi_{M_a}}x)} \\ &= \frac{\epsilon(1_M \oplus \chi_a, \psi_M, d_{\psi_M}x)}{\epsilon(1_{M_a}, \psi_{M_a}, d_{\psi_{M_a}}x)} \\ &= \frac{\epsilon(1_M, \psi_M, d_{\psi_M}x)\epsilon(\chi_a, \psi_M, d_{\psi_M}x)}{\epsilon(1_{M_a}, \psi_{M_a}, d_{\psi_{M_a}}x)}. \end{aligned}$$

Hierbei ist

$$\epsilon(1_M, \psi_M, d_{\psi_M}x) = \omega_M^{-1}(1)\int_{\mathcal{O}_M} 1 d_{\psi_M}x = 1$$

und

$$\epsilon(\chi_a, \psi_M, d_{\psi_M}x) = r^n.$$

Wir bestimmen jetzt den Führer von $\psi_{M_a} = \psi_M \circ \text{Tr}_{M_a}^M$. Indem wir 1.5.3 und 4.3.5 anwenden erhalten wir

$$\text{cond}(\psi_{M_a}) = \text{cond}(\psi_M) - \text{d}(M_a/M) = -2n.$$

Nach 1.5.2 folgt

$$\begin{aligned} \epsilon(1_{M_a}, \psi_{M_a}, d_{\psi_{M_a}}x) &= \omega_{M_a}^{-1}(T^{2n})\int_{\mathcal{O}_M} 1\, d_{\psi_{M_a}}x \\ &= r^{2n}r^n \\ &= r^{3n}. \end{aligned}$$

Insgesamt erhalten wir

$$\lambda(M_a/M, \psi_M, d_{\psi_M}, d_{\psi_{M_a}}) = r^{2n} = r^{1-\nu_M(a')}.$$

□

Korollar 7.4.5 *Wir setzen $n := 1 - \nu_K(\gamma')$. Dann gilt für jeden Charakter χ von $W(K^{\text{sep}}/K)$ die Gleichung*

$$\epsilon(\chi \otimes \pi_{\alpha,\beta}^K, \psi_K, d_{\psi_K}) = 2^{fn}\epsilon(\text{Res}_K^{K(D)}(\chi)\Omega_{K(D)}^{-1}\chi_{K(D)}, \psi_{K(D)}, d_{\psi_{K(D)}}x).$$

Beweis: Unter Anwendung von 1.5.2 und 7.2.3 erhalten wir

$$\begin{aligned}\epsilon(\chi \otimes \pi^K_{\alpha,\beta}, \psi_K, d_{\psi_K} x) &= (2^f)^n \epsilon(\chi \otimes \mathrm{Ind}^K_{K(D)}(\Omega^{-1}_{K(D)}\chi_{K(D)}), \psi_K, d_{\psi_K} x) \\ &= 2^{fn}\epsilon(\mathrm{Res}^{K(D)}_K(\chi)\Omega^{-1}_{K(D)}\chi_{K(D)}, \psi_{K(D)}, d_{\psi_{K(D)}} x).\end{aligned}$$

□

Kapitel 8

Verzweigt induzierte elliptische Kurven vom D_4-Typ

In diesem Kapitel befassen wir uns mit dem Fall, daß $[K(\varphi), K] = 2$, $[K(\varphi,\gamma), K(\varphi)] = 1$ und $[K(\varphi, E), K(\varphi,\gamma)] = 4$ ist.

8.1 Charakterisierung von β

Lemma 8.1.1 *Sei f ungerade. Dann gilt die Bedingung $[K(\varphi,\gamma), K(\varphi)] = 1$ genau dann, wenn es ein $\tilde{\gamma} \in K$ gibt mit $\beta = \tilde{\gamma}^3$.*

Beweis: Wenn es ein $\tilde{\gamma} \in K$ gibt mit $\beta = \tilde{\gamma}^3$, so gilt $\gamma \in \{\tilde{\gamma}, \varphi\tilde{\gamma}, \varphi^2\tilde{\gamma}\}$ und $[K(\varphi,\gamma) : K(\varphi)] = 1$. Wir nehmen nun an, daß $[K(\varphi,\gamma), K(\varphi)] = 1$ ist. Dann ist $\nu_K(\beta)$ durch 3 teilbar. Also gibt es ein $l \in \mathbb{Z}$ mit $\nu_K(\beta T^{3l}) = 0$. Sei nun $\beta_0 \in \mathbb{F}_{2^f}$ mit

$$\beta T^{3l} \equiv \beta_0 \mod (T).$$

Nach 5.1.2 gibt es ein $\gamma_0 \in \mathbb{F}_{2^f}$ mit $\beta_0 = \gamma_0^3$. Aus dem Lemma von Hensel folgt, daß βT^{3l} und damit auch β selbst eine dritte Potenz in K ist. □

Wir erinnern an die Bezeichnung $Q(K) := \{x + x^2 \mid x \in K\}$.

Satz 8.1.2 *Die Bedingung $[K(\varphi), K] = 2$, $[K(\varphi,\gamma), K(\varphi)] = 1$ und $[K(\varphi, E), K(\varphi,\gamma)] = 4$ gilt genau dann, wenn f ungerade ist und es ein $\tilde{\gamma} \in K$ gibt mit $\beta = \tilde{\gamma}^3$ und $\tilde{\gamma}, \tilde{\gamma} + 1 \notin Q(K)$.*

Beweis: Sei $[K(\varphi), K] = 2$, $[K(\varphi,\gamma), K(\varphi)] = 1$ und $[K(\varphi, E), K(\varphi,\gamma)] = 4$. Dann ist f ungerade. Außerdem gibt es ein $\tilde{\gamma} \in K$ gibt mit $\beta = \tilde{\gamma}^3$. Daraus folgt $\tilde{\gamma} = \gamma, \varphi\gamma$ oder $\varphi^2\gamma$. Läge nun $\tilde{\gamma}$ oder $\tilde{\gamma} + 1$ in $Q(K)$, so hätte man $\tilde{\gamma} \in Q(K(\varphi))$. Damit läge eines der Elemente D,D_φ, D_{φ^2} in $K(\varphi)$. Dies steht im Widerspruch zur Bedingung $[K(\varphi, E), K(\varphi,\gamma)] = 4$. Also gilt $\tilde{\gamma}, \tilde{\gamma} + 1 \notin Q(K)$.

Wir nehmen nun an, daß f ungerade ist und es ein $\tilde{\gamma} \in K$ gibt mit $\beta = \tilde{\gamma}^3$ und $\tilde{\gamma}, \tilde{\gamma}+1 \notin Q(K)$. Dann gilt $[K(\varphi), K] = 2$. Wäre nun $\tilde{\gamma} \in Q(K(\varphi))$, so gäbe es $a, b \in K$ mit

$$\begin{aligned}\tilde{\gamma} &= a + b\varphi + (a + b\varphi)^2 \\ &= (b + b^2)\varphi + a + a^2 + b^2.\end{aligned}$$

Hieraus ergäbe sich $b + b^2 = 0$ und $\tilde{\gamma} = a + a^2 + b^2$. Die erste Gleichung liefert $b = 0$ oder $b = 1$. Damit kann dann allerdings die zweite Gleichung wegen $\tilde{\gamma}, \tilde{\gamma} + 1 \notin Q(K)$ nicht erfüllt sein. Also gilt $\tilde{\gamma} \notin K(\varphi)$. Wäre nun $\varphi\tilde{\gamma} \in Q(K(\varphi))$, so gäbe es $a, b \in K$ mit

$$\begin{aligned}\varphi\tilde{\gamma} &= a + b\varphi + (a + b\varphi)^2 \\ &= (b + b^2)\varphi + a + a^2 + b^2.\end{aligned}$$

Daraus folgte $\tilde{\gamma} = b + b^2$, was wegen $\tilde{\gamma} \notin Q(K)$ nicht sein kann. Also gilt $\varphi\tilde{\gamma} \notin K(\varphi)$. Analog dazu zeigt man $\varphi^2\tilde{\gamma} \notin K(\varphi)$. Wegen $\gamma \in \{\tilde{\gamma}, \varphi\tilde{\gamma}, \varphi^2\tilde{\gamma}\}$ erhält man $\gamma \notin Q(K(\varphi))$. Daraus folgt $D \notin K(\varphi) = K(\varphi, \gamma)$ und somit $[K(\varphi, E) : K(\varphi, \gamma)] = 4$. □

8.2 Die Brauerzerlegung von $\pi^K_{\alpha,\beta}$

Für den gesamten Rest dieses Kapitels nehmen wir $[K(\varphi) : K] = 2$, $[K(\varphi, \gamma) : K(\varphi)] = 1$ und $[K(\varphi, E) : K(\varphi, \gamma)] = 4$ an. Außerdem wählen wir gemäß 8.1.2 ein $\tilde{\gamma}$ in K mit $\beta = \tilde{\gamma}^3$ und $\tilde{\gamma}, \tilde{\gamma} + 1 \notin Q(K)$. Weiter sei $k \in \{0, 1, 2\}$ mit $\tilde{\gamma} = \varphi^k\gamma$. Wir setzen $\tilde{E} := \varphi^k E$, $\tilde{D} := \tilde{E} + \tilde{E}^2$ und $\tilde{F_\alpha} := F_\alpha + (\varphi + 1)E$. Dann gilt

$$\tilde{D} + \tilde{D}^2 = \varphi^k E + (\varphi^k E)^4 = \varphi^k(E + E^4) = \tilde{\gamma}.$$

und

$$\begin{aligned}
\tilde{F_\alpha} + \tilde{F_\alpha}^2 &= F_\alpha + F_\alpha^2 + (\varphi^k + 1)E + ((\varphi^k + 1)E)^2 \\
&= (D + 1)E + \alpha + \varphi^k E + (\varphi^k E)^2 + E + E^2 \\
&= (E^2 + E + 1)E + \alpha + \tilde{E} + \tilde{E}^2 + E + E^2 \\
&= E^3 + \tilde{E} + \tilde{E}^2 + \alpha \\
&= (\varphi^k E)^3 + \tilde{E} + \tilde{E}^2 + \alpha \\
&= \tilde{E}^3 + \tilde{E}^2 + \tilde{E} + \alpha \\
&= (\tilde{D} + 1)\tilde{E} + \alpha.
\end{aligned}$$

Nach 2.2.4 und 2.2.7 gilt $K(\varphi, E) = K(\varphi, \tilde{E})$ und $L = K(\varphi, \tilde{E}, \tilde{F_\alpha})$.

Satz 8.2.1 *Es gibt $\sigma_1, \sigma_2 \in G(L/K)$ mit $\sigma_1(\varphi) = \varphi + 1$, $\sigma_1(\tilde{E}) = \tilde{E} + \varphi$ und $\sigma_1(\tilde{F_\alpha}) = \tilde{F_\alpha} + (\varphi + 1)\tilde{E}$ sowie $\sigma_2(\varphi) = \varphi + 1$, $\sigma_2(\tilde{E}) = \tilde{E}$ und $\sigma_2(\tilde{F_\alpha}) = \tilde{F_\alpha}$. Weiter gelten die Relationen $\mathrm{ord}(\sigma_1) = 8$, $\mathrm{ord}(\sigma_2) = 2$ und $\sigma_2\sigma_1\sigma_2 = \sigma_1^3$*

Beweis: Nach 2.4.1 gilt $[L : K(\varphi, E)] = 2$. Damit erhält man insgesamt $[L : K] = 16$. Für alle $\sigma \in G(L/K)$ gilt $\sigma(\tilde{\gamma}) = \tilde{\gamma}$. Daraus folgt $\sigma(\tilde{E}) = \tilde{E}$, $\tilde{E} + 1$, $\tilde{E} + \varphi$ oder $\tilde{E} + \varphi + 1$. Mit der Tabelle von 2.2.8 lassen sich die 16 Automorphismen finden, die diesen Bedingungen genügen. Hierunter befinden sich auch die Automorphismen σ_1 und σ_2. Wir ersetzen nun E durch $\tilde{E}$ sowie F_α durch $\tilde{F_\alpha}$ und identifizieren $G(L/K)$ gemäß 2.3.3 mit einer Untergruppe von $GL_2(\mathbb{F}_3)$. Dann entsprechen die Automorphismen σ_1 und σ_2 den Matrizen

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \text{ und } \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Hiermit lassen sich leicht die angegeben Relationen nachprüfen. □

Korollar 8.2.2 *Die Darstellung $\pi^K_{\alpha,\beta}$ ist irreduzibel und besitzt den projektiven Typ D_4.*

Beweis: Weil $G(L/K)$ offensichtlich nichtabelsch ist, folgt die Irreduzibilität von $\pi^K_{\alpha,\beta}$ nach 3.1.7. Die Galoisgruppe $G(K(\varphi, E)/K)$ des projektiven Kernkörpers hat die Ordnung 8. Nach 1.6.1 kommt nur D_4 als Isomorphietyp von $G(K(\varphi, E)/K)$ in Betracht. □

Wir fixieren die Automorphismen σ_1 und σ_2 aus 8.2.1. Wegen $\varphi + \tilde{D} + (\varphi + \tilde{D})^2 = \tilde{\gamma} + 1 \notin Q(K)$ hat $K(\tilde{D} + \varphi)/K$ den Grad 2 und $G(L/K(\tilde{D} + \varphi))$ die Ordnung 8. Weiter gilt

$$\sigma_1(\tilde{D} + \varphi) = \sigma_1(\tilde{E} + \tilde{E}^2 + \varphi) = \tilde{E} + \varphi + (\tilde{E} + \varphi)^2 + \varphi + 1 = \tilde{D} + \varphi,$$

woraus $\sigma_1 \in G(L/K(\tilde{D}+\varphi))$ folgt. Mit $\chi_{K(\tilde{D}+\varphi)}$ bezeichnen wir den eindeutig bestimmten Charakter von $G(L/K(\tilde{D}+\varphi))$, für den $\chi_{K(\tilde{D}+\varphi)}(\sigma_1) = e^{\frac{1}{4}\pi i}$ gilt.

Satz 8.2.3 *Es gilt* $\rho^K_{\alpha,\beta} \cong \mathrm{Ind}^K_{K(\tilde{D}+\varphi)}(\chi_{K(\tilde{D}+\varphi)})$.

Beweis: Weil $\pi^K_{\alpha,\beta}$ irreduzibel ist, muß auch $\rho^K_{\alpha,\beta}$ irreduzibel sein. Für jede ganze Zahl h definieren wir den Charakter χ_h von $G(L/K(\tilde{D}+\varphi))$ durch $\chi_h(\sigma_1) = e^{\frac{h}{4}\pi i}$. Mit dieser Bezeichnung gilt $\chi_{K(\tilde{D}+\varphi)} = \chi_1$. Wir definieren weiter den zu χ_h konjugierten Charakter $\chi_h^{\sigma_2}$ von $G(L/K(\tilde{D}+\varphi))$ durch die Bedingung $\chi_h^{\sigma_2}(\sigma) = \chi_h(\sigma_2^{-1}\sigma\sigma_2)$ für alle $\sigma \in G(L/K(\tilde{D}+\varphi))$. Durch Anwendung von 8.2.1 erhalten wir $\chi_h^{\sigma_2} = \chi_{3h}$. Nach dem Kriterium von Mackey ist $\mathrm{Ind}^K_{K(\tilde{D}+\varphi)}(\chi_h)$ genau dann irreduzibel, wenn $\chi_h \neq \chi_h^{\sigma_2}$ ist. Diese Bedingung gilt z. B. für $h = 1$, 2 oder 5. Nach [22, Chap. 7, Prop. 22] gilt die Formel

$$\mathrm{Tr}(\mathrm{Ind}^K_{K(\tilde{D}+\varphi)}(\chi_h)(\sigma_1)) = \chi_h(\sigma_1) + \chi_h^{\sigma_2}(\sigma_1) = e^{\frac{h}{4}\pi i} + e^{\frac{3h}{4}\pi i}.$$

Daraus folgt

$$\mathrm{Tr}(\mathrm{Ind}^K_{K(\tilde{D}+\varphi)}(\chi_1)(\sigma_1)) = \sqrt{2}i$$

sowie

$$\mathrm{Tr}(\mathrm{Ind}^K_{K(\tilde{D}+\varphi)}(\chi_2)(\sigma_1)) = 0$$

und

$$\mathrm{Tr}(\mathrm{Ind}^K_{K(\tilde{D}+\varphi)}(\chi_5)(\sigma_1)) = -\sqrt{2}.$$

Also sind die induzierten Darstellungen von χ_1, χ_2 und χ_5 paarweise nichtisomorph. Weil eine Gruppe der Ordnung 16 höchstens drei nichtisomorphe zweidimensionale Darstellungen besitzen kann, muß sich $\rho^K_{\alpha,\beta}$ unter diesen induzierten Darstellungen befinden. Ein Blick auf die Tabelle von 3.4.3 liefert $\mathrm{Tr}(\rho^K_{\alpha,\beta}(\sigma_1)) = \sqrt{2}i$. Damit ist der Satz bewiesen. □

Wenn wir $\chi_{K(\tilde{D}+\varphi)}$ als Charakter von $W(K^{\mathrm{sep}}/K(\tilde{D}+\varphi))$ auffassen und beachten, daß Twist und Induktion vertauschen, erhalten wir das folgende Korollar.

Korollar 8.2.4 *Es gilt* $\pi^K_{\alpha,\beta} \cong \mathrm{Ind}^K_{K(\tilde{D}+\varphi)}(\Omega^{-1}_{K(\tilde{D}+\varphi)}\chi_{K(\tilde{D}+\varphi)})$.

Satz 8.2.5 *Die Darstellung* $\pi^K_{\alpha,\beta}$ *ist verzweigt induziert.*

Beweis: Wir müssen lediglich zeigen, daß es keinen Charakter von $G(L/K(\varphi))$ gibt, der $\rho^K_{\alpha,\beta}$ induziert. Wenn wir K durch $K(\varphi)$ ersetzen, können wir 7.1.2 anwenden und erhalten das Ergebnis, daß $G(L/K(\varphi))$ nichtabelsch ist. Folglich können die Elemente von $G(L/K(\varphi))$ nur die Ordnung 1, 2 oder 4 haben. Angenommen, es gäbe einen Charakter χ von $G(L/K(\varphi))$ mit $\rho^K_{\alpha,\beta} \cong \mathrm{Ind}^K_{K(\varphi)}(\chi)$. Dann kann χ nur die Werte 1, -1, i und $-i$ annehmen. Die Anwendung von [22, Chap. 7, Prop. 20] liefert die Aussage, daß $\mathrm{Tr}(\rho^K_{\alpha,\beta}(\sigma_1))$ eine $\mathbb{Q}$-Linearkombination von $\{1, i\}$ sein muß. Dies steht im Widerspruch zu 3.4.3, wonach $\mathrm{Tr}(\rho^K_{\alpha,\beta}(\sigma_1)) = \sqrt{2}i$ gilt. □

8.3 Führer und minimale Twists

Lemma 8.3.1 *Es gilt* $\gamma' \neq 0$.

Beweis: Wäre $\gamma' = 0$, so müßte $K(\varphi, D)/K$ unverzweigt vom Grad 4 sein. Folglich wäre die Erweiterung $K(\varphi, D)/K$ eine Galoiserweiterung mit zyklischer Galoisgruppe der Ordnung 4 und $G(K(\varphi, E)/K(\varphi, D))$ ein Normalteiler von $G(K(\varphi, E)/K)$ der Ordnung 2. Wegen der Isomorphie

$$G(K(\varphi, D)/K) \cong G(K(\varphi, E)/K)/G(K(\varphi, E)/K(\varphi, D))$$

müßte $G(K(\varphi,E)/K)$ ein Element der Ordnung 4 besitzen, das mit dem Erzeuger der Untergruppe $G(K(\varphi,E)/K(\varphi,D))$ kommutiert und dessen erste 3 Potenzen alle nicht in $G(K(\varphi,E)/K(\varphi,D))$ liegen. Folglich würde $G(K(\varphi,E)/K)$ von zwei miteinander kommutierenden Elementen erzeugt. Dies ist ein Widerspruch zur Nichtkommutativität von $G(K(\varphi,E)/K)$. □

Lemma 8.3.2 *Die Gruppe $<\sigma_1^2>$ ist der einzige Normalteiler von $G(L/K)$ der Ordnung 4.*

Beweis: Wegen $\mathrm{ord}(\sigma_1)=8$ gilt $\#<\sigma_1^2>=4$. Außerdem ist

$$\sigma_2<\sigma_1^2>\sigma_2^{-1}=<\sigma_1^6>=<\sigma_1^2>.$$

Hieraus folgt, daß $<\sigma_1^2>$ ein Normalteiler ist.

Sei nun H ein Normalteiler von $G(L/K)$ der Ordnung 4. Dann ist die Faktorgruppe aus Kardinalitätsgründen abelsch. Folglich enthält H den Kommutator. Insbesondere gilt

$$\sigma_1^2=\sigma_2\sigma_1\sigma_2^{-1}\sigma_1^{-1}\in H.$$

Daraus folgt $H=<\sigma_1^2>$. □

Korollar 8.3.3 *Es gilt $\nu_{K(\varphi)}(\gamma')=\nu_{K(\varphi)}(\tilde{\gamma}')$.*

Beweis: Im Fall $\tilde{\gamma}=\gamma$ gilt die Aussage trivialerweise. Deshalb nehmen wir $\tilde{\gamma}=\varphi\gamma$ oder $\tilde{\gamma}=\varphi^2\gamma$ an. Nach 4.5.8 erhalten wir

$$\nu_{K(\varphi)}(\tilde{\gamma})=\nu_{K(\varphi)}((\varphi\gamma)')=\nu_{K(\varphi)}((\varphi^2\gamma)').$$

Weiter gilt $\sigma_1^2(\varphi)=\varphi$ und $\sigma_1^2(\tilde{E})=\sigma_1(\tilde{E}+\varphi)=\tilde{E}+1$. Nach 4.1.6 und 4.5.4 folgt

$$\begin{aligned}\mathrm{i}_{L/K}(\sigma_1^2)&=\mathrm{d}(K(\tilde{E})/K(\tilde{D}))\\&=1-\nu_{K(\varphi)}\left(\frac{(\varphi\tilde{\gamma})'(\varphi^2\tilde{\gamma})'}{\tilde{\gamma}'}\right)\\&=1-\nu_{K(\varphi)}(\gamma').\end{aligned}$$

Wir benutzen die Abkürzungen $r:=1-\nu_{K(\varphi)}(\gamma')$ und $s:=1-2\nu_{K(\varphi)}((\varphi\gamma)')+\nu_{K(\varphi)}(\gamma')$. Dann gilt $\mathrm{i}_{L/K}(\sigma_1^2)=r$.

Wäre nun $\nu_{K(\varphi)}(\gamma')>\nu_{K(\varphi)}(\tilde{\gamma}')$, so hätte man $r<s$. Die Anwendung von 4.1.12 und 4.5.9 lieferte die Isomorphie $G_r(L/K)\cong\mathbb{Z}/4\mathbb{Z}$. Weil $G_r(L/K)$ nach [21, Chap. IV, Prop. 1] ein Normalteiler von $G(L/K)$ ist, müßte $G_r(L/K)=<\sigma_1^2>$ und somit $\mathrm{i}_{L/K}(\sigma_1^2)>r$ gelten, was ein Widerspruch ist. Also ist $\nu_{K(\varphi)}(\gamma')\le\nu_{K(\varphi)}(\tilde{\gamma}')$. Wegen 4.5.7 folgt $\nu_{K(\varphi)}(\gamma')=\nu_{K(\varphi)}(\tilde{\gamma}')$. □

Falls $\nu_{K(\varphi)}(\gamma')>\nu_{K(\varphi)}((\varphi\gamma)')$ ist, folgt $\tilde{\gamma}=\gamma$. Im Fall $\nu_{K(\varphi)}(\gamma')=\nu_{K(\varphi)}((\varphi\gamma)')$ können wir γ durch $\tilde{\gamma}$ ersetzen, ohne gegen 4.5.7 zu verstoßen. Wir können also ohne Einschränkung annehmen, daß $\tilde{\gamma}=\gamma$ ist.

Satz 8.3.4 *Für den Führer gilt*

$$\mathrm{cond}(\pi_{\alpha,\beta}^K)=1-\nu_{K(\varphi)}((\varphi\gamma)')+\frac{\mathrm{d}(L/K(\varphi,E))-\nu_{K(\varphi)}(\gamma')+1}{2}.$$

Beweis: Nach 4.5.10 gilt

$$\begin{aligned}\mathrm{cond}(\pi_{\alpha,\beta}^K)&=2+\frac{4(\mathrm{d}(L/K(E,\varphi))-\nu_{K(\varphi)}(\gamma')-2\nu_{K(\varphi)}((\varphi\gamma)')-1)}{\mathrm{e}(L/K)}\\&=2+\frac{4(\mathrm{d}(L/K(E,\varphi))-\nu_{K(\varphi)}(\gamma')-2\nu_{K(\varphi)}((\varphi\gamma)')-1)}{8}\\&=1-\nu_{K(\varphi)}((\varphi\gamma)')+\frac{\mathrm{d}(L/K(E))-\nu_{K(\varphi)}(\gamma')+1}{2}.\end{aligned}$$

□

Korollar 8.3.5 *Es gilt*

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) \geq 2 - 4\nu_{K(\varphi)}((\varphi\gamma)') + \nu_{K(\varphi)}(\gamma').$$

Beweis: Durch Anwendung von 4.6.6 erhält man

$$\begin{aligned}\mathrm{cond}(\pi^K_{\alpha,\beta}) &\geq 1 - \nu_{K(\varphi)}((\varphi\gamma)') + \frac{1 - 3\nu_{K(\varphi)}(\frac{(\varphi\gamma)'(\varphi^2\gamma)'}{\gamma'}) - \nu_{K(\varphi)}(\gamma') + 1}{2} \\ &= 2 - \nu_{K(\varphi)}((\varphi\gamma)') + \frac{-6\nu_{K(\varphi)}((\varphi\gamma)') + 2\nu_{K(\varphi)}(\gamma')}{2} \\ &= 2 - 4\nu_{K(\varphi)}((\varphi\gamma)') + \nu_{K(\varphi)}(\gamma').\end{aligned}$$

□

Für die weiteren Betrachtungen benötigen wir den konjugierten Charakter

$$\begin{aligned}\chi^{\sigma_2}_{K(\tilde{D}+\varphi)} : G(L/K(\tilde{D}+\varphi)) &\longrightarrow \mathbb{C}^* \\ \sigma &\longmapsto \chi_{K(\tilde{D}+\varphi)}(\sigma_2^{-1}\sigma\sigma_2).\end{aligned}$$

Lemma 8.3.6 *Es gilt*

$$\mathrm{Kern}\left(\chi_{K(\tilde{D}+\varphi)}(\chi^{\sigma_2}_{K(\tilde{D}+\varphi)})^{-1}\right) = G(L/K(\varphi,E)).$$

Beweis: Die Anwendung von 8.2.1 liefert

$$\chi^{\sigma_2}_{K(\tilde{D}+\varphi)}(\sigma_1) = \chi_{K(\tilde{D}+\varphi)}(\sigma_2^{-1}\sigma_1\sigma_2) = \chi_{K(\tilde{D}+\varphi)}(\sigma_1^3).$$

Daraus folgt

$$\left(\chi_{K(\tilde{D}+\varphi)}(\chi^{\sigma_2}_{K(\tilde{D}+\varphi)})^{-1}\right)(\sigma_1) = \chi_{K(\tilde{D}+\varphi)}(\sigma_1^{-2}) = e^{\frac{3\pi}{2}i}.$$

Hieraus ergibt sich

$$\mathrm{Kern}\left(\chi_{K(\tilde{D}+\varphi)}(\chi^{\sigma_2}_{K(\tilde{D}+\varphi)})^{-1}\right) = \{\sigma_1^4, \mathrm{id}_L\}.$$

Weil $K(\varphi,E)/K(\tilde{D}+\varphi)$ die eindeutig bestimmte Zwischenerweiterung vom Grad 4 der zyklischen Erweiterung $L/K(\tilde{D}+\varphi)$ ist, folgt die Aussage des Lemmas. □

Satz 8.3.7 *Für den relativen Führer gilt*

$$\mathrm{cond}_{K(\tilde{D}+\varphi)/K}(\chi_{K(\tilde{D}+\varphi)}) = \mathrm{d}(K(\tilde{E})/K(\tilde{D})).$$

Beweis: Wir können

$$\chi_{K(\tilde{D}+\varphi)}\left(\chi^{\sigma}_{K(\tilde{D}+\varphi)}\right)^{-1}$$

als injektiven Charakter der Galoisgruppe $G(K(\varphi,E)/K(\tilde{D}+\varphi))$ auffassen. Diese Galoisgruppe ist zyklisch der Ordnung 4 und wird erzeugt von $\tilde{\sigma_1} := \sigma_1|_{K(\varphi,E)}$. Die eindeutig bestimmte quadratische Zwischenerweiterung lautet $K(\varphi,\tilde{D})$ und ist unverzweigt, während $K(\varphi,E)/K(\varphi,\tilde{D})$

verzweigt ist. Die Anwendung von [21, Chap. IV, Prop. 2 und 4] liefert

$$\begin{aligned}
\mathrm{cond}_{K(\tilde{D}+\varphi)/K}(\chi_{K(\tilde{D}+\varphi)}) &= \mathrm{cond}\left(\chi_{K(\tilde{(}D)+\varphi)}\left(\chi^{\sigma}_{K(\tilde{D}+\varphi)}\right)^{-1}\right)\\
&= \sum_{i=0}^{\infty}\frac{\#G_i(K(\varphi,E)/K(\tilde{D}+\varphi))}{\#G_0(K(\varphi,E)/K(\tilde{D}+\varphi))}\dim\mathbb{C}^{G_i(K(\varphi,E)/K(\tilde{D}+\varphi))}\\
&= \sum_{i=0}^{\infty}\frac{\#G_i(K(\varphi,E)/K(\varphi,\tilde{D}))}{2}\dim\mathbb{C}^{G_i(K(\varphi,E)/K(\varphi,\tilde{D}))}\\
&= \sum_{i=0}^{\mathrm{i}_{K(\varphi,E)/K(\varphi,\tilde{D})}(\tilde{\sigma}_1)-1}\frac{\#G_i(K(\varphi,E)/K(\varphi,\tilde{D}))}{2}\\
&= \sum_{i=0}^{\mathrm{i}_{K(\varphi,E)/K(\varphi,\tilde{D})}(\tilde{\sigma}_1)-1}1\\
&= \mathrm{i}_{K(\varphi,E)/K(\varphi,\tilde{D})}(\tilde{\sigma_1})\\
&= \mathrm{d}(K(\varphi,E)/K(\varphi,\tilde{D}))\\
&= \mathrm{d}(K(\tilde{E})/K(\tilde{D})).
\end{aligned}$$

□

Korollar 8.3.8 *Für den minimalen Führer gilt*

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 2-\nu_{K(\varphi)}(\gamma')-2\nu_{K(\varphi)}((\varphi\gamma)').$$

Beweis: Nach 1.6.5 gilt

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 2\mathrm{d}(K(\tilde{D}+\varphi)/K)+\mathrm{d}(K(\tilde{E})/K(\tilde{D}))-1.$$

Die Anwendung von 4.3.5 und 4.5.4 liefert die Ergebnisse

$$\mathrm{d}(K(\tilde{D}+\varphi)/K) = \mathrm{d}(K(\tilde{D})/K) = 1-\nu_{K(\varphi)}((\tilde{\gamma})')$$

und

$$\mathrm{d}(K(\tilde{E})/K(\tilde{D})) = 1-\nu_{K(\varphi)}\left(\frac{(\varphi\tilde{\gamma})'(\varphi^2\tilde{\gamma})'}{\tilde{\gamma}'}\right).$$

Insgesamt erhält man

$$\begin{aligned}
\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) &= 2(1-\nu_{K(\varphi)}(\tilde{\gamma}))+1-\nu_{K(\varphi)}\left(\frac{(\varphi\tilde{\gamma})'(\varphi^2\tilde{\gamma})'}{\tilde{\gamma}'}\right)-1\\
&= 2-\nu_{K(\varphi)}(\tilde{\gamma})-\nu_{K(\varphi)}((\varphi\tilde{\gamma})')-\nu_{K(\varphi)}((\varphi^2\tilde{\gamma})')\\
&= 2-\nu_{K(\varphi)}(\gamma')-\nu_{K(\varphi)}((\varphi\gamma)')-\nu_{K(\varphi)}((\varphi^2\gamma)')\\
&= 2-\nu_{K(\varphi)}(\gamma')-2\nu_{K(\varphi)}((\varphi\gamma)').
\end{aligned}$$

□

8.4 Berechnung von ϵ-Faktoren

Satz 8.4.1 *Wir setzen $n := 1-\nu_K(\tilde{\gamma}')$. Für jeden Charakter χ von $W(K^{\mathrm{sep}}/K)$ gilt*

$$\epsilon(\chi\otimes\pi^K_{\alpha,\beta},\psi_K,d_{\psi_K}x) = 2^{fn}\epsilon(\mathrm{Res}^{K(\tilde{D}+\varphi)}_K(\chi)\Omega^{-1}_{K(\tilde{D}+\varphi)}\chi_{K(\tilde{D}+\varphi)},\psi_{K(\tilde{D}+\varphi)},d_{\psi_{K(\tilde{D}+\varphi)}}x).$$

Beweis: Nach 7.4.4 gilt

$$\lambda(K(\tilde{D}+\varphi)/K, \psi_K, d_{\psi_K}, d_{\psi_{K(\tilde{D}+\varphi)}}) = 2^{fn}.$$

Damit erhalten wir

$$\begin{aligned}\epsilon(\chi \otimes \pi^K_{\alpha,\beta}, \psi_K, d_{\psi_K} x) &= 2^{fn}\epsilon(\chi \otimes \mathrm{Ind}^K_{K(\tilde{D}+\varphi)}(\Omega^{-1}_{K(\tilde{D}+\varphi)}\chi_{K(\tilde{D}+\varphi)}), \psi_K, d_{\psi_K} x) \\ &= 2^{fn}\epsilon(\mathrm{Res}^{K(\tilde{D}+\varphi)}_K(\chi)\Omega^{-1}_{K(\tilde{D}+\varphi)}\chi_{K(\tilde{D}+\varphi)}, \psi_{K(\tilde{D}+\varphi)}, d_{\psi_{K(\tilde{D}+\varphi)}} x).\end{aligned}$$

□

Kapitel 9

Primitive elliptische Kurven vom A_4-Typ

In diesem Kapitel befassen wir uns mit dem Fall $[K(\varphi) : K] = 1$, $[K(\varphi,\gamma) : K(\varphi)] = 3$ und $[K(\varphi,E) : K(\varphi,\gamma)] = 4$.

9.1 Charakterisierung von β

Wir erinnern an die Bezeichnung $Q(K) := \{x + x^2 \mid x \in K\}$.

Satz 9.1.1 *Es gilt genau dann $[K(\varphi) : K] = 1$, $[K(\varphi,\gamma) : K(\varphi)] = 3$ und $[K(\varphi,E) : K(\varphi,\gamma)] = 4$, wenn f gerade ist und für jede dritte Wurzel $\tilde{\gamma}$ von β die Bedingungen $\tilde{\gamma} \notin K$ und $\tilde{\gamma} \notin Q(K(\tilde{\gamma}))$ erfüllt sind.*

Beweis: Zunächst nehmen wir an, daß f gerade ist und für jede dritte Wurzel $\tilde{\gamma}$ die Bedingungen $\tilde{\gamma} \notin K$ und $\tilde{\gamma} \notin Q(K(\tilde{\gamma}))$ erfüllt sind. Dann gilt $[K(\varphi) : K] = 1$. Außerdem ist $\gamma \notin K$ und $\gamma \notin Q(K(\gamma))$. Daraus folgt $[K(\varphi,\gamma) : K(\varphi)] = 3$ und $D \notin K(\varphi)$. Wegen 2.4.4 erhält man $[K(\varphi,E) : K(\varphi,\gamma)] = 4$.

Wir nehmen nun $[K(\varphi) : K] = 1$, $[K(\varphi,\gamma) : K(\varphi)] = 3$ und $[K(\varphi,E) : K(\varphi,\gamma)] = 4$ an. Dann ist f ungerade, und die dritten Wurzeln $\gamma, \varphi\gamma, \varphi^2\gamma$ liegen alle außerhalb von K. Für $i = 1, 2, 3$ gilt

$$\varphi^i\gamma = \varphi^i(E + E^4) = \varphi^i E + (\varphi^i E)^4 = \varphi^i E + (\varphi^i E)^2 + (\varphi^i E + (\varphi^i E)^2)^2.$$

Wäre nun $\varphi^i\gamma \in Q(K(\gamma))$, so läge $\varphi^i E + (\varphi^i E)^2$ in $K(\gamma)$. Dies ist mit $[K(\varphi,E) : K(\varphi,\gamma)] = 4$ unvereinbar. Also liegt keine dritte Wurzel von β in $Q(K(\gamma))$. □

9.2 Die Brauerzerlegung von $\pi^K_{\alpha,\beta}$

Für den Rest des Kapitels nehmen wir an, daß $[K(\varphi) : K] = 1$, $[K(\varphi,\gamma) : K(\varphi)] = 3$ und $[K(\varphi,E) : K(\varphi,\gamma)] = 4$ gilt. Nach 2.4.1 ist $[L : K(\varphi,E)] = 2$, so daß L/K den Grad 24 hat. Weil $SL_2(\mathbb{F}_3)$ die einzige Untergruppe von $GL_2(\mathbb{F}_3)$ der Ordnung 24 ist, können wir $G(L/K)$ mit $SL_2(\mathbb{F}_3)$ identifizieren.

Satz 9.2.1 *Die Darstellung $\pi_{\alpha,\beta}$ ist primitiv mit projektivem Typ A_4.*

Beweis: Nach 2.2.4 ist der projektive Kernkörper $K(\varphi,E) = K(E)$ der Zerfällungskörper des Polynoms $X^4 + X^3 + \beta$ über K. Folglich läßt sich $G(K(E)/K)$ als Untergruppe von S_4 auffassen. Wegen $[K(E) : K] = 12$ muß es sich dabei um eine Untergruppe vom Index 2 handeln. Weil A_4

die einzige Untergruppe von S_4 vom Index 2 ist, hat $\pi_{\alpha,\beta}$ den Typ A_4. Daß $\pi_{\alpha,\beta}$ primitiv ist, folgt aus 1.6.2. □

Wir erinnern daran, daß $x_1 := (D+1)E$ ist.

Lemma 9.2.2 *Es gilt* $[K(x_1) : K] = 4$.

Beweis: Nach 2.2.3 ist x_1 Nullstelle des Polynoms $f := X^4+X^3+\beta$. Daraus folgt $[K(x_1) : K] \leq 4$. Wäre nun $[K(x_1) : K] < 4$, so müßte f reduzibel sein. Damit könnte der Zerfällungskörper von f über K höchstens den Grad 6 haben. Nach 2.2.4 lautet dieser Zerfällungskörper $K(E)$. Wegen $[K(E) : K] = 12$ erhalten wir einen Widerspruch. Also gilt $[K(x_1) : K] = 4$. □

Lemma 9.2.3 *Es gilt* $G(L/K(x_1)) \cong \mathbb{Z}/6\mathbb{Z}$. *Dabei wird* $G(L/K(x_1))$ *erzeugt von einem Automorphismus* σ_1 *mit* $\sigma_1(\varphi) = \varphi$, $\sigma_1(E) = \varphi E + \varphi + 1$ *und* $\sigma_1(F_\alpha) = F_\alpha + 1$.

Beweis: Wegen $K(\varphi) = K$ gilt $\sigma(\varphi) = \varphi$ für alle $\sigma \in G(L/K)$. Mit Hilfe der Tabelle von 2.2.8 lassen sich leicht die 24 Elemente von $G(L/K)$ beschreiben. Hierunter befindet sich auch ein Automorphismus σ_1 mit $\sigma_1(E) = \varphi E + \varphi + 1$ und $\sigma_1(F_\alpha) = F_\alpha + 1$. Nach der Tabelle von 2.3.3 entspricht σ_1 der Matrix

$$\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}.$$

Weil es sich hierbei um eine obere Dreiecksmatrix handelt, folgt $\sigma_1 \in G(L/K(x_1))$ nach 2.3.4. Außerdem läßt sich leicht verifizieren, daß σ_1 die Ordnung 6 hat. Wegen $[K(x_1) : K] = 4$ gilt $[L : K(x_1)] = 6$. Daraus folgt $G(L/K(D)) =< \sigma_1 >$. □

Für die weiteren Betrachtungen sei $\chi_{K(D)}$ ein injektiver Charakter von $G(L/K(D))$ und $\chi_{K(x_1)}$ der eindeutig bestimmte Charakter von $G(L/K(x_1))$ mit $\chi_{K(x_1)}(\sigma_1) = -1$.

Satz 9.2.4 *Es gilt*

$$\rho^K_{\alpha,\beta} \oplus \mathrm{Ind}^K_{K(x_1)}(\chi_{K(x_1)}) \cong \mathrm{Ind}^K_{K(D)}(\chi_{K(D)}).$$

Beweis: (Vgl. [11, Lemma 5.1.1.]) Nach 7.2.2 gilt

$$\mathrm{Ind}^{K(\gamma)}_{K(D)}(\chi_{K(D)}) \cong \rho^{K(\gamma)}_{\alpha,\beta},$$

wobei $\rho^{K(\gamma)}_{\alpha,\beta}$ irreduzibel nach 7.1.2 und 3.1.7 ist. Im folgenden bezeichnen wir für jede Untergruppe G von $G(L/K)$ mit $(\cdot,\cdot)_G$ die Verkettungszahlen zweier Darstellungen von G. Sei θ ein Charakter von $G(L/K)$ mit $\mathrm{Kern}(\theta) = G(L/K(\gamma))$. Weil $K(\gamma)$ als Zerfällungskörper des Polynoms $X^3+\beta$ eine Galoiserweiterung ist, muß es einen solchen Charakter geben. Unter Anwendung der Frobeniusreziprozität erhalten wir die Aussage

$$\begin{aligned}\left(\theta^i \otimes \rho^K_{\alpha,\beta}, \mathrm{Ind}^K_{K(D)}(\chi_{K(D)})\right)_{G(L/K)} &= \left(\rho^{K(\gamma)}_{\alpha,\beta}, \mathrm{Ind}^{K(\gamma)}_{K(D)}(\chi_{K(D)})\right)_{G(L/K(\gamma))} \\ &= 1\end{aligned}$$

für $i = 0, 1$ und 2. Daraus folgt

$$\mathrm{Ind}^K_{K(D)}(\chi_{K(D)}) = \rho^K_{\alpha,\beta} \oplus (\theta \otimes \rho^K_{\alpha,\beta}) \oplus (\theta^2 \otimes \rho^K_{\alpha,\beta}).$$

Wegen $[K(x_1) : K] = 4$ und $[K(\gamma) : K] = 3$ müssen die Identitäten $K(x_1) \cap K(\gamma) = K$ und $[K(x_1)K(\gamma) : K] = 12$ gelten. Andererseits gilt $K(x_1), K(\gamma) \subset K(E)$ und $[K(E) : K] = 12$. Daraus folgt $K(x_1)K(\gamma) = K(E)$. Insgesamt erhalten wir die Identitäten

$$G(L/K(x_1))G(L/K(\gamma)) = G(L/K)$$

und

$$G(L/K(x_1)) \cap G(L/K(\gamma)) = G(L/K(E)).$$

Nach [22, Chap. 7, Prop. 22] gilt

$$\mathrm{Res}_K^{K(\gamma)}(\mathrm{Ind}_{K(x_1)}^K(\chi_{K(x_1)})) \cong \mathrm{Ind}_{K(E)}^{K(\gamma)}(\mathrm{Res}_{K(x_1)}^{K(E)}(\chi_{K(x_1)})).$$

Daraus folgt

$$\begin{aligned}\Big(\mathrm{Ind}_{K(D)}^K(\chi_{K(D)}), \mathrm{Ind}_{K(x_1)}^K(\chi_{K(x_1)})\Big)_{G(L/K)} &= \Big(\rho_{\alpha,\beta}^{K(\gamma)}, \mathrm{Ind}_{K(E)}^{K(\gamma)}(\mathrm{Res}_{K(x_1)}^{K(E)}(\chi_{K(x_1)}))\Big)_{G(L/K(\gamma))} \\ &= \Big(\rho_{\alpha,\beta}^{K(E)}, \mathrm{Res}_{K(x_1)}^{K(E)}(\chi_{K(x_1)})\Big)_{G(L/K(E))}.\end{aligned}$$

Weiter gilt $G(L/K(E)) =< \sigma_2 >$, wobei $\sigma_2(\varphi) = \varphi$, $\sigma_2(E) = E$ und $\sigma_2(F_\alpha) = F_\alpha + 1$ ist. Unter Anwendung von 3.4.3 erhalten wir

$$\begin{aligned}\Big(\mathrm{Ind}_{K(D)}^K(\chi_{K(D)}), \mathrm{Ind}_{K(x_1)}^K(\chi_{K(x_1)})\Big)_{G(L/K)} &= \frac{1}{2}\sum_{i=0}^{1} \mathrm{Tr}(\rho_{\alpha,\beta}^{K(E)}(\sigma_2^i))\overline{\chi_{K(x_1)}(\sigma_2^i)} \\ &= \frac{1}{2}(2 - 2(-1)) \\ &= 2.\end{aligned}$$

Also besitzen $\mathrm{Ind}_{K(D)}^K(\chi_{K(D)})$ und $\mathrm{Ind}_{K(x_1)}^K(\chi_{K(x_1)})$ zwei gemeinsame irreduzible Summanden.

Wäre $\rho_{\alpha,\beta}^K$ ein Summand von $\mathrm{Ind}_{K(x_1)}^K(\chi_{K(x_1)})$, so müßte

$$\Big(\rho_{\alpha,\beta}^K, \mathrm{Ind}_{K(x_1)}^K(\chi_{K(x_1)})\Big)_{G(L/K)} = \Big(\rho_{\alpha,\beta}^{K(x_1)}, \chi_{K(x_1)}\Big)_{G(L/K(x_1))} \neq 0$$

sein. Folglich gäbe es einen Charakter χ von $G(L/K(x_1))$ mit $\rho_{\alpha,\beta}^{K(x_1)} = \chi_{K(x_1)} \oplus \chi$. Unter Anwendung von 3.4.3 ergäbe sich daraus

$$\begin{aligned}\chi(\sigma_1) &= \mathrm{Tr}(\rho^{K(x_1)}(\sigma_1)) - \chi_{K(x_1)}(\sigma_1) \\ &= 1 - (-1) \\ &= 2.\end{aligned}$$

Weil dies ein Widerspruch ist, kann $\rho_{\alpha,\beta}^K$ kein Summand von $\mathrm{Ind}_{K(x_1)}^K(\chi_{K(x_1)})$ sein. Daraus folgt

$$\mathrm{Ind}_{K(x_1)}^K(\chi_{K(x_1)}) \cong (\theta \otimes \rho_{\alpha,\beta}^K) \oplus (\theta^2 \otimes \rho_{\alpha,\beta}^K).$$

Hieraus ergibt sich die Aussage des Satzes. □

Wenn wir $\chi_{K(D)}$ als Charakter der Weilgruppe $W(K^{\mathrm{sep}}/K(D))$ und $\chi_{K(x_1)}$ als Charakter von $W(K^{\mathrm{sep}}/K(x_1))$ auffassen, erhalten wir das folgende Korollar.

Korollar 9.2.5 *Es gilt*

$$\pi_{\alpha,\beta}^K \oplus \mathrm{Ind}_{K(x_1)}^K(\Omega_{K(x_1)}^{-1}\chi_{K(x_1)}) \cong \mathrm{Ind}_{K(D)}^K(\Omega_{K(D)}^{-1}\chi_{K(D)}).$$

9.3 Führer und minimale Twists

Lemma 9.3.1 *Es gilt $\gamma' \neq 0$.*

Beweis: Weil $G(K(E)/K) \cong A_4$ keine Elemente der Ordnung 4 hat, kann $G(K(E)/K(\gamma))$ nicht isomorph zu $\mathbb{Z}/4\mathbb{Z}$ sein. Folglich ist die Erweiterung $K(E)/K(\gamma)$ verzweigt. Wäre nun $\gamma' = 0$, so müßte $K(D)/K(\gamma)$ unverzweigt sein. Somit wäre $K(D)/K$ die maximale zahm verzweigte Zwischenerweiterung von $K(E)/K$ und müßte insbesondere eine Galoiserweiterung sein.

Wegen $(D + D^2)^3 = \beta$ und $[K(D) : K] = 6$ ist

$$f := (X^2 + X)^3 + \beta = X^6 + X^5 + X^4 + X^3 + \beta$$

das Minimalpolynom von D über K. Außerdem gilt $f(D_\varphi) = 0$ und $f(D_{\varphi^2}) = 0$. Folglich liegen D_φ und D_{φ^2} in der galoisschen Hülle von $K(D)/K$. Man beachte nun, daß

$$\varphi D_\varphi + \varphi^2 D_{\varphi^2} = \varphi(\varphi E + (\varphi E)^2) + \varphi^2(\varphi^2 E + (\varphi^2 E)^2) = \varphi^2 E + \varphi E = E$$

gilt. Wäre nun $K(D)/K$ eine Galoiserweiterung, so müßte auch E in $K(D)$ liegen, was wegen $[K(E) : K(\gamma)] = 4$ ein Widerspruch ist. Also gilt $\gamma' \neq 0$. □

Satz 9.3.2 *Es gilt $\nu_{K(\gamma)}(\gamma') = \nu_{K(\gamma)}((\varphi\gamma)')$.*

Beweis: Wäre $\nu_{K(\gamma)}(\gamma') > \nu_{K(\gamma)}((\varphi\gamma)')$, so ergäbe sich unter Anwendung von 4.5.9 die Ungleichung

$$\begin{aligned} \mathrm{d}(K(E)/K(D)) &= 1 - 2\nu_{K(\gamma)}((\varphi\gamma)') + \nu_{K(\gamma)}(\gamma') \\ &> 1 - \nu_{K(\gamma)}(\gamma') \\ &= \mathrm{d}(K(E)/K(D_\varphi)). \end{aligned}$$

Nach 4.1.12 folgte $G_r(L/K) \cong \mathbb{Z}/4\mathbb{Z}$ für $r := \mathrm{d}(K(E)/K(D))$. Andererseits ist $G_r(L/K)$ nach [21, Chap. IV, Prop. 1] ein Normalteiler von $G(L/K)$, und es gilt die Isomorphie $G(L/K) \cong SL_2(\mathbb{F}_3)$. Nach A.9 besitzt $SL_2(\mathbb{F}_3)$ aber keinen Normalteiler der Ordnung 4. Somit erhalten wir einen Widerspruch und damit die Aussage des Satzes.

Lemma 9.3.3 *Für die Körpererweiterung $K(\gamma)/K$ gilt*

$$\mathrm{e}(K(\gamma)/K) = \begin{cases} 1, & \textit{falls } 3 \mid \nu_K(\beta) \\ 3, & \textit{falls } 3 \nmid \nu_K(\beta). \end{cases}$$

Beweis: Dieser Sachverhalt folgt direkt aus 4.4.2. □

Korollar 9.3.4 *Für den Führer gilt*

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = \begin{cases} \frac{1}{2}(3 + \mathrm{d}(L/K(E)) - 3\nu_{K(\gamma)}(\gamma')), & \textit{falls } 3 \mid \nu_K(\beta) \\ \frac{1}{6}(11 + \mathrm{d}(L/K(E)) - 3\nu_{K(\gamma)}(\gamma')), & \textit{falls } 3 \nmid \nu_K(\beta). \end{cases}$$

Beweis: Wir wenden 4.5.10 an. Im Fall $3 \mid \nu_K(\beta)$ erhalten wir

$$\begin{aligned} \mathrm{cond}(\pi^K_{\alpha,\beta}) &= 2 + \frac{4(\mathrm{d}(L/K(E)) - \nu_{K(\gamma)}(\gamma') - 2\nu_{K(\gamma)}((\varphi\gamma)') - 1)}{\mathrm{e}(L/K)} \\ &= 2 + \frac{4(\mathrm{d}(L/K(E)) - 3\nu_{K(\gamma)}(\gamma') - 1)}{8} \\ &= \frac{3 + \mathrm{d}(L/K(E)) - 3\nu_{K(\gamma)}(\gamma')}{2}. \end{aligned}$$

Im Fall 3 $\not| \nu_K(\beta)$ gilt

$$\begin{aligned}\mathrm{cond}(\pi^K_{\alpha,\beta}) &= 2 + \frac{4(\mathrm{d}(L/K(E)) - \nu_{K(\gamma)}(\gamma') - 2\nu_{K(\gamma)}((\varphi\gamma)') - 1)}{\mathrm{e}(L/K)} \\ &= 2 + \frac{4(\mathrm{d}(L/K(E)) - 3\nu_{K(\gamma)}(\gamma') - 1)}{24} \\ &= \frac{11 + \mathrm{d}(L/K(E)) - 3\nu_{K(\gamma)}(\gamma')}{6}.\end{aligned}$$

□

Nun berechnen wir den minimalen Führer.

Satz 9.3.5 *Es gilt*

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 2 - \frac{3}{\mathrm{e}(K(\gamma)/K)}\nu_{K(\gamma)}(\gamma').$$

Beweis: Wir befassen uns zunächst mit den höheren Verzweigungsgruppen des projektiven Kernkörpers. Wegen $\gamma' \neq 0$ gilt $\#G_1(L/K) = 8$ nach 4.1.12 und 4.5.9. Aus Gradgründen muß $K(\gamma)/K$ die maximale zahm verzweigte Zwischenerweiterung von L/K und damit auch von $K(E)/K$ sein. Somit gilt $G_1(K(E)/K) = G(K(E)/K(\gamma))$. Für alle $\sigma \in G_1(K(E)/K) \setminus \{\mathrm{id}_{K(E)}\}$ muß

$$\gamma = \sigma(\gamma) = \sigma(E + E^4) = \sigma(E) + \sigma(E)^4$$

gelten. Daraus folgt $\sigma(E) \in \{E+1, E+\varphi, E+\varphi+1\}$. Damit lassen sich nun die 4 Elemente von $G_1(K(E)/K)$ vollständig beschreiben. Es gibt eindeutig bestimmte Elemente $\sigma_1, \sigma_2, \sigma_3$ von $G_1(K(E)/K) \setminus \{\mathrm{id}_{K(E)}\}$ mit $\sigma_1(E) = E+1$, $\sigma_2(E) = E+\varphi$ und $\sigma_3(E) = E+\varphi+1$. Nach 1.6.6 gilt

$$\begin{aligned}\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) &= 2 + \frac{3}{\mathrm{e}(K(\gamma)/K)} \max\left\{r \in \mathbb{N} \mid G_r(K(E))/K \neq \{\mathrm{id}_{K(E)}\}\right\} \\ &= 2 + \frac{3}{\mathrm{e}(K(\gamma)/K)} \left(\min\left\{r \in \mathbb{N} \mid G_r(K(E))/K = \{\mathrm{id}_{K(E)}\}\right\} - 1\right) \\ &= 2 + \frac{3}{\mathrm{e}(K(\gamma)/K)} \left(\max\left\{\mathrm{i}_{K(E)/K}(\sigma_1), \mathrm{i}_{K(E)/K}(\sigma_2), \mathrm{i}_{K(E)/K}(\sigma_3)\right\} - 1\right).\end{aligned}$$

Nach [21, Chap IV, Prop. 3] gilt

$$\mathrm{i}_{K(E)/K}(\sigma_i) = \frac{1}{2} \sum_{\substack{g \in G(L/K) \\ g|_{K(E)} = \sigma_i}} \mathrm{i}_{L/K}(g).$$

Die Anwendung von 4.1.6, 4.1.10 und 4.1.11 liefert

$$\begin{aligned}\mathrm{i}_{K(E)/K}(\sigma_1) &= \mathrm{d}(K(E)/K(D)), \\ \mathrm{i}_{K(E)/K}(\sigma_2) &= \mathrm{d}(K(E)/K(D_\varphi)), \\ \mathrm{i}_{K(E)/K}(\sigma_3) &= \mathrm{d}(K(E)/K(D_{\varphi^2})).\end{aligned}$$

Mit 4.5.9 erhalten wir

$$\begin{aligned}\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) &= 2 + \frac{3}{\mathrm{e}(K(\gamma)/K)} \left(-2\nu_{K(\gamma)}((\varphi\gamma)') + \nu_{K(\gamma)}(\gamma')\right) \\ &= 2 - \frac{3}{\mathrm{e}(K(\gamma)/K)}\nu_{K(\gamma)}(\gamma').\end{aligned}$$

□

Die Kombination von mit 9.3.5 und 9.3.3 liefert das folgende Korollar.

Korollar 9.3.6 *Es gilt*

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = \begin{cases} 2 - 3\nu_{K(\gamma)}(\gamma'), & \textit{falls } 3 \mid \nu_K(\beta) \\ 2 - \nu_{K(\gamma)}(\gamma'), & \textit{falls } 3 \nmid \nu_K(\beta). \end{cases}$$

9.4 Berechnung von ϵ-Faktoren

Satz 9.4.1 *Es gilt*

$$\lambda(K(D)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(D)}}x) = \lambda(K(x_1)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(x_1)}}x).$$

Beweis: (Vgl. [11, Lemma 5.1.3.].) Weil $K(\gamma)$ der Zerfällungskörper des Polynoms $X^3 + \beta$ über K ist, ist $K(\gamma)/K$ galoissch. Die Erweiterung $K(D)/K(\gamma)$ ist galoissch, weil sie den Grad 2 hat. Sei θ_K ein Charakter von $W(K^{\mathrm{sep}}/K)$ mit $\mathrm{Kern}(\theta_K) = W(K^{\mathrm{sep}}/K(\gamma))$ und $\theta_{K(\gamma)}$ der Charakter von $W(K^{\mathrm{sep}}/K(D))$ mit $\mathrm{Kern}(\theta_{K(\gamma)}) = W(K^{\mathrm{sep}}/K(D))$. Dann gilt

$$\begin{aligned} \mathrm{Ind}^K_{K(D)}(1_{K(D)}) &\cong \mathrm{Ind}^K_{K(\gamma)}(\mathrm{Ind}^{K(\gamma)}_{K(D)}(1_{K(D)})) \\ &\cong \mathrm{Ind}^K_{K(\gamma)}(1_{K(\gamma)} \oplus \theta_{K(\gamma)}) \\ &\cong \mathrm{Ind}^K_{K(\gamma)}(1_{K(\gamma)}) \oplus \mathrm{Ind}^K_{K(\gamma)}(\theta_{K(\gamma)}) \\ &\cong 1_K \oplus \theta_K \oplus \theta_K^2 \oplus \mathrm{Ind}^K_{K(\gamma)}(\theta_{K(\gamma)}). \end{aligned}$$

Wir fassen nun θ_K und $\mathrm{Ind}^K_{K(\gamma)}(\theta_{K(\gamma)})$ als Darstellungen von $G(K(E)/K) \cong A_4$ auf. Aufgrund der Frobeniusreziprozität gilt

$$\left(\theta_K^i, \mathrm{Ind}^K_{K(\gamma)}(\theta_{K(\gamma)})\right)_{G(K(E)/K)} = \left(1_{K(\gamma)}, \theta_{K(\gamma)}\right)_{G(K(E)/K(\gamma))} = 0$$

für $i = 0, 1$ und 2. Weil A_4 nur drei eindimensionale Darstellungen besitzt (siehe z. B. [22, Chap. 5.7]), folgt die Irreduzibilität von $\mathrm{Ind}^K_{K(\gamma)}(\theta_{K(\gamma)})$.

Wegen

$$G(K(E)/K(\gamma))G(K(E)/K(x_1)) = G(K(E)/K)$$

und

$$G(K(E)/K(\gamma)) \cap G(K(E)/K(x_1)) = \{\mathrm{id}_{K(E)}\}$$

gilt

$$\mathrm{Res}^{K(x_1)}_K(\mathrm{Ind}^K_{K(\gamma)}(\theta_{K(\gamma)})) \cong \mathrm{Ind}^{K(x_1)}_{K(E)}(\mathrm{Res}^{K(E)}_{K(\gamma)}(\theta_{K(\gamma)})) \cong \mathrm{Ind}^{K(x_1)}_{K(E)}(1_{K(E)})$$

nach [22, Chap. 7, Prop. 22]. Daraus folgt

$$\begin{aligned} \left(\mathrm{Ind}^K_{K(x_1)}(1_{K(x_1)}), \mathrm{Ind}^K_{K(\gamma)}(\theta_{K(\gamma)})\right)_{G(K(E)/K)} &= \left(1_{K(x_1)}, \mathrm{Ind}^{K(x_1)}_{K(E)}(1_{K(E)})\right)_{G(K(E)/K(x_1))} \\ &= \left(1_{K(E)}, 1_{K(E)}\right)_{\{\mathrm{id}_{K(E)}\}} \\ &= 1. \end{aligned}$$

Wegen

$$\left(\mathrm{Ind}^K_{K(x_1)}(1_{K(x_1)}), 1_K\right)_{G(K(E)/K)} = \left(1_{K(x_1)}, 1_{K(x_1)}\right)_{G(K(E)/K(x_1))} = 1$$

ergibt sich die Aussage

$$\mathrm{Ind}^K_{K(x_1)}(1_K(x_1)) \cong 1_K \oplus \mathrm{Ind}^K_{K(\gamma)}(\theta_{K(\gamma)}).$$

Insgesamt erhalten wir

$$\mathrm{Ind}^K_{K(D)}(1_{K(D)}) = \theta_K \oplus \theta_K^2 \oplus \mathrm{Ind}^K_{K(x_1)}(1_{K(x_1)}).$$

Daraus folgt

$$\begin{aligned}
&\frac{\lambda(K(D)/K,\psi_K,d_{\psi_K}x,d_{\psi_{K(D)}}x)}{\lambda(K(x_1)/K,\psi_K,d_{\psi_K}x,d_{\psi_{K(x_1)}}x)}\\
&\qquad=\frac{\epsilon(\mathrm{Ind}_{K(D)}^{K}(1_{K(D)}),\psi_K,d_{\psi_K}x)}{\epsilon(1_{K(D)},\psi_{K(D)},d_{\psi_{K(D)}x})}\,\frac{\epsilon(1_{K(x_1)},\psi_{K(x_1)},d_{\psi_{K(x_1)}}x)}{\epsilon(\mathrm{Ind}_{K(x_1)}^{K}(1_{K(x_1)}),\psi_K,d_{\psi_K}x)}\\
&\qquad=\epsilon(\theta_K,\psi_K,d_{\psi_K}x)\epsilon(\theta_K^2,\psi_K,d_{\psi_K}x)\frac{\epsilon(1_{K(x_1)},\psi_{K(x_1)},d_{\psi_{K(x_1)}}x)}{\epsilon(1_{K(D)},\psi_{K(D)},d_{\psi_{K(D)}}x)}.
\end{aligned}$$

Wegen

$$\begin{aligned}
\overline{\epsilon(\theta_K,\psi_K,d_{\psi_K}x)}&=\epsilon(\overline{\theta}_K,\overline{\psi}_K,d_{\psi_K}x)\\
&=\epsilon(\theta_K^2,\psi_K,d_{\psi_K}x)
\end{aligned}$$

liefert die Anwendung von 1.5.5 die Gleichung

$$\begin{aligned}
\epsilon(\theta_K,\psi_K,d_{\psi_K}x)\epsilon(\theta_K^2,\psi_K,d_{\psi_K}x)&=\mid\epsilon(\theta_K,\psi_K,d_{\psi_K}x)\mid^2\\
&=q^{-\mathrm{cond}(\psi_K)+\mathrm{cond}(\theta_K)}\\
&=\begin{cases}1, & \text{falls } K(\gamma)/K \text{ unverzweigt ist}\\ q, & \text{falls } K(\gamma)/K \text{ verzweigt ist.}\end{cases}
\end{aligned}$$

Wir erinnern daran, daß q die Elementanzahl des Restklassenkörpers von K ist. Wir wählen nun $c_1\in K(x_1)$ mit $\nu_{K(x_1)}=-\mathrm{cond}(\psi_{K(x_1)})$ und c_2 in $K(D)$ mit $\nu_{K(D)}(c_2)=-\mathrm{cond}(\psi_{K(D)})$. Wegen $[K(E):K]=12$, $\mathrm{e}(K(E)/K(\gamma))=4$, $[K(x_1):K]=4$ und $K(x_1)\subset K(E)$ muß die Erweiterung $K(x_1)/K$ voll verzweigt sein. Die Erweiterung $K(D)/K$ dagegen hat den Trägheitsgrad 3 oder 1, je nachdem ob $K(\gamma)/K$ unverzweigt ist oder nicht. Unter Anwendung von 1.5.3 erhalten wir

$$\begin{aligned}
\epsilon(1_{K(x_1)},\psi_{K(x_1)},d_{\psi_{K(x_1)}}x)&=\omega_{K(x_1)}^{-1}(c_1)\int_{\mathcal{O}_{K(x_1)}}1\,d_{\psi_{K(x_1)}}x\\
&=q^{\nu_{K(x_1)}(c_1)}q^{\frac{1}{2}\mathrm{cond}(\psi_{K(x_1)})}\\
&=q^{-\frac{1}{2}\mathrm{cond}(\psi_{K(x_1)})}\\
&=q^{\frac{1}{2}\mathrm{d}(K(x_1)/K)}
\end{aligned}$$

und

$$\begin{aligned}
\epsilon(1_{K(D)},\psi_{K(D)},d_{\psi_{K(D)}}x)&=\omega_{K(D)}^{-1}(c_2)\int_{\mathcal{O}_{K(D)}}1\,d_{\psi_{K(D)}}x\\
&=\begin{cases}q^{\frac{3}{2}\mathrm{d}(K(D)/K)}, & \text{falls } K(\gamma)/K \text{ unverzweigt ist}\\ q^{\frac{1}{2}\mathrm{d}(K(D)/K)}, & \text{falls } K(\gamma)/K \text{ verzweigt ist.}\end{cases}
\end{aligned}$$

Aufgrund der Transitivität der Differente gilt

$$\begin{aligned}
\mathrm{d}(K(E)/K)&=\mathrm{d}(K(E)/K(x_1))+\mathrm{e}(K(E)/K(x_1))\mathrm{d}(K(x_1)/K)\\
&=\mathrm{d}(K(E)/K(x_1))+\mathrm{e}(K(\gamma)/K)\mathrm{d}(K(x_1)/K).
\end{aligned}$$

Hieraus ergibt sich

$$\begin{aligned}
\mathrm{d}(K(x_1)/K)&=\frac{\mathrm{d}(K(E)/K)-\mathrm{d}(K(E)/K(x_1))}{\mathrm{e}(K(\gamma)/K)}\\
&=\frac{\mathrm{d}(K(E)/K(D))+2\mathrm{d}(K(D)/K)-\mathrm{d}(K(E)/K(x_1))}{\mathrm{e}(K(\gamma)/K)}\\
&=\frac{\mathrm{d}(K(E)/K(D))+2\mathrm{d}(K(D)/K(\gamma))+4\mathrm{d}(K(\gamma)/K)-\mathrm{d}(K(E)/K(x_1))}{\mathrm{e}(K(\gamma)/K)}.
\end{aligned}$$

Nach 4.5.4 und 9.3.2 gilt

$$\begin{aligned}\mathrm{d}(K(E)/K(D)) &= 1 - \nu_{K(\gamma)}\left(\frac{(\varphi\gamma)'(\varphi^2\gamma)'}{\gamma'}\right)\\ &= 1 - \nu_{K(\gamma)}(\gamma')\\ &= \mathrm{d}(K(D)/K(\gamma)).\end{aligned}$$

Falls $K(\gamma)/K$ unverzweigt ist, so ist auch $K(E)/K(x_1)$ unverzweigt. Daraus folgt

$$\mathrm{d}(K(E)/K(D)) = 3\mathrm{d}(K(D)/K(\gamma)) = 3\mathrm{d}(K(D)/K).$$

Insgesamt erhält man

$$\frac{\lambda(K(D)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(D)}}x)}{\lambda(K(x_1)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(x_1)}}x)} = \frac{q^{\frac{1}{2}\mathrm{d}(K(x_1)/K)}}{q^{\frac{3}{2}\mathrm{d}(K(D)/K)}} = 1.$$

Wir betrachten nun den Fall, daß $K(\gamma)/K$ verzweigt ist. Dann ist auch $K(E)/K(x_1)$ verzweigt von Grad 3. Nach [21, Chap. III, Prop. 13] gilt

$$\mathrm{d}(K(\gamma)/K) = \mathrm{d}(K(E)/K(x_1)) = 2.$$

Daraus folgt

$$\mathrm{d}(K(x_1)/K) = \mathrm{d}(K(D)/K(\gamma)) + 2.$$

Insgesamt erhält man

$$\begin{aligned}\frac{\lambda(K(D)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(D)}}x)}{\lambda(K(x_1)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(x_1)}}x)} &= q\frac{q^{\frac{1}{2}\mathrm{d}(K(x_1)/K)}}{q^{\frac{1}{2}\mathrm{d}(K(D)/K)}}\\ &= q\frac{q^{\frac{1}{2}(\mathrm{d}(K(D)/K(\gamma))+2)}}{q^{\frac{1}{2}(\mathrm{d}(K(D)/K(\gamma))+2\cdot 2)}}\\ &= 1.\end{aligned}$$

□

Korollar 9.4.2 *Für jeden Charakter χ von $W(K^{\mathrm{sep}}/K)$ gilt*

$$\epsilon(\chi \otimes \pi^K_{\alpha,\beta}, \psi_K, d_{\psi_K}x) = \frac{\epsilon(\mathrm{Res}^{K(D)}_K(\chi)\Omega^{-1}_{K(D)}\chi_{K(D)}, \psi_{K(D)}, d_{\psi_{K(D)}}x)}{\epsilon(\mathrm{Res}^{K(x_1)}_K(\chi)\Omega^{-1}_{K(x_1)}\chi_{K(x_1)}, \psi_{K(x_1)}, d_{\psi_{K(x_1)}}x)}.$$

Beweis: Aus 9.2.5 folgt

$$(\chi \otimes \pi^K_{\alpha,\beta}) \oplus \mathrm{Ind}^K_{K(x_1)}\left(\mathrm{Res}^{K(x_1)}_K(\chi)\Omega^{-1}_{K(x_1)}\chi_{K(x_1)}\right) \cong \mathrm{Ind}^K_{K(D)}\left(\mathrm{Res}^{K(D)}_K(\chi)\Omega^{-1}_{K(D)}\chi_{K(D)}\right).$$

Die Anwendung von 1.5.2 und 9.4.1 liefert das gewünschte Resultat. □

Kapitel 10

Primitive elliptische Kurven vom S_4-Typ

Für dieses gesamte Kapitel nehmen wir den Fall $[K(\varphi) : K] = 2$, $[K(\varphi, \gamma) : K(\varphi)] = 3$ und $[K(\varphi, E) : K(\varphi, \gamma)] = 4$ an. Nach 5.1.3 und 5.1.4 ist dies genau dann der Fall, wenn f ungerade, $\nu_K(\beta)$ nicht durch 3 teilbar ist und es kein $\tilde{\alpha} \in K$ gibt mit $\beta = \tilde{\alpha} + \tilde{\alpha}^2 + \tilde{\alpha}^3 + \tilde{\alpha}^3$. Nach 2.4.1 gilt $[L : K(\varphi, E)] = 2$, so daß L/K den größtmöglichen Grad 48 hat. Gemäß der Tabelle von 2.3.3 identifizieren wir $G(L/K)$ mit $GL_2(\mathbb{F}_3)$.

10.1 Die Brauerzerlegung von $\pi^K_{\alpha,\beta}$

Satz 10.1.1 *Die Darstellung $\pi^K_{\alpha,\beta}$ ist primitiv mit projektivem Typ S_4.*

Beweis: Nach 2.2.4 ist der projektive Kernkörper $K(\varphi, E)$ von $\pi^K_{\alpha,\beta}$ der Zerfällungskörper des Polynoms $X^4+X^3+\beta$ über K. Folglich läßt sich $G(K(\varphi, E)/K)$ als Untergruppe von S_4 auffassen. Wegen $[K(\varphi, E) : K] = 24$ folgt $G(K(\varphi, E)/K) \cong S_4$. Nach 1.6.2 muß $\pi^K_{\alpha,\beta}$ primitiv sein. □

Wir erinnern daran, daß $x_1 = (D + 1)E$ ist.

Lemma 10.1.2 *Es gilt $[K(x_1, F_\alpha) : K(x_1)] = 2$.*

Beweis: Wegen $F_\alpha + F_\alpha^2 = x_1 + \alpha$ gilt $[K(x_1, F_\alpha) : K(x_1)] \leq 2$. Wäre nun $[K(x_1, F_\alpha) : K(x_1)] = 1$, so müßte $F_\alpha \in K(x_1) \subset K(\varphi, E)$ sein und L/K könnte nicht den maximalen Grad 48 haben. Also gilt $[K(x_1, F_\alpha) : K(x_1)] = 2$. □

Wir bezeichnen nun mit $\chi_{K(x_1)}$ den eindeutig bestimmten Charakter von $G(L/K(x_1))$, der $G(L/K(x_1, F_\alpha))$ als Kern besitzt.

Lemma 10.1.3 *Es gilt $G(L/K(D + \varphi)) \cong \mathbb{Z}/8\mathbb{Z}$. Dabei wird $G(L/K(D + \varphi))$ von einem Automorphismus σ erzeugt mit $\sigma(\varphi) = \varphi + 1$, $\sigma(E) = E + \varphi + 1$ und $\sigma(F_\alpha) = F_\alpha + \varphi E$.*

Beweis: Wegen

$$\sigma(D + \varphi) = \sigma(E + E^2 + \varphi) = E + \varphi + 1 + (E + \varphi + 1)^2 + \varphi + 1 = E + E^2 + \varphi = D + \varphi$$

folgt $\sigma \in G(L/K(D + \varphi))$. Weil σ der Matrix

$$\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$$

entspricht, läßt sich leicht verifizieren, daß σ die Ordnung 8 hat. Andererseits gilt

$$[L : K(D+\varphi)] = [L : K(\varphi, D)][K(\varphi, D) : K(D+\varphi)] \leq 8.$$

Daraus folgt $G(L/K(D+\varphi)) =< \sigma >$. □

Für die weiteren Betrachtungen sei $\chi_{K(D+\varphi)}$ der eindeutig bestimmte injektive Charakter von $G(L/K(D+\varphi))$ mit $\chi_{K(D+\varphi)}(\sigma) = e^{\frac{\pi}{4}i}$.

Satz 10.1.4 *Es gilt*

$$\rho^K_{\alpha,\beta} \oplus \mathrm{Ind}^K_{K(x_1)}(\chi_{K(x_1)}) \cong \mathrm{Ind}^K_{K(D+\varphi)}(\chi_{K(D+\varphi)}).$$

Beweis: Sei B diejenige Untergruppe von $GL_2(\mathbb{F}_3)$, die der Galoisgruppe $G(L/K(x_1))$ entspricht, und H diejenige Untergruppe von $GL_2(\mathbb{F}_3)$, die der Galoisgruppe $G(L/K(D+\varphi))$ entspricht. Wir fassen $\chi_{K(x_1)}$ als Charakter von B und $\chi_{K(D+\varphi)}$ als Charakter von H auf. Nach 2.3.4 ist B die Gruppe der oberen Dreiecksmatrizen. Aus 10.1.3 und 2.3.3 folgt

$$H =< \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} > .$$

Zunächst zeigen wir, daß $\mathrm{Ind}^K_{K(x_1)}(\chi_{K(x_1)})$ irreduzibel ist. Nach [17, Th. 7.1] gibt es zwei Charaktere μ, μ' von $\mathbb{F}_3^*$ mit

$$\chi_{K(x_1)}(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix}) = \mu(a)\mu'(b)$$

für alle $a, b \in \mathbb{F}_3^*$ und $c \in \mathbb{F}_3$. Sei $\sigma \in G(L/K(x_1))$ der Automorphismus, der der Matrix

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

entspricht. Dann gilt $\sigma(F_\alpha) = F_\alpha + 1$ Daraus ergibt sich

$$\chi_{K(x_1)}(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}) = -1.$$

Insbesondere ist $\mu(-1)\mu'(-1) = -1$ und somit $\mu \neq \mu'$. Nach [17, Th. 8.12] folgt, daß die vierdimensionale Darstellung $\mathrm{Ind}^K_{K(x_1)}(\chi_{K(x_1)})$ irreduzibel ist.

Indem wir die Potenzen des Erzeugers von H ausrechnen und nachprüfen, welche dieser Matrizen obere Dreiecksmatrizen sind, erhalten wir

$$H \cap B = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

Außerdem verifizieren wir leicht, daß $\chi_{K(x_1)}$ und $\chi_{K(D+\varphi)}$ auf $H \cap B$ übereinstimmen. Nach [16, Th. 3] muß die Verkettungszahl von $\mathrm{Ind}^K_{K(x_1)}(\chi_{K(x_1)})$ und $\mathrm{Ind}^K_{K(D+\varphi)}\chi_{K(D+\varphi)}$ mindestens 1 sein. Folglich ist $\mathrm{Ind}^K_{K(x_1)}(\chi_{K(x_1)})$ ein Summand von $\mathrm{Ind}^K_{K(D+\varphi)}(\chi_{K(D+\varphi)})$.

Nach 8.2.3 gilt $\rho^{K(\gamma)}_{\alpha,\beta} \cong \mathrm{Ind}^{K(\gamma)}_{K(D+\varphi)}(\chi_{K(D+\varphi)})$. Hierbei ist $\rho^{K(\gamma)}_{\alpha,\beta}$ irreduzibel nach 8.2.2. Aufgrund der Frobeniusreziprozität erhalten wir für die Verkettungszahl der Darstellungen $\rho^{K(\gamma)}_{\alpha,\beta}$ und $\mathrm{Ind}^K_{K(D+\varphi)}(\chi_{K(D+\varphi)})$ die Identität

$$\begin{aligned} \left(\rho^K_{\alpha,\beta}, \mathrm{Ind}^K_{K(D+\varphi)}(\chi_{K(D+\varphi)})\right)_{G(L/K)} &= \left(\rho^{K(\gamma)}_{\alpha,\beta}, \mathrm{Ind}^{K(\gamma)}_{K(D+\varphi)}(\chi_{K(D+\varphi)})\right)_{G(L/K(\gamma))} \\ &= 1. \end{aligned}$$

Also ist auch $\rho^K_{\alpha,\beta}$ ein Summand von $\mathrm{Ind}^K_{K(D+\varphi)}(\chi_{K(D+\varphi)})$.

Aus Dimensionsgründen erhält man

$$\rho^K_{\alpha,\beta} \oplus \mathrm{Ind}^K_{K(x_1)}(\chi_{K(x_1)}) \cong \mathrm{Ind}^K_{K(D+\varphi)}(\chi_{K(D+\varphi)}).$$

□

Wenn wir $\chi_{K(D+\varphi)}$ als Charakter von $W(K^{\mathrm{sep}}/K(D+\varphi))$ und $\chi_{K(x_1)}$ als Charakter von $W(K^{\mathrm{sep}}/K(x_1))$ auffassen, erhalten wir das folgende Korollar.

Korollar 10.1.5 *Es gilt*

$$\pi^K_{\alpha,\beta} \oplus \mathrm{Ind}^K_{K(x_1)}(\Omega^{-1}_{K(x_1)}\chi_{K(x_1)}) \cong \mathrm{Ind}^K_{K(D+\varphi)}(\Omega^{-1}_{K(D+\varphi)}\chi_{K(D+\varphi)}).$$

10.2 Führer und minimale Twists

Zunächst verweisen wir darauf, daß nach 9.3.1 die Ungleichung $\gamma' \neq 0$ gilt. Hieraus erhalten wir $\mathrm{e}(L/K(\varphi,\gamma)) = 8$.

Lemma 10.2.1 *Es gilt* $\nu_{K(\varphi,\gamma)}(\gamma') = \nu_{K(\varphi,\gamma)}((\varphi\gamma)')$.

Beweis: Wenn wir K durch $K(\varphi)$ ersetzen, befinden wie uns in der Situation von Kapitel 9. Folglich können wir 9.3.2 anwenden und erhalten so die Aussage des Lemmas. □

Lemma 10.2.2 *Es gilt* $\mathrm{e}(K(\varphi,\gamma)/K) = 3$.

Beweis: Weil $K(\varphi)/K$ unverzweigt ist, kann $K(\varphi,\gamma)/K$ nur den Verzweigungsgrad 1 oder 3 haben. Andererseits ist $K(\varphi,\gamma)$ der Zerfällungskörper des Polynoms $X^3+\beta$ über K und folglich eine Galoiserweiterung, deren Galoisgruppe sich als eine Untergruppe von S_3 auffassen läßt. Wegen $[K(\varphi,\gamma):K] = 6$ folgt $G(K(\varphi,\gamma)/K) \cong S_3$. Weil diese Gruppe nicht zyklisch ist, kann $K(\varphi,\gamma)/K$ nicht unverzweigt sein. □

Satz 10.2.3 *Für den Führer gilt*

$$\mathrm{cond}(\pi^K_{\alpha,\beta}) = \frac{11 + \mathrm{d}(L/K(\varphi,E)) - 3\nu_{K(\varphi,\gamma)}(\gamma')}{6}.$$

Beweis: Weil der Führer nur durch die Operation der Verzweigungsgruppen bestimmt wird, gilt $\mathrm{cond}(\pi^K_{\alpha,\beta}) = \mathrm{cond}(\pi^{K(\varphi)}_{\alpha,\beta})$. Also können wir 9.3.4 anwenden und erhalten die gewünschte Formel für $\mathrm{cond}(\pi^K_{\alpha,\beta})$. □

Satz 10.2.4 *Für den minimalen Führer gilt*

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = 2 - \nu_{K(\varphi,\gamma)}(\gamma').$$

Beweis: Wir wählen einen Charakter χ von $W(K^{\mathrm{sep}}/K)$, so daß $\mathrm{cond}(\chi \otimes \pi^K_{\alpha,\beta}) = \mathrm{cond}_{\min}(\pi^K_{\alpha,\beta})$ gilt. Weil $K(\varphi)/K$ unverzweigt ist, gilt

$$\mathrm{cond}(\chi \otimes \pi^K_{\alpha,\beta}) = \mathrm{cond}\left(\mathrm{Res}^{K(\varphi)}_K(\chi \otimes \pi^K_{\alpha,\beta})\right) = \mathrm{cond}\left(\mathrm{Res}^{K(\varphi)}_K(\chi) \otimes \pi^{K(\varphi)}_{\alpha,\beta}\right).$$

Nach [27] ist der Führer eines Twists einer primitiven irreduziblen zweidimensionalen Darstellung genau dann minimal, wenn er ungerade ist. Weil $\pi^{K(\varphi)}_{\alpha,\beta}$ nach 9.2.1 primitiv ist, folgt

$$\mathrm{cond}_{\min}(\pi^K_{\alpha,\beta}) = \mathrm{cond}_{\min}(\pi^{K(\varphi)}_{\alpha,\beta}).$$

Hieraus ergibt sich die gewünschte Aussage durch Anwendung von 9.3.6. □

10.3 Berechnung von ϵ-Faktoren

Satz 10.3.1 *Es gilt*

$$\lambda(K(D)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(D)}}x) = \lambda(K(x_1)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(x_1)}}x).$$

Beweis: Sei $\theta_{K(\gamma)}$ der eindeutig bestimmte Charakter von $W(K^{\mathrm{sep}}/K(\gamma))$, der $W(K^{\mathrm{sep}}/K(D))$ als Kern besitzt. Dann gilt

$$\begin{aligned}\mathrm{Ind}_{K(D)}^{K}(1_{K(D)}) &\cong \mathrm{Ind}_{K(\gamma)}^{K}(\mathrm{Ind}_{K(D)}^{K(\gamma)}(1_{K(D)}))\\ &\cong \mathrm{Ind}_{K(\gamma)}^{K}(1_{K(\gamma)} \oplus \theta_{K(\gamma)})\\ &\cong \mathrm{Ind}_{K(\gamma)}^{K}(1_{K(\gamma)}) \oplus \mathrm{Ind}_{K(\gamma)}^{K}(\theta_{K(\gamma)}).\end{aligned}$$

Sei nun θ_K der eindeutig bestimmte Charakter von $W(K^{\mathrm{sep}}/K)$, der $W(K^{\mathrm{sep}}/K(\varphi))$ als Kern besitzt, und $\theta_{K(\varphi)}$ ein Charakter von $W(K^{\mathrm{sep}}/K(\varphi))$ mit $\mathrm{Kern}(\theta_{K(\varphi)}) = W(K^{\mathrm{sep}}/K(\varphi,\gamma))$. Für die folgenden Betrachtungen verweisen wir darauf, daß $K(\varphi,\gamma)/K$ eine Galoiserweiterung ist, und fassen θ_K als Charakter von $G(K(\varphi,\gamma)/K(\varphi))$ auf. Dann gilt

$$\begin{aligned}&\Big(\mathrm{Ind}_{K(\varphi)}^{K}(\theta_{K(\varphi)}), \mathrm{Ind}_{K(\gamma)}^{K}(1_{K(\gamma)})\Big)_{G(K(\varphi,\gamma)/K)}\\ &\quad= \Big(\mathrm{Res}_{K}^{K(\gamma)}(\mathrm{Ind}_{K(\varphi)}^{K}(\theta_{K(\varphi)})), 1_{K(\gamma)}\Big)_{G(K(\varphi,\gamma)/K(\gamma))}\\ &\quad= \Big(\mathrm{Ind}_{K(\varphi,\gamma)}^{K(\gamma)}(1_{K(\varphi,\gamma)})), 1_{K(\gamma)}\Big)_{G(K(\varphi,\gamma)/K(\gamma))}\\ &\quad= 1.\end{aligned}$$

Wegen

$$\Big(1_K, \mathrm{Ind}_{K(\gamma)}^{K}(1_{K(\gamma)})\Big)_{G(K(\varphi,\gamma)/K)} = 1$$

erhalten wir

$$\mathrm{Ind}_{K(D)}^{K}(1_{K(D)}) \cong 1_K \oplus \mathrm{Ind}_{K(\varphi)}^{K}(\theta_{K(\varphi)}) \oplus \mathrm{Ind}_{K(\gamma)}^{K}(\theta_{K(\gamma)}).$$

Wir fassen nun θ_K und $\mathrm{Ind}_{K(\gamma)}^{K}(\theta_{K(\gamma)})$ als Darstellungen von $G(K(\varphi,E)/K) \cong S_4$ auf. Nach [22, Chap. 5.8] hat S_4 nur zwei eindimensionale Darstellungen. Wegen

$$\Big(\theta_K, \mathrm{Ind}_{K(\gamma)}^{K}(\theta_{K(\gamma)})\Big)_{G(K(\varphi,E)/K)} = \Big(\mathrm{Res}_{K}^{K(\gamma)}(\theta_K), \theta_{K(\gamma)}\Big)_{G(K(\varphi,E)/K(\gamma))} = 0$$

und

$$\Big(1_K, \mathrm{Ind}_{K(\gamma)}^{K}(\theta_{K(\gamma)})\Big)_{G(K(\varphi,E)/K)} = \big(1_{K(\gamma)}, \theta_{K(\gamma)}\big)_{G(K(\varphi,E)/K(\gamma))} = 0$$

folgt die Irreduzibilität von $\mathrm{Ind}_{K(\gamma)}^{K}(\theta_{K(\gamma)})$.

Aufgrund der Identitäten

$$G(K(\varphi,E)/K(x_1))G(K(\varphi,E)/K(\gamma)) = G(K(\varphi,E)/K(E))$$

und

$$G(K(\varphi,E)/K(x_1)) \cap G(K(\varphi,E)/K(\gamma)) = G(K(\varphi,E)/K)$$

erhalten wir

$$\mathrm{Res}_{K}^{K(x_1)}(\mathrm{Ind}_{K(\gamma)}^{K}(\theta_{K(\gamma)})) \cong \mathrm{Ind}_{K(E)}^{K(x_1)}(\mathrm{Res}_{K(\gamma)}^{K(E)}(\theta_{K(\gamma)})) \cong \mathrm{Ind}_{K(E)}^{K(x_1)}(1_{K(E)})$$

nach [22, Chap. 7, Prop. 22]. Daraus folgt

$$\begin{aligned}\Big(\mathrm{Ind}_{K(x_1)}^{K}(1_{K(x_1)}), \mathrm{Ind}_{K(\gamma)}^{K}(\theta_{K(\gamma)})\Big)_{G(K(\varphi,E)/K)} &= \Big(1_{K(x_1)}, \mathrm{Ind}_{K(E)}^{K(x_1)}(1_{K(E)})\Big)_{G(K(\varphi,E)/K(x_1))}\\ &= \big(1_{K(E)}, 1_{K(E)}\big)_{G(K(\varphi,E)/K(E))}\\ &= 1.\end{aligned}$$

Wegen

$$\Big(1_K, \mathrm{Ind}_{K(x_1)}^K(1_{K(x_1)})\Big)_{G(K(\varphi,E)/K)} = 1$$

erhalten wir

$$\mathrm{Ind}_{K(x_1)}^K(1_{K(x_1)}) \cong 1_K \oplus \mathrm{Ind}_{K(\gamma)}^K(\theta_{K(\gamma)}).$$

Insgesamt haben wir damit

$$\mathrm{Ind}_{K(D)}^K(1_{K(D)}) \cong \mathrm{Ind}_{K(\varphi)}^K(\theta_{K(\varphi)}) \oplus \mathrm{Ind}_{K(x_1)}^K(1_{K(x_1)})$$

gezeigt. Daraus folgt

$$\begin{aligned}
&\frac{\lambda(K(D)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(D)}}x)}{\lambda(K(x_1)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(x_1)}}x)} \\
&\qquad = \frac{\epsilon(\mathrm{Ind}_{K(D)}^K(1_{K(D)}), \psi_K, d_{\psi_K}x)}{\epsilon(1_{K(D)}, \psi_{K(D)}, d_{\psi_{K(D)}x})} \frac{\epsilon(1_{K(x_1)}, \psi_{K(x_1)}, d_{\psi_{K(x_1)}}x)}{\epsilon(\mathrm{Ind}_{K(x_1)}^K(1_{K(x_1)}), \psi_K, d_{\psi_K}x)} \\
&\qquad = \epsilon(\mathrm{Ind}_{K(\varphi)}^K(\theta_{K(\varphi)}), \psi_K, d_{\psi_K}) \frac{\epsilon(1_{K(x_1)}, \psi_{K(x_1)}, d_{\psi_{K(x_1)}}x)}{\epsilon(1_{K(D)}, \psi_{K(D)}, d_{\psi_{K(D)}x})}.
\end{aligned}$$

Für die folgenden Betrachtungen wählen wir $c_1 \in K(x_1)$ mit $\nu_{K(x_1)}(c_1) = -\mathrm{cond}(\psi_{K(x_1)})$ und $c_2 \in K(D)$ mit $\nu_{K(D)}(c_2) = -\mathrm{cond}(\psi_{K(D)})$. Weil $\mathrm{e}(L/K) = 24$ und $K(\varphi)/K$ unverzweigt ist, muß $K(E)/K$ voll verzweigt sein. Insbesondere sind die beiden Erweiterungen $K(x_1)/K$ und $K(D)/K$ voll verzweigt. Unter Anwendung von 1.5.3 erhalten wir

$$\begin{aligned}
\epsilon(1_{K(x_1)}, \psi_{K(x_1)}, d_{\psi_{K(x_1)}}x) &= \omega_{K(x_1)}^{-1}(c_1) \int_{\mathcal{O}_{K(x_1)}} 1 \, d_{\psi_{K(x_1)}}x \\
&= q^{\nu_{K(x_1)}(c_1)} q^{\frac{1}{2}\mathrm{cond}(\psi_{K(x_1)})} \\
&= q^{-\frac{1}{2}\mathrm{cond}(\psi_{K(x_1)})} \\
&= q^{\frac{1}{2}\mathrm{d}(K(x_1)/K)}
\end{aligned}$$

und

$$\begin{aligned}
\epsilon(1_{K(D)}, \psi_{K(D)}, d_{\psi_{K(D)}}x) &= \omega_{K(D)}^{-1}(c_2) \int_{\mathcal{O}_{K(D)}} 1 \, d_{\psi_{K(D)}}x \\
&= q^{\frac{1}{2}\mathrm{d}(K(D)/K)}.
\end{aligned}$$

Wir erinnern daran, daß q die Elementanzahl des Restklassenkörpers von K ist. Weil $K(E)/K(x_1)$ den Verzweigungsgrad 3 hat, erhalten wir aufgrund der Transitivität der Differente die Identität

$$\mathrm{d}(K(E)/K) = \mathrm{d}(K(E)/K(x_1)) + 3\mathrm{d}(K(x_1)/K).$$

Hieraus folgt

$$\begin{aligned}
\mathrm{d}(K(x_1)/K) &= \frac{\mathrm{d}(K(E)/K) - \mathrm{d}(K(E)/K(x_1))}{3} \\
&= \frac{\mathrm{d}(K(E)/K(D)) + 2\mathrm{d}(K(D)/K) - \mathrm{d}(K(E)/K(x_1))}{3} \\
&= \frac{\mathrm{d}(K(E)/K(D)) + 2\mathrm{d}(K(D)/K(\gamma)) + 4\mathrm{d}(K(\gamma)/K) - \mathrm{d}(K(E)/K(x_1))}{3}.
\end{aligned}$$

Nach [21, Chap. III, Prop. 13] gilt $\mathrm{d}(K(\gamma)/K) = 2$ und $\mathrm{d}(K(E)/K(x_1)) = 2$. Die Anwendung von 4.5.4 und 9.3.2 liefert

$$\begin{aligned}
\mathrm{d}(K(E)/K(D)) &= 1 - \nu_{K(\gamma)}\left(\frac{(\varphi\gamma)'(\varphi^2\gamma)'}{\gamma'}\right) \\
&= 1 - \nu_{K(\gamma)}(\gamma') \\
&= \mathrm{d}(K(D)/K(\gamma)).
\end{aligned}$$

Damit erhalten wir

$$\mathrm{d}(K(x_1)/K) = \mathrm{d}(K(D)/K(\gamma)) + 2.$$

Dies liefert uns das Zwischenergebnis

$$\begin{aligned}\frac{\epsilon(1_{K(x_1)}, \psi_{K(x_1)}, d_{\psi_{K(x_1)}}x)}{\epsilon(1_{K(D)}, \psi_{K(D)}, d_{\psi_{K(D)}}x)} &= \frac{q^{\frac{1}{2}\mathrm{d}(K(x_1)/K)}}{q^{\frac{1}{2}\mathrm{d}(K(D)/K)}} \\ &= \frac{q^{\frac{1}{2}(\mathrm{d}(K(D)/K(\gamma))+2)}}{q^{\frac{1}{2}(\mathrm{d}(K(D)/K(\gamma))+2\cdot 2)}} \\ &= q^{-1}.\end{aligned}$$

Unter Anwendung von 5.4.1 erhalten wir

$$\begin{aligned}\epsilon(\mathrm{Ind}_{K(\varphi)}^{K}(\theta_{K(\varphi)}), \psi_K, d_{\psi_K}x) &= \lambda(K(\varphi)/K, \psi_K, d_{\psi_K}x, d_{\psi_{K(\varphi)}}x)\epsilon(\theta_{K(\varphi)}, \psi_{K(\varphi)}, d_{\psi_{K(\varphi)}}x) \\ &= \epsilon(\theta_{K(\varphi)}, \psi_{K(\varphi)}, d_{\psi_{K(\varphi)}}x).\end{aligned}$$

Wir fassen nun $\theta_{K(\varphi)}$ als Charakter von $K(\varphi)^*$ auf. Weil $K(\varphi,\gamma)/K(\varphi)$ voll verzweigt vom Grad 3 ist, gilt $\theta_{K(\varphi)}(T) = 1$ und $\theta_{K(\varphi)}(1 + \mathfrak{p}_{K(\varphi)}) = 1$. Daraus folgt

$$\begin{aligned}\epsilon(\mathrm{Ind}_{K(\varphi)}^{K}(\theta_{K(\varphi)}), \psi_K, d_{\psi_K}x) &= \int\limits_{T^{-1}\mathcal{O}_{K(\varphi)}^*} \theta_{K(\varphi)}(x)\psi_{K(\varphi)}(x)\, d_{\psi_{K(\varphi)}}x \\ &= \int\limits_{T^{-1}\biguplus\limits_{a\in\mathbb{F}_{q^2}^*} a(1+\mathfrak{p}_{K(\varphi)})} \theta_{K(\varphi)}(x)\psi_{K(\varphi)}(x)\, d_{\psi_{K(\varphi)}}x \\ &= \sum_{a\in\mathbb{F}_{q^2}^*} \int\limits_{aT^{-1}(1+\mathfrak{p}_{K(\varphi)})} \theta_{K(\varphi)}(x)\psi_{K(\varphi)}(x)\, d_{\psi_{K(\varphi)}}x \\ &= \sum_{a\in\mathbb{F}_{q^2}^*} \int\limits_{aT^{-1}(1+\mathfrak{p}_{K(\varphi)})} \theta_{K(\varphi)}(a)\psi_{K(\varphi)}(aT^{-1})\, d_{\psi_{K(\varphi)}}x \\ &= \sum_{a\in\mathbb{F}_{q^2}^*} \theta_{K(\varphi)}(a)\psi_{K(\varphi)}(aT^{-1}) \int\limits_{aT^{-1}+\mathcal{O}_{K(\varphi)}} 1\, d_{\psi_{K(\varphi)}}x \\ &= \sum_{a\in\mathbb{F}_{q^2}^*} \theta_{K(\varphi)}(a)\psi_{K(\varphi)}(aT^{-1}).\end{aligned}$$

Wir definieren nun den Charakter ψ^* von $\mathbb{F}_4$ durch die Vorschrift $b \longmapsto (-1)^{\mathrm{Tr}_{\mathbb{F}_4}^{\mathbb{F}_2}(b)}$. Dann gilt

$$\psi_{K(\varphi)}(aT^{-1}) = \psi^*(\mathrm{Tr}_{\mathbb{F}_{q^2}}^{\mathbb{F}_4}(a))$$

für alle $a \in \mathbb{F}_{q^2}$. Weiter sei e ein zyklischer Erzeuger von $\mathbb{F}_{q^2}^*$ und $\tilde{\varphi} := \mathrm{N}_{\mathbb{F}_{q^2}}^{\mathbb{F}_4}(e)$. Wegen der Surjektivität von $\mathrm{N}_{\mathbb{N}_{q^2}}^{\mathbb{F}_4}$ muß $\tilde{\varphi}$ eine **primitive** dritte Einheitswurzel sein. Sei nun θ^* der eindeutig bestimmte Charakter von $\mathbb{F}_4$ mit $\theta^*(\tilde{\varphi}) = \theta_{K(\varphi)}(e)$. Dann gilt

$$\theta_{K(\varphi)}(a) = \theta^*(\mathrm{N}_{\mathbb{F}_{q^2}}^{\mathbb{F}_4}(a))$$

für alle $a \in \mathbb{F}_{q^2}$. Unter Anwendung von [14, Lemma 7.7] erhalten wir

$$\begin{aligned}
\epsilon(\mathrm{Ind}_{K(\varphi)}^{K}(\theta_{K(\varphi)}), \psi_K, d_{\psi_K} x) &= \sum_{a \in \mathbb{F}_{q^2}^*} \theta^*(a)\psi^*(a) \\
&= \left(\sum_{a \in \mathbb{F}_4^*} \theta^*(a)\psi^*(a) \right)^{[\mathbb{F}_{q^2}:\mathbb{F}_4]} \\
&= \left(\theta^*(\varphi)\psi^*(\varphi) + \theta^*(\varphi^2)\psi^*(\varphi^2) + \theta^*(1)\psi^*(1) \right)^{[\mathbb{F}_{q^2}:\mathbb{F}_4]} \\
&= \left(-\theta^*(\varphi) - (\theta^*(\varphi))^2 + 1 \right)^{[\mathbb{F}_{q^2}:\mathbb{F}_4]} \\
&= 2^{[\mathbb{F}_{q^2}:\mathbb{F}_4]} \\
&= q.
\end{aligned}$$

Insgesamt erhalten wir damit

$$\frac{\lambda(K(D)/K, \psi_K, d_{\psi_K} x, d_{\psi_{K(D)}} x)}{\lambda(K(x_1)/K, \psi_K, d_{\psi_K} x, d_{\psi_{K(x_1)}} x)} = q^{-1} q = 1.$$

□

Korollar 10.3.2 *Für jeden Charakter χ von $W(K^{\mathrm{sep}}/K)$ gilt*

$$\epsilon(\chi \otimes \pi_{\alpha,\beta}^K, \psi_K, d_{\psi_K} x) = \frac{\epsilon(\mathrm{Res}_K^{K(D)}(\chi)\Omega_{K(D)}^{-1}\chi_{K(D)}, \psi_{K(D)}, d_{\psi_{K(D)}} x)}{\epsilon(\mathrm{Res}_K^{K(x_1)}(\chi)\Omega_{K(x_1)}^{-1}\chi_{K(x_1)}, \psi_{K(x_1)}, d_{\psi_{K(x_1)}} x)}.$$

Beweis: Aus 10.1.5 folgt

$$(\chi \otimes \pi_{\alpha,\beta}^K) \oplus \mathrm{Ind}_{K(x_1)}^K \left(\mathrm{Res}_K^{K(x_1)}(\chi)\Omega_{K(x_1)}^{-1}\chi_{K(x_1)} \right) \cong \mathrm{Ind}_{K(D)}^K \left(\mathrm{Res}_K^{K(D)}(\chi)\Omega_{K(D)}^{-1}\chi_{K(D)} \right).$$

Die Anwendung von 1.5.2 und 10.3.1 liefert das gewünschte Resultat. □

Kapitel 11

Schlußbemerkung

Wir erinnern daran, daß die Darstellung $\pi^K_{\alpha,\beta}$ im Fall $\nu_K(\beta) < 0$ genau dann irreduzibel ist, wenn $G(L/K)$ nichtabelsch ist (s. 3.1.7). In 2.4.6 sind in Tabellenform alle Fälle aufgelistet, in denen $G(L/K)$ nichtabelsch ist. Diese Tabelle haben wir in den Kapiteln 5-10 abgearbeitet. Somit haben wir alle Fälle abgehandelt, in denen $\pi^K_{\alpha,\beta}$ irreduzibel ist. In allen diesen Fällen ist es uns gelungen, den projektiven Typ von $\pi^K_{\alpha,\beta}$ zu bestimmen. Wenn der projektive Typ von $\pi^K_{\alpha,\beta}$ eine Diedergruppe ist (Kap. 5-8) haben wir eine quadratische Erweiterung M/K und einen Charakter χ_M von $W(K^{\mathrm{sep}}/M)$ bestimmt, der die Darstellung $\pi^K_{\alpha,\beta}$ induziert. In den Fällen, in denen $\pi^K_{\alpha,\beta}$ vom Typ A_4 oder S_4 ist, konnten wir eine Brauerzerlegung im Sinne von 1.1.3 angeben. Darüber hinaus haben wir in allen Fällen die zugehörigen λ-Faktoren ausgerechnet, so daß wir insgesamt (zumindest prinzipiell) die ϵ-Faktoren aller Twists bestimmen können. Weil der Determinantencharakter von $\pi^K_{\alpha,\beta}$ schon a priori bekannt ist (s. 1.10.6), haben wir es geschafft, den Isomorphietyp von $\pi^K_{\alpha,\beta}$ vollständig zu bestimmen.

Anhang A

Die abgeleitete Reihe von $GL_2(\mathbb{F}_3)$

Weil wir keine geeignete Referenz gefunden haben, wollen wir kurz auf die abgeleitete Reihe von $GL_2(\mathbb{F}_3)$ eingehen. Dabei verwenden wir für die auftretenden Kommutatorgruppen eckige Klammern $[,]$ und erlauben uns, das Element

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

mit -1 zu bezeichnen.

Bezeichnung A.1 *In $GL_2(\mathbb{F}_3)$ zeichnen wir folgende Elemente aus:*

$$A := \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \quad B := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad C := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Lemma A.2 *Es gilt*

(i) $B^2 = C^2 = -1$,

(ii) $\mathrm{ord}(A) = 3$, $\mathrm{ord}(B) = \mathrm{ord}(C) = 4$,

(iii) $CB = -CB$,

(iv) $ABA^{-1} = C$, $ACA^{-1} = CB$,

(v) $A \in [GL_2(\mathbb{F}_3), GL_2(\mathbb{F}_3)]$ *und* $B, C \in [SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$.

Beweis: Die Aussagen (i) bis (iv) lassen sich durch einfache Rechnungen verifizieren. Damit bleibt nur noch (v) zu zeigen. Wegen

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}^{-1}$$

folgt $A \in [GL_2(\mathbb{F}_3), GL_2(\mathbb{F}_3)]$. Außerdem gilt

$$B := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}^{-1}$$

und

$$C := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{-1} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}^{-1},$$

womit man wegen

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \in SL_2(\mathbb{F}_3)$$

die Aussage $B, C \in [SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$ erhält. □

Satz A.3 *Es gilt* $< B, C >= \{B^i C^j \mid i = 0, 1, \text{ und } j = 0, 1, \ldots, 3\}$.

Beweis: Wegen der Vertauschungsrelation $BC = -CB$ haben alle Elemente von $< B, C >$ die Form $B^i C^j$. Weil $\text{ord}(B) = \text{ord}(C) = 4$ ist, können i und j in $\{0, 1, 2, 3\}$ gewählt werden. Aufgrund der Relation $B^2 = C^2$ kann man zusätzlich $i \in \{0, 1\}$ annehmen. □

Das folgende Korollar erhält man, indem man nun die Elemente der Form explizit $B^i C^j$ berechnet.

Korollar A.4 *Es gilt*

$$< B, C >= \{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix} \}.$$

Korollar A.5 *Jede echte Untergruppe von* $< B, C >$ *ist zyklisch.*

Beweis: Für alle $j = 0, 1, 2, 3$ gilt

$$BC^j BC^j = BB(-1)^j C^j C^j = -1(-1)^j (-1)^j = -1.$$

Außerdem gilt $C^2 = -1$. Also hat $< B, C >$ mindestens fünf Elemente, deren Ordnung größer als 2 ist. Sei nun H eine echte Untergruppe von $< B, C >$. Dann kann H nur dann nicht zyklisch sein, wenn $\#H = 4$ ist. In diesem Fall besäße $< B, C >$ mindestens vier verschiedene Elemente, deren Ordnung kleiner oder gleich 2 ist. □

Satz A.6 *Es gilt* $< A, B, C >= SL_2(\mathbb{F}_3)$.

Beweis: Wegen $A, B, C \in SL_2(\mathbb{F}_3)$ gilt $< A, B, C > \subset SL_2(\mathbb{F}_3)$. Wegen $\text{ord}(A) = 3$ muß $A \notin < A, B, C >$ sein. Daraus folgt $\# < A, B, C > \geq 8$. Weil $\#SL_2(\mathbb{F}_3) = 24$ ist, erhält man $< A, B, C >= SL_2(\mathbb{F}_3)$. □

Korollar A.7 *Es gilt* $[GL_2(\mathbb{F}_3), GL_2(\mathbb{F}_3)] = SL_2(\mathbb{F}_3)$.

Beweis: Die Relation $\subset$ gilt wegen der Multiplikativität der Determinantenabbildung. Mit A.6 und A.2(v) erhält man die Gleichheit. □

Satz A.8 *Es gilt* $< B, C >= [SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$.

Beweis: Wegen $< A, B, C >= SL_2(\mathbb{F}_3)$ und den Relationen $ABA^{-1} = C$ und $ACA^{-1} = CB$ muß $< B, C >$ ein Normalteiler von $SL_2(\mathbb{F}_3)$ sein. Die zugehörige Faktorgruppe hat den Grad 3 und ist somit abelsch. Also gilt $< B, C > \supset [SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$. Wegen $B, C \in [SL_2(\mathbb{F}_3), SL_2(\mathbb{F}_3)]$ erhält man die Gleichheit. □

Korollar A.9 *Die Gruppe* $SL_2(\mathbb{F}_3)$ *hat keinen Normalteiler der Ordnung* 4.

Beweis: Wir nehmen an, $SL_2(\mathbb{F}_3)$ hätte einen Normalteiler H der Ordnung 4. Dann müßte insbesondere $AHA^{-1} = H$ sein. Wegen $\text{ord}(A) = 3$ erhielte man die Aussage, daß $< A, H >$ als Untergruppe von $SL_2(\mathbb{F}_3)$ die Ordnung 12 und damit den Index 2 hätte. Also wäre $< A, H >$ ein Normalteiler mit abelscher Faktorgruppe und enthielte die Kommutatorgruppe $< B, C >$ von $SL_2(\mathbb{F}_3)$, was nicht sein kann, weil diese Untergruppe von der Ordnung 8 ist. □

Satz A.10 *Es gilt* $\{1,-1\} = [< B,C >, < B,C >]$.

Beweis: Wegen $CBC^{-1}B^{-1} = -BCC^{-1}B^{-1} = -1$ gilt $\{1,-1\} \subset [< B,C >, < B,C >]$. Andererseits gilt für alle $x = B^iC^j, y = B^kC^l \in < B,C >$ die Identität

$$\begin{aligned} xyx^{-1}y^{-1} &= B^iC^jB^kC^lC^{-j}B^{-i}C^{-l}B^{-k} \\ &= B^iB^kC^j(-1)^{jk}C^lC^{-j}C^{-l}B^{-i}(-1)^{il}B^{-k} \\ &= (-1)^{jk+il}. \end{aligned}$$

Daraus folgt $\{1,-1\} = [< B,C >, < B,C >]$. □

Anhang B

Die Darstellung ρ_{μ_5} von $GL_2(\mathbb{F}_3)$

Für jede Matrix $A \in GL_2(\mathbb{F}_3)$ bezeichnen wir mit $[A]$ ihre Konjugationsklasse. Nach [17, §5] hat $A \in GL_2(\mathbb{F}_3)$ folgende Konjugationsklassen:

$$\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right], \left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right], \left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right], \left[\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}\right],$$
$$\left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right], \left[\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\right], \left[\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right], \left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right].$$

Hierbei werden die ersten fünf Konjugationsklassen durch Jordanmatrizen repräsentiert, während die Vertreter der letzten drei Konjugationsklassen von der Form

$$\begin{pmatrix} 0 & -a\bar{a} \\ 1 & a+\bar{a} \end{pmatrix}$$

mit $a \in \mathbb{F}_9$ sind. Diese haben jeweils die Eigenwerte a und $\bar{a}$, wobei $\bar{a} \in \mathbb{F}_9$ das zu a über $\mathbb{F}_3$ konjugierte Element sein soll. Indem man nun explizit das charakteristische Polynom und ggf. noch das Minimalpolynom berechnet, läßt sich jede Matrix von $GL_2(\mathbb{F}_3)$ einer der angegebenen Konjugationsklassen zuordnen. Wir geben nur das Ergebnis an.

Satz B.1 *Es gilt*

- $\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right] = \left\{\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\}$,
- $\left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right] = \left\{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right\}$,
- $\left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right] = \left\{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}\right\}$,
- $\left[\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}\right] = \left\{\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}\right\}$,
- $\left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right] = \left\{\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}\right\}$,

- $\left[\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\right] = \left\{\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 0 \end{pmatrix}\right\}$,
- $\left[\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right] = \left\{\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ 1 & -1 \end{pmatrix}\right\}$,
- $\left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right] = \left\{\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix}\right\}$.

Wenn nun $\mu_5 : GL_2(\mathbb{F}_3) \longrightarrow \mathbb{C}^*$ der eindeutig bestimmte Charakter ist mit $\mu_5(1+\sqrt{-1}) = e^{i\frac{4\pi}{8}}$ und ρ_{μ_5} die zugehörige cuspidale Darstellung, so erhalten wir die folgende Aussage nach [17, S. 70].

Satz B.2 *Die Spurabbildung* $\mathrm{Tr}(\rho_{\mu_5})$ *von* ρ_{μ_5} *ist durch folgende Tabelle gegeben:*

Konjugationsklasse	*Wert von* $\mathrm{Tr}(\rho_{\mu_5})$
$\left[\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right]$	2
$\left[\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right]$	-2
$\left[\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\right]$	-1
$\left[\begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}\right]$	1
$\left[\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}\right]$	0
$\left[\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}\right]$	$\sqrt{2}i$
$\left[\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}\right]$	$-\sqrt{2}i$
$\left[\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\right]$	0

Literaturverzeichnis

[1] J. Buhler, *An Icosahedral Modular Form of Weight One*, in: Modular Functions of One Variable V, Springer Lecture Notes **601**, (1977), S. 289-294.

[2] D. Bump, *Automorphic Forms and Representations*, Cambridge Studies in Advanced Mathematics: 55, Cambridge, 1998.

[3] A. Brumer und K. Kramer, *The Conductor of an Abelian Variety*, Compositio Math. **92**, (1994), S. 227-248.

[4] H. Carayol, *Reperésentations cuspidales du groupe linéaire*, Ann. Scient. Éc. Norm. Sup. 4^e série **17**, (1984), S. 191-225.

[5] P. Deligne, *Les constantes des équations fonctionnelles des fonctions L*, in: Modular Functions of One Variable II, Springer Lecture Notes **349**, (1973), S. 501-597.

[6] E.-U. Gekeler, *Pencils of Elliptic Curves in Characteristic 2*, Duke Math. J. **89**, (1997), S. 95-107.

[7] P. Gérardin und P. Kutzko, *Facteurs locaux pour $GL(2)$*, Ann. scient. Éc. Norm. Sup. 4^e série **13**, (1980), S. 349-384.

[8] R. Godement und H. Jacquet, *Zeta Functions of Simple Algebras*, Springer Lecture Notes **260**, (1972).

[9] H. Jacquet und R. P. Langlands, *Automorphic Forms on $GL(2)$*, Springer Lecture Notes **114**, (1970).

[10] H. Koch, *Zahlentheorie*, Vieweg, Braunschweig/Wiesbaden, 1997.

[11] P. Kutzko, *The Langlands Conjecture for GL_2 of a Local Field*, Ann. of Math. **112**, (1980), S. 381-412.

[12] P. Kutzko, *The Irreducible Imprimitive Local Galois Representations of Prime Dimension*, J. Algebra **57**, (1979), S. 101-110.

[13] E. Lamprecht, *Allgemeine Theorie der Gaußschen Summen in endlichen kommutativen Ringen*, Math. Nachr. **9**, (1953), S. 149-196.

[14] R. P. Langlands, *On the Functional Equation of the Artin L-Functions*, (1970), unveröffentlicht, erhältlich unter: *http://www.sunsite.ubc.ca/DigitalMathArchive/Langlands/*.

[15] J. Lubin und J. Tate, *Formal Complex Multiplication in Local Fields*, Ann. of Math. **81**, (1965), S. 380-387.

[16] G. W. Mackey, *On Induced Representations of Groups*, Amer. J. Math. **73**, (1951), S. 576-592.

[17] I. Piatetski-Shapiro, *Complex Representations of $GL(2, K)$ for Finite Fields K*, Contemporary Mathematics **16**, Amer. Math. Soc. 1983.

[18] D. E. Rohrlich, *Elliptic Curves and the Weil-Deligne Group*, in: Elliptic Curves and Related Topics, CRM Proceedings & Lecture Notes **4**, herausgegeben von H. Kisilevsky und R. Murty, Amer. Math. Soc. Providence, RI, 1994, S. 125-157.

[19] P. Roquette, *Analytic Theory of Elliptic Functions Over Local Fields*, Vandenhoeck & Rubrecht, Göttingen 1970.

[20] H. L. Schmid, *Über das Reziprozitätsgesetz in relativ-zyklischen algebraischen Funktionenkörpern mit endlichem Konstantenkörper*, Math. Zeit. **40**, (1936) S. 94-109.

[21] J. P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.

[22] J. P. Serre, *Linear Representations of Finite Groups*, Springer-Verlag, New York, 1977.

[23] J. P. Serre und J. Tate, *Good Reduction of Abelian Varieties*, Ann. Math. **88**, (1968), S. 492-517.

[24] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[25] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1999.

[26] J. Tate, *Fourier Analysis in Number Fields and Hecke's Zeta-Functions*, in: Algebraic Number Theory, herausgegeben von J.W.S Cassels und A. Fröhlich, Academic Press, London, 1967, S. 305-347.

[27] E.-W. Zink, *Ergänzungen zu Weils Exercices dyadiques*, Math. Nachr. **92**, (1979), S. 163-183.

Stichwortverzeichnis

Symbolverzeichnis

	Grundobjekte
K	lokaler Körper der Charakteristik 2, Seite 30
α,β	Elemente von K, Seite 30
$\mathcal{E}_{\alpha,\beta}$	elliptische Kurve uber K, Seite 30
L	Körper der der 3-Torsionspunkte von $\mathcal{E}_{\alpha,\beta}$, Seite 30
$\pi^K_{\alpha,\beta}$	zu $\mathcal{E}_{\alpha,\beta}$ gehörige Weildarstellung, Seite 28
$(\pi^K_{\alpha,\beta})'$	zu $\mathcal{E}_{\alpha,\beta}$ gehörige Weil-Deligne-Darstellung, Seite 28
	Hilfsobjekte
φ	primitive dritte Einheitswurzel, Seite 30
γ	dritte Wurzel von γ, Seite 30
ϵ, δ	Elemente einer zahmen Erweiterung von K, Seite 64
D, E, F_α	Elemente von K^{sep}, Seite 30
x_1, x_2, x_3, x_4	x-Koordinaten von 3-Torsionspunkten, Seite 31
Ω_K	unverzweigter Charakter von $W(K^{\text{sep}}/K)$, Seite 47
$\rho^K_{\alpha,\beta}$	unverzweigter Twist von $\pi^K_{\alpha,\beta}$, Seite 48
	Operationen mit Darstellungen
$(\cdot,\cdot)_G$	Verkettungszahl zweier Darstellungen einer Gruppe G
Tr	Spurabbildung einer Darstellung
$\bar{\pi}$	Restdarstellung der unverzweigten Weildarstellung π, Seite 12
$\tilde{\pi}$	projektive Darstellung der Weildarstellung π, Seite 14
Ind,Res	Induktion und Restriktion von Weildarstellungen, Seite 13
$\epsilon(\pi, \psi, dx)$	ϵ-Faktor der Weildarstellung π, Seite 17
$\lambda(M/K, \psi, dx, d_M x)$	λ-Faktor der Erweiterung M/K, Seite 18
$\text{cond}(\pi)$	Führer der Weildarstellung π, Seite 15
$\text{cond}(\pi')$	Führer der Weil-Deligne-Darstellung π', Seite 23
$\text{cond}_{\min}(\pi)$	minimaler Führer der Weildarstellung π, Seite 15

$\mathrm{cond}_{M/K}$	relativer Führer, Seite 20
$\mathrm{cond}(\psi)$	Führer des additiven Charakters ψ von K, Seite 17
	Verschiedenes
$G_i(M/K)$	i-te Verzweigungsgruppe von M/K
$\mathrm{i}_{M/K}(\sigma)$	kleinste nat. Zahl i mit $\sigma \notin G_i(M/K)$
$W(K^{\mathrm{sep}}/K)$	Weilgruppe von K, Seite 12
Φ_K	Frobeniuselement, Seite 12
ω_K	Betragscharakter von K bzw. $W(K^{\mathrm{sep}}/K)$, Seite 13, 14
ψ_K	fest gewählter additiver Charakter von K, Seite 17
$d_\psi x$	selbsduales Haarsches Maß, Seite 18
$\mathrm{e}(M/K)$	Verzweigungsindex von M/K
$\mathrm{f}(M/K)$	Trägheitsindex von M/K
$\mathrm{d}(M/K)$	Differentenexponent von M/K
Tr_M^K	Spurabbildung von M nach K
N_M^K	Normabbildung von M nach K
$[\cdot,\cdot]$	Kommutator zweier Gruppen
ρ_μ	cuspidale Darstellung von $GL_2(\mathbb{F}_3)$, Seite 50