Klassenkörpertheorie globaler Funktionenkörper und Anwendungen

Diplomarbeit

von
Maike Massierer

betreut von
Prof. Dr. Florian Heß

angefertigt am
Institut für Mathematik
der Technischen Universität Berlin

Juli 2009

Abstract. Das Ziel der Klassenkörpertheorie ist die Klassifizierung aller abelschen Erweiterungen eines gegebenen Grundkörpers. Sie erreicht dies, indem sie diese Erweiterungen bijektiv gewissen Untergruppen der Strahlklassengruppen zuordnet. Wir geben einen neuen Beweis des Existenzsatzes für globale Funktionenkörper und zeigen, wie man alle weiteren wesentlichen Aussagen der Klassenkörpertheorie daraus folgern kann. Die wichtigsten Werkzeuge dabei sind eine verallgemeinerte Tatepaarung und der Dichtigkeitssatz von Tschebotarev sowie Argumente aus Kummertheorie und Galoistheorie.

Inhaltsverzeichnis

Einführung

Die Klassenkörpertheorie als Teilgebiet der algebraischen Zahlentheorie entstand in der zweiten Hälfte des 19. Jahrhunderts aus der Frage heraus, wie die Stellen in einer gegebenen Erweiterung von Zahlkörpern verzweigen und zerlegen. Mit „Stellen“ sind hier die Äquivalenzklassen von nichttrivialen Bewertungen auf dem Grundkörper gemeint.

Es stellte sich heraus, dass sich die Galoiserweiterungen eines gegebenen Grundkörpers schon durch die Menge von Stellen, die in der jeweiligen Erweiterung voll zerlegt sind, klassifizieren lassen. Also versuchte man, die Menge aller Stellen zu bestimmen, die in einer gegebenen Erweiterung voll zerlegt sind, und umgekehrt Erweiterungen zu finden, in denen eine gegebene Menge von Stellen voll zerlegt ist.

Für abelsche Erweiterungen, das sind *endliche* Galoiserweiterungen mit abelscher Galoisgruppe, konnten diese Fragen in den folgenden Jahrzehnten konkret beantwortet werden. Dadurch wurde eine Klassifizierung aller abelschen Erweiterungen eines gegebenen Grundkörpers (aufgefasst als Teilerweiterungen in einem festen algebraischen Abschluss) erreicht. Mit anderen Worten konnte man die abelschen Erweiterungen nur durch die Arithmetik im Grundkörper selbst beschreiben.

Die Zukunft der nichtabelschen Klassenkörpertheorie war dagegen lange unklar, da der Ansatz für abelsche Erweiterungen nicht übertragen werden konnte. Erst mit der Vermutung von Langlands [Lan70b] wurden ab ca. 1970 auch auf diesem Gebiet Fortschritte gemacht. Diese Richtung ist heute als Langlands-Programm bekannt und liefert eine analytische Beschreibung der nichtabelschen Erweiterungen.

Trotzdem befasst sich die „klassische“ Klassenkörpertheorie mit *abelschen* Erweiterungen, und auch wir widmen uns ab sofort nur diesen. Die erste Fassung der abelschen Klassenkörpertheorie wurde ungefähr zwischen 1850 und 1930 von Kronecker, Weber, Hilbert, Furtwängler, Takagi, Artin, Hasse und anderen entwickelt.

Zahlkörper

Hilbert betrachtete zunächst nur unverzweigte Erweiterungen eines Zahlkörpers K. Für eine Untergruppe H der Idealklassengruppe $\mathcal{C}\ell_K$ definierte er einen *Klassenkörper zu* H als eine abelsche Erweiterung $L|K$, in der genau

die Ideale aus H total zerlegt sind. Alle wichtigen Aussagen die bis heute zum Hauptsatz der Klassenkörpertheorie gezählt werden wurden für diesen unverzweigten Fall schon 1907 von Hilberts Schüler Furtwängler bewiesen. Nämlich existiert zu jeder Untergruppe von $\mathcal{C}\ell_K$ ein eindeutig bestimmter Klassenkörper, und umgekehrt ist jede unverzweigte abelsche Erweiterung von K der Klassenkörper zu einer Untergruppe der Klassengruppe. Für den Klassenkörper L zu H gilt $\mathrm{Gal}(L|K) \cong \mathcal{C}\ell_K/H$ und die Ordnung des Bildes eines Primideals $\mathfrak{p}$ von K in der Gruppe $\mathcal{C}\ell_K/H$ ist sein Trägheitsgrad. Zur trivialen Untergruppe von $\mathcal{C}\ell_K$ gehört der *Hilbertsche Klassenkörper*, er ist die größte abelsche unverzweigte Erweiterung von K.

Im Jahr 1897 führte Weber (zunächst für imaginär-quadratische Körper) die *Strahlklassengruppen* $\mathcal{C}\ell_\mathfrak{m}$ ein, die es erlauben, auch die verzweigten abelschen Erweiterungen auf eine analoge Weise zu klassifizieren. Bei der Betrachtung von verzweigten Erweiterungen muss man die verzweigten Stellen gesondert behandeln. Sie werden in einem sogenannten *Erklärungsmodul* $\mathfrak{m}$ zusammengefasst, und die Strahlklassengruppe $\mathcal{C}\ell_\mathfrak{m}$ wird nur von denjenigen Idealen erzeugt, die $\mathfrak{m}$ nicht teilen. Für $\mathfrak{m} = 1$ ist $\mathcal{C}\ell_\mathfrak{m} = \mathcal{C}\ell_K$ die gewöhnliche Idealklassengruppe. Der Klassenkörper zu einer Untergruppe H von $\mathcal{C}\ell_\mathfrak{m}$ wird analog definiert, und alle abelschen Erweiterungen von K entstehen nun als Klassenkörper zu den Untergruppen der Strahlklassengruppen. Ist L der Klassenkörper zu $H \subseteq \mathcal{C}\ell_\mathfrak{m}$, so gilt wieder $\mathrm{Gal}(L|K) \cong \mathcal{C}\ell_\mathfrak{m}/H$, alle Stellen die $\mathfrak{m}$ nicht teilen sind unverzweigt in $L|K$ und die Ordnung ihres Bildes in $\mathcal{C}\ell_\mathfrak{m}/H$ ist wieder ihr jeweiliger Trägheitsgrad. Diese Aussagen wurden von Hilbert und Weber vermutet und von Takagi in einer Reihe von Veröffentlichungen zwischen 1915 und 1922 bewiesen.

Bis zu diesem Punkt gab man sich damit zufrieden, dass $\mathrm{Gal}(L|K)$ und $\mathcal{C}\ell_\mathfrak{m}/H$ isomorph sind, ohne den Isomorphismus explizit anzugeben. Erst Artin zeigte 1927 in [Art27], dass es einen kanonischen Isomorphismus $\mathcal{C}\ell_\mathfrak{m}/H \cong \mathrm{Gal}(L|K)$ gibt. Er wird gegeben durch die sogenannte Artinabbildung $(\cdot, L|K)$, die zu einer Galoiserweiterung $L|K$ gehört und die jedes unverzweigte Primideal auf seinen Frobeniusautomorphismus, also ein Element der Galoisgruppe, abbildet. Inspiriert vom Beweis des Tschebotarevschen Dichtigkeitssatzes [Tsc26] 1926 war Artin in der Lage, sein berühmtes Reziprozitätsgesetz zu beweisen, das heute als wichtiges Resultat der Klassenkörpertheorie gilt. Dazu bestimmte er den Kern seiner Artinabbildung so, dass dabei für den Klassenkörper L zu H genau die bekannte Isomorphie $\mathrm{Gal}(L|K) \cong \mathcal{C}\ell_\mathfrak{m}/H$ herauskommt. Im Grunde genommen zeigte er also, dass die Artinabbildung eine surjektive Abbildung $(\cdot, L|K) : \mathcal{C}\ell_\mathfrak{m} \to \mathrm{Gal}(L|K)$ induziert (die Surjektivität folgt schon aus dem Satz von Tschebotarev), und dass der Klassenkörper L zu H genau diejenige Erweiterung von K ist, für die H der Kern der zugehörigen Artinabbildung ist. Diese Charakterisierung liefert eine alternative und äquivalente Definition des Klassenkörpers, denn die Ordnung von $(\mathfrak{p}, L|K)$ ist genau der Trägheitsgrad von $\mathfrak{p}$. Also liegt $\mathfrak{p}$ genau dann in H, wenn $\mathfrak{p}$

voll zerlegt ist. Damit waren die Kernaussagen der Klassenkörpertheorie für Zahlkörper komplett.

Trotzdem steht die Forschung zur Klassenkörpertheorie seitdem nicht still. Viele Versuche, die Theorie zu verallgemeinern oder anders geartete Beweise zu finden, haben zu zahlreichen weiteren Ansätzen geführt. Zum Beispiel bedient sich der ursprüngliche Beweis von Artin in umfangreichem Maße einer analytischen Methode, der Theorie der L-Reihen. Viele waren jedoch der Meinung, dass algebraische Aussagen auch rein algebraische Beweise erlauben sollten. So untersuchten Albert, Brauer, Hasse und Noether zentrale einfache Algebren und Brauergruppen und fanden auf diesem Weg alternative Beweise, veröffentlicht 1932. Artin selbst hatte die Idee, dass Kohomologiegruppen in der Klassenkörpertheorie nützlich sein könnten. Hochschild, Nakayama, Tate, Weil, Serre und andere entwickelten um 1950 einen Ansatz, der die Brauergruppen-Argumente ersetzen konnte. Sowohl Brauergruppen als auch der Kohomologie-Ansatz finden sich in vielen Werken, die heute zur Standardliteratur der Klassenkörpertheorie gezählt werden, so auch in den meisten hier zitierten. Lediglich [Lan70a] bemüht sich um möglichst originalgetreue Beweise, [Mil08] gibt neben dem algebraisch-kohomologischen Ansatz auch den analytischen Ansatz für Zahlkörper wieder.

Schon 1930 übertrug Hasse die Klassenkörpertheorie auch auf lokale Körper und fragte sich, ob man die Aussagen für globale Körper nicht auch umgekehrt aus denen für die (eigentlich einfacher gearteten) lokalen Körper ableiten, oder zumindest einen rein lokalen Beweis für die lokale Klassenkörpertheorie finden könnte. Chevalley [Che54] löste mit seiner Einführung des neuen Begriffs „Idel“ zwischen 1933 und 1940 diese Fragen und noch eine weitere. Mit Hilfe der Ideltheorie ist es möglich, alle abelschen Erweiterungen durch Untergruppen *einer einzigen* Gruppe, der Idelklassengruppe, zu klassifizieren. Das ist nicht so natürlich, scheint aber eleganter, da man nicht mit den verschiedenen Strahlklassengruppen umgehen muss, und gilt vielen als der modernere Ansatz. Tatsächlich wählen alle hier erwähnten Lehrbücher außer Janusz [Jan73] und Serre [Ser88] den ideltheoretischen Ansatz (und folgern den globalen Fall uns dem lokalen), Gras [Gra03] behandelt beide im Vergleich. Im Gegensatz zu dieser „ideltheoretischen“ Variante der Klassenkörpertheorie nennt man den ursprünglichen Ansatz auch den „idealtheoretischen“.

Funktionenkörper

Die für diese Arbeit relevanteste Verallgemeinerung der Klassenkörpertheorie ist die auf Funktionenkörper. Hier leisteten Artin, Hasse, Dedekind, Schmidt, Witt, Weil, Chevalley, Lang, Serre und Drinfeld und andere entscheidende Beiträge. Artin und Tate [AT67] sowie Weil [Wei73] axiomatisieren die Klassenkörpertheorie soweit, dass sie neben Zahlkörpern auch auf globale Funktionenkörper zutrifft, ebenso Tate [CF67], der jedoch selbst auf eine Lücke in sei-

ner Argumentation im Funktionenkörper-Fall hinweist. Auch Lang [Lan70a] behauptet, dass seine Beweise mit „only minor modifications“ auch auf Funktionenkörper zutreffen. Serre beschäftigt sich in [Ser88] ausschließlich mit globalen Funktionenkörpern und präsentiert die Klassenkörpertheorie in der Sprache algebraischer Varietäten. Villa Salvador [Vil06] behandelt sowohl globale als auch lokale Funktionenkörper. Er präsentiert die idealtheoretische Fassung und wählt einen expliziten Ansatz nach Carlitz und Hayes, der auf dem Studium von Drinfeldmoduln beruht.

Viele der Argumente für Zahlkörper können tatsächlich mehr oder weniger direkt auch auf globale Funktionenkörper übertragen werden, so zum Beispiel Dichtigkeitsargumente nach Tschebotarev, und in mancherlei Hinsicht sind Funktionenkörper sogar einfacher zu behandeln, da sie im Gegensatz zu Zahlkörpern keine archimedischen Bewertungen besitzen. Trotzdem ist bei der Übertragung natürlich Vorsicht geboten.

Unabhängig von den Beweisen lassen sich die Aussagen der Klassenkörpertheorie für globale Funktionenkörper ganz analog zum Zahlkörper-Fall formulieren, hier studiert man also Erweiterungen eines Grundkörpers, in dem bestimmte Stellen total zerlegt sind. Wir wählen in dieser Arbeit eine moderne aber idealtheoretische Formulierung. Als Modul $\mathfrak{m}$ dient immer ein effektiver Divisor des Grundkörpers F und die Strahlklassen aus $\mathcal{C}\ell_{\mathfrak{m}}$ enthalten nur Divisoren mit Träger disjunkt zu $\mathfrak{m}$. Dann existiert laut Klassenkörpertheorie zu jeder Untergruppe H von $\mathcal{C}\ell_{\mathfrak{m}}$ von endlichem Index eine abelsche Erweiterung E von F so dass $\mathrm{Gal}(E|F) \cong \mathcal{C}\ell_{\mathfrak{m}}/H$, wobei die Isomorphie durch die Artinabbildung $(\cdot, E|F)$ gegeben wird. Im Gegensatz zu Zahlkörpern sind bei Funktionenkörpern die Strahlklassengruppen unendlich, deshalb können nur Untergruppen von endlichem Index betrachtet werden, um endliche Erweiterungen zu produzieren. Man kann leicht zeigen, dass E durch diese Bedingung bereits eindeutig bestimmt ist, und dass $E|F$ unverzweigt außerhalb des Trägers von $\mathfrak{m}$ ist. Weiter entstehen schon alle abelschen Erweiterungen von F auf diese Weise. Da diese Resultate in erster Linie Existenzaussagen sind, werden sie auch *Existenzsatz der Klassenkörpertheorie* genannt. Zusammen mit einigen weiteren Aussagen (zum Beispiel funktorielle Eigenschaften der Abbildung $H \mapsto E$), die leicht daraus folgen, bilden sie den Hauptsatz der Klassenkörpertheorie, und auch das Artinsche Reziprozitätsgesetz lässt sich mit wenig Aufwand daraus herleiten.

Diese Arbeit

Diese Arbeit reiht sich ein in die lange Folge von Versuchen, die Klassenkörpertheorie zu vereinfachen und zu verschönern. Wir geben einen neuen Beweis des Existenzsatzes für globale Funktionenkörper und zeigen, wie man die restlichen Aussagen daraus folgert. Während die bekannten Beweise zwar elegant, aber sehr abstrakt, lang und technisch sind, sich ihrerseits tiefer Theorien wie L-Reihen, Brauergruppen oder Kohomologiegruppen bedienen

und dabei manchmal die Intuition verloren geht, was eigentlich passiert, wählen wir einen recht konkreten Ansatz.

Wir konstruieren eine neue Paarung, eine Verallgemeinerung der aus der Kryptographie bekannten Tatepaarung, und bedienen uns außerdem noch der Kummertheorie, um explizit eine Korrespondenz zwischen den Untergruppen der Strahlklassengruppen und den abelschen Erweiterungen herzustellen, die dann offensichtlich die geforderten Eigenschaften besitzt. Dabei gehen einige bekannte und eher elementare Resultate über Paarungen ein. Außerdem benötigen wir den (hochgradig nichttrivialen) Tschebotarevschen Dichtigkeitssatz, der längst auf globale Funktionenkörper übertragen wurde. Die Kummertheorie ist wohlbekannt, erfordert jedoch die folgende Fallunterscheidung. Erweiterungen mit Grad teilerfremd zur Charakteristik, die sogenannten Kummererweiterungen, müssen separat von den Artin-Schreier-Witt-Erweiterungen, deren Grad eine Potenz der Charakteristik ist, behandelt werden. Deshalb müssen wir sogar zwei Paarungen definieren, eine von multiplikativem, die andere von additivem Charakter, um mit beiden dann dieselbe Konstruktion durchzuführen. Im Kummer-Fall erfordern Erweiterungen vom Grad n, für die nicht alle n-ten Einheitswurzeln im Grundkörper enthalten sind, eine recht aufwändige besondere Behandlung. Dort spielen Argumente aus der Galoistheorie eine wesentliche Rolle.

Trotz dieses Beweises in mehreren Schritten glauben wir, dass dieser Ansatz sehr intuitiv und gut nachvollziehbar ist. Interessant ist auch, dass eine bisher eher aus der Anwendung, vor allem der paarungsbasierten Kryptographie, bekannte Paarung hier Anwendung in einem sehr reinen Gebiet der algebraischen Zahlentheorie findet. Paarungen sind ein Bindeglied zwischen diesen beiden verwandten Disziplinen, das es sich lohnt besser zu versehen.

Roadmap

Zu Beginn dieser Arbeit legen wir die notwendigen Grundlagen und führen wichtige Notation ein. In Kapitel 2 stellen wir die Hauptaussagen der Klassenkörpertheorie vor. Wie bereits erwähnt steckt die meiste Arbeit im Beweis des Existenzsatzes. Wir nehmen zunächst seine Gültigkeit an und folgern daraus alle weiteren wichtigen Aussagen der Klassenkörpertheorie im Funktionenkörper-Fall. Dies ist ohne großen Aufwand möglich. Wir zeigen hier auch eine Aussage über die Größe des Konstantenkörpers des Klassenkörpers, das natürlich nicht zum Standardstoff der Klassenkörpertheorie in Zahlkörpern gehört. Am Ende des Kapitels formulieren wir im Hauptsatz der Klassenkörpertheorie zusammenfassend alle Aussagen, die im Laufe der Arbeit gezeigt wurden und werden.

Dann machen wir uns an den Hauptinhalt dieser Arbeit, nämlich an den Beweis des Existenzsatzes. Dazu definieren wir in Kapitel 3 eine neue Paarung, die eine Verallgemeinerung von Kummer- und Tatepaarung ist, und

zeigen deren Nichtausartung. Damit beweisen wir in Kapitel 4 den Existenzsatz in einer Unterscheidung von drei Fällen, wobei wir nur für die ersten beiden Fälle alle Details ausführen. Wir behandeln zunächst Kummererweiterungen, d.h. Erweiterungen vom Grad n teilerfremd zur Charakteristik des Grundkörpers F, wobei die n-ten Einheitswurzeln in F enthalten sind. Danach verallgemeinern wir die Resultate auf den Fall, dass die Einheitswurzeln nicht alle in F enthalten sind. Schließlich machen wir einige Bemerkungen zu den Artin-Schreier-Witt-Erweiterungen und bauen die betrachteten Fälle zusammen, um allgemeine Erweiterungen behandeln zu können.

Am Anfang jedes Kapitels und Abschnitts werden Voraussetzungen definiert. Sie sind durch kursive Schrift hervorgehoben und gelten jeweils für das ganze Kapitel bzw. den Abschnitt.

Schlussbemerkungen

Als Standardwerke der Klassenkörpertheorie gelten heute (unter anderem) [AT67, CF67, Lan70a, Wei73, Jan73, Ser79, Ser88, Neu92] und [Mil08]. Letzteres gibt auch eine ausführliche historische Einführung in die Klassenkörpertheorie, aus der viele Informationen in diesem Kapitel stammen. Gras [Gra03] ist ein unkonventionelleres Werk, das die Beweise der zentralen Aussagen auslässt, dafür aber mehr Gewicht auf Anschauung und Anwendung legt.

Zum Schluss weisen wir noch darauf hin, dass es sich bei der Klassenkörpertheorie um ein sehr altes und tiefes Gebiet der algebraischen Zahlentheorie handelt, und dass sowohl die hier genannten Ansätze und Namen als auch die zitierten Werke nicht den geringsten Anspruch auf Vollständigkeit erheben. Wir verzichten sogar weitestgehend darauf, die ursprünglichen Publikationen anzugeben, da sie sehr zahlreich und zum Teil schwer zugänglich sind. Ausführliche Darstellungen der geschichtlichen Entwicklung der Klassenkörpertheorie inklusive langen Listen von Originalreferenzen sind zu finden in [Has66] sowie [CF67, Kap. XI], für globale Funktionenkörper in [Roq02].

Dank

Mein Dank gilt zuerst meinem Betreuer Florian Heß für das interssante Thema, die tatkräftige Unterstützung und viele gute Ideen. Ebenso geht ein herzliches Dankeschön an alle Kommilitonen und Kollegen der KANT-Gruppe und insbesondere an Doris, Gerriet, Moritz und Thorsten für viele interessante und anregende Gespräche und die Antworten auf unzählige Fragen sowie an Doris, Florin und Osman für das sorgfältige Korrekturlesen dieser Arbeit. Zum Abschluss meines Studiums möchte ich auch meinen Eltern für ihre liebevolle Unterstützung während meiner gesamten Studienzeit danken.

Kapitel 1

Grundlagen

In diesem Kapitel werden die wichtigsten Grundlagen eingeführt, die in dieser Arbeit benötigt werden und den Standardstoff einer Algebra-II-Vorlesung überschreiten. Insbesondere Körpertheorie und Galoistheorie werden also vorausgesetzt. Wir bemühen uns, die hier eingeführte Notation in der gesamten Arbeit beizubehalten, die wichtigsten Bezeichnungen finden sich auch im Symbolverzeichnis.

Wir starten mit allgemeineren Themen wie Funktionenkörpern, Paarungen und Kummertheorie und widmen uns im Anschluss den spezielleren Grundbegriffen und Voraussetzungen für die Klassenkörpertheorie, insbesondere den Strahlklassengruppen, der Artinabbildung und dem Tschebotarevschen Dichtigkeitssatz.

1.1 Funktionenkörper

Dieser Abschnitt führt die grundlegenden Begriffe der Funktionenkörpertheorie ein. Eine ausführlichere Darstellung des Stoffes ist in [Sti93] und [Vil06] zu finden.

$$\begin{array}{c} F \\ \Big| \text{ algebraisch} \\ K(x) \\ \Big| \text{ transzendent} \\ K \end{array}$$

Definition 1.1. Sei K ein Körper. Ein *algebraischer Funktionenkörper F in einer Variablen über K,* kurz *Funktionenkörper,* ist eine endlich erzeugte Körpererweiterung $F|K$ vom Transzendenzgrad 1. In diesem Zusammenhang wird K der *Konstantenkörper* von F genannt. Der algebraische Abschluss K_0 von K in F heißt *exakter Konstantenkörper* von F. Ein Funktionenkörper mit endlichem Konstantenkörper heißt *globaler Funktionenkörper.*

In dieser Arbeit betrachten wir ausschließlich globale Funktionenkörper F über dem endlichen Körper $K = \mathbb{F}_q$ mit q Elementen. Die Erweiterung $K_0|K$ hat endlichen Grad, und so können wir ohne Beschränkung der Allgemeinheit davon ausgehen, dass K der *exakte* Konstantenkörper von F ist.

Voraussetzungen und Notation 1.2. *Im Folgenden sei also F ein globaler Funktionenkörper über dem exakten Konstantenkörper $K = \mathbb{F}_q$.*

Definition 1.3. Eine *Stelle* $\mathfrak{p}$ von $F|K$ ist das (eindeutig bestimmte) maximale Ideal eines (diskreten) Bewertungsrings von F, der K enthält. Wir bezeichnen den zugehörigen Bewertungsring mit $\mathcal{O}_\mathfrak{p}$, die zugehörige (exponentielle) diskrete Bewertung mit $v_\mathfrak{p} : F \to \mathbb{Z} \cup \{\infty\}$ und die Menge aller Stellen von $F|K$ mit $\mathcal{S}_F$.

$\mathcal{O}_\mathfrak{p}$ ist ein Hauptidealring und $\mathfrak{p}$ demnach ein Hauptideal. Ein Erzeuger t von $\mathfrak{p}$ heißt *Primelement* für $\mathfrak{p}$ und hat Bewertung $v_\mathfrak{p}(t) = 1$. Es ist $\mathfrak{p} = \mathcal{O}_\mathfrak{p} \setminus \mathcal{O}_\mathfrak{p}^\times$ und für $f \in F^\times$ gilt $f \in \mathfrak{p} \Leftrightarrow f^{-1} \notin \mathcal{O}_\mathfrak{p}$. Für jede Stelle $\mathfrak{p}$ von F ist $K \subseteq \mathcal{O}_\mathfrak{p}$ und $K \cap \mathfrak{p} = \{0\}$. Die Bewertungen $v_\mathfrak{p}$ sind surjektiv und es gilt $v_\mathfrak{p}(c) = 0$ für alle $c \in K^\times$. Stellen, Bewertungsringe und diskrete Bewertungen hängen folgendermaßen zusammen.

$$\begin{aligned} \mathcal{O}_\mathfrak{p} &= \{f \in F \mid v_\mathfrak{p}(f) \geq 0\} \\ \mathcal{O}_\mathfrak{p}^\times &= \{f \in F \mid v_\mathfrak{p}(f) = 0\} \\ \mathfrak{p} &= \{f \in F \mid v_\mathfrak{p}(f) > 0\} \end{aligned}$$

Definition 1.4. Sei $\mathfrak{p}$ eine Stelle von $F|K$. Der Körper $F_\mathfrak{p} := \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ heißt *Restklassenkörper* von $\mathfrak{p}$. Die *Restklassenabbildung* $F \to F_\mathfrak{p} \cup \{\infty\}, f \mapsto f(\mathfrak{p})$ wird definiert durch

$$f(\mathfrak{p}) := \begin{cases} \text{Restklasse von } f \text{ modulo } \mathfrak{p} & \text{für } f \in \mathcal{O}_\mathfrak{p} \\ \infty & \text{für } f \in F \setminus \mathcal{O}_\mathfrak{p}. \end{cases}$$

Haben wir es mit einem *globalen* Funktionenkörper zu tun, so sind alle Restklassenkörper endlich. Die Elemente des Körpers F können auch als Funktionen $f : \mathcal{S}_F \to F_\mathfrak{p} \cup \{\infty\},\ \mathfrak{p} \mapsto f(\mathfrak{p})$ verstanden werden (daher der Name „Funktionenkörper“), dabei sind die Elemente aus K konstante Funktionen (daher der Name „Konstantenkörper“). Die Restklassenabbildung liefert eine kanonische Einbettung $K \hookrightarrow F_\mathfrak{p}$, weshalb wir K als Teilkörper von $F_\mathfrak{p}$ auffassen können, und der Körpergrad $[F_\mathfrak{p} : K]$ ist stets endlich.

Definition 1.5. Der *Grad* einer Stelle $\mathfrak{p}$ wird definiert durch

$$\deg(\mathfrak{p}) := [F_\mathfrak{p} : K].$$

Man nennt $\mathfrak{p}$ eine *Nullstelle* von $f \in F$, wenn $v_\mathfrak{p}(f) > 0$ und einen *Pol* von f, wenn $v_\mathfrak{p}(f) < 0$.

Es ist leicht zu zeigen, dass ein transzendentes Element aus F mindestens eine Nullstelle und einen Pol besitzt. Insbesondere ist also $\mathcal{S}_F \neq \emptyset$, mehr noch, jeder Funktionenkörper hat sogar unendlich viele Stellen. Letzteres folgt aus

dem Approximationssatz 1.8. Ebenso folgt daraus, dass jedes Element $f \in F^\times$ nur endlich viele Nullstellen und Polstellen haben kann.

Ein sehr grundlegender Begriff der Funktionenkörpertheorie sind die Divisoren. Hierbei handelt es sich um formale (endliche) Summen der Stellen eines Funktionenkörpers.

Definition 1.6. Die freie abelsche Gruppe, die von den Stellen von $F|K$ erzeugt wird, heißt *Divisorengruppe* und wird mit $\mathcal{D}_F$ bezeichnet. Die Gruppe wird additiv geschrieben, ein *Divisor* $\mathfrak{D} \in \mathcal{D}_F$ ist also eine formale Summe

$$\mathfrak{D} = \sum_{\mathfrak{p} \in \mathcal{S}_F} d_\mathfrak{p} \cdot \mathfrak{p} \quad \text{mit } d_\mathfrak{p} \in \mathbb{Z} \text{ und fast allen } d_\mathfrak{p} = 0.$$

Die Menge

$$\operatorname{supp}(\mathfrak{D}) := \{\mathfrak{p} \in \mathcal{S}_F \mid d_\mathfrak{p} \neq 0\}$$

ist daher stets endlich, sie heißt *Träger* von $\mathfrak{D}$. Eine Stelle $\mathfrak{p} \in \mathcal{S}_F$ wird oft auch *Primdivisor* genannt. Die Gradfunktion wird auf der Divisorengruppe linear fortgesetzt und liefert einen Homomorphismus $\mathcal{D}_F \to \mathbb{Z}$,

$$\deg(\mathfrak{D}) := \sum_{\mathfrak{p} \in \mathcal{S}_F} d_\mathfrak{p} \cdot \deg(\mathfrak{p}).$$

Oft bezeichnet man $d_\mathfrak{p}$ auch mit $v_\mathfrak{p}(\mathfrak{D})$. Für zwei Divisoren schreibt man $\mathfrak{D} \geq \mathfrak{C}$, wenn $v_\mathfrak{p}(\mathfrak{D}) \geq v_\mathfrak{p}(\mathfrak{C})$ für alle Koeffizienten gilt. Ein Divisor $\mathfrak{D} \geq 0$ heißt *effektiv*.

Da jedes Element $f \in F^\times$ nur endlich viele Nullstellen und Pole in $\mathcal{S}_F$ hat, ist die folgende Definition sinnvoll.

Definition 1.7. Für $f \in F^\times$ heißt der Divisor

$$(f) := \sum_{\mathfrak{p} \in \mathcal{S}_F} v_\mathfrak{p}(f) \cdot \mathfrak{p}$$

Hauptdivisor von f, die Gruppe der Hauptdivisoren bezeichnen wir mit $\mathcal{P}_F$. Die Faktorgruppe $\mathcal{C}\ell_F := \mathcal{D}_F/\mathcal{P}_F$ heißt *Divisorenklassengruppe* von F und ihre Elemente, die *Divisorenklassen,* bezeichnen wir mit $[\mathfrak{D}]$.

Es gilt $(f) = 0 \Leftrightarrow f \in K^\times$, die Abbildung $(\cdot) : F^\times \to \mathcal{D}_F$ ist also ein Homomorphismus mit Kern $K^\times$ und Bild $\mathcal{P}_F$ und man erhält die exakte Sequenz

$$1 \to K^\times \to F^\times \to \mathcal{D}_F \to \mathcal{C}\ell_F \to 0.$$

Hauptdivisoren haben den Grad 0, für zwei Divisoren $\mathfrak{C}$ und $\mathfrak{D}$ mit $[\mathfrak{C}] = [\mathfrak{D}]$ ist also $\deg(\mathfrak{C}) = \deg(\mathfrak{D})$ und die Gradfunktion $\deg : \mathcal{C}\ell_F \to \mathbb{Z}$ ist auch auf Divisorenklassen wohldefiniert. Mit $\mathcal{C}\ell_F^0$ bezeichnen wir die *Nullklassengruppe,*

die genau die Divisorenklassen vom Grad 0 umfasst. Die Nullklassengruppe eines globalen Funktionenkörpers ist immer endlich (siehe [Sti93, Prop. V.1.3, S. 159]), während die Klassengruppe unendlich ist.

Der Satz von Schmidt (siehe [Sti93, Kor. V.1.11, S. 164]) sagt aus, dass ein globaler Funktionenkörper immer Divisoren vom Grad 1 besitzt. Damit erhält man eine exakte Sequenz

$$0 \to \mathcal{C}\ell_F^0 \to \mathcal{C}\ell_F \to \mathbb{Z} \to 0$$

(siehe [Ros02, S. 50]), wobei $\mathcal{C}\ell_F \to \mathbb{Z}$ die Gradfunktion ist. Es gilt die Isomorphie $\mathcal{C}\ell_F \cong \mathcal{C}\ell_F^0 \times \mathbb{Z}$, sie ist gegeben durch $[\mathfrak{D}] \xmapsto{\sim} ([\mathfrak{D} - \mathfrak{A} \cdot \deg(\mathfrak{D})], \deg(\mathfrak{D}))$, wenn $\mathfrak{A}$ ein fest gewählter Divisor vom Grad 1 ist.

Der folgende Satz wird auch *starker Approximationssatz* genannt, er ist eine Verschärfung des schwachen Approximationssatzes und ein wichtiges Hilfsmittel in der Divisorentheorie.

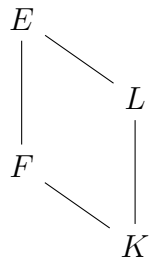
Satz 1.8 (Approximationssatz)**.** *Sei $F|K$ ein Funktionenkörper und $\mathcal{T}$ eine echte Teilmenge von $\mathcal{S}_F$ mit $\mathfrak{p}_1, \ldots, \mathfrak{p}_r \in \mathcal{T}$. Es seien $f_1, \ldots, f_r \in F$ und $\alpha_1, \ldots, \alpha_r \in \mathbb{Z}$ gegeben. Dann gibt es ein $f \in F$ so dass*

$$v_{\mathfrak{p}_i}(f - f_i) = \alpha_i \quad \forall\ i = 1, \ldots, r \quad \textit{und}$$
$$v_{\mathfrak{p}}(f) \geq 0 \quad \forall\ \mathfrak{p} \in \mathcal{T} \setminus \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}.$$

Beweis. [Sti93, Thm. I.6.4, S. 31], das Resultat ist eine Folgerung aus dem Satz von Riemann-Roch. □

Bei uns kommt dieser Satz häufig in der folgenden Form zur Anwendung: Der Repräsentant $\mathfrak{D} = \sum_{\mathfrak{p} \in \mathcal{S}_F} d_{\mathfrak{p}} \cdot \mathfrak{p}$ einer Divisorenklasse $[\mathfrak{D}] \in \mathcal{C}\ell_F$ kann an endlich vielen Stellen $\mathfrak{p}_i$ so abgeändert werden, dass die Koeffizienten beliebig vorgegebene Werte $\tilde{d}_{\mathfrak{p}_i}$ annehmen. Wählt man nämlich $f_i = 0$ und $\alpha_i = \tilde{d}_{\mathfrak{p}_i} - d_{\mathfrak{p}_i}$, so gibt es nach dem Approximationssatz ein $f \in F^\times$ mit $v_{\mathfrak{p}_i}(f) = \tilde{d}_{\mathfrak{p}_i} - d_{\mathfrak{p}_i}$, und der Repräsentant $\mathfrak{D} + (f)$ von $[\mathfrak{D}]$ hat bei $\mathfrak{p}_i$ den Koeffizienten $\tilde{d}_{\mathfrak{p}_i}$.

Zuletzt wenden wir uns noch den Erweiterungen von Funktionenkörpern zu. Darunter verstehen wir immer eine *algebraische* Erweiterung E von F mit (exaktem) Konstantenkörper $L \supseteq K$. Dabei soll E selbstverständlich wieder ein algebraischer Funktionenkörper sein.



Sei also $E|L$ eine Erweiterung von $F|K$. Dann ist auch $L|K$ eine algebraische Körpererweiterung und es gilt $F \cap L = K$. Die Erweiterung $E|F$ hat genau dann endlichen Grad, wenn $L|K$ endlich ist.

Im Zusammenhang mit Funktionenkörpererweiterungen studiert man unter anderem die Beziehungen zwischen Stellen und Divisoren im „oberen“ und „unteren“ Körper.

Definition 1.9. Eine Stelle $\mathfrak{P}$ von E *liegt über* $\mathfrak{p} \in \mathcal{S}_F$, wenn $\mathfrak{p} \subseteq \mathfrak{P}$ gilt. Man sagt auch $\mathfrak{p}$ *liegt unter* $\mathfrak{P}$ und schreibt $\mathfrak{P}|\mathfrak{p}$.

Für Stellen $\mathfrak{P}|\mathfrak{p}$ gilt $\mathfrak{p} = \mathfrak{P} \cap F$ und $\mathcal{O}_\mathfrak{p} = \mathcal{O}_\mathfrak{P} \cap F$, unter jeder Stelle von E liegt also eindeutig eine Stelle $\mathfrak{p}$ von F. Umgekehrt liegen über einer Stelle von F mindestens eine und stets nur endlich viele Stellen von E.

Definition 1.10. Für ein $\mathfrak{P} \in \mathcal{S}_E$ über $\mathfrak{p} \in \mathcal{S}_F$ gibt es ein $e \in \mathbb{Z}^{>0}$ mit $v_\mathfrak{P}(f) = e \cdot v_\mathfrak{p}(f)$ für alle $f \in F$. Die Zahl $e(\mathfrak{P}|\mathfrak{p}) := e$ heißt *Verzweigungsindex* von $\mathfrak{P}$ über $\mathfrak{p}$. Wenn $e(\mathfrak{P}|\mathfrak{p}) = 1$ gilt, ist $\mathfrak{P}|\mathfrak{p}$ *unverzweigt,* sonst *verzweigt,* und eine verzweigte Stelle heißt *zahm verzweigt*, wenn $\mathrm{char}(F) \nmid e(\mathfrak{P}|\mathfrak{p})$, sonst *wild verzweigt*. Die Stelle $\mathfrak{p}$ heißt *unverzweigt in* $E|F$, wenn $\mathfrak{P}|\mathfrak{p}$ für alle Stellen $\mathfrak{P}$ über $\mathfrak{p}$ unverzweigt ist, sonst *verzweigt.* Die Erweiterung $E|F$ heißt *unverzweigt*, wenn alle Stellen $\mathfrak{p}$ von F unverzweigt in $E|F$ sind, sonst *verzweigt*, und Entsprechendes gilt für zahme und wilde Verzweigung. Die Stelle $\mathfrak{p}$ heißt *total verzweigt* in $E|F$, wenn nur genau eine Stelle $\mathfrak{P}$ darüber liegt mit $e(\mathfrak{P}|\mathfrak{p}) = [E : F]$, und sie heißt *voll zerlegt*, wenn genau $[E : F]$ Stellen darüber liegen.

Jede endliche separable Erweiterung von Funktionenkörpern besitzt nur endlich viele verzweigte Stellen (siehe [Sti93, Kor. III.5.5., S. 95]). Dies ist ein sehr nützliches Resultat, da verzweigte Stellen oft eine besondere Behandlung erfordern. Um die Verzweigung von Stellen genauer studieren zu können, definiert man eine weitere damit zusammenhängende Größe, den Trägheitsgrad.

Für $\mathfrak{P}|\mathfrak{p}$ kann der Restklassenkörper $F_\mathfrak{p}$ kanonisch in den Restklassenkörper $E_\mathfrak{P}$ eingebettet werden durch $f(\mathfrak{p}) \mapsto f(\mathfrak{P})$ für $f \in \mathcal{O}_\mathfrak{p}$. So betrachten wir $F_\mathfrak{p}$ als Teilkörper von $E_\mathfrak{P}$.

Definition 1.11. Der Körpergrad $f(\mathfrak{P}|\mathfrak{p}) := [E_\mathfrak{P} : F_\mathfrak{p}]$ heißt *Trägheitsgrad* von $\mathfrak{P}|\mathfrak{p}$.

Während der Verzweigungsindex immer eine natürliche Zahl ist, kann der Trägheitsgrad auch unendlich sein. Er ist genau dann endlich, wenn $E|F$ endlichen Erweiterungsgrad hat. In diesem Fall gilt ein weiteres sehr nützliches Resultat über den Zusammenhang der beiden Größen.

Satz 1.12. *Es sei $E|L$ eine endliche Erweiterung von $F|K$, $\mathfrak{p}$ eine Stelle von F und $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ alle über $\mathfrak{p}$ liegenden Stellen von E. Dann gilt*

$$[E : F] = \sum_{i=1}^{k} e(\mathfrak{P}_i|\mathfrak{p}) \cdot f(\mathfrak{P}_i|\mathfrak{p}).$$

Beweis. [Sti93, Thm. III.1.11, S. 64] □

Ist eine Stelle $\mathfrak{p}$ voll zerlegt, so gilt also $e(\mathfrak{P}|\mathfrak{p}) = f(\mathfrak{P}|\mathfrak{p}) = 1$ für alle $\mathfrak{P}$ über $\mathfrak{p}$. Eine recht konkrete Aussage über die Art der Verzweigung in bestimmten Situationen macht der Satz von Kummer (siehe [Sti93, Thm. III.3.7, S. 76]). Auch sehr hilfreich ist der folgende Satz.

Satz 1.13. *Seien E_1 und E_2 Galoiserweiterungen von F. Eine Stelle von F ist genau dann im Kompositum E_1E_2 unverzweigt (total zerlegt), wenn sie in E_1 und E_2 unverzweigt (total zerlegt) ist.*

Beweis. [Ros02, Prop. 9.8, S. 120] □

Definition 1.14. $E|L$ ist eine *Konstantenkörpererweiterung* von $F|K$, wenn $E = FL$ gilt.

Konstantenkörpererweiterungen haben viele besondere Eigenschaften, für eine Zusammenfassung hiervon siehe zum Beispiel [Sti93, Kap. III.6].

1.2 Paarungen

Paarungen spielen eine wichtige Rolle in der modernen Funktionenkörpertheorie allgemein und in dieser Arbeit speziell. Insbesondere verwenden wir eine aus der Tatepaarung und der Kummerpaarung zusammengesetzte Paarung, um den Existenzsatz zu beweisen. Bevor diese beiden speziellen Paarungen eingeführt werden, stellt dieser Abschnitt einige wichtige allgemeine Aspekte dar. Der Aufbau orientiert sich an [Hes08, Kap. 6.8] und [Lan93, Kap. I §9].

Voraussetzungen und Notation 1.15. *In diesem Abschnitt seien A und B stets endliche abelsche Gruppen, n eine natürliche Zahl und μ_n die Gruppe der n-ten Einheitswurzeln.*

Definition 1.16. Eine *Paarung* von A und B in die multiplikative Gruppe μ_n ist eine bilineare Abbildung $\pi : A \times B \to \mu_n$.

Eine Paarung definiert und wird definiert durch die zwei Homomorphismen $\psi_1 : A \to \mathrm{Hom}(B, \mu_n)$ und $\psi_2 : B \to \mathrm{Hom}(A, \mu_n)$.

Definition 1.17. Die Paarung π heißt *nicht ausgeartet*, falls ψ_1 und ψ_2 injektiv sind.

Bemerkung 1.18. Oft werden Paarungen auch mit Bildbereich $\mathbb{Z}/n\mathbb{Z}$ definiert. Dies ist für alles Weitere unerheblich, wichtig ist nur, dass es sich hier um eine zyklische Gruppe der Ordnung n handelt.

Wir geben nun ein paar elementare Resultate über Paarungen an. Dabei sagen wir, dass eine Gruppe A den *Exponenten* n hat, falls $a^n = 1$ für alle $a \in A$.

Lemma 1.19. *Sei A eine endliche abelsche Gruppe vom Exponenten n. Dann existiert ein (nicht kanonischer) Isomorphismus $A \cong \mathrm{Hom}(A, \mu_n)$.*

Beweis. [Bos06, Kap. 4.9 Lemma 2, S. 208] □

Lemma 1.20. *Seien A und B endliche abelsche Gruppen und $\pi : A \times B \to \mu_n$ eine nicht ausgeartete Paarung. Dann gilt:*

(*i*) *A und B besitzen den Exponenten n.*

(*ii*) $\#A = \#B$

(*iii*) *Die Monomorphismen ψ_1 und ψ_2 sind Isomorphismen, demnach gilt also $A \cong \mathrm{Hom}(B, \mu_n)$ und $B \cong \mathrm{Hom}(A, \mu_n)$. Daraus ergibt sich eine (nicht kanonische) Isomorphie $A \cong B$.*

Beweis. Klar, für die letzte Aussage verwende Lemma 1.19. □

Mit diesen beiden Lemmata zeigt sich ganz leicht:

Lemma 1.21. *Es seien A und B endliche abelsche Gruppen vom Exponenten n. Eine Paarung $\pi : A \times B \to \mu_n$ ist genau dann nicht ausgeartet, wenn der zugehörige Homomorphismus $\psi_1 : A \to \mathrm{Hom}(B, \mu_n)$ injektiv ist und A und B dieselbe Kardinalität haben.*

Beweis. [Hes04, Bem. 5] □

Mit Hilfe einer nicht ausgearteten Paarung $\pi : A \times B \to \mu_n$ können wir nun eine Bijektion zwischen der Menge $\mathcal{U}_A$ der Untergruppen von A und der Menge $\mathcal{U}_B$ der Untergruppen von B definieren. Eine solche Bijektion spielt im Kapitel 4 beim Beweis des Existenzsatzes eine wichtige Rolle. Wir definieren die Abbildungen

$$\begin{aligned} \eta_1 : \mathcal{U}_A &\to \mathcal{U}_B \\ U &\mapsto \{b \in B \mid \pi(u, b) = 1 \quad \forall\, u \in U\} \end{aligned}$$

und

$$\begin{aligned} \eta_2 : \mathcal{U}_B &\to \mathcal{U}_A \\ V &\mapsto \{a \in A \mid \pi(a, v) = 1 \quad \forall\, v \in V\}. \end{aligned}$$

Wir bilden also eine Untergruppe U von A auf den Kern der Abbildung $\psi_2 : B \to \mathrm{Hom}(U, \mu_n)$, den sogenannten „rechten Kern“ von π, ab, der ja eine

Untergruppe von B ist. Dabei entsteht $\mathrm{Hom}(U, \mu_n)$ aus $\mathrm{Hom}(A, \mu_n)$ durch Einschränkung. Ganz analog bilden wir eine Untergruppe V von B auf den „linken Kern“ von π ab. Hiermit gilt nun der folgende Satz.

Satz 1.22. *Es seien A und B endliche abelsche Gruppen und $\pi : A \times B \to \mu_n$ eine nicht ausgeartete Paarung.*

(*i*) *Es gilt $\#U = \#B/\eta_1(U)$ für alle $U \in \mathcal{U}_A$ und $\#V = \#A/\eta_2(V)$ für alle $V \in \mathcal{U}_V$.*

(*ii*) *Die beiden induzierten Paarungen $U \times B/\eta_1(U) \to \mu_n$ für $U \in \mathcal{U}_A$ und $A/\eta_2(V) \times V \to \mu_n$ für $B \in \mathcal{U}_B$ sind nicht ausgeartet.*

(*iii*) *Es ist $\eta_2 \circ \eta_1 = \mathrm{id}_{\mathcal{U}_A}$ und $\eta_1 \circ \eta_2 = \mathrm{id}_{\mathcal{U}_B}$.*

Beweis. [Hes08, Lemma 6.43, S. 209] □

Die Abbildungen η_1 und η_2 sind also zueinander inverse Bijektionen zwischen den Mengen $\mathcal{U}_A$ und $\mathcal{U}_B$. Man überprüft auch leicht, dass sie inklusionsumkehrend sind.

1.3 Multiplikative Kummertheorie

Dieser Abschnitt ist einer kurzen Einführung in die Kummertheorie gewidmet. Eine ausführliche Darstellung des Stoffes findet man in [Hes08, Kap. 6.8], [Bos06, Kap. 4.9] und vielen anderen Algebra-Lehrbüchern (man beachte die leicht unterschiedlichen Definitionen des Exponenten einer Gruppe A als ein *beliebiges* bzw. das *kleinste* n so dass $a^n = 1$ für alle $a \in A$ in der Literatur – wir verstehen darunter ein *beliebiges* solches n).

Eine Galoiserweiterung $E|F$ heißt abelsch, zyklisch, vom Exponenten n, etc., wenn ihre Galoisgruppe diese Eigenschaft hat. Wenn wir von „abelschen“, etc. Erweiterungen sprechen, meinen wir damit also ab sofort immer implizit (endliche) Galoiserweiterungen, da solche Begriffe sonst keinen Sinn ergeben. Die Kummertheorie beschäftigt sich mit abelschen Erweiterungen vom Exponenten n (für festes $n \in \mathbb{Z}^{>0}$), den sogenannten *Kummererweiterungen*.

Voraussetzungen und Notation 1.23. *Wir geben uns also eine natürliche Zahl n und einen Grundkörper F vor. Dabei setzen wir $\mathrm{char}(F) \nmid n$ und $\mu_n \subseteq F$ voraus.*

Die letzte Forderung ist äquivalent dazu, dass F eine primitive n-te Einheitswurzel enthält. Für ein Element $f \in F$ definieren wir $F(\sqrt[n]{f})$ als Zerfällungskörper des Polynoms $t^n - f \in F[t]$, mit $\sqrt[n]{f}$ bezeichnen wir also eine beliebige aber fest gewählte Nullstelle des Polynoms. Wegen der Forderung $\mu_n \subseteq F$ sind mit einer Wurzel dann schon alle in der Erweiterung enthalten, $F(\sqrt[n]{f})$

ist durch Adjunktion einer einzigen Wurzel an F wohldefiniert und $F(\sqrt[n]{f})|F$ ist normal. Für solche Erweiterungen gilt der folgende bekannte Satz aus der Kummertheorie.

Satz 1.24. *Sei $n \in \mathbb{Z}^{>0}$ und F ein Körper mit $\mathrm{char}(F) \nmid n$ und $\mu_n \subseteq F$. Dann gilt:*

(*i*) *Die Erweiterung $F(\sqrt[n]{f})|F$ ist galoissch, zyklisch und hat den Exponenten n. Gilt weiter $f \neq g^d$ für alle $g \in F$ und alle $d \mid n$ mit $d > 1$, so hat die Erweiterung den Grad n.*

(*ii*) *Ist umgekehrt $E|F$ eine zyklische Galoiserweiterung vom Grad n, so ist $E = F(\sqrt[n]{f})$ für ein $f \in F$ mit $f \neq g^d$ für alle $g \in F$ und alle $d \mid n$ mit $d > 1$.*

(*iii*) *Ist $[F(\sqrt[n]{f}) : F] = n$, so gilt $\mathrm{Gal}(F(\sqrt[n]{f})|F) = \{\sigma : \sqrt[n]{f} \mapsto \zeta^i \cdot \sqrt[n]{f} \mid 0 \leq i \leq n-1\} \cong \mu_n \cong \mathbb{Z}/n\mathbb{Z}$ für eine primitive n-te Einheitswurzel ζ.*

(*iv*) *Ist F ein globaler Funktionenkörper, so ist $F(\sqrt[n]{f})|F$ genau in den Stellen $\mathfrak{p}$ unverzweigt, für die $n \mid v_\mathfrak{p}(f)$ gilt.*

Beweis. [Bos06, Kap. 4.8 Satz 3, S. 201] und [Sti93, Prop. III.7.3, S. 111], wobei man sich leicht überlegen kann, dass (iv) auch für $[F(\sqrt[n]{f}) : F] < n$ gilt. □

Nun verallgemeinern wir die obige Situation, indem wir nicht eine einzelne Wurzel, sondern eine ganze Menge von Wurzeln an den Grundkörper F adjungieren. Für eine Teilmenge Δ von F bezeichnen wir mit $F(\sqrt[n]{\Delta})$ den Körper, der durch Adjunktion aller n-ten Wurzeln $\sqrt[n]{f}$ von Elementen f aus Δ entsteht. Alternativ kann man $F(\sqrt[n]{\Delta})$ auch als Kompositum $\coprod_{f\in\Delta} F(\sqrt[n]{f})$ auffassen. Im Folgenden betrachten wir Erweiterungen $F(\sqrt[n]{\Delta})|F$, die aus Untergruppen Δ von $F^\times$ entstehen. Weiter nehmen wir immer an, dass $(F^\times)^n = \{f^n \mid f \in F^\times\} \subseteq \Delta$. Dies ist keine Einschränkung, da

$$F(\sqrt[n]{\Delta}) = F(\sqrt[n]{\Delta \cdot (F^\times)^n}).$$

Außerdem beachte man, dass

$$\begin{aligned} F(\sqrt[n]{f}) &= F(\sqrt[n]{\{f^i \mid 0 \leq i \leq n-1\}}) \\ &= F(\sqrt[n]{\langle f \rangle}) \\ &= F(\sqrt[n]{\langle f \rangle \cdot (F^\times)^n}). \end{aligned}$$

Die Untersuchung von Erweiterungen $F(\sqrt[n]{\Delta})|F$ schließt also den anfangs betrachteten Fall $F(\sqrt[n]{f})|F$ mit ein. Der folgende Satz gibt die Eigenschaften solcher allgemeinerer Kummererweiterungen an. Seine Aussagen sind analog zum vorherigen Satz.

Satz 1.25. *Sei $n \in \mathbb{Z}^{>0}$, F ein Körper mit $\mathrm{char}(F) \nmid n$ und $\mu_n \subseteq F$ und Δ eine Untergruppe von $F^\times$, die $(F^\times)^n$ enthält. Dann gilt:*

(i) Die Erweiterung $F(\sqrt[n]{\Delta})|F$ ist abelsch und hat den Exponenten n.

(ii) $[F(\sqrt[n]{\Delta}) : F] = (\Delta : (F^\times)^n)$ und $\Delta/(F^\times)^n$ besitzt den Exponenten n.

(iii) Ist F ein globaler Funktionenkörper, so ist $F(\sqrt[n]{\Delta})|F$ genau dann in einer Stelle $\mathfrak{p}$ unverzweigt, wenn $n \mid v_\mathfrak{p}(f)$ für alle $f \in \Delta$.

Beweis. Satz 1.24, 1.13 und [Hes08, Satz 6.40, S. 205] □

Es folgt der zentrale Satz der Kummertheorie. Er stellt eine bijektive Beziehung zwischen den Gruppen Δ mit $(F^\times)^n \subseteq \Delta \subseteq F^\times$ und den abelschen Erweiterungen von F vom Exponenten n her. Dabei ist Δ der Erweiterung $F(\sqrt[n]{\Delta})|F$ zugeordnet. Eine ähnliche Situation hat man in der Klassenkörpertheorie, wo man Untergruppen einer Strahlklassengruppe eines Körpers zu abelschen Erweiterungen desselben Körpers in Beziehung setzt. Und tatsächlich ist der hier angegebene Satz aus der Kummertheorie für uns ein wichtiges Hilfsmittel beim Beweis des Existenzsatzes.

Bemerkung 1.26. Um von der *Menge* aller Erweiterungen von F sprechen zu können, wählen wir einen festen algebraischen Abschluss von F und fassen alle Erweiterungen als Teilkörper hiervon auf.

Satz 1.27. *Sei $n \in \mathbb{Z}^{>0}$ und F ein Körper mit $\mathrm{char}(F) \nmid n$ und $\mu_n \subseteq F$. Dann sind die Abbildungen*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Untergruppen } \Delta \subseteq F^\times \\ \text{mit } (F^\times)^n \subseteq \Delta \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{abelsche Erweiterungen} \\ E|F \text{ vom Exponenten } n \end{array} \right\} \\ \Delta & \longmapsto & F(\sqrt[n]{\Delta}) \\ E^n \cap F^\times & \longmapsto & E \end{array}$$

zueinander inverse inklusionserhaltende Bijektionen.

Beweis. [Bos06, Kap. 4.9 Thm. 3, S. 209]; zentraler Bestandteil dieses Beweises ist der Satz Hilbert 90 (siehe [Bos06, Kap. 4.8 Thm. 1, S. 200]). □

Es seien Δ und F_Δ unter der obigen Bijektion einander zugeordnet, und G_Δ bezeichne die Galoisgruppe der Erweiterung $F_\Delta|F$. Für $\sigma \in G_\Delta$ und $f \in F$ ist

$$\sigma(\sqrt[n]{f}) = \zeta^i \cdot \sqrt[n]{f}$$

für ein $i \in \{0, \ldots, n-1\}$. Da i unabhängig von der speziellen Wahl der n-ten Wurzel von f ist und der Galoisautomorphismus σ alle Elemente aus F fix lässt, ist die folgende Abbildung wohldefiniert.

Definition 1.28. Die Abbildung

$$\begin{aligned} \kappa_n : \Delta/(F^\times)^n \times G_\Delta &\to \mu_n \\ (\bar{f}, \sigma) &\mapsto \frac{\sigma(\sqrt[n]{f})}{\sqrt[n]{f}} \end{aligned}$$

heißt *Kummerpaarung.*

Satz 1.29. *Die Kummerpaarung ist bilinear und nicht ausgeartet.*

Beweis. [Bos06, Kap. 4.9 Satz 1, S. 206] □

Falls $(\Delta : (F^\times)^n) < \infty$, so liefert die Kummerpaarung nach Lemma 1.20 die Isomorphien $\Delta/(F^\times)^n \cong \mathrm{Hom}(G_\Delta, \mu_n)$ und $G_\Delta \cong \mathrm{Hom}(\Delta/(F^\times)^n, \mu_n)$, und mit Lemma 1.19 auch $G_\Delta \cong \Delta/(F^\times)^n$.

1.4 Die Tatepaarung

Die Tatepaarung ist unter anderem aus der Kryptographie mit elliptischen Kurven bekannt. Ihre erste Anwendung dort war destruktiver Art, sie ermöglicht nämlich einen Angriff auf das diskrete Logarithmus Problem in elliptischen Kurven (siehe [FR94]). Seit ca. zehn Jahren wird die Tatepaarung jedoch hauptsächlich auf konstruktive Weise in einer als „paarungsbasierte Kryptographie“ bekannt gewordenen Disziplin (siehe [BSS05, Part 4]) eingesetzt, die vielfältige Anwendungen (beispielsweise die identitätsbasierten Kryptosysteme) erlaubt. Dies ist möglich, da Millers Algorithmus eine effiziente Berechnung von Paarungswerten bietet. Wir geben hier eine von elliptischen Kurven unabhängige Definition für allgemeine globale Funktionenkörper nach [Hes04].

Ein Teil der Relevanz dieser Arbeit besteht sicherlich darin, diese eher aus der Anwendung bekannte Paarung auch im Rahmen der algebraischen Zahlentheorie, insbesondere der Klassenkörpertheorie, besser zu verstehen.

Voraussetzungen und Notation 1.30. *Sei F ein globaler Funktionenkörper mit exaktem Konstantenkörper $\mathbb{F}_q$. Sei $n \in \mathbb{Z}^{>0}$ so, dass*

- $\mathrm{char}(F) \nmid n$ *und*
- $\mu_n \subseteq \mathbb{F}_q$.

Es bezeichne $\mathrm{N}_{F_\mathfrak{p}|\mathbb{F}_q}$ die Körpernorm der Erweiterung $F_\mathfrak{p}|\mathbb{F}_q$. Für ein $f \in F$ und einen Divisor $\mathfrak{D} \in \mathcal{D}_F$ definieren wir

$$f(\mathfrak{D}) := \prod_{\mathfrak{p} \in \mathcal{S}_F} \mathrm{N}_{F_\mathfrak{p}|\mathbb{F}_q}(f(\mathfrak{p}))^{v_\mathfrak{p}(\mathfrak{D})} \in \mathbb{F}_q.$$

Dabei darf f für $v_{\mathfrak{p}}(\mathfrak{D}) > 0$ keinen Pol und für $v_{\mathfrak{p}}(\mathfrak{D}) < 0$ keine Nullstelle in $\mathfrak{p}$ haben. Offensichtlich erfüllt diese Abbildung die Homomorphieeigenschaft in f und $\mathfrak{D}$. Zur Notation sei bemerkt, dass der Wert von $f(\mathfrak{p})$ davon abhängt, ob wir $\mathfrak{p}$ als Stelle oder als Divisor betrachten. Wir werden in kritischen Situationen darauf hinweisen.

Es bezeichne $\mathcal{C}\ell_F^0[n] := \{[\mathfrak{D}] \in \mathcal{C}\ell_F^0 \mid n[\mathfrak{D}] = [0]\}$ die n-Torsion. Für $[\mathfrak{D}] \in \mathcal{C}\ell_F^0[n]$ gilt also stets $[n\mathfrak{D}] = n[\mathfrak{D}] = [0] = 0 + \mathcal{P}_F$, deshalb gibt es ein $f \in F^\times$ mit $n\mathfrak{D} = (f)$. Schließlich kann man für ein gegebenes Paar $([\mathfrak{C}], [\mathfrak{D}]) \in \mathcal{C}\ell_F^0[n] \times \mathcal{C}\ell_F^0$ wegen des Approximationssatzes 1.8 stets Repräsentanten $\mathfrak{C}$ und $\mathfrak{D}$ mit disjunktem Träger wählen.

Definition 1.31. Die Abbildung

$$\begin{aligned} \tau_n : \mathcal{C}\ell_F^0[n] \times \mathcal{C}\ell_F^0/n\mathcal{C}\ell_F^0 &\to \mathbb{F}_q{}^\times/(\mathbb{F}_q{}^\times)^n \\ ([\mathfrak{C}], \overline{[\mathfrak{D}]}) &\mapsto f(\mathfrak{D}) \end{aligned}$$

heißt *Tatepaarung*. Dabei seien ohne Beschränkung der Allgemeinheit $\mathfrak{C}$ und $\mathfrak{D}$ teilerfremd, und f sei so gewählt, dass $n\mathfrak{C} = (f)$.

Wegen der Teilerfremdheit von $\mathfrak{C}$ und $\mathfrak{D}$ ist $f(\mathfrak{D})$ wohldefiniert (Pole bzw. Nullstellen von f machen keine Probleme), und aus der Bilinearität von $(f, \mathfrak{D}) \mapsto f(\mathfrak{D})$ folgt die Bilinearität der Paarung.

Um die Wohldefiniertheit der Paarung im rechten Argument (insbesondere die Trivialität auf Hauptdivisoren) zu überprüfen, benötigt man ein wichtiges Resultat über Funktionenkörper, die Weil-Reziprozität. Sie wird auch später in dieser Arbeit noch nützlich sein.

Satz 1.32 (Weil-Reziprozität)**.** *Es seien f und g aus $F^\times$ so gewählt, dass die Hauptdivisoren (f) und (g) disjunkte Träger haben. Dann gilt*

$$f((g)) = g((f)).$$

Beweis. [BSS05, Thm. IX.3, S. 185] □

Mit Hilfe der Weil-Reziprozität gilt nun $f((g)) = g((f)) = g(n\mathfrak{C}) = g(\mathfrak{C})^n \in (\mathbb{F}_q{}^\times)^n$ für $g \in F^\times$ (wobei wieder ohne Einschränkung der Repräsentant $\mathfrak{C}$ so gewählt sei, dass (f) und (g) teilerfremd sind). Also ist $f(\mathfrak{D}) = \bar{1} \in \mathbb{F}_q{}^\times/(\mathbb{F}_q{}^\times)^n$ für alle $\mathfrak{D} \in \mathcal{P}_F$. Für $[\mathfrak{D}] \in n\mathcal{C}\ell_F^0$ gibt es ein $[\mathfrak{B}] \in \mathcal{C}\ell_F^0$ mit $[\mathfrak{D}] = n[\mathfrak{B}]$ und folglich $f(\mathfrak{D}) = f(n\mathfrak{B}) = f(\mathfrak{B})^n = \bar{1} \in \mathbb{F}_q{}^\times/(\mathbb{F}_q{}^\times)^n$. Dies liefert die Wohldefiniertheit im rechten Argument.

Zuletzt überprüfen wir noch die Wohldefiniertheit im linken Argument. Durch $\mathfrak{C}$ ist f nur bis auf eine Konstante bestimmt, da $(f) = (cf)$ für $c \in \mathbb{F}_q{}^\times$.

Allerdings gilt hierfür

$$\begin{aligned} c(\mathfrak{D}) &= \prod_{\mathfrak{p}\in\mathcal{S}_F} \mathrm{N}_{F_\mathfrak{p}|\mathbb{F}_q}(c(\mathfrak{p}))^{v_\mathfrak{p}(\mathfrak{D})} = \prod_{\mathfrak{p}\in\mathcal{S}_F} \left(c^{[F_\mathfrak{p}:\mathbb{F}_q]}\right)^{v_\mathfrak{p}(\mathfrak{D})} \\ &= \prod_{\mathfrak{p}\in\mathcal{S}_F} c^{v_\mathfrak{p}(\mathfrak{D})\cdot\deg\mathfrak{p}} = c^{\deg(\mathfrak{D})} = 1, \end{aligned}$$

da $\mathfrak{D}$ den Grad 0 hat. Also ist die Tatepaarung insgesamt wohldefiniert.

Satz 1.33. *Unter den in diesem Abschnitt angenommenen Voraussetzungen (insbesondere $q \equiv 1 \bmod n$) ist die Tatepaarung nicht ausgeartet.*

Beweis. [Hes04, Thm. 4] □

Bemerkung 1.34. Falls n die Ordnung der Gruppe $\mathcal{C}\ell_F^0$ nicht teilt, sind die beiden Gruppen $\mathcal{C}\ell_F^0[n]$ und $\mathcal{C}\ell_F^0/n\mathcal{C}\ell_F^0$ trivial. In diesem Fall ist auch die Paarung trivial und die Nichtausartung folgt sofort.

Unter der Abbildung $\bar{x} \mapsto x^{\frac{q-1}{n}}$ ist ${\mathbb{F}_q}^\times/({\mathbb{F}_q}^\times)^n \cong \mu_n$. Hiermit wird eine leichte Modifikation der Tatepaarung definiert.

Definition 1.35. Die Abbildung

$$\begin{aligned} \tau_n^{\mathrm{red}} : \mathcal{C}\ell_F^0[n] \times \mathcal{C}\ell_F^0/n\mathcal{C}\ell_F^0 &\to \mu_n \\ ([\mathfrak{C}], \overline{[\mathfrak{D}]}) &\mapsto \left(\tau_n([\mathfrak{C}], \overline{[\mathfrak{D}]})\right)^{\frac{q-1}{n}} \end{aligned}$$

heißt *reduzierte Tatepaarung.*

Offensichtlich ist die reduzierte Tatepaarung wieder bilinear und nicht ausgeartet.

1.5 Strahlklassengruppen

Bei der Behandlung verzweigter Erweiterungen sind die Strahlklassengruppen als Verallgemeinerungen der Klassengruppe von Interesse. Die hier gegebenen Definitionen sind entnommen aus [HPP03] und [Ros02], für Zahlkörper sind sie in der Standardliteratur wie [Jan73] und [Nar90] zu finden. Funktionenkörper sind jedoch etwas einfacher zu handhaben, da es hier keine archimedischen Bewertungen gibt und die unendlichen Stellen bei Zahlkörpern oft eine gesonderte Behandlung erfordern. Andererseits gibt es im Funktionenkörper keine kanonische Maximalordnung, weshalb es praktisch ist, mit Divisoren anstatt Idealen zu arbeiten.

Voraussetzungen und Notation 1.36. *Wie immer sei F ein globaler Funktionenkörper über dem exakten Konstantenkörper $\mathbb{F}_q$. Weiter sei $\mathcal{M}$ eine endliche Menge von Stellen in F. Betrachtet man eine Körpererweiterung $E|F$, so wird $\mathcal{M}$ oft als die Menge aller verzweigten Stellen von F in E definiert. Es sei*

$$\mathfrak{m} = \sum_{\mathfrak{p}\in\mathcal{M}} m_{\mathfrak{p}} \cdot \mathfrak{p}$$

ein effektiver Divisor mit Träger $\mathcal{M}$, d.h. alle $m_{\mathfrak{p}}$ seien echt positiv.

Ein solches $\mathfrak{m}$ wird in diesem Zusammenhang üblicherweise *Erklärungsmodul* oder auch nur *Modul* genannt.

Für $f \in F$ schreibt man

$$f \equiv 1 \bmod^* \mathfrak{m},$$

falls $f \equiv 1 \bmod \mathfrak{p}^{m_{\mathfrak{p}}}$, d.h. also $v_{\mathfrak{p}}(f-1) \geq m_{\mathfrak{p}}$, für alle $\mathfrak{p} \in \mathcal{M}$. Wir bemerken, dass aus $v_{\mathfrak{p}}(f-1) \geq m_{\mathfrak{p}} > 0$ schon $v_{\mathfrak{p}}(f) = 0$ folgt.

Nun bezeichnen wir mit

$$\mathcal{D}^{\mathfrak{m}} := \{\mathfrak{D} \in \mathcal{D}_F \mid \operatorname{supp}\mathfrak{D} \cap \operatorname{supp}\mathfrak{m} = \emptyset\}$$

alle Divisoren von F, deren Träger außerhalb von $\mathcal{M}$ liegt und entsprechend mit

$$\mathcal{P}^{\mathfrak{m}} := \mathcal{D}^{\mathfrak{m}} \cap \mathcal{P}_F$$

die Gruppe aller solcher Hauptdivisoren. Für $(f) \in \mathcal{P}^{\mathfrak{m}}$ gilt also $v_{\mathfrak{p}}(f) = 0$ für alle $\mathfrak{p} \in \mathcal{M}$. Da diese Definitionen nur vom Träger von $\mathfrak{m}$ abhängen, schreiben wir auch manchmal $\mathcal{D}^{\mathcal{M}}$ bzw. $\mathcal{P}^{\mathcal{M}}$. Die Erzeuger solcher Hauptdivisoren bezeichnen wir mit

$$F^{\mathfrak{m}} := \{f \in F^{\times} \mid (f) \in \mathcal{P}^{\mathfrak{m}}\}.$$

Die Untergruppe

$$F_{\mathfrak{m}} := \{f \in F^{\mathfrak{m}} \mid f \equiv 1 \bmod^* \mathfrak{m}\}$$

erzeugt die Gruppe

$$\mathcal{P}_{\mathfrak{m}} := \{(f) \in \mathcal{P}^{\mathfrak{m}} \mid f \in F_{\mathfrak{m}}\},$$

den sogenannten *Strahl modulo* $\mathfrak{m}$. Die *Strahlklassengruppe modulo* $\mathfrak{m}$ ist nun definiert als

$$\mathcal{C}\ell_{\mathfrak{m}} := \mathcal{D}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}}.$$

Für $\mathcal{M} = \emptyset$ ist $\mathfrak{m}$ trivial und man erhält $\mathcal{D}^{\mathfrak{m}} = \mathcal{D}_F$ und $\mathcal{P}^{\mathfrak{m}} = \mathcal{P}_{\mathfrak{m}} = \mathcal{P}_F$. Dann ist $\mathcal{C}\ell_{\mathfrak{m}} = \mathcal{C}\ell_F$ die bekannte Divisorenklassengruppe. Ist $\mathfrak{m}' \leq \mathfrak{m}$, so gibt es einen kanonischen Epimorphismus

$$\Psi_{\mathfrak{m}'} : \mathcal{C}\ell_{\mathfrak{m}} \to \mathcal{C}\ell_{\mathfrak{m}'},$$

insbesondere ist also $\mathcal{C}\ell_F$ das epimorphe Bild jeder Strahlklassengruppe. Die Surjektivität folgt aus dem Approximationssatz 1.8, nach dem man den Repräsentanten einer Strahlklasse aus $\mathcal{C}\ell_{\mathfrak{m}'}$ so abändern kann, dass er schon in $\mathcal{D}^{\mathfrak{m}}$ liegt. Mehr über die Beziehungen zwischen Strahlklassengruppen (und den beteiligten Gruppen) zu verschiedenen Moduln findet sich in [Jan73, Kap. V.6].

Für eine gegebene Untergruppe H von $\mathcal{C}\ell_{\mathfrak{m}}$ heißt das eindeutig bestimmte kleinste Modul $\mathfrak{f}$ mit

$$\mathcal{C}\ell_{\mathfrak{f}}/\Psi_{\mathfrak{f}}(H) \cong \mathcal{C}\ell_{\mathfrak{m}}/H$$

der *Führer* von H. Der Führer von $\mathcal{C}\ell_{\mathfrak{m}}$ wird definiert als der Führer der Untergruppe $H = \{0\}$.

Man erhält die exakten Sequenzen

$$1 \to K^{\times} \to F^{\mathfrak{m}}/F_{\mathfrak{m}} \to \mathcal{C}\ell_{\mathfrak{m}} \to \mathcal{D}^{\mathfrak{m}}/\mathcal{P}^{\mathfrak{m}} \to 0$$

und

$$0 \to \mathcal{P}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}} \to \mathcal{C}\ell^0_{\mathfrak{m}} \to \mathcal{C}\ell^0_F \to 0,$$

wobei $\mathcal{C}\ell^0_{\mathfrak{m}}$ wie üblich alle Klassen vom Grad 0 bezeichnet. Wie auch die Klassengruppe ist $\mathcal{C}\ell_{\mathfrak{m}}$ im Allgemeinen unendlich, aber $\mathcal{C}\ell^0_{\mathfrak{m}}$ für globale Funktionenkörper immer endlich. Wichtig ist auch noch die Isomorphie

$$F^{\mathfrak{m}}/F_{\mathfrak{m}} \cong \prod_{\mathfrak{p}\in\mathcal{M}} (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{m_{\mathfrak{p}}})^{\times}.$$

1.6 Frobeniusautomorphismen und die Artinabbildung

Der Frobeniusautomorphismus ist ein wichtiger Begriff in der Zahlentheorie lokaler und globaler Körper, und die daraus entstehende Artinabbildung spielt eine zentrale Rolle in der Klassenkörpertheorie. Durch sie ist der charakteristische Isomorphismus $\mathcal{C}\ell_{\mathfrak{m}}/H \cong \mathrm{Gal}(F_H|F)$ für den Klassenkörper F_H zu $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ gegeben. In dieser Arbeit liefert die Artinabbildung die entscheidende Verbindung zwischen Kummer- und Tatepaarung, worauf unser Beweis des Existenzsatzes beruht. Alle Beweise der in diesem Abschnitt erwähnten Aussagen sind nachzulesen in [Ros02, Kap. 9].

Voraussetzungen und Notation 1.37. *In diesem Abschnitt sei $E|F$ eine endliche abelsche Galoiserweiterung globaler Funktionenkörper. (Die ersten Aussagen dieses Abschnittes gelten auch ohne die Voraussetzungen „abelsch“ und „global“ (siehe hierzu [Ros02, Kap. 9]), aber uns interessiert nur der*

betrachtete Spezialfall.) Es bezeichne $G := \mathrm{Gal}(E|F)$ *die Galoisgruppe,* $\mathfrak{P}$ *eine Stelle von* E*,* $\mathfrak{p}$ *die darunter liegende Stelle von* F *und* $\mathcal{M}$ *die Menge der in* E *verzweigten Stellen von* F*.*

Für $\sigma \in G$ ist offensichtlich auch $\sigma\mathfrak{P}$ eine Stelle von E über $\mathfrak{p}$, mehr noch, G operiert sogar transitiv auf der Menge der Stellen von E über $\mathfrak{p}$. In diesem Setting gilt weiter, dass $e(\mathfrak{P}_1|\mathfrak{p}) = e(\mathfrak{P}_2|\mathfrak{p})$ und $f(\mathfrak{P}_1|\mathfrak{p}) = f(\mathfrak{P}_2|\mathfrak{p})$ für zwei Stellen $\mathfrak{P}_1$ und $\mathfrak{P}_2$ über $\mathfrak{p}$. Bezeichnet $e(\mathfrak{p})$ bzw. $f(\mathfrak{p})$ den gemeinsamen Verzweigungsindex bzw. Trägheitsgrad der Stellen über $\mathfrak{p}$ und $g(\mathfrak{p})$ die Anzahl der Stellen von E über $\mathfrak{p}$ (sie ist endlich nach [Sti93, Prop. III.1.7, S. 62]), so gilt nach Satz 1.12: $[E : F] = e(\mathfrak{p})f(\mathfrak{p})g(\mathfrak{p})$.

Definition 1.38. $Z(\mathfrak{P}|\mathfrak{p}) := \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}$ heißt *Zerlegungsgruppe* von $\mathfrak{P}$ über $\mathfrak{p}$.

$Z(\mathfrak{P}|\mathfrak{p})$ hat die Ordnung $e(\mathfrak{P}|\mathfrak{p})f(\mathfrak{P}|\mathfrak{p})$. Für ein $\sigma \in G$ ist $Z(\sigma\mathfrak{P}|\mathfrak{p}) = \sigma Z(\mathfrak{P}|\mathfrak{p})\sigma^{-1}$, insbesondere sind die Zerlegungsgruppen der Stellen von E über $\mathfrak{p}$ also alle Konjugierte. Die Erweiterung $E_{\mathfrak{P}}|F_{\mathfrak{p}}$ der Restklassenkörper ist galoissch und für unverzweigtes $\mathfrak{P}|\mathfrak{p}$ ist $Z(\mathfrak{P}|\mathfrak{p}) \cong \mathrm{Gal}(E_{\mathfrak{P}}|F_{\mathfrak{p}})$. Da $E_{\mathfrak{P}}$ und $F_{\mathfrak{p}}$ endlich sind wird die Galoisgruppe $\mathrm{Gal}(E_{\mathfrak{P}}|F_{\mathfrak{p}})$ vom Frobeniusautomorphismus $\varphi_{\mathfrak{p}} : x \mapsto x^{\mathfrak{N}(\mathfrak{p})}$ für alle $x \in E_{\mathfrak{P}}$ erzeugt. Dabei bezeichnet $\mathfrak{N}$ die Idealnorm, d.h. es gilt

$$\mathfrak{N}(\mathfrak{p}) = (\mathcal{O}_{\mathfrak{p}} : \mathfrak{p}) = \#F_{\mathfrak{p}} = q^{\deg(\mathfrak{p})}.$$

Wenn $\mathfrak{P}|\mathfrak{p}$ unverzweigt ist, haben wir $\langle\varphi_{\mathfrak{p}}\rangle = \mathrm{Gal}(E_{\mathfrak{P}}|F_{\mathfrak{p}}) \cong Z(\mathfrak{P}|\mathfrak{p})$ und deshalb gibt es ein eindeutiges Element aus $Z(\mathfrak{P}|\mathfrak{p})$, das unter dieser Isomorphie zum Frobeniusautomorphismus $\varphi_{\mathfrak{p}}$ korrespondiert.

Definition 1.39. Für unverzweigtes $\mathfrak{P}|\mathfrak{p}$ heißt das Element aus $Z(\mathfrak{P}|\mathfrak{p})$, das unter der Isomorphie $\mathrm{Gal}(E_{\mathfrak{P}}|F_{\mathfrak{p}}) \cong Z(\mathfrak{P}|\mathfrak{p})$ zum Frobeniusautomorphismus $\varphi_{\mathfrak{p}}$ korrespondiert, der *Frobeniusautomorphismus von* $\mathfrak{P}$ *für die Erweiterung* $E|F$ und wird mit $(\mathfrak{P}, E|F)$ bezeichnet.

Durch Inspektion der Isomorphie $\mathrm{Gal}(E_{\mathfrak{P}}|F_{\mathfrak{p}}) \cong Z(\mathfrak{P}|\mathfrak{p})$ sieht man leicht, dass der Frobeniusautomorphismus von $\mathfrak{P}$ auch durch die Bedingung

$$(\mathfrak{P}, E|F)z \equiv z^{\mathfrak{N}(\mathfrak{p})} \bmod \mathfrak{P} \quad \forall\, z \in \mathcal{O}_{\mathfrak{P}}$$

beschrieben werden kann. Da $(\mathfrak{P}, E|F)$ die Zerlegungsgruppe erzeugt, hat $(\mathfrak{P}, E|F)$ die Ordnung $f(\mathfrak{P}|\mathfrak{p})$ (wegen $\mathfrak{P}|\mathfrak{p}$ unverzweigt war ja $e(\mathfrak{P}|\mathfrak{p}) = 1$). Für $\sigma \in G$ gilt $(\sigma\mathfrak{P}, E|F) = \sigma(\mathfrak{P}, E|F)\sigma^{-1}$, also füllt $(\mathfrak{P}, E|F)$ eine Konjugationsklasse in G aus, wenn $\mathfrak{P}$ die Stellen von E über $\mathfrak{p}$ durchläuft.

Definition 1.40. Für eine in E unverzweigte Stelle $\mathfrak{p}$ von F setzen wir

$$(\mathfrak{p}, E|F) := \{(\mathfrak{P}, E|F) \mid \mathfrak{P}|\mathfrak{p}\}.$$

Dadurch wird die *Artinabbildung*

$$\begin{aligned} \mathcal{S}_F \setminus \mathcal{M} &\to \text{Konjugationsklassen von } G \\ \mathfrak{p} &\mapsto (\mathfrak{p}, E|F) \end{aligned}$$

definiert, wobei $\mathcal{S}_F \setminus \mathcal{M}$ die Menge der unverzweigten Stellen von F ist.

Lemma 1.41. *Sei $E|F$ eine abelsche Erweiterung globaler Funktionenkörper und L ein Zwischenkörper. Sei $\mathfrak{P}$ eine Stelle von E und $\mathfrak{q}$ bzw. $\mathfrak{p}$ die Stellen, die in L bzw. F darunter liegen. Wenn $\mathfrak{P}|\mathfrak{p}$ unverzweigt ist, dann gilt*

$$(\mathfrak{P}, E|F)|_L = (\mathfrak{q}, L|F) \quad \textit{und} \quad (\mathfrak{P}, E|F)^{f(\mathfrak{q}|\mathfrak{p})} = (\mathfrak{P}, E|L).$$

Beweis. [Ros02, Prop. 9.11, S. 122] □

Für zwei Stellen $\mathfrak{P}_1$ und $\mathfrak{P}_2$ über $\mathfrak{p}$ sind $(\mathfrak{P}_1, E|F)$ und $(\mathfrak{P}_2, E|F)$ konjugiert in G, d.h. es gibt ein $\sigma \in G$ mit $(\mathfrak{P}_1, E|F) = \sigma(\mathfrak{P}_2, E|F)\sigma^{-1}$. Unter der Annahme, dass G abelsch ist, gilt also $(\mathfrak{P}_1, E|F) = (\mathfrak{P}_2, E|F)$. Folglich besteht die Konjugationsklasse $(\mathfrak{p}, E|F)$ im abelschen Fall nur aus einem einzigen Element, das wir wieder mit $(\mathfrak{p}, E|F)$ bezeichnen und *Artinautomorphismus von* $\mathfrak{p}$ nennen.

Definition 1.42. Bezeichnet $\mathcal{D}^{\mathcal{M}} \subseteq \mathcal{D}_F$ die Menge der Divisoren $\mathfrak{D}$ von F mit Träger außerhalb von $\mathcal{M}$, so lässt sich die Artinabbildung auf $\mathcal{D}^{\mathcal{M}}$ linear fortsetzen zu

$$\begin{aligned} \mathcal{D}^{\mathcal{M}} &\to G \\ \mathfrak{D} &\mapsto (\mathfrak{D}, E|F) := \prod_{\mathfrak{p} \in \mathcal{S}_F} (\mathfrak{p}, E|F)^{v_{\mathfrak{p}}(\mathfrak{D})}. \end{aligned}$$

Diese Abbildung wird auch *Artinsymbol* genannt und ist ein Gruppenhomomorphismus. Wenn klar ist in welcher Körpererweiterung wir arbeiten bezeichnen wir $(\mathfrak{D}, E|F)$ auch mit $\sigma_{\mathfrak{D}}$.

Es sei $\hat{\mathcal{M}}$ die Menge der Stellen von E, die über F unverzweigt sind. Dann ist $\mathcal{D}^{\hat{\mathcal{M}}}$ die von den Stellen in $\hat{\mathcal{M}}$ erzeugte Untergruppe von $\mathcal{D}_E$. Außerdem benötigen wir an dieser Stelle die Divisornorm $\mathcal{N}_{E|F} : \mathcal{D}_E \to \mathcal{D}_F$, die für eine Stelle $\mathfrak{P}|\mathfrak{p}$ durch $\mathcal{N}_{E|F}(\mathfrak{P}) = f(\mathfrak{P}|\mathfrak{p}) \cdot \mathfrak{p}$ definiert ist und auf $\mathcal{D}_E$ linear fortgesetzt wird.

Satz 1.43. *Die Artinabbildung $(\cdot, E|F) : \mathcal{D}^{\mathcal{M}} \to G$ ist surjektiv und ihr Kern enthält die Gruppe $\mathcal{N}_{E|F}(\mathcal{D}^{\hat{\mathcal{M}}})$.*

Beweis. [Ros02, Prop. 9.18, S. 136], beim Beweis der Surjektivität geht entscheidend der Tschebotarevsche Dichtigkeitssatz ein, den wir im folgenden Abschnitt 1.7 behandeln. □

Die genaue Bestimmung des Kerns der Artinabbildung ist eine zentrale Frage der Klassenkörpertheorie, das Ergebnis führt zum Reziprozitätsgesetz. Wir behandeln dieses Problem in Kapitel 2.

1.7 Der Dichtigkeitssatz von Tschebotarev

Wir behalten die Notation und Voraussetzungen 1.37 des vorherigen Abschnitts bei. Eine wichtige Frage in der Zahlentheorie lautet, welche Stellen $\mathfrak{p}$ von F durch die Artinabbildung $\mathfrak{p} \mapsto (\mathfrak{p}, E|F)$ auf eine gegebene Konjugiertenklasse $\mathfrak{K}$ von G abgebildet werden. Insbesondere liefert die Antwort darauf auch eine Aussage über die Surjektivität der Artinabbildung. Das zentrale Resultat hierzu ist der Tschebotarevsche Dichtigkeitssatz. Er gilt sowohl für Zahlkörper als auch für Funktionenkörper und ist von entscheidender Bedeutung in der Klassenkörpertheorie.

Bei dem berühmten Satz handelt es sich um eine weitreichende Verallgemeinerung des bekannten Dirichletschen Primzahlsatzes. Er sagt aus, dass für gegebene teilerfremde natürliche Zahlen a und m in jeder arithmetischen Progression $a, a \pm m, a \pm 2m, \ldots$ unendlich viele Primzahlen vorkommen. Eine quantitative Version besagt, dass sich die Primzahlen gleichverteilt auf diese verteilen, d.h. dass die Menge der Primzahlen in jeder solchen Folge die Dichtigkeit $\frac{1}{\phi(m)}$ in der Menge aller Primzahlen hat.

Der Satz von Tschebotarev verallgemeinert diese Aussage auf die Menge der Primideale in Zahlkörpern. Hierbei handelt es sich um eine Vermutung von Frobenius, der jedoch nur ein schwächeres Resultat zeigen konnte. Der vollständige Beweis wurde von Tschebotarev 1923 zunächst auf russisch veröffentlicht, 1926 dann auf deutsch (siehe [Tsc26]).

Wir formulieren hier eine Variante von Tschebotarevs Satz für globale Funktionenkörper, die wir im Laufe der Arbeit verwenden. Sie ist ein zentrales Argument in unserem Beweis des Existenzsatzes der Klassenkörpertheorie. Dies entspricht der historischen Reihenfolge, denn Tschebotarevs Beweis lieferte Artin die entscheidende Idee zum Beweis seines Reziprozitätsgesetzes (siehe [SH96, S. 35]), allerdings verwenden wir eine ganz andere Methode als damals Artin. Heute wird auch manchmal umgekehrt die Klassenkörpertheorie unabhängig bewiesen und die Tschebotarevsche Dichtigkeitsaussage dann daraus gefolgert, zum Beispiel in [Lan70a] und [Neu92].

Unsere Formulierung orientiert sich an [Ros02, Thm. 9.13A, S. 125], der jedoch keinen vollständigen Beweis liefert. Ein Beweis für den Funktionenkörper-Fall, der ohne Klassenkörpertheorie auskommt, findet sich in [FJ86, Kap. 5.4]. Er beruht nur auf der Riemannschen Vermutung für algebraische Zahlkörper, wie sie zum Beispiel in [Sti93, Thm. V.2.1] elementar bewiesen wird.

Definition 1.44. Es sei $\mathcal{T} \subseteq \mathcal{S}_F$ eine beliebige Menge von Stellen von F.

$$\delta(\mathcal{T}) := \lim_{s \searrow 1} \frac{\sum_{\mathfrak{p} \in \mathcal{T}} \mathfrak{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p} \in \mathcal{S}_F} \mathfrak{N}(\mathfrak{p})^{-s}}$$

heißt *Dirichlet-Dichtigkeit von* $\mathcal{T}$. Dabei bedeutet der Ausdruck „$s \searrow 1$“, dass s sich in den reellen Zahlen von oben der 1 annähert.

Für globale Funktionenkörper existiert dieser Limes immer. Offensichtlich gilt stets $0 \leq \delta(\mathcal{T}) \leq 1$. Außerdem haben endliche Mengen die Dichtigkeit 0 und $\mathcal{S}_F$ hat die Dichtigkeit 1. Für weitere Eigenschaften siehe [Ros02, Prop. 9.12, S. 124] oder [FJ86, S. 58].

Satz 1.45 (Dichtigkeitssatz von Tschebotarev)**.** *Es sei $E|F$ eine galoissche Erweiterung globaler Funktionenkörper, $\mathfrak{K}$ eine Konjugationsklasse in $\mathrm{Gal}(E|F)$ und $\mathcal{M}$ die Menge der in E verzweigten Stellen von F. Dann gilt*

$$\delta(\{\mathfrak{p} \in \mathcal{S}_F \setminus \mathcal{M} \mid (\mathfrak{p}, E|F) = \mathfrak{K}\}) = \frac{\#\mathfrak{K}}{\#\,\mathrm{Gal}(E|F)}.$$

Auch eine noch stärkere asymptotische Formulierung des Satzes wie in [Ros02, Thm. 9.13B, S. 125] ist üblich. Für uns sind jedoch die Folgerungen aus dem Tschebotarevschen Dichtigkeitssatz wichtiger, die wir im Folgenden formulieren wollen.

Korollar 1.46. *Es sei $E|F$ eine abelsche Erweiterung von globalen Funktionenkörpern und $\mathcal{M}$ die Menge der darin verzweigten Stellen von F. Dann gibt es für jedes $\sigma \in \mathrm{Gal}(E|F)$ unendlich viele $\mathfrak{p} \in \mathcal{S}_F \setminus \mathcal{M}$ mit $(\mathfrak{p}, E|F) = \sigma$. Insbesondere ist die Artinabbildung $(\cdot, E|F) : \mathcal{D}^{\mathcal{M}} \to \mathrm{Gal}(E|F)$ surjektiv.*

Aus der asymptotischen Fassung von Tschebotarevs Satz folgt sogar, dass es für gegebenes σ und d groß genug eine Stelle $\mathfrak{p}$ vom vorgegebenen Grad d gibt mit $(\mathfrak{p}, E|F) = \sigma$. Hier ist am besten die enge Verwandtschaft zum folgenden Resultat zu erkennen. Wir nennen es den Primzahlsatz für Klassen, da seine Aussage eine offensichtliche Ähnlichkeit zum Primzahlsatz aufweist.

Satz 1.47 (Primzahlsatz für Klassen)**.** *Es sei $E|F$ eine abelsche Erweiterung globaler Funktionenkörper und $\mathfrak{m}$ ein Modul, dessen Träger alle in E verzweigten Stellen von F enthält. Dann existiert für jede Klasse $[\mathfrak{D}] \in \mathcal{C}\ell_{\mathfrak{m}}$ vom Grad d groß genug eine Stelle $\mathfrak{p} \in \mathcal{S}_F \setminus \operatorname{supp}\mathfrak{m}$ mit $[\mathfrak{p}] = [\mathfrak{D}]$.*

Setzt man die Klassenkörpertheorie voraus, so kann der Primzahlsatz leicht aus dem Satz von Tschebotarev gefolgert werden. Beweist man umgekehrt Tschebotarev und den Primzahlsatz unabhängig von der Klassenkörpertheorie, so kann man daraus die Aussagen der Klassenkörpertheorie folgern. Wir wollen letztere Strategie verfolgen und geben daher selbst in [HM10] den Beweis dieses Satzes für Funktionenkörper. Im Zahlkörperfall ist der Satz beispielsweise in [Nar90, Cor. 7, S. 358] zu finden.

Kapitel 2

Aussagen der Klassenkörpertheorie

Ziel der Klassenkörpertheorie ist die Beschreibung der endlichen abelschen Erweiterungen eines gegebenen Grundkörpers. Zum Teil erreicht das schon die Galoistheorie, indem sie jeder galoisschen (d.h. normalen und separablen) Erweiterung $E|F$ ihre Galoisgruppe $\mathrm{Gal}(E|F) = \mathrm{Aut}_F(E)$ zuordnet. Sie bildet auch die Zwischenkörper von $E|F$ bijektiv auf die Untergruppen von $\mathrm{Gal}(E|F)$ ab. Allerdings ist es mittels Galoistheorie nicht möglich, eine Erweiterung mit gegebener Galoisgruppe *und* gegebenem Grundkörper zu bestimmen (inverse Galoistheorie).

Dieses Problem kann–für abelsche Gruppen–mit Hilfe der Klassenkörpertheorie gelöst werden. Für eine vorgegebene Untergruppe H einer Strahlklassengruppe $\mathcal{C}\ell_{\mathfrak{m}}$ beweist die Klassenkörpertheorie die Existenz einer Erweiterung, deren Galoisgruppe isomorph zu $\mathcal{C}\ell_{\mathfrak{m}}/H$ ist. Dabei ist die Isomorphie durch die zugehörige Artinabbildung gegeben. Eine solche Erweiterung heißt dann *Klassenkörper* zu H. Die Klassenkörpertheorie zeigt noch mehr, es entstehen nämlich alle abelschen Erweiterungen eines gegebenen Grundkörpers als Klassenkörper zu den Untergruppen der Strahlklassengruppen. Beschränkt man sich auf die Betrachtung bestimmter Untergruppen, so kann man sogar eine Bijektion zwischen Gruppen und Erweiterungen angeben. Dies sind im Wesentlichen die Aussagen des Existenzsatzes der Klassenkörpertheorie.

Hauptgegenstand dieser Arbeit ist ein neuer Beweis dieses Existenzsatzes für den Fall, dass der Grundkörper ein globaler Funktionenkörper ist. Dabei spielt die Kummertheorie eine wichtige Rolle, die sich in ähnlicher Weise wie die Klassenkörpertheorie mit der Beschreibung abelscher Erweiterungen beschäftigt und immer gleichzeitig Erweiterungen von fest vorgegebenem Exponenten betrachtet. Die Aussagen der Klassenkörpertheorie sind jedoch weitreichender und mächtiger.

In der (multiplikativen) Kummertheorie betrachtet man abelsche Erweiterungen eines Grundkörpers F von fest gewähltem Exponenten n, der teilerfremd zur Charakteristik von F ist. Außerdem muss man voraussetzen, dass

die n-ten Einheitswurzeln μ_n in F enthalten sind. Dann existiert zu jeder vorgegebenen Untergruppe Δ von $F^\times$ mit $(F^\times)^n \subseteq \Delta$ eine Erweiterung, deren Galoisgruppe isomorph zu $\Delta/(F^\times)^n$ ist, und diese Erweiterung ist durch $F(\sqrt[n]{\Delta})$ gegeben. Umgekehrt ist jede abelsche Erweiterung vom Exponenten n von der Form $F(\sqrt[n]{\Delta})$ für ein geeignetes $\Delta \supseteq (F^\times)^n$. Hat man eine Erweiterung $E|F$, so erhält man Δ als $E^n \cap F^\times$. Erweiterungen, deren Exponent eine Potenz der Charakteristik von F ist, kann man auf ähnliche Weise behandeln, hierfür benötigt man die Artin-Schreier-Theorie und Witt-Vektoren (siehe [Bos06, Kap. 4.10]). Allerdings kann man nie *alle* abelschen Erweiterungen auf einmal betrachten, immer nur die eines gegebenen Exponenten, und für diesen Exponenten muss man die genannte Fallunterscheidung machen. Im Kummer-Fall ist auch noch die Bedingung $\mu_n \subseteq F$ eine echte Einschränkung.

Im Gegensatz dazu unterliegt die Klassenkörpertheorie keinerlei Einschränkungen, und man kann alle abelschen Erweiterungen auf einmal klassifizieren. Zum Beweis benutzen wir allerdings die Kummertheorie und machen somit die genannte Fallunterscheidung, wobei wir nur für Kummererweiterungen alle Details ausführen. Wir konstruieren für gegebenes $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ den Klassenkörper mit Hilfe der Kummertheorie (und einer neuen Paarung) und zeigen umgekehrt, wie man zu einer gegebenen abelschen Erweiterung die zugehörige Gruppe erhält. Wir verallgemeinern die Konstruktion auch auf den (in der Kummertheorie nicht behandelten) Fall $\mu_n \nsubseteq F$. So kann man analog zur Galoistheorie und zur Kummertheorie nur eben noch allgemeiner zwischen Gruppen und Erweiterungen hin- und herschalten.

Die Klassenkörpertheorie macht noch weitere Aussagen. Sie folgen alle aus dem Existenzsatz, die Hauptarbeit steckt also in seinem Beweis. Diesen treten wir erst in Kapitel 4 an und zeigen in diesem Kapitel zunächst, wie die anderen Aussagen folgen, wenn man die Existenz von Klassenkörpern annimmt. Dazu gehören funktorielle Eigenschaften der Abbildung, die eine Gruppe auf ihren Klassenkörper abbildet, alternative Beschreibungen des Klassenkörpers (da die Artin-Isomorphie manchmal doch recht umständlich ist), das Artinsche Reziprozitätsgesetz und eine Aussage über die Größe des Konstantenkörpers des Klassenkörpers (relativ zum Konstantenkörper des Grunkörpers). Sämtliche Aussagen in diesem Kapitel sind also von der Form „Angenommen der Existenzsatz gilt, dann ...“. Am Schluss des Kapitels formulieren wir als Zusammenfassung nochmals alle wichtigen Aussagen der Klassenkörpertheorie in einem Hauptsatz. Dieses Vorgehen ist sinnvoll, da wir den Existenzsatz in mehreren Schritten beweisen und die Aussagen, die daraus folgen, für die bereits behandelten Fälle gleichzeitig schon verwenden wollen.

Manche der hier allgemein bewiesenen Aussagen lassen sich auf direktere Weise einsehen, wenn man die genaue Struktur des Klassenkörpers kennt. Darauf wird an den geeigneten Stellen hingewiesen.

Die Beweise der Sätze in diesem Kapitel findet man zum großen Teil auch in

der Literatur, jedoch muss man sie sich dort zusammensuchen und sich an unterschiedliche Notation sowie Formulierungen gewöhnen. Außerdem werden dort meist nur Zahlkörper behandelt. Deshalb geben wir hier eine Zusammenfassung der wichtigsten Resultate inklusive kurzen Beweisen.

Wir legen für das vorliegende Kapitel sowie die gesamte Arbeit die folgende Notation fest.

Voraussetzungen und Notation 2.1. *Es sei F ein globaler Funktionenkörper mit dem exakten Konstanenkörper $\mathbb{F}_q$, und $\mathfrak{m}$ sei stets ein Erklärungsmodul, also ein effektiver Divisor, von F.*

2.1 Der Existenzsatz der Klassenkörpertheorie

Wir geben nun die präzise Definition eines Klassenkörpers und formulieren den Existenzsatz.

Definition 2.2. Es sei ein Modul $\mathfrak{m}$ von F und eine Untergruppe H der Strahlklassengruppe $\mathcal{C}\ell_{\mathfrak{m}}$ gegeben. Eine endliche abelsche außerhalb vom Träger von $\mathfrak{m}$ unverzweigte Erweiterung E von F heißt *Klassenkörper zu H*, falls

$$H = \ker(\cdot, E|F)$$

gilt. Dabei meinen wir mit $(\cdot, E|F)$ die von der Artinabbildung auf der Strahlklassengruppe $\mathcal{C}\ell_{\mathfrak{m}}$ induzierte Abbildung. Diese Schreibweise beinhaltet also implizit, dass diese Abbildung überhaupt wohldefiniert ist, d.h. dass $\mathcal{P}_{\mathfrak{m}}$ im Kern der Artinabbildung enthalten ist.

Da die Artinabbildung nach dem Satz von Tschebotarev surjektiv ist, folgt für Klassenkörper E zu H sofort die Isomorphie

$$\mathrm{Gal}(E|F) \cong \mathcal{C}\ell_{\mathfrak{m}}/H.$$

Genau wie die Kummertheorie und die (klassische) Galoistheorie befasst sich auch die Klassenkörpertheorie nur mit *endlichen* Erweiterungen. Deshalb können wir auch nur Untergruppen H von *endlichem* Index in $\mathcal{C}\ell_{\mathfrak{m}}$ betrachten. Hat man mit Zahlkörpern zu tun, so sind sämtliche Strahlklassengruppen endlich und Untergruppen haben automatisch endlichen Index, bei Funktionenkörpern muss man dies explizit fordern.

Bemerkung 2.3. Bezieht man die unendliche Galoistheorie mit ein, so besitzt F natürlich auch unendliche abelsche Erweiterungen (z.B. ist die maximale abelsche Erweiterung F^{ab} von F unendlich). Trotzdem begnügt man sich damit, die endlichen abelschen Erweiterungen zu betrachten. Jede unendliche Galoiserweiterung ist nämlich die Vereinigung von endlichen galoisschen

Teilerweiterungen (siehe [Bou03, S. V.56]). In damit kompatibler Weise setzt sich die Galoisgruppe einer unendlichen Erweiterung aus den Galoisgruppen der endlichen (galoisschen) Teilerweiterungen zusammen. Ist nämlich $L|F$ eine unendliche Galoiserweiterung, so ist $\mathrm{Gal}(L|K) \cong \varprojlim \mathrm{Gal}(E|F)$ (der projektive Limes, siehe [Neu92, S. 286]) und $L = \bigcup E$, wobei E alle endlichen (galoisschen) Teilerweiterungen von $L|F$ durchläuft. Salopp ausgedrückt lässt sich also jede unendliche Galoiserweiterung sowie ihre Galoisgruppe durch endliche „approximieren“, und Entsprechendes gilt für Untergruppen von $\mathcal{C}\ell_{\mathfrak{m}}$ von unendlichem Index. Alle Teilerweiterungen von abelschen Erweiterungen sowie beliebige Vereinigungen von abelschen Erweiterungen sind wieder abelsch (siehe [Bou03, S. V.77]). Damit umgeht man die Schwierigkeiten der unendlichen Galoistheorie wie die Definition einer geeigneten Topologie (Krull-Topologie) und die Behandlung proendlicher Gruppen. Siehe auch [Bos06, Kap. 4.2] und [Vil06, Bem. 11.5.7, S. 411].

Nun soll überprüft werden, dass ein Klassenkörper durch die gegebenen Eigenschaften schon eindeutig definiert ist.

Lemma 2.4. *Es seien zwei Untergruppen H_1 und H_2 von $\mathcal{C}\ell_{\mathfrak{m}}$ von endlichem Index und je ein zugehöriger Klassenkörper F_1 bzw. F_2 gegeben. Dann ist das Kompositum F_1F_2 ein Klassenkörper zu $H_1 \cap H_2$.*

Beweis. Es ist $H_1 \cap H_2 = \ker(\cdot, F_1F_2|F)$ zu zeigen. Die Inklusion „$\supseteq$“ folgt sofort aus Lemma 1.41, da für $(\mathfrak{D}, F_1F_2|F) = \mathrm{id}_{F_1F_2}$ auch $(\mathfrak{D}, F_1|F) = \mathrm{id}_{F_1}$ und $(\mathfrak{D}, F_2|F) = \mathrm{id}_{F_2}$ gilt, also $\mathfrak{D} \in H_1 \cap H_2$ ist.

Umgekehrt sei $\mathfrak{D} \in H_1 \cap H_2$, also $(\mathfrak{D}, F_1|F) = \mathrm{id}_{F_1} \in \mathrm{Gal}(F_1|F)$ und $(\mathfrak{D}, F_2|F) = \mathrm{id}_{F_2} \in \mathrm{Gal}(F_2|F)$. Dann ist auch $(\mathfrak{D}, F_1F_2|F) = \mathrm{id}_{F_1F_2} \in \mathrm{Gal}(F_1F_2|F)$, denn laut Galoistheorie (siehe [Bos06, Kap. 4.1 Satz 12, S. 145]) ist der Homomorphismus

$$\mathrm{Gal}(F_1F_2|F) \to \mathrm{Gal}(F_1|F) \times \mathrm{Gal}(F_2|F),$$

der durch Einschränkung entsteht, injektiv. □

Satz 2.5. *Existiert ein Klassenkörper zu $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$, so ist er eindeutig bestimmt.*

Beweis. Angenommen es gäbe ein $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ und zwei endliche abelsche Erweiterungen F_1 und F_2 von F so dass

$$H = \ker(\cdot, F_1|F) = \ker(\cdot, F_2|F).$$

Dann folgt mit Lemma 2.4 für das Kompositum von F_1 und F_2

$$H = H \cap H = \ker(\cdot, F_1F_2|F),$$

also

$$\mathrm{Gal}(F_1|F) \cong \mathrm{Gal}(F_1F_2|F) \cong \mathrm{Gal}(F_2|F).$$

Folglich ist $[F_1 : F] = [F_1F_2 : F] = [F_2 : F]$ und es gilt $F_1 = F_1F_2 = F_2$. □

Voraussetzungen und Notation 2.6. *Den Klassenkörper zu H bezeichnen wir mit F_H.*

Schließlich formulieren wir den Existenzsatz, dessen Beweis wir in Kapitel 4 antreten.

Satz 2.7 (Existenzsatz)**.** *Zu jedem Modul $\mathfrak{m}$ und jeder Untergruppe H von $\mathcal{C}\ell_\mathfrak{m}$ von endlichem Index existiert der Klassenkörper. Umgekehrt existiert zu jeder endlichen abelschen Erweiterung E von F ein Modul $\mathfrak{m}$ und eine Untergruppe H von $\mathcal{C}\ell_\mathfrak{m}$ so dass E der Klassenkörper zu H ist.*

Mit anderen Worten gibt es zu H eine Erweiterung F_H, so dass die Isomorphie $\mathrm{Gal}(F_H|F) \cong \mathcal{C}\ell_\mathfrak{m}/H$ durch die Artinabbildung gegeben wird. Dafür ist also wie bereits erwähnt auch zu überprüfen, dass $(\cdot, F_H|F)$ auf $\mathcal{C}\ell_\mathfrak{m}$ überhaupt wohldefiniert ist, denn ursprünglich war die Artinabbildung ja nur auf der Divisorengruppe $\mathcal{D}^\mathfrak{m}$ definiert. Der Nachweis, dass $\mathcal{P}_\mathfrak{m}$ im Kern der Artinabbildung $(\cdot, F_H|F) : \mathcal{D}^\mathfrak{m} \to \mathrm{Gal}(F_H|F)$ liegt, wird im Beweis des Existenzsatzes erbracht.

Bemerkung 2.8. Ab sofort sprechen wir oft von einer Abbildung $H \mapsto F_H$, die H auf den zugehörigen Klassenkörper abbildet. Für fest gewähltes $\mathfrak{m}$ ist sie per Definition injektiv, denn aus $F_{H_1} = F_{H_2}$ folgt natürlich

$$H_1 = \ker(\cdot, F_{H_1}|F) = \ker(\cdot, F_{H_2}|F) = H_2.$$

Sie ist aber für festes $\mathfrak{m}$ nicht surjektiv. Halten wir hingegen $\mathfrak{m}$ nicht fest, so ist die Abbildung surjektiv aber nicht mehr injektiv da die Wahl von $\mathfrak{m}$ zu gegebener Erweiterung nicht eindeutig ist. In Abschnitt 2.5 werden wir sehen, durch welche zusätzlichen Bedingungen wir die eindeutige Wahl von $\mathfrak{m}$ erzwingen können.

2.2 Eigenschaften des Klassenkörpers

Als nächstes wollen wir die Eigenschaften eines Klassenkörpers untersuchen, unter der Annahme, dass er existiert. Zuerst widmen wir uns der Frage, wie der Klassenkörper von $H_1 \cap H_2$ oder H_1H_2 (der von H_1 und H_2 erzeugten Gruppe) mit den Klassenkörpern zu H_1 und H_2 in Beziehung steht. Es lassen sich hübsche und nützliche funktorielle Eigenschaften beweisen, eine erste Aussage in diese Richtung wurde bereits in Lemma 2.4 gemacht. Allerdings wurden dort nur Untergruppen *derselben* Strahlklassengruppe betrachtet. Allgemein kann wie folgt vorgegangen werden.

Bemerkung 2.9. Angenommen es ist $H_1 \subseteq \mathcal{C}\ell_{\mathfrak{m}_1}$ und $H_2 \subseteq \mathcal{C}\ell_{\mathfrak{m}_2}$. Dann sei

$$\mathfrak{m} := \mathrm{kgV}(\mathfrak{m}_1, \mathfrak{m}_2) := \sum_{\mathfrak{p} \in \mathcal{S}_F} \max(v_{\mathfrak{p}}(\mathfrak{m}_1), v_{\mathfrak{p}}(\mathfrak{m}_2)) \cdot \mathfrak{p}.$$

(Schreibt man Divisoren multiplikativ, so ist dies genau die bekannte Definition des kleinsten gemeinsamen Vielfachen.) Dann haben wir für $i = 1, 2$ surjektive Abbildungen

$$\Psi_i : \mathcal{C}\ell_{\mathfrak{m}} \to \mathcal{C}\ell_{\mathfrak{m}_i}/H_i$$

induziert von der kanonischen Surjektion, und folglich Isomorphien

$$\mathcal{C}\ell_{\mathfrak{m}}/\ker(\Psi_i) \cong \mathcal{C}\ell_{\mathfrak{m}_i}/H_i.$$

Also definieren wir

$$H_i' := \ker(\Psi_i) \subseteq \mathcal{C}\ell_{\mathfrak{m}}$$

und erhalten

$$\mathrm{Gal}(F_{H_i}|F) \cong \mathcal{C}\ell_{\mathfrak{m}_i}/H_i \cong \mathcal{C}\ell_{\mathfrak{m}}/H_i'.$$

Also ist der Klassenkörper F_{H_i} zu $H_i \subseteq \mathcal{C}\ell_{\mathfrak{m}_i}$ gleichzeitig auch der Klassenkörper zu $H_i' \subseteq \mathcal{C}\ell_{\mathfrak{m}}$.

Im Folgenden identifizieren wir stillschweigend wenn nötig H_i' mit H_i um Ausdrücke wie $H_1 \cap H_2$, H_1H_2 oder auch $H_1 \subseteq H_2$ verwenden zu können, auch wenn die H_i ursprünglich in unterschiedlichen Strahlklassengruppen enthalten waren.

Satz 2.10. *Es seien F_1 und F_2 die Klassenkörper zu H_1 bzw. H_2. Dann gilt:*

(*i*) $H_1 \subseteq H_2 \Leftrightarrow F_1 \supseteq F_2$

(*ii*) F_1F_2 *ist der Klassenkörper zu* $H_1 \cap H_2$

(*iii*) $F_1 \cap F_2$ *ist der Klassenkörper zu* H_1H_2.

Beweis. (i) Angenommen $F_1 \supseteq F_2$, dann ist $(\cdot, F_1|F)$ eine Fortsetzung von $(\cdot, F_2|F)$ und für deren Kerne gilt $H_1 \subseteq H_2$. Sei nun umgekehrt $H_1 \subseteq H_2$. Dann ist nach Lemma 2.4

$$H_1 = H_1 \cap H_2 = \ker(\cdot, F_1F_2|F),$$

also $\mathrm{Gal}(F_1|F) \cong \mathrm{Gal}(F_1F_2|F)$. Es folgt $F_2 \subseteq F_1$.

(ii) Folgt sofort aus Lemma 2.4 und Bemerkung 2.9.

(iii) Nach dem Existenzsatz existiert ein H, so dass $F_1 \cap F_2$ der Klassenkörper zu H ist. Wegen $F_1 \cap F_2 \subseteq F_1, F_2$ gilt $H \supseteq H_1, H_2$, also $H \supseteq H_1H_2$. Wegen $H_1, H_2 \subseteq H_1H_2$ gilt $F_1, F_2 \supseteq F_{H_1H_2}$, also $F_1 \cap F_2 \supseteq F_{H_1H_2}$ und deshalb $H \subseteq H_1H_2$. □

Im Folgenden leiten wir eine weitere Charakterisierung des Klassenkörpers her, die vor allem für den Beweis der Sätze 2.13 und 2.20 sehr nützlich ist.

Lemma 2.11. *Es sei F_0 der Klassenkörper zu H_0 und $H \supseteq H_0$. Dann gilt*

$$F_H = \mathrm{Fix}_{F_0}\{(\mathfrak{D}, F_0|F) \mid \mathfrak{D} \in H\}.$$

Beweis. Es bezeichne E den Fixkörper

$$E := \mathrm{Fix}_{F_0}\{(\mathfrak{D}, F_0|F) \mid \mathfrak{D} \in H\} = \{f \in F_0 \mid (\mathfrak{D}, F_0|F)f = f \quad \forall\, \mathfrak{D} \in H\}.$$

Wegen Lemma 1.41 gilt $(\mathfrak{D}, F_0|F)|_E = (\mathfrak{D}, E|F)$ und nach Voraussetzung ist $H_0 \subseteq H$. Damit sieht man leicht, dass

$$\ker(\cdot, E|F) = \{\mathfrak{D} \in \mathcal{C}\ell_{\mathfrak{m}} \mid (\mathfrak{D}, E|F) = \mathrm{id}_E\} = H.$$

Also ist E der Klassenkörper zu H. □

2.3 Vom Klassenkörper zur Normgruppe

In der Kummertheorie kann für eine gegebene Erweiterung $E|F$ die zugehörige Gruppe Δ leicht als $E^n \cap F^\times$ bestimmt werden. Auch in der Klassenkörpertheorie gibt es eine einfache Beschreibung der Gruppe H, die zu einer Erweiterung $E|F$ gehört. Dazu muss man voraussetzen, dass man bereits ein geeignetes $\mathfrak{m}$ kennt. Dies konstruieren wir im Beweis des Existenzsatzes. Dann gilt $H = \mathcal{N}_{E|F}(\mathcal{C}\ell_{\hat{\mathfrak{m}}})$ für $\hat{\mathfrak{m}} = \mathrm{Con}_{E|F}(\mathfrak{m})$.

Um das zu zeigen, müssen wir noch überprüfen, dass Divisornorm und Conorm auf den Strahlklassengruppen überhaupt wohldefiniert sind. Wir geben gleich zusammenfassend einige nützliche Resultate über diese beiden Abbildungen an, die wir auch später noch benötigen.

Die Divisornorm ist definiert durch

$$\mathcal{N}_{E|F}(\mathfrak{P}) = f(\mathfrak{P}|\mathfrak{p}) \cdot \mathfrak{p} \quad \text{für } \mathfrak{P} \in \mathcal{S}_E$$

und wird auf $\mathcal{D}_E$ linear fortgesetzt. Klar ist dann, dass die Divisornorm auch als Abbildung $\mathcal{N}_{E|F} : \mathcal{D}^{\hat{\mathfrak{m}}} \to \mathcal{D}^{\mathfrak{m}}$ wohldefiniert ist. Lemma 1.41 liefert übrigens für die abelsche Erweiterung $E|F$ mit zwischenkörper L die wichtige Formel

$$(\mathcal{N}_{L|F}(\mathfrak{D}), E|F) = (\mathfrak{D}, E|L)$$

für alle erlaubten Divisoren $\mathfrak{D}$ von L. Sie wird im Folgenden häufig zum Einsatz kommen.

Ebenso wird auch die Conorm, definiert durch

$$\mathrm{Con}_{E|F}(\mathfrak{p}) = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}|\mathfrak{p}) \cdot \mathfrak{P} \quad \text{für } \mathfrak{p} \in \mathcal{S}_F,$$

linear auf $\mathcal{D}_F$ fortgesetzt und ist auch als Abbildung $\mathrm{Con}_{E|F} : \mathcal{D}^{\mathfrak{m}} \to \mathcal{D}^{\hat{\mathfrak{m}}}$ wohldefiniert.

Lemma 2.12. *Es sei $E|\mathbb{F}_{q^r}$ eine endliche Erweiterung von $F|\mathbb{F}_q$, die Konstantenkörper jeweils exakt, außerdem $\mathfrak{m}$ ein Modul von F und $\hat{\mathfrak{m}} = \mathrm{Con}_{E|F}(\mathfrak{m})$. Dann gilt für die Divisornorm $\mathcal{N}_{E|F} : \mathcal{D}_E \to \mathcal{D}_F$:*

(i) Für $\mathfrak{D} \in \mathcal{D}_F$ ist $\mathcal{N}_{E|F}(\mathrm{Con}_{E|F}(\mathfrak{D})) = [E : F]\mathfrak{D}$.

(ii) Für $f \in E$ ist $\mathcal{N}_{E|F}((f)_E) = (\mathrm{N}_{E|F}(f))_F$ für die Körpernorm $\mathrm{N}_{E|F}$. Also induziert die Divisornorm eine Abbildung $\mathcal{N}_{E|F} : \mathcal{C}\ell_E \to \mathcal{C}\ell_F$ auf Divisorklassen.

(iii) Es gilt $\mathcal{N}_{E|F}(\mathcal{P}_{\hat{\mathfrak{m}}}) \subseteq \mathcal{P}_{\mathfrak{m}}$, also ist die Divisornorm auch als Abbildung $\mathcal{N}_{E|F} : \mathcal{C}\ell_{\hat{\mathfrak{m}}} \to \mathcal{C}\ell_{\mathfrak{m}}$ wohldefiniert.

(iv) Wegen $\deg(\mathcal{N}_{E|F}(\mathfrak{D})) = r \deg(\mathfrak{D})$ für $\mathfrak{D} \in \mathcal{D}_E$ induziert die Divisornorm eine Abbildung $\mathcal{N}_{E|F} : \mathcal{C}\ell^0_{\hat{\mathfrak{m}}} \to \mathcal{C}\ell^0_{\mathfrak{m}}$.

Beweis. [Vil06, Thm. 5.3.7, S. 130], zu zeigen bleibt noch (iii): Es sei $(f) \in \mathcal{P}_{\hat{\mathfrak{m}}}$, d.h. $f \equiv 1 \bmod^* \hat{\mathfrak{m}}$. Wir wollen zeigen, dass $\mathrm{N}_{E|F}(f) \equiv 1 \bmod^* \mathfrak{m}$. Dann folgt $\mathrm{N}_{E|F}(f) \in \mathcal{P}_{\mathfrak{m}}$ und (ii) liefert die Behauptung.

Es bezeichne $\mathcal{M} := \operatorname{supp} \mathfrak{m}$ und $\hat{\mathcal{M}} := \operatorname{supp} \hat{\mathfrak{m}}$. Wir definieren den Holomorphiering

$$R := \bigcap_{\mathfrak{p} \in \mathcal{M}} \mathcal{O}_{\mathfrak{p}} \quad \text{mit Ideal} \quad I := \prod_{\mathfrak{p} \in \mathcal{M}} (R \cap \mathfrak{p})^{v_{\mathfrak{p}}(\mathfrak{m})}$$

und ganz analog

$$\hat{R} := \bigcap_{\hat{\mathfrak{p}} \in \hat{\mathcal{M}}} \mathcal{O}_{\hat{\mathfrak{p}}} \quad \text{mit Ideal} \quad \hat{I} := \prod_{\hat{\mathfrak{p}} \in \hat{\mathcal{M}}} (\hat{R} \cap \hat{\mathfrak{p}})^{v_{\hat{\mathfrak{p}}}(\hat{\mathfrak{m}})}.$$

Dann gilt für die Ideale $\hat{I} = I\hat{R}$. Laut [Sti93, Cor. III.3.5, S. 75] ist $\hat{R}$ ein freier R-modul vom Rang $[E : F]$.

Nach Voraussetzung ist $v_{\hat{\mathfrak{p}}}(f-1) \geq v_{\hat{\mathfrak{p}}}(\hat{\mathfrak{m}}) > 0$ für alle $\hat{\mathfrak{p}} \in \hat{\mathcal{M}}$, also $f - 1 \in \hat{R}$ und folglich $f \in \hat{R}$. Außerdem gilt nach Voraussetzung $f \equiv 1 \bmod \hat{I}$. Der Wert von $\mathrm{N}_{E|F}(f)$ wird gegeben durch die Determinante der Darstellungsmatrix der Abbildung „Multiplikation mit f“ auf einer R-Basis von $\hat{R}$. Nun ist diese Darstellungsmatrix Koeffizientenweise äquivalent zur Einheitsmatrix modulo I, also gilt $\mathrm{N}_{E|F}(f) \equiv 1 \bmod I$, und daraus folgt $\mathrm{N}_{E|F} \equiv 1 \bmod^* \mathfrak{m}$ wie behauptet. □

Satz 2.13. *Es sei E der Klassenkörper zur Gruppe $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$. Dann gilt*

$$H = \mathcal{N}_{E|F}(\mathcal{C}\ell_{\hat{\mathfrak{m}}})$$

für $\hat{\mathfrak{m}} = \mathrm{Con}_{E|F}(\mathfrak{m})$.

Beweis. Es sei r der Grad der Konstantenkörpererweiterung enthalten in $E|F$. Zu zeigen ist $\ker(\cdot, E|F) = \mathcal{N}_{E|F}(\mathcal{C}\ell_{\hat{\mathfrak{m}}})$. Die Inklusion „$\supseteq$“ folgt aus Satz 1.43. Für die Inklusion „$\subseteq$“ sei $[\mathfrak{D}] \in \ker(\cdot, E|F) \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ und $[\mathfrak{A}] \in \mathcal{C}\ell_{\mathfrak{m}}$ eine Divisorklasse vom Grad 1. Wir wählen nun d so groß, dass sowohl die Ordnung des Artinautomorphismus $(\mathfrak{A}, E|F)$ als auch r die Zahl d teilt, und dass außerdem laut Primzahlsatz 1.47 eine Stelle $\mathfrak{p}$ von F mit $[\mathfrak{D} + d\mathfrak{A}] = [\mathfrak{p}]$ existiert. Dann gilt wegen $[\mathfrak{D}] \in \ker(\cdot, E|F)$ und nach Wahl von d

$$([\mathfrak{p}], E|F) = ([\mathfrak{D}], E|F)([\mathfrak{A}], E|F)^d = \mathrm{id}_E\,.$$

Deshalb ist $\mathfrak{p}$ in $E|F$ voll zerlegt und für alle Stellen $\mathfrak{P}$ von E über $\mathfrak{p}$ ist der Trägheitsgrad $f(\mathfrak{P}|\mathfrak{p}) = 1$. Weiter sei $\hat{\mathfrak{A}} := \mathrm{Con}_{E|F}(\mathfrak{A})$. Dann erhalten wir für eine beliebige Stelle $\mathfrak{P}$ über $\mathfrak{p}$

$$\mathcal{N}_{E|F}([\mathfrak{P} - \frac{d}{r}\hat{\mathfrak{A}}]) = [f(\mathfrak{P}|\mathfrak{p})\mathfrak{p} - d\mathfrak{A}] = [\mathfrak{p} - d\mathfrak{A}] = [\mathfrak{D}]$$

und wir haben ein Urbild von $[\mathfrak{D}]$ unter der Normabbildung gefunden. □

2.4 Das Artinsche Reziprozitätsgesetz

Das (Artinsche) Reziprozitätsgesetz bestimmt den Kern der Artinabbildung. Unsere Formulierung orientiert sich an [Ros02, Thm. 9.23, S. 140], wo allerdings kein Beweis angegeben wird. Unser sehr kurzer Beweis folgt schon aus den in diesem Kapitel aufgeführten Aussagen über die Klassenkörpertheorie, insbesondere aus dem Satz 2.13, natürlich weiterhin unter der Annahme, der Existenzsatz wäre bereits bewiesen. In der Literatur wird das Reziprozitätsgesetz oft zuerst bewiesen und der Existenzsatz dann daraus gefolgert.

Satz 2.14 (Reziprozitätsgesetz)**.** *Es sei $E|F$ eine endliche abelsche Erweiterung globaler Funktionenkörper, $\mathcal{M}$ die Menge aller in E verzweigten Stellen von F und $\mathcal{D}^{\mathcal{M}}$ die Gruppe der Divisoren mit Träger disjunkt zu $\mathcal{M}$. Dann ist die Artinabbildung*

$$(\cdot, E|F) : \mathcal{D}^{\mathcal{M}} \to \mathrm{Gal}(E|F)$$

surjektiv und es existiert ein effektiver Divisor $\mathfrak{m}$ mit Träger $\mathcal{M}$ so dass $\mathcal{P}_{\mathfrak{m}}\mathcal{N}_{E|F}(\mathcal{D}^{\hat{\mathcal{M}}})$ der Kern der Abbildung ist. Dabei bezeichnet $\hat{\mathcal{M}}$ die Menge der Stellen von E, die verzweigt über F sind.

Beweis. Die Surjektivität des Artinsymbols folgt sofort aus dem Satz von Tschebotarev 1.45. Da $E|F$ endlich und abelsch ist, existiert nach dem Existenzsatz und Satz 2.13 ein effektiver Divisor $\mathfrak{m}$ von F so dass E der Klassenkörper zu $\mathcal{N}_{E|F}(\mathcal{C}\ell_{\hat{\mathfrak{m}}})$ mit $\hat{\mathfrak{m}} := \mathrm{Con}_{E|F}(\mathfrak{m})$ ist. Also ist $\mathcal{N}_{E|F}(\mathcal{C}\ell_{\hat{\mathfrak{m}}})$ der Kern der induzierten Artinabbildung $(\cdot, E|F) : \mathcal{C}\ell_{\mathfrak{m}} \to \mathrm{Gal}(E|F)$ und folglich ist $\mathcal{P}_{\mathfrak{m}}\mathcal{N}_{E|F}(\mathcal{D}^{\hat{\mathfrak{m}}})$ der Kern der Artinabbildung $(\cdot, E|F) : \mathcal{D}^{\mathfrak{m}} \to \mathrm{Gal}(E|F)$. □

Die Artinabbildung wird auch Normrestsymbol genannt (siehe [Neu92, S. 409]), und die Aussage des Reziprozitätsgesetzes wird oft als Isomorphie

$$\mathrm{Gal}(E|F) \cong \mathcal{C}\ell_{\mathfrak{m}}/\mathcal{N}_{E|F}(\mathcal{C}\ell_{\hat{\mathfrak{m}}})$$

formuliert.

Bemerkung 2.15. Für Konstantenkörpererweiterungen $E = F\mathbb{F}_{q^r}$ von F lässt sich der Kern der Artinabbildung deutlich leichter bestimmen, man muss nicht die mächtigen Werkzeuge aus der Klassenkörpertheorie benutzen. Dies liegt daran, dass für Konstantenkörpererweiterungen die Artinabbildung $(\mathfrak{D}, E|F)$ durch $\varphi_q^{\deg(\mathfrak{D})}$ gegeben ist. Dabei ist φ_q der Frobeniusautomorphismus $x \mapsto x^q$ (siehe [Ros02, Prop. 9.19, S. 136]). Da Konstantenkörpererweiterungen generell unverzweigt sind, kann man $\mathfrak{m} \geq 0$ ganz beliebig wählen. Dann sieht man sofort, dass sowohl alle Divisoren vom Grad 0 als auch alle Elemente aus $r \cdot \mathcal{D}^{\mathfrak{m}}$ im Kern der Artinabbildung $(\cdot, E|F) : \mathcal{D}^{\mathfrak{m}} \to \mathrm{Gal}(E|F)$ enthalten sind. Tatsächlich wird der Kern schon von $\mathcal{D}^{\mathfrak{m},0}$ (den Divisoren teilerfremd zu $\mathfrak{m}$ vom Grad 0) und $r\mathcal{D}^{\mathfrak{m}}$ erzeugt, da das Erzeugnis den Index r in $\mathcal{D}^{\mathfrak{m}}$ hat (siehe hierzu auch [Ros02, Prop. 9.20, S. 137]). Insbesondere liegen die Hauptdivisoren $\mathcal{P}_{\mathfrak{m}}$ immer im Kern, da sie Grad 0 haben.

Die Wahl von $\mathfrak{m}$ ist für Konstantenkörpererweiterungen also trivial, und mit einer Rechnung wie im Beweis zu Satz 2.13 kann man auch die Aussage über die Normgruppe leicht nachprüfen. Dann hat man das Reziprozitätsgesetz auf elementare Weise bewiesen.

Bemerkung 2.16. Tatsächlich ist das bekannte quadratische Reziprozitätsgesetz

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

für zwei verschiedene ungerade Primzahlen p und q ein Spezialfall des Artinschen Reziprozitätsgesetzes. Nämlich kann man für den einfachen Fall eines quadratischen Zahlkörpers $\mathbb{Q}(\sqrt{m})$ tatsächlich am Legendre-Symbol $\left(\frac{m}{p}\right)$ das Verzweigungs-/Zerlegungsverhalten von p ablesen (für Details hierzu siehe [Mil08, S. 2f] und [Neu92, S. 434ff]). Manche sehen deshalb schon das quadratische Reziprozitätsgesetz als das erste Resultat der Klassenkörpertheorie an.

2.5 Führer von abelschen Erweiterungen

Der Existenzsatz der Klassenkörpertheorie wie wir ihn formuliert haben garantiert die Existenz eines Klassenkörpers zu gegebener Gruppe H und die Existenz eines geeigneten $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ für gegebene abelsche Erweiterung, wobei hier die Schwierigkeit im Beweis der Existenz eines geeigneten $\mathfrak{m}$ liegt (die

Untergruppe H bestimmt man dann leicht als Kern der Artinabbildung). Wir haben auch leicht gesehen, dass der Klassenkörper eindeutig bestimmt ist. Umgekehrt ist aber der Modul $\mathfrak{m}$ bei weitem nicht eindeutig bestimmt. Es gibt sogar unendlich viele Möglichkeiten, ein geeignetes $\mathfrak{m}$ zu wählen. Hat man eines gefunden, so tut es jedes größere $\mathfrak{m}$ auch. Die Abbildung $H \mapsto F_H$ ist also zunächst nur surjektiv aber nicht injektiv, wenn man alle Untergruppen aller Strahlklassengruppen zulässt.

Um trotzdem *bijektiv* zwischen Gruppen und Erweiterungen hin- und herzuschalten (wie es auch die Kummertheorie erlaubt) schränkt man die Menge der Gruppen wie folgt ein. Ist $E|F$ gegeben, so kann man ein minimales $\mathfrak{m}$ wählen. Wir erinnern an die Definition des *Führers* aus Abschnitt 1.5: Für $\mathfrak{m}' \leq \mathfrak{m}$ gibt es einen kanonischen Epimorphismus

$$\Psi_{\mathfrak{m}'} : \mathcal{C}\ell_{\mathfrak{m}} \to \mathcal{C}\ell_{\mathfrak{m}'}.$$

Für eine gegebene Untergruppe H von $\mathcal{C}\ell_{\mathfrak{m}}$ heißt das eindeutig bestimmte kleinste Modul $\mathfrak{f}$ mit

$$\mathcal{C}\ell_{\mathfrak{f}}/\Psi_{\mathfrak{f}}(H) \cong \mathcal{C}\ell_{\mathfrak{m}}/H$$

der *Führer* von H.

Wie schon in Bemerkung 2.9 festgestellt, ist der Klassenkörper zu $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ auch der Klassenkörper zu $\Psi_{\mathfrak{f}}(H) \subseteq \mathcal{C}\ell_{\mathfrak{f}}$ und $\mathfrak{f}$ heißt dann der *Führer* der Erweiterung. Auf diese Weise kann einer gegebenen abelschen Erweiterung also ein eindeutiger Modul, nämlich sein Führer, zugeordnet werden. Wir bemerken, dass der Führer einer abelschen Körpererweiterung erst im Kontext der Klassenkörpertheorie definiert ist. Ohne diesen mächtigen Apparat ist die Definition nicht offensichtlich.

Man kann nun eine Äquivalenzrelation definieren, in der zwei Untergruppen von Strahlklassengruppen dann als äquivalent gelten, wenn sie denselben Führer haben. Dabei können wie in Bemerkung 2.9 auch Untergruppen verschiedener Strahlklassengruppen verglichen werden. Janusz nennt diese Äquivalenzklassen „ideal groups“ (siehe [Jan73, S. 168]), sie ermöglichen die gewünschte Bijektion.

Satz 2.17. *Die Abbildung $H \mapsto F_H$ ist eine Bijektion zwischen den Äquivalenzklassen von Untergruppen der Strahlklassengruppen (von endlichem Index) und allen endlichen abelschen Erweiterungen von F. Die Umkehrabbildung ist durch $E \mapsto \mathcal{N}_{E|F}(\mathcal{C}\ell_{\hat{\mathfrak{f}}})$ gegeben, wobei $\mathfrak{f}$ der Führer von $E|F$ und $\hat{\mathfrak{f}}$ dessen Conorm ist.*

Reden wir von der Menge aller Erweiterungen, so sind stets die Erweiterungen innerhalb eines fest gewählten algebraischen Abschlusses gemeint.

Es ist klar, dass der Führer einer Erweiterung genau die verzweigten Stellen enthält. Geht man nämlich davon aus, dass eine Stelle im Träger des Führers

$\mathfrak{f}$ von $F_H|F$ unverzweigt ist, so kann man ein $\mathfrak{m}$ mit echt kleinerem Träger definieren, so dass $F_H|F$ immer noch unverzweigt außerhalb $\operatorname{supp}\mathfrak{m}$ ist. Die Klassenkörpertheorie liefert dann eine Untergruppe H' von $\mathcal{C}\ell_{\mathfrak{m}}$ mit $\mathcal{C}\ell_{\mathfrak{m}}/H' \cong \mathrm{Gal}(F_H|F) \cong \mathcal{C}\ell_{\mathfrak{f}}/H$, ein Widerspruch zur Minimalität von $\mathfrak{f}$. Also besitzt jede unverzweigte Erweiterung den Führer 0.

Bemerkung 2.18. In der Literatur finden sich Resultate darüber, wie die Koeffizienten des Führers genau aussehen, für (abelsche) Erweiterungen von Funktionenkörpern siehe [Aue99, Kap. 3]. Kennt man den Führer einer Erweiterung, kann man an seinen Koeffizienten die Art der Verzweigung aller Stellen ablesen: Die Stellen mit Koeffizienten 0 sind unverzweigt, die mit Koeffizienten 1 sind zahm verzweigt, und die mit Koeffizienten > 1 sind sogar wild verzweigt.

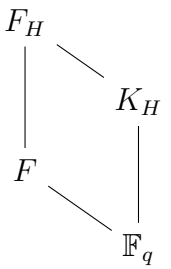
An der eben geführten Diskussion wird die schon in der Einführung erwähnte Problematik deutlich, dass es eher umständlich ist, zu einer gegebenen Erweiterung $E|F$ erst einen Modul $\mathfrak{m}$ zu wählen bzw. den Führer $\mathfrak{f}$ zu bestimmen, um dann eine Untergruppe H von $\mathcal{C}\ell_{\mathfrak{m}}$ bzw. $\mathcal{C}\ell_{\mathfrak{f}}$ zu erhalten mit

$$\mathrm{Gal}(E|F) \cong \mathcal{C}\ell_{\mathfrak{m}}/H.$$

Praktischer wäre es, nur Untergruppen einer einzigen Gruppe betrachten zu müssen, um die abelschen Erweiterungen alle klassifizieren zu können, so wie man beispielsweise nur die Untergruppen der (gewöhnlichen) Klassengruppe betrachten muss, um die *unverzweigten* abelschen Erweiterugen zu klassifizieren. Chevalleys idealtheoretischer Ansatz der Klassenkörpertheorie erreicht genau das. Er umgeht das Problem der Wahl von $\mathfrak{m}$, indem er sich der Idelklassengruppe bedient. So müssen nur Untergruppen der einen Idelklassengruppe betrachtet werden.

2.6 Grad der Konstantenkörpererweiterung

Zum Schluss widmen wir uns der Frage, wie groß der (exakte) Konstanenkörper von F_H im Vergleich zu dem von F ist, mit anderen Worten welchen Grad die Konstantenkörpererweiterung hat, die $F_H|F$ beinhaltet. Dies gehört nicht zum Standardstoff der Klassenkörpertheorie, da sie sich klassischerweise mit Zahlkörpern beschäftigt. Die Aussage findet sich allerdings in [Hal90] mit idealtheoretischem Beweis. Wir geben hier einen direkten und elementaren Beweis an.



Definition 2.19. Für eine Gruppe $H \neq \{0\}$ von Divisoren oder Divisorklassen definieren wir den Grad

$$\deg(H) := \mathrm{ggT}\{\deg(\mathfrak{D}) \mid \mathfrak{D} \in H\}.$$

Er ist stets endlich.

Satz 2.20. *Es sei F_H der Klassenkörper über $F|\mathbb{F}_q$ zur Gruppe $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$. Für den exakten Konstantenkörper K_H von F_H gilt*

$$[K_H : \mathbb{F}_q] = \deg(H).$$

Beweis. Es sei $\ell := \deg(H)$. Wir betrachten zunächst die Konstantenkörpererweiterung $F\mathbb{F}_{q^\ell}|F$. Die entsprechende Galoisgruppe wird erzeugt vom Frobeniusautomorphismus φ_q, der auf $\mathbb{F}_{q^\ell}$ durch $\varphi_q(x) = x^q$ operiert, siehe [Sti93, Lemma V.1.9, S. 163]. Weiter für jeden Divisor $\mathfrak{D}$ von F der Artinautomorphismus $(\mathfrak{D}, F\mathbb{F}_{q^\ell}|F)$ durch $\varphi_q^{\deg \mathfrak{D}}$ gegeben, siehe [Ros02, Prop. 9.19, S. 136]). Also erhalten wir

$$\ker(\cdot, F\mathbb{F}_{q^\ell}|F) = \{\mathfrak{D} \in \mathcal{C}\ell_{\mathfrak{m}} \mid \varphi_q^{\deg \mathfrak{D}} = \mathrm{id}_{F\mathbb{F}_{q^\ell}}\} = \{\mathfrak{D} \in \mathcal{C}\ell_{\mathfrak{m}} \mid \ell \mid \deg \mathfrak{D}\} \supseteq H.$$

Die Erweiterung $F_H\mathbb{F}_{q^\ell}|F$ ist als Kompositum der beiden abelschen Erweiterungen $F_H|F$ und $F\mathbb{F}_{q^\ell}|F$ wieder abelsch. Es gilt mit Lemma 2.4

$$\ker(\cdot, F_H\mathbb{F}_{q^\ell}|F) = \ker(\cdot, F_H|F) \cap \ker(\cdot, F\mathbb{F}_{q^\ell}|F) = H,$$

und deshalb $F_H\mathbb{F}_{q^\ell} = F_H$ und $\mathbb{F}_{q^\ell} \subseteq K_H$.

Umgekehrt sei $\mathfrak{p}$ eine Stelle von F und $\sigma_{\mathfrak{p}}$ der zugehörige Artinautomorphismus $(\mathfrak{p}, F_H|F)$. Dann gilt für die Stellen $\mathfrak{P}$ von F_H über $\mathfrak{p}$

$$\sigma_{\mathfrak{p}}(x) \equiv x^{\mathfrak{N}(\mathfrak{p})} \bmod \mathfrak{P} \quad \text{für alle } x \in \mathcal{O}_{\mathfrak{P}}.$$

Wegen $K_H \cap \mathfrak{P} = \{0\}$ gilt

$$\sigma_{\mathfrak{p}}(x) = x^{\mathfrak{N}(\mathfrak{p})} = x^{q^{\deg(\mathfrak{p})}} \quad \text{für alle } x \in K_H,$$

d.h. $\sigma_{\mathfrak{p}}|_{K_H} = \varphi_q^{\deg(\mathfrak{p})}|_{K_H}$, und für einen Divisor $\mathfrak{D}$ gilt entsprechend

$$\sigma_{\mathfrak{D}}|_{K_H} = \varphi_q^{\deg(\mathfrak{D})}|_{K_H}.$$

Nun ist $\sigma_{\mathfrak{D}} = \mathrm{id}_{F_H}$ und folglich $\varphi_q^{\deg \mathfrak{D}}|_{K_H} = \mathrm{id}_{K_H}$ für alle $\mathfrak{D} \in H$. Nach Definition von ℓ erhalten wir $\varphi_q^{\ell}|_{K_H} = \mathrm{id}_{K_H}$ und folglich $K_H \subseteq \mathbb{F}_{q^\ell}$. □

Ist unter der Isomorphie

$$\mathcal{C}\ell_{\mathfrak{m}} \cong \mathcal{C}\ell^0_{\mathfrak{m}} \times \mathbb{Z}$$

die Gruppe H isomorph zu $H^0 \times \ell\mathbb{Z}$ (für Untergruppen H^0 von $\mathcal{C}\ell^0_{\mathfrak{m}}$ und $\ell\mathbb{Z}$ von $\mathbb{Z}$), so ist $\deg(H) = \ell$ und $\mathbb{F}_{q^\ell}$ der exakte Konstantenkörper von F_H. Der „$\mathbb{Z}$-Anteil“ von H ist also allein für die Konstantenkörpererweiterungen zuständig.

Hier sieht man auch, was mit den Untergruppen von *unendlichem* Index passiert. $\mathcal{C}\ell^0_{\mathfrak{m}}$ ist endlich, hat also nur Untergruppen von endlichem Index, und

die einzige Untergruppe von $\mathbb{Z}$ von unendlichem Index ist die triviale. Sämtliche Untergruppen H von $\mathcal{Cl}_{\mathfrak{m}}$ von unendlichem Index haben also die Form $H \cong H^0 \times \{0\}$. Solche Gruppen sind dann lediglich für weitere Konstantenkörpererweiterungen (von unendlichem Grad) des Klassenkörpers zu $H^0 \times \mathbb{Z}$ zuständig.

An den Konstantenkörpererweiterungen liegt es auch, dass bei Funktionenkörpern die Definition eines Strahlklassenkörpers nicht so einfach möglich ist wie bei Zahlkörpern. Dort wird der *Strahlklassenkörper modulo* $\mathfrak{m}$ als der Klassenkörper zur Untergruppe $\{0\}$ von $\mathcal{Cl}_{\mathfrak{m}}$ definiert, und alle Klassenkörper zu Untergruppen von $\mathcal{Cl}_{\mathfrak{m}}$ sind dann Teilkörper des Strahlklassenkörpers. Bei Funktionenkörpern hat die triviale Untergruppe aber unendlichen Index. Man könnte den Klassenkörper zu einer Untergruppe der Form $\{0\} \times \ell\mathbb{Z}$ als den Strahlklassenkörper zu $\mathfrak{m}$, ℓ und $\mathfrak{A}$ definieren, hier ist das $\mathfrak{A}$ gemeint, durch das die Isomorphie

$$\mathcal{Cl}_{\mathfrak{m}} \cong \mathcal{Cl}_{\mathfrak{m}}^0 \times \mathbb{Z},\ [\mathfrak{D}] \mapsto ([\mathfrak{D} - \mathfrak{A} \cdot \deg(\mathfrak{D})], \deg(\mathfrak{D}))$$

gegeben ist. Nimmt man aber das Kompositum über alle solchen Körper, so erhält man stets eine *unendliche* Erweiterung.

Auch der Hilbertsche Klassenkörper existiert für Funktionenkörper so nicht. Bei Zahlkörpern hat er eine besondere Stellung unter den Strahlklassenkörpern, es ist der Strahlklassenkörper modulo $\mathfrak{m} = 0$, also die maximale abelsche unverzweigte Erweiterung. Bei Funktionenkörpern hat auch sie unendlichen Grad.

2.7 Zusammenfassung Hauptsatz der Klassenkörpertheorie

Zum Schluss dieses Kapitels wollen wir noch einmal die wichtigsten Aussagen der Klassenkörpertheorie, die in dieser Arbeit bewiesen werden/wurden, in einem großen Hauptsatz möglichst kurz und bündig zusammenfassen. An diesem Hauptsatz kann man auch schon direkt das Artinsche Reziprozitätsgesetz ablesen.

Satz 2.21 (Hauptsatz der Klassenkörpertheorie)**.** *Es sei F ein globaler Funktionenkörper mit exaktem Konstantenkörper $\mathbb{F}_q$. Dann liefert die Abbildung*

$$E \mapsto \mathcal{N}_{E|F}(\mathcal{Cl}_{\mathrm{Con}_{E|F}(\mathfrak{f})}),$$

wobei $\mathfrak{f}$ den Führer von $E|F$ bezeichnet, eine 1-1-Korrespondenz zwischen den endlichen abelschen Erweiterungen von F und den Äquivalenzklassen von Untergruppen der Strahlklassengruppen von endlichem Index mit gleichem Führer.

Sind H und F_H einander unter dieser Abbildung zugeordnet, so heißt F_H der Klassenkörper zu H und es gilt

$$\mathcal{C}\ell_{\mathfrak{f}}/H \cong \mathrm{Gal}(F_H|F).$$

Der Isomorphismus wird gegeben durch die Artinabbildung $(\cdot, F_H|F)$. Der exakte Konstantenkörper von F_H ist $\mathbb{F}_{q^{\deg(H)}}$.

Darüber hinaus gilt für zwei Untergruppen H_1 und H_2 und deren Klassenkörper F_{H_1} bzw. F_{H_2} :

- $H_1 \subset H_2 \Leftrightarrow F_{H_1} \supset F_{H_2}$
- *$F_{H_1}F_{H_2}$ ist der Klassenkörper zu $H_1 \cap H_2$*
- *$F_{H_1} \cap F_{H_2}$ ist der Klassenkörper zu H_1H_2.*

Wir fassen auch noch einmal die Beschreibungen des Klassenkörpers F_H zu $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ zusammen, die wir im Laufe des Kapitels gewonnen haben:

- F_H ist diejenige abelsche Erweiterung von F, für die $\mathrm{Gal}(F_H|F) \cong \mathcal{C}\ell_{\mathfrak{m}}/H$ (unter der Artinabbildung) gilt.
- F_H ist diejenige abelsche Erweiterung von F, für die $H = \ker(\cdot, F_H|F)$ gilt.
- $F_H = \mathrm{Fix}\{(\mathfrak{D}, F_{H_0}|F) \mid \mathfrak{D} \in H\}$ für jedes $H_0 \subseteq H$.
- F_H ist der Klassenkörper zu $\mathcal{N}_{F_H|F}(\mathcal{C}\ell_{\mathrm{Con}_{F_H|F}(\mathfrak{m})})$.

Kapitel 3

Eine verallgemeinerte Tatepaarung

Ein sehr zentraler Baustein in dem Zugang zur Klassenkörpertheorie, der in der vorliegenden Arbeit präsentiert wird, ist eine neue Paarung. Sie geht aus einer Verbindung von Kummer- und Tatepaarung durch das Artinsymbol hervor. Ihre wichtigste Eigenschaft ist die Nichtausartung, die im Wesentlichen auf der Surjektivität der Artinabbildung beruht, welche wiederum aus dem Dichtigkeitssatz von Tschebotarev folgt.

Die Tatepaarung findet heutzutage vielerlei Anwendungen, die wichtigste vielleicht in der paarungsbasierte Kryptographie (siehe [BSS05, Part 4]). Deshalb ist auch die hier gegebene Verallgemeinerung der Tatepaarung an sich schon von Interesse, über ihre Anwendung in der Klassenkörpertheorie hinaus. Es lohnt sich also, der Paarung und ihren Eigenschaften ein gesamtes Kapitel zu widmen.

Um die Paarung definieren zu können, führen wir in Abschnitt 3.1 zunächst die n-Selmergruppe ein. Dann stellen wir in Abschnitt 3.2 den wichtigen Zusammenhang zwischen Kummer- und Tatepaaurung her, auf dem ein großer Teil der folgenden Theorie beruht. Schließlich definieren wir in Abschnitt 3.3 die neue Paarung und zeigen, dass sie nicht ausgeartet ist.

Voraussetzungen und Notation 3.1. *Es sei F ein globaler Funktionenkörper mit dem exakten Konstantenkörper $\mathbb{F}_q$ und $\mathfrak{m}$ ein Modul, also ein effektiver Divisor von F. Mit $\mathcal{M}$ bezeichnen wir den Träger von $\mathfrak{m}$, er ist eine endliche Teilmenge von $\mathcal{S}_F$. Dazu sei eine natürliche Zahl n fest gewählt, so dass $\mathrm{ggT}(n, q) = 1$ und die Gruppe μ_n der n-ten Einheitswurzeln komplett in F enthalten ist.*

F und n erfüllen also alle Voraussetzungen für die multiplikative Kummertheorie. Dies ist wichtig, da wir Kummererweiterungen der Form $F(\sqrt[n]{\Delta})|F$ betrachten werden, und erst mit den gemachten Voraussetzungen sind sie überhaupt normal und somit galoissch. Mehr noch, sie sind sogar abelsch. Da $\mathbb{F}_q$ der exakte Konstantenkörper von F ist, gilt $\mu_n \subseteq F$ genau dann, wenn

$\mu_n \subseteq \mathbb{F}_q$, und das gilt genau für solche n, für die $q \equiv 1 \bmod n$. Aus dieser Bedingung folgt $\mathrm{ggT}(n, q) = 1$, was allerdings echt schwächer ist.

3.1 Die Selmergruppe

Der linke Definitionsbereich der neuen Paarung ist die sogenannte n-Selmergruppe. Sie hängt eng mit dem Verzweigungsverhalten von Kummererweiterungen zusammen.

Definition 3.2. Sei $S_{n,\mathfrak{m}} := \{f \in F^\times \mid v_\mathfrak{p}(f) \equiv 0 \bmod n \ \ \forall\, \mathfrak{p} \notin \operatorname{supp} \mathfrak{m}\}$. Die Gruppe $S_{n,\mathfrak{m}}/(F^\times)^n$ heißt die *zu* $\mathfrak{m}$ *gehörende* n*-Selmergruppe* oder auch nur *Selmergruppe*.

Für Kummererweiterungen $F(\sqrt[n]{f})|F$ ist bekannt, dass eine Stelle $\mathfrak{p}$ von F genau dann unverzweigt ist, wenn $v_\mathfrak{p}(f) \equiv 0 \bmod n$ gilt (siehe Satz 1.24). Ist $f \in S_{n,\mathfrak{m}}$, so ist $F(\sqrt[n]{f})|F$ also unverzweigt für alle Stellen $\mathfrak{p} \notin \mathcal{M} = \operatorname{supp} \mathfrak{m}$. Analog dazu ist $F(\sqrt[n]{\Delta})|F$ unverzweigt für alle Stellen $\mathfrak{p} \notin \mathcal{M}$ falls $\Delta \subseteq S_{n,\mathfrak{m}}$.

Unsere Definition der Selmergruppe ist eine Verallgemeinerung der bereits bekannten Definition aus [Coh00, Def. 5.2.4, S. 231]. Ist nämlich $\mathfrak{m} = 0$, so ist die n-Selmergruppe, die wir dann auch nur mit S_n bezeichnen, gegeben durch

$$\begin{aligned} S_n &= \{f \in F^\times \mid v_\mathfrak{p}(f) \equiv 0 \bmod n \ \forall\, \mathfrak{p} \in \mathcal{S}_F\} \\ &= \{f \in F^\times \mid \exists\, \mathfrak{D} \in \mathcal{D}_F : (f) = n\mathfrak{D}\}. \end{aligned}$$

Für $\Delta \subseteq S_n$ ist die Erweiterung $F(\sqrt[n]{\Delta})|F$ dann sogar komplett unverzweigt. In diesem Fall lässt sich auch ein Resultat über die Kardinalität der Selmergruppe sehr leicht nachprüfen, das wir weiter unten für den allgemeineren Fall mit ein wenig Aufwand beweisen müssen. Dazu betrachten wir die kurze exakte Sequenz

$$1 \to {\mathbb{F}_q}^\times/({\mathbb{F}_q}^\times)^n \to S_n/(F^\times)^n \to \mathcal{C}\ell_F^0[n] \to 0,$$

wobei die Abbildung $S_n/(F^\times)^n \to \mathcal{C}\ell_F^0[n]$ durch $\bar{f} \mapsto [\mathfrak{D}]$ mit $n\mathfrak{D} = (f)$ gegeben ist. (Offensichtlich ist das $\mathfrak{D}$ mit $(f) = n\mathfrak{D}$ durch seine Koeffizienten eindeutig bestimmt, falls es existiert.) Den Beweis der Exaktheit sparen wir uns hier, sie ist aber leicht nachzurechnen, wie auch die Isomorphien

$$S_n/(F^\times)^n \cong \mathcal{C}\ell_F^0[n] \times {\mathbb{F}_q}^\times/({\mathbb{F}_q}^\times)^n \cong \mathcal{C}\ell_F^0[n] \times \mathbb{Z}/n\mathbb{Z}$$

unter Berücksichtigung der Voraussetzung $\mu_n \subseteq F$. Insbesondere ist diese spezielle Selmergruppe also endlich und für ihre Kardinalität gilt

$$\#S_n/(F^\times)^n = n \cdot \#\mathcal{C}\ell_F^0[n].$$

Zusammen mit der bekannten Isomorphie $\mathcal{C}\ell_F/n\mathcal{C}\ell_F \cong \mathcal{C}\ell_F^0/n\mathcal{C}\ell_F^0 \times \mathbb{Z}/n\mathbb{Z}$ erhalten wir sofort

$$\#S_n/(F^\times)^n = \#\mathcal{C}\ell_F/n\mathcal{C}\ell_F.$$

Auch die allgemeine Selmergruppe $S_{n,\mathfrak{m}}/(F^\times)^n$ ist endlich, für ihre Kardinalität gilt ein analoges Resultat unter der Annahme, dass die Stellen in $\mathcal{M}$ bereits die gewöhnliche Klassengruppe $\mathcal{C}\ell_F$ erzeugen. Da $\mathcal{C}\ell_F^0$ endlich ist, sieht man an der Isomorphie $\mathcal{C}\ell_F \cong \mathcal{C}\ell_F^0 \times \mathbb{Z}$, dass $\mathcal{C}\ell_F$ endlich erzeugt ist. Deshalb ist es möglich, eine solche endliche Menge $\mathcal{M}$ groß genug zu wählen. Das folgende Lemma ist zentraler Bestandteil des Beweises der Nichtausartung der neuen Paarung in Abschnitt 3.3.

Lemma 3.3. *Ist der Träger $\mathcal{M}$ von $\mathfrak{m}$ so groß, dass die Stellen in $\mathcal{M}$ die Klassengruppe $\mathcal{C}\ell_F$ erzeugen, so gilt*

$$\#S_{n,\mathfrak{m}}/(F^\times)^n = \#\mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}}.$$

Beweis. Es sei $m := \#\mathcal{M}$. Wir zeigen zunächst $\#S_{n,\mathfrak{m}}/(F^\times)^n = n^m$. Dazu betrachten wir die Gruppe der $\mathcal{M}$-Einheiten

$$U_{\mathcal{M}} := \{f \in F^\times \mid v_{\mathfrak{p}}(f) = 0 \ \forall\, \mathfrak{p} \notin \mathcal{M}\},$$

also die Erzeuger der Hauptdivisoren (f) mit $\operatorname{supp}(f) \subseteq \mathcal{M}$. Offensichtlich gilt $U_{\mathcal{M}} \subseteq S_{n,\mathfrak{m}}$ und die Einbettung $U_{\mathcal{M}} \hookrightarrow S_{n,\mathfrak{m}}$ induziert einen Homomorphismus

$$\theta : U_{\mathcal{M}} \to S_{n,\mathfrak{m}}/(F^\times)^n.$$

Dieser ist surjektiv, denn: Sei $f \in S_{n,\mathfrak{m}}$. Da die Menge $\mathcal{M}$ die Klassengruppe erzeugt, gibt es einen Divisor $\mathfrak{D}$ mit Träger in $\mathcal{M}$, so dass

$$\left[\frac{1}{n}\sum_{\mathfrak{p}\notin\mathcal{M}} v_{\mathfrak{p}}(f)\cdot\mathfrak{p}\right] = [\mathfrak{D}].$$

Dann gilt aber

$$\left[\frac{1}{n}(f)\right] = \left[\frac{1}{n}(f) - \frac{1}{n}\sum_{\mathfrak{p}\notin\mathcal{M}} v_{\mathfrak{p}}(f)\cdot\mathfrak{p}\right] + [\mathfrak{D}] = \left[\frac{1}{n}\sum_{\mathfrak{p}\in\mathcal{M}} v_{\mathfrak{p}}(f)\cdot\mathfrak{p}\right] + [\mathfrak{D}].$$

Also gibt es ein $g \in F^\times$ mit

$$\frac{1}{n}(f) + (g) = \frac{1}{n}\sum_{\mathfrak{p}\in\mathcal{M}} (v_{\mathfrak{p}}(f) + n\, v_{\mathfrak{p}}(\mathfrak{D}))\cdot\mathfrak{p}.$$

Dann ist mit $\operatorname{supp}\left(\frac{1}{n}(f)+(g)\right) \subseteq \mathcal{M}$ auch $\operatorname{supp}(fg^n) \subseteq \mathcal{M}$. Wir haben also ein Element $h = fg^n \in U_{\mathcal{M}}$ gefunden mit $\bar{h} = \bar{f} \in S_{n,\mathfrak{m}}/(F^\times)^n$.

Der Kern von θ ist $(U_{\mathcal{M}})^n$, denn: Sei $f \in U_{\mathcal{M}}$ mit $\bar{f} = 1 \in S_{n,\mathfrak{m}}/(F^\times)^n$. Dann ist $f \in U_{\mathcal{M}} \cap (F^\times)^n = (U_{\mathcal{M}})^n$. Nach Homomorphiesatz gilt dann die Isomorphie $U_{\mathcal{M}}/(U_{\mathcal{M}})^n \cong S_{n,\mathfrak{m}}/(F^\times)^n$. Der Dirichletsche Einheitensatz besagt, dass die Gruppe der $\mathcal{M}$-Einheiten das Produkt aus μ_n und einer freien abelschen Gruppe vom Rang $m-1$ ist. Folglich hat $U_{\mathcal{M}}/(U_{\mathcal{M}})^n$ die Kardinalität n^m (siehe [Jan73, Kor 8.3, S. 173]). Schließlich gilt auch für die Selmergruppe $\#S_{n,\mathfrak{m}}/(F^\times)^n = n^m$.

Als nächstes zeigen wir $\#\mathcal{C}\ell^0_{\mathfrak{m}}[n] = n^{m-1}$ und betrachten hierzu die bekannte exakte Sequenz

$$0 \to \mathcal{P}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}} \xrightarrow{\psi} \mathcal{C}\ell^0_{\mathfrak{m}} \to \mathcal{C}\ell^0_F \to 0.$$

Wir zeigen $\mathcal{C}\ell^0_{\mathfrak{m}}[n] \subseteq \psi(\mathcal{P}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}})$, dann gilt nämlich schon $(\mathcal{P}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}})[n] \cong \mathcal{C}\ell^0_{\mathfrak{m}}[n]$. Hierzu sei $[\mathfrak{D}]_{\mathfrak{m}} \in \mathcal{C}\ell^0_{\mathfrak{m}}[n]$, also insbesondere $n[\mathfrak{D}]_{\mathfrak{m}} = 0$. Bezeichnet nun $[\mathfrak{D}]_F$ die Divisorklasse von $\mathfrak{D}$ in $\mathcal{C}\ell_F$, so gilt für die Tatepaarung $\tau_n([\mathfrak{D}]_F, [\mathfrak{C}]) = f(\mathfrak{C}) = 1$ für alle $\mathfrak{C} \in \mathcal{D}^0_F$ mit $\operatorname{supp}\mathfrak{C} \subseteq \mathcal{M}$, wobei $n\mathfrak{D} = (f) \in \mathcal{P}_{\mathfrak{m}}$. Da $\mathcal{C}\ell^0_F$ aber schon von den Stellen in $\mathcal{M}$ erzeugt wird und die Tatepaarung nicht ausgeartet ist, folgt $[\mathfrak{D}]_F = 0$. Also ist das Bild $[\mathfrak{D}]_F$ von $[\mathfrak{D}]_{\mathfrak{m}}$ in $\mathcal{C}\ell^0_F$ gleich 0 und es gilt $[\mathfrak{D}]_{\mathfrak{m}} \in \psi(\mathcal{P}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}})$.

Nun müssen wir also noch $\#(\mathcal{P}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}})[n] = n^{m-1}$ zeigen und nehmen zunächst an, dass es ein $\mathfrak{p} \in \mathcal{M}$ gibt, dessen Grad teilerfremd zu n ist. Für ein solches $\mathfrak{p}$ gibt es nämlich kein $f \in F_{\mathfrak{p}} = \mathbb{F}_{q^{\deg\mathfrak{p}}}$ mit $f^n \in \mathbb{F}_q$ und $f \notin \mathbb{F}_q$, also ist in diesem Fall $\mathbb{F}_q^\times[n] = F_{\mathfrak{p}}^\times[n]$. Wegen

$$\mathcal{P}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}} \cong (F^{\mathfrak{m}}/F_{\mathfrak{m}})/{\mathbb{F}_q}^\times \cong \left(\prod_{\mathfrak{p}\in\mathcal{M}} (\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})})^\times\right)/{\mathbb{F}_q}^\times$$

interessieren wir uns für die n-Torsion von $\left(\prod_{\mathfrak{p}\in\mathcal{M}}(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})})^\times\right)/{\mathbb{F}_q}^\times$. Dabei ist jeweils $(\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})})^\times \cong F_{\mathfrak{p}}^\times \times (1+\mathfrak{p})/(1+\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})})$ und die Kardinalität von $(1+\mathfrak{p})/(1+\mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{m})})$ eine Potenz von q und somit teilerfremd zu n. Daher ist für die n-Torsion nur der Teil $\left(\prod_{\mathfrak{p}\in\mathcal{M}} F_{\mathfrak{p}}^\times\right)/\mathbb{F}_q^\times$ relevant. Aus der exakten Sequenz

$$1 \to \mathbb{F}_q^\times \to \prod_{\mathfrak{p}\in\mathcal{M}} F_{\mathfrak{p}}^\times \to \left(\prod_{\mathfrak{p}\in\mathcal{M}} F_{\mathfrak{p}}^\times\right)/\mathbb{F}_q^\times \to 1$$

folgt die Exaktheit der Sequenz

$$1 \to \mathbb{F}_q^\times[n^\infty] \to \prod_{\mathfrak{p}\in\mathcal{M}} F_{\mathfrak{p}}^\times[n^\infty] \to \left(\left(\prod_{\mathfrak{p}\in\mathcal{M}} F_{\mathfrak{p}}^\times\right)/\mathbb{F}_q^\times\right)[n^\infty] \to 1,$$

da $G[n^\infty] = \{g \in G \mid \exists\ r \text{ mit } g^{n^r} = 1\}$ für endliche Gruppen G als Lokalisierung dargestellt werden kann und Lokalisierung als Funktor exakt ist.

Für die multiplikative Gruppe eines endlichen Körpers gilt $\mathbb{F}_q^\times[n^\infty] \cong \mathbb{Z}/N\mathbb{Z}$ mit $n \mid N$. Schreiben wir $\mathcal{M} = \{\mathfrak{p}_1, \dots \mathfrak{p}_m\}$, wobei $\mathfrak{p}_1$ eine Stelle mit Grad teilerfremd zu n sei, so ist $\prod_{i=1}^m F_{\mathfrak{p}^i}^\times[n^\infty] \cong \prod_{i=1}^m \mathbb{Z}/N_i\mathbb{Z}$ mit $N \mid N_i$ für $i = 1, \dots, m$. Wegen $F_{\mathfrak{p}_1}^\times[n^\infty] \cong \mathbb{F}_q^\times[n^\infty]$ ist $N_1 = N$. Ein Erzeuger von $\mathbb{Z}/N\mathbb{Z}$ wird daher auf $(1, a_2, \dots, a_m) \in \prod_{i=1}^m \mathbb{Z}/N_i\mathbb{Z}$ mit $\mathrm{ord}_{\mathbb{Z}/N_i\mathbb{Z}}(a_i) = N$ abgebildet, und

$$\begin{aligned}\left(\left(\prod_{\mathfrak{p}\in\mathcal{M}} F_{\mathfrak{p}}^\times\right)/\mathbb{F}_q^\times\right)[n^\infty] &\cong \left(\prod_{\mathfrak{p}\in\mathcal{M}} F_{\mathfrak{p}}^\times[n^\infty]\right)/(\mathbb{F}_q^\times[n^\infty]) \\ &\cong \left(\prod_{i=1}^m \mathbb{Z}/N_i\mathbb{Z}\right)/\langle(1, a_2, \dots, a_m)\rangle_{\mathbb{Z}/N\mathbb{Z}} \\ &\cong 0 \times \prod_{i=2}^m \mathbb{Z}/N_i\mathbb{Z}.\end{aligned}$$

Schließlich erhalten wir

$$(\mathcal{P}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}})[n] \cong \left(\left(\left(\prod_{\mathfrak{p}\in\mathcal{M}} F_{\mathfrak{p}}^\times\right)/\mathbb{F}_q^\times\right)[n^\infty]\right)[n] \cong \prod_{i=2}^m (\mathbb{Z}/n\mathbb{Z})$$

und daraus folgt sofort $\#\mathcal{C}\ell_{\mathfrak{m}}^0[n] = \#(\mathcal{P}^{\mathfrak{m}}/\mathcal{P}_{\mathfrak{m}})[n] = n^{m-1}$.

Im allgemeinen Fall wissen wir nicht, dass es in $\mathcal{M}$ stets eine Stelle vom Grad teilerfremd zu n gibt. Die Voraussetzung, dass $\mathcal{M}$ die gewöhnliche Klassengruppe erzeugen muss, liefert jedoch für jede Primzahl r: Es gibt eine Stelle $p \in \mathcal{M}$ mit $r \nmid \deg \mathfrak{p}$ (denn sonst gäbe es in der Klassengruppe nur Divisoren, deren Grad ein Vielfaches von r ist), und wegen r prim gilt $\mathrm{ggT}(\deg \mathfrak{p}, r) = 1$. Also können wir für jede Primzahlpotenz r^ℓ, die n teilt, die obige Argumentation durchführen und erhalten auch hier

$$\#\mathcal{C}\ell_{\mathfrak{m}}^0[n] = \prod_{r^\ell \mid n} (r^\ell)^{m-1} = n^{m-1}.$$

Schließlich liefert die einfache Rechnung

$$\begin{aligned}\#\mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}} &= \#\mathbb{Z}/n\mathbb{Z} \times \mathcal{C}\ell_{\mathfrak{m}}^0/n\mathcal{C}\ell_{\mathfrak{m}}^0 = n \cdot \#\mathcal{C}\ell_{\mathfrak{m}}^0[n] \\ &= n \cdot n^{m-1} = n^m = \#S_{n,\mathfrak{m}}/(F^\times)^n\end{aligned}$$

die Behauptung. □

3.2 Kummer- und Tatepaarung

Lemma 3.4. *Es sei ein $f \in F^\times$ so gewählt, dass die Kummererweiterung $F(\sqrt[n]{f})|F$ außerhalb der Menge $\mathcal{M}$ unverzweigt ist. Dann besitzt jede Klasse*

aus $\mathcal{C}\ell_{\mathfrak{m}}$ *einen Repräsentanten* $\mathfrak{D} \in \mathcal{D}^{\mathfrak{m}}$ *mit*

$$f(\mathfrak{D})^{\frac{q-1}{n}} = \frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}},$$

wobei $\sigma_{\mathfrak{D}} := (\mathfrak{D}, F(\sqrt[n]{f})|F)$ *der Artinautomorphismus zu* $\mathfrak{D}$ *sei.*

Beweis. Nach dem Approximationssatz 1.8 können wir den Repräsentanten $\mathfrak{D}$ so wählen, dass $\operatorname{supp}\mathfrak{D} \cap \operatorname{supp}(f) = \emptyset$ gilt. Dann ist der Ausdruck $f(\mathfrak{D})$ wohldefiniert. Weiter ist auch der Automorphismus $\sigma_{\mathfrak{D}}$ wohldefiniert, da $F(\sqrt[n]{f})|F$ außerhalb $\mathcal{M}$ unverzweigt ist. Die Wohldefiniertheit von $\frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}}$ ist für $\sigma_{\mathfrak{D}} \in \operatorname{Gal}(F(\sqrt[n]{f})|F)$ von der Kummerpaarung her bekannt.

Sei $\mathfrak{p} \in \operatorname{supp}\mathfrak{D}$ und $\sigma_{\mathfrak{p}} = (\mathfrak{p}, F(\sqrt[n]{f})|F)$ der zugehörige Artinautomorphismus. Dabei sei der Repräsentant $\mathfrak{D}$ nun zusätzlich so gewählt, dass $\sqrt[n]{f} \in \mathcal{O}_{\mathfrak{P}}$ für alle Stellen $\mathfrak{P}$ von $F(\sqrt[n]{f})$ über $\mathfrak{p}$ und für alle $\mathfrak{p} \in \operatorname{supp}\mathfrak{D}$. Dies ist nach dem Approximationssatz 1.8 möglich, da $\sqrt[n]{f}$ nur endlich viele Pole $\mathfrak{P}$ hat (siehe [Sti93, Kor. I.3.4, S. 14]). Dann gilt $\sigma_{\mathfrak{p}}(\sqrt[n]{f}) \equiv (\sqrt[n]{f})^{\mathfrak{N}(\mathfrak{p})} \bmod \mathfrak{P}$ für $\mathfrak{P}|\mathfrak{p}$, und damit

$$\frac{\sigma_{\mathfrak{p}}(\sqrt[n]{f})}{\sqrt[n]{f}} \equiv \frac{(\sqrt[n]{f})^{\mathfrak{N}(\mathfrak{p})}}{\sqrt[n]{f}} = f^{\frac{\mathfrak{N}(\mathfrak{p})-1}{n}} = f^{(1+q+q^2+\ldots+\frac{\mathfrak{N}(\mathfrak{p})}{q})\frac{q-1}{n}} \bmod \mathfrak{P}.$$

Da $\operatorname{Gal}(F_{\mathfrak{p}}|\mathbb{F}_q)$ vom Frobeniusautomorphismus φ_q erzeugt wird, ist

$$\mathrm{N}_{F_{\mathfrak{p}}|\mathbb{F}_q}(x) = \prod_{\sigma \in \operatorname{Gal}(F_{\mathfrak{p}}|\mathbb{F}_q)} \sigma(x) = \prod_{i=0}^{[F_{\mathfrak{p}}:\mathbb{F}_q]-1} \varphi_q^i(x) = x^{1+q+q^2+\ldots+q^{\deg(\mathfrak{p})-1}} \quad \forall\, x \in F_{\mathfrak{p}}.$$

Dann gilt aber wegen $\mathfrak{N}(\mathfrak{p}) = q^{\deg(\mathfrak{p})}$

$$f^{(1+q+q^2+\ldots+\frac{\mathfrak{N}(\mathfrak{p})}{q})\frac{q-1}{n}} = \mathrm{N}_{F_{\mathfrak{p}}|\mathbb{F}_q}(f(\mathfrak{p}))^{\frac{q-1}{n}}.$$

Wir haben gezeigt:

$$\frac{\sigma_{\mathfrak{p}}(\sqrt[n]{f})}{\sqrt[n]{f}} \equiv \mathrm{N}_{F_{\mathfrak{p}}|\mathbb{F}_q}(f(\mathfrak{p}))^{\frac{q-1}{n}} \bmod \mathfrak{P}.$$

Beide Seiten dieser Gleichung sind in $\mathbb{F}_q$, also folgt mit $\mathbb{F}_q \cap \mathfrak{P} = \{0\}$ (wegen $\mathbb{F}_q \cap \mathfrak{p} = \{0\}$) sogar die Gleichheit

$$\frac{\sigma_{\mathfrak{p}}(\sqrt[n]{f})}{\sqrt[n]{f}} = \mathrm{N}_{F_{\mathfrak{p}}|\mathbb{F}_q}(f(\mathfrak{p}))^{\frac{q-1}{n}}.$$

Wegen der Linearität der Artinabbildung und der Linearität der Kummerpaarung im zweiten Argument gilt nun

$$\frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}} = \prod_{\mathfrak{p} \in \mathcal{S}_F} \left(\frac{\sigma_{\mathfrak{p}}(\sqrt[n]{f})}{\sqrt[n]{f}}\right)^{v_{\mathfrak{p}}(\mathfrak{D})} = \left(\prod_{\mathfrak{p} \in \mathcal{S}_F} \mathrm{N}_{F_{\mathfrak{p}}|\mathbb{F}_q}(f(\mathfrak{p}))^{v_{\mathfrak{p}}(\mathfrak{D})}\right)^{\frac{q-1}{n}} = f(\mathfrak{D})^{\frac{q-1}{n}}.$$

Eine ähnliche Beweistechnik wurde von Helmut Hasse schon 1935 verwendet (siehe [Has35, S. 40]). □

Um die Bedeutung dieses Lemmas für Kummer- und Tatepaarung deutlich zu machen, erinnern wir kurz an ihre Definitionen. Die Kummerpaarung ist definiert durch

$$\begin{aligned} \kappa_n : \Delta/(F^\times)^n \times \mathrm{Gal}(F(\sqrt[n]{\Delta})|F) &\to \mu_n \\ (\bar{f}, \sigma) &\mapsto \frac{\sigma(\sqrt[n]{f})}{\sqrt[n]{f}}, \end{aligned}$$

wobei Δ eine Gruppe mit $(F^\times)^n \subseteq \Delta \subseteq F^\times$ ist. Die reduzierte Tatepaarung wird definiert durch

$$\begin{aligned} \tau_n^{\mathrm{red}} : \mathcal{C}\ell_F^0[n] \times \mathcal{C}\ell_F^0/n\mathcal{C}\ell_F^0 &\to \mu_n \\ ([\mathfrak{C}], \overline{[\mathfrak{D}]}) &\mapsto f(\mathfrak{D})^{\frac{q-1}{n}}, \end{aligned}$$

wobei $f \in F^\times$ so gewählt wird, dass $n\mathfrak{C} = (f)$. Beide Paarungen sind nicht ausgeartet.

Nun sei $([\mathfrak{C}], \overline{[\mathfrak{D}]}) \in \mathcal{C}\ell_F^0[n] \times \mathcal{C}\ell_F^0/n\mathcal{C}\ell_F^0$ und $\sigma_{\mathfrak{D}}$ der Artinautomorphismus $(\mathfrak{D}, F(\sqrt[n]{f})|F)$ von $\mathfrak{D}$ und $n\mathfrak{C} = (f)$. Dann gilt laut Lemma 3.4 die Gleichung

$$\tau_n^{\mathrm{red}}([\mathfrak{C}], \overline{[\mathfrak{D}]}) = f(\mathfrak{D})^{\frac{q-1}{n}} = \frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}} = \kappa_n(\bar{f}, \sigma_{\mathfrak{D}}).$$

Dies ist allerdings nur ein Spezialfall des Lemmas, das eine allgemeinere Aussage beweist.

Bemerkung 3.5. Man beachte hierbei, dass f nur bis auf eine Konstante bestimmt ist, und dass $F(\sqrt[n]{f}) \neq F(\sqrt[n]{cf})$ für $c \in {\mathbb{F}_q}^\times \setminus ({\mathbb{F}_q}^\times)^n$. Wie soeben gezeigt spielt die Wahl der Erweiterung jedoch für die Kombination der beiden Paarungen keine Rolle, denn der Satz gilt natürlich für jede gültige Wahl von f. Man kann dies auch elementar nachrechnen, indem man $\frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}} = \frac{\sigma_{\mathfrak{D}}(\sqrt[n]{cf})}{\sqrt[n]{cf}}$ für $c \in {\mathbb{F}_q}^\times$ überprüft. Hier geht dann die Tatsache $\deg(\mathfrak{C}) = 0$ (wie im Definitionsbereich der Tatepaarung gefordert) ein, daraus folgt nämlich $\sigma_{\mathfrak{D}}(\sqrt[n]{c}) = \sqrt[n]{c}$.

Das folgende kommutative Diagramm illustriert noch einmal den Zusammenhang zwischen den beiden Paarungen.

$$\begin{array}{rcccc} \tau_n^{\mathrm{red}} : & \mathcal{C}\ell_F^0[n] \times \mathcal{C}\ell_F^0/n\mathcal{C}\ell_F^0 & \longrightarrow & \mu_n & F(\sqrt[n]{f}) \\ & ([\mathfrak{C}], \overline{[\mathfrak{D}]}) \mathrel{\widehat{=}} (f, \mathfrak{D}) & \longmapsto & f(\mathfrak{D})^{\frac{q-1}{n}} & | \\ & \downarrow{\scriptstyle (\cdot, F(\sqrt[n]{f})|F)} & & \| & F \\ \kappa_n : & (\bar{f}, \sigma_{\mathfrak{D}}) & \longmapsto & \frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}} & | \\ & \langle f \rangle/(F^\times)^n \times \mathrm{Gal}(F(\sqrt[n]{f})|F) & \longrightarrow & \mu_n & \mathbb{F}_q \end{array}$$

3.3 Eine neue Paarung

Endlich sind wir in der Lage, die neue verallgemeinerte Paarung zu definieren.

Definition 3.6. Es sei $\pi_{n,\mathfrak{m}}$ die Abbildung

$$\begin{aligned} \pi_{n,\mathfrak{m}} : S_{n,\mathfrak{m}}/(F^\times)^n \times \mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}} &\to \mu_n \\ (\bar{f}, \overline{[\mathfrak{D}]}) &\mapsto f(\mathfrak{D})^{\frac{q-1}{n}}. \end{aligned}$$

Dabei sei der Repräsentant $\mathfrak{D}$ nach Approximationssatz 1.8 so gewählt, dass $f(\mathfrak{D})$ wohldefiniert ist.

Bemerkung 3.7. Nach Lemma 3.4 ist dieselbe Paarung auch definiert durch

$$\pi_{n,\mathfrak{m}}(\bar{f}, \overline{[\mathfrak{D}]}) = \frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}}$$

mit $\sigma_{\mathfrak{D}} = (\mathfrak{D}, F(\sqrt[n]{f})|F)$, für einen wie im Beweis von Lemma 3.4 korrekt gewählten Repräsentanten $\mathfrak{D}$. Diese Darstellung ist im Umgang mit der Paarung oft sehr nützlich, wie schon der Beweis des folgenden Satzes zeigt.

Satz 3.8. *Die Abbildung $\pi_{n,\mathfrak{m}}$ ist eine wohldefinierte, nicht ausgeartete Paarung.*

Beweis. WOHLDEFINIERTHEIT. Für $f \in S_{n,\mathfrak{m}}$ ist die Erweiterung $F(\sqrt[n]{f})|F$ unverzweigt für alle Stellen außerhalb von $\mathcal{M}$. Im Beweis von Lemma 3.4 haben wir gesehen, dass die Ausdrücke $f(\mathfrak{D})^{\frac{q-1}{n}} = \frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}}$ wohldefiniert sind, und von der Kummerpaarung her wissen wir, dass sie Elemente von μ_n sind.

Für $f = g^n \in (F^\times)^n$ gilt offensichtlich $f(\mathfrak{D})^{\frac{q-1}{n}} = g(\mathfrak{D})^{q-1} = 1$ in $\mathbb{F}_q$ für alle zulässigen $\mathfrak{D}$, also ist die Paarung im linken Argument wohldefiniert.

Für die Wohldefiniertheit im rechten Argument sei $f \in S_{n,\mathfrak{m}}/(F^\times)^n$ beliebig und $\mathfrak{D} = (g) \in \mathcal{P}_{\mathfrak{m}}$. Für alle Stellen $\mathfrak{p} \in \mathcal{M}$ gilt dann $g \equiv 1 \bmod \mathfrak{p}$, d.h. $g(\mathfrak{p}) = 1$ im Restklassenkörper $F_{\mathfrak{p}}$ und deshalb auch $\mathrm{N}_{F_{\mathfrak{p}}|\mathbb{F}_q}(g(\mathfrak{p})) = 1$. Für alle Stellen $\mathfrak{p} \notin \mathcal{M}$ gilt andererseits $n \mid v_{\mathfrak{p}}(f)$ und deshalb können wir (f) schreiben als

$$(f) = \sum_{\mathfrak{p} \in \mathcal{S}_F} v_{\mathfrak{p}}(f) \cdot \mathfrak{p} = n\mathfrak{C} + \sum_{\mathfrak{p} \in \mathcal{M}} v_{\mathfrak{p}}(f) \cdot \mathfrak{p}$$

für einen Divisor $\mathfrak{C}$ mit Träger außerhalb von $\mathcal{M}$. Mittels Weil-Reziprozität 1.32 erhalten wir schließlich

$$\begin{aligned} f(\mathfrak{D}) &= f((g)) = g((f)) \\ &= g\left(n\mathfrak{C} + \sum_{\mathfrak{p} \in \mathcal{M}} v_{\mathfrak{p}}(f) \cdot \mathfrak{p}\right) \\ &= g(\mathfrak{C})^n \cdot \prod_{\mathfrak{p} \in \mathcal{M}} \mathrm{N}_{F_{\mathfrak{p}}|\mathbb{F}_q}(g(\mathfrak{p}))^{v_{\mathfrak{p}}(f)} = g(\mathfrak{C})^n \cdot 1 \end{aligned}$$

und daraus folgt $f(\mathfrak{D})^{\frac{q-1}{n}} = g(\mathfrak{C})^{q-1} = 1 \in \mathbb{F}_q$. Somit ist die Paarung wohldefiniert für Elemente $[\mathfrak{D}]$ aus $\mathcal{C}\ell_{\mathfrak{m}}$. Offensichtlich gilt auch $f(\mathfrak{D})^{\frac{q-1}{n}} = 1$ für alle $[\mathfrak{D}] \in n\mathcal{C}\ell_{\mathfrak{m}}$ und somit ist die Paarung wohldefiniert im gesamten rechten Argument $\mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}}$.

Bililnearität. Die Bilinearität folgt direkt aus der Bilinearität des Ausdrucks $f(\mathfrak{D})$ in f und $\mathfrak{D}$.

Nichtausartung. Diese Tatsache folgt im Wesentlichen aus der Nichtausartung der Kummerpaarung, der Surjektivität der Artinabbildung und Lemma 3.3. Um letzteres verwenden zu können, nehmen wir zunächst wieder an, dass $\mathcal{M}$ groß genug ist um die gesamte (gewöhnliche) Klassengruppe zu erzeugen. Aus Lemma 3.10 folgt die Nichtausartung der Paarung dann sofort auch für jedes $\mathfrak{m}$ mit echt kleinerem Träger.

Bekannt ist die nicht ausgeartete Kummerpaarung

$$\begin{aligned} \kappa_n : \Delta/(F^\times)^n \times G(F(\sqrt[n]{\Delta})|F) &\to \mu_n \\ (\bar{f}, \sigma) &\mapsto \frac{\sigma(\sqrt[n]{f})}{\sqrt[n]{f}} \end{aligned}$$

für Untergruppen Δ von $F^\times$ die $(F^\times)^n$ enthalten. Die Selmergruppe $S_{n,\mathfrak{m}}$ ist eine solche Untergruppe. Gehen wir nun mit Hilfe der Artinabbildung einen „Umweg“ über $\sigma_{\mathfrak{D}} := (\mathfrak{D}, F(\sqrt[n]{S_{n,\mathfrak{m}}})|F)$, so beschreibt

$$\begin{aligned} \pi_{n,\mathfrak{m}} : S_{n,\mathfrak{m}}/(F^\times)^n \times \mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}} &\to \mu_n \\ (\bar{f}, \overline{[\mathfrak{D}]}) &\mapsto \frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}} \end{aligned}$$

dieselbe Paarung (und offensichtlich hat $\sigma_{\mathfrak{D}}(\sqrt[n]{f})$ denselben Wert für $\sigma_{\mathfrak{D}} = (\mathfrak{D}, F(\sqrt[n]{S_{n,\mathfrak{m}}})|F)$ und $\sigma_{\mathfrak{D}} = (\mathfrak{D}, F(\sqrt[n]{f})|F)$). Wegen der Surjektivität der Artinabbildung $(\cdot, F(\sqrt[n]{S_{n,\mathfrak{m}}})|F) : \mathcal{D}^{\mathfrak{m}} \to \mathrm{Gal}(F(\sqrt[n]{S_{n,\mathfrak{m}}})|F)$ nach Tschebotarev 1.45 ist die Paarung $\pi_{n,\mathfrak{m}}$ im linken Argument nicht ausgeartet. Ist nämlich $\frac{\sigma_{\mathfrak{D}}(\sqrt[n]{f})}{\sqrt[n]{f}} = 1$ für alle $\mathfrak{D} \in \mathcal{D}^{\mathfrak{m}}$, so gilt auch $\frac{\sigma(\sqrt[n]{f})}{\sqrt[n]{f}} = 1$ für alle $\sigma \in \mathrm{Gal}(F(\sqrt[n]{S_{n,\mathfrak{m}}})|F)$ und daraus folgt $\bar{f} = 1$. Deshalb ist der zur Paarung gehörende Homomorphismus $S_{n,\mathfrak{m}}/(F^\times)^n \to \mathrm{Hom}(\mathcal{D}^{\mathfrak{m}}, \mu_n)$ injektiv. Weiter oben haben wir gesehen, dass sich Elemente aus $\mathcal{P}_{\mathfrak{m}}$ und aus $n\mathcal{C}\ell_{\mathfrak{m}}$ mit jedem $\bar{f}$ trivial paaren, also ist auch $S_{n,\mathfrak{m}}/(F^\times)^n \to \mathrm{Hom}(\mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}}, \mu_n)$ injektiv.

Hiermit folgt die Nichtausartung im rechten Argument nun direkt aus Lemma 1.21 und Lemma 3.3. Damit ist die Paarung $\pi_{n,\mathfrak{m}}$ nicht ausgeartet für $\mathcal{M}$ groß genug. □

Bemerkung 3.9. Es ist nicht zu vergessen, dass in diesen Beweis an entscheidender Stelle der Tschebotarevsche Dichtigkeitssatz eingeht. Er ist ein hochgradig nichttriviales Resultat. Außerdem wird die Weil-Reziprozität benötigt. Da kein identisches Resultat für Zahlkörper bekannt ist, kann dieser

gesamte Ansatz nicht unmittelbar auf Zahlkörper übertragen werden, obwohl viele weitere wichtige Argumente (zum Beispiel Dichtigkeitsaussagen wie der Satz vom Tschebotarev) im Zahlkörper-Fall ganz analog gelten.

Lemma 3.10. *Ist $\pi_{n,\mathfrak{m}}$ nicht ausgeartet, so auch $\pi_{n,\mathfrak{m}'}$ für jedes $\mathfrak{m}' \leq \mathfrak{m}$ mit* $\operatorname{supp}\mathfrak{m}' \subsetneq \operatorname{supp}\mathfrak{m}$.

Beweis. Es sei $\mathcal{M}'$ der Träger von $\mathfrak{m}'$. Dann gilt $\mathcal{M}' \subsetneq \mathcal{M}$ und $S_{n,\mathfrak{m}'} \subsetneq S_{n,\mathfrak{m}}$, wir haben also einen kanonischen Monomorphismus

$$\Phi : S_{n,\mathfrak{m}'}/(F^\times)^n \to S_{n,\mathfrak{m}}/(F^\times)^n.$$

Außerdem sei Ψ der kanonische Epimorphismus

$$\Psi : \mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}} \to \mathcal{C}\ell_{\mathfrak{m}'}/n\mathcal{C}\ell_{\mathfrak{m}'}.$$

Offensichtlich gilt eine Adjungiertheitsbedingung der Form

$$\pi_{n,\mathfrak{m}}(\Phi(\bar{f}), \overline{[\mathfrak{D}]}) = f(\mathfrak{D})^{\frac{q-1}{n}} = \pi_{n,\mathfrak{m}'}(\bar{f}, \Psi(\overline{[\mathfrak{D}]}))$$

für alle $\bar{f} \in S_{n,\mathfrak{m}'}/(F^\times)^n$ und $\overline{[\mathfrak{D}]} \in \mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}}$, und wir erhalten das kommutative Diagramm

$$\begin{array}{ccccc} S_{n,\mathfrak{m}'}/(F^\times)^n & \times & \mathcal{C}\ell_{\mathfrak{m}'}/n\mathcal{C}\ell_{\mathfrak{m}'} & \longrightarrow & \mu_n \\ \Phi\downarrow & & \uparrow\Psi & & \| \\ S_{n,\mathfrak{m}}/(F^\times)^n & \times & \mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}} & \longrightarrow & \mu_n \end{array}$$

Nun zeigen wir, dass $\operatorname{im}(\Phi)$ das orthogonale Komplement

$$(\ker\Psi)^\perp = \{\bar{f} \in S_{n,\mathfrak{m}}/(F^\times)^n \mid \pi_{n,\mathfrak{m}}(\bar{f}, \overline{[\mathfrak{D}]}) = 1 \quad \forall\, \overline{[\mathfrak{D}]} \in \ker\Psi\}$$

unter $\pi_{n,\mathfrak{m}}$ zu $\ker\Psi$ ist. Die Inklusion $\operatorname{im}(\Phi) \subseteq (\ker\Psi)^\perp$ sieht man leicht, denn für $\overline{[\mathfrak{D}]} \in \ker\Psi$ und $\bar{f} \in S_{n,\mathfrak{m}'}/(F^\times)^n$ gilt

$$\pi_{n,\mathfrak{m}}(\Phi(\bar{f}), \overline{[\mathfrak{D}]}) = \pi_{n,\mathfrak{m}'}(\bar{f}, \Psi(\overline{[\mathfrak{D}]})) = \pi_{n,\mathfrak{m}'}(\bar{f}, 0) = 1.$$

Für die umgekehrte Inklusion sei $\bar{f} \in S_{n,\mathfrak{m}}/(F^\times)^n$ und $\pi_{n,\mathfrak{m}}(\bar{f}, \overline{[\mathfrak{D}]}) = 1$ für alle $\overline{[\mathfrak{D}]} \in \ker\Psi$. Zu zeigen ist, dass schon $\bar{f} \in S_{n,\mathfrak{m}'}/(F^\times)^n$ gilt. Wir nehmen also an es gäbe ein $\mathfrak{q} \in \mathcal{M} \setminus \mathcal{M}'$ mit $n \nmid v_\mathfrak{q}(f)$. Der Approximationssatz 1.8 liefert ein $g \in F^\times$ mit $v_\mathfrak{p}(g-1) \geq v_\mathfrak{p}(\mathfrak{m})$ für alle $\mathfrak{p} \in \mathcal{M} \setminus \{\mathfrak{q}\}$ sowie $v_\mathfrak{q}(g-1) = 0$. Dann gilt $(g) \in \mathcal{P}_{\mathfrak{m}'}$, also $\overline{[(g)]} = \overline{(g) + \mathcal{P}_\mathfrak{m}} \in \ker\Psi$, aber mit Weil-Reziprozität erhalten wir

$$\pi_{n,\mathfrak{m}}(\bar{f}, \overline{[(g)]}) = f((g))^{\frac{q-1}{n}} = g((f))^{\frac{q-1}{n}} = \left(\prod_{\mathfrak{p}\in\mathcal{S}_F} \mathrm{N}_{F_\mathfrak{p}|\mathbb{F}_q}(g(\mathfrak{p}))^{v_\mathfrak{p}(f)}\right)^{\frac{q-1}{n}} \neq 1,$$

denn wegen $g \not\equiv 1 \bmod \mathfrak{q}$ ist $g(\mathfrak{q}) \neq 1 \in F_\mathfrak{q}$ und $n \nmid v_\mathfrak{q}(f)$. Widerspruch. Es gilt also $(\ker \Psi)^\perp = \operatorname{im} \Phi$.

Mit Hilfe der Konstruktion aus Satz 1.22 sieht man, dass die nicht ausgeartete Paarung $\pi_{n,\mathfrak{m}}$ die nicht ausgeartete Paarung

$$\operatorname{im} \Phi \times (\mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m})/\ker \Psi \to \mu_n$$

induziert. Wegen $\operatorname{im} \Phi \cong S_{n,\mathfrak{m}'}/(F^\times)^n$ und $(\mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m})/\ker \Psi \cong \mathcal{C}\ell_{\mathfrak{m}'}/n\mathcal{C}\ell_{\mathfrak{m}'}$ und der Adjungiertheitsbedingung ist das aber gerade die Paarung $\pi_{n,\mathfrak{m}'}$. □

Das Lemma 1.20 liefert an dieser Stelle auch die Isomorphien

- $S_{n,\mathfrak{m}}/(F^\times)^n \cong \operatorname{Hom}(\mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m}, \mu_n)$,
- $\mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m} \cong \operatorname{Hom}(S_{n,\mathfrak{m}}/(F^\times)^n, \mu_n)$ und
- $S_{n,\mathfrak{m}}/(F^\times)^n \cong \mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m}$.

Nun haben wir also für Körper $F|\mathbb{F}_q$ und Zahlen n, die die Kummer-Voraussetzungen erfüllen, eine nicht ausgeartete Paarung

$$S_{n,\mathfrak{m}}/(F^\times)^n \times \mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m} \to \mu_n.$$

Im folgenden Kapitel werden wir sehen, wie sie sich für den Beweis des Existenzsatzes der Klassenkörpertheorie verwenden lässt.

Kapitel 4

Beweis des Existenzsatzes

Zum Beweis des Existenzsatzes betrachten wir separat die Kummererweiterungen vom Grad n mit $\mu_n \subseteq F$, die Erweiterungen vom Grad n mit $\mu_n \nsubseteq F$, in beiden Fällen n teilerfremd zur Charakteristik p von F, und die Artin-Schreier-Witt-Erweiterungen vom Grad p^α. Dabei führen wir nur für die ersten beiden Fälle alle Details aus. Im ersten Fall argumentieren wir hauptsächlich mit der Paarung $\pi_{n,\mathfrak{m}}$ aus Kapitel 3. Der zweite Fall baut darauf auf und verwendet zusätzlich Argumente aus der Galoistheorie. Zu den Artin-Schreier-Witt-Erweiterungen machen wir lediglich einige Bemerkungen, da eine ebenso ausführliche Bearbeitung den Rahmen dieser Arbeit gesprengt hätte. Dieser Fall ist jedoch mit ähnlichen Methoden zu lösen wie der Kummer-Fall. Am Ende bauen wir alle drei Fälle zusammen und erhalten Klassenkörper von beliebigem Grad.

Voraussetzungen und Notation 4.1. *Es sei F ein globaler Funktionenkörper in einer Variablen mit dem exakten Konstantenkörper $\mathbb{F}_q$. Weiter bezeichne $\mathfrak{m}$ stets einen effektiven Divisor von F mit Träger $\mathcal{M}$.*

4.1 Kummererweiterungen mit Einheitswurzeln im Grundkörper

Zuerst beweisen wir den Existenzsatz für Kummererweiterungen von F. Hierbei spielt die nicht ausgeartete Paarung $\pi_{n,\mathfrak{m}}$, die wir in Kapitel 3 definiert haben, eine zentrale Rolle. Unter der folgenden Annahme können wir sie verwenden.

Voraussetzungen und Notation 4.2. *Zu $F|\mathbb{F}_q$ sei eine natürliche Zahl n mit $\mathrm{ggT}(n,q) = 1$ und $\mu_n \subseteq F$ fest gewählt.*

Wir betrachten Klassenkörper F_H zu Untergruppen H von Strahlklassengruppen $\mathcal{C}\ell_\mathfrak{m}$ vom Index n. Wegen $n = \#\mathcal{C}\ell_\mathfrak{m}/H = \#\operatorname{Gal}(F_H|F) = [F_H : F]$ ist dann der Grad der Erweiterung $F_H|F$ teilerfremd zur Charakteristik von F und somit handelt es sich um eine Kummererweiterung.

Umgekehrt liefert die Kummertheorie unter der Voraussetzung 4.2, dass alle Erweiterungen von F vom Grad n die Form $F(\sqrt[n]{\Delta})|F$ für eine geeignete Gruppe $\Delta \subseteq F^\times$ mit $(F^\times)^n \subseteq \Delta$ haben. Für solche Erweiterungen zeigen wir die Existenz eines Moduls $\mathfrak{m}$, so dass $\mathcal{P}_\mathfrak{m}$ im Kern des zugehörigen Artinsymbols enthalten ist.

Dabei werden wir feststellen, dass die Führer solcher Erweiterungen immer Koeffizienten 1 haben, wie schon in Kapitel 2.5 bemerkt. Das liegt daran, dass Kummererweiterungen generell zahm verzweigt sind. Wegen der Eigenschaft $\mathrm{ggT}(n, q) = 1$ kann keine wilde Verzweigung auftreten. Für den Beweis der Existenz von Klassenkörpern verwenden wir trotzdem allgemeine Erklärungsmoduln, die Argumentation wird dadurch nicht komplizierter.

Satz 4.3 (Existenzsatz für Kummererweiterungen)**.** *Es sei ein globaler Funktionenkörper $F|\mathbb{F}_q$ und eine natürliche Zahl n mit $\mu_n \subseteq F$ gegeben. Zu jedem Modul $\mathfrak{m}$ und jeder Untergruppe H von $\mathcal{C}\ell_\mathfrak{m}$ vom Index n existiert der Klassenkörper. Umgekehrt existiert zu jeder abelschen Erweiterung $E|F$ vom Grad n ein Erklärungsmodul $\mathfrak{m}$ und eine Untergruppe H von $\mathcal{C}\ell_\mathfrak{m}$ so dass E der Klassenkörper zu H ist.*

Der Beweis des Satzes erfolgt in zwei Schritten. Wir benutzen erst die Paarung $\pi_{n,\mathfrak{m}}$, um die Gruppe H in einer Konstruktion analog zu Satz 1.22 bijektiv auf eine Untergruppe Δ_H von $S_{n,\mathfrak{m}}$ mit $(F^\times)^n \subseteq \Delta_H$ abzubilden. Im zweiten Schritt liefert die aus der Kummertheorie bekannte Bijektion eine Körpererweiterung $F_H = F(\sqrt[n]{\Delta_H})$. Mit Hilfe der Paarung $\pi_{n,\mathfrak{m}}$ und der Kummerpaarung überprüft man leicht die Struktur der Galoisgruppe. Die umgekehrte Richtung lässt sich auf ähnliche Weise einsehen.

Bemerkung 4.4. Bezüglich der Notation sei noch bemerkt, dass ganz allgemein für zwei abelsche Gruppen A und B mit $B \subseteq A$ die Untergruppen U von A mit $B \subseteq U$ bijektiv den Untergruppen $\bar{U}$ der Faktorgruppe A/B entsprechen, es ist nämlich $\bar{U} = U/B$ (siehe zum Beispiel [Poh08, S. 76]). Dies verwenden wir hier und im Folgenden, um stillschweigend die Untergruppen Δ von $S_{n,\mathfrak{m}}$ mit $(F^\times)^n \subseteq \Delta$ und die Untergruppen $\bar{\Delta} := \Delta/(F^\times)^n$ von $S_{n,\mathfrak{m}}/(F^\times)^n$ zu identifizieren. Wenn es wichtig ist werden wir darauf hinweisen, ob Δ als Untergruppe von $S_{n,\mathfrak{m}}$ oder von $S_{n,\mathfrak{m}}/(F^\times)^n$ aufzufassen ist.

Nach dem 2. Isomorphiesatz gilt $(S_{n,\mathfrak{m}}/(F^\times)^n)/\bar{\Delta} = \frac{S_{n,\mathfrak{m}}/(F^\times)^n}{\Delta/(F^\times)^n} \cong S_{n,\mathfrak{m}}/\Delta$, also ist diese Identifizierung auch mit der Bildung von Faktorgruppen kompatibel.

Ebenso verfahren wir auch mit den Untergruppen H von $\mathcal{C}\ell_\mathfrak{m}$ mit $n\mathcal{C}\ell_\mathfrak{m} \subseteq H$ und den Untergruppen $\bar{H} := H/n\mathcal{C}\ell_\mathfrak{m}$ von $\mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m}$. Auch hier gilt, dass $(\mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m})/\bar{H} \cong \mathcal{C}\ell_\mathfrak{m}/H$.

Wichtig ist auch noch, dass für Untergruppen H vom Index n in $\mathcal{C}\ell_\mathfrak{m}$ automatisch $n\mathcal{C}\ell_\mathfrak{m} \subseteq H$ gilt. Die Untergruppen H vom Exponenten n sind sogar genau diejenigen Untergruppen, für die $n\mathcal{C}\ell_\mathfrak{m} \subseteq H$ gilt.

Beweis von Satz 4.3. Existenz des Klassenkörpers. Für Teilmengen $\Delta \subseteq S_{n,\mathfrak{m}}/(F^\times)^n$ und $H \subseteq \mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m}$ definieren wir die Abbildungen

$$\begin{aligned} \Delta &\mapsto H_\Delta := \{\overline{[\mathfrak{D}]} \in \mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m} \mid \pi_{n,\mathfrak{m}}(\bar{f}, \overline{[\mathfrak{D}]}) = 1 \quad \forall\ \bar{f} \in \Delta\} \\ H &\mapsto \Delta_H := \{\bar{f} \in S_{n,\mathfrak{m}}/(F^\times)^n \mid \pi_{n,\mathfrak{m}}(\bar{f}, \overline{[\mathfrak{D}]}) = 1 \quad \forall\ \overline{[\mathfrak{D}]} \in H\}. \end{aligned}$$

Nach Satz 1.22 sind sie zueinander inverse Bijektionen zwischen der Menge der Untergruppen Δ von $S_{n,\mathfrak{m}}/(F^\times)^n$ und der Menge der Untergruppen H von $\mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m}$, da $\pi_{n,\mathfrak{m}}$ nicht ausgeartet ist. Es werden nach Satz 1.22 zwei nicht ausgeartete Paarungen

$$\Delta \times (\mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m})/H_\Delta \to \mu_n \quad \text{und} \quad (S_{n,\mathfrak{m}}/(F^\times)^n)/\Delta_H \times H \to \mu_n$$

induziert. Mit Lemma 1.20 (und Bemerkung 4.4) folgt aus der ersten Paarung die Isomorphie

$$\begin{aligned} \mathcal{C}\ell_\mathfrak{m}/H &\cong \mathrm{Hom}(\Delta_H, \mu_n) \\ \overline{[\mathfrak{D}]} &\xmapsto{\sim} \frac{\sigma_\mathfrak{D}(\sqrt[n]{\cdot})}{\sqrt[n]{\cdot}}. \end{aligned}$$

Nun definieren wir F_H als den aus der Kummertheorie bekannten Erweiterungskörper

$$F_H := F(\sqrt[n]{\Delta_H})$$

von F. Dann ist die Erweiterung $F_H|F$ abelsch vom Exponenten n. Wegen $\Delta_H \subseteq S_{n,\mathfrak{m}}$ ist F_H auch unverzweigt außerhalb von $\operatorname{supp}\mathfrak{m}$.

Zu überprüfen bleibt jetzt noch die Isomorphie. Die Kummerpaarung

$$\kappa_n : \Delta_H/(F^\times)^n \times \mathrm{Gal}(F_H|F) \to \mu_n$$

liefert nach Lemma 1.20 die Isomorphie

$$\begin{aligned} \mathrm{Gal}(F_H|F) &\cong \mathrm{Hom}(\Delta_H, \mu_n) \\ \sigma &\xmapsto{\sim} \frac{\sigma(\sqrt[n]{\cdot})}{\sqrt[n]{\cdot}}. \end{aligned}$$

Zusammen mit der weiter oben gegebenen Isomorphie folgt sofort

$$\mathrm{Gal}(F_H|F) \cong \mathcal{C}\ell_\mathfrak{m}/H$$

und an der Definition 3.6 der Paarung $\pi_{n,\mathfrak{m}}$ als Kummerpaarung mit Artinsymbol sieht man auch sofort, dass dieser Isomorphismus gegeben ist durch die Artinabbildung $(\cdot, F_H|F)$.

Existenz des Erklärungsmoduls. Nun sei umgekehrt eine abelsche Erweiterung $E|F$ vom Grad n gegeben. Laut Kummertheorie gibt es eine Gruppe Δ mit $(F^\times)^n \subseteq \Delta \subseteq F^\times$ so dass

$$E = F(\sqrt[n]{\Delta}).$$

Wir definieren $\mathcal{M}$ als die Menge der in E verzweigten Stellen von F und

$$\mathfrak{m} := \sum_{\mathfrak{p} \in \mathcal{M}} \mathfrak{p}.$$

Dann gilt $\Delta \subseteq S_{n,\mathfrak{m}}$ und die Paarung

$$\pi_{n,\mathfrak{m}} : S_{n,\mathfrak{m}}/(F^\times)^n \times \mathcal{C}\ell_\mathfrak{m}/n\mathcal{C}\ell_\mathfrak{m} \to \mu_n$$

ist nach Satz 3.8 nicht ausgeartet. Wir definieren H als den rechten Kern der induzierten Paarung

$$\Delta/(F^\times)^n \times \mathcal{C}\ell_\mathfrak{m} \to \mu_n$$

und erhalten eine weitere induzierte Paarung

$$\Delta/(F^\times)^n \times \mathcal{C}\ell_\mathfrak{m}/H \to \mu_n,$$

die wieder nicht ausgeartet ist. Also sehen wir wie im ersten Teil dieses Beweises, dass

$$\mathcal{C}\ell_\mathfrak{m}/H \cong \mathrm{Hom}(\Delta/(F^\times)^n, \mu_n) \cong \mathrm{Gal}(E|F)$$

unter der Artinabbildung $(\cdot, E|F)$ gilt, weshalb E der Klassenkörper zu H ist. □

Bemerkung 4.5. Aus den beiden im Beweis angegebenen nicht ausgearteten Paarungen folgen mit Lemma 1.20 noch weitere nützliche Isomorphien, beispielsweise

$$\mathcal{C}\ell_\mathfrak{m}/H \cong \Delta_H/(F^\times)^n.$$

An diesem Beweis sieht man direkt die in Satz 2.5 gezeigte Tatsache, dass der Klassenkörper schon durch die Isomorphie $\mathrm{Gal}(F_H|F) \cong \mathcal{C}\ell_\mathfrak{m}/H$ eindeutig definiert ist. Nämlich folgt aus der Isomorphie, dass $F_H|F$ abelsch vom Exponenten n ist. Dann liefert aber die Kummer-Bijektion ein eindeutig bestimmtes Δ mit $F_H = F(\sqrt[n]{\Delta})$. Die Paarungs-Bijektion ordnet dem Δ eindeutig ein H zu und umgekehrt. Also ist dadurch $F_H = F(\sqrt[n]{\Delta_H})$ eindeutig bestimmt.

Außerdem geht aus dem Beweis auch die Wohldefiniertheit der Artinabbildung $(\cdot, F_H|F)$ auf der Strahlklassengruppe $\mathcal{C}\ell_\mathfrak{m}$ hervor, denn ursprünglich ist sie ja nur auf der Divisorengruppe $\mathcal{D}^\mathfrak{m}$ definiert. Genauer sieht man im Beweis der Wohldefiniertheit der Paarung $\pi_{n,\mathfrak{m}}$, dass die Abbildung auf Elementen aus $\mathcal{P}_\mathfrak{m}$ trivial sein muss.

An der Konstruktion sieht man auch speziell, dass die Abbildung $H \mapsto F_H$ inklusionsumkehrend ist, was wir in Satz 2.10 allgemein gezeigt haben. Das liegt daran, dass $H \mapsto \Delta_H$ inklusionsumkehrend ist, wie man leicht nachprüft, und dass $\Delta_H \mapsto F_H$ inklusionserhaltend ist.

Man sieht hier auch direkt die Bijektivität der Abbildung $H \mapsto F_H$ auf den betrachteten Mengen *für fest gewähltes* $\mathfrak{m}$. Es gilt nämlich, wie bereits in

Kapitel 3.1 gesehen, $\Delta \subseteq S_{n,\mathfrak{m}}$ genau dann, wenn die Erweiterung $F(\sqrt[n]{\Delta})|F$ außerhalb von $\operatorname{supp}\mathfrak{m}$ unverzweigt ist. Deshalb liefert die Kummertheorie die Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Gruppen } \Delta \subseteq S_{n,\mathfrak{m}} \\ \text{mit } (F^\times)^n \subseteq \Delta \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{abelsche, außerhalb } \operatorname{supp}\mathfrak{m} \text{ unverzw.} \\ \text{Erw. } E|F \text{ vom Exponenten } n \end{array} \right\} \\ \Delta & \longmapsto & F(\sqrt[n]{\Delta}) \\ E^n \cap F^\times & \longmapsto & E. \end{array}$$

Schalten wir noch die von der Paarung kommende Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Gruppen } H \subseteq \mathcal{C}\ell_{\mathfrak{m}} \\ \text{vom Exponenten } n \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{Gruppen } \Delta \subseteq S_{n,\mathfrak{m}} \\ \text{mit } (F^\times)^n \subseteq \Delta \end{array} \right\} \\ H & \longmapsto & \Delta_H \\ H_\Delta & \longmapsto & \Delta \end{array}$$

davor, so erhalten wir insgesamt die Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Gruppen } H \subseteq \mathcal{C}\ell_{\mathfrak{m}} \\ \text{vom Exponenten } n \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{abelsche, außerhalb } \operatorname{supp}\mathfrak{m} \text{ unverzw.} \\ \text{Erw. } E|F \text{ vom Exponenten } n \end{array} \right\} \\ H & \longmapsto & F_H. \end{array}$$

Betrachtet man nur unverzweigte Erweiterungen, so ist automatisch $\mathfrak{m} = 0$ und man kann von einer Bijektion zwischen allen unverzweigten abelschen Erweiterungen vom Exponenten n und allen Untergruppen der gewöhnlichen Klassengruppe vom Exponenten n sprechen. In diesem Fall bekommt man die maximale abelsche unverzweigte Erweiterung von F vom Exponenten n durch Adjunktion aller n-ten Wurzeln von Elementen aus S_n.

Allgemein definiert

$$F(\sqrt[n]{S_{n,\mathfrak{m}}})$$

die maximale abelsche Erweiterung vom Exponenten n, die unverzweigt außerhalb von $\operatorname{supp}\mathfrak{m}$ ist.

4.2 Erweiterungen ohne Einheitswurzeln im Grundkörper

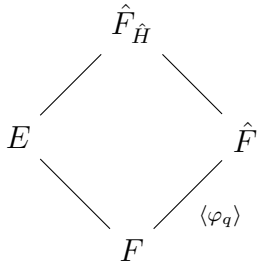
Nun wollen wir den Existenzsatz der Klassenkörpertheorie auch für solche n herleiten, für die $\mu_n \subseteq F$ nicht gilt (wir nehmen aber immer noch $\operatorname{ggT}(n, q) = 1$ an). Wir führen diesen Fall auf den uns bekannten Kummer-Fall zurück. Dazu bilden wir jeweils einen Körper $\hat{F} := F(\mu_n)$, der die n-ten Einheitswurzeln enthält, und betrachten von $\hat{F}$ aus eine Klassenkörpererweiterung $\hat{F}_{\hat{H}}|\hat{F}$.

Schließlich führt die Untersuchung des zur Erweiterung $\hat{F}_{\hat{H}}|F$ gehörenden Artinsymbols zum Ziel.

Die Konstruktion des Klassenkörpers ist wieder deutlich schwieriger als die Rückrichtung. Das liegt daran, dass wir in diesem Fall erst beweisen müssen, dass die Erweiterung $\hat{F}_{\hat{H}}|F$ überhaupt abelsch ist. Bei der umgekehrten Richtung gilt das automatisch. Danach überprüfen wir in beiden Fällen, dass die Artinabbildung auch eine Abbildung auf der Strahlklassengruppe $\mathcal{C}\ell_{\mathfrak{m}}$ induziert, dass $\mathcal{P}_{\mathfrak{m}}$ also im Kern von $(\cdot, \hat{F}_{\hat{H}}|F)$ enthalten ist. Das erreichen wir durch die Herleitung einer konkreten Darstellung dieser Artinabbildung, und diese Argumente gelten für beide Richtungen des Beweises. Am Ende bleibt dann nur noch, den Klassenkörper F_H bzw. die Untergruppe H zu definieren. Dies ist jeweils nicht sehr schwer, für F_H verwenden wir ein Fixkörperargument aus der Galoistheorie.

Wir führen hier zunächst die Konstruktion des Klassenkörpers F_H zu gegebenem H ausführlich vor und zeigen am Ende, wie die Rückrichtung mit ähnlichen Argumenten folgt. Es sei also ein $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ vom Index n gegeben. Die Idee ist dann folgendermaßen.

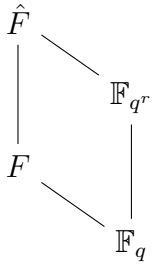
Zunächst bilden wir $\hat{F} := F(\mu_n)$ durch Adjunktion der n-ten Einheitswurzeln an F. Wir definieren $\hat{\mathfrak{m}} := \mathrm{Con}_{\hat{F}|F}(\mathfrak{m}) \in \mathcal{D}_{\hat{F}}$ und „liften“ auch H zu einer Untergruppe $\hat{H}$ von $\mathcal{C}\ell_{\hat{\mathfrak{m}}}$. Wir bilden wie in Abschnitt 4.1 den Klassenkörper $\hat{F}_{\hat{H}}$ zu $\hat{H}$. Die Galoisgruppe von $\hat{F}|F$ wird vom Frobeniusautomorphismus φ_q erzeugt, und dieser lässt sich auf $\hat{F}_{\hat{H}}$ zu einem Automorphismus $\hat{\varphi}_q$ fortsetzen. Mit Hilfe dieser Fortsetzung erhalten wir eine konkrete Beschreibung der Artinabbildung $(\cdot, \hat{F}_{\hat{H}}|F)$ und definieren E als Fixkörper der Menge $\{(\mathfrak{D}, \hat{F}_{\hat{H}}|F) \mid \mathfrak{D} \in H\}$. Dann ist H der Kern von $(\cdot, E|F)$ und E ist der Klassenkörper zu H.



Voraussetzungen und Notation 4.6. *Es sei eine Untergruppe H vom Index n in $\mathcal{C}\ell_{\mathfrak{m}}$ gegeben, wobei n teilerfremd zu q aber μ_n nicht in F enthalten ist. In diesem Fall ist eine Erweiterung $F(\sqrt[n]{f})|F$ nicht mehr normal, da für eine fest gewählte Wurzel $\sqrt[n]{f}$ von $t^n - f$ nicht mehr alle anderen Nullstellen des Polynoms in $F(\sqrt[n]{f})$ enthalten sind. Deshalb definieren wir $\hat{F}$ als die Köpererweiterung $F(\mu_n) = F(\zeta)$ von F für eine (fest gewählte) primitive n-te Einheitswurzel ζ. Dann ist $\hat{F}|F$ die Konstantenkörpererweiterung $F\mathbb{F}_{q^r}$ vom Grad r. Dabei ist r ein Teiler von $\phi(n)$, und r ist minimal so dass $q^r \equiv 1 \bmod n$. Die Galoisgruppe $\mathrm{Gal}(\hat{F}|F)$ wird vom Frobeniusautomorphismus $\varphi_q : \zeta \mapsto \zeta^q$ erzeugt (siehe [Sti93, Lemma V.1.9, S. 163]).*

Wir definieren $\hat{\mathfrak{m}} := \mathrm{Con}_{\hat{F}|F}(\mathfrak{m})$ als Element der zu $\hat{F}$ gehörenden Divisorengruppe $\mathcal{D}_{\hat{F}}$. Der Träger $\hat{\mathcal{M}}$ von $\hat{\mathfrak{m}}$ besteht also genau aus den Stellen von $\hat{F}$,

die über den Stellen in $\mathcal{M}$ liegen. Da $\hat{F}|F$ als Konstanenkörpererweiterung unverzweigt ist (siehe [Sti93, Thm. III.6.3, S. 103]), sind alle Verzweigungsindizes gleich 1 und der Koeffizient einer jeden Stelle aus $\hat{\mathcal{M}}$ ist gleich dem Koeffizienten der darunter liegenden Stelle aus $\mathcal{M}$.



In Lemma 2.12 haben wir gesehen, dass die Divisornorm auch auf Elementen der Strahlklassengruppen wohldefiniert ist. Es sei

$$\hat{H} := \mathcal{N}_{\hat{F}|F}^{-1}(H) = \{[\mathfrak{D}] \in \mathcal{C}\ell_{\hat{\mathfrak{m}}} \mid \mathcal{N}_{\hat{F}|F}([\mathfrak{D}]) \in H\}$$

und $\hat{n}$ der Index von $\hat{H}$ in $\mathcal{C}\ell_{\hat{\mathfrak{m}}}$.

Wir wollen den Klassenkörper zu $\hat{H}$ über $\hat{F}$ bilden. Dazu bleibt noch zu überprüfen, dass auch $\hat{n}$ teilerfremd zu q ist. Hierfür untersuchen wir im folgenden Lemma das Verhalten der Divisornorm in Konstantenkörpererweiterungen. Auch später in diesem Abschnitt wird dieses Resultat noch nützlich sein.

Lemma 4.7. *Für die Konstantenkörpererweiterung $\hat{F}|\mathbb{F}_{q^r}$ von $F|\mathbb{F}_q$ gilt: Die von der Divisornorm induzierte Abbildung $\mathcal{N}_{\hat{F}|F} : \mathcal{C}\ell^0_{\hat{\mathfrak{m}}} \to \mathcal{C}\ell^0_{\mathfrak{m}}$ ist surjektiv. Folglich hat die Abbildung $\mathcal{N}_{\hat{F}|F} : \mathcal{C}\ell_{\hat{\mathfrak{m}}} \to \mathcal{C}\ell_{\mathfrak{m}}$ das Bild*

$$\{[\mathfrak{D}] \in \mathcal{C}\ell_{\mathfrak{m}} \mid \deg[\mathfrak{D}] \in r\mathbb{Z}\}.$$

Beweis. Es sei $[\mathfrak{D}] \in \mathcal{C}\ell^0_{\mathfrak{m}}$ und $[\mathfrak{A}] \in \mathcal{C}\ell_{\mathfrak{m}}$ eine Divisorklasse vom Grad 1 (diese Existiert nach dem Satz von Schmidt [Sti93, Cor. V.1.11, S. 164] und dem Approximationssatz 1.8). Nach Satz 1.47 existiert dann für d groß genug eine Stelle $\mathfrak{p} \in \mathcal{P}^{\mathfrak{m}}$ vom Grad d mit $r \mid d$ und $[\mathfrak{D}] = [\mathfrak{p} - d\mathfrak{A}]$. Nach [Sti93, Lemma V.1.9, S. 163] gilt $\mathrm{Con}_{\hat{F}|F}(\mathfrak{p}) = \mathfrak{P}_1 + \ldots + \mathfrak{P}_r$ mit $\deg(\mathfrak{P}_i) = \frac{d}{r}$ und $\mathfrak{P}_i \in \mathcal{P}^{\hat{\mathfrak{m}}}$ für $i = 1, \ldots, r$. Wegen $\frac{d}{r} = \deg(\mathfrak{P}_i) = [\hat{F}_{\mathfrak{P}_i} : \mathbb{F}_{q^r}]$ und $\deg(\mathfrak{p}) = [F_{\mathfrak{p}} : \mathbb{F}_q]$ gilt $\hat{F}_{\mathfrak{P}_i} = \mathbb{F}_{q^d} = F_{\mathfrak{p}}$, also jeweils $f(\mathfrak{P}_i|\mathfrak{p}) = 1$. Nun sei $\hat{\mathfrak{A}} := \mathrm{Con}_{\hat{F}|F}(\mathfrak{A})$. Dann ist

$$\mathcal{N}_{\hat{F}|F}([\mathfrak{P}_1 - \frac{d}{r}\hat{\mathfrak{A}}]) = [f(\mathfrak{P}_1|\mathfrak{p})\mathfrak{p} - d\mathfrak{A}] = [\mathfrak{p} - d\mathfrak{A}] = [\mathfrak{D}]$$

und somit haben wir ein Urbild $[\mathfrak{P}_1 - \frac{d}{r}\hat{\mathfrak{A}}] \in \mathcal{C}\ell^0_{\hat{\mathfrak{m}}}$ von $[\mathfrak{D}]$ gefunden. □

Unter Beachtung der Isomorphie $\mathcal{C}\ell_{\mathfrak{m}} \cong \mathcal{C}\ell^0_{\mathfrak{m}} \times \mathbb{Z}$ ist das Bild also isomorph zu $\mathcal{C}\ell^0_{\mathfrak{m}} \times r\mathbb{Z}$. Für eine Untergruppe $H \cong H^0 \times \ell\mathbb{Z}$ mit $\ell \mid n$ erhalten wir

$$\hat{H} \cong \hat{H}^0 \times \frac{\mathrm{kgV}(\ell, r)}{r}\mathbb{Z}.$$

Für den Index von $\hat{H}$ in $\mathcal{C}\ell_{\hat{\mathfrak{m}}}$ gilt also

$$\hat{n} = (\mathcal{C}\ell^0_{\hat{\mathfrak{m}}} : \hat{H}^0) \cdot \frac{\mathrm{kgV}(\ell, r)}{r}.$$

Da die Normabbildung auf den Nullklassengruppen surjektiv ist und $\hat{H}^0$ genau als Urbild von H^0 unter dieser Abbildung definiert ist, gilt die Isomorphie

$$\mathcal{C}\ell^0_{\hat{\mathfrak{m}}}/\hat{H}^0 \cong \mathcal{C}\ell^0_{\mathfrak{m}}/H^0,$$

also ist $(\mathcal{C}\ell^0_{\hat{\mathfrak{m}}} : \hat{H}^0) = (\mathcal{C}\ell^0_{\mathfrak{m}} : H^0) = \frac{n}{\ell}$. Falls $\mathrm{ggT}(\ell, r) = 1$ gilt $\frac{\mathrm{kgV}(\ell,r)}{r} = \ell$, aber auch im allgemeinen Fall ist $\frac{\mathrm{kgV}(\ell,r)}{r}$ ein Teiler von ℓ. Also gilt auch immer $\hat{n} \mid n$. Dies ist wichtig für die folgenden Überlegungen, denn es garantiert, dass mit n auch der Index $\hat{n}$ von $\hat{H}$ in $\mathcal{C}\ell_{\hat{\mathfrak{m}}}$ teilerfremd zu q ist.

Wir sind nun in der Situation von Abschnitt 4.1: Es ist $\hat{H} \subseteq \mathcal{C}\ell_{\hat{\mathfrak{m}}}$ vom Index $\hat{n}$ gegeben, und $\hat{F}$ enthält $\mu_{\hat{n}}$. Also existiert nach Satz 4.3 der Klassenkörper $\hat{F}_{\hat{H}}$ zu $\hat{H}$.

Fortsetzung des Frobeniusautomorphismus

Das nächste Ziel besteht darin, den Frobeniusautomorphismus $\varphi_q \in \mathrm{Gal}(\hat{F}|F)$ auf $\hat{F}_{\hat{H}}$ fortzusetzen und eine handhabbare Beschreibung dieser Fortsetzung zu finden.

Die Paarung $\pi_{\hat{n},\hat{\mathfrak{m}}}$ spielt wieder eine wichtige Rolle. Hier ist die zur Erweiterung $\hat{F}_{\hat{H}}|\hat{F}$ gehörende Paarung gemeint, also

$$\pi_{\hat{n},\hat{\mathfrak{m}}} : \Delta_{\hat{H}} \times \mathcal{C}\ell_{\hat{\mathfrak{m}}}/\hat{H} \to \mu_{\hat{n}}.$$

Dabei wird $\Delta_{\hat{H}}$ als Untergruppe von $S_{\hat{n},\hat{\mathfrak{m}}}/(\hat{F}^\times)^{\hat{n}}$, also der zu $\hat{F}$ gehörenden $\hat{n}$-Selmergruppe, aufgefasst.

Wir untersuchen mit Hilfe dieser Paarung zunächst, wie die Galoisautomorphismen $\sigma \in \mathrm{Gal}(\hat{F}|F)$ auf den Gruppen $\Delta_{\hat{H}}$ und $\mathcal{C}\ell_{\hat{\mathfrak{m}}}/\hat{H}$ operieren und leiten damit eine konkretere Darstellung von φ_q her.

Für $\mathfrak{D} \in \mathcal{D}_{\hat{F}}$ ist $\sigma\mathfrak{D}$ definiert durch

$$\sigma\mathfrak{D} = \sum_{\mathfrak{p} \in \mathcal{S}_{\hat{F}}} v_{\mathfrak{p}}(\mathfrak{D}) \cdot \sigma\mathfrak{p},$$

und wegen $v_{\mathfrak{p}}(f) = v_{\sigma\mathfrak{p}}(\sigma f)$ gilt für die Hauptdivisoren $\sigma(f) = (\sigma f)$, und σ ist auch auf $\mathcal{C}\ell_{\hat{F}}$ sowie $\mathcal{C}\ell_{\hat{\mathfrak{m}}}$ wohldefiniert.

Lemma 4.8. *Für jedes $\sigma \in \mathrm{Gal}(\hat{F}|F)$ ist die Paarung $\pi_{\hat{n},\hat{\mathfrak{m}}}$ σ-equivariant, d.h. es gilt*

$$\pi_{\hat{n},\hat{\mathfrak{m}}}(\sigma\bar{f}, \sigma\overline{[\mathfrak{D}]}) = \sigma\pi_{\hat{n},\hat{\mathfrak{m}}}(\bar{f}, \overline{[\mathfrak{D}]})$$

für alle $\bar{f} \in \Delta_{\hat{H}}$ und $\overline{[\mathfrak{D}]} \in \mathcal{C}\ell_{\hat{\mathfrak{m}}}/\hat{H}$.

Im Gegensatz zu den folgenden Aussagen gilt dieses Lemma ganz allgemein für die Paarung $\pi_{n,\mathfrak{m}}$. Die spezielle Struktur der Gruppe $\hat{H}$ (als Norm-Urbild einer Gruppe H) wird im Beweis nicht verwendet.

Beweis. Es sei $\bar{f} \in \Delta_{\hat{H}}$ und $\mathfrak{D} \in \mathcal{D}^{\hat{\mathfrak{m}}}$. Für eine Stelle $\mathfrak{p} \in \mathcal{S}_{\hat{F}}$ werden beide Galoisgruppen $\mathrm{Gal}(\hat{F}_{\sigma\mathfrak{p}}|\mathbb{F}_{q^r})$ und $\mathrm{Gal}(\hat{F}_{\mathfrak{p}}|\mathbb{F}_{q^r})$ vom Frobeniusautomorphismus φ_{q^r} erzeugt, also ist

$$\mathrm{N}_{\hat{F}_{\sigma\mathfrak{p}}|\mathbb{F}_{q^r}}((\sigma f)(\sigma\mathfrak{p})) \overset{\mathrm{mod}\,\sigma\mathfrak{p}}{\equiv} \prod_{i=0}^{[\hat{F}_{\sigma\mathfrak{p}}:\mathbb{F}_{q^r}]-1} (\sigma f)^{q^{ir}} = \sigma \prod_{i=0}^{[\hat{F}_{\mathfrak{p}}:\mathbb{F}_{q^r}]-1} f^{q^{ir}} \overset{\mathrm{mod}\,\sigma}{\equiv} \sigma\,\mathrm{N}_{\hat{F}_{\mathfrak{p}}|\mathbb{F}_{q^r}}(f(\mathfrak{p})).$$

Da die linke und rechte Seite der Gleichung in $\mathbb{F}_{q^r}$ liegen und $\mathbb{F}_{q^r} \cap \mathfrak{p} = \mathbb{F}_{q^r} \cap \sigma\mathfrak{p} = \{0\}$, gilt schon die Gleichheit

$$\mathrm{N}_{\hat{F}_{\sigma\mathfrak{p}}|\mathbb{F}_{q^r}}((\sigma f)(\sigma\mathfrak{p})) = \sigma\,\mathrm{N}_{\hat{F}_{\mathfrak{p}}|\mathbb{F}_{q^r}}(f(\mathfrak{p})).$$

Schließlich erhalten wir

$$\begin{aligned}(\sigma f)(\sigma\mathfrak{D}) &= (\sigma f)\left(\sum_{\mathfrak{p}\in\mathcal{S}_{\hat{F}}} v_{\mathfrak{p}}(\mathfrak{D})\cdot\sigma\mathfrak{p}\right) = \prod_{\mathfrak{p}\in\mathcal{S}_{\hat{F}}} \mathrm{N}_{\hat{F}_{\sigma\mathfrak{p}}|\mathbb{F}_{q^r}}((\sigma f)(\sigma\mathfrak{p}))^{v_{\mathfrak{p}}(\mathfrak{D})} \\ &= \prod_{\mathfrak{p}\in\mathcal{S}_{\hat{F}}} \sigma\,\mathrm{N}_{\hat{F}_{\mathfrak{p}}|\mathbb{F}_{q^r}}(f(\mathfrak{p}))^{v_{\mathfrak{p}}(\mathfrak{D})} = \sigma(f(\mathfrak{D})),\end{aligned}$$

woraus die Behauptung direkt folgt. □

Lemma 4.9. *Es gilt $\sigma\Delta_{\hat{H}} = \Delta_{\hat{H}}$ für alle $\sigma \in \mathrm{Gal}(\hat{F}|F)$.*

Beweis. Es ist $\sigma\hat{H} = \hat{H}$, denn für $[\mathfrak{D}] \in \hat{H}$ gilt

$$\begin{aligned}\mathcal{N}_{\hat{F}|F}(\sigma[\mathfrak{D}]) &= \sum_{\tau\in\mathrm{Gal}(\hat{F}|F)} \tau(\sigma[\mathfrak{D}]) = \sum_{\tau\in\mathrm{Gal}(\hat{F}|F)} \sigma\tau[\mathfrak{D}] \\ &= \sigma \sum_{\tau\in\mathrm{Gal}(\hat{F}|F)} \tau[\mathfrak{D}] = \sigma\mathcal{N}_{\hat{F}|F}([\mathfrak{D}])\end{aligned}$$

da $\mathrm{Gal}(\hat{F}|F)$ abelsch ist. Nun ist $\mathcal{N}_{\hat{F}|F}([\mathfrak{D}]) \in \mathcal{C}\ell_{\mathfrak{m}}$, also gilt $\mathcal{N}_{\hat{F}|F}(\sigma[\mathfrak{D}]) = \mathcal{N}_{\hat{F}|F}([\mathfrak{D}])$. D.h. $\sigma[\mathfrak{D}]$ liegt genau dann in $\hat{H} = \mathcal{N}^{-1}_{\hat{F}|F}(H)$, wenn $[\mathfrak{D}]$ in $\hat{H}$ liegt.

Nun wollen wir $\sigma\Delta_{\hat{H}} = \Delta_{\hat{H}}$ zeigen. Nach Definition von $\Delta_{\hat{H}}$ ist $\bar{f} \in \Delta_{\hat{H}}$ genau dann, wenn $\pi_{\hat{n},\hat{\mathfrak{m}}}(\bar{f}, [\mathfrak{D}]) = 1$ für alle $[\mathfrak{D}] \in \hat{H}$. Wegen der σ-Equivarianz ist das genau dann der Fall, wenn $\pi_{\hat{n},\hat{\mathfrak{m}}}(\sigma\bar{f}, \sigma[\mathfrak{D}]) = 1$ für alle $[\mathfrak{D}] \in \hat{H}$, und mit dem eben gezeigten $\sigma\hat{H} = \hat{H}$ ist das äquivalent zu $\pi_{\hat{n},\hat{\mathfrak{m}}}(\sigma\bar{f}, \sigma[\mathfrak{D}]) = 1$ für alle $[\mathfrak{D}] \in \sigma\hat{H}$. Anders geschrieben ist das $\pi_{\hat{n},\hat{\mathfrak{m}}}(\sigma\bar{f}, [\mathfrak{D}]) = 1$ für alle $[\mathfrak{D}] \in \hat{H}$, äquivalent zu $\sigma\bar{f} \in \Delta_{\hat{H}}$. Mit $\sigma\bar{f} = \overline{\sigma f}$ folgt die Behauptung. □

Korollar 4.10. *Die Erweiterung $\hat{F}_{\hat{H}}|F$ ist galoissch.*

Beweis. Die Erweiterungen $\hat{F}_{\hat{H}}|\hat{F}$ und $\hat{F}|F$ sind galoissch, somit ist auch $\hat{F}_{\hat{H}}|F$ separabel, zu zeigen bleibt die Normalität. Es bezeichne L den algebraischen Abschluss von $\hat{F}_{\hat{H}}$, und es sei $\tau \in \mathrm{Hom}_F(\hat{F}_{\hat{H}}, L)$ gegeben. Dann ist $\tau \in \mathrm{Aut}_F(\hat{F}_{\hat{H}})$ zu zeigen. L ist gleichzeitig auch der algebraische Abschluss von $\hat{F}$, und $\hat{F}|F$ ist normal, deshalb gilt $\tau|_{\hat{F}} \in \mathrm{Aut}_F(\hat{F}) = \mathrm{Gal}(\hat{F}|F)$. Dann ist nach Lemma 4.9 $\tau|_{\hat{F}}(\Delta_{\hat{H}}) = \Delta_{\hat{H}}$, also gilt für $f \in \Delta_{\hat{H}}$

$$\tau(\sqrt[\hat{n}]{f})^{\hat{n}} = \tau|_{\hat{F}}(f) \in \Delta_{\hat{H}}.$$

Folglich gilt $\tau(\sqrt[\hat{n}]{\Delta_{\hat{H}}}) \subseteq \sqrt[\hat{n}]{\Delta_{\hat{H}}} \subseteq \hat{F}_{\hat{H}}$. Klar ist, dass für eine primitive $\hat{n}$-te Einheitswurzel ζ auch $\tau(\zeta) \in \hat{F}_{\hat{H}}$ ist. Nun ist $\hat{F}_{\hat{H}} = F(\zeta, \sqrt[\hat{n}]{\Delta_{\hat{H}}})$ der kleinste Körper, der F, ζ und $\sqrt[\hat{n}]{\Delta_{\hat{H}}}$ enthält und es gilt $\tau(\hat{F}_{\hat{H}}) \subseteq \hat{F}_{\hat{H}}$. Daraus folgt sofort $\tau \in \mathrm{Aut}_F(\hat{F}_{\hat{H}})$, was zu beweisen war. □

Mit Hilfe der beiden vorhergehenden Lemmata können wir jetzt genau beschreiben, wie φ_q auf der Gruppe $\Delta_{\hat{H}}$ operiert. Das Ergebnis geht bereits auf Shafarevich [Sha89, Lemma 1] zurück.

Lemma 4.11. *Für $\bar{f} \in \Delta_{\hat{H}}$ gilt $\varphi_q \bar{f} = \bar{f}^q$.*

Beweis. Wir wollen zunächst $\varphi_q\overline{[\mathfrak{D}]} = \overline{[\mathfrak{D}]}$ für $\overline{[\mathfrak{D}]} \in \mathcal{C}\ell_{\hat{\mathfrak{m}}}/\hat{H}$ zeigen. Wegen $\mathcal{N}_{\hat{F}|F}(\hat{H}) \subseteq H$ ist die Divisornorm $\mathcal{N}_{\hat{F}|F} : \mathcal{C}\ell_{\hat{\mathfrak{m}}}/\hat{H} \to \mathcal{C}\ell_{\mathfrak{m}}/H$ wohldefiniert und es gilt

$$\begin{aligned}
\mathcal{N}_{\hat{F}|F}(\varphi_q\overline{[\mathfrak{D}]} - \overline{[\mathfrak{D}]}) &= \prod_{\tau \in \mathrm{Gal}(\hat{F}|F)} \tau\varphi_q\overline{[\mathfrak{D}]} - \prod_{\tau \in \mathrm{Gal}(\hat{F}|F)} \tau\overline{[\mathfrak{D}]} \\
&= \prod_{\tau \in \mathrm{Gal}(\hat{F}|F)} \tau\overline{[\mathfrak{D}]} - \prod_{\tau \in \mathrm{Gal}(\hat{F}|F)} \tau\overline{[\mathfrak{D}]} \\
&= 0 \quad \text{in } \mathcal{C}\ell_{\mathfrak{m}}/H,
\end{aligned}$$

denn wenn τ alle Elemente von $\mathrm{Gal}(\hat{F}|F)$ durchläuft, dann durchläuft auch $\tau\varphi_q$ alle Elemente der Galoisgruppe. Folglich ist $\mathcal{N}_{\hat{F}|F}(\varphi_q[\mathfrak{D}] - [\mathfrak{D}]) \in H$, also $\varphi_q[\mathfrak{D}] - [\mathfrak{D}] \in \hat{H}$ und somit $\varphi_q\overline{[\mathfrak{D}]} - \overline{[\mathfrak{D}]} = 0$ in $\mathcal{C}\ell_{\hat{\mathfrak{m}}}/\hat{H}$. Das beweist die erste Behauptung.

Für die Darstellung von φ_q auf $\Delta_{\hat{H}}$ verwenden wir die Paarung. Für $\bar{f} \in \Delta_{\hat{H}}$ und $\overline{[\mathfrak{D}]} \in \mathcal{C}\ell_{\hat{\mathfrak{m}}}/\hat{H}$ gilt

$$\begin{aligned}
\pi_{\hat{n},\hat{\mathfrak{m}}}(\varphi_q\bar{f}, \overline{[\mathfrak{D}]}) &= \pi_{\hat{n},\hat{\mathfrak{m}}}(\varphi_q\bar{f}, \varphi_q\overline{[\mathfrak{D}]}) = \varphi_q\pi_{\hat{n},\hat{\mathfrak{m}}}(\bar{f}, \overline{[\mathfrak{D}]}) \\
&= \pi_{\hat{n},\hat{\mathfrak{m}}}(\bar{f}, \overline{[\mathfrak{D}]})^q = \pi_{\hat{n},\hat{\mathfrak{m}}}(\bar{f}^q, \overline{[\mathfrak{D}]}).
\end{aligned}$$

Dabei haben wir in der ersten Zeile Lemma 4.8 verwendet und in der zweiten Zeile die Bilinearität von $\pi_{\hat{n},\hat{\mathfrak{m}}}$ und dass $\pi_{\hat{n},\hat{\mathfrak{m}}}(\bar{f}, \overline{[\mathfrak{D}]}) \in \mu_{\hat{n}}$. Da $\pi_{\hat{n},\hat{\mathfrak{m}}}$ nicht ausgeartet ist, folgt $\varphi_q\bar{f} = \bar{f}^q$. □

Für jeden Repräsentanten f von $\bar{f} \in \Delta_{\hat{H}}$ gibt es also ein $g \in \hat{F}^\times$ so dass $\varphi_q f = f^q g^{\hat{n}}$ ist. Mit dieser Darstellung von φ_q können wir nun leicht eine Fortsetzung $\hat{\varphi}_q$ auf $\hat{F}_{\hat{H}}$ definieren. Dafür legen wir die folgende Notation fest.

Voraussetzungen und Notation 4.12. *Es seien $\bar{f}_1, \dots, \bar{f}_k$ Erzeuger von $\Delta_{\hat{H}}$. Weiter sei*

$$\Gamma := \{f_1, \dots, f_k\}$$

und $y_i \in \hat{F}_{\hat{H}}$ so, dass $y_i^{\hat{n}} = f_i$ für $i = 1, \dots, k$. Dann ist $\hat{F}_{\hat{H}} = \hat{F}(y_1, \dots, y_k)$.

Die Automorphismen aus $\mathrm{Gal}(\hat{F}_{\hat{H}}|\hat{F})$ sind nun durch ihre Aktion auf den y_i eindeutig festgelegt.

Satz 4.13. *Für jede Fortsetzung $\hat{\varphi}_q$ von φ_q auf $\hat{F}_{\hat{H}}$ gilt: Zu jedem $f \in \Gamma$ und zugehörigem y mit $y^{\hat{n}} = f$ existiert ein $g \in \hat{F}^\times$ so dass*

$$\hat{\varphi}_q(y) = y^q g \quad \text{und} \quad g^{\hat{n}} = \frac{\varphi_q f}{f^q}.$$

Jedes Element g ist also bestimmt bis auf eine $\hat{n}$-te Einheitswurzel.

Beweis. Nach Lemma 4.11 gibt es zu jedem f ein $g \in \hat{F}^\times$ so dass $g^{\hat{n}} = \frac{\varphi_q f}{f^q}$. Für eine Fortsetzung $\hat{\varphi}_q$ von φ_q gilt dann

$$\hat{\varphi}_q(y)^{\hat{n}} = \varphi_q(y^{\hat{n}}) = \varphi_q(f) = f^q g^{\hat{n}},$$

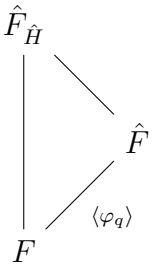
woraus die Behauptung durch Wurzelziehen direkt folgt. Hier sieht man auch, dass eine Fortsetzung existiert: Man kann sie wie hier angegeben definieren. □

An dieser Stelle kann man leicht nachrechnen, dass die Potenzen von $\hat{\varphi}_q$ gegeben sind durch

$$\hat{\varphi}_q^i(y) = y^{q^i} \prod_{j=0}^{i-1} \varphi_q^j(g)^{q^{i-1-j}}.$$

Die Erweiterung $\hat{F}_{\hat{H}}|F$

Nun widmen wir uns der Erweiterung $\hat{F}_{\hat{H}}|F$, überprüfen dass sie abelsch ist und leiten eine Darstellung der zugehörigen Artinabbildung her.



Voraussetzungen und Notation 4.14. *Im Folgenden bezeichne $\hat{\varphi}_q$ immer eine Fortsetzung von φ_q auf $\hat{F}_{\hat{H}}$. Weiter sei f immer ein Element aus Γ, $y^{\hat{n}} = f$ und g ein zugehöriges Element aus $\hat{F}^\times$ mit $g^{\hat{n}} = \frac{\varphi_q f}{f^q}$ so dass $\hat{\varphi}_q(f) = f^q g^{\hat{n}}$ bzw. $\hat{\varphi}_q(y) = y^q g$.*

Lemma 4.15. *Für jede Fortsetzung $\hat{\varphi}_q$ von φ_q ist die Abbildung*

$$\mathrm{Gal}(\hat{F}_{\hat{H}}|\hat{F}) \times \langle\hat{\varphi}_q\rangle \to \mathrm{Gal}(\hat{F}_{\hat{H}}|F), \quad (\tau, \hat{\varphi}_q^i) \mapsto \tau \circ \hat{\varphi}_q^i$$

bijektiv.

Beweis. Die inverse Abbildung ist folgendermaßen gegeben. Für ein $\sigma \in \mathrm{Gal}(\hat{F}_{\hat{H}}|F)$ bestimme i so, dass $\sigma|_{\hat{F}} = \varphi_q^i$ und bilde σ ab auf $(\sigma \circ \hat{\varphi}_q^{-i}, \hat{\varphi}_q^i)$. □

Lemma 4.16. *Jedes $\hat{\varphi}_q$ kommutiert mit jedem Element aus* $\mathrm{Gal}(\hat{F}_{\hat{H}}|\hat{F})$.

Beweis. Es sei $\tau \in \mathrm{Gal}(\hat{F}_{\hat{H}}|\hat{F})$ und $f \in \Gamma$, $y^{\hat{n}} = f$. Dann ist $\tau y = \zeta y$ für ein $\zeta \in \mu_{\hat{n}}$. Für $\hat{\varphi}_q y = y^q g$ gilt

$$\hat{\varphi}_q \circ \tau y = \hat{\varphi}_q(\zeta y) = \zeta^q y^q g = (\zeta y)^q g = \tau(y^q g) = \tau \circ \hat{\varphi}_q y,$$

daraus folgt direkt die Behauptung. □

Korollar 4.17. *Die Erweiterung $\hat{F}_{\hat{H}}|F$ ist abelsch.*

Beweis. Die Behauptung folgt sofort mit Lemma 4.16 und Lemma 4.15, da $\hat{F}_{\hat{H}}|\hat{F}$ als Klassenkörpererweiterung abelsch ist und die $\hat{\varphi}_q$-Potenzen natürlich miteinander kommutieren. □

Man sieht leicht, dass die Erweiterung $\hat{F}_{\hat{H}}|F$ auch unverzweigt außerhalb von $\operatorname{supp}\mathfrak{m}$ ist, denn $\hat{F}_{\hat{H}}|\hat{F}$ ist unverzweigt außerhalb $\operatorname{supp}\hat{\mathfrak{m}}$ und $\hat{F}|F$ ist sowieso unverzweigt. Für Stellen $\mathfrak{P}$ von $\hat{F}_{\hat{H}}$ und die darunter liegenden Stellen $\hat{\mathfrak{p}}$ und $\mathfrak{p}$ von $\hat{F}$ bzw. F gilt also mit der Formel aus [Sti93, Prop. III.1.6, S. 62] für die Verzweigungsindizes

$$e(\mathfrak{P}|\mathfrak{p}) = e(\mathfrak{P}|\hat{\mathfrak{p}}) \cdot e(\hat{\mathfrak{p}}|\mathfrak{p}) = e(\mathfrak{P}|\hat{\mathfrak{p}}).$$

Also können wir die zugehörige Artinabbildung $(\cdot, \hat{F}_{\hat{H}}|F) : \mathcal{D}^{\mathfrak{m}} \to \mathrm{Gal}(\hat{F}_{\hat{H}}|F)$ betrachten.

Die beiden folgenden Aussagen Lemma 4.18 und Satz 4.19 gelten allein unter der Voraussetzung, dass $\hat{F}_{\hat{H}}|F$ abelsch und außerhalb von $\operatorname{supp}\mathfrak{m}$ unverzweigt ist, und dass wir eine Darstellung $\varphi_q f \equiv f^q \bmod (\hat{F}^\times)^{\hat{n}}$ für alle $f \in \Delta$ haben, wobei $\hat{F}_{\hat{H}} = \hat{F}(\sqrt[\hat{n}]{\Delta})$. Sie sind auch für den Beweis der Rückrichtung des Existenzsatzes entscheidend.

Lemma 4.18. *Es sei $\hat{\varphi}_q(y_i) = y_i^q g_i$, $i = 1, \ldots, k$ eine feste Fortsetzung von φ_q. Für jeden Divisor $\mathfrak{D} \in \mathcal{D}^{\mathfrak{m}}$ ist der Artinautomorphismus $(\mathfrak{D}, \hat{F}_{\hat{H}}|F)$ dann eindeutig bestimmt durch das Tupel* $(\deg\mathfrak{D}, g_i(\mathrm{Con}_{\hat{F}|F}(\mathfrak{D}))^{-q^{-1}}) \in \mathbb{Z} \times (\mu_n)^k$.

Beweis. Wir halten ein y und zugehöriges g fest. Dabei nehmen wir an, $f = y^{\hat{n}}$ wäre so gewählt, dass $f \in \mathcal{O}_{\hat{\mathfrak{p}}}$ für alle $\hat{\mathfrak{p}} \notin \operatorname{supp} \hat{\mathfrak{m}}$. Dies ist ohne Beschränkung der Allgemeinheit möglich, da f mit einer $\hat{n}$-ten Potenz eines Elements von $\hat{F}$ multipliziert werden kann, ohne den Körper $\hat{F}(\sqrt[\hat{n}]{f})$ zu verändern. Da $f \in S_{\hat{n},\hat{\mathfrak{m}}}$, kann man mit dem Approximationssatz 1.8 also eine Funktion $h \in \hat{F}$ finden, so dass $fh^{\hat{n}}$ keine Pole in $\mathcal{S}_{\hat{F}} \setminus \operatorname{supp} \hat{\mathfrak{m}}$ hat.

Es sei zunächst $\sigma_{\mathfrak{p}} = (\mathfrak{p}, \hat{F}_{\hat{H}}|F)$ für eine Stelle $\mathfrak{p} \in \mathcal{S}_F \setminus \operatorname{supp} \mathfrak{m}$. Dann ist wie in Lemma 4.15 $\sigma_{\mathfrak{p}} = \tau_{\mathfrak{p}} \circ \hat{\varphi}_q^d$ für ein d und $\tau_{\mathfrak{p}} \in \operatorname{Gal}(\hat{F}_{\hat{H}}|\hat{F})$. Dabei ist $\varphi_q^d = (\mathfrak{p}, \hat{F}_{\hat{H}}|F)|_{\hat{F}} = (\mathfrak{p}, \hat{F}|F) = \varphi_q^{\deg \mathfrak{p}}$, die letzte Gleichheit gilt nach [Ros02, Prop. 9.19, S.136], da $\hat{F}|F$ eine Konstantenkörpererweiterung ist. Also gilt $d = \deg \mathfrak{p}$. Weiter gilt $\tau_{\mathfrak{p}} y = \zeta_{\mathfrak{p}} y$ für ein $\zeta_{\mathfrak{p}} \in \mu_{\hat{n}}$. Also wird $\sigma_{\mathfrak{p}}$ eindeutig durch $\deg \mathfrak{p}$ und ein $\zeta_{\mathfrak{p}}$ für jedes y beschrieben.

Zu zeigen bleibt noch $\zeta_{\mathfrak{p}} = g(\operatorname{Con}_{\hat{F}|F}(\mathfrak{p}))^{-q^{-1}}$. Es gilt

$$\sigma_{\mathfrak{p}}(y) = \tau_{\mathfrak{p}} \circ \hat{\varphi}_q^d(y) = \tau_{\mathfrak{p}} \left(y^{q^d} \prod_{j=0}^{d-1} \varphi_q^j(g)^{q^{d-1-j}} \right) = \zeta_{\mathfrak{p}}^{q^d} y^{q^d} \prod_{j=0}^{d-1} \varphi_q^j(g)^{q^{d-1-j}}$$

und

$$\sigma_{\mathfrak{p}}(y) \equiv y^{q^d} \bmod \mathfrak{P}$$

für alle $\mathfrak{P} \in \mathcal{S}_{\hat{F}_{\hat{H}}}$ über $\mathfrak{p}$, denn wir hatten y ja so gewählt, dass $y \in \mathcal{O}_{\mathfrak{P}}$ für alle diese $\mathfrak{P}$. Durch Gleichsetzen der beiden Gleichungen erhalten wir

$$\zeta_{\mathfrak{p}}^{q^d} \prod_{j=0}^{d-1} \varphi_q^j(g)^{q^{d-1-j}} \equiv 1 \bmod \mathfrak{P}.$$

Dabei sind beide Seiten bereits in $\hat{F}$ und die Äquivalenz gilt auch modulo aller Stellen von $\hat{F}$ über $\mathfrak{p}$.

Wir betrachten eine Konstantenkörpererweiterung L von $\hat{F}$, die groß genug ist, so dass $\mathfrak{p}$ in L total zerlegt ist, d.h.

$$\operatorname{Con}_{\hat{F}|F}(\mathfrak{p}) = \sum_{j=0}^{d-1} \mathfrak{q}_j$$

mit $\deg \mathfrak{q}_j = 1$ für $j = 0, \ldots, d-1$. Dann sind die $\mathfrak{q}_i$ alle konjugiert: $\mathfrak{q}_j = \varphi_q^j(\mathfrak{q})$ for $\mathfrak{q} = \mathfrak{q}_0$. Wir berechnen

$$\begin{aligned} g(\operatorname{Con}_{\hat{F}|F}(\mathfrak{p}))^{q^{d-1}} &= g(\operatorname{Con}_{L|F}(\mathfrak{p}))^{q^{d-1}} = \prod_{j=0}^{d-1} g(\varphi_q^j(\mathfrak{q}))^{q^{d-1}} \\ &= \prod_{j=0}^{d-1} \varphi_q^{-j}(\varphi_q^j(g)(\mathfrak{q}))^{q^{d-1}} \\ &\equiv \prod_{j=0}^{d-1} \varphi_q^j(g)^{q^{d-1-j}} \equiv \zeta_{\mathfrak{p}}^{-q^d} \bmod \mathfrak{q}. \end{aligned}$$

Da beide Seiten der Gleichung bereits im Konstantenkörper liegen, welcher wiederum trivialen Schnitt mit $\mathfrak{q}$ hat, erhalten wir $g(\mathrm{Con}_{\hat{F}|F}(\mathfrak{p}))^{q^{d-1}} = \zeta_{\mathfrak{p}}^{-q^d}$, und daraus folgt $g(\mathrm{Con}_{\hat{F}|F}(\mathfrak{p}))^{-q^{-1}} = \zeta_{\mathfrak{p}}$.

Durch die Linearität und mit Lemma 4.16 folgt für Divisoren $\mathfrak{D}$ entsprechend:

$$(\mathfrak{D}, \hat{F}_{\hat{H}}|F) = \sigma_{\mathfrak{D}} = \tau_{\mathfrak{D}} \circ \hat{\varphi}_q^{\deg \mathfrak{D}}$$

mit $\tau_{\mathfrak{D}} y = \zeta_{\mathfrak{D}} y$ und $\zeta_{\mathfrak{D}} = g(\mathrm{Con}_{\hat{F}|F}(\mathfrak{D}))^{-q^{-1}}$. □

Satz 4.19. *Es gilt $\mathcal{P}_{\mathfrak{m}} \subseteq \ker(\cdot, \hat{F}_{\hat{H}}|F)$, also ist das Artinsymbol auch als Abbildung $(\cdot, \hat{F}_{\hat{H}}|F) : \mathcal{C}\ell_{\mathfrak{m}} \to \mathrm{Gal}(\hat{F}_{\hat{H}}|F)$ wohldefiniert und surjektiv.*

Beweis. Es sei $\mathfrak{D} = (h)_F \in \mathcal{P}_{\mathfrak{m}}$. Dann gilt nach [Sti93, Prop. III.1.9, S. 63] $\mathrm{Con}_{\hat{F}|F}((h)_F) = (h)_{\hat{F}}$, also $g(\mathrm{Con}_{\hat{F}|F}(\mathfrak{D})) = g((h)_{\hat{F}}) = h((g)_{\hat{F}})$ nach Weil-Reziprozität. Wegen $\Delta_{\hat{H}} \subseteq S_{\hat{n},\hat{\mathfrak{m}}}$ gibt es für $f \in \Gamma$ ein $\mathfrak{C} \in \mathcal{D}^{\hat{\mathfrak{m}}}$ mit

$$(f)_{\hat{F}} = \hat{n}\mathfrak{C} + \sum_{\hat{\mathfrak{p}} \in \hat{\mathcal{M}}} v_{\hat{\mathfrak{p}}}(f) \cdot \hat{\mathfrak{p}} =: \hat{n}\mathfrak{C} + \mathfrak{B}$$

und aus $g^{\hat{n}} = \frac{\varphi_q f}{f^q}$ folgt damit

$$\hat{n}(g)_{\hat{F}} = (\varphi_q f)_{\hat{F}} - (f^q)_{\hat{F}} = \varphi_q(\hat{n}\mathfrak{C}) - \hat{n}q\mathfrak{C} + \varphi_q\mathfrak{B} - q\mathfrak{B}$$

oder auch

$$(g)_{\hat{F}} = \varphi_q\mathfrak{C} - q\mathfrak{C} + \mathfrak{B}'$$

für $\mathfrak{B}' = \frac{1}{\hat{n}}(\varphi_q\mathfrak{B} - q\mathfrak{B})$, und wegen $\varphi_q(\hat{\mathcal{M}}) = \hat{\mathcal{M}}$ hat auch $\mathfrak{B}'$ Träger in $\hat{\mathcal{M}}$. Es ist

$$h((g)_{\hat{F}}) = h(\varphi_q\mathfrak{C} - q\mathfrak{C}) \cdot h(\mathfrak{B}').$$

Wegen $h(\varphi_q\mathfrak{C}) = (\varphi_q h)(\varphi_q\mathfrak{C}) = \varphi_q(h(\mathfrak{C})) = h(\mathfrak{C})^q$ ist

$$h(\varphi_q\mathfrak{C} - q\mathfrak{C}) = 1.$$

Außerdem war nach Voraussetzung $(h) \in \mathcal{P}_{\mathfrak{m}}$, deshalb ist für alle $\mathfrak{p} \in \mathcal{M}$ $v_{\mathfrak{p}}(h-1) \geq v_{\mathfrak{p}}(\mathfrak{m})$ und da $\hat{F}|F$ unverzweigt folgt sofort für alle $\hat{\mathfrak{p}} \in \hat{\mathcal{M}}$ $v_{\hat{\mathfrak{p}}}(h-1) \geq v_{\hat{\mathfrak{p}}}(\hat{\mathfrak{m}})$. Also ist $h(\hat{\mathfrak{p}}) = 1$ für alle $\hat{\mathfrak{p}} \in \hat{\mathcal{M}}$ und deshalb

$$h(\mathfrak{B}') = 1,$$

denn der Träger von $\mathfrak{B}'$ liegt in $\hat{\mathcal{M}}$. Insgesamt folgt

$$g(\mathrm{Con}_{\hat{F}|F}(\mathfrak{D})) = 1.$$

$\mathfrak{D}$ hat den Grad 0 und wir erhalten $(\mathfrak{D}, \hat{F}_{\hat{H}}|F) = \tau_{\mathfrak{D}} \circ \hat{\varphi}_q^{\deg \mathfrak{D}} = \mathrm{id}_{\hat{F}_{\hat{H}}}$ aus Lemma 4.18. □

Um den Zusammenhang zwischen dem Term $g(\mathrm{Con}_{\hat{F}|F}(\mathfrak{D}))^{-q^{-1}}$ und der Paarung $\pi_{\hat{n},\hat{\mathfrak{m}}}$ noch besser zu verstehen, zeigen wir noch das folgende Resultat.

Lemma 4.20. *Für $\hat{\mathfrak{D}} \in \mathcal{D}^{\hat{\mathfrak{m}}}$ und $f \in S_{\hat{n},\hat{\mathfrak{m}}}$ gilt*

$$f(\hat{\mathfrak{D}})^{\frac{q^r-1}{\hat{n}}} = g(\mathrm{Con}_{\hat{F}|F}(\mathcal{N}_{\hat{F}|F}\hat{\mathfrak{D}}))^{-q^{-1}}.$$

Beweis. Wir benutzen die Paarung

$$\begin{aligned} \pi_{\hat{n},\hat{\mathfrak{m}}} : S_{\hat{n},\hat{\mathfrak{m}}}/(\hat{F}^\times)^{\hat{n}} \times \mathcal{C}\ell_{\hat{\mathfrak{m}}}/\hat{n}\mathcal{C}\ell_{\hat{\mathfrak{m}}} &\to \mu_{\hat{n}} \\ (\bar{f}, \overline{[\hat{\mathfrak{D}}]}) &\mapsto f(\hat{\mathfrak{D}})^{\frac{q^r-1}{\hat{n}}} = \frac{\tau_{\hat{\mathfrak{D}}}(y)}{y} \end{aligned}$$

wobei $y^{\hat{n}} = f$ und $\tau_{\hat{\mathfrak{D}}} = (\hat{\mathfrak{D}}, \hat{F}_{\hat{H}}|\hat{F}) = (\mathcal{N}_{\hat{F}|F}\hat{\mathfrak{D}}, \hat{F}_{\hat{H}}|F)$. Sei nun $\mathfrak{D} := \mathcal{N}_{\hat{F}|F}\hat{\mathfrak{D}}$ und $\sigma_{\mathfrak{D}} = (\mathfrak{D}, \hat{F}_{\hat{H}}|F)$. Dann ist $\sigma_{\mathfrak{D}} = \tau_{\hat{\mathfrak{D}}} \in \mathrm{Gal}(\hat{F}_{\hat{H}}|\hat{F})$ und wie in Lemma 4.18 ist $\tau_{\hat{\mathfrak{D}}}$ dann gegeben durch $\tau_{\hat{\mathfrak{D}}}y = \zeta_{\hat{\mathfrak{D}}}y$ mit $\zeta_{\hat{\mathfrak{D}}} = g(\mathrm{Con}_{\hat{F}|F}\mathfrak{D})^{-q^{-1}}$. Also erhalten wir

$$f(\hat{\mathfrak{D}})^{\frac{q^r-1}{\hat{n}}} = \frac{\tau_{\hat{\mathfrak{D}}}(y)}{y} = \zeta_{\hat{\mathfrak{D}}} = g(\mathrm{Con}_{\hat{F}|F}(\mathcal{N}_{\hat{F}|F}\hat{\mathfrak{D}}))^{-q^{-1}},$$

was zu beweisen war. □

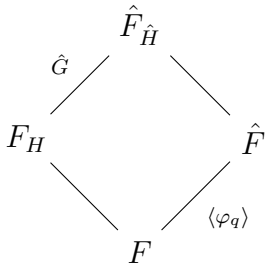
Der Klassenkörper zu H

Endlich sind wir in der Lage, den Klassenkörper zu H zu definieren und den Existenzsatz im Fall $\mu_n \nsubseteq F$ zu beweisen.

Satz 4.21 (Existenzsatz im Fall $\mu_n \nsubseteq F$)**.** *Es sei ein globaler Funktionenkörper $F|\mathbb{F}_q$ und eine natürliche Zahl n mit $\mathrm{ggT}(n,q) = 1$ gegeben. Zu jeder Untergruppe H einer Strahlklassengruppe $\mathcal{C}\ell_{\mathfrak{m}}$ vom Index n existiert der Klassenkörper. Umgekehrt existiert zu jeder endlichen abelschen Erweiterung $E|F$ vom Grad n ein $\mathfrak{m}$ und ein $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ so dass E der Klassenkörper zu H ist.*

Im Gegensatz zum Kummer-Fall können wir hier keine explizite Gleichung für den Klassenkörper zu H angeben. Stattdessen benutzen wir die Galoistheorie und alle in diesem Kapitel hergeleiteten Fakten und definieren den Klassenkörper zu H als Fixkörper

$$F_H := \mathrm{Fix}_{\hat{F}_{\hat{H}}}\{(\mathfrak{D}, \hat{F}_{\hat{H}}|F) \mid \mathfrak{D} \in H\}.$$



Klar ist, dass F_H ein Zwischenkörper von $\hat{F}_{\hat{H}}|F$ ist, dass die Erweiterung $\hat{F}_{\hat{H}}|F_H$ galoissch und abelsch ist und dass sie die Galoisgruppe $\mathrm{Gal}(\hat{F}_{\hat{H}}|F_H) = \hat{G} := \{(\mathfrak{D}, \hat{F}_{\hat{H}}|F) \mid \mathfrak{D} \in H\}$ hat. Zum Beweis des Satzes müssen wir jedoch die Eigenschaften der Erweiterung $F_H|F$ untersuchen.

Beweis. Existenz des Klassenkörpers. Es sei

$$E := \mathrm{Fix}_{\hat{F}_{\hat{H}}}\{(\mathfrak{D}, \hat{F}_{\hat{H}}|F) \mid \mathfrak{D} \in H\}.$$

Das ist wohldefiniert mittels Satz 4.19. Da $\hat{F}_{\hat{H}}|F$ nach Korollar 4.17 abelsch ist, ist $\hat{G}$ ein Normalteiler in $\mathrm{Gal}(\hat{F}_{\hat{H}}|F)$, also ist nach dem Hauptsatz der Galoistheorie [Bos06, Kap. 4.1 Thm. 6, S. 142] $E|F$ galoissch. Da die Automorphismen durch Einschränkung der Elemente von $\mathrm{Gal}(\hat{F}_{\hat{H}}|F)$ entstehen, ist die Erweiterung auch abelsch. Offensichtlich ist $E|F$ unverzweigt außerhalb von $\operatorname{supp}\mathfrak{m}$, da selbiges schon für die Erweiterung $\hat{F}_{\hat{H}}|F$ gilt.

Es bleibt noch zu zeigen, dass H der Kern der Artinabbildung $(\cdot, E|F) : \mathcal{C}\ell_{\mathfrak{m}} \to \mathrm{Gal}(E|F)$ ist. Für $\mathfrak{D} \in H$ gilt $(\mathfrak{D}, E|F) = (\mathfrak{D}, \hat{F}_{\hat{H}}|F)|_E = \mathrm{id}_E$ per Definition von E, also ist $H \subseteq \ker(\cdot, E|F)$. Umgekehrt sei $\mathfrak{D} \in \ker(\cdot, E|F)$, dann ist $\mathrm{id}_E = (\mathfrak{D}, E|F) = (\mathfrak{D}, \hat{F}_{\hat{H}}|F)|_E$, also $(\mathfrak{D}, \hat{F}_{\hat{H}}|F) \in \mathrm{Gal}(\hat{F}_{\hat{H}}|E) = \{(\mathfrak{D}, \hat{F}_{\hat{H}}|F) \mid \mathfrak{D} \in H\}$. Wir zeigen noch $\ker(\cdot, \hat{F}_{\hat{H}}|F) \subseteq H$, denn dann folgt sofort $\mathfrak{D} \in H$ und wir haben $H = \ker(\cdot, E|F)$ bewiesen.

Hierzu sei nun $\mathfrak{D} \in \ker(\cdot, \hat{F}_{\hat{H}}|F)$. Dann ist

$$\mathrm{id}_{\hat{F}} = (\mathfrak{D}, \hat{F}_{\hat{H}}|F)|_{\hat{F}} = (\mathfrak{D}, \hat{F}|F) = \varphi_q^{\deg \mathfrak{D}},$$

also teilt r den Grad von $\mathfrak{D}$, da φ_q die Ordnung r hat. Nun ist die Divisornorm $\mathcal{N}_{\hat{F}|F} : \mathcal{C}\ell_{\hat{\mathfrak{m}}} \to \{[\mathfrak{D}] \in \mathcal{C}\ell_{\mathfrak{m}} \mid \deg[\mathfrak{D}] \in r\mathbb{Z}\}$ nach Lemma 4.7 surjektiv, also gibt es ein $\hat{\mathfrak{D}} \in \mathcal{C}\ell_{\hat{\mathfrak{m}}}$ mit $\mathcal{N}_{\hat{F}|F}(\hat{\mathfrak{D}}) = \mathfrak{D}$ und es gilt

$$(\hat{\mathfrak{D}}, \hat{F}_{\hat{H}}|\hat{F}) = (\mathcal{N}_{\hat{F}|F}(\hat{\mathfrak{D}}), \hat{F}_{\hat{H}}|F) = (\mathfrak{D}, \hat{F}_{\hat{H}}|F) = \mathrm{id}_{\hat{F}_{\hat{H}}}$$

nach Voraussetzung. Folglich gilt $\hat{\mathfrak{D}} \in \hat{H}$, da $\hat{H}$ ja gerade der Kern von $(\cdot, \hat{F}_{\hat{H}}|\hat{F})$ war. Daraus folgt aber $\mathfrak{D} \in H$, was zu zeigen war.

Existenz des Erklärungsmoduls. Sei nun eine abelsche Erweiterung $E|F$ vom Grad n gegeben. Dann adjungieren wir wieder die n-ten Einheitswurzeln an F und auch an E und erhalten

$$\hat{F} := F(\mu_n) \text{ und } \hat{E} := E(\mu_n).$$

Der Grad $\hat{n}$ der Erweiterung $\hat{E}|\hat{F}$ ist dann ein Teiler von n und somit auch teilerfremd zu q. Außerdem ist $\hat{E}|F = E\hat{F}|F$ als Kompositum abelscher Erweiterungen wieder abelsch. Also existiert nach dem Existenzsatz für Kummererweiterungen 4.3 ein Modul $\hat{\mathfrak{m}}$ und eine Gruppe $\hat{H} \subseteq \mathcal{C}\ell_{\hat{\mathfrak{m}}}$ so dass $\hat{E}$ der Klassenkörper zu $\hat{H}$ über $\hat{F}$ ist. Es gibt eine Gruppe $\Delta \subseteq \hat{F}^\times$ mit $\hat{E} = \hat{F}_{\hat{H}} = \hat{F}(\sqrt[\hat{n}]{\Delta})$. Wir wissen auch, dass $\hat{\mathfrak{m}} = \sum_{\mathfrak{p} \in \hat{\mathcal{M}}} \mathfrak{p}$ nur Koeffizienten 1 hat und definieren $\mathfrak{m}$ als die Summe aller Stellen von F, die unter den Stellen in $\hat{\mathcal{M}}$ liegen. Dann gilt $\mathrm{Con}_{\hat{F}|F}(\mathfrak{m}) = \hat{\mathfrak{m}}$ und $\hat{E}|F$ ist außerhalb von $\operatorname{supp}\mathfrak{m}$ unverzweigt. Wir zeigen noch, dass $\varphi_q \bar{f} = \bar{f}^q$ für alle $\bar{f} \in \Delta/(\hat{F}^\times)^{\hat{n}}$,

dann haben wir für jede Fortsetzung $\hat{\varphi}_q$ von φ_q wieder eine Darstellung wie in Satz 4.13 und aus Satz 4.19 folgt, dass $\mathcal{P}_{\mathfrak{m}} \subseteq \ker(\cdot, \hat{F}_{\hat{H}}|F)$ und somit erst recht $\mathcal{P}_{\mathfrak{m}} \subseteq \ker(\cdot, E|F)$. Also ist $(\cdot, E|F) : \mathcal{C}\ell_{\mathfrak{m}} \to \mathrm{Gal}(E|F)$ wohldefiniert. Wir definieren H als Kern dieser Abbildung. Dann ist $H \subseteq \mathcal{C}\ell_{\mathfrak{m}}$ und E ist der Klassenkörper zu H über F.

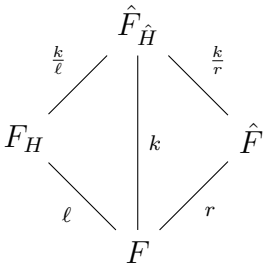
Wir zeigen also noch $\varphi_q f \equiv f^q \bmod (\hat{F}^\times)^{\hat{n}}$ für alle Erzeuger $f \in \Gamma$. Dabei sei Γ definiert wie in 4.12, es gelte also $\hat{E} = \coprod_{f\in\Gamma} \hat{F}(\sqrt[\hat{n}]{f})$. Für jede Fortsetzung $\hat{\varphi}_q$ von φ_q auf $\hat{E}$ und für jedes $f \in \Gamma$ gilt $\hat{\varphi}_q(\sqrt[\hat{n}]{f}) = \sqrt[\hat{n}]{\varphi_q f}$. Für jedes $L_f := \hat{F}(\sqrt[\hat{n}]{f})$ gilt nach dem Hauptsatz der Galoistheorie [Hes08, Satz 6.12, S. 188] $\hat{\varphi}_q|_{L_f} \in \mathrm{Gal}(L_f|\hat{F})$, also $\hat{\varphi}_q|_{L_f}(\sqrt[\hat{n}]{f}) = \sqrt[\hat{n}]{\varphi_q f} \in L_f$ und das heißt $\varphi_q f \in \langle f\rangle \cdot (\hat{F}^\times)^{\hat{n}}$. Also gilt $\varphi_q f \equiv f^\nu \bmod (\hat{F}^\times)^{\hat{n}}$ für ein $\nu \geq 1$.

Schließlich bleibt noch $\nu \equiv q \bmod \hat{n}$ zu zeigen. Wie in Satz 4.13 sieht man, dass jede Fortsetzung $\hat{\varphi}_q$ von φ_q auf $\hat{F}_{\hat{H}}$ die Gestalt $\hat{\varphi}_q(y) = y^\nu g$ hat. Da $\hat{F}_{\hat{H}}|F$ abelsch ist, kommutiert $\hat{\varphi}_q$ mit jedem $\tau \in \mathrm{Gal}(\hat{F}_{\hat{H}}|\hat{F}), \tau y = \zeta y$ für eine primitive $\hat{n}$-te Einheitswurzel ζ. Wir berechnen

$$\zeta^q y^\nu g = \hat{\varphi}_q(\zeta y) = \hat{\varphi}_q \circ \tau y = \tau \circ \hat{\varphi}_q y = \tau(y^\nu g) = \zeta^\nu y^\nu g$$

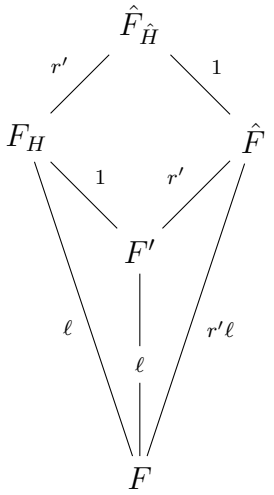
und erhalten $\nu \equiv q \bmod \hat{n}$. Damit ist alles gezeigt. □

Zum Schluss werfen wir noch einen kurzen Blick auf die Konstantenkörpererweiterungen, die die betrachteten Erweiterungen von Funktionenkörpern beinhalten. Dazu sei wieder die Gruppe H isomorph zu $H^0 \times \ell\mathbb{Z}$ und $\hat{H}$ isomorph zu $\hat{H}^0 \times \frac{k}{r}\mathbb{Z}$ für $k := \mathrm{kgV}(r, \ell)$. Dann wissen wir aus Satz 2.20, dass $F_H|F$ eine Konstantenkörpererweiterung vom Grad ℓ und $\hat{F}_{\hat{H}}|\hat{F}$ eine vom Grad $\frac{k}{r}$ beinhaltet. Außerdem wissen wir, dass $\hat{F}|F$ die Konstantenkörpererweiterung vom Grad r ist. Folglich ist der Grad der Konstantenkörpererweiterung in $\hat{F}_{\hat{H}}|F_H$ gleich $\frac{k}{\ell}$ und der von $\hat{F}_{\hat{H}}|F$ gleich k. Die jeweiligen Grade der Konstantenkörpererweiterungen sind im nebenstehenden Diagramm eingezeichnet.



An dieser Stelle sei auch noch kurz eine ähnlich aber etwas anders geartete Konstruktion erwähnt, die im Laufe dieser Arbeit untersucht wurde. Dies liegt daran, dass die Annahme $\deg(H) = 1$ uns in die Lage versetzt, einige schöne strukturelle Aussagen zu machen, die im allgemeinen Fall nicht möglich sind. Denn im Fall $\deg(H) = 1$ gilt auch $\deg(\hat{H}) = 1$ und die Erweiterung $\hat{F}_{\hat{H}}|\hat{F}$ beinhaltet dann keine Konstantenkörpererweiterung. Weiter gilt die Isomorphie $\mathcal{C}\ell_{\mathfrak{m}}/H \cong \mathcal{C}\ell_{\hat{\mathfrak{m}}}/\hat{H}$ und $\hat{H}$ hat in $\mathcal{C}\ell_{\hat{\mathfrak{m}}}$ auch denselben Index wie H in $\mathcal{C}\ell_{\mathfrak{m}}$. Dies funktioniert im Allgemeinen nicht.

Wir betrachten also die folgende Konstruktion, im nebenstehenden Diagramm sind wieder die Erweiterungsgrade der jeweiligen (exakten) Konstantenkörper eingezeichnet. Für $H \cong H^0 \times \ell\mathbb{Z}$ sei F' die Konstantenkörpererweiterung $F\mathbb{F}_{q^\ell}$ und H' die zugehörige Untergruppe $\mathcal{N}_{F'|F}^{-1}(H)$ von $\mathcal{C}\ell_{\mathfrak{m}'}$ mit $\mathfrak{m}' = \mathrm{Con}_{F'|F}(\mathfrak{m})$. Dann ist $\deg(H') = 1$. Von F' und H' aus führen wir die Konstruktion wie bisher durch und erhalten den Klassenkörper $\hat{F}_{\hat{H}}$ zu $\hat{H}$ und mit Satz 4.21 den Klassenkörper $F'_{H'}$ zu H'. Schließlich ist es leicht zu zeigen, dass $F'_{H'}$ auch der Klassenkörper F_H zu H ist (wegen $\mathcal{N}_{F'|F}(H') = H$).



Man kann auch zeigen, dass $F_H|F'$ und $\hat{F}|F'$ linear disjunkt sind, $\mathrm{Gal}(\hat{F}_{\hat{H}}|\hat{F}) \cong \mathrm{Gal}(F_H|F')$ und $\mathrm{Gal}(\hat{F}_{\hat{H}}|F_H) \cong \mathrm{Gal}(\hat{F}|F')$. Dann setzt sich die große Galoisgruppe als direktes Produkt

$$\mathrm{Gal}(\hat{F}_{\hat{H}}|F') \cong \mathrm{Gal}(\hat{F}_{\hat{H}}|F_H) \times \mathrm{Gal}(\hat{F}_{\hat{H}}|\hat{F})$$

zusammen und man erhält weitere Beschreibungen davon, indem man die eben genannten Isomorphien einsetzt. $\hat{F}_{\hat{H}}$ ist dann die Konstantenkörpererweiterung $F_H\mathbb{F}_{q^r}$ von F_H.

Mit $\mathrm{Gal}(\hat{F}|F')$ ist auch $\mathrm{Gal}(\hat{F}_{\hat{H}}|F_H)$ zyklisch von der Ordnung r und es ist leicht, einen Erzeuger letzterer Galoisgruppe anzugeben. Man wählt sich einen Divisor $\mathfrak{D} \in H'$ vom Grad 1 (dies ist nur wegen $\deg(H') = 1$ möglich) und für jedes $f \in \Gamma$ ein passendes g mit $g^n = \frac{\varphi_q f}{f^q}$ und $g(\mathrm{Con}_{\hat{F}|F'}\,\mathfrak{D}) = 1$. Dann ist die Fortsetzung $\hat{\varphi}_q$ von φ_q, definiert durch $\hat{\varphi}_q y = y^q g$ für alle y, ein Erzeuger von $\mathrm{Gal}(\hat{F}_{\hat{H}}|F_H)$. Dies kann man leicht nachrechnen.

In $\hat{F}_{\hat{H}}|\hat{F}$ findet keine Konstantenkörpererweiterung statt. Ebenso enthält $F_H|F'$ keine Konstantenkörpererweiterung. Also enthält $F_H|F$ genau die Konstantenkörpererweiterung vom Grad ℓ, wie in Satz 2.20 für den Klassenkörper zu H gefordert.

Dieser Ansatz ist sicherlich von theoretischem Interesse wegen der soeben erklärten Besonderheiten, jedoch schien es uns am Ende praktischer, alle Fälle (also auch den allgemeinen Fall $\deg(H) \neq 1$) auf einmal zu „erschlagen“, ohne erst Spezialfälle zu betrachten und dann Verallgemeinerungen durchzuführen.

Gleiches gilt für Spezialfälle wie die Annahme, dass mit einer zyklischen Erweiterung $\hat{F}_{\hat{H}}|\hat{F}$ gearbeitet wird oder dass n eine Primzahlpotenz ist. Sie verschaffen zwar vorübergehende Erleichterungen, erfordern dann aber wieder die Übertragung auf den allgemeinen Fall.

Erwähnen wollen wir in diesem Zusammenhang auch noch eine weitere ähnliche Konstruktion, die in [Coh00, Kap. 5.3] (für Zahlkörper) zu finden ist.

Leider funktioniert diese Vorgehensweise so nur, wenn n eine Primzahl ist. Die Überlegungen basieren darauf, dass man in diesem Fall sehr leicht eine Fortsetzung $\hat{\varphi}_q$ von φ_q der Ordnung r findet. Dann definiert man $\hat{G} := \langle \hat{\varphi}_q \rangle$ und $F_H := \mathrm{Fix}_{\hat{F}_{\hat{H}}}(\hat{G})$. Man erhält $\mathrm{Gal}(\hat{F}_{\hat{H}}|F_H) = \hat{G} \cong \mathrm{Gal}(\hat{F}|F)$ und eine ähnliche Struktur wie im eben erklärten Ansatz, aus der alles weitere folgt. Unsere Versuche, diesen Ansatz durch eine Art Iterationsverfahren auf Primzahlpotenzen n zu übertragen hat nicht zum Ziel geführt.

Schließlich ist es uns jedoch gelungen, den in diesem Abschnitt ausführlich präsentierten eleganten Ansatz zu finden, der ohne die gesonderte Betrachtung von Spezialfällen direkt zum Ziel führt. Zwar liefert er nicht so viel Struktur wie mögliche Spezialfälle, ist dafür aber allgemein gültig und durchaus ausreichend für unser langfristiges Ziel, nämlich den Beweis des Existenzsatzes der Klassenkörpertheorie.

4.3 Artin-Schreier-Witt-Erweiterungen

Bisher haben wir den Existenzsatz der Klassenkörpertheorie für Untergruppen vom Index n teilerfremd zu q vollständig bewiesen. Es bleibt also noch der Fall $n = p^\alpha,\ \alpha \geq 1$ für die Charakteristik p von F zu behandeln. Hierfür benötigt man die additive Kummertheorie, insbesondere Artin-Schreier-Erweiterungen und Witt-Vektoren. Damit konstruiert man eine Paarung ähnlich wie $\pi_{n,\mathfrak{m}}$ jedoch von additivem Charakter, mit der man dann einen Beweis analog zu Satz 4.3 führen kann. Da im additiven Fall die Einheitswurzeln immer automatisch im Grundkörper enthalten sind, ist eine Argumentation wie in Abschnitt 4.2 nicht mehr nötig. Trotzdem hätte die ausführliche Behandlung des Falls $n = p^\alpha$ den Rahmen dieser Arbeit gesprengt. Wir erläutern hier lediglich einige Ideen ohne Details. Dieser Abschnitt stellt auch eine gute Zusammenfassung der wichtigsten verwendeten Argumente dar.

Voraussetzungen und Notation 4.22. *Es sei F ein globaler Funktionenkörper mit exaktem Konstantenkörper $\mathbb{F}_q$ der Charakteristik p. Weiter sei ein Modul $\mathfrak{m}$ und eine Untergruppe H von $\mathcal{C}\ell_\mathfrak{m}$ vom Index $n = p^\alpha$ mit $\alpha \geq 1$ gegeben. Wir wollen den Klassenkörper dazu konstruieren.*

Wir bezeichnen mit R einen beliebigen (kommutativen) Ring und mit $W_\alpha(R)$ den Ring der Witt-Vektoren der Länge α über R, wie von Witt selbst in [Wit37] eingeführt. Modernere Fassungen der Witt-Vektoren-Theorie sind unter anderem nachzulesen in [Bos06, Kap. 4.10] und [Ser79, Kap. 2.6]. Die Elemente von $W_\alpha(R)$ sind Tupel $(w_0, \ldots, w_{\alpha-1}) \in R^\alpha$. Polynome S_i und P_i aus $\mathbb{Z}[X_0, Y_0, X_1, Y_1, \ldots, X_{\alpha-1}, Y_{\alpha-1}]$ definieren darauf eine Addition bzw.

Multiplikation

$$\begin{aligned} v+w &= (S_0(v,w), S_1(v,w), \ldots, S_{\alpha-1}(v,w)) \\ v\cdot w &= (P_0(v,w), P_1(v,w), \ldots, P_{\alpha-1}(v,w)), \end{aligned}$$

wodurch $W_\alpha(R)$ zum Ring wird. Weiter sei φ_p die komponentenweise Frobeniusabbildung

$$\varphi_p(w_0, \ldots, w_{\alpha-1}) = (w_0^p, \ldots, w_{\alpha-1}^p).$$

Für $\alpha = 1$ erhält man $W_\alpha(R) = R$ und φ_p ist der gewöhnliche Frobenius.

Für die Kummertheorie wählen wir nun $R := \bar{F}$ als den separablen Abschluss von F und definieren

$$\begin{aligned} \wp : W_\alpha(\bar{F}) &\to W_\alpha(\bar{F}) \\ w &\mapsto \varphi_p(w) - w. \end{aligned}$$

Die Abbildung $\wp$ hat den Kern $W_\alpha(\mathbb{F}_p) \cong \mathbb{Z}/p^\alpha\mathbb{Z}$ mit $W_\alpha(\mathbb{F}_p) \subseteq W_\alpha(F)$ und erfüllt auch alle weiteren notwendigen Voraussetzungen für die Kummertheorie. Der (allgemeine) Hauptsatz der Kummertheorie liefert also eine Bijektion

$$\begin{array}{ccc} \left\{ \begin{array}{c} \text{Untergruppen } \Delta \subseteq W_\alpha(F) \\ \text{mit } \wp(W_\alpha(F)) \subseteq \Delta \end{array} \right\} & \longleftrightarrow & \left\{ \begin{array}{c} \text{abelsche Erweiterungen} \\ E|F \text{ vom Exponenten } p^\alpha \end{array} \right\} \\ \Delta & \longmapsto & F(\wp^{-1}(\Delta)) \\ \wp(W_\alpha(E)) \cap W_\alpha(F) & \longmapsto & E. \end{array}$$

Dabei bedeutet $F(\wp^{-1}(\Delta))$ die komponentenweise Adjunktion aller Lösungen der Gleichungen $f = \varphi_p(w) - w$ mit $f \in \Delta$ und $w \in W_\alpha(\bar{F})$. Weiter erhält man eine nicht ausgeartete Kummerpaarung

$$\begin{aligned} \kappa_n : \Delta/\wp(W_\alpha(F)) \times \mathrm{Gal}(F(\wp^{-1}(\Delta))|F) &\to W_\alpha(\mathbb{F}_p) \\ (\bar{f}, \sigma) &\mapsto \sigma(w) - w \end{aligned}$$

für ein $w \in \wp^{-1}(f)$. Dabei operiert σ komponentenweise auf $W_\alpha(\bar{F})$.

Nun machen wir uns wieder daran, eine eigene Paarung zu definieren. Im Gegensatz zu $\pi_{n,\mathfrak{m}}$ hat sie additiven Charakter. Deshalb ersetzen wir Norm durch Spur. Die Spur auf Witt-Vektoren wird wie üblich definiert durch

$$\mathrm{Tr}_{K|\mathbb{F}_p}(w) = \sum_{i=0}^{[K:\mathbb{F}_p]-1} \varphi_p^i(w)$$

für einen endlichen Körper K. Ganz analog zu Lemma 3.4, nach der Idee von Hasse [Has35, S. 40], rechnet man leicht nach, dass

$$\sigma_{\mathfrak{D}}(w) - w = \sum_{\mathfrak{p}\in\mathcal{S}_F} v_{\mathfrak{p}}(\mathfrak{D}) \cdot \mathrm{Tr}_{F_{\mathfrak{p}}|\mathbb{F}_p}(f(\mathfrak{p}))$$

für $f = \varphi_q(w) - w$ und $\sigma_{\mathfrak{D}} = (\mathfrak{D}, F(\wp^{-1}(f))|F)$. Dabei bedeutet $f(\mathfrak{p})$ die komponentenweise Einbettung in den Restklassenkörper $F_{\mathfrak{p}}$. Also definieren wir eine Paarung

$$\begin{aligned} \theta_{p,\mathfrak{m}} : \Delta/\wp(W_\alpha(F)) \times \mathcal{D}^{\mathfrak{m}} &\to W_\alpha(\mathbb{F}_p) \\ (\bar{f}, \mathfrak{D}) &\mapsto \sum_{\mathfrak{p} \in \mathcal{S}_F} v_{\mathfrak{p}}(\mathfrak{D}) \cdot \mathrm{Tr}_{F_{\mathfrak{p}}|\mathbb{F}_p}(f(\mathfrak{p})) = \sigma_{\mathfrak{D}}(w) - w. \end{aligned}$$

Wegen der Surjektivität der Artinabbildung (Tschebotarev) ist $\theta_{p,\mathfrak{m}}$ automatisch wieder im linken Argument nicht ausgeartet.

Nun bleibt noch, das Δ so zu bestimmen, dass $F(\wp^{-1}(\Delta))|F$ außerhalb von $\operatorname{supp}\mathfrak{m}$ unverzweigt ist (also als Analogon $T_{p,\mathfrak{m}}/\wp(W_\alpha(F))$ zur Selmergruppe $S_{n,\mathfrak{m}}/(F^\times)^n$). Die Kriterien dafür, welche Stellen in solchen Erweiterungen verzweigen, sind nachzulesen in [Sch37], für den Fall $\alpha = 1$ auch in [Sti93, Prop. III.7.8, S. 115]. In letzterem Fall wäre eine Definition der Art

$$T_{p,\mathfrak{m}} := \{f \in F^+ \mid \forall\, \mathfrak{p} \notin \operatorname{supp}\mathfrak{m}\ \exists\, z \in F : v_{\mathfrak{p}}(f - (z^p - z)) \geq 0\}$$

denkbar. Außerdem ist zu zeigen, dass für ein solches Δ die Gruppe $\mathcal{P}_{\mathfrak{m}}$ im rechten Kern der Paarung liegt, so dass sie auch auf $\mathcal{C}\ell_{\mathfrak{m}}$ wohldefiniert ist. Schließlich muss man die Argumente der Paarung so anpassen, dass sie auch im rechten Argument nicht ausgeartet wird (insbesondere noch durch den rechten Kern faktorisieren), zum Beispiel durch einen Kardinalitätsvergleich wie in Lemma 3.3. Für den unverzweigten Fall geschieht dies bereits in [HW36]. Wir gehen hierauf nicht weiter ein.

Gehen wir jedoch davon aus, dass wir eine nicht ausgeartete Paarung haben, sagen wir auf einer „Selmergruppe“ $T_{p,\mathfrak{m}}/\wp(W_\alpha(F))$ und einer Gruppe der Form $\mathcal{C}\ell_{\mathfrak{m}}/p^\alpha\mathcal{C}\ell_{\mathfrak{m}}$, so können wir nun wieder durch eine Abbildung

$$H \mapsto \Delta_H \mapsto F_H := F(\wp^{-1}(\Delta_H))$$

den Klassenkörper F_H zu H definieren. Umgekehrt gilt: Ist H der rechte Kern der Paarung $\theta_{p,\mathfrak{m}}$ für ein $\Delta \subseteq T_{p,\mathfrak{m}}$, so ist die induzierte Paarung

$$\Delta/\wp(W_\alpha(F)) \times \mathcal{C}\ell_{\mathfrak{m}}/H \to W_\alpha(\mathbb{F}_p)$$

nicht ausgeartet und $F(\wp^{-1}(\Delta))$ der Klassenkörper zu H. So lässt sich dann auch die umgekehrte Richtung, also die Bestimmung der Gruppe H zu gegebener Erweiterung (vom Grad p^α), bewältigen.

4.4 Beliebige abelsche Erweiterungen

Endlich können wir die bisher betrachteten Fälle zusammenbauen, um den Existenzsatz für Untergruppen H von $\mathcal{C}\ell_{\mathfrak{m}}$ von ganz beliebigem Index n zu zeigen. Dies ist nicht mehr schwierig, man zerlegt lediglich das n in einen Faktor

teilerfremd zu q und einen Faktor p^α, bildet nach der bekannten Theorie zwei Klassenkörper und nimmt dann das Kompositum davon. In der umgekehrten Richtung wird eine Erweiterung ebenso in zwei linear disjunkte Erweiterungen zerlegt, zu denen wir die Gruppen H bestimmen können, und dann der Schnitt dieser Gruppen gebildet.

Satz 4.23 (Existenzsatz)**.** *Es sei F ein globaler Funktionenkörper. Zu jedem Modul $\mathfrak{m}$ von F und jeder Untergruppe H von $\mathcal{C}\ell_\mathfrak{m}$ von endlichem Index existiert der Klassenkörper. Zu jeder endlichen abelschen Erweiterung $E|F$ existiert ein $\mathfrak{m}$ und ein $H \subseteq \mathcal{C}\ell_\mathfrak{m}$ so dass E der Klassenkörper zu H ist.*

Beweis. Existenz des Klassenkörpers. Es sei p die Charakteristik von F. Der Hauptsatz über endlich erzeugte abelsche Gruppen liefert für gegebenes $H \subseteq \mathcal{C}\ell_\mathfrak{m}$ vom Index n

$$\mathcal{C}\ell_\mathfrak{m}/H \cong \prod_{i=1}^{\ell} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

für (nicht notwendigerweise verschiedene) Primzahlen p_i mit $n = \prod_{i=1}^{\ell} p_i^{e_i}$. Wir sortieren so um, dass wir

$$\mathcal{C}\ell_\mathfrak{m}/H \cong \prod_{i=1}^{k} \mathbb{Z}/p_i^{e_i}\mathbb{Z} \times \prod_{i=k+1}^{\ell} \mathbb{Z}/p^{e_i}\mathbb{Z} =: A \times B$$

erhalten, wobei die Primzahlen im linken Teil teilerfremd zu p seien. Dann sind $A \times \prod_{i=k+1}^{\ell}\{0\}$ und $\prod_{i=1}^{k}\{0\} \times B$ zwei Untergruppen von $\mathcal{C}\ell_\mathfrak{m}/H$. Da die Untergruppen von $\mathcal{C}\ell_\mathfrak{m}/H$ genau den Zwischengruppen $H \subseteq H_j \subseteq \mathcal{C}\ell_\mathfrak{m}$ entsprechen (und zwar inklusionsumkehrend), erhalten wir zwei Zwischengruppen H_1 und H_2 mit $\mathcal{C}\ell_\mathfrak{m}/H_1 \cong A \times \{0\} \cong A$ und $\mathcal{C}\ell_\mathfrak{m}/H_2 \cong \{0\} \times B \cong B$. Es gilt $\mathcal{C}\ell_\mathfrak{m}/H \cong \mathcal{C}\ell_\mathfrak{m}/H_1 \times \mathcal{C}\ell_\mathfrak{m}/H_2$ und folglich $H = H_1 \cap H_2$.

H_1 hat den Index $n_1 = \prod_{i=1}^{k} p_i^{e_i}$ in $\mathcal{C}\ell_\mathfrak{m}$. Das ist teilerfremd zu q, also existiert nach den Sätzen 4.3 und 4.21 der Klassenkörper F_1 zu H_1. Ebenso hat H_2 den Index $n_2 = \prod_{i=k+1}^{\ell} p^{e_i} = p^\alpha$ in $\mathcal{C}\ell_\mathfrak{m}$. Deshalb existiert nach Abschnitt 4.3 der Klassenkörper F_2 zu H_2.

Da die Grade von F_1 und F_2 teilerfremd sind, gilt $F_1 \cap F_2 = F$ und wir erhalten

$$\mathrm{Gal}(F_1F_2|F) \cong \mathrm{Gal}(F_1|F) \times \mathrm{Gal}(F_2|F) \cong \mathcal{C}\ell_\mathfrak{m}/H_1 \times \mathcal{C}\ell_\mathfrak{m}/H_2 \cong \mathcal{C}\ell_\mathfrak{m}/H.$$

Die Isomorphien sind wieder gegeben durch die entsprechenden Artinsymbole, und das Kompositum F_1F_2 ist der Klassenkörper zu H.

Existenz des Erklärungsmoduls. Ist nun $E|F$ vom Grad n gegeben, so zerlegen wir E in zwei linear disjunkte Erweiterungen F_1 vom Grad n_1

teilerfremd zu q und F_2 vom Grad $n_2 = p^\alpha$. Wieder erhalten wir mit den entsprechenden Existenzsätzen Moduln $\mathfrak{m}_1$ und $\mathfrak{m}_2$ und Untergruppen $H_1 \subseteq \mathcal{C}\ell_{\mathfrak{m}_1}$ bzw. $H_2 \subseteq \mathcal{C}\ell_{\mathfrak{m}_2}$ so dass F_1 der Klassenkörper zu H_1 und F_2 der Klassenkörper zu H_2 ist. Nach Bemerkung 2.9 können wir H_1 und H_2 wieder als Untergruppen derselben Strahlklassengruppe auffassen, und nach Lemma 2.4 ist $E = F_1F_2$ der Klassenkörper zu $H_1 \cap H_2$. □

Zum Schluss fassen wir noch einmal die wichtigsten Argumente zusammen, die wir für den Beweis des Existenzsatzes verwenden. Wir unterscheiden für den Index n von H in $\mathcal{C}\ell_{\mathfrak{m}}$ (bzw. den Grad der Erweiterung $E|F$) die drei Fälle

(i) $\mathrm{ggT}(n, q) = 1,\ \mu_n \subseteq F$: Kummererweiterung

(ii) $\mathrm{ggT}(n, q) = 1,\ \mu_n \nsubseteq F$: Galoistheorie, Fixkörper

(iii) $\mathrm{ggT}(n, q) = p^\alpha$: Artin-Schreier-Witt-Erweiterung

und konstruieren den jeweiligen Klassenkörper zu H (bzw. die Untergruppe zu E). Der allgemeine Klassenkörper für beliebiges n (bzw. die Untergruppe) entsteht schließlich als ein Kompositum aus einem Klassenkörper der Form (i) oder (ii) und einem Klassenkörper der Form (iii) (bzw. als Schnitt der entsprechenden Gruppen).

Die Fälle (i) und (iii) verlaufen analog, wobei wir für (iii) nicht alle Details ausgearbeitet haben. Das wichtigste Werkzeug hierbei sind die Paarungen $\pi_{n,\mathfrak{m}}$ bzw. $\theta_{p,\mathfrak{m}}$, insbesondere die Tatsache, dass sie nicht ausgeartet sind. Dies folgt im Wesentlichen aus der Surjektivität der Artinabbildung, also dem Tschebotrevschen Dichtigkeitssatz. Bei (i) geht auch noch die Weil-Reziprozität ein, und für den Kardinalitätsvergleich von Selmergruppe und $\mathcal{C}\ell_{\mathfrak{m}}/n\mathcal{C}\ell_{\mathfrak{m}}$ der Dirichletsche Einheitensatz. Des Weiteren verwenden wir bekannte Resultate über nicht ausgeartete Paarungen auf endlichen Gruppen, insbesondere die daraus folgenden Isomorphien, und wir bedienen uns aller wichtigen Aussagen der (multiplikativen und allgemeinen) Kummertheorie. Die nicht ausgeartete Kummerpaarung spielt eine entscheidende Rolle bei der Definition der neuen Paarungen, und die Kummer-Bijektion bei der Konstruktion der Klassenkörper. Sie sind nämlich allesamt Kummer- bzw. Artin-Schreier-Witt-Erweiterungen, abgesehen vom Fall (ii). Hier verwenden wir hauptsächlich Argumente aus der Galoistheorie, insbesondere die Fixkörperbildung, um (ii) aus (i) zu folgern.

Zusammenfassung und Ausblick

Die Klassenkörpertheorie hat in ihrer 150-jährigen Geschichte zahlreiche Formen angenommen. Ihre Hauptaussagen haben sich zwar seit 1930 kaum verändert, doch wurden viele neuartige Formulierungen und Beweise gefunden. Neben der Suche nach immer neuen Ansätzen sind auch zahlreiche Verallgemeinerungen der ursprünglich für Zahlkörper entwickelten Theorie von großer Bedeutung. Sie alle haben zum besseren Verständnis verschiedener Zusammenhänge in der algebraischen Zahlentheorie beigetragen, und „you should be warned that acquaintance with only one of the approaches will deprive you of techniques and understandings reflected by the other approaches“, wie Lang [Lan70a, S. 176] so passend bemerkt.

Auch diese Arbeit präsentiert einen neuartigen Ansatz, eine sehr konkrete Methode für globale Funktionenkörper. Wir geben eine moderne Formulierung des Existenzsatzes und beweisen ihn nach klassischem Vorbild (wie beispielsweise von Lang [Lan70a] dargestellt), aber unter Verwendung moderner Mittel. Wir zeigen auch, wie die anderen wichtigen Aussagen der Klassenkörpertheorie daraus folgen und weisen auf Besonderheiten hin, die Funktionenkörper im Gegensatz zu Zahlkörpern aufweisen—manche vereinfachen ihre Handhabung, wie die Abwesenheit archimedischer Bewertungen, andere wiederum verkomplizieren sie, wie die Unendlichkeit der Divisorenklassengruppe.

Mit „modernen Mitteln“ meinen wir vor allem die Verwendung der Tatepaarung, die erst in den letzten zehn Jahren durch ihren Einsatz in der Kryptographie bekannt wurde. Überhaupt ist seitdem ein reges Interesse an Paarungen und ihren Anwendungen erwacht. Wir haben hiermit eine eher theoretische Anwendung aufgezeigt und damit zum besseren Verständnis von Paarungen auch im theoretischen Kontext der algebraischen Zahlentheorie beigetragen. Allerdings gilt unser Verfahren gerade durch die Verwendung der Tatepaarung zunächst nur für Funktionenkörper, eine Übertragung auf Zahlkörper wäre noch auszuarbeiten.

Daneben verwendet unser Ansatz noch bekannte Methoden der Algebra und Zahlentheorie, insbesondere die Galoistheorie, Kummertheorie und Dichtigkeitsargumente nach Tschebotarev, die analog auch für Zahlkörper gelten.

Im Gegensatz zu den „traditionellen“ Beweisen kommen wir hier allerdings ganz ohne analytische Methoden (L-Reihen) aus, wenn man den Beweis von

Tschebotarevs Dichtigkeitssatz als gegeben hinnimmt. Auch brauchen wir keinerlei Galoiskohomologie, Brauergruppen, Ideltheorie oder sonstige tiefgreifende Konstrukte der algebraischen Zahlentheorie. Ein Grundwissen über Paarungen und Kummertheorie vorausgesetzt ist unser Ansatz also vielleicht direkter zugänglich.

Attraktiv ist auch die Konstruktivität unserer Methode. Aus der Kryptographie ist bekannt, dass die Tatepaarung sehr effizient ausgewertet werden kann (siehe zum Beispiel [BSS05, Algo IX.1, S. 196]), und auch bei der Berechnung von (Strahl-)Klassengruppen hat sich in den letzten Jahren einiges getan (siehe zum Beispiel [Hes99], [Aue99], [Fie01], [HPP03]). In der Tat ist dieser explizite Ansatz zur Berechnung von Klassenkörpern bereits im Computeralgebrasystem Magma [BC04, Kap. 59.13] implementiert. Allerdings funktioniert der Algorithmus dort nur unter der Annahme des Existenzsatzes und liefert keinen Beweis. Dieser Beweis ist das Ergebnis der vorliegenden Arbeit.

Im Anschluss an diese Arbeit stellt sich noch die Frage, wie sich weitere bekannte Paarungen in der Klassenkörpertheorie einsetzen lassen. Die Weilpaarung zum Beispiel ist der Tatepaarung sehr ähnlich und wird auch in der Kryptographie auf analoge Weise verwendet. In [How96] findet sich bereits eine erste Interpretation der Weilpaarung im Rahmen von Kummertheorie und Klassenkörpertheorie. Das lässt hoffen, dass sie auch im theoretischen Kontext von Bedeutung ist. Auch die effizienteren Varianten Ate- und Etapaarung sind hier von Interesse, sie werden sogar definiert durch einen Ausdruck der Form $g(\mathrm{Con}_{\hat{F}|F}(\mathfrak{D}))^{q^{-1}}$, der auch bei uns in Kapitel 4.2 vorkommt.

Natürlich bleibt auch noch die detaillierte Ausarbeitung des Artin-Schreier-Witt-Falls. Trotzdem haben wir in dieser Arbeit eine neue Beweismethode für den Hauptsatz der Klassenkörpertheorie für globale Funktionenkörper aufgezeigt und über die Tatepaarung eine vielversprechende Verbindung zwischen der reinen algebraischen Zahlentheorie und ihren Anwendungen hergestellt.

Symbolverzeichnis

$(\cdot, E\|F)$	zu $E\|F$ gehörende Artinabbildung	29
$(\mathfrak{p}, E\|F)$	Frobeniusautomorphismus von $\mathfrak{p}$	29
Aut	Automorphismengruppe	
char	Charakteristik eines Körpers	
$\mathcal{C}\ell_F$	Divisorenklassengruppe von F	15
$\mathcal{C}\ell_F^0$	Nullklassengruppe von F	16
$\mathcal{C}\ell_\mathfrak{m}$	Strahlklassengruppe modulo $\mathfrak{m}$	26
$\mathrm{Con}_{E\|F}$	Conorm	40
$\mathfrak{D}$	Divisor	15
$[\mathfrak{D}]$	Divisorenklasse von $\mathfrak{D}$	15
deg	Grad einer Stelle oder eines Divisors	14
$\deg(H)$	Grad der Gruppe H	45
δ	Dirichlet-Dichtigkeit	30
Δ_H		63
$\mathcal{D}_F$	Divisorengruppe von F	15
$\mathcal{D}^\mathfrak{m} = \mathcal{D}^\mathcal{M}$	Divisoren teilerfremd zu $\operatorname{supp}\mathfrak{m} = \mathcal{M}$	26
E	Erweiterungskörper von F	16
$e(\mathfrak{P}\|\mathfrak{p})$	Verzweigungsindex von $\mathfrak{P}\|\mathfrak{p}$	17
$f(\mathfrak{P}\|\mathfrak{p})$	Trägheitsgrad von $\mathfrak{P}\|\mathfrak{p}$	17
(f)	Hauptdivisor von $f \in F^\times$	15
$\mathfrak{f}$	Führer	27
F	globaler Funktionenkörper über $\mathbb{F}_q$	13
$\hat{F}$		66
F_H	Klassenkörper zu H	37
$F^\mathfrak{m}$		26
$F_\mathfrak{m}$		26
$F_\mathfrak{p}$	Restklassenkörper von $\mathfrak{p}$	14
$\mathbb{F}_q$	endlicher Körper mit q Elementen	13
$F(\sqrt[n]{\Delta})$	Kummererweiterung von F	21
Fix	Fixkörper	
Gal	Galoisgruppe	
ggT	größter gemeinsamer Teiler	
H	Untergruppe von $\mathcal{C}\ell_\mathfrak{m}$	35

$\hat{H}$		67
Hom	Homomorphismengruppe	
id	Identitätsabbildung	
K	Konstantenkörper	13
ker	Kern einer Abbildung	
kgV	kleinstes gemeinsames Vielfaches	
κ_n	Kummerpaarung	23
$\mathcal{M}$	Träger von $\mathfrak{m}$, endliche Menge von Stellen	26
$\mathfrak{m}$	Erklärungsmodul	26
$\hat{\mathfrak{m}}$		66
mod^*		26
μ_n	Gruppe der n-ten Einheitswurzeln	
$\mathfrak{N}$	Idealnorm	28
$\mathrm{N}_{L\|K}$	Körpernorm	
n	Index von H in $\mathcal{C}\ell_{\mathfrak{m}}$ bzw. Grad der Erweiterung $E\|F$	
$\mathcal{N}_{E\|F}$	Divisornorm	39
$\mathcal{O}_{\mathfrak{p}}$	Bewertungsring der Stelle $\mathfrak{p}$	14
$\mathfrak{p}$	Stelle von F	14
$\mathfrak{P}$	Stelle eines Erweiterungskörpers von F	17
$\mathcal{P}_F$	Hauptdivisoren von F	15
$\mathcal{P}^{\mathfrak{m}}$	Hauptdivisoren teilerfremd zu $\operatorname{supp}\mathfrak{m}$	26
$\mathcal{P}_{\mathfrak{m}}$		26
ϕ	Eulersche ϕ-Funktion	
$\varphi_{\mathfrak{p}}$	Frobeniusautomorphismus $x \mapsto x^{\mathfrak{N}(\mathfrak{p})}$	28
φ_q	Frobeniusautomorphismus $x \mapsto x^q$	66
π	Paarung	18
$\pi_{n,\mathfrak{m}}$	verallgemeinerte Tatepaarung	56
$\mathbb{Q}$	rationale Zahlen	
$\mathcal{S}_F$	Menge der Stellen von F	14
$S_{n,\mathfrak{m}}/(F^\times)^n$	Selmergruppe	50
supp	Träger eines Divisors	15
$\sigma_{\mathfrak{D}}$	Frobeniusautomorphismus von $\mathfrak{D}$	29
τ_n	Tatepaarung	24
τ_n^{red}	reduzierte Tatepaarung	25
$\mathrm{Tr}_{L\|K}$	Spur	
$U_{\mathcal{M}}$	$\mathcal{M}$-Einheiten	51
$v_{\mathfrak{p}}$	zu $\mathfrak{p}$ gehörende exponentielle Bewertung	14
$\mathbb{Z}$	ganze Zahlen	
ζ	(primitive) n-te Einheitswurzel	

Literaturverzeichnis

[Art27] Artin, E.: *Beweis des allgemeinen Reziprozitätsgesetzes.* Abh. Math. Semin. Univ. Hamb., 5(1):353–363, 1927.

[AT67] Artin, E. und J. Tate: *Class Field Theory.* Benjamin, New York-Amsterdam, 1967.

[Aue99] Auer, R.: *Ray Class Fields of Global Function Fields with Many Rational Places.* PhD Thesis, Carl-von-Ossietzky-Universität Oldenburg, 1999.

[BC04] Bosma, W. und J. Cannon (Herausgeber): *Handbook of Magma Functions.* Version 2.11. 2004.

[Bos06] Bosch, S.: *Algebra.* 6. Aufl. Springer-Verlag, Berlin-Heidelberg-New York, 2006.

[Bou03] Bourbaki, N.: *Algebra II. Chapters 4–7.* Springer-Verlag, Berlin-Heidelberg-New York, 2003.

[BSS05] Blake, I. F., G. Seroussi und N. P. Smart (Herausgeber): *Advances in Elliptic Curve Cryptography.* Cambridge University Press, Cambridge, 2005.

[CF67] Cassels, J. und A. Fröhlich: *Algebraic Number Theory.* Academic Press, New York-London, 1967.

[Che54] Chevalley, C.: *Class Field Theory.* Nagoya University, Nagoya, 1954.

[Coh00] Cohen, H.: *Advanced Topics in Computational Number Theory.* Springer-Verlag, Berlin-Heidelberg-New York, 2000.

[Fie01] Fieker, C.: *Class Fields via the Artin Map.* Math. Comp., 70(235):1293–1303, 2001.

[FJ86] Fried, M. D. und M. Jarden: *Field Arithmetic.* Springer-Verlag, Berlin-Heidelberg-New York, 1986.

[FR94] Frey, G. und H.-G. Rück: *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves.* Math. Comp., 62(206):865–874, 1994.

[Gra03] Gras, G.: *Class Field Theory. From Theory to Practice.* Springer-Verlag, Berlin-Heidelberg-New York, 2003.

[Hal90] Halter-Koch, F.: *A note on ray class fields of global fields*. Nagoya Math. J., 120:61–66, 1990.

[Has35] Hasse, H.: *Theorie der relativ-zyklischen algebraischen Funktionenkörper, insbesondere bei endlichem Konstantenkörper*. J. reine angew. Math., 172:37–54, 1935.

[Has66] Hasse, H.: *Geschichte der Klassenkörpertheorie*. Jahresbericht DMV, 68:166(80)–181(95), 1966.

[Hes99] Hess, F.: *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*. Dissertation, Technische Universität Berlin, 1999.

[Hes04] Hess, F.: *A note on the Tate pairing of curves over finite fields*. Archiv der Mathematik, 82(1):28–32, 2004.

[Hes08] Hess, F.: *Skript zur Algebra I + II*. Technische Universität Berlin, 2008.

[HM10] Hess, F. und M. Massierer: *Paper without a title including a proof of the prime number theorem*. In preparation, 2010.

[How96] Howe, E. W.: *The Weil pairing and the Hilbert symbol*. Math. Ann., 305:337–392, 1996.

[HPP03] Hess, F., S. Pauli und M. Pohst: *Computing the multiplicative group of residue class rings*. Math. Comp., 72(243):1531–1548, 2003.

[HW36] Hasse, H. und E. Witt: *Zyklische unverzweigte Erweiterungskörper vom Primzahlgrade p über einem algebraischen Funktionenkörper der Charakteristik p*. Monatshefte f. Math., 43(1):477–492, 1936.

[Jan73] Janusz, G. J.: *Algebraic Number Fields*. Academic Press, New York-London, 1973.

[Lan70a] Lang, S.: *Algebraic Number Theory*. Addison-Wesley Publishing Company, Reading, Massachusetts, 1970.

[Lan70b] Langlands, R.: *Problems in the Theory of Automorphic Forms*. In: Taam, C. T. (Herausgeber): *Lectures in Modern Analysis and Applications III*, LNM 170, Seiten 18–61. Springer-Verlag, Berlin-Heidelberg-New York, 1970.

[Lan93] Lang, S.: *Algebra*. 3rd edition. Addison-Wesley Publishing Company, Reading, Massachusetts, 1993.

[Mil08] Milne, J. S.: *Class Field Theory (v4.00)*, 2008.

[Nar90] Narkiewicz, W.: *Elementary and Analytic Theory of Algebraic Numbers*. Springer-Verlag, Berlin-Heidelberg-New York, 1990.

[Neu92] Neukirch, J.: *Algebraische Zahlentheorie*. Springer-Verlag, Berlin-Heidelberg-New York, 1992.

[Poh08] POHST, M.: *Einführung in die Algebra. Vorlesung im Sommersemester 2008*. Technische Universität Berlin, 2008.

[Roq02] ROQUETTE, P.: *Class Field Theory in Characteristic p, its Origin and Development*. In: *The Proceedings of the International Conference on Class Field Theory (Tokyo)*, 2002.

[Ros02] ROSEN, M.: *Number Theory in Function Fields*. Springer-Verlag, Berlin-Heidelberg-New York, 2002.

[Sch37] SCHMID, H. L.: *Zur Arithmetik der zyklischen p-Körper*. J. reine angew. Math., 176:161–167, 1937.

[Ser79] SERRE, J.-P.: *Local Fields*. Springer-Verlag, Berlin-Heidelberg-New York, 1979.

[Ser88] SERRE, J.-P.: *Algebraic Groups and Class Fields*. Springer-Verlag, Berlin-Heidelberg-New York, 1988.

[SH96] STEVENHAGEN, P. und H. W. LENSTRA, JR.: *Chebotarëv and his Density Theorem*. Math. Intelligencer, 18(2):26–37, 1996.

[Sha89] SHAFAREVICH, I. R.: *A new proof of the Kronecker-Weber theorem*. In: *Collected Mathematical Papers*, Seiten 54–58. Springer-Verlag, Berlin-Heidelberg-New York, 1989.

[Sti93] STICHTENOTH, H.: *Algebraic Function Fields and Codes*. Springer-Verlag, Berlin-Heidelberg-New York, 1993.

[Tsc26] TSCHEBOTAREFF, N.: *Die Bestimmung der Dichtigkeit einer Menge von Primzahlen, welche zu einer gegebenen Substitutionsklasse gehören*. Math. Ann., 95:191–228, 1926.

[Vil06] VILLA SALVADOR, G. D.: *Topics in the Theory of Algebraic Function Fields*. Birkhäuser Verlag, Boston-Basel-Berlin, 2006.

[Wei73] WEIL, A.: *Basic Number Theory*. 2nd edition. Springer-Verlag, Berlin-Heidelberg-New York, 1973.

[Wit37] WITT, E.: *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*. J. reine angew. Math., 176:126–140, 1937.