DIPLOMARBEIT

Zur Arithmetik der endlichen Überlagerungen von Schemata

Angefertigt am
Mathematischen Institut

Vorgelegt der

Mathematisch-Naturwissenschaftlichen Fakultät der
Rheinischen Friedrich-Wilhelms-Universität Bonn

März 2004

Von

Armin Holschbach

Aus

Wissen/Sieg

Inhaltsverzeichnis

0 Einleitung

Schon in einer einführenden Vorlesung über algebraische Zahlentheorie lernt man (unter dem Stichwort Hilbertsche Verzweigungstheorie), dass im Falle einer Galoiserweiterung $L|K$ von Zahlkörpern Verweigungsindex $e(\mathfrak{P}|\mathfrak{p})$ und Trägheitsgrad $f(\mathfrak{P}|\mathfrak{p})$ zweier überanderliegender Primideale $\mathfrak{P} \subset \mathcal{O}_L$, $\mathfrak{p} \subset \mathcal{O}_K$ nur von dem zugrundeliegenden Primideal $\mathfrak{p}$ abhängen, nicht aber von der Wahl von $\mathfrak{P}$ über $\mathfrak{p}$. Erstaunlicherweise lässt sich diese Folgerung auch umkehren: Gilt obige Aussage für jedes Primideal $\mathfrak{p}$ von $\mathcal{O}_K$, so ist die Erweiterung $L|K$ notwendigerweise galoissch. Damit lässt sich also mit arithmetischen Methoden (d.h. hier durch Kenntnis der Verzweigungsindizes und Trägheitsgrade) feststellen, ob eine Erweiterung von Zahlkörpern galoissch ist oder nicht.

Ebenso erstaunlich mag es klingen, dass für den Beweis dieser Umkehrung analytische Methoden notwendig zu sein scheinen, zumindest ist mir kein rein algebraischer Beweis bekannt. Das Herz des Beweises ist der Satz von Čebotarev, der wiederum auf Kenntnisse über Zetafunktionen und L-Reihen beruht.

Die natürliche Verallgemeinerung von Zahlkörpern bzw. ihren Ganzzahlringen sind Schemata vom endlichen Typ über $\mathbb{Z}$. Die Theorie der eindimensionalen Schemata dieser Art ist im wesentlichen die Theorie der Zahlkörper und der Funktionenkörper über einem endlichen Körper, der zweiten großen Klasse der zahlentheoretisch interessanten Körper.

Es stellt sich die Frage, ob es möglich ist, obiges Konzept der arithmetischen Beschreibung von Galoiserweiterungen/-überlagerungen auf Schemata auch höherer Dimension zu übertragen.

Die vorliegende Arbeit beschäftigt sich im wesentlichen mit eben dieser Fragestellung. Ohne zuviel verraten zu wollen: Man kann sie mit ja beantworten.

Dazu wendet sich der erste Teil der Arbeit dem Zahlkörperfall zu und versucht, dem Leser den Beweis der obigen Aussage in diesem Fall näher zu bringen, um den Weg für eine spätere Übertragung auf den allgemeinen Fall zu bereiten. Die Ausarbeitung der wesentlichen Konzepte der L-Reihen und der Beweis des Satzes von Čebotarev nehmen dabei den größten Teil dieses ersten Kapitels ein.

Kapitel 2 beschäftigt sich zunächst einmal mit der Suche nach einer Verallgemeinerung der Begrifflichkeiten des ersten Teils. Dabei werden normale Schemata vom endlichen Typ über $\mathbb{Z}$ als geeignete Äquivalente der Ganzzahlringe von Zahlkörpern erkannt, die Rolle der Erweiterungen von Ganzzahlringen übernehmen endliche dominante Morphismen, die wir als endliche Überlagerungen bezeichnen werden. Nachdem auch ein passender Begriff der Galoisüberlagerung gefunden ist, lässt sich die Verallgemeinerung in den Theoremen 2.1.3 und 2.2.7 formulieren und der leichte Teil auch direkt beweisen.

Auch der hier vorgestellte Beweis im allgemeinen Fall bedarf analytischer Methoden. Daher werden im dritten Kapitel wieder Zeta- und L-Funktionen definiert und eine Variante des Satzes von Čebotarev bewiesen. Ich richte mich in der Darstellung in diesem Kapitel im wesentlichen nach einem Übersichtsartikel von Serre ([Se65]). Mit den umfangreicheren Beweisen, die in diesem Fall notwendig sind, nimmt dieses Kapitel den größten Teil meiner Arbeit ein. Dafür ist am Ende dieses Kapitels dann aber der Hauptsatz 2.2.7 bewiesen.

Das vierte Kapitel schließlich rundet die Darstellung ab, indem einige Anwendungen des Satzes oder der Zwischenschritte zusammengestellt werden.

Danksagung

Herrn Prof. Pop gebührt mein Dank für das reizvolle Thema und die Betreuung meiner Arbeit. Ebenso möchte ich mich bei Christian Kaiser und Jakob Stix bedanken, die ich des öfteren mit mehr oder weniger sinnvollen Fragen löchern durfte. Jakob schulde ich auch ein besonderen Dank für die kompetente und immer hilfsbereite Betreuung während des gesamten Hauptstudiums sowie die kritische Durchsicht meiner Arbeit. Für letzteres danke ich gleichermaßen Igor Ronkine, in dem ich meinen Meister gefunden habe (zumindest was den Abgabetermin der Diplomarbeit angeht). Igor und Benjamin Ko will ich auch für die schöne Zeit danken, die ich an der Universität und auch außerhalb mit ihnen verbracht habe. Ich habe Eure Art des Savoir-vivre zu schätzen gelernt. Ebenso sei an dieser Stelle allen anderen gedankt, die meinen Studienalltag bereichert haben. Es wären zu viele, um sie alle aufzuzählen. Meiner Mutter, Gertrud Holschbach, und meinen Brüdern Markus, Ulrich und Volker möchte ich für den steten Rückhalt danken, den ich jederzeit bei ihnen fand. Mein tiefster Dank gilt meiner Freundin Verena Schwarzer, die mich immer unterstützt und angetrieben hat und die einfach immer für mich da war, wenn ich sie brauchte.

Teil I
Der Zahlkörperfall

1 Arithmetik von Zahlkörpererweiterungen

1.1 Die algebraische Seite

Wir wiederholen kurz die für uns wesentlichen Eigenschaften in diesem Kontext: Der Ganzzahlring $\mathcal{O}_K$ eines Zahlkörpers K ist ein Dedekindring; insbesondere hat in $\mathcal{O}_K$ jedes Ideal $\mathfrak{a}$, $\mathfrak{a} \neq (0)$ eine eindeutige Zerlegung in Primideale

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \mathfrak{p}_2^{e_2} \cdots \mathfrak{p}_r^{e_r}$$

Hat man nun eine endliche Erweiterung von Zahlkörpern $L|K$, so können wir für ein maximales Ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ auch die Primzerlegung

$$\mathfrak{p}\mathcal{O}_L = \mathfrak{P}_1^{e_1} \mathfrak{P}_2^{e_2} \cdots \mathfrak{P}_r^{e_r}$$

des Ideals $\mathfrak{p}\mathcal{O}_L$ betrachten. Die darin auftretenden Ideale sind gerade die Primideale $\mathfrak{P}_i$ von $\mathcal{O}_L$ über $\mathfrak{p}$ (d.h. die Primideale $\mathfrak{P}_i$ von $\mathcal{O}_L$ mit $\mathfrak{P}_i \cap \mathcal{O}_K = \mathfrak{p}$). Nun definiert man $e(\mathfrak{P}_i|\mathfrak{p}) = e_i$ als den Verzweigungsindex und $f(\mathfrak{P}_i|\mathfrak{p}) = f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/\mathfrak{p}]$ als den Trägheitsgrad von $\mathfrak{P}_i$ über $\mathfrak{p}$.

Damit sind wir nun bereit, unseren Haupsatz im Zahlkörperfall zu formulieren:

Theorem 1.1.1. *Sei $L|K$ eine endliche Erweiterung algebraischer Zahlkörper. $L|K$ ist genau dann galoissch, falls folgendes gilt:*

Für je zwei beliebige Primideale $\mathfrak{P}_1, \mathfrak{P}_2$ von $\mathcal{O}_L$, welche über dem gleichen Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ liegen, gilt $e(\mathfrak{P}_1|\mathfrak{p}) = e(\mathfrak{P}_2|\mathfrak{p})$ und $f(\mathfrak{P}_1|\mathfrak{p}) = f(\mathfrak{P}_2|\mathfrak{p})$.

Eine Richtung dieses Theorems ist sehr einfach und sollte dem geneigten Leser bekannt sein. Sei basiert im wesentlichen auf folgender Aussage:

Proposition 1.1.2. *Sei A ganzabgeschlossen, $K = \operatorname{Quot} A$, L eine endliche Galoiserweiterung von K mit Galoisgruppe G und B der ganze Abschluss von A in L. Sei $\mathfrak{p}$ ein maximales Ideal in A. Dann wirkt G transitiv auf der Menge der über $\mathfrak{p}$ gelegenen Primideale von B.*

Mit dieser Proposition folgt die Hin-Richtung unseres Hauptsatzes dann leicht aus der Primzerlegung von $\mathfrak{p}\mathcal{O}_L$ bzw. der Tatsache, dass die Restklassenkörper $k(\mathfrak{P}_1) = \mathcal{O}_L/\mathfrak{P}_1$ und $k(\mathfrak{P}_2) = \mathcal{O}_L/\mathfrak{P}_2$ damit konjugiert sind.

Für die Rückrichtung hingegen bedarf es analytischer Methoden, die wir im folgenden betrachten wollen.

1.2 Zetafunktionen und L-Reihen

Die *Riemannsche Zetafunktion* $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ ist wohl auch dem mit der analytischen Zahlentheorie nicht Vertrauten hinreichend bekannt. Diese Funktion ist nur ein Spezialfall einer deutlich größeren Klasse von Funktionen, die wir nun definieren:

Definition 1.2.1. *Eine* ***Dirichletreihe*** *ist eine Reihe* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *mit* $a_n \in \mathbb{C}$.

Das Konvergenzgebiet einer Dirichletreihe ist immer eine rechte Halbebene $\operatorname{Re} s > \sigma_0$ mit $\sigma_0 \in \mathbb{R} \cup \{-\infty, \infty\}$ (über das Verhalten auf dem Rand dieser Halbebene können wir aber im allgemeinen keine Aussage machen). Dies entnimmt man folgendem Lemma:

Lemma 1.2.2. *Konvergiert die Dirichletreihe* $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ *für ein* $s = s_0$*, so ist sie in der gesamten Halbebene* $\operatorname{Re} s > \operatorname{Re} s_0$ *kompakt konvergent.*

Beweis. [La94, VIII.1.1] □

Wesentliche Hilfe beim Abschätzen des Konvergenzgebietes bietet folgendes

Lemma 1.2.3. *Gibt es zu den Koeffizienten einer Dirichletreihe* $\sum \frac{a_n}{n^s}$ *Konstanten* C*,* $\sigma_1 \geq 0$*, so dass*

$$|a_1 + \ldots + a_n| \leq C n^{\sigma_1} \ \forall\, n,$$

so konvergiert die Dirichletreihe in der Halbebene $\operatorname{Re} s > \sigma_1$ *kompakt.*

Beweis. [La94, VIII.1.2] □

Aus diesen beiden Aussagen lässt sich für die Riemannsche Zetafunktion leicht folgern:

Satz 1.2.4. *Die Reihe* $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ *ist in der Halbebene* $\operatorname{Re} s > 1$ *absolut und kompakt konvergent, stellt also dort eine holomorphe Funktion dar, genannt* ***Riemannsche Zetafunktion****. Die Riemannsche Zetafunktion lässt sich in den Bereich* $\operatorname{Re} s > 0$ *holomorph fortsetzen, bis auf einen einfachen Pol bei* $s = 1$ *mit Residuum 1.*

Beweis. Dies folgt leicht durch Anwenden von Lemma 1.2.3 auf die Reihen zu $\zeta(s)$, $(1 - \frac{1}{2^{s-1}})\zeta(s)$ und $(1 - \frac{1}{3^{s-1}})\zeta(s)$ (vgl. dazu [La94, VIII.1.3]). □

Korollar 1.2.5. *Gibt es zu den Koeffizienten einer Dirichletreihe* $f := \sum \frac{a_n}{n^s}$ *Konstanten* $C > 0$*,* $0 \leq \sigma_1 < 1$ *und* $\rho \in \mathbb{C}$*,* $\rho \neq 0$*, so dass*

$$|a_1 + \ldots + a_n - n\rho| \leq C n^{\sigma_1} \ \forall\, n,$$

so konvergiert die Dirichletreihe in der Halbebene $\operatorname{Re} s > 1$ *kompakt und besitzt eine analytische Fortsetzung auf* $\operatorname{Re} s > \sigma_1$ *bis auf einen einfachen Pol mit Residuum* ρ *bei* $s = 1$.

Beweis. Betrachte $f - \rho \cdot \zeta$ und wende 1.2.3 und 1.2.4 an. □

Die Riemannsche Zetafunktion reicht uns für die folgenden Argumentationen allerdings noch nicht aus. Wir müssen ein Äquivalent für jeden beliebigen Zahlkörper K schaffen.

Definition 1.2.6. *Sei K ein Zahlkörper. Dann definieren wir die* ***Dedekindsche Zetafunktion*** *ζ_K zu K als die unendliche Summe*

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s}.$$

Dabei läuft die Summe über alle von 0 verschiedenen Ideale von $\mathcal{O}_K$, und mit $\mathfrak{N}(\mathfrak{a}) = \# \mathcal{O}_K/\mathfrak{a}$ bezeichnen wir die Norm von $\mathfrak{a}$.

Damit nicht genug: Wir brauchen darüber hinaus noch eine zweite, umfassendere Art von Funktionen:

Definition 1.2.7. *Sei K ein Zahlkörper, $\mathfrak{m} \neq 0$ ein (ganzes) Ideal in $\mathcal{O}_K$. Mit $I_{\mathfrak{m}}$ bezeichnen wir die Menge der zu $\mathfrak{m}$ primen gebrochenen Ideale $\mathfrak{a}$ von K, d.h. $v_{\mathfrak{p}}(\mathfrak{a}) = 0$ für jedes $\mathfrak{p}|\mathfrak{m}$; $P_{\mathfrak{m}}$ sei die Gruppe der gebrochenen Hauptideale (a) mit*

$$a \equiv 1 \mod m \quad \textit{und} \quad a \textit{ total positiv}^1.$$

Ein ***Dirichlet-Charakter*** mod $\mathfrak{m}$ *ist ein Charakter*

$$\chi : I_{\mathfrak{m}}/P_{\mathfrak{m}} \to \mathbb{S}^1,$$

d.h. ein Charakter $\chi : I_{\mathfrak{m}} \to \mathbb{S}^1$ mit $\chi(P_{\mathfrak{m}}) = 1$.

Zu einem Dirichlet-Charakter $\chi \bmod \mathfrak{m}$ definieren wir die ***Dirichletsche L-Reihe*** *$L(\chi, s)$ als unendliche Summe*

$$L(\chi, s) = \sum_{\mathfrak{a}} \frac{\chi(\mathfrak{a})}{\mathfrak{N}(\mathfrak{a})^s}.$$

Dabei durchläuft die Summe wiederum alle von 0 verschiedenen Ideale von $\mathcal{O}_K$, und für $(\mathfrak{a}, \mathfrak{m}) \neq 1$ setzen wir $\chi(\mathfrak{a}) = 0$.

Diese Definitionen machen natürlich nur Sinn im Bereich ihrer absoluten Konvergenz, denn wir haben die Ideale $\mathfrak{a}$ von $\mathcal{O}_K$ nicht angeordnet.

Proposition 1.2.8. *Die Dedekindsche Zetafunktion $\zeta_K(s)$ und die Dirichletsche L-Reihe $L(\chi, s)$ konvergieren für $\operatorname{Re} s > 1$ absolut, und es gelten dort die* ***Euler-Produktdarstellungen****:*

$$\begin{aligned} \zeta_K(s) &= \prod_{\mathfrak{p}} \frac{1}{1 - \frac{1}{\mathfrak{N}(\mathfrak{p})^s}} \\ L(\chi, s) &= \prod_{\mathfrak{p} \nmid \mathfrak{m}} \frac{1}{1 - \frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}} \end{aligned}$$

Dabei laufen die Produkte über alle Primideale $\mathfrak{p} \neq 0$ von $\mathcal{O}_K$.

[1] a total positiv bedeutet: $\tau a > 0$ für jede Einbettung $\tau : K \hookrightarrow \mathbb{R}$.

Beweis. Wir zeigen zunächst die absolute Konvergenz der obigen Produkte. Wegen $|1-\frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}| \geq 1-|\,\mathfrak{N}(\mathfrak{p})^{-s}| = 1-\mathfrak{N}(\mathfrak{p})^{-\sigma}$ mit $\sigma = \operatorname{Re} s$ reicht es zu zeigen, dass $\prod_\mathfrak{p}(1-\mathfrak{N}(\mathfrak{p})^{-\sigma})^{-1}$ für $\sigma > 1$ konvergiert. Zu jedem $\mathfrak{p}$ gilt für das zugrundeliegende Primideal $(p) = \mathfrak{p}\cap\mathbb{Z}$: $p\,|\,\mathfrak{N}(\mathfrak{p})$, also $1-\mathfrak{N}(\mathfrak{p})^{-\sigma} > 1-p^{-\sigma}$; und über jedem Primideal (p) von $\mathbb{Z}$ liegen höchstens $d = [K:\mathbb{Q}]$ Primideale in $\mathcal{O}_K$. Damit wird das Produkt $\prod_\mathfrak{p}(1-\mathfrak{N}(\mathfrak{p})^{-\sigma})^{-1}$ durch $\prod_p(1-p^{-\sigma})^{-d} = \zeta(\sigma)^d$ majorisiert; dies liefert uns die gewünschte absolute Konvergenz. Die Produktformel (und damit auch die Konvergenz von $\zeta_K(s)$ und $L(\chi,s)$) ergibt sich recht leicht aus der Multiplikativität von χ und $\mathfrak{N}$ und der eindeutigen Primidealzerlegung in Dedekindringen, vgl. dazu [Ne92, VII.8.1] oder [Ko97, 7.17.1]. □

Insbesondere ergibt sich für den trivialen Dirichletcharakter $\chi = 1_\mathfrak{m} \pmod{\mathfrak{m}}$:

$$L(1_\mathfrak{m}, s) = \zeta_K(s)\prod_{\mathfrak{p}|\mathfrak{m}}\left(1-\frac{1}{\mathfrak{N}(\mathfrak{p})^s}\right) \tag{1}$$

Wir wollen nun die Fortsetzbarkeit der obigen Funktionen über die Gerade $\operatorname{Re} s = 1$ hinaus, insbesondere das Verhalten bei $s = 1$, untersuchen. Wegen obiger Gleichung (1) reicht es, im folgenden nur noch Dirichlet-L-Reihen zu betrachten.

Proposition 1.2.9. *Die Dirichletschen L-Reihen $L(\chi,s)$ (und damit auch die Dedekindsche Zetafunkion) lassen sich meromorph fortsetzen in die rechte Halbebene* $\operatorname{Re} s > 1-\frac{1}{[K:\mathbb{Q}]}$. *Für $\chi \neq 1_\mathfrak{m}$ ist die Fortsetzung sogar analytisch; für $\chi = 1_\mathfrak{m}$ und daher auch für die Dedekindsche Zetafunktion ergibt als einzige Singularität ein einfacher Pol bei $s = 1$.*

Beweisidee. Sei $d = [K:\mathbb{Q}]$. Wir unterteilen zunächst $I_\mathfrak{m}$ in Nebenklassen $\mathcal{K}$ von $P_\mathfrak{m}$. Da χ auf jeder Nebenklasse immer den gleichen Wert annimmt, schreiben wir kurz $\chi(\mathcal{K}) = \chi(\mathfrak{a})$ für ein $\mathfrak{a} \in \mathcal{K}$ und

$$L(\chi,s) = \sum_\mathcal{K}\chi(\mathcal{K})\sum_{\mathfrak{a}\in\mathcal{K},\mathfrak{a}\subseteq\mathcal{O}_K}\frac{1}{\mathfrak{N}(\mathfrak{a})^s}.$$

Nun wenden wir uns den Summen $\sum_{\mathfrak{a}\in\mathcal{K},\mathfrak{a}\subseteq\mathcal{O}_K}\frac{1}{\mathfrak{N}(\mathfrak{a})^s}$ zu. Es reicht zu zeigen, dass

$$\#\{\mathfrak{a}\in\mathcal{K}|\mathfrak{a}\subseteq\mathcal{O}_K;\mathfrak{N}(\mathfrak{a})\leq n\} = \rho n + O(n^{1-\frac{1}{d}}) \tag{2}$$

mit einer von $\mathcal{K}$ unabhängigen Konstanten $\rho \in \mathbb{C}$, $\rho \neq 0$. Denn dann folgt aus Korollar 1.2.5 leicht, dass $\sum_{\mathfrak{a}\in\mathcal{K},\mathfrak{a}\subseteq\mathcal{O}_K}\frac{1}{\mathfrak{N}(\mathfrak{a})^s}$ eine in $\operatorname{Re} s > 1-\frac{1}{d}$ meromorphe Funktion mit einfachen Pol bei $s = 1$ mit Residuum ρ darstellt - und dies unabhängig von $\mathcal{K}$. Wegen

$$\sum_\mathcal{K}\chi(\mathcal{K}) = \begin{cases} h_\mathfrak{m} = \#I_\mathfrak{m}/P_\mathfrak{m} < \infty, & \text{falls } \chi = 1_\mathfrak{m},\\ 0 & \text{sonst,}\end{cases}$$

folgt daraus die Behauptung.

Wenden wir uns daher Gleichung (2) zu. Sei $\mathcal{K}$ im folgenden fest gewählt, ebenso $\mathfrak{b} \in \mathcal{K}^{-1}$. Für jedes $\mathfrak{a} \in \mathcal{K}, \mathfrak{a} \subseteq \mathcal{O}_K$ gilt $\mathfrak{a}\mathfrak{b} = (a)$ mit $(a) \in P_{\mathfrak{m}}$, $a \in \mathfrak{b}$, und umgekehrt liefert ein jedes solche a ein $\mathfrak{a} = a\mathfrak{b}^{-1} \in \mathcal{K}$, $\mathfrak{a} \subseteq \mathcal{O}_K$. Wegen $|N(a)| = \mathfrak{N}((a)) = \mathfrak{N}(\mathfrak{a})\,\mathfrak{N}(\mathfrak{b})$ gilt offenbar

$$\#\{\mathfrak{a} \in \mathcal{K} |\, \mathfrak{a} \subseteq \mathcal{O}_K; \mathfrak{N}(\mathfrak{a}) \leq n\} = \#\{a \in \mathfrak{b}^*/\mathcal{O}_K^* |\; |N(\mathfrak{a})| \leq n\,\mathfrak{N}(\mathfrak{b})\}$$

Wer die Minkowskische Gitterpunkttheorie kennt, weiß, dass die $a \in \mathfrak{b}$ als Punkte eines gewissen d-dimensionalen Gitters dargestellt werden können, und das Problem ist im wesentlich das, die Anzahl solcher Gitterpunkte in einem bestimmten Simplex zu bestimmen. Wir verweisen nun auf [La94, VI.§3]; obige Gleichung (2) samt eines genauen Terms für ρ entnimmt man [La94, VI.3.3]. □

Der Vollständigkeit halber sei noch angemerkt, dass die Dedekindsche Zetafunktion und die Dirichletschen L-Reihen sogar auf ganz $\mathbb{C}$ meromorph fortsetzbar sind und dort einer Funktionalgleichung genügen. (Wir verwenden die Fortsetzbarkeit in die Halbebene $\operatorname{Re} s > \frac{1}{2}$ auch im Kapitel 3 - allerdings hätte es keine wesentlichen Auswirkungen, wenn wir nur die Fortsetzbarkeit in eine Umgebung von $s = 1$ zeigen könnten.) Der Beweis der Fortsetzbarkeit auf $\mathbb{C}$ erfordert tiefere analytische Methoden - wir verweisen den interessierten Leser dazu auf [Ne92, VII.§1 - §8] und [La94, XIV].

Als ein für unsere spätere Argumentation wichtiges Beispiel Dirichletscher L-Reihen zeigen wir nun noch folgendes Beispiel:

Sei K ein beliebiger Zahlkörper, m eine beliebige natürliche Zahl > 0. Die Abbildung $\mathfrak{p} \mapsto \mathfrak{N}(\mathfrak{p}) \mod \mathfrak{m}$ setzt sich zu einem Morphismus $\psi : I_{m\mathcal{O}_K} \to (\mathbb{Z}/m\mathbb{Z})^\times$ fort. Ist $(a) \in P_{m\mathcal{O}_K}$, so folgt aus der totalen Positivität von a, dass $N_{K|\mathbb{Q}}(a) > 0$, und aus $a \equiv 1 \mod m\mathcal{O}_K$ folgert man leicht $\mathfrak{N}((a)) = N_{K|\mathbb{Q}}(a) \equiv 1 \mod m$; also gilt $\psi(P_{\mathfrak{m}}) = 1$. Jeder Homomorphismus $\tilde{\chi} : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{S}^1$ induziert damit einen Dirichletcharakter $\chi = \tilde{\chi} \circ \psi \mod m\mathcal{O}_K$.

Proposition 1.2.10. *Sei $L = K(\zeta_m)$, $n := [L : K]$. Dann ist n offenbar ein Teiler von $\varphi(m) = \#(\mathbb{Z}/m\mathbb{Z})^\times = [\mathbb{Q}(\zeta_m) : \mathbb{Q}]$. Durchläuft χ alle verschiedenen Dirichletcharaktere $\chi = \tilde{\chi} \circ \psi$, bei denen $\tilde{\chi} : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{S}^1$ über die zyklische Gruppe $\mu_n(\mathbb{C}) \subset \mathbb{S}^1$ faktorisiert, so gilt*

$$\prod_{\chi} L(\chi, s) = L(1_{m\mathcal{O}_L}, s) \tag{3}$$

Man beachte dabei, dass die letzte Dirichletsche L-Reihe über L definiert ist.

Beweis. Zunächst zeigen wir: Jedes in L verzweigte Primideal $\mathfrak{p}$ von $\mathcal{O}_K$ ist ein Teiler von $m\mathcal{O}_K$. Denn $\mathfrak{p}$ ist verzweigt in L genau dann, wenn $\mathfrak{p}$ die Diskriminante $\mathfrak{d}_{L|K}$ teilt ([Ne92, III.2.12]). Da $1, \zeta_m, \ldots, \zeta_m^{n-1}$ eine in $\mathcal{O}_L$ gelegene Basis von $L|K$

ist, folgt $\mathfrak{d}_{L|K} \supseteq d(1, \zeta_m, \ldots, \zeta_m^{n-1})\mathcal{O}_K$. Da $1, \zeta_m, \ldots, \zeta_m^{n-1}$ sogar eine Ganzheitsbasis von $\mathcal{O}_{\mathbb{Q}(\zeta_m)}$ über $k = K \cap \mathbb{Q}(\zeta_m)$ ist, folgt $d(1, \zeta_m, \ldots, \zeta_m^{n-1}) = d_{\mathbb{Q}(\zeta_m)|k}$. Man sieht leicht, dass $d_{\mathbb{Q}(\zeta_m)|k}\mathcal{O}_k \mid d_{\mathbb{Q}(\zeta_m)|\mathbb{Q}}\mathcal{O}_k$ (vgl. z.B. [a.a.O., III.2.10]); die Aussage folgt damit aus der bisherigen Argumentation und der Tatsache, dass alle Primteiler von $d_{\mathbb{Q}(\zeta_m)|\mathbb{Q}}$ gleichzeitig Teiler von m sind ([a.a.O., I.2.11 & I.10.1]).

Um (3) zu zeigen, reicht es, die Gleichung lokal zu beweisen, d.h. über einem in L unverzweigten Primideal $\mathfrak{p}$ von $\mathcal{O}_K$. Zu zeigen ist also

$$\prod_{\chi} \left(1 - \frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s}\right) = \prod_{\mathfrak{P}|\mathfrak{p}} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{P})^s}\right)$$

Da $L|K$ galoisch ist, ist $f(\mathfrak{P}|\mathfrak{p}) =: f$ unabhängig von $\mathfrak{P}|\mathfrak{p}$, es gilt $\mathfrak{N}(\mathfrak{P}) = \mathfrak{N}(\mathfrak{p})^f$, und die Zahl der $\mathfrak{P}$ über $\mathfrak{p}$ ist gerade $\frac{n}{f}$. Mit $y = \mathfrak{N}(\mathfrak{p})^{-s}$ und $\bar{a} = \psi(\mathfrak{p}) \in (\mathbb{Z}/m\mathbb{Z})^\times$ wird die letzte Gleichung zu

$$\prod_{\tilde{\chi}} (1 - \tilde{\chi}(\bar{a})y) = \left(1 - y^f\right)^{n/f}.$$

Um diese Gleichung zu zeigen, müssen wir noch eine weitere Beschreibung von f finden. Offenbar ist $\mathcal{O}_L/\mathfrak{P}$ die kleinste Körpererweiterung von $\mathcal{O}_K/\mathfrak{p}$, die eine primitive m-te Einheitswurzel enthält. Für einen endlichen Körper $\mathbb{F}_q$ ist $\mathbb{F}_q^\times$ gerade die Menge der $(q-1)$-ten Einheitswurzeln. Daher gilt $\zeta_m \in \mathbb{F}_q$ genau dann, wenn $m \mid q-1$, also $q \equiv 1 \mod m$. Daraus kann man ablesen, dass f die kleinste natürliche Zahl ist, für die $\mathfrak{N}(\mathfrak{p})^f \equiv 1 \mod m$ gilt, d.h. es gilt $f = \operatorname{ord} \bar{a}$. Daher durchläuft notwendigerweise $\tilde{\chi}(\bar{a})$ mit $\tilde{\chi}$ alle f-ten Einheitswurzeln, jede genau $\frac{n}{f}$ Mal. Danach ist obige Gleichung klar. □

Korollar 1.2.11. *Im obigen Kontext gilt für jedes der χ mit $\chi \neq 1_{m\mathcal{O}_K}$:*

$$L(\chi, 1) \neq 0. \tag{4}$$

Beweis. Aus (3) folgt

$$\frac{L(1_{m\mathcal{O}_L}, s)}{L(1_{m\mathcal{O}_K}, s)} = \prod_{\chi \neq 1_{m\mathcal{O}_K}} L(\chi, s).$$

Die linke Seite ist bei $s = 1$ holomorph und $\neq 0$, da sich die beiden einfachen Pole gerade aufheben. Da jeder der Faktoren auf der rechten Seite an dieser Stelle holomorph ist, folgt das Korollar. □

1.3 Der Satz von Cebotarev

Definition 1.3.1. *Sei K ein Zahlkörper, M eine Menge von Primidealen von K. Als **Dirichlet-Dichte** von M bezeichnet man - im Falle der Existenz - den Grenzwert*

$$d(M) = \lim_{s \to 1+0} \frac{\sum_{\mathfrak{p} \in M} \mathfrak{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{-s}}. \tag{5}$$

Wir versuchen, den Term im Nenner ein wenig umzuformen. Dabei schreiben wir $f(s) \sim g(s)$, wenn $f(s) - g(s)$ eine in einer Umgebung von $s = 1$ analytische Funktion ist. Wegen

$$\log \zeta_K(s) = -\sum_{\mathfrak{p}} \log(1 - \mathfrak{N}(\mathfrak{p})^{-s}) = \sum_{\mathfrak{p},m} \frac{1}{m\,\mathfrak{N}(\mathfrak{p})^{ms}} = \sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}(\mathfrak{p})^s} + \sum_{\mathfrak{p},m\geq 2} \frac{1}{m\,\mathfrak{N}(\mathfrak{p})^{ms}}$$

gilt $\log \zeta_K(s) \sim \sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}(\mathfrak{p})^s}$, denn für $s = \sigma + it$, $\sigma, t \in \mathbb{R}, \sigma > \frac{1}{2}$ gilt

$$\left| \sum_{\mathfrak{p},m\geq 2} \frac{1}{m\,\mathfrak{N}(\mathfrak{p})^{ms}} \right| \leq \sum_{\mathfrak{p},k\geq 1} \frac{2}{2k\,\mathfrak{N}(\mathfrak{p})^{2k\sigma}} = \log \zeta_K(2\sigma).$$

Da zudem $\zeta_K(s)$ einen einfachen Pol bei $s = 1$ hat, folgt schließlich

$$\sum_{\mathfrak{p}} \frac{1}{\mathfrak{N}(\mathfrak{p})^s} \sim \log \zeta_K(s) \sim \log \frac{1}{s-1}. \tag{6}$$

Wegen $\log \zeta_K(s) \longrightarrow \infty$ für $s \searrow 1$ hat also jede der obigen Funktionen einen Pol bei $s = 1$. Daher muss erstens auch der Zähler in dem Quotienten in der Definitionsgleichung (5) einen einfachen Pol bei 1 haben, damit die Dirichlet-Dichte nicht verschwindet, und zweitens könnte man jeden der Ausdrücke aus (6) als Nenner bei der obigen Definition der Dirichletreihe verwenden.

Insbesondere ändert sich die Dirichlet-Dichte einer Menge M nicht, wenn man endlich viele Primideale hinzufügt oder weglässt.

Wir werden nun im folgenden die Dichtigkeiten einiger Mengen von Primidealen berechnen, bei denen die Primideale eine Kenngröße gemeinsam haben. Dazu noch ein Hinweis zur Notation:

Sei $L|K$ eine Galoiserweiterung von Zahlkörpern mit Galoisgruppe G, sei $\mathfrak{P}$ ein unverzweigtes Primideal von $\mathcal{O}_L$ über einem Primideal $\mathfrak{p}$ von $\mathcal{O}_K$. Nach der Hilbertschen Verzweigungstheorie gibt es genau ein Element aus G, das $\mathfrak{P}$ festlässt und auf der $k(\mathfrak{P})|k(\mathfrak{p})$ als Frobenius wirkt. Dieses Element bezeichnen wir mit $(\frac{L|K}{\mathfrak{P}})$.

Für zwei Primideale $\mathfrak{P}$, $\mathfrak{P}'$ über $\mathfrak{p}$ sind $(\frac{L|K}{\mathfrak{P}})$ und $(\frac{L|K}{\mathfrak{P}'})$ konjugiert. Dies folgt leicht aus Proposition 1.1.2. Ist insbesondere G abelsch, so ist bei vorgegebenem $\mathfrak{p}$ das Element $(\frac{L|K}{\mathfrak{P}})$ unabhängig von der Wahl von $\mathfrak{P}|\mathfrak{p}$; in diesem Fall schreiben wir in Abwandlung unserer obigen Notation dafür auch $(\frac{L|K}{\mathfrak{p}})$.

Damit lässt sich der Satz formulieren, der sich als Kernstück unseres Beweises entpuppen wird.

Theorem 1.3.2 (Satz von Čebotarev). *Sei $L|K$ eine Galoiserweiterung von algebraischen Zahlkörpern, $\sigma \in \mathrm{Gal}(L|K)$. Sei $\mathcal{C}(\sigma)$ die Konjugationsklasse von σ, $M_\sigma^{L|K}$ die Menge der in L unverzweigten Primideale von $\mathcal{O}_K$, so dass es ein*

$\mathfrak{P} \in \operatorname{Spec} \mathcal{O}_L$ *gibt mit* $\mathfrak{P}|\mathfrak{p}$ *und* $(\frac{L|K}{\mathfrak{P}}) = \sigma$*. Dann hat* $M_\sigma^{L|K}$ *eine Dichte, und es gilt:*

$$d(M_\sigma^{L|K}) = \frac{\#\mathcal{C}(\sigma)}{[L:K]}.$$

Vor dem allgemeinen Beweis ist es sinnvoll, zunächst mal einen Spezialfall zu betrachten.

Satz 1.3.3 (Čebotarev-Spezialfall). *Sei* K *ein Zahlkörper,* $L = K(\zeta_m)$ *eine zyklotomische Erweiterung,* $\sigma \in G = \operatorname{Gal}(L|K)$*. Dann hat die soeben definierte Menge* $M_\sigma^{L|K}$ *eine Dichte, nämlich*

$$d(M_\sigma^{L|K}) = \frac{1}{\operatorname{ord} G}.$$

Beweis des Spezialfalls. In diesem Fall ist σ durch seine Wirkung auf ζ_m eindeutig bestimmt, also durch das $\bar{a} \in (\mathbb{Z}/m\mathbb{Z})^\times$ mit $\sigma\zeta_m = \zeta_m^a$. Andererseits wirkt σ genau dann als Frobenius auf einem Restklassenkörper $\mathcal{O}_L/\mathfrak{P}$ für ein Primideal $\mathfrak{P}|\mathfrak{p}$, wenn es dies auf dem Bild der Einheitswurzel ζ_m tut, d.h. wenn $\sigma\bar{\zeta}_m = \bar{\zeta}_m^{\mathfrak{N}(\mathfrak{p})}$. Dies ist gleichbedeutend mit $\sigma\zeta_m = \zeta_m^{\mathfrak{N}(\mathfrak{p})}$, also $\mathfrak{N}(\mathfrak{p}) \equiv a \mod m$ oder (in der Schreibweise der Konstruktion vor Proposition 1.2.10) $\psi(\mathfrak{p}) = \bar{a}$. Folglich gilt $M_\sigma^{L|K} = \{\mathfrak{p} : \psi(\mathfrak{p}) = \bar{a}\}$.

Es liegt also nahe, die obigen Dirichletschen L-Reihen einzusetzen. Analog zu obiger Argumentation (siehe (6)) erhalten wir für jeden Dirichletcharakter χ, der als Komposition eines Charakters $\tilde{\chi} : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{S}^1$ mit ψ entsteht:

$$\log L(\chi, s) = \sum_{\mathfrak{p} \nmid m\mathcal{O}_K} \sum_{\nu=1}^{\infty} \frac{\chi(\mathfrak{p})^\nu\, \mathfrak{N}(\mathfrak{p})^{-\nu s}}{\nu} \sim \sum_{\mathfrak{p} \nmid m\mathcal{O}_K} \frac{\chi(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^s} = \sum_{\bar{b} \in (\mathbb{Z}/m\mathbb{Z})^\times} \sum_{\mathfrak{p}:\psi(\mathfrak{p})=\bar{b}} \frac{\tilde{\chi}(\bar{b})}{\mathfrak{N}(\mathfrak{p})^s}.$$

Multiplizieren wir mit $\tilde{\chi}(\bar{a}^{-1})$ und summieren über alle $\tilde{\chi} : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{S}^1$, die über $\mu_n(\mathbb{C})$ mit $n := [L:K] = \operatorname{ord} G$ faktorisieren, so ergibt sich

$$\sum_{\tilde{\chi}} \tilde{\chi}(\bar{a}^{-1}) \log L(\chi, s) \sim \sum_{\tilde{\chi}} \sum_{\bar{b} \in (\mathbb{Z}/m\mathbb{Z})^\times} \tilde{\chi}(\bar{b}\bar{a}^{-1}) \sum_{\mathfrak{p}:\psi(\mathfrak{p})=\bar{b}} \frac{1}{\mathfrak{N}(\mathfrak{p})^s} = n \sum_{\mathfrak{p}:\psi(\mathfrak{p})=\bar{a}} \mathfrak{N}(\mathfrak{p})^{-s},$$

denn es gilt

$$\sum_{\tilde{\chi}} \tilde{\chi}(\bar{b}\bar{a}^{-1}) = \begin{cases} n, & \text{falls } \bar{b}\bar{a}^{-1} = 1, \\ 0 & \textit{sonst.} \end{cases}$$

Für jedes $\tilde{\chi} \neq 1$ ist $\log L(\chi, s)$ nach Proposition 1.2.10 holomorph bei 1, folglich erhalten wir

$$\log \zeta_K(s) \sim \log L(1_{m\mathcal{O}_K}, s) \sim \sum_{\tilde{\chi}} \tilde{\chi}(\bar{a}^{-1}) \log L(\chi, s) \sim \operatorname{ord} G \sum_{\mathfrak{p} \in M_\sigma^{L|K}} \mathfrak{N}(\mathfrak{p})^{-s}$$

und damit unmittelbar unsere Behauptung. □

Korollar 1.3.4 (Dirichletscher Primzahlsatz). *Sei $K = \mathbb{Q}$, a und m natürliche Zahlen mit $m > 1$ und $ggT(a, m) = 1$. Die Menge der Primzahlen p mit $p \equiv a \mod m$ hat Dirichlet-Dichte $\frac{1}{\varphi(m)}$. Insbesondere gibt es unendlich viele solcher Primzahlen.*

Beweis. Sei $L = \mathbb{Q}(\zeta_m)$. Wie im Beweis von Satz 1.3.3 gesehen, hängt der Frobenius $(\frac{L|\mathbb{Q}}{p})$ nur von $p \mod m$ ab. Sei σ der zu $\zeta_m \mapsto \zeta_m^a$ gehörige Automorphismus. Dann ist $M_\sigma^{L|\mathbb{Q}}$ gerade die Menge der Primzahlen p mit $p \equiv a \mod m$, und der obige Satz liefert die erwünschte Aussage. $\square$

Nun können wir uns auch dem Beweis des allgemeinen Falles zuwenden:

Beweis des Satzes von Cebotarev. Sei $G = \operatorname{Gal} L|K$. Wir zerlegen den Beweis in kleinere Schritte.

Schritt 1: Zunächst reduzieren wir auf den zyklischen Fall:

$$d(M_\sigma^{L|L^\sigma}) = \frac{1}{[L : L^\sigma]} \Leftrightarrow d(M_\sigma^{L|K}) = \frac{\#\mathcal{C}(\sigma)}{[L : K]} \tag{7}$$

Denn zu $\mathfrak{p} \in M_\sigma^{L|K}$ betrachte $X_{\sigma,\mathfrak{p}} = \{\mathfrak{P} \in \operatorname{Spec} \mathcal{O}_L |\ \mathfrak{P} \cap \mathcal{O}_K = \mathfrak{p}, (\frac{L|K}{\mathfrak{P}}) = \sigma\}$. Für $\mathfrak{P} \in X_{\sigma,\mathfrak{p}}$, $\tau \in G$ ist $(\frac{L|K}{\tau\mathfrak{P}}) = \tau\sigma\tau^{-1}$, also gilt $\tau\mathfrak{P} \in X_{\sigma,\mathfrak{p}} \Leftrightarrow \tau$ liegt im Zentralisator $Z(\sigma)$ von σ. Es folgt $\#X_{\sigma,\mathfrak{p}} = \frac{\#Z(\sigma)}{\#G_\mathfrak{P}} = \frac{\#G}{\#\mathcal{C}(\sigma)\#G_\mathfrak{P}} = \frac{[L:K]}{\#\mathcal{C}(\sigma)\cdot[L:L^\sigma]}$. Entsprechend erhalten wir für $\mathfrak{q} \in M_\sigma^{L|L^\sigma}$: $\#X_{\sigma,\mathfrak{q}} = 1$.

Wegen $G_\mathfrak{P} = \operatorname{Gal}(L|L^\sigma)$ gilt für $\mathfrak{q}|\mathfrak{p}, \mathfrak{q} \in M_\sigma^{L|L^\sigma}, \mathfrak{p} \in M_\sigma^{L|K}$: $f(\mathfrak{q}|\mathfrak{p}) = 1$, die Anzahl aller $\mathfrak{q} \in M_\sigma^{L|L^\sigma}$ über einem festen $\mathfrak{p} \in M_\sigma^{L|K}$ beträgt also $\frac{[L:K]}{\#\mathcal{C}(\sigma)\cdot[L:L^\sigma]}$. Wir erhalten damit

$$\sum_{\mathfrak{q}\in M_\sigma^{L|L^\sigma}} \mathfrak{N}(\mathfrak{q})^{-s} = \frac{[L : K]}{\#\mathcal{C}(\sigma) \cdot [L : L^\sigma]} \sum_{\mathfrak{p}\in M_\sigma^{L|K}} \mathfrak{N}(\mathfrak{p})^{-s};$$

falls also eine der beiden Zahlen $d(M_\sigma^{L|L^\sigma}), d(M_\sigma^{L|K})$ existiert, so auch die andere, und es gilt

$$d(M_\sigma^{L|L^\sigma}) = \frac{[L : K]}{\#\mathcal{C}(\sigma) \cdot [L : L^\sigma]}\, d(M_\sigma^{L|K})$$

Schritt 2: Sei also nun $L|K$ zyklisch, insbesondere abelsch. Sei $n = [L : K]$, p ein in L unverzweigtes Primideal, ζ_p eine primitive p-te Einheitswurzel. Dann gilt $L \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ und $K(\zeta_p) \cap L = K$, und die Galoisgruppe $H := \operatorname{Gal}(L(\zeta_p)|L)$ ist isomorph zu $(\mathbb{Z}/p\mathbb{Z})^\times$. Desweiteren gilt $\operatorname{Gal}(L(\zeta_p)|K) \cong G \times H$, der Isomorphismus entsteht auf dem ersten Faktor durch Einschränkung.

Denn: Da p in $\mathbb{Q}(\zeta_p)$ rein verzweigt ([Ne92, I.10.1]) und in L unverzweigt ist, folgt $L \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$. Damit folgt dann auch $K(\zeta_p) \cap L = K \cdot (\mathbb{Q}(\zeta_p) \cap L) = K \cdot \mathbb{Q} = K$

und $\mathrm{Gal}(L(\zeta_p)|L) = \mathrm{Gal}(L \cdot \mathbb{Q}(\zeta_p)|L) \cong \mathrm{Gal}(\mathbb{Q}(\zeta_p)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.
Zudem gilt $\mathrm{Gal}(L(\zeta_p)|K) = \mathrm{Gal}(L(\zeta_p)|K(\zeta_p)) \times \mathrm{Gal}(L(\zeta_p)|L)$, da $K(\zeta_p) \cap L = K$.
Wegen $L \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ ist $\mathrm{Gal}(L(\zeta_p)|K(\zeta_p)) = \mathrm{Gal}(L \cdot \mathbb{Q}(\zeta_p)|K \cdot \mathbb{Q}(\zeta_p)) \cong \mathrm{Gal}(L|K)$.

Schritt 3: Mit den obigen Bezeichnungen sei $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ unverzweigt in $L(\zeta_p)$, $(\frac{L(\zeta_p)|K}{\mathfrak{p}}) \cong (\sigma, \tau)$, $\sigma \in G$, $\tau \in H$, und damit $(\frac{L|K}{\mathfrak{p}}) = (\sigma, \tau)|_L = \sigma$. Nun definieren wir analog zu der Dirichlet-Dichte $d(M)$ die untere Dirichlet-Dichte $d_{\inf}(M) = \liminf_{s \to 1} \frac{\sum_{\mathfrak{p} \in M} \mathfrak{N}(\mathfrak{p})^{-s}}{\sum_{\mathfrak{p}} \mathfrak{N}(\mathfrak{p})^{-s}}$. Es gilt

$$d_{\inf}(M_\sigma^{L|K}) = d_{\inf}(\dot{\bigcup_{\tau \in H}} M_{(\sigma,\tau)}^{L(\zeta_p)|K}) \geq \sum_{\tau \in H} d_{\inf}(M_{(\sigma,\tau)}^{L(\zeta_p)|K}) \tag{8}$$

Sei nun $\sigma \in G$ fest gewählt, $H_n = \{\tau \in H; n | \operatorname{ord} \tau\}$, $\tau \in H_n$. Man prüft leicht nach, dass $< (\sigma, \tau) > \cap\ G \times \{\mathrm{id}\} = \{\mathrm{id}\}$; setzen wir also $E = L(\zeta_p)^{(\sigma,\tau)}$, so erhalten wir $E(\zeta_p) = L(\zeta_p)$. Daher ist $L(\zeta_p)|E$ zyklotomisch, nach dem Spezialfall des Cebotarev gilt also $d(M_{(\sigma,\tau)}^{L(\zeta_p)|E}) = \frac{1}{[L(\zeta_p):E]}$. Mit (7) folgt daher $d(M_{(\sigma,\tau)}^{L(\zeta_p)|K}) = \frac{1}{[L(\zeta_p):K]} = \frac{1}{\#G \cdot \#H}$. Eingesetzt in (8) ergibt dies

$$d_{\inf}(M_\sigma^{L|K}) \geq \sum_{\tau \in H_n} d_{\inf}(M_{(\sigma,\tau)}^{L(\zeta_p)|K}) = \frac{\#H_n}{\#G \cdot \#H}.$$

Nach dem folgenden Lemma können wir allerdings p so wählen, dass $\frac{\#H_n}{\#H}$ beliebig nahe bei 1 liegt. Es folgt daher $d_{\inf}(M_\sigma^{L|K}) \geq \frac{1}{\#G}$.
Definieren wir nun analog zu $d_{\inf}$ auch $d_{\sup}$, so folgt zudem

$$d_{\sup}(M_\sigma^{L|K}) = 1 - d_{\inf}(\dot{\bigcup_{\sigma' \neq \sigma}} M_{\sigma'}^{L|K}) \leq 1 - \sum_{\sigma' \neq \sigma} d_{\inf}(M_{\sigma'}^{L|K}) \leq \frac{1}{\#G}$$

und daher schließlich und letztendlich wie gewünscht

$$d(M_\sigma^{L|K}) = \frac{1}{\#G} = \frac{1}{[L:K]}. \qquad \square$$

Lemma 1.3.5. *Sei $n \in \mathbb{N}$ fest, p eine Primzahl, $H = (\mathbb{Z}/p\mathbb{Z})^\times$, $H_n = \{\tau \in H |$ n teilt $\operatorname{ord} \tau\}$. Dann kann p so gewählt werden, dass $\frac{\#H_n}{\#H}$ beliebig nahe bei 1 liegt.*

Beweis. Nach dem Dirichletschen Primzahlsatz gibt es eine Primzahl p (sogar unendlich viele) mit $p \equiv 1 \mod n^k$, $k \in \mathbb{N}$. Sei also $p = an^k + 1$, $m = p - 1 = an^k$, $a \in \mathbb{N}$. Sei $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ die Primfaktorzerlegung von n, $m = p_1^{\mu_1} \cdots p_r^{\mu_r} m'$ mit $\mathrm{ggT}(m', p_i) = 1\ \forall\ i$ ($\Rightarrow \mu_i \geq k\nu_i\ \forall\ i$). Es gilt offenbar $H \cong C_m$. Aus der Gruppentheorie ist bekannt, dass es für einen beliebigen Teiler d von m genau $\varphi(d)$ Elemente der Ordnung d gibt (nämlich gerade die Zahlen $b\frac{n}{d}$ mit $b < d$, $\mathrm{ggT}(b, d) = 1$). Damit gilt für die Anzahl der Elemente in H_n:

$$\begin{aligned}
\#H_n &= \sum_{n|d|m} \varphi(d) \geq \sum_{d|m} \varphi(d) - \sum_{i=1}^{r} \sum_{p_i^{\nu_i} \nmid d|m} \varphi(d) \\
&= m - \sum_{i=1}^{r} \sum_{d|\frac{m}{p_i^{\mu_i}} p_i^{\nu_i - 1}} \varphi(d) = m - \sum_{i=1}^{r} \frac{m}{p_i^{\mu_i - \nu_i + 1}} \\
&\geq m \left(1 - \sum_{i=1}^{r} \frac{1}{p_i^{(k-1)\nu_i}} \right)
\end{aligned}$$

Es folgt

$$1 \geq \frac{\#H_n}{\#H} \geq 1 - \frac{1}{p_1^{(k-1)\nu_1}} - \ldots - \frac{1}{p_r^{(k-1)\nu_r}},$$

für beliebig großes k und entsprechendes p liegt also $\frac{\#H_n}{\#H}$ beliebig nahe bei 1. □

Nun können wir uns dem Beweis des Theorems 1.1.1 zuwenden. Zu Beginn ein paar Notationen. Sei K ein Zahlkörper, M, N Mengen von Primidealen in K. Dann bedeute $M \dot{\subseteq} N$, dass $M - N$ endlich ist; $M \subseteq_d N$ drücke aus, dass $d(M - N) = 0$. Entsprechend seien $\doteq$ und $=_d$ definiert. Offenbar gilt

$$M \subseteq N \Rightarrow M \dot{\subseteq} N \Rightarrow M \subseteq_d N$$

Definition 1.3.6. *Sei $L|K$ eine Erweiterung von Zahlkörpern. Dann ist die* ***Kroneckermenge*** *$D(L|K)$ die Menge der Primideale $\mathfrak{p}$ von $\mathcal{O}_K$, für die es ein Primideal $\mathfrak{P} \subset \mathcal{O}_L$ über $\mathfrak{p}$ gibt mit $f(\mathfrak{P}|\mathfrak{p}) = 1$. Als* ***Zerlegungsmenge*** *$S(L|K)$ definieren wir die Menge aller in L voll zerlegten Primideale von K.*

Im Fall einer Galoiserweiterung gilt $D(L|K) \doteq S(L|K)$; wir versuchen, im folgenden die Umkehrung zu beweisen. Dazu führen wir noch zwei Notationen ein: Für eine Untergruppe H einer Gruppe G bezeichnen wir mit

$$\begin{aligned}
H^G &:= \bigcup_{\sigma \in G} H^\sigma \text{ die Vereinigung aller Konjugierten von } H, \text{ und mit} \\
H_G &:= \bigcap_{\sigma \in G} H^\sigma \text{ den Schnitt aller Konjugierten von } H.
\end{aligned}$$

Lemma 1.3.7. *Sei $N|K$ eine Galoiserweiterung von Zahlkörpern, die L als Zwischenkörper enthält. Sei $G = \mathrm{Gal}(N|K)$ und $H = \mathrm{Gal}(N|L)$. Unter Notationsmissbrauch bezeichne man mit $(\frac{N|K}{\mathfrak{Q}})$ das Urbild des Frobenius von $\mathrm{Gal}(k(\mathfrak{Q})|k(\mathfrak{p}))$ in $G_\mathfrak{Q} \subseteq G$. (Diese Menge ist auch für verzweigte Primideale $\mathfrak{Q}|\mathfrak{p}$ definiert; genau für diese besteht sie aus mehr als einem Element.) Dann gilt*

$$\begin{aligned}
D(L|K) &= \{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K | (\frac{N|K}{\mathfrak{Q}}) \cap H^G \neq \emptyset \textit{ für ein (jedes) } \mathfrak{Q} \in \operatorname{Spec} \mathcal{O}_N, \mathfrak{Q}|\mathfrak{p}\} \\
S(L|K) &= \{\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K | (\frac{N|K}{\mathfrak{Q}}) \subseteq H_G \textit{ für ein (jedes) } \mathfrak{Q} \in \operatorname{Spec} \mathcal{O}_N, \mathfrak{Q}|\mathfrak{p}\}
\end{aligned}$$

Beweis. Zunächst zu $D(L|K)$: Sei $\mathfrak{p} \in D(L|K)$, $\mathfrak{P} \subset \mathcal{O}_L$, $\mathfrak{P}|\mathfrak{p}$ mit $f(\mathfrak{P}|\mathfrak{p}) = 1$, $\mathfrak{Q} \in \operatorname{Spec} \mathcal{O}_N$ mit $\mathfrak{Q} \cap \mathcal{O}_L = \mathfrak{P}$. Wegen $k(\mathfrak{P}) = k(\mathfrak{p})$ gilt dann $(\frac{N|L}{\mathfrak{Q}}) \subseteq (\frac{N|K}{\mathfrak{Q}})$, also insbesondere $(\frac{N|K}{\mathfrak{Q}}) \cap H^G \neq \emptyset$. Gilt umgekehrt $(\frac{N|K}{\mathfrak{Q}}) \cap H^G \neq \emptyset$, so gibt es ein $\sigma \in G$ mit $(\frac{N|K}{\sigma\mathfrak{Q}}) \cap H \neq \emptyset$, also ein $h \in H$, das als Frobenius auf $k(\sigma\mathfrak{Q})|k(\mathfrak{p})$ wirkt. h operiert aber trivial auf $\mathcal{O}_L$ und damit auf $k(\mathfrak{P})$ für $\mathfrak{P} = \sigma\mathfrak{Q} \cap \mathcal{O}_L$, folglich gilt $k(\mathfrak{P}) = k(\mathfrak{p})$, also $f(\mathfrak{P}|\mathfrak{p}) = 1$ und daher $\mathfrak{p} \in D(L|K)$.

Nun zu $S(L|K)$; dazu gebrauchen wir folgende Aussage:
Sei $\mathfrak{Q} \in \operatorname{Spec} \mathcal{O}_N$, $\mathfrak{p} = \mathfrak{Q} \cap \mathcal{O}_K$, $H \backslash G / G_{\mathfrak{Q}}$ die Menge der Doppelnebenklassen $H\sigma G_{\mathfrak{Q}}$, $\sigma \in G$. Dann liefert die Abbildung $H\sigma G_{\mathfrak{Q}} \mapsto \sigma\mathfrak{Q} \cap \mathcal{O}_L$ eine Bijektion zwischen $H \backslash G / G_{\mathfrak{Q}}$ und der Menge der Primideale $X_{\mathfrak{p}}^{L|K}$ von L über $\mathfrak{p}$. Die Wohldefiniertheit und Surjektivität ist klar; zur Injektivität: Seien $\sigma, \tau \in G$ mit $\sigma\mathfrak{Q} \cap \mathcal{O}_L = \tau\mathfrak{Q} \cap \mathcal{O}_L$. Dann gibt es ein $h \in H = \operatorname{Gal}(N|L)$ mit $\sigma\mathfrak{Q} = h\tau\mathfrak{Q}$, also $\sigma^{-1}h\tau \in G_{\mathfrak{Q}}$. Nun gilt:

$$\begin{aligned}\mathfrak{p} \in S(L|K) \;&\Leftrightarrow\; \#X_{\mathfrak{p}}^{L|K} = \frac{1}{[L:K]} \;\Leftrightarrow\; \#H\backslash G/G_{\mathfrak{Q}} = \#H\backslash G \\ &\Leftrightarrow\; Hg\sigma = Hg \;\forall\, g \in G, \sigma \in G_{\mathfrak{Q}} \Leftrightarrow G_{\mathfrak{Q}} \subseteq H_G \Leftrightarrow (\frac{N|K}{\mathfrak{Q}}) \subseteq H_G \qquad \square\end{aligned}$$

Korollar 1.3.8. *Im obigen Kontext gilt*

$$D(L|K) \doteq \dot{\bigcup}_{\mathcal{C}(\sigma) \subseteq H^G} M_{\sigma}^{N|K}$$

Korollar 1.3.9. *Für eine Zahlkörpererweiterung $L|K$ hat $D(L|K)$ eine Dichte*

$$d(D(L|K)) \geq \frac{1}{[L:K]}.$$

Gleichheit gilt genau dann, wenn $L|K$ galoissch ist.

Beweis. Sei N eine Galoiserweiterung von K, die L enthält; sei G die Galoisgruppe von $N|K$, $H = \operatorname{Gal}(N|L)$. Aus obigem Lemma folgt

$$d(D(L|K)) = \sum_{\mathcal{C}(\sigma) \subseteq H^G} d(M_{\sigma}^{L|K}) = \sum_{\mathcal{C}(\sigma) \subseteq H^G} \frac{\#\mathcal{C}(\sigma)}{\#G} = \frac{\#H^G}{\#G} \geq \frac{\#H}{\#G} = \frac{1}{[L:K]}$$

Gleichheit gilt offenbar genau dann, wenn H normal in G ist, also L galoissch über K. $\square$

Korollar 1.3.10. *Sei $L|K$ eine Erweiterung von Zahlkörpern, $\tilde{L}$ die normale Hülle von $L|K$. Dann gilt $S(L|K) = S(\tilde{L}|K)$.*

Beweis. Im obigen Kontext gilt $\operatorname{Gal}(N|\tilde{L}) = H_G$, und $(H_G)_G = H_G$. $\square$

Satz 1.3.11. *Eine Erweiterung von Zahlkörpern ist genau dann galoissch, wenn $D(L|K) \doteq S(L|K)$ gilt.*

Beweis. Zu beweisen bleibt nur die Rückrichtung. Sei $\tilde{L}$ die normale Hülle von $L|K$. Aus $D(L|K) \doteq S(L|K)$ folgern wir

$$\frac{1}{[\tilde{L}:K]} = d(D(\tilde{L}|K)) = d(S(\tilde{L}|K)) = d(S(L|K)) = d(D(L|K)) \geq \frac{1}{[L:K]}$$

und damit $[\tilde{L}:L] = \frac{[\tilde{L}:K]}{[L:K]} \leq 1 \Rightarrow \tilde{L} = L$. $\square$

Damit haben wir jetzt offenbar auch die Rückrichtung unseres Theorems 1.1.1 bewiesen. Denn wenn Trägheits- und Verweigungsgrad nur von dem zugrundeliegenden Primideal abhängen, folgt aus $f(\mathfrak{P}|\mathfrak{p}) = 1$ für ein Primideal $\mathfrak{P}|\mathfrak{p}$ automatisch $f(\mathfrak{P}'|\mathfrak{p}) = 1$ für alle Primideale $\mathfrak{P}'$ über $\mathfrak{p}$. Lassen wir die endlich vielen verzweigten Primideale beiseite, so folgt $D(L|K) \doteq S(L|K)$, mit obiger Proposition also unsere Behauptung.

Teil II
Arithmetik der Überlagerungen von Schemata

2 Überlagerungen von Schemata

2.1 Definitionen und Grundlagen

Im folgenden setzen wir wesentliche Begriffe der algebraischen Geometrie im Umfang von etwa [Ha77, Kapitel II und III] als bekannt voraus.

Die erste Frage, die bei der Suche nach einer Verallgemeinerung des Satzes 1.1.1 aufkommt, ist die, was denn in dem Analogon den Zahlkörpern L und K bzw. den Ganzzahlringen $\mathcal{O}_L$ und $\mathcal{O}_K$ entsprechen soll. Wir wollen uns im folgenden dem Konzept zuwenden, an die Stelle der Ganzzahlringe zwei Schemata X und Y zusammen mit einem Morphismus $g : X \to Y$ treten zu lassen. Schnell sieht man ein, dass man es nicht bei so allgemeinen Begriffen lassen kann, sondern dass man sich einschränken muss.

Definition 2.1.1. *Wir nennen einen endlichen dominanten Morphismus $X \to Y$ irreduzibler Schemata eine **endliche Überlagerung**. Ist $K(X)|K(Y)$ zudem separabel, so nennen wir $X \to Y$ eine **endliche separable Überlagerung**.*

Eine endliche Überlagerung ist insbesondere surjektiv: Endlich dominant ist gleichbedeutend mit ganz, und für ganze Ringerweiterungen gilt *Lying Over*.

Wir werden uns im folgenden auf den Fall einer endlichen Überlagerung $g : X \to Y$ normaler Schemata beschränken. Diese Einschränkungen erscheinen durchaus einleuchtend, denn auch die Ganzzahlringe $\mathcal{O}_L$ und $\mathcal{O}_K$ waren normal, und die Körpererweiterung $L|K$ war endlich und separabel. (Insbesondere die Separabilität betrachten wir später noch einmal genauer, siehe Abschnitt 2.3.)

Mit dieser Einschränkung ist es aber noch nicht getan: Eine weitere Eigenschaft der Ganzzahlringe ist es, das sie allesamt endliche $\mathbb{Z}$-Moduln sind. Würden wir uns jetzt allerdings auf Schemata beschränken, die endlich über $\operatorname{Spec}\mathbb{Z}$ sind, hätten wir nicht viel gewonnen. Es erweist sich aber als wichtig zu fordern, dass X und Y *vom endlichen Typ* über $\mathbb{Z}$ sind. In diesem Fall ist die Dimension von X endlich, und es gilt:

Lemma 2.1.2. *Sei X ein irreduzibles Schema vom endlichen Typ über $\mathbb{Z}$, $K(X)$ der zugehörige Funktionenkörper. Dann gilt:*

$$\begin{aligned}\dim X &= \textit{Kronecker-Dimension von } K(X) \\ &= \begin{cases} \operatorname{trdeg}(K(X)|\mathbb{F}_p), & \textit{falls } \operatorname{char} K(X) = p > 0, \\ \operatorname{trdeg}(K(X)|\mathbb{Q}) + 1, & \textit{falls } \operatorname{char} K(X) = 0. \end{cases}\end{aligned} \tag{9}$$

Beweis. Es reicht, dies für $X = \operatorname{Spec} A$ zu zeigen. Gilt dies nämlich für jede affine Teilmenge, so folgt es automatisch auch für X. Nachdem Übergang zum reduzierten Schema X_{red} können wir davon ausgehen, dass A ganz ist, also $K(X) = \operatorname{Quot} A$ gilt.

- Im Falle $\operatorname{char} k(x) = p > 0$ ist A automatisch v.e.T. über $\mathbb{F}_p$. Nach dem Noetherschen Normalisierungssatz gibt es $r = \operatorname{trdeg}(K(X)|\mathbb{F}_p)$ algebraisch unabhängige Elemente $y_1, \ldots, y_r \in A$, so dass A ganz über $\mathbb{F}_p[y_1, \ldots, y_r]$ ist. Daraus folgt unmittelbar die Aussage.

- Im zweiten Fall ist A_S mit $S = \mathbb{Z} - \{0\}$ v.e.T. über $\mathbb{Q}$, also gibt es analog zum ersten Fall $r = \operatorname{trdeg}(K(X)|\mathbb{Q})$ algebraisch unabhängige Elemente $y_1, \ldots, y_r \in A_S$, so dass A_S ganz über $\mathbb{Q}[y_1, \ldots, y_r]$ ist.
  Sei $\{\xi_1, \ldots, \xi_r\}$ ein Erzeugendensystem von A als $\mathbb{Z}-$Algebra, $P_1(T)$, $P_2(T), \ldots, P_r(T) \in \mathbb{Q}[y_1, \ldots, y_r][T]$ zugehörige Hauptpolynome, so dass $P_i(\xi_i) = 0 \ \forall \ i$; $n \in \mathbb{N}$ sei der Hauptnenner aller Koeffizienten dieser Polynome (aufgefasst als Polynom in $y_1, \ldots, y_r$ und T). Dann gilt $P_i(T) \in \mathbb{Z}_n[y_1, \ldots, y_r][T]$ für alle i, die ξ_i und damit auch A_n sind also ganz über $\mathbb{Z}_n[y_1, \ldots, y_r]$; folglich gilt $\dim A = \dim A_n = \dim \mathbb{Z}_n[y_1, \ldots, y_r] = \dim \mathbb{Z}_n + r = \dim \mathbb{Z} + r = r + 1$. □

Wir wollen nun unseren Hauptsatz formulieren:

Theorem 2.1.3. *Sei $g : X \to Y$ eine endliche separable Überlagerung von normalen Schemata vom endlichen Typ über $\mathbb{Z}$. Dann sind folgende Aussagen äquivalent:*

(i) $K(X)$ ist eine Galoiserweiterung von $K(Y)$.

(ii) Für alle abgeschlossenen Punkte $y \in Y$ ist $[k(x) : k(y)]$ unabhängig von der Wahl von $x \in g^{-1}(y)$.

(iii) Es gibt eine offene Teilmenge $U \subseteq Y$, so dass für alle abgeschlossenen Punkte $y \in U$ $[k(x) : k(y)]$ unabhängig von der Wahl von $x \in g^{-1}(y)$ ist.

(i) $\Rightarrow$ *(ii)* $\Rightarrow$ *(iii)* bekommen wir - wie im Zahlkörperfall - mit Hilfe von Proposition 1.1.2 praktisch geschenkt; allerdings müssen wir uns dazu überlegen, wie eine endliche Gruppe auf einem Schema wirken kann. Dies geschieht im nächsten Abschnitt. Der schwierigere Teil der Rückrichtung nimmt dann die nächsten beiden Kapitel ein.

Ab jetzt seien, auch wenn dies nicht weiter erwähnt wird, alle Schemata vom endlichen Typ über $\mathbb{Z}$.

2.2 Endliche Gruppenwirkung auf einem Schema

Zunächst bemerken wir folgende Verallgemeinerung von Proposition 1.1.2:

Fakt 2.2.1. *Sei B ein Ring, $G \subseteq \operatorname{Aut}(B)$ eine endliche Untergruppe. Setze $A = B^G$. Dann gilt:*

- *$B|A$ ist ganz und quasi-Galoissch.*
- *Sei $\mathfrak{p} \in \operatorname{Spec} A$, $X_\mathfrak{p} = \{\mathfrak{q} \in \operatorname{Spec} B | \mathfrak{q} \cap A = \mathfrak{p}\}$. Dann gilt $X_\mathfrak{p} \neq \varnothing$, und G wirkt transitiv auf $X_\mathfrak{p}$.*

Sei nun $X = \operatorname{Spec} B$, $Y = \operatorname{Spec} A$.

- *Die Wirkung von G auf X ergibt sich wie folgt: Für $x = \mathfrak{q} \in X$ gilt $x.g = g^{-1}\mathfrak{q}$, für $U \subseteq X$ offen gilt $g^\# : \mathcal{O}(U) \to \mathcal{O}(g^{-1}(U)), t \mapsto g.t$.*
- *Die durch die Inklusion $A \hookrightarrow B$ induzierte Abbildung $p : X \to Y$ erfüllt $pg = p \,\forall\, g \in G$ und ist affin, surjektiv und abgeschlossen; Y trägt also die Quotiententopologie.*

  Die ersten beiden Aussagen sind trivial, die dritte folgt aus dem obigen; für die vierte betrachte man eine abgeschlossene Teilmenge $V(\mathfrak{b})$ von X. Wegen $p(V(\mathfrak{b})) = p(g(V(\mathfrak{b}))$ gilt $p(V(\mathfrak{b})) = \bigcup p(g(V(\mathfrak{b}))) = p(\bigcup V(g^{-1}\mathfrak{b})) = p(V(\prod g^{-1}\mathfrak{b}))$; wir können daher annehmen, dass $\mathfrak{b}$ G-stabil ist. Für $\mathfrak{a} = \mathfrak{b} \cap A$ gilt dann $p(V(\mathfrak{b})) = V(\mathfrak{a})$. Die eine Inklusion ist trivial, gilt umgekehrt $\mathfrak{q} \cap A \supseteq \mathfrak{a}$, so folgt für $b \in \mathfrak{b} : \prod_{g \in G} gb \in \mathfrak{b} \cap A = \mathfrak{a} \subseteq \mathfrak{q}$, also $gb \in \mathfrak{q}$ für ein g. Da $\mathfrak{b}$ G-stabil ist, folgt die Aussage.

- *Kategoriell gesehen ist $Y = X/G$, d.h. der Morphismus $p : X \to Y$ liefert für jedes Schema Z eine Bijektion $\operatorname{Hom}(Y, Z) \to \operatorname{Hom}(X, Z)^G, \alpha \mapsto \alpha p$.*

  Topologisch folgt die Aussage aus dem Vorangegangen; somit kann man bei der Betrachtung zum affinen Fall $Z = \operatorname{Spec} C$ übergehen, wenn man beachtet, dass für $f \in A$ gilt: $(B_f)^G = (B^G)_f$, d.h $p^{-1}(D_Y(f)) = D_X(f)$. In dem Fall folgt die Aussage aus dem kommutativen Diagramm

$$\begin{array}{ccc} \operatorname{Hom}(Y,Z) & \xrightarrow{\cong} & \operatorname{Hom}(C,A) \\ \downarrow & & \cong\downarrow \\ \operatorname{Hom}(X,Z)^G & \xrightarrow{\cong} & \operatorname{Hom}(C,B)^G \end{array}$$

Wenden wir uns nun dem allgemeinen Fall zu: Sei X ein Schema, G eine endliche Gruppe, die auf X wirkt. Man sagt, G **operiert auf zulässige Weise**[2] auf X, falls es eine Überdeckung von X durch offene affine Unterschemata gibt, die

[2]für alle SGA-Fans: *opère de façon admissible* [SGA 1, V.1.7]

invariant unter G sind. In dem Fall folgert man leicht aus den obigen Bemerkungen, dass ein Quotientenschema $Y = X/G$ existiert. Man vergleiche zu diesem Thema auch [SGA 1, Exposé V].

Damit können wir eine weitere Form der Überlagerung definieren:

Definition 2.2.2. *Sei $X \to Y$ eine endliche Überlagerung irreduzibler Schemata. Wir nennen $X|Y$ eine* ***Galoisüberlagerung****, falls es eine endliche Gruppe G gibt, die zulässig auf X operiert, so dass $X/G = Y$ gilt und G treu auf $K(X)|K(Y)$ wirkt. G heißt* ***Galoisgruppe*** *von $X|Y$.*

Wie man leicht überprüft, gibt es dann eine nichtleeres offenes Unterschema V von Y, dessen Urbild $U \subseteq X$ eine étale Galoisüberlagerung von V ist. Diese Definition stellt also ein Analogon zu den Galoiserweiterungen von Ganzzahlringen dar, in denen bekanntlich nur endlich viele Primideale verzweigt sind.

Konstruktion der normalen Hülle

Für den späteren Beweis der schwierigen Richtung benötigen wir nun noch ein Äquivalent der normalen Hülle einer Zahlkörpererweiterung, d.h. ein Schema W zusammen mit einer endlichen Gruppenwirkung G, so dass $W/G \cong Y$ und eine Untergruppe H existiert, für die $W/H \cong X$. Dazu brauchen wir zunächst eine Vorbemerkung:

Fakt 2.2.3. *Sei R ein Integritätsbereich, der endlich erzeugt ist über $\mathbb{Z}$ oder einem Körper, und sei L eine endliche Erweiterung von* $\operatorname{Quot} R$. *Dann ist der ganze Abschluss von R in L ein endlicher R-Modul.*

Beweis. [Ei99, 13.13],[EGA IV$_2$, IV.7.8.3] □

Nun leistet folgendes Lemma das Gewünschte:

Lemma 2.2.4. *Sei $g : X \to Y$ ein endlicher dominanter Morphismus von normalen Schemata v.e.T. über $\mathbb{Z}$; $K(X)|K(Y)$ sei separabel. Dann gibt es ein ganzes Schema W, mit g verträgliche* endliche *Morphismen $p_X : W \to X$ und $p_Y : W \to Y$ sowie eine endliche Gruppe G, die auf W durch Automorphismen wirkt, so dass gilt:*

- *G wirkt in zulässiger Weise auf W, und $W/G \cong Y$, die zugehörige Projektion ist gerade p_Y;*
- *Es gibt eine Untergruppe H von G, für die $W/H \cong X$ mit p_X als zugehöriger Projektion.*

Beweis. Zunächst seien $Y = \operatorname{Spec} A$ und damit auch $X = \operatorname{Spec} B$ affin. Sei L die normale Hülle von $K(X)|K(Y)$ in einem algebraischen Abschluss Ω von $K(Y)$, C der ganze Abschluss von B in L, $G = \operatorname{Gal}(L|K(Y)), H = \operatorname{Gal}(L|K(X)) \subseteq G$.

Dann gilt $C^G = C \cap K(Y) = A$, da A normal, und ebenso $C^H = C \cap K(X) = B$. $W = \operatorname{Spec} C$ und die durch $A \hookrightarrow C$ bzw. $B \hookrightarrow C$ entstehenden Morphismen p_Y und p_X leisten das Gewünschte. Bleibt nur noch zu zeigen, dass C ein endlicher B- bzw. A-Modul ist. Dies folgt aber aus dem obigem Fakt 2.2.3.

Im allgemeinen Fall beobachtet man, das sich so entstandene Schemata zusammenkleben lassen und so die allgemeine normale Hülle ergeben. □

Bemerkung 2.2.5. *Ist $K(X)|K(Y)$ galoissch, so ist der oben konstruierte Morphismus $p_X : W \to X$ ein Isomorphismus.*

Bemerkung 2.2.6. *Eine zu obigem Lemma analoge Aussage lässt sich auch dann treffen, wenn man zwei endliche dominante Morphismen $g : X \to Y$, $g' : X' \to Y$ vorgibt. In diesem Fall findet man ein ganzes Schema W mit einer zulässigen endlichen Gruppenwirkung G sowie Untergruppen H, H', so dass $W/G \cong Y$, $W/H \cong X$ und $W/H' \cong X'$.*

Beweis der einfachen Richtung

Mit dem Begriff der Gruppenwirkung bzw. der Galoisüberlagerung lässt sich unser ursprünglicher Hauptsatz noch etwas ausbauen:

Theorem 2.2.7. *Sei $g : X \to Y$ eine endliche separable Überlagerung von normalen Schemata vom endlichen Typ über $\mathbb{Z}$. Dann sind folgende Aussagen äquivalent:*

(i) *$K(X)$ ist eine Galoiserweiterung von $K(Y)$.*

(ii) *$X|Y$ ist eine Galoisüberlagerung.*

(iii) *Für alle abgeschlossenen Punkte $y \in Y$ ist $[k(x) : k(y)]$ unabhängig von der Wahl von $x \in g^{-1}(y)$.*

(iv) *Es gibt eine offene Teilmenge $U \subseteq Y$, so dass für alle abgeschlossenen Punkte $y \in U$ $[k(x) : k(y)]$ unabhängig von der Wahl von $x \in g^{-1}(y)$ ist.*

Wir wollen nun die einfachen Folgerungen beweisen:

Teilbeweis. *(i)* $\Leftrightarrow$ *(ii)*: Die Hin-Richtung ist gerade Bemerkung 2.2.5; die Rückrichtung ist trivial. *(ii)* $\Rightarrow$ *(iii)* Man sieht leicht, dass man sich oBdA auf $Y = \operatorname{Spec} A$ und $X = \operatorname{Spec} B$ affin beschränken kann. Sei G die Galoisgruppe von $K(X)|K(Y)$. Nach Proposition 1.1.2 wirkt G transitiv auf den Urbildern x jedes beliebigen Punktes $y \in \overline{Y}$, folglich sind alle Restklassenkörper $k(x), x \mapsto y$ konjugiert, also die Trägheitsgrade gleich. *(iii)* $\Rightarrow$ *(iv)* ist wiederum trivial. □

Daher ist nur noch *(iv)* $\Rightarrow$ *(ii)* offen. Diese Implikation wird uns aber dafür eine ganze Weile beschäftigen, da wir wieder einiges an Vorarbeit leisten müssen.

2.3 Inseparable Überlagerungen

Bevor wir den Beweis der Rückrichtung angehen, sollten wir uns vielleicht kurz die Frage stellen, ob der Satz nicht noch weiter verallgemeinert werden kann, indem die Forderung fallen lässt, dass $X \to Y$ ein separabler Morphismus ist, und dafür nur noch von einer normalen statt einer Galoiserweiterung $K(X)|K(Y)$ spricht.

Leider wäre ein solcher Satz falsch. Zur Konstruktion eines Gegenbeispiels benötigen wir folgendes

Lemma 2.3.1. *Seien $g : X \to Y$ eine endliche Überlagerung zweier normaler Schemata vom endlichen Typ über $\mathbb{Z}$, so dass $K(X)|K(Y)$ rein inseparabel ist. Dann gilt:*

1. *g ist als topologische Abbildung ein Isomorphismus.*
2. *Sei $x \in X$ ein beliebiger abgeschlossener Punkt, z das Bild von x in Y. Dann gilt $f(x|y) = [k(x) : k(y)] = 1$.*

Beweis.
1. OBdA seien $X = \operatorname{Spec} B$ und $Y = \operatorname{Spec} A$ affin. Für den Beweis der Aussage muss man nur zeigen, dass jeder Punkt in Y genau ein Urbild in X hat, und dafür reicht es zu beweisen, dass für ein beliebiges Primideal $\mathfrak{p} \subseteq A$ das Ideal $\sqrt{\mathfrak{p}} \subseteq B$ prim ist. Seien also $b_1, b_2 \in B$, $b_1 b_2 \in \sqrt{\mathfrak{p}}$. Dann gibt es eine Potenz $q = p^n$ von der Charakteristik p von $\operatorname{Quot} B$, so dass $b_1^q, b_2^q \in A$ und $b_1^q b_2^q \in \mathfrak{p}$. Es folgt $b_1^q \in \mathfrak{p}$ oder $b_2^q \in \mathfrak{p}$ und damit $b_1 \in \sqrt{\mathfrak{p}}$ oder $b_2 \in \sqrt{\mathfrak{p}}$.
2. Mit $K(X)|K(Y)$ ist notwendigerweise auch $k(x)|k(y)$ rein inseparabel. Da $k(y)$ als endlicher Körper aber perfekt ist, bleibt nur $k(x) = k(y)$. □

Nun können wir ein einfaches Gegenbeispiel vorbringen:

Beispiel 2.3.2. *Betrachten wir die normalen Schemata $X = \operatorname{Spec} \mathbb{F}_2[S,T]$, $Y = \operatorname{Spec} \mathbb{F}_2[S^2,T]$, $Z = \operatorname{Spec} \mathbb{F}_2[S^2+T, S^2T]$. Dann sind die durch die Inklusionen induzierten Morphismen $X \xrightarrow{g} Y \xrightarrow{h} Z$ endliche Überlagerungen; die Körpererweiterung $K(X)|K(Y)$ ist offenbar rein inseparabel, während $K(Y)|K(Z)$ galoissch ist. Nach dem, was wir bereits gezeigt haben, trifft damit die Aussage (ii) von Theorem 2.1.3 auf $Y \to Z$ zu, d.h. für alle abgeschlossenen Punkte $z \in Z$ ist $[k(y) : k(z)]$ unabhängig von der Wahl von $y \in h^{-1}(z)$. Betrachten wir obiges Lemma und die Multiplizität der Trägheitsgrade, so sehen wir ein, dass (ii) auch für die Überlagerung $X \to Z$ gilt.*

*Allerdings ist $K(X)|K(Z)$ **nicht** normal. Wir betrachten dazu das irreduzible Polynom $f(\xi) = \xi^4 - (S^2+T)\xi^2 + S^2T \in K(Z)[\xi]$: Über $K(X)$ zerfällt es in die Primfaktoren $(\xi - S)^2(\xi^2 - T)$.*

Auch wenn das Beispiel und das dazugehörende Lemma die Hoffnung auf eine einfache Erweiterung unseres Theorems auf den inseparablen Fall zerstören, haben sie doch etwas Gutes:

Zum einen bemerken wir, dass rein inseparable Überlagerungen topologisch und arithmetisch uninteressant sind. Zum anderen lässt sich zumindest eine Richtung des Satzes retten. Dabei hilft uns folgende

Proposition 2.3.3. *Sei $g : X \to Y$ eine endliche Überlagerung von ganzen Schemata. Dann faktorisiert dieser Morphismus über ein ganzes Schema $\tilde{X}$, so dass die beiden Morphismen $\pi_X : X \to \tilde{X}$ und $\tilde{g} : \tilde{X} \to Y$ ebenfalls endliche Überlagerungen sind und $K(\tilde{X})$ gerade der separable Abschluss von $K(Y)$ in $K(X)$ ist. Ist X normal, so ist auch $\tilde{X}$ normal. Wir nennen $\tilde{X}$ den* ***separablen Abschluss*** *von Y in X.*

Der separable Abschluss hat folgende universelle Eigenschaft: Sind $X \to Y$, $Z \to Y$ zwei Überlagerungen von Y, und gibt es einen endlichen dominanten Morphismus $h : X \to Z$, so existiert dazu genau ein Morphismus $\tilde{h} : \tilde{X} \to \tilde{Z}$, der folgendes Diagramm kommutativ macht:

$$\begin{tikzcd}
X \arrow[rr, "h"] \arrow[d, "\pi_X"] & & Z \arrow[d, "\pi_Z"] \\
\tilde{X} \arrow[rr, dashed, "\exists! \, \tilde{h}"'] \arrow[dr] & & \tilde{Z} \arrow[dl] \\
& Y &
\end{tikzcd}$$

Der Morphismus h ist durch $\tilde{h}$ eindeutig bestimmt.

Beweis. Zunächst der affine Fall: Sei $Y = \operatorname{Spec} A$ affin, also auch $X = \operatorname{Spec} B$. Sei $K = \operatorname{Quot} A = K(Y)$, $L = \operatorname{Quot} B = K(X)$, M der separable Abschluss von K in L. Dann definiere man $\tilde{B} = \{b \in B : b \text{ separabel über } K\} = B \cap M$. Offenbar ist $\tilde{B}$ ein Ring mit $A \subseteq \tilde{B} \subseteq B$, und $\tilde{X} = \operatorname{Spec} \tilde{B}$ erfüllt mit den durch die Inklusionen induzierten Morphismen die Aussagen der Proposition. Ist B ganz abgeschlossen, so auch $\tilde{B}$.

Sei nun $\operatorname{Spec} B = X \to Z = \operatorname{Spec} C$ ein endlicher dominanter Morphismus von endlichen Überlagerungen von $Y = \operatorname{Spec} A$. Auf Ringseite entspricht dem eine injektive Abbildung $C \hookrightarrow B$ über A. Ein über $K = \operatorname{Quot} A$ separables Element aus C wird dabei wieder auf ein über K separables Element von B abgebildet; dies induziert den Morphismus $\tilde{X} \to \tilde{Z}$. Die Eindeutigkeit von $\tilde{h}$ ist klar. Umgekehrt lässt sich aus einem so konstruierten Morphismus $\tilde{h}$ auch auf h schließen: Denn zunächst mal ist durch $\tilde{h}$ der Morphismus $h^{\#} : C \to B$ für alle $\tilde{c} \in \tilde{C} \subseteq C$ vorgegeben. Zu jedem $c \in C$ existiert aber eine Potenz p^n mit $p = \operatorname{char} K$, so dass $\tilde{c} := c^{p^n} \in \tilde{C}$ gilt. Für jedes $b \in B$, dass als Wert von c unter $h^\#$ in Frage kommt, muss daher gelten $b^{p^n} = h^\#(\tilde{c})$. Diese Gleichung hat aber bekanntlich (wenn überhaupt) nur eine Lösung; daher ist h durch $\tilde{h}$ eindeutig bestimmt.

Da diese Konstruktion offensichtlich auch stabil unter Lokalisierungen ist, lassen sich die lokal konstruierten Schemata verkleben, und damit ergibt sich auch der allgemeine Fall. □

Aus dieser Proposition lässt sich nun analog zu der Argumentation im obigen Beipspiel leicht schließen:

Korollar 2.3.4. *Sei $g : X \to Y$ eine endliche Überlagerung von normalen Schemata vom endlichen Typ über $\mathbb{Z}$; $K(X)|K(Y)$ sei eine normale Körpererweiterung. Dann ist für alle abgeschlossenen Punkte $y \in Y$ der Trägheitsgrad $f(x|y) = [k(x) : k(y)]$ unabhängig von der Wahl von $x \in g^{-1}(y)$.*

3 Zeta- und L-Funktionen

Wie nicht anders zu erwarten, gelingt auch im allgemeinen Fall der Beweis der Rückrichtung des Satzes nicht allein mit algebraischen Methoden[3]. Vielmehr müssen wir in Analogie zu den Betrachtungen im Zahlkörperfall auch hier Zeta- und L-Funktionen betrachten und ein Analogon des Satzes von Čebotarev beweisen. Folgende Darstellung stützt sich ganz wesentlich auf einen bekannten Übersichtsartikel von Serre ([Se65]), der allerdings hier um die fehlenden Beweise ergänzt ist.

3.1 Die Zeta-Funktion eines Schemas

Statt die Zetafunktion wie im klassischen Fall als unendliche Reihe zu definieren, sucht man ein Analogon zu der Eulerprodukt-Darstellung, deren Faktoren $\frac{1}{1-\mathfrak{N}\mathfrak{p}^{-s}}$ im wesentlichen bestimmt sind durch die Norm des Primideals $\mathfrak{p}$, d.h. der Anzahl der Elemente des Restklassenkörper $k(\mathfrak{p})$. Damit also ein solcher Faktor der Form $\frac{1}{1-N(x)^{-s}}, N(x) = \#k(x)$ überhaupt sinnvoll ist, muss der Restklassenkörper bei x endlich sein. Wir bedienen uns nun des folgenden Lemmas:

Lemma 3.1.1. *Sei X ein Schema (v.e.T über $\mathbb{Z}$), $x \in X$. Dann sind äquivalent:*

a) $\{x\}$ ist abgeschlossen in X.

b) Der Restklassenkörper $k(x)$ ist endlich.

Beweis. OBdA sei X affin, $= \operatorname{Spec} A$. Wir müssen zeigen:
Für jedes $\mathfrak{p} \in \operatorname{Spec} A$ gilt: $\mathfrak{p}$ maximal $\Longleftrightarrow A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p}$ endlich.
„$\Rightarrow$ ": Für $\mathfrak{p}$ maximal ist $A_\mathfrak{p}/\mathfrak{p}A_\mathfrak{p} = (A/\mathfrak{p})_{\overline{A-\mathfrak{p}}} = A/\mathfrak{p}$ eine endliche $\mathbb{Z}$-Algebra und ein Körper. Sei κ der zugehörige Primkörper. Nach dem Hilbertschen Nullstellensatz ist $A/\mathfrak{p}$ dann eine algebraische Erweiterung von κ. Ist κ endlich, so auch $A/\mathfrak{p}$. Auszuschließen bleibt also der Fall, dass $\mathbb{Q}$ der zugehörige Primkörper ist. In diesem Fall ist $A/\mathfrak{p}$ wegen des Hilbertschen Nullstellensatzes eine endliche algebraische Erweiterung von $\mathbb{Q}$. Seien $\xi_1, \dots, \xi_r$ ein Erzeugendensystem von $A/\mathfrak{p}$ als $\mathbb{Z}-$Algebra, $P_1(X), \dots, P_r(X) \in \mathbb{Q}[X]$ die zugehörigen Minimalpolynome, n der Hauptnenner aller Koeffizienten dieser Polynome. Dann gilt $P_i(X) \in \mathbb{Z}_n[X]$ für alle i, die ξ_i und damit auch $A/\mathfrak{p}$ sind also ganz über $\mathbb{Z}_n$; damit müssten aber auch die Krulldimensionen von $A/\mathfrak{p}$ und $\mathbb{Z}_n$ übereinstimmen. Da der eine Ring aber nulldimensional ist, der andere Dimension 1 hat, ergibt sich der gewünschte Widerspruch.
„$\Leftarrow$ ": Ist $\mathfrak{p}$ nicht maximal, so gibt es ein maximales Ideal $\mathfrak{m}$ mit $\mathfrak{p} \subsetneq \mathfrak{m}$. Sei $t \in \mathfrak{m} \backslash \mathfrak{p}$. Dann gilt: $t^n \in \mathfrak{m} \backslash \mathfrak{p}$, also insbesondere $\bar{t}^n \neq 1 \in A/\mathfrak{p}\ \forall\, n \in \mathbb{N}$ (denn aus $t^n - 1 \in \mathfrak{p}$ folgte $1 \in \mathfrak{m} ⇲$). Folglich enthält $(A/\mathfrak{p})_{\overline{A-\mathfrak{p}}}$ unendlich viele Elemente, $k(\mathfrak{p})$ ist also nicht endlich. □

[3] bzw. ist zumindest ein solcher Beweis dem Autor nicht bekannt

Definition 3.1.2. *Den Raum*

$$\overline{X} = \{x \in X | \{x\} \text{ abgeschlossen}\},$$

aufgefasst als diskreter topologischer Raum mit Garbe $k(x)$, nennt man ***Atomisierung*** *von X. Für jedes $x \in \overline{X}$ sei die* ***Norm*** *$N(x)$ definiert als Anzahl der Elemente von $k(x)$.*

Wir sind nun bereit zur Definition der Zeta-Funktion.

Definition 3.1.3. *Die* ***Zeta-Funktion*** *eines Schemas X v.e.T. über $\mathbb{Z}$ ist definiert als Euler-Produkt*

$$\zeta(X, s) = \prod_{x \in \overline{X}} \frac{1}{1 - \frac{1}{N(x)^s}} \tag{10}$$

Lemma 3.1.4. *Zu jedem $n \in \mathbb{N}$ gibt es nur endlich viele $x \in \overline{X}$ mit $N(x) = n$.*

Beweis. OBdA sei X affin, $= \operatorname{Spec} B$, $B = A/\mathfrak{a}$ mit $A = \mathbb{Z}[T_1, \dots, T_r]$. Für $\bar{\mathfrak{m}} \in \operatorname{Spec} B$ maximal gilt $B/\bar{\mathfrak{m}} = (A/\mathfrak{a})/(\mathfrak{m}/\mathfrak{a}) = A/\mathfrak{m}$, also können wir oBdA annehmen, dass $B = A = \mathbb{Z}[T_1, \dots, T_r]$.
Sei $n = p^k$. Aus Abzählargumenten folgt: Für jedes maximale Ideal $\mathfrak{m}$ mit $N(\mathfrak{m}) = p^k$ gibt es Polynome $P_1(X), \dots, P_r(X)$ vom Grad $\leq k$ und mit Koeffizienten aus $\{0, \dots, p-1\}$, so dass $P_i(T_i) \in \mathfrak{m}$ für $i = 1, \dots, r$. Da es aber nur endlich viele solcher Polynome gibt und jeweils nur endlich viele Ideale darüberliegen, stimmt die Behauptung. □

Somit ist $\zeta(X, s)$ eine formale Dirichletreihe $\sum \frac{a_n}{n^s}$ mit ganzen Koeffizienten. Noch aber hat diese Definition wenig Wert, solange keine Konvergenzaussagen gewährleistet sind.

Satz 3.1.5. *Das Produkt $\zeta(X, s)$ konvergiert absolut für $\operatorname{Re} s > \dim X$.*

Der Beweis erfordert die Zuhilfenahme einiger Hilfssätze:

Lemma 3.1.6. *(a) Sei X eine endliche Vereinigung von Schemata X_i. Gilt Satz 3.1.5 für jedes der X_i, so auch für X.*

(b) Falls $X \to Y$ ein endlicher dominanter Morphismus ist und Satz 3.1.5 für Y gilt, so gilt er auch für X.

Beweis. (a) ist trivial, denn konvergiert ζ absolut für X, so auch für jede Teilmenge, und die Aufteilung $X = X_1 \dot\cup (X_2 \backslash X_1) \dot\cup (X_3 \backslash (X_1 \cup X_2)) \dot\cup \dots$ liefert die Aussage für X. (Man beachte $\dim X \geq \dim X_i$ für jedes Schema $X_i \subset X$.)

(b) Sei oBdA $Y = \operatorname{Spec} B$ affin, also auch $X = \operatorname{Spec} A$. Da $X \to Y$ endlich und dominant ist, ist $A \to B$ injektiv und B ein endlicher und damit auch ganzer A-Modul. Per Induktion können wir annehmen, dass B über A durch ein einziges ganzes Element erzeugt ist, d.h. $B = A[T]/\mathfrak{a}$ mit einem Ideal $\mathfrak{a} = (f_1, \ldots, f_n) \subset A[T]$. Sei nun $\mathfrak{m}$ ein maximales Ideal in A, $k = A/\mathfrak{m}$. Dann gilt $\bar{\mathfrak{a}} = (\bar{f}(T))$ mit $\bar{f} = \operatorname{ggT}(\bar{f}_1, \ldots, \bar{f}_n) \in k[T]$; die maximalen Ideale in B über $\mathfrak{m}$ stehen in 1-zu-1-Korrespondenz zu den maximalen Idealen von $B/\mathfrak{m}B = k[T]/\bar{f}(T)$. Sei nun $p_1^{\alpha_1}(T) \cdots p_r^{\alpha_r}(T)$ die Primfaktorzerlegung von $\bar{f}(T)$ in $k[T]$. Nach dem chinesischen Restsatz gilt dann $B/\mathfrak{m}B \cong k[T]/(p_1^{\alpha_1}(T)) \oplus \ldots \oplus k[T]/(p_r^{\alpha_r}(T))$; da die Ringe $k[T]/(p_i^{\alpha_i})$ lokal sind, gibt es genau r maximale Ideale in $B/\mathfrak{m}B$. Nun gilt offenbar $r \leq \deg \bar{f} \leq \deg f_1$, und für jedes maximale Ideal $\mathfrak{m}' \subset B$ über $\mathfrak{m}$ gilt $N(\mathfrak{m}') \geq N(\mathfrak{m})$; daher erhalten wir für $s = \sigma + it$

$$\prod_{\mathfrak{m}'|\mathfrak{m}} \frac{1}{|1 - N(\mathfrak{m}')^{-s}|} \leq \prod_{\mathfrak{m}'|\mathfrak{m}} \frac{1}{1 - N(\mathfrak{m}')^{-\sigma}} \leq \left(\frac{1}{1 - N(\mathfrak{m})^{-\sigma}}\right)^{\deg f_1};$$

somit bildet $\zeta(Y, \sigma)^{\deg f_1}$ eine konvergente Majorante zu $\zeta(X, s)$. Da $\dim X = \dim Y$, folgt unmittelbar die Aussage. □

Lemma 3.1.7. *Sei $\psi_q(k)$ die Anzahl der irreduziblen Polynome vom Grad k in $\mathbb{F}_q$. Dann gilt*

$$\sum_{d|k} d\psi_q(d) = q^k \tag{11}$$

und

$$\prod_{k=1}^{\infty} (1 - z^k)^{\psi_q(k)} = 1 - qz \qquad \textit{für } |z| < \frac{1}{q} \tag{12}$$

Beweis. Für ein irreduzibles Polynom $P(X)$ vom Grad k gilt $\mathbb{F}_q[X]/P(X) = \mathbb{F}_{q^k}$. Dieser Körper ist genau die Lösungsmenge des Zerfällungspolynoms $X^{q^k} - X$. Dieses muss über $\mathbb{F}_q$ in paarweise verschiedene irreduzible Faktoren vom Grad $d|k$ zerfallen, und ein jeder solcher muss enthalten sein. Durch Gradvergleich ergibt sich die Gleichung (11).

Folgende Gleichungskette liefert die formale Aussage von Gleichung (12):

$$\begin{aligned}
\log\left(\prod_{k=1}^{\infty}(1-z^k)^{\psi_q(k)}\right) &= \sum_{k=1}^{\infty}\psi_q(k)\log(1-z^k)\\
&= \sum_{k=1}^{\infty}\left(\psi_q(k)\sum_{l=1}^{\infty}\frac{z^{kl}}{l}\right)\\
&= \sum_{m=1}^{\infty}\left(\sum_{d|m}d\psi_q(d)\right)\frac{z^m}{m}\\
&\overset{(a)}{=} \sum_{m=1}^{\infty}\frac{q^m z^m}{m} = \log(1-qz)
\end{aligned}$$

Man beachte, dass für $|z| < \frac{1}{q}$ die letzte Summe und damit nach dem großen Umordnungssatz alle Summen absolut konvergieren. □

Lemma 3.1.8. *Sei X ein Schema v.e.T. über $\mathbb{Z}$. Dann gilt formal*

$$\zeta(\mathbb{A}^1_X, s) = \zeta(X, s-1), \tag{13}$$

insbesondere haben beide Funktionen den gleichen Bereich der absoluten Konvergenz.

Beweis. OBdA können wir davon ausgehen, dass X affin ist, also $X = \operatorname{Spec} A$, A eine endlich erzeugte $\mathbb{Z}$-Algebra, und $\mathbb{A}^1_X = \operatorname{Spec} A[T]$.

Da jedes maximale Ideal $\mathfrak{m}$ von $A[T]$ über einem maximalen Ideal $\mathfrak{m}'$ in A liegt, können wir die Faktoren der Zetafunktion nach dem Durchschnitt des jeweiligen maximalen Ideals mit A sortieren. Es reicht daher zu zeigen, dass für ein beliebiges festes maximales Ideal $\mathfrak{m}' \in \operatorname{Specmax} A$ gilt:

$$\prod_{\substack{\mathfrak{m}\in\operatorname{Specmax} A[T]\\ \mathfrak{m}\cap A=\mathfrak{m}'}}(1-N(\mathfrak{m})^{-s}) = 1-N(\mathfrak{m}')^{1-s}$$

Sei $N(\mathfrak{m}') = q$. Bei der kanonischen Projektion $A[T] \longrightarrow A[T]/(\mathfrak{m}'A[T]) \cong \mathbb{F}_q[T]$ wird ein maximales Ideal $\mathfrak{m}$ in $A[T]$ über $\mathfrak{m}'$ auf ein maximales Ideal $(P(T))$ in dem Hauptidealring $\mathbb{F}_q[T]$ abgebildet. Umgekehrt wird $\mathfrak{m}$ durch das irreduzible Polynom $P(T)$ festgelegt. Ist $P(T)$ vom Grad k, so gilt $A[T]/\mathfrak{m} \cong \mathbb{F}_q[T]/P(T) = \mathbb{F}_{q^k}$, also $N(\mathfrak{m}) = q^k$. Sei $\psi_q(k)$ die Anzahl der irreduziblen Polynome vom Grad k in $\mathbb{F}_q$, $z = q^{-s}$. Mit der soeben beschriebenen 1:1-Beziehung {maximale Ideale über $\mathfrak{m}'$} $\Leftrightarrow$ {irreduzible Polynome in $\mathbb{F}_q[T]$} ergibt sich

$$\prod_{\substack{\mathfrak{m}\in\operatorname{Specmax} A[T]\\ \mathfrak{m}\cap A=\mathfrak{m}'}}(1-N(\mathfrak{m})^{-s}) = \prod_{k=1}^{\infty}(1-z^k)^{\psi_q(k)} \overset{L.\,3.1.7}{=} 1-qz = 1-N(\mathfrak{m}')^{1-s}$$ □

Korollar 3.1.9. *Ist $\mathbb{A}_X^n$ der affine n-dimensionale Raum über einem Schema X, so haben wir*

$$\zeta(\mathbb{A}_X^n, s) = \zeta(X, s-n).$$

Ebenso gilt

$$\zeta(\mathbb{P}_X^n, s) = \prod_{m=0}^{n} \zeta(X, s-m).$$

Beweis von Satz 3.1.5. Wegen Lemma 3.1.6 a) reicht es zunächst einmal, sich auf irreduzible Schemata zu beschränken; danach können wir oBdA sogar annehmen, dass $X = \operatorname{Spec} A$ affin und ganz ist. Nach dem Beweis von Lemma 2.1.2 können wir nach eventuellem weiteren Lokalisieren davon ausgehen, dass A ganz ist über $B[T_1, \ldots, T_r]$ mit $B = \mathbb{F}_p$ oder $\mathbb{Z}_n$; dank Lemma 3.1.6 b) müssen wir uns also nur mit dem Fall $A = B[T_1, \ldots, T_r]$ auseinandersetzen.

Der Fall $r = 0$ ist klar: Offenbar konvergiert

$$\zeta(\operatorname{Spec} \mathbb{Z}_n, s) = \prod_{p \nmid n} \frac{1}{1-p^{-s}} = \zeta(s) \prod_{p \mid n} (1-p^{-s})$$

für $\operatorname{Re} s > 1$ absolut; auch $\zeta(\operatorname{Spec} \mathbb{F}_p, s) = \frac{1}{1-p^{-s}}$ stellt für $\operatorname{Re} s > 0$ eine holomorphe Funktion dar. Der Rest folgt nun aus Korollar 3.1.9. □

Einige Eigenschaften und Beispiele

Bemerkung 3.1.10.
1. *$\zeta(X, s)$ hängt nur von der Atomisierung $\overline{X}$ von X ab. Insbesondere ändert es sich nicht unter einem radiziellen Morphismus, und wir haben*

$$\zeta(X_{red}, s) = \zeta(X, s)$$

2. *Ist X eine disjunkte Vereinigung (möglicherweise unendlich) von Unterschemata X_i, so haben wir*

$$\zeta(X, s) = \prod \zeta(X_i, s),$$

mit absoluter Konvergenz für $\operatorname{Re} s > \dim X$. Es reicht sogar, dass $\overline{X}$ die disjunkte Vereinigung der $\overline{X}_i$'s ist.

Beispiel 3.1.11. *Sei $f : X \to Y$ ein Morphismus, so können wir als X_i die Fasern $X_y = f^{-1}(y), y \in \overline{Y}$ nehmen und erhalten:*

$$\zeta(X, s) = \prod_{y \in \overline{Y}} \zeta(X_y, s) \tag{14}$$

(Mit $Y = \operatorname{Spec} Z$ war dies die ursprüngliche Definition von Hasse-Weil.) Dies werden wir beim Beweis der analytischen Fortsetzbarkeit ausnutzen. Es sei darauf hingewiesen, dass eine solche Schreibweise nur im Bereich der absoluten Konvergenz Sinn macht und dort auch nur, weil $\overline{Y}$ abzählbar ist, wie man nachträglich ebenfalls dem Beweis von 3.1.5 entnehmen kann.

Bemerkung 3.1.12. *Für $X = \operatorname{Spec} \mathcal{O}_K$, wobei $\mathcal{O}_K$ der Ring der ganzen Zahlen in einem Zahlkörper K ist, stimmt $\zeta(X, s)$ mit der klassischen Dedekindschen Zetafunktion ζ_K überein. Insbesondere erhalten wir für $K = \mathbb{Q}$, also $\mathcal{O}_K = \mathbb{Z}$, Riemanns Zetafunktion.*

3.2 L-Funktionen auf einem Schema

Sei X ein Schema, G eine zulässige endliche Gruppenwirkung auf X, Y der Quotient X/G. Zu einem $x \in X$ (nicht notwendig abgeschlossen) sei y das Bild in Y und $D(x) = \{g \in G : x.g = x\}$ die zugehörige Zerlegungsgruppe. Dann gibt einen natürlichen Epimorphismus

$$D(x) \to \operatorname{Gal}(k(x)|k(y))$$

Sein Kern $I(x)$ wird Trägheitsgruppe von x genannt; für $I(x) = \{1\}$ ist der Morphismus $X \to Y$ étale bei x. Diese Fakten sind bekannt aus der Hilbertschen Zerlegungstheorie, sollte dies nicht der Fall sein, so entnehme man sie bitte [SGA 1, Exposé V].

Wegen $D(x)/I(x) \cong \operatorname{Gal}(k(x)|k(y))$ ist $D(x)/I(x)$ eine zyklische Gruppe mit einem kanonischen Erzeuger F_x, genannt **Frobenius-Element** von x.

Definition 3.2.1. *Sei χ ein Charakter von G. Für jedes $y \in \overline{Y}$ und jedes $n \in \mathbb{N}$ setze*

$$\chi(y^n) = \frac{1}{e(x)} \sum_{\substack{g \in D(x) \\ \bar{g} = F_x^n}} \chi(g). \tag{15}$$

Dabei sei $x \in \overline{X}$ ein beliebiger Lift von y, $e(x) = \operatorname{ord} I(x)$ und $F_x \in D(x)/I(x)$ das Frobenius-Element von x. Diese Definition ist unabhängig von der Wahl von x, denn für zwei Lifts x, x' von y sind sowohl die Trägheitsgruppen als auch die Zerlegungsgruppen konjugiert, also insbesondere auch die entsprechenden Frobenius-Elemente.

*Nun definiert man die **Artinsche L-Funktion** $L(X, \chi, s)$ folgendermaßen:*

$$\log L(X, \chi; s) = \sum_{y \in \overline{Y}} \sum_{n=1}^{\infty} \frac{\chi(y^n) N(y)^{-ns}}{n}. \tag{16}$$

Satz 3.2.2. *(a) Ist χ der Charakter einer linearen Darstellung $g \mapsto \rho(g)$, so gilt*

$$L(X, \chi; s) = \prod_{y \in \overline{Y}} \frac{1}{\det(1 - \rho(F_x) N(y)^{-s})}\ , \tag{17}$$

wobei erneut $\rho(F_x) = \frac{1}{e(x)} \sum_{g \in D(x) : \bar{g} = F_x} \rho(g)$ und x irgendein Lift von y sei.

(b) Beide Ausdrücke (16) und (17) konvergieren absolut für $\operatorname{Re} s > \dim X$.

Beweis. (a) Für $\sigma := \frac{1}{e(x)} \sum_{g \in I(x)} \rho(g)$ gilt zunächst $\rho(g) \cdot \sigma = \sigma$ für $g \in I(x)$ und deswegen $\sigma^2 = \sigma$, folglich $\sigma^n = \sigma$. Aus dieser Gleichheit folgert man leicht, dass

$$\chi(y^n) = \operatorname{tr}\left(\frac{1}{e(x)} \sum_{\substack{g \in D(x) \\ \bar{g} = F_x^n}} \rho(g) \right) = \operatorname{tr}(\rho(g_0)^n \sigma) = \operatorname{tr}((\rho(g_0)\sigma)^n) = \operatorname{tr}(\rho(F_x)^n)$$

mit einem beliebigen Lift $g_0 \in D(x) \subseteq G$ von $F_x \in D(x)/I(x)$. Damit erhält man im Falle absoluter Konvergenz die Äquivalenz der Formeln aus

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\chi(y^n) N(y)^{-ns}}{n} &= \operatorname{tr} \sum_{n=1}^{\infty} \frac{\rho(F_x)^n N(y)^{-ns}}{n} \\ &= -\operatorname{tr} \log(1 - \rho(F_x) N(y)^{-s}) \\ &= -\log \det(1 - \rho(F_x) N(y)^{-s}) \end{aligned}$$

(b) Der Wertebereich von χ ist beschränkt, daher reicht es, die Aussage für den trivialen Charakter (bzw. die triviale Darstellung) zu beweisen. Für diesen gilt aber wegen (17)

$$L(X, \chi_{triv}; s) = \zeta(Y, s),$$

also haben wir absolute Konvergenz für $\operatorname{Re} s > \dim Y = \dim X$. □

Formale Eigenschaften der L-Funktionen

Proposition 3.2.3. *(a) $L(X, \chi)$ hängt nur von der Atomisierung $\overline{X}$ von X ab.*

(b) $L(X, \chi + \chi') = L(X, \chi) \cdot L(X, \chi')$.

(c) Ist $\overline{X}$ die disjunkte Vereinigung von den $\overline{X}_i$s, wobei jedes der X_i stabil unter G ist, so gilt

$$L(X, \chi; s) = \prod L(X_i, \chi; s)$$

mit absoluter Konvergenz für $\operatorname{Re} s > \dim X$.

(d) Sei $\pi : G \to G'$ ein Homomorphismus, und sei $\pi_* X = X \times_G G'$ das Schema, das aus X durch „Erweiterung der Strukturgruppe“entsteht. Sei χ' ein Charakter von G', und sei $\pi^* \chi' = \chi' \circ \pi$ der entsprechende Charakter von G. Dann gilt

$$L(X, \pi^* \chi') = L(\pi_* X, \chi'). \tag{18}$$

(e) Sei $\pi : G' \to G$ ein Homomorphismus, und sei $\pi^* X$ das Schema X, auf dem G' durch π operiert. Sei χ' ein Charakter von G', und sei $\pi_* \chi'$ dessen direktes

Bild; dies ist ein Charakter von G. (Ist G' eine Untergruppe von G, so ist $\pi_*\chi'$ der induzierte Charakter von χ'). Es gilt

$$L(X, \pi_*\chi') = L(\pi^* X, \chi'). \tag{19}$$

(f) Für $\chi = 1$ (trivialer Charakter) gilt $L(X, 1) = \zeta(X/G)$.

(g) Für $\chi = r$ (Charakter der regulären Darstellung) gilt $L(X, r) = \zeta(X)$.

Beweis. (a), (b), (c) und (f) sind trivial.

(d) Es gilt $\pi_* X = \coprod_{\bar{g}' \in \operatorname{im}\pi \backslash G'} X/\ker\pi$, also insbesondere $(\pi_* X)/G' = X/G = Y$. Sei y ein Punkt in $\overline{Y}$, x' ein Urbild in $\overline{\pi_* X}$ und x ein Urbild von x' in $\overline{X}$. Dann gilt $D'(x') = \pi(D(x))$. Da x' in einer Kopie von $X/\ker\pi$ enthalten ist, ist $k(x')$ eine Zwischenerweiterung von $k(x)|k(y)$; für $\bar{g} = F_x^n$ gilt dann $\overline{\pi(g)} = F_{x'}^n$, und jedes g' mit $\bar{g}' = F_{x'}^n$ hat genau $\frac{\operatorname{ord} I(x)}{\operatorname{ord} I'(x')}$ Urbilder g mit $\bar{g} = F_x^n$. Die Behauptung ergibt sich dann unmittelbar aus

$$\begin{aligned} \chi'(y^n) &= \frac{1}{\operatorname{ord} I'(x')} \sum_{\substack{g' \in D'(x') \\ \bar{g}' = F_{x'}^n}} \chi'(g') = \frac{\operatorname{ord} I'(x')}{\operatorname{ord} I(x) \cdot \operatorname{ord} I'(x')} \sum_{\substack{g \in D(x) \\ \bar{g} = F_x^n}} \chi'(\pi(g)) \\ &= \pi^*\chi'(y^n). \end{aligned}$$

(e) Sei $Y' = \pi^* X/G' \cong X/\pi(G')$; sei $y \in \bar{Y}$ fest gewählt, $x \in \bar{X}$ ein beliebiger Punkt darüber und y' der zugehörige Punkt in $\bar{Y}'$. $k(y')$ ist offenbar ein Zwischenkörper von $k(x)|k(y)$, sei $m = [k(y') : k(y)] = \frac{[D(x):I(x)]}{[D'(x):I'(x)]}$. Dann gilt $N(y') = N(y)^m$; insbesondere gilt für den Frobenius von $k(x)|k(y)$: $F_x' = F_x^m$. Offenbar gilt $\pi(D'(x)) \subseteq D(x)$, getroffen werden gerade diejenigen $g \in D(x)$, die einen $k(y')$-Morphismus darstellen, d.h. für die $\bar{g} = F_x^{mk}$ mit $k \in \mathbb{N}$. Über y liegen in Y' mehrere Punkte $y_1' = y', \ldots, y_r'$; deren Anzahl bestimmt sich per Bahnformel zu $r = \frac{[G:D(x)]}{[G':D'(x)]}$. Das direkte Bild $\pi_*\chi'$ von χ' ist definiert durch

$$\pi_*\chi'(g) = \frac{1}{\operatorname{ord} G'} \sum_{h \in G} \sum_{g' \in \pi^{-1}(hgh^{-1})} \chi'(g')$$

Damit gilt insbesondere

$$\begin{aligned} \pi_*\chi'(y^n) &= \frac{1}{e(x) \cdot \operatorname{ord} G'} \sum_{\substack{g \in D(x) \\ \bar{g} = F_x^n}} \sum_{h \in G} \sum_{g' \in \pi^{-1}(hgh^{-1})} \chi'(g') \\ &= \frac{1}{e(x) \cdot \operatorname{ord} G'} \sum_{h \in G} \sum_{\substack{g \in D(hx) \\ \bar{g} = F_{hx}^n}} \sum_{g' \in \pi^{-1}(g)} \chi'(g') \end{aligned}$$

Ist n kein Vielfaches von m, so ist dieser Ausdruck notwendigerweise Null, für $n = mk$ erhalten wir

$$\begin{aligned} \pi_*\chi'(y^{mk}) &= \frac{1}{e(x)\cdot \operatorname{ord} G'} \sum_{h\in G} \sum_{\substack{g'\in D'(hx) \\ \bar{g}'=F'^k_{hx}}} \chi'(g') \\ &= \frac{e'(x)\cdot \operatorname{ord} G}{r\cdot e(x)\cdot \operatorname{ord} G'} \sum_{i=1}^{r} \chi'(y_i'^k) \end{aligned}$$

Wegen

$$\frac{e'(x)\cdot \operatorname{ord} G}{r\cdot e(x)\cdot \operatorname{ord} G'} = \frac{[G' : D'(x)]\cdot e'(x)\cdot \operatorname{ord} G}{[G : D(x)]\cdot e(x)\cdot \operatorname{ord} G'} = \frac{[D(x) : I(x)]}{[D'(x) : I'(x)]} = m$$

folgt

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\pi_*\chi'(y^n)N(y)^{-ns}}{n} &= \sum_{k=1}^{\infty} \left(\frac{N(y)^{-mks}}{mk} \sum_{i=1}^{r} m\, \chi'(y_i'^k) \right) \\ &= \sum_{i=1}^{r} \sum_{k=1}^{\infty} \frac{\chi'(y_i'^k) N(y_i')^{-ks}}{k} \end{aligned}$$

und damit die Behauptung.

(g) Für $G' = \{1\} \overset{\pi}{\hookrightarrow} G$, $\chi' = 1$ gilt $\pi_*\chi' = r$. Aus (e) und (f) folgt nun die Aussage. □

Beispiel 3.2.4. *Sei* $X = \operatorname{Spec} \mathbb{F}_{q^n}, Y = \operatorname{Spec} \mathbb{F}_q, G = \operatorname{Gal}(\mathbb{F}_{q^n} | \mathbb{F}_q)$, *und* χ *ein irreduzibler Charakter von* G. *Dann gilt*

$$L(X,\chi;s) = \frac{1}{1-\chi(F)q^{-s}}\ , \tag{20}$$

wobei F *das Frobeniuselement von* G *ist. Denn in diesem Fall ist* G *zyklisch; daher sind alle irreduziblen Darstellungen eindimensional. Insbesondere gilt* $\chi(F^n) = \chi(F)^n$, *und daraus ergibt sich unmittelbar die Formel.*

Bemerkung 3.2.5. *Indem man (b) und (g) kombiniert, erhält man folgende Formel (die einer der Hauptgründe für die Einführung der L-Funktionen war):*

$$\zeta(X) = \prod_{\chi\in \operatorname{Irr}(G)} L(X,\chi)^{\deg(\chi)}; \tag{21}$$

dabei sei $\operatorname{Irr}(G)$ *die Menge der irreduziblen Charaktere von* G *und* $\deg(\chi) = \chi(1)$.

3.3 Spezialfall: Schemata über einem endlichen Körper

Fakt 3.3.1. *Sei X ein Schema über $\mathbb{F}_q$. Für $x \in \overline{X}$ ist der Restklassenkörper $k(x)$ eine endliche Erweiterung von $\mathbb{F}_q$; sei* $\deg(x)$ *ihr Grad. Wir haben*

$$\begin{aligned} N(x) &= q^{\deg(x)} \text{ und} \\ \zeta(X,s) &= Z(X,q^{-s}), \end{aligned} \tag{22}$$

wobei Z(t) die durch das Produkt

$$Z(X,t) = \prod_{x \in \overline{X}} \frac{1}{1 - t^{\deg(x)}} \tag{23}$$

definierte Potenzreihe ist. Dieses Produkt konvergiert für $|t| < q^{-\dim X}$.

Diese Schreibweise erlaubt eine andere Definition der Zetafunktion $Z(X,t)$: Sei $k = \mathbb{F}_q$, und sei k_n die Erweiterung vom Grad n von k. Sei $X_n = X(k_n)$ die Menge der Punkte von X mit Werten in k_n. Solch ein Punkt P lässt sich darstellen als Paar (x,f) mit $x \in \overline{X}$, und wobei f ein k-Isomorphismus von $k(x)$ in k_n ist. Wir haben

$$\bigcup X_n = X(\bar{k});$$

dabei ist $\bar{k}$ der algebraische Abschluss von k.

Proposition 3.3.2. *Die X_n sind endlich; setzt man*

$$\nu_n = \operatorname{Card}(X_n),$$

hat man

$$\log Z(X,t) = -\sum_{n=1}^{\infty} \frac{\nu_n t^n}{n} \tag{24}$$

Beweis. Dass die X_n endlich sind, folgt aus Lemma 3.1.4 und der Tatsache, dass es zu gegebenem x nur endlich viele Möglichkeiten gibt, $k(x)$ in k_n einzubetten. Genauer gesagt lässt sich $k(x)$ nur dann in k_n einbetten, wenn n ein Vielfaches von $\deg(x)$ ist; und in diesem Fall beträgt die Anzahl der möglichen Einbettungen $\operatorname{ord} \operatorname{Gal}(k(x)|k) = \deg(x)$. Es gilt also

$$\nu_n = \sum_{\substack{x \in \overline{X} \\ \deg(x)|n}} \deg x \tag{25}$$

Damit folgt aber

$$\log Z(X,t) = -\sum_{x \in \overline{X}} \log(1 - t^{\deg(X)}) = -\sum_{x \in \overline{X}} \sum_{m=1}^{\infty} \frac{t^{m\deg(X)}}{m} = -\sum_{n=1}^{\infty} \frac{\nu_n t^n}{n} \qquad \square$$

Diese veränderte Darstellung ist mehr als bloße Spielerei. Sie erlaubt es, Zeta- und L-Funktionen über Anzahlen von Fixpunkten gewisser Morphismen darzustellen; eine wesentliche Grundlage für die weiterführende Theorie. Wir gebrauchen dazu folgende

Definition 3.3.3. *Sei X ein Schema über einem endlichen Körper $k = \mathbb{F}_q$. Wir definieren einen $\mathbb{F}_q$-Morphismus $F : X \to X$, genannt* ***Frobenius-Morphismus****, auf folgende Art: Topologisch gesehen sei F die Identität, auf der Garbe $\mathcal{O}_X$ wirke F durch $\phi \mapsto \phi^q$.*

F wirkt auf der Menge der geometrischen Punkte $X(\bar{k}) = \mathrm{Hom}(\mathrm{Spec}\,\bar{k}, X)$ durch $\xi \mapsto F \circ \xi$ für $\xi \in X(\bar{k})$. Dies ermöglicht uns folgende Aussage:

Proposition 3.3.4. *(i) Sei X wie oben, $\Lambda(F^n)$ die Anzahl der Fixpunkte des Morphismus F^n bei Wirkung auf $X(\bar{k}) = \mathrm{Hom}(\mathrm{Spec}\,\bar{k}, X)$. Dann gilt in obiger Schreibweise: $\nu_n = \Lambda(F^n)$.*

(ii) Allgemeiner gilt: Sei X ein Schema über $\mathbb{F}_q$, G eine endliche Gruppe von $\mathbb{F}_q$-Automorphismen von X, die auf zulässige Weise auf X wirkt. Dann ist das Schema $Y = X/G$ auch ein $\mathbb{F}_q$-Schema, und die Automorphismen zu den Gruppenelementen $\sigma \in G$ vertauschen mit dem Frobenius-Endomorphismus F. Setzen wir wie üblich $t = q^{-s}$, so erhalten wir:

$$\log L(X, \chi; t) = \sum_{n=1}^{\infty} \frac{\nu_n(\chi) t^n}{n} \tag{26}$$

mit

$$\nu_n(\chi) = \frac{1}{\mathrm{ord}\, G} \sum_{\sigma \in G} \chi(\sigma) \Lambda(\sigma^{-1} F^n), \tag{27}$$

wobei $\Lambda(\sigma F^n)$ die Anzahl der Fixpunkte von σF^n bei Wirkung auf $X(\bar{k})$ ist.

Beweis. (i) ist erstens trivial und folgt zweitens aus (ii).

(ii) Ein Punkt $\xi = (x, f) \in X(\bar{k})$ ist genau dann ein Fixpunkt unter $\sigma^{-1} F^n$, wenn $\sigma \in D(x)$ und $f = f \circ \sigma^{-1} F^n$ gilt. Dies wiederum ist äquivalent dazu, dass $F^n \in \mathrm{Gal}(k(x)|k(y))$, also $\deg(y)|n$, und $\bar{\sigma} = F^n = F_x^{n/\deg y}$ ist. In diesem Fall gibt es - wie oben bereits erwähnt - $\deg(x)$ Einbettungen von $k(x)$ in $\bar{k}$. Es folgt also

$$
\begin{aligned}
\nu_n(\chi) &= \frac{1}{\operatorname{ord} G} \sum_{\substack{x \in \overline{X} \\ \deg(y)|n}} \sum_{\substack{\sigma \in D(x) \\ \bar{\sigma} = F^n}} \chi(\sigma) \deg(x) \\
&= \frac{1}{\operatorname{ord} G} \sum_{\substack{y \in \overline{Y} \\ \deg(y)|n}} [G : D(x)] \deg(x) \sum_{\substack{\sigma \in D(x) \\ \bar{\sigma} = F_x^{n/\deg(y)}}} \chi(\sigma) \\
&= \sum_{\substack{y \in \overline{Y} \\ \deg(y)|n}} \frac{\deg(x)}{[D(x) : I(x)]} \chi(y^{n/\deg(y)}) = \sum_{\substack{y \in \overline{Y} \\ \deg(y)|n}} \deg(y) \chi(y^{n/\deg(y)})
\end{aligned}
$$

und damit $\displaystyle\sum_{n=1}^{\infty} \frac{\nu_n(\chi) t^n}{n} = \sum_{y \in \overline{Y}} \sum_{m=1}^{\infty} \frac{\deg(y)\chi(y^m) q^{-\deg(y) \cdot ms}}{m \deg(y)} = \log L(X, \chi, s).$

□

Geschichtlich gesehen ist dies der Ursprung für die Studien der Zeta- und L-Funktionen von Varietäten über endlichen Körpern. Ursprünglich betrachtete man dabei nur glatte projektive Kurven; Emil Artin und Friedrich Karl Schmidt verallgemeinerten den Begriff der Zetafunktion von Zahlkörpern auf ebensolche Kurven; mit Hilfe des Satzes von Riemann-Roch fand F.K. Schmidt 1931 [Sch31] einen Beweis für die Rationalität der Zetafunktion einer Kurve (als Funktion in t) und deren Funktionalgleichung.

Es blieb noch das Analogon zur Riemannschen Vermutung. Dessen Beweis gelang Weil 1948 [We48], indem er folgende dazu äquivalente Abschätzung zeigte:

Satz 3.3.5 (Weil). *Für die Anzahl ν_n der $\mathbb{F}_{q^n}$-rationalen Punkte einer geometrisch irreduziblen*[4] *glatten projektiven Kurve vom Geschlecht g über einem endlichen Körper $k = \mathbb{F}_q$ gilt*

$$|\nu_n - q^n - 1| \leq 2g q^{\frac{n}{2}}.$$

Wir werden die Aussage im nächsten Abschnitt beweisen, allerdings einem späteren Beweis von Grothendieck folgend. Mit dieser Abschätzung gelang es Weil auch, die Rationalität der L-Funktionen nachzuweisen.

1949 stieß Weil dann ein ganz neues Forschungsgebiet auf: Er veröffentlichte einige Mutmaßungen über Zetafunktionen von höherdimensionalen Varietäten, heute bekannt als Weil-Vermutungen. Dies umfassen die Rationalität der Funktion, die Funktionalgleichung und ein Analogon zur Riemannschen Vermutung. Gleichzeitig gab er auch die Idee vor, dass das Problem mit einer geeigneten Kohomologietheorie zu knacken sei.

[4] Die Definition von *geometrisch irreduzibel* steht im nächsten Abschnitt.

Dwork [Dw60] war 1960 der erste, dem es gelang, die Rationalität und die Funktionalgleichung der Zetafunktion im Allgemeinfall nachzuweisen - mit Methoden der p-adischen Analysis.

Die weiteren Erfolge auf diesem Gebiet aber ergaben sich tatsächlich durch die Entwicklung einer entsprechenden Kohomologietheorie: der étalen und der ℓ-adischen Kohomologie. Mit diesen Mitteln glückte es Grothendieck [Gr65] 1965, die Rationalität und Funktionalgleichung der L-Funktionen zu demonstrieren. Der Beweis des Analogons zur Riemannschen Vermutung durch Deligne [De74] im Jahre 1973 kann wohl auch aus heutiger Sicht noch als einer der Höhepunkte der algebraischen Geometrie betrachtet werden.

Als eine gelungene Einführung in diese Thematik lese man [Ha77, Appendix C].

3.4 Divisoren und Schnittzahlen

Soweit nicht ausdrücklich anders erwähnt, sind in diesem Abschnitt alle Varietäten über einem algebraischen abgeschlossenen Körper k definiert; der Begriff *Fläche* bedeute durchgehend eine nichtsinguläre projektive Fläche über k.

Der Begriff des *Divisors*, auch der des *amplen Divisors*, sollte hinreichend bekannt sein; nicht so bekannt ist möglicherweise der Terminus *Schnittzahl.* Um diesen zu definieren, benötigen wir zunächst folgende

Definition 3.4.1. *Sei X eine Fläche. Wir sagen, zwei Kurven C und D auf X* ***schneiden sich transversal*** *in $x \in C \cap D$, wenn die lokalen Gleichungen f und g von C und D bei x das maximale Ideal $\mathfrak{m}_x$ von $\mathcal{O}_{x,X}$ erzeugen.*

Äquivalent zu dieser Forderung ist (bei genauerer Betrachtung und nach Nakayama), dass die Abbildung von Tangentialräumen $T_\imath \oplus T_\jmath : T_xC \oplus T_xD \to T_xX$, die durch $\imath : C \hookrightarrow X$ und $\jmath : D \hookrightarrow X$ induziert wird, ein Isomorphismus ist.

Man beachte, dass zwei Kurven, die sich in einem Punkt x transversal schneiden, nur endlich viele Punkte gemeinsam haben können und beide bei x nichtsingulär sein müssen.

Definition 3.4.2. *Auf den Divisoren von X sei eine bilineare symmetrische Paarung $\operatorname{Div} X \times \operatorname{Div} X \to \mathbb{Z}$, genannt* ***Schnittzahl*** *und bezeichnet mit $C.D$ für beliebige Paare von Divisoren (C, D), mit folgenden Eigenschaften definiert:*

- *Sind C und D zwei nichtsinguläre Kurven, die sich transversal schneiden, so gilt $C.D = \#(C \cap D)$.*
- *Die Schnittzahl hängt nur von den linearen Äquivalenzklassen ab: Gilt für zwei Divisoren $C_1 \sim C_2$, so folgt $C_1.D = C_2.D$.*

Es gibt genau eine solche Paarung ([Ha77, V.1.1]), und für diese wollen wir ein paar weitere Eigenschaften zusammentragen:.

Beispiel 3.4.3. *Sei X das Produkt zweier projektiver nichtsingulärer Kurven $X = C_1 \times C_2$. Seien $P \in C_1$, $Q \in C_2$ abgeschlossene Punkte; betrachte dazu die Divisoren $H_1 = C_1 \times Q$ und $H_2 = P \times C_2$. Offenbar schneiden sich H_1 und H_2 genau einmal, und dort transversal; daher gilt $H_1.H_2 = 1$. Die Selbstschnittzahlen $H_1^2 = H_1.H_1$ und H_2^2 sind etwas schwieriger zu bestimmen; dazu untersuchen wir zunächst die Schnittzahl von H_1 mit einem beliebigen weiteren Divisor der Form $H_1' = C_1 \times Q'$, $Q' \neq Q$. Da H_1 und H_2 keinen Punkt gemeinsam haben, gilt $H_1.H_1' = 0$. Nun betrachte man ein $0 \neq f \in \mathfrak{m}_Q \subset K(C_2)$. Der zugehörige Hauptdivisor ist von der Form $(f) = \sum_{i=1}^r n_i Q_i$ mit $Q_1 = Q, n_1 \neq 0$. Wegen $n_1 Q_1 \sim -\sum_{i=2}^r n_i Q_i$ folgt daher $n_1 H_1 \sim -\sum_{i=2}^r n_i (C_1 \times Q_i)$, damit also $n_1 H_1.H_1 = 0$ und daraus schließlich $H_1^2 = 0$. Analog zeigt man $H_2^2 = 0$.*

Proposition 3.4.4 (Adjunktionsformel). *Ist C eine nichtsinguläre Kurve vom Geschlecht g auf der Fläche X und K der kanonische Divisor von X, so gilt*

$$2g - 2 = C.(C + K) \tag{28}$$

Beweis. [Ha77, V.1.5] □

Satz 3.4.5 (Hodge Index Theorem). *Sei H ein ampler Divisor auf einer Fläche X, D ein Divisor mit $D.H = 0$. Dann gilt entweder $D \equiv 0$ oder $D^2 < 0$.*

Beweis. [Ha77, V.1.9] □

Korollar 3.4.6. *Ist H ein ampler Divisor auf einer Fläche X, D ein beliebiger Divisor, so gilt*

$$(D^2)(H^2) \leq (D.H)^2 \tag{29}$$

Beweis. Setze $E := (H^2)D - (D.H)H$. Dann gilt $E.H = 0$, also

$$0 \geq E^2 = (H^2)^2(D^2) - 2(H^2)(D.H)^2 + (D.H)^2(H^2) = (H^2)[(H^2)(D^2) - (D.H)^2]$$

Wegen $H^2 > 0$ folgt die Behauptung. □

Lemma 3.4.7. *Sei erneut $X = C_1 \times C_2$ das Produkt zweier projektiver nichtsingulärer Kurven, die diesmal auch irreduzibel sein sollen. Wir betrachten wieder die Divisoren $H_1 = C_1 \times Q$ und $H_2 = P \times C_2$, $P \in C_1, Q \in C_2$. Seien $n, m \in \mathbb{N}$; dann ist der Divisor $H = mH_1 + nH_2$ ample.*

Beweis. Wegen $\deg(mQ) = m > 0$ ist mQ ample auf C_2, gleiches gilt für nP auf C_1 ([Ha77, IV.3.3]). Statt die Eigenschaft ample direkt auf H zu übertragen, nutzen wir die Tatsache aus, dass ein Divisor genau dann ample ist, wenn ein Vielfaches von ihm sehr ample über k ist. Damit reicht es also zu zeigen, dass H sehr ample über k ist, falls dies für mQ und nP gilt. Die Behauptung folgt damit aus folgender allgemeiner Aussage:

Seien X, Y zwei Schemata über einem Basisschema Z, $\mathcal{L}$ bzw. $\mathcal{M}$ sehr ample invertierbare Garben auf X bzw. Y. Dann ist die Garbe $\mathcal{L}\boxtimes\mathcal{M} := {\mathrm{pr}_1}^*\mathcal{L}\otimes{\mathrm{pr}_2}^*\mathcal{M}$ auf $X\times_S Y$ sehr ample über S.

Denn seien $\imath : X \hookrightarrow \mathbb{P}^r_S$ und $\jmath : Y \hookrightarrow \mathbb{P}^s_S$ die abgeschlossenen Immersionen, für die $\mathcal{L} = \imath^*(\mathcal{O}_{\mathbb{P}^r_S}(1))$ und $\mathcal{M} = \jmath^*(\mathcal{O}_{\mathbb{P}^s_S}(1))$. Bilden wir das Produkt von $\imath$ und $\jmath$, so erhalten wir eine abgeschlossene Immersion $f : X\times_S Y \hookrightarrow \mathbb{P}^r_S\times_S\mathbb{P}^s_S$, und es gilt $\mathcal{L}\boxtimes\mathcal{M} = f^*(\mathcal{O}_{\mathbb{P}^r_S}(1)\boxtimes\mathcal{O}_{\mathbb{P}^s_S}(1))$. Diese Abbildung verketten wir jetzt mit der Segre-Einbettung $g : \mathbb{P}^r_S\times\mathbb{P}^r_S \hookrightarrow \mathbb{P}^{rs+r+s}_S$ und beachten, dass offenbar nach Konstruktion $g^*(\mathcal{O}_{\mathbb{P}^{rs+r+s}_S}(1)) = \mathcal{O}_{\mathbb{P}^r_S}(1)\boxtimes\mathcal{O}_{\mathbb{P}^s_S}(1)$. Für $h = g\circ f : X\times_S Y \hookrightarrow \mathbb{P}^{rs+r+s}_S$ gilt damit $\mathcal{L}\boxtimes\mathcal{M} = h^*(\mathcal{O}_{\mathbb{P}^{rs+r+s}_S}(1))$, also ist $\mathcal{L}\boxtimes\mathcal{M}$ sehr ample über S. □

Bemerkung 3.4.8. *Im obigem Kontext sei $H_1' = C_1\times Q'$ ein weiterer Divisor mit $Q\neq Q'$. Für den Divisor $D = H_1 - H_1'$ gilt dann $D.H = D.(mH_1+nH_2) = 0$ und $D^2 = 0$, nach dem Hodge Index Theorem also $D\equiv 0$. Insbesondere hängt die numerische Äquivalenzklasse von $H_1 = C_1\times Q$ nicht von der Wahl von Q ab; man schreibt daher in der Regel einfach $H_1 = C_1\times \mathrm{pt}$. Gleiches gilt für $\mathrm{pt}\times C_2$.*

Proposition 3.4.9 (Ungleichung von Castelnuovo-Severi). *Sei X das Produkt zweier irreduzibler projektiver nichtsingulärer Kurven $X = C_1\times C_2$; sei $H_1 = C_1\times\mathrm{pt}$, $H_2 = \mathrm{pt}\times C_2$. Dann gilt für jeden Divisor D auf X mit $D.H_1 > 0$ und $D.H_2 > 0$*

$$D^2 \leq 2(D.H_1)(D.H_2), \tag{30}$$

mit Gleichheit genau dann, wenn $D\equiv (D.H_2)H_1 + (D.H_1)H_2$.

Beweis. Wie oben gezeigt, ist der Divisor $H = (D.H_2)H_1 + (D.H_1)H_2$ ample. Es gilt $H^2 = 2(D.H_1)(D.H_2) = D.H$; die Ungleichung ergibt sich nun unmittelbar aus Korollar 3.4.6. Wie man dem Beweis dieses Korollars und dem Hodge Index Theorem 3.4.5 entnehmen kann, gilt Gleichheit genau dann, wenn $(H^2)D - (D.H)H \equiv 0$, also $D\equiv H$. □

Proposition 3.4.10. *Sei $f : C_1\to C_2$ ein endlicher Morphismus von nichtsingulären projektiven Kurven vom Geschlecht g_1 bzw. g_2. Sei $\Gamma\subset X = C_1\times C_2$ der Graph von f. Dann gilt*

$$\Gamma.H_1 = \deg f,\quad \Gamma.H_2 = 1 \textit{ und } \Gamma^2 = (2-2g_2)\deg f; \tag{31}$$

dabei bezeichnen wir mit H_1 und H_2 wieder die Divisoren $C_1\times\mathrm{pt}$ und $\mathrm{pt}\times C_2$.

Beweis. Zuerst zeigen wir $\Gamma.H_1 = \deg f$. Die Verkettung $\mathrm{pr}_2\circ\Gamma$ ist der Morphismus f, und $\Gamma.H_1$ zählt offenbar gerade die Anzahl der Punkte von Γ (mit jeweiligen Vielfachheiten) über jedem der Punkte von C_2. Dieser Wert ist aber nach [Ha77, II.6.9] gerade $\deg f$. Analog zeigt man $\Gamma.H_2 = 1$.

Seien $K_1 = \sum m_iP_i$ und $K_2 = \sum n_jQ_j$ die kanonischen Divisoren von C_1 und C_2. Wie man leicht einsieht, gilt $\Omega_{X|k} = p_1^*\Omega_{C_1|k}\oplus p_2^*\Omega_{C_2|k}$ und daher $K =$

$p_1^* K_1 + p_2^* K_2 = \sum m_i \ P_i \times C_2 + \sum n_j \ C_1 \times Q_j$ (vgl. [Ha77, Ex. II.8.3]). Wegen $\deg K_1 = \sum m_i = 2g_1 - 2$ und $\deg K_2 = \sum n_j = 2g_2 - 2$ folgt somit

$$K \equiv (2g_1 - 2)H_2 + (2g_2 - 2)H_1$$

Insbesondere gilt $\Gamma.K = 2g_1 - 2 + (2g_2 - 2)\deg f$. Bedenkt man, dass Γ isomorph zu C_1 und daher auch von Geschlecht g_1 ist, so folgt aus der Adjunktionsformel (28) wie behauptet $\Gamma^2 = (2 - 2g_2)\deg f$. □

Nun betrachten wir wieder Schemata über einem endlichen Körper; bei der Untersuchung müssen wir aber zum algebraischen Abschluss übergehen. Daher gebrauchen wir folgende

Definition 3.4.11. *Ein Schema X vom endlichen Typ über einem Körper k heißt **geometrisch irreduzibel**, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:*

(i) $X \times_k \bar{k}$ ist irreduzibel; dabei bezeichne $\bar{k}$ den algebraischen Abschluss von k.

(ii) $X \times_k K$ ist irreduzibel für jede algebraische Erweiterung K von k (insbesondere ist X irreduzibel).

*Entsprechend definiert man **geometrisch reduziert** und **geometrisch ganz**.*

Satz 3.4.12. *Sei C eine geometrisch irreduzible glatte projektive Kurve vom Geschlecht g über einem endlichen Körper $k = \mathbb{F}_q$, F der Frobeniusmorphismus auf C. Dann gilt*

$$|\Lambda(F^n) - 1 - q^n| \leq 2gq^{\frac{n}{2}} \ \forall \, n \in \mathbb{N}. \tag{32}$$

Beweis. Wir betrachten die Kurve $\bar{C} = C \times_k \bar{k}$ über dem einem algebraischen Abschluss $\bar{k}$ von k und lassen F durch Basiswechsel darauf wirken. Dann entsprechen die geometrischen Punkte von C offenbar gerade den Punkten von $\bar{C}$, und daher ist $\Lambda(F^n)$ gerade gleich der Anzahl der Fixpunkte von $\bar{C}$ unter Wirkung von F^n.

$\bar{C}$ ist irreduzibel, glatt und projektiv, nach [Ha77, III.10.0.3] also auch nichtsingulär. Da Kohomologie mit flachen Basiswechsel vertauscht ([Ha77, III.9.3]), ist wegen $H^1(\bar{C}, \mathcal{O}_{\bar{C}}) = H^1(C, \mathcal{O}_C) \otimes_k \bar{k}$ offenbar auch $\bar{C}$ vom Geschlecht g. Man sieht leicht, dass $\deg F = q$. Sei nun $f = F^n$, $\Gamma = \Gamma_f \subset C \times C$ der Graph von f, $\Delta \subset C \times C$ die Diagonale. Nach Proposition 3.4.10 erhalten wir $\Delta.H_1 = \Delta.H_2 = 1, \Delta^2 = 2 - 2g$ für Δ und $\Gamma.H_1 = \deg f = q^n, \Gamma.H_2 = 1$, $\Gamma^2 = q^n(2 - 2g)$ für Γ.

Als nächstes zeigen wir, dass Γ und Δ sich transversal schneiden. Sei (x, x) ein Schnittpunkt von Γ und Δ. Für den Zariski-Kotangentialraum in (x, x) gilt $T^*_{(x,x)}(C \times C) = \mathfrak{m}_x/\mathfrak{m}_x^2 \oplus \mathfrak{m}_x/\mathfrak{m}_x^2$, wie man der Gleichung $\mathfrak{m}_{(x,x)} = \mathfrak{m}_x \otimes \mathcal{O}_x + \mathcal{O}_x \otimes \mathfrak{m}_x$ entnimmt. Ein Element $(\bar{a}, \bar{b}) \in T^*_{(x,x)}(C \times C)$ wird dabei repäsentiert durch das Element $a \otimes 1 + 1 \otimes b \in \mathfrak{m}_x \otimes \mathcal{O}_x + \mathcal{O}_x \otimes \mathfrak{m}_x$.

Der Diagonalmorphismus $\Delta : C \to C \times C$ wird auf der Ringseite bekanntlich induziert durch $a_1 \otimes a_2 \mapsto a_1 a_2$, daher wirkt $T^*_\Delta : T^*_{(x,x)}(C \times C) \to T^*_x C = \mathfrak{m}_x/\mathfrak{m}_x^2$ mittels $(\bar{a}, \bar{b}) \mapsto \bar{a} + \bar{b}$. Für den Graphen Γ von f hingegen gilt auf Ringseite $a_1 \otimes a_2 \mapsto a_1 \cdot f^\#(a_2)$, und als Basiswechsel des n-fachen Frobeniusendomorphismus bildet $f^\#$ das maximale Ideal $\mathfrak{m}_x$ in $\mathfrak{m}_x^{q^n}$ ab. Folglich wirkt die Abbildung $T^*_\Gamma : T^*_{(x,x)}(C \times C) \to T^*_x C$ mittels $(\bar{a}, \bar{b}) \mapsto \bar{a}$. Somit sind die Homomorphismen $(T^*_\Gamma, T^*_\Delta) : T^*_{(x,x)}(C \times C) \to T^*_x C \oplus T^*_x C$ und $T_\Gamma \oplus T_\Delta : T_x C \oplus T_x C \to T_{(x,x)}(C \times C)$ Isomorphismen. Γ und Δ schneiden sich also transversal. Aus der Definition der Schnittzahl folgt $N := \Gamma.\Delta = \#(\Gamma \cap \Delta) = \Lambda(F^n)$.

Für $D = r\Gamma + s\Delta$ gilt nach (30)

$$r^2 q^n (2 - 2g) + 2rsN + s^2(2 - 2g) = D^2 \leq 2(D.H_1)(D.H_2) = 2(r + s)(q^n r + s),$$

also $2gq^n r^2 + 2(1 + q^n - N)rs + 2gs^2 \geq 0 \;\forall\, r, s \in \mathbb{Z}$. Damit gilt notwendigerweise für die Diskriminante: $4(1+q^n-N)^2 - 4 \cdot 2gq^n \cdot 2g \leq 0$; daraus schließlich erhalten wir unsere Behauptung. □

3.5 L-Funktionen für Kurven

Auf dem Weg zum Beweis der analytischen Fortsetzbarkeit müssen wir uns zunächst einem Spezialfall zuwenden, dem klassischen Fall von Weil: Kurven über einem endlichen Körper. Sei im folgenden also X eine ganze, projektive und glatte Kurve vom Geschlecht g_X mit endlichem Konstantenkörper l. Auf X (und damit automatisch auch auf l) wirke eine endliche Gruppe G in zulässiger Weise, sei $Y = X/G$ der Quotient, k der Konstantenkörper und g_Y das Geschlecht von Y; Y ist ebenfalls ganz, projektiv (über k), und es gilt $k = l^G$. Außerdem ist Y glatt: Für Kurven über perfekten Körpern bedeutet glatt nichts anderes als normal; da X aber somit normal ist, muss es Y als Quotientenschema auch sein (auf Ringseite folgt nämlich aus B ganz abgeschlossen automatisch auch $A = B^G$ ganz abgeschlossen).

Betrachten wir nun die folgenden beiden Bemerkungen:

Fakt 3.5.1. *Sei X ein ganzes Schema v.e.T. über einem Körper k. Dann gilt:*

(i) X ist geometrisch irreduzibel genau dann, wenn k separabel-algebraisch abgeschlossen in $K(X)$ ist.

(ii) X ist geometrisch reduziert genau dann, wenn $K(X)$ separabel über k ist (d.h. es gibt eine Transzendenzbasis $T_1, \ldots T_r$ von $K(X)|k$ so, dass $K(X)$ algebraisch separabel über $k(T_1, \ldots, T_r)$ ist).

Beweis. [Mu99, II.4.4] □

Fakt 3.5.2. *Über einem perfekten Körper ist jeder Erweiterungskörper separabel.*

Beweis. [Ma86, 26.3] □

Folglich sind die Kurven X bzw. Y geometrisch ganz über l bzw. k, lassen sich also mit Satz 3.4.12 behandeln. Dies werden wir im folgenden ausnützen. Vorher brauchen wir allerdings noch ein paar Bezeichnungen und Konventionen. G wirke treu auf $K(X)|K(Y)$, und mit G' werde in diesem Abschnitt immer die Untergruppe von G bezeichnet, die trivial auf l wirkt, so dass also G/G' die Galoisgruppe von $l|k$ darstellt. Desweiteren sei $q := \#k$, und φ_k bezeichne den Frobenius von $\bar{k}|k$ (d.h. $z \mapsto z^q \ \forall\, z \in \bar{k}$), wobei $\bar{k}$ ein algebraischer Abschluss von k ist. Dieser Frobenius lässt sich auf jede endliche Erweiterung von k eindeutig einschränken. Schließlich benötigen wir noch folgende

Definition 3.5.3. *Sei $\mathcal{C}$ eine Konjugationsklasse in G, $d, n \in \mathbb{N}$. Wir definieren*

$$C_d(X/Y) = \{y \in \overline{Y} |\, y \text{ unverzweigt in } X, \deg_k y = d\},$$

$$C_{d,n}(X/Y, \mathcal{C}) = \{y \in C_d(X/Y) |\, F_x^n \in \mathcal{C} \text{ für ein (alle) } x \in X \text{ über } y\}.$$

Offenbar gilt $C_d(X/Y) = \dot{\bigcup}_{\mathcal{C}} C_{d,n}(X/Y, \mathcal{C})$ für alle festen d und n.

Die Verbindung zu unseren bisherigen Untersuchungen zeigt sich unmittelbar in folgender Aussage:

Lemma 3.5.4. *Bezeichnen wir mit $\Lambda_{\mathrm{uv}}(\sigma^{-1}F^n)$ die Anzahl der über Y unverzweigten Fixpunkte von $\sigma^{-1}F^n$ bei Wirkung auf $X(\bar{k})$, so gilt*

$$\sum_{\sigma \in \mathcal{C}} \Lambda_{\mathrm{uv}}(\sigma^{-1}F^n) = \operatorname{ord} G \cdot \sum_{d|n} d \cdot \# C_{d,\frac{n}{d}}(X/Y, \mathcal{C}) \tag{33}$$

Beweis. Wie im Beweis von Proposition 3.3.4 sieht man zunächst, dass

$$\Lambda_{\mathrm{uv}}(\sigma^{-1}F^n) = \sum_{\substack{x \in \overline{X};\, x \text{unverzweigt über } Y \\ \deg(y)|n;\, \sigma = F_x^{n/\deg y}}} \deg x = \sum_{d|n} \sum_{\substack{x \in \overline{X};\, x \text{unverzweigt über } Y \\ \deg(y) = d;\, \sigma = F_x^{n/d}}} d \cdot \operatorname{ord} D(x).$$

Nun summieren wir diese Ausdrücke und sortieren neu nach dem Bild y von x in Y. Die Summe läuft gerade über alle $y \in C_{d,\frac{n}{d}}(X/Y, \mathcal{C})$ mit $d|n$, und über jedem solchen Punkt liegen $(G : D(x))$ Urbilder (dabei sei x eines von diesen). Es folgt

$$\sum_{\sigma \in \mathcal{C}} \Lambda_{\mathrm{uv}}(\sigma^{-1}F^n) = \sum_{d|n} \sum_{y \in C_{d,\frac{n}{d}}(X/Y,\mathcal{C})} d \cdot \operatorname{ord} G = \operatorname{ord} G \cdot \sum_{d|n} d \cdot \# C_{d,\frac{n}{d}}(X/Y, \mathcal{C}). \quad \square$$

Lemma 3.5.5. *Für die Kardinalität der $C_d(X/Y)$ gilt:*

$$\# C_d(X/Y) \le \frac{2 + 2g_Y}{d}\, q^d. \tag{34}$$

Beweis. Vergessen wir für kurze Zeit einmal die Überlagerung X und betrachten nur die Kurve Y, so gilt wegen $\deg y = d \; \forall \; y \in C_d(X/Y)$ nach (25) trivialerweise $d \cdot \#C_d(X/Y) \leq \nu_d(Y)$. Nach (32) folgt unmittelbar

$$\nu_d(Y) = \Lambda_d(F^d) \leq 1 + q^d + 2g_Y q^{d/2} < (2 + 2g_Y)q^d$$

und daraus die Behauptung. □

Korollar 3.5.6. *Es gilt*

$$|\sum_{\sigma \in \mathcal{C}} \Lambda_{\mathrm{uv}}(\sigma^{-1}F^n) - \operatorname{ord} G \cdot n \cdot \#C_{n,1}(X/Y, \mathcal{C})| \leq 4(g_Y + 1)q^{\frac{n}{2}} \tag{35}$$

Beweis. Nach den Lemmata 3.5.4 und 3.5.5 folgt

$$|\sum_{\sigma \in \mathcal{C}} \Lambda_{\mathrm{uv}}(\sigma^{-1}F^n) - \operatorname{ord} G \cdot n \cdot \#C_{n,1}(X/Y, \mathcal{C})|$$

$$\overset{(33)}{=} \sum_{d|n; d<n} d \cdot \#C_{d,\frac{n}{d}}(X/Y, \mathcal{C}) \leq \sum_{d \leq \frac{n}{2}} d \cdot \#C_d(X/Y) \overset{(34)}{\leq} \sum_{d \leq \frac{n}{2}} (2 + 2g_Y)q^d$$

$$\leq (2 + 2g_Y) \sum_{d=0}^{[\frac{n}{2}]} q^d \leq (2 + 2g_Y) \left(q^{[\frac{n}{2}]} + \frac{q^{[\frac{n}{2}]} - 1}{q - 1} \right) \leq 4(g_Y + 1)q^{\frac{n}{2}} \qquad \square$$

Damit lässt sich $\sum_{\mathcal{C}} \Lambda_{\mathrm{uv}}(\sigma^{-1}F^n)$ gegen einen Term in $\#C_{n,1}(X/Y, \mathcal{C})$ abschätzen. Wie wir später sehen werden, ist dies der wesentliche Beitrag zu dieser Summe; daher betrachten wir im folgenden nur noch Mengen dieser Form und lassen, da dann keine Verwechslungen auftreten können, den zweiten Index weg:

$$C_d(X/Y, \mathcal{C}) := C_{d,1}(X/Y, \mathcal{C}) = \{y \in C_d(X/Y) | \, F_x \in \mathcal{C} \text{ für alle } x \in X \text{ über } y\}$$

Wir wollen nun die Kardinalität dieser Mengen abschätzen. Dazu brauchen wir einige Hilfssätze; wir orientieren uns dabei an [FJ86, 5.4].

Lemma 3.5.7. *Sei H eine Untergruppe von G, $Y' = X/H$, $k' = l^H$; zu einem Element $\sigma \in H$ seien $\mathcal{C}$ bzw. $\mathcal{C}'$ die zugehörigen Konjugationsklassen in G bzw. H. Sei d ein Vielfaches von $r := [k' : k]$; setze*

$$C'_{d/r} = C_{d/r}(X/Y', \mathcal{C}') - \{y' \in \overline{Y}' | \text{ für das Bild } y \text{ von } y' \text{ in } Y \text{ gilt } \deg_k y \leq \frac{d}{2}\}.$$

Dann gilt

$$\#C_d(X/Y, \mathcal{C}) = \frac{\#\mathcal{C} \cdot \#C'_{d/r}}{\#\mathcal{C}' \cdot (G : H)} \tag{36}$$

Beweis. Für einen Punkt $y' \in C_{d/r}(X/Y', \mathcal{C}')$ und sein Bild y in Y ist $\deg_k y$ ein Teiler von $\deg_k y' = [k' : k] \deg_{k'} y' = r \cdot \frac{d}{r} = d$; folglich gilt zunächst $C'_{d/r} = C_{d/r}(X/Y', \mathcal{C}') \cap \{y' \in \overline{Y}' | \deg_k \pi_Y(y') = d\}$.

Nehmen wir nun einen Punkt $y \in C_d(X/Y, \mathcal{C})$. Über diesem liegt ein Punkt $x \in X$ mit $F_x = \sigma$; sei y' das Bild von x in Y'. Wegen $\sigma \in H$ und $Y' = X/H$ wirkt σ trivial auf $k(y')$; es folgt daher $k(y') = k(y)$ und damit $F'_x = \sigma$ sowie $\deg_{k'} y' = \frac{1}{r} \deg_k y = \frac{d}{r}$, also $y' \in C'_{d/r}$. Ist umgekehrt $y' \in C'_{d/r}$, y das Bild in Y und $x \in X$ ein Punkt darüber mit $F'_x = \sigma$, so folgern wir rückwärts, dass $k(y) = k(y')$ und daher auch $F_x = \sigma$ gilt, also $y \in C_d(X/Y, \mathcal{C})$.

Um die Anzahlen zu vergleichen, zählen wir einfach, wie viele Punkte $x \in X$ mit $F_x = \sigma$ über einem gegebenem $y \in C_d(X/Y, \mathcal{C})$ bzw. $y' \in C'_{d/r}$ liegen. Nimmt man einen festen Punkt x_0 mit $F_{x_0} = \sigma$ heraus, so haben gerade die Punkte τx_0 mit $\tau \in Z_G(\sigma)$ bzw. $Z_H(\sigma)$ den gleichen Frobenius; davon sind aber je $\operatorname{ord} D(x_0) = \operatorname{ord} \sigma$ identisch. Damit erhalten wir

$$\#C_d(X/Y, \mathcal{C}) \frac{\# Z_G(\sigma)}{\operatorname{ord} \sigma} = \# C'_{d/r} \frac{\# Z_H(\sigma)}{\operatorname{ord} \sigma}$$

und daraus wegen $\#\mathcal{C} = (G : Z_G(\sigma)), \#\mathcal{C}' = (H : Z_H(\sigma))$ die Behauptung. □

Korollar 3.5.8. *Im Kontext des vorigen Lemmas 3.5.7 gilt*

$$|\#C_d(X/Y, \mathcal{C}) - \frac{\#\mathcal{C}}{\#\mathcal{C}' \cdot (G : H)} \#C_{d/r}(X/Y', \mathcal{C}')| \leq 4 \frac{\#\mathcal{C}}{\#\mathcal{C}'} (g_Y + 1) q^{\frac{d}{2}} \tag{37}$$

Beweis. Ist $\pi_Y : Y' \to Y$ der Quotientenmorphismus, so gilt nach Definition $\pi_Y(C_{d/r}(X/Y', \mathcal{C}') - C'_{d/r}) \subseteq \bigcup_{m \leq \frac{d}{2}} C_m(Y/Y)$ (man beachte, dass man hier nicht $C_m(X/Y)$ schreiben darf, da wir über die Verzweigtheit der Punkte in der Ausnahmemenge keine Aussage gemacht hatten). Nach Lemma 3.5.5 gilt

$$\frac{1}{2g_Y + 2} \cdot \# \left(\bigcup_{m \leq \frac{d}{2}} C_m(Y/Y) \right) \leq \sum_{m=1}^{[\frac{d}{2}]} \frac{q^m}{m} \leq (q^{\frac{d}{2}} + \sum_{m=0}^{[\frac{d}{2}]-1} q^m) = q^{\frac{d}{2}} + \frac{q^{[\frac{d}{2}]} - 1}{q - 1} \leq 2q^{\frac{d}{2}}.$$

Über jedem Punkt in Y liegen höchstens $\deg \pi_Y = [K(Y') : K(Y)] = (G : H)$ Punkte in Y' (vgl. [Ha77, II.6.9]), daher erhalten wir $|\#C_{d/r}(X/Y', \mathcal{C}') - \#C'_{d/r}| \leq 4(G : H)(g_Y + 1) q^{\frac{d}{2}}$. Multiplizieren wir diese Ungleichung mit $\frac{\#\mathcal{C}}{\#\mathcal{C}' \cdot (G:H)}$ und verwenden nun (36), so ergibt sich die Behauptung. □

Lemma 3.5.9. *Zu gegebenem $n \in \mathbb{N}$ setze man $X^{(n)} = X \times_l l_n$; dabei sei l_n die Körpererweiterung von l vom Grad n. $X^{(n)}$ ist ebenfalls eine ganze, projektive und glatte Kurve vom Geschlecht $g_{X^{(n)}} = g_X$ und mit Konstantenkörper l_n.*

Zu jedem $\sigma \in G$ und jedem $d \in \mathbb{N}$ mit $\sigma|_l = \varphi_k^m|_l$ gibt es einen Automorphismus σ' von $X^{(n)}$, so dass $\sigma'|_X = \sigma$ und $\sigma'|_{l_n} = \varphi_k^m|_{l_n}$. Auf diese Weise entsteht

$$\begin{tikzcd}
X^{(n)} \arrow[rr] \arrow[dd] \arrow[dr, "\sigma'"'] & & \operatorname{Spec} l_n \arrow[dd] \arrow[dr, "\varphi_k^m|_{l_n}"] & \\
& X^{(n)} \arrow[rr] \arrow[dd] & & \operatorname{Spec} l_n \arrow[dd] \\
X \arrow[rr] \arrow[dr, "\sigma"'] & & \operatorname{Spec} l \arrow[dr, "\sigma|_l = \varphi_k^m|_l"'] & \\
& X \arrow[rr] & & \operatorname{Spec} l
\end{tikzcd}$$

eine Gruppe $G^{(n)}$, die auf zulässige Weise auf $X^{(n)}$ operiert und für die gilt: $X^{(n)}/G^{(n)} = Y$. Die Menge $G^{(n)'}$ aller $\sigma' \in G^{(n)}$, die trivial auf l_n wirken, ist gerade $\{\sigma' \in G^{(n)} : \sigma'|_X \in G', \sigma'|_{l_n} = \mathrm{id}_{l_n}\}$; insbesondere gilt $\operatorname{ord} G^{(n)'} = \operatorname{ord} G'$.

Seien nun $\tau \in G$, $d \in \mathbb{N}$ mit $\tau|_l = \varphi_k^d|_l$ fest gewählt, $\mathcal{C}$ die zugehörige Konjugationsklasse in G. Für $\tau' = (\tau, \varphi_k^d)$ gilt dann $\operatorname{ord} \tau' = \operatorname{kgV}(\operatorname{ord} \tau, [l_n : l_n \cap k_d])$. *Die Menge $\mathcal{C}' = \{\sigma' \in G^{(n)} : \sigma'|_X \in \mathcal{C}, \sigma'|_{l_n} = \varphi_k^d|_{l_n}\}$ ist die Konjugationsklasse von τ' in $G^{(n)}$, und es gilt $C_d(X^{(n)}/Y, \mathcal{C}') = C_d(X/Y, \mathcal{C})$.*

Beweis. Nach den obigen Ausführungen ist X geometrisch ganz über l, daher ist $X^{(n)}$ ganz; für den Quotientenkörper gilt offenbar $K(X^{(n)}) = K(X) \cdot l_n$, daher ist der Konstantenkörper von $X^{(n)}$ gerade l_n. Projektivität und Glattheit sind stabil unter Basiswechsel, und die Argumentation für das Geschlecht hatten wir in ähnlicher Form schon im Beweis von Satz 3.4.12.

Die Aussagen über die Gruppenwirkung $G^{(n)}$ entnimmt man leicht der Tatsache, dass $K(X) \cap l_n = l$ und $K(X^{(n)}) = K(X) l_n$ (vgl. auch obiges Diagramm); $X^{(n)}/G^{(n)} = Y$ ist dann klar nach Konstruktion. Die Aussage über $G^{(n)'}$ ist dann ebenfalls trivial.

Für die Ordnung von $\tau' = (\tau, \varphi^k)$ beachte man

$$\operatorname{ord} \tau' = \operatorname{kgV}(\operatorname{ord} \tau'|_X, \operatorname{ord} \tau'|_{l_n}) = \operatorname{kgV}(\operatorname{ord} \tau, \operatorname{ord} \varphi^k|_l) = \operatorname{kgV}(\operatorname{ord} \tau, [l_n : l_n \cap k_k]).$$

Die Aussage über $\mathcal{C}'$ ist klar aus der Tatsache, dass die Erweiterung $l_n|l$ abelsch ist. Zu $C_d(X^{(n)}/Y, \mathcal{C}') = C_d(X/Y, \mathcal{C})$: Sei zunächst $y \in C_d(X/Y, \mathcal{C})$, $x \in X$ ein Punkt darüber mit $F_x = \tau$. Sei $V = \operatorname{Spec} A$ eine offene affine Umgebung von y in Y, $U = \operatorname{Spec} B$ das Urbild in X und $U^{(n)} = \operatorname{Spec} B'$ (mit $B' = B \otimes_l l_n$) das Urbild in $X^{(n)}$. Sei $\mathfrak{q}$ das Primideal von B, das zu x gehört. Dann gilt $\tau b \equiv b^{q^d} \mod \mathfrak{q}\ \forall\, b \in B$. Wegen $\tau'|_{l_n} = \varphi_k^d|_{l_n}$ gilt $\tau' l' = l'^{q^d}\ \forall\, l' \in l_n$ und daher $\tau' b' \equiv b'^{q^d} \mod \mathfrak{q} \otimes l_n\ \forall\, b' \in B'$. Jedes Primideal $\mathfrak{q}' \subset B'$ über $\mathfrak{q}$ enthält notwendigerweise $\mathfrak{q} \otimes l_n$, also gilt für jeden (!) Punkt $x' \in X^{(n)}$ über x: $\bar{\tau}' = F_{x'}$. Es bleibt zu zeigen, dass y auch in $X^{(n)}$ unverzweigt ist. Für jedes $\sigma' \in G^{(n)}$ mit $\bar{\sigma}' = F_{x'}$ folgt wegen $k(x), l_n \subseteq k(x')$ unmittelbar $\sigma'|_X = F_x = \tau$ und $\sigma'|_{l_n} = \varphi_k^d|_{l_n}$, also $\sigma' = \tau'$; daher gilt $y \in C_d(X^{(n)}/Y, \mathcal{C}')$, d.h. $C_d(X^{(n)}/Y, \mathcal{C}') \subseteq C_d(X/Y, \mathcal{C})$. Die umgekehrte Inklusion ist trivial. □

Korollar 3.5.10. *Gilt $G' = 1$, so folgt $g_X = g_Y$; für $\tau \in G$ mit $\tau|_l = \varphi_k^d|_l$ gilt*

$$C_d(X/Y, \{\tau\}) = C_d(Y/Y, 1) = C_d(Y/Y). \tag{38}$$

Beweis. In diesem Fall gilt nämlich gerade $X = Y^{(n)}$ und $G = \{\mathrm{id}_Y\}^{(n)}$ mit $n = \operatorname{ord} G$, wie man leicht nachprüft. □

Proposition 3.5.11. *Seien $d \in \mathbb{N}$, $\tau \in G$ und $\mathcal{C}$ die zugehörige Konjugationsklasse. Gilt $\tau|_l \neq \varphi_k^d|_l$, so ist $C_d(X/Y, \mathcal{C})$ leer. Gilt dagegen $\tau|_l = \varphi_k^d|_l$, so folgt*

$$|\#C_d(X/Y, \mathcal{C}) - \frac{\#\mathcal{C}}{d \cdot \operatorname{ord} G'}\, q^d| < \#\mathcal{C} \cdot 2(g_X + 2g_Y + 3) \cdot q^{\frac{d}{2}} \tag{39}$$

Beweis. Ist $y \in C_d(X/Y, \mathcal{C})$, so gibt es darüber einen Punkt $x \in \overline{X}$ mit $F_x = \tau$, wegen $\#k(y) = q^d$ also $\tau a = a^{q^d}$ $\forall\, a \in k(x)$, somit wegen $l \subseteq k(x)$ auch $\tau|_l = \varphi_k^d|_l$. Damit ist der erste Punkt erledigt.

Sei nun also $\tau|_l = \varphi_k^d|_l$. Indem wir von X zu der Überlagerung $X^{(n)}$ mit $n = d \cdot \operatorname{ord} \tau$ übergehen, können wir oBdA davon ausgehen, dass $k_d \subset l$ und $\operatorname{ord} \tau = [l : k_d]$ (dies folgt aus Lemma 3.5.9; man beachte, dass $g_{X^{(n)}} = g_X$, $\operatorname{ord} G^{(n)'} = \operatorname{ord} G'$ und $C_d(X^{(n)}/Y, \mathcal{C}') = C_d(X/Y, \mathcal{C})$).

Wir betrachten jetzt die Untergruppe $H = <\tau>$ und den zugehörigen Quotientenraum $Y' = X/H$. Wegen $\operatorname{ord} \tau = [l : k_d]$ gilt $d \cdot \operatorname{ord} H = [l : k]$; da andererseits G/G' gerade die Galoisgruppe von $l|k$ darstellt, folgt $(G : H) = d \cdot \operatorname{ord} G'$. Zudem gilt wegen $\tau|_l = \varphi_k^d|_l$ und $k_d \subseteq l$ in der Sprechweise von Lemma 3.5.7 $k' = l^H = l^\tau = k_d$, also $r = [k' : k] = d$. Die Konjugationsklasse von τ in H ist $\mathcal{C}' = \{\tau\}$; nach Korollar 3.5.8 gilt also

$$|\#C_d(X/Y, \mathcal{C}) - \frac{\#\mathcal{C}}{d \cdot \operatorname{ord} G'}\, \#C_1(X/Y', \{\tau\})| \leq 4\#\mathcal{C}(g_Y + 1) q^{\frac{d}{2}} \tag{40}$$

Wegen $\operatorname{ord} H = [l : k']$ wirkt H treu auf $l|k'$; also gilt für die Untergruppe von H, die trivial auf l wirkt, $H' = 1$. Wegen $\tau|_l = \varphi_k^d|_l = \varphi_{k'}|_l$ folgt nach Korollar 3.5.10: $C_1(X/Y', \{\tau\}) = C_1(Y'/Y')$. Die Kardinalität der letzteren Menge ist offenbar gerade $\nu_1(Y')$ (bei der trivialen Überlagerung haben wir keine Probleme mit Verzweigung). Nach (32) haben daher $|\nu_1(Y') - q^d| \leq 1 + 2g_X\, q^{\frac{d}{2}}$ (man beachte, dass $g_X = g_{Y'}$ und $\operatorname{card} K' = q^d$); daraus erhalten wir durch Multiplikation mit $\frac{\#\mathcal{C}}{d \cdot \operatorname{ord} G'}$

$$|\frac{\#\mathcal{C}}{d \cdot \operatorname{ord} G'}\, \#C_1(X/Y', \{\tau\}) - \frac{\#\mathcal{C}}{d \cdot \operatorname{ord} G'}\, q^d| \leq \frac{\#\mathcal{C} \cdot (1 + 2g_X)}{d \cdot \operatorname{ord} G'}\, q^{\frac{d}{2}} \tag{41}$$

Addition von (40) und (41) ergibt

$$|\#C_d(X/Y,\mathcal{C}) - \frac{\#\mathcal{C}}{d\cdot \operatorname{ord} G'}\, q^d| \le \#\mathcal{C}\cdot q^{\frac{d}{2}}\left(4(g_Y+1) + \frac{1+2g_X}{d\cdot \operatorname{ord} G'}\right)$$

Daraus folgt unmittelbar die Behauptung. □

Korollar 3.5.12. *Mit obigen Bezeichnungen gilt* $\Lambda_{\mathrm{uv}}(\sigma^{-1}F^n) = 0$ *für* $\sigma|_l \neq \varphi^n|_l$*; im Fall* $\tau|_l = \varphi^n|_l$ *gilt für die Konjugationsklasse* $\mathcal{C}$ *von* τ

$$|\sum_{\sigma\in\mathcal{C}} \Lambda_{\mathrm{uv}}(\sigma^{-1}F^n) - (G:G')\cdot\#\mathcal{C}\cdot q^n| \le \#\mathcal{C}\cdot \operatorname{ord} G\cdot 2(g_X+4g_Y+5)\cdot nq^{\frac{n}{2}} \quad (42)$$

Beweis. Diese leichte Folgerung aus (35) und (39) sei dem Leser überlassen. □

Proposition 3.5.13. *Sei* X_{uv} *das offene Unterschema von* X*, das aus allen über* Y *unverzweigten Punkten von* X *besteht. Auch auf* X_{uv} *wirkt* G *auf zulässige Weise, und es gilt*

$$\begin{aligned} &|\log L(X_{\mathrm{uv}},\chi;s) - \log L(\operatorname{Spec} l,\chi;s-1)| \\ \le\ & ||\chi||\cdot \operatorname{ord} G\cdot 4(g_X+4g_Y+5)\left(-\frac{\zeta'(\operatorname{Spec} k;\operatorname{Re} s-\frac{1}{2})}{\zeta(\operatorname{Spec} k;\operatorname{Re} s-\frac{1}{2})}\right) \end{aligned} \quad (43)$$

Beweis. Nach Proposition 3.3.4 gilt

$$\log L(X_{\mathrm{uv}},\chi;t) = \sum_{n=1}^{\infty} \frac{\nu_n(X_{\mathrm{uv}},\chi)t^n}{n}$$

mit

$$\nu_n(X_{\mathrm{uv}},\chi) = \frac{1}{\operatorname{ord} G}\sum_{\sigma\in G}\chi(\sigma)\Lambda_{\mathrm{uv}}(\sigma^{-1}F^n),$$

und für die Ein-Punkt-Schemata $\operatorname{Spec} l$ und $\operatorname{Spec} k = \{y_0\}$ gilt nach Definition 3.2.1

$$\log L(\operatorname{Spec} l,\chi;qt) = \sum_{n=1}^{\infty}\frac{\chi(y_0^n)q^nt^n}{n}.$$

mit

$$\chi(y_0^n) = \frac{1}{\operatorname{ord} G'}\sum_{\substack{\sigma\in G\\ \sigma|_l=\varphi_k^n|_l}}\chi(\sigma).$$

Betrachten wir die jeweiligen Koeffizienten von $\frac{t^n}{n}$. Es gilt nach Korollar 3.5.12

$$\begin{aligned}
|\nu_n(X_{\mathrm{uv}},\chi)-\chi(y_0^n)q^n| &= \left|\frac{1}{\operatorname{ord} G}\sum_{\sigma\in G}\chi(\sigma)\Lambda_{\mathrm{uv}}(\sigma^{-1}F^n) - \frac{1}{\operatorname{ord} G'}\sum_{\substack{\sigma\in G\\ \sigma|_l=\varphi_k^n|_l}}\chi(\sigma)q^n\right| \\
&= \frac{1}{\operatorname{ord} G}\left|\sum_{\substack{\sigma\in G\\ \sigma|_l=\varphi_k^n|_l}}\chi(\sigma)\left(\Lambda_{\mathrm{uv}}(\sigma^{-1}F^n)-(G:G')q^n\right)\right| \\
&= \frac{1}{\operatorname{ord} G}\left|\sum_{\mathcal{C}:\mathcal{C}\mapsto\varphi_k^n|_l}\chi(\mathcal{C})\left(\sum_{\sigma\in\mathcal{C}}\Lambda_{\mathrm{uv}}(\sigma^{-1}F^n)-\#\mathcal{C}(G:G')q^n\right)\right| \\
&\le \frac{||\chi||}{\operatorname{ord} G}\sum_{\mathcal{C}:\mathcal{C}\mapsto\varphi_k^n|_l}\#\mathcal{C}\cdot\operatorname{ord} G\cdot 2(g_X+4g_Y+5)\cdot nq^{\frac{n}{2}} \\
&= ||\chi||\cdot(G:G')\cdot 2(g_X+4g_Y+5)\cdot nq^{\frac{n}{2}}
\end{aligned}$$

Dabei beachte man, dass alle Elemente innerhalb einer Konjugationsklasse den gleichen Charakter und die gleiche Wirkung auf l haben, es daher Sinn hat, von $\chi(\mathcal{C})$ und $\mathcal{C}\mapsto\varphi_k^n|_l$ zu sprechen.

Mit $t=q^{-s}$, also $qt=q^{-(s-1)}$ folgt daher aus dem bisherigen

$$\begin{aligned}
&|\log L(X_{\mathrm{uv}},\chi;s)-\log L(\operatorname{Spec} l,\chi;s-1)| \\
&\le \sum_{n=1}^{\infty}\frac{||\chi||\cdot(G:G')\cdot 2(g_X+4g_Y+5)\cdot nq^{\frac{n}{2}}\cdot|q^{-ns}|}{n} \\
&= ||\chi||\cdot(G:G')\cdot 2(g_X+4g_Y+5)\cdot\sum_{n=1}^{\infty}q^{-n(\operatorname{Re} s-\frac{1}{2})}
\end{aligned}$$

Mit $\frac{\zeta'(\operatorname{Spec} k;s)}{\zeta(\operatorname{Spec} k;s)} = \frac{d}{ds}(\log\zeta(\operatorname{Spec} k;s)) = -\log q\cdot\sum_{n=1}^{\infty}q^{-ns}$ und $\log q\ge\frac{1}{2}$ wegen $q^2\ge 4\ge e$ folgt schließlich die Behauptung. □

3.6 Analytische Fortsetzung von L-Funktionen

Um den Satz von Cebotarev zu beweisen, müssen wir die analytische Struktur der L-Funktionen besser untersuchen. Wir benötigen hier nicht so machtvolle Aussagen wie die Rationalität der Zetafunktion über einem endlichen Körper; wir brauchen lediglich die meromorphe Fortsetzbarkeit in eine Umgebung von $s=\dim X$, dies aber für allgemeine Zeta- und L-Funktionen (also nicht nur über einem endlichen Körper).

Es wird nicht verwundern, dass entsprechende Ergebnisse für Artinsche L-Funktionen im Fall von Zahlkörpern bereits lange bekannt sind; schließlich war dies genau der Fall, in dem Artin sie 1923 als Verallgemeinerung der Dirichletschen L-Reihen einführte ([Ar23]). Wir zitieren hier nur folgenden

Fakt 3.6.1. *Sei* $X = \operatorname{Spec} \mathcal{O}_L$ *für einen Zahlkörper* L *und* G *eine endliche Gruppe, die auf* X *operiere (per definitionem auf zulässige Weise);* G *wirke treu auf* $L = K(X)$*. Für jeden Charakter* χ *von* G *ist die L-Funktion* $L(X, \chi; s)$ *dann auf ganz* $\mathbb{C}$ *meromorph fortsetzbar. Ist* χ *irreduzibel und nicht-trivial, so ist* $L(X, \chi; s)$ *bei* $s = 1$ *holomorph und* $\neq 0$*; für* $\chi = 1$ *hingegen besitzt* $L(X, \chi; s)$ *bei* $s = 1$ *einen Pol der Ordnung 1.*

Beweis. Mit $Y = X/G$, $K := K(Y) = L^G$ ist G gerade die Galoisgruppe von $L|K$. Die Idee des Beweises ist, sich mit Hilfe eines Theorems von Brauer auf abelsche Erweiterungen $L|K$ und damit abelsche irreduzible Charaktere zu beschränken; in diesem Fall ist $L(X, \chi; s)$ bis auf die Faktoren an den verzweigten Stellen eine Dirichletsche L-Reihe. Damit ist die Aussage dann klar. Für Details vergleiche man die gut lesbaren Darstellungen aus [Ne92, VII.10 und VII.12, insbesondere VII.12.6] und [CF67, VIII.3, insbesondere Theorem 7 und die folgenden Anmerkungen]. □

Im allgemeinen Fall lässt sich zwar nicht die Fortsetzbarkeit auf die gesamte komplexe Ebene zeigen (zumindest ist ein solcher Beweis meines Wissens bis heute nicht gelungen); allerdings reicht uns auch ein schwächeres Ergebnis, nämlich die meromorphe Fortsetzbarkeit auf die Halbebene $\operatorname{Re} s > \dim X - \frac{1}{2}$.

Einen wesentlichen Schritt dem Beweis dieser Aussage haben wir bereits im letzten Abschnitt gemacht (auch wenn es noch nicht aufgefallen sein sollte). Unser Beweis der meromorphen Fortsetzbarkeit wird nämlich mittels eines Faserungsargument induktiv nach $\dim X$ verlaufen. Wie das genau aussehen soll, verrät folgendes

Lemma 3.6.2. *Sei* G *eine endliche Gruppe, die auf zwei ganzen Schemata* $\hat{X}$, X' *(v.e.T. über* $\mathbb{Z}$*) auf zulässige Weise operiert.* $h : \hat{X} \to X'$ *sei ein dominanter flacher Morphismus, der mit der Wirkung der Gruppe* G *vertauscht. Alle Fasern des Morphismus seien geometrisch ganz. Auch für die Quotienten* $\hat{Y} = \hat{X}/G$ *und* $Y' = X'/G$ *sei der Morphismus* $Y \to Y'$ *dominant und flach, auch hier seien alle Fasern geometrisch ganz. Es gebe einen endlichen dominanten Morphismus* $Y \to \mathbb{P}^1_{Y'}$*, über den dieser Morphismus faktorisiere. In* $\mathbb{P}^1_{Y'}$ *existiere ein offenes Unterschema* $\mathbb{A}^1_{Y'}$*, so dass für dessen Urbilder* $X \subset \hat{X}$ *und* $Y \subset \hat{Y}$ *gilt:* X *ist unverzweigt über* Y *und glatt über* X' *(siehe auch die Abbildung auf der nächsten Seite).*

Sei χ *ein beliebiger Charakter von* G*. Dann lässt sich die Funktion*

$$H(s) = \frac{L(X, \chi; s)}{L(X', \chi; s - 1)}$$

auf die Halbebene $\operatorname{Re} > \dim X - \frac{1}{2}$ *holomorph und ohne Nullstellen fortsetzen.*

$$\begin{tikzcd}
X \arrow[r, hook] \arrow[rr, bend left, "\text{glatt}"] \arrow[d, "\text{unverzw.}"'] & \hat{X} \arrow[r, "\text{flach, geom. ganze Fasern}"] \arrow[d] & X' \arrow[d] \\
Y \arrow[r, hook] \arrow[d] & \hat{Y} \arrow[r, "\text{flach, geom. ganze Fasern}"] \arrow[d, "\text{endl. dom.}"] & Y' \\
\mathbb{A}^1_{Y'} \arrow[r, hook] & \mathbb{P}^1_{Y'} \arrow[ur] &
\end{tikzcd}$$

Beweis. Da endliche Morphismen projektiv sind ([EGA II, 6.1.11]) und die Verkettung zweier projektiver Morphismen wieder projektiv ist (zumindest für noethersche Schemata, siehe [EGA II, 5.5.5]), sind $\hat{X}$ und $\hat{Y}$ projektiv über Y'. Per Basiswechsel sieht man zudem, dass $\hat{X}$ auch projektiv über X' ist.

Weil der Morphismus $\hat{X} \to X'$ zudem flach ist, hängt insbesondere das Geschlecht g_X und die Dimension der Faser $\hat{X}_{x'}$ nicht von der Wahl von $x' \in X'$ ab (siehe [Ha77, III.9.10]); Analoges gilt für $\hat{Y} \to Y'$. Folglich sind alle Fasern $\hat{X}_{x'}$ bzw. $\hat{Y}_{y'}$ geometrisch ganze projektive Kurven vom Geschlecht g_X bzw. g_Y, unabhängig von der Wahl von $x' \in X'$ bzw. $y' \in Y'$.

Zu einem gegebenen Punkt $y' \in \overline{Y'}$ und einem beliebigen Punkt $x' \in \overline{X'}$ darüber sei dazu zunächst $H = D(x')$, $\imath : H \to G$ die Inklusion. In der Sprechweise von Propostion 3.2.3 d) gilt dann $X_{y'} = \imath_* X_{x'}$ und $X'_{y'} = \imath_* \operatorname{Spec} k(x')$, insbesondere $X_{x'}/H = X_{y'}/G = Y_{y'}$ sowie

$$L(X_{y'}, \chi) = L(X_{x'}, \imath^* \chi) \text{ und } L(X'_{y'}, \chi) = L(\operatorname{Spec} k(x'), \imath^* \chi). \qquad (44)$$

Um Proposition 3.5.13 anwenden zu können, fehlt uns aber noch eine Glattheitsaussage. Zwar ist $X_{x'}$ glatt über $k(x')$, aber an die komplette projektive Kurve $\hat{X}_{x'}$ hatten wir eine solche Forderung nicht gestellt. Wir müssen daher zu der Normalisierung $(\hat{X}_{x'})^{\mathrm{n}}$ von $\hat{X}_{x'}$ übergehen. Dies ist jetzt tatsächlich eine ganze, projektive glatte Kurve mit Konstantenkörper $k(x')$; auch auf ihr wirkt H auf zulässige Weise, und der Quotient ist gerade $(\hat{Y}_{y'})^{\mathrm{n}}$, eine ganze, projektive glatte Kurve mit Konstantenkörper $k(y')$. Nach Voraussetzung ändert sich beim Normalisieren an $X_{x'}$ nichts, d.h. $X_{x'}$ ist ein offenes Unterschema von $(\hat{X}_{x'})^{\mathrm{n}}$, das nach Vorgabe sogar in $(\hat{X}_{x'})^{\mathrm{n}}_{\mathrm{uv}}$, der Menge der über $(\hat{Y}_{y'})^{\mathrm{n}}$ unverzweigten Punkte, enthalten ist.

$(\hat{X}_{x'})^{\mathrm{n}}_{\mathrm{uv}} - X_{x'}$ besteht lediglich aus Punkten, die über dem unendlichen Punkt in $\mathbb{P}^1_{k(y')}$ liegen. Deren Beitrag zur L-Funktion lässt sich leicht abschätzen: Sei $d := [K(Y) : K(\mathbb{A}^1_{Y'})]$. Für den Grad der Abbildung $\bar{\pi} : (\hat{Y}_{y'})^{\mathrm{n}} \to \mathbb{P}^1_{k(y')}$ gilt dann offenbar $\deg(\overline{\pi}) \leq d$, also gibt es auch höchstens d Punkte in $(\hat{Y}_{y'})^{\mathrm{n}}$, welche über dem unendlichen Punkt in $\mathbb{P}^1_{k(y')}$ liegen; ihre Norm lässt sich jeweils durch $N(y')$ nach unten abschätzen. Es folgt:

$$\begin{aligned} &|\log L((\hat{X}_{x'})^{\mathrm{n}}_{\mathrm{uv}}, \imath^*\chi; s) - \log L(X_{x'}, \imath^*\chi; s)| \\ \leq\ & d \cdot ||\imath^*\chi|| \cdot \sum_{n=1}^{\infty} \frac{N(y')^{-n\cdot \mathrm{Re}\, s}}{n} = d \cdot ||\imath^*\chi|| \cdot \log \zeta(\mathrm{Spec}\, k(y'); \mathrm{Re}\, s). \end{aligned} \tag{45}$$

Proposition 3.5.13 ergibt nun die Abschätzung

$$\begin{aligned} &|\log L((\hat{X}_{x'})^{\mathrm{n}}_{\mathrm{uv}}, \imath^*\chi; s) - \log L(\mathrm{Spec}\, k(x'), \imath^*\chi; s-1)| \\ \leq\ & -||\imath^*\chi|| \cdot \mathrm{ord}\, G \cdot 4(g_X + 4g_Y + 5) \frac{\zeta'(\mathrm{Spec}\, k(y'); \mathrm{Re}\, s - \frac{1}{2})}{\zeta(\mathrm{Spec}\, k(y'); \mathrm{Re}\, s - \frac{1}{2})} \end{aligned} \tag{46}$$

Definieren wir nun

$$\begin{aligned} f_{y'}(s) &:= \log L(X_{y'}, \chi; s) - \log L(X'_{y'}, \chi, s-1) \\ \text{und } \xi_{y'}(s) &:= \log \zeta(\mathrm{Spec}\, k(y'); s) \qquad \Rightarrow \qquad \xi'_{y'}(s) = \frac{\zeta'(\mathrm{Spec}\, k(y'); s)}{\zeta(\mathrm{Spec}\, k(y'); s)}. \end{aligned}$$

Die Ungleichungen (45) und (46) liefern zusammen mit (44) und der Abschätzung $||\imath^*\chi|| \leq ||\chi||$ die Ungleichung

$$|f_{y'}(s)| \leq ||\chi|| \left(d \cdot \xi_{y'}(\mathrm{Re}\, s) - \mathrm{ord}\, G \cdot 4(g_X + 4g_Y + 5) \cdot \xi'_{y'}(\mathrm{Re}\, s - \frac{1}{2}) \right) \tag{47}$$

Damit ist $f_{y'}(s)$ per Majorantenkriterium für $s > \frac{1}{2}$ definiert und holomorph. Ich erinnere nochmals daran, dass keine der Größen $||\chi||$, d, $\mathrm{ord}\, G$, g_X und g_Y von der Wahl von y' abhängt.
Sei $\xi(Y'; s) := \log \zeta(Y'; s)$. Aus der Definition der Zetafunktion bzw. Bemerkung 3.1.10 folgt, dass $\xi(Y'; s) = \sum_{y' \in \overline{Y'}} \xi_{y'}(s)$ und damit $\xi'(Y'; s) = \sum_{y' \in \overline{Y'}} \xi'_{y'}(s)$. Damit folgt aus (47) durch Aufsummieren aber automatisch die absolute und kompakte Konvergenz von $\sum_{y' \in \overline{Y'}} f_{y'}(s)$ für $\mathrm{Re}\, s - \frac{1}{2} > \dim Y'$, d.h. $\sum_{y' \in \overline{Y'}} f_{y'}(s)$ ist definiert und holomorph für $\mathrm{Re}\, s > \dim X' + \frac{1}{2} = \dim X - \frac{1}{2}$.

Andererseits gilt wegen Proposition 3.2.3 c) für $\mathrm{Re}\, s > \dim X$ (da $X_{y'}$ und $X'_{y'}$ G-stabil sind):

$$\begin{aligned} &\log L(X, \chi; s) - \log L(X', \chi; s-1) \\ =\ & \sum_{y' \in \overline{Y'}} (\log L(X_{y'}, \chi; s) - \log L(X'_{y'}, \chi; s-1)) = \sum_{y' \in \overline{Y'}} f_{y'}(s) \end{aligned}$$

Die Funktion $H(s) := \exp(\sum_{y' \in \overline{Y'}} f_{y'}(s))$ ist somit für $\mathrm{Re}\, s > \dim X - \frac{1}{2}$ definiert, in diesem Bereich analytisch und ohne Nullstelle, und für $\mathrm{Re}\, s > \dim X$ gilt:

$$H(s) = \frac{\log L(X, \chi; s)}{\log L(X', \chi; s-1)} \qquad \square$$

Bevor wir den allgemeinen Fall auf obige Konstellation zurückführen können, müssen wir aber noch etwas Geschütz auffahren:

Fakt 3.6.3. *Sei $X \to S$ ein endlich präsentierter Schemamorphismus. Dann ist die Menge E der Punkte $s \in S$, über denen die Fasern geometrisch irreduzibel (bzw. geometrisch reduziert, bzw. glatt) sind, lokal konstruierbar (für noethersches S also konstruierbar).*

Insbesondere gilt: Ist S irreduzibel und noethersch und ist die Faser X_η über dem generischen Punkt $\eta \in S$ geometrisch irreduzibel (bzw. geometrisch reduziert, bzw. glatt), so gibt es eine offene Teilmenge $U \subset S$, über der alle Fasern diese Eigenschaft haben.

Beweis. [EGA IV_3, 9.7.7],[EGA IV_4, 17.7.11] □

So gewappnet, können wir den Angriff wagen:

Proposition 3.6.4. *Sei G eine endliche Gruppe, die auf zwei irreduziblen Schemata X, X' (v.e.T. über $\mathbb{Z}$) auf zulässige Weise operiert. $h : X \to X'$ sei ein dominanter Morphismus, der mit der Wirkung der Gruppe G vertauscht. Der Funktionenkörper $K(X')$ sei separabel-algebraisch abgeschlossen in $K(X)$, und es gelte* $\operatorname{trdeg}(K(X)|K(X')) = 1$. *Dann gilt*

$$L(X, \chi; s) = H(s) \cdot L(X', \chi; s-1);$$

wobei $H(s)$ holomorph und $\neq 0$ für $\operatorname{Re} s > \dim X - \frac{1}{2}$ ist.

Beweis. Ziel ist es, diese Proposition auf obiges Lemma 3.6.2 zurückzuführen. Dazu ist aber einige Vorarbeit zu leisten, schließlich müssen Eigenschaften wie Glattheit und Projektivität erfüllt sein. Deswegen werden wir uns mehrmals auf offene G-stabile Unterschemata $U' \subseteq X'$ und $U \subseteq h^{-1}(U') \subseteq X$ einschränken bzw. von offenen Unterschemata auf die ganzen Räume ausdehnen. Dies macht aber nichts, denn $Z' = X' - U'$ und $Z = X - U$ sind abgeschlossene Teilmengen von den irreduziblen Räumen X und X', haben also niedrigere Dimension. Für $\operatorname{Re} s > \dim X$ gilt $\frac{L(X,\chi;s)}{L(U,\chi;s)} = L(Z, \chi; s)$; da letztere Funktion aber sogar für $\operatorname{Re} s > \dim X - 1$ holomorph und ohne Nullstellen ist, folgt aus der Aussage für U und U' die Aussage für X und X' und umgekehrt.

Zunächst einmal gilt offenbar $L(X, \chi; s) = L(X_{red}, \chi; s)$; wir können daher oBdA davon ausgehen, dass X und X' reduziert, also ganz sind. Als nächstes können wir nach obiger Argumentation oBdA davon ausgehen, dass $Y := X/G = \operatorname{Spec} A$ und $Y' := X'/G = \operatorname{Spec} A'$ und damit auch $X = \operatorname{Spec} B$ und $X' = \operatorname{Spec} B'$ affin sind. Da der Morphismus $X \to X'$ dominant ist, kann man B' als Unterring von B auffassen; gleiches gilt für $A' \subset A$.

Nach Fakt 2.2.3 ist die Normalisierung $\check{X} \to X$ von X endlich; genauer drückt sich Fakt 2.2.3 darin aus, dass sich für die zugehörige Normalisierung $\check{X} = \operatorname{Spec} \check{B}$ von $X = \operatorname{Spec} B$ gilt: $\check{B} = \sum_{i=1}^{n} \frac{r_i}{s_i} B$ mit $r_i, s_i \in B$, also $B \subseteq \check{B} \subseteq \frac{1}{s} B$ mit

$s = \prod s_i$. Es folgt $B_s = \check{B}_s$, also $X_s = \check{X}_s$; somit sind X und $\check{X}$ birational, und wir können im folgenden ohne Einschränkung voraussetzen, dass X und damit auch Y normal sind.

Da beide Schemata v.e.T. über $\mathbb{Z}$ sind, ist A eine endlich erzeugte A'-Algebra. Setzt man $S = A' - \{0\}$, so gibt es daher wegen $\operatorname{trdeg}(K(Y)|K(Y')) = 1$ nach dem noetherschen Normalisierungssatz ein $T \in A_S$, so dass A_S ein endlicher $K'[T]$-Modul (mit $K' = K(Y')$) ist. Indem man an einem geeigneten $\alpha' \in A'$ lokalisiert (vgl. den Beweis von Lemma 2.1.2), erhält man, dass $A_{\alpha'}$ ganz über $A'_{\alpha'}[T]$ ist. Wir können also oBdA davon ausgehen, dass A ganz über $A'[T]$ ist. Dies entspricht einem endlichen dominanten Morphismus $Y \to \mathbb{A}^1_{Y'}$. Nun betrachten wir die in Proposition 2.3.3 konstruierten separablen Abschlüsse $\tilde{X}$ bzw. $\tilde{Y}$ von $\mathbb{A}^1_{Y'}$ in X bzw. Y'. Man entnimmt dieser Proposition auch leicht, dass G auf zulässige Weise auf $\tilde{X}$ wirkt mit $\tilde{X}/G = \tilde{Y}$. Die Argumentation aus Lemma 2.3.1 macht dann unmittelbar klar, dass der Morphismus $h : X \to X'$ über $\tilde{X}$ faktorisiert und dass $L(X, \chi; s) = L(\tilde{X}, \chi; s)$. Wir können daher ohne Einschränkung davon ausgehen, dass $K(X)|K(X')$ und $K(Y)|K(Y')$ separabel erzeugte Körpererweiterungen sind. Weiterhin sind X wie Y normal und affin.

Wenden wir uns nun der generischen Faser $X_{\eta'}$ zu: Da $K(X)|K(X')$ separabel erzeugt und $K(X')$ separabel-algebraisch abgeschlossen in $K(X)$ ist, ist sie wegen Fakt 3.5.1 auf jeden Fall eine geometrisch ganze Kurve. Wir wollen nun zeigen, dass sie (nach eventuellem Verkleinern von X) glatt ist. Dazu betrachten wir zunächst einmal das Verhalten im generischen Punkt η von $X_{\eta'}$: Der Morphismus $X_{\eta'} \to \eta'$ ist flach in η, da trivialerweise $\mathcal{O}_{\eta,X} = K(X)$ flach über $k(\eta') = K(X')$ ist. Außerdem gilt für die Garbe der Differentiale $\Omega_{X_{\eta'}|\eta'}$ wegen der Separabilität von $K(X)|K(X')$ nach [Ha77, II.8.6]: $\dim_{k(\eta)}(\Omega_{X_{\eta'}|\eta'} \otimes k(\eta)) = \dim_{K(X)} \Omega_{K(X)|K(X')} = \operatorname{trdeg}(K(X)|K(X')) = 1 = \dim X - \dim X'$. Damit ist die Abbildung $X_{\eta'} \to \eta'$ per Definition glatt in η. Da Glattheit eine offene Eigenschaft ist, gibt es ein offenes Unterschema von $X_{\eta'}$, welches glatt über $k(\eta')$ ist. Nach eventuellem Einschränken von X ist also die generische Faser $X_{\eta'}$ tatsächlich eine geometrisch ganze, glatte Kurve. Nach Fakt 3.6.3 können wir nach eventuellem Verkleinern von X' daher davon ausgehen, dass alle Fasern von $X \to X'$ geometrisch ganz und glatt sind.

Desweiteren können wir annehmen, dass G treu auf $K(X)$ wirkt. Denn sei G_0 die Untergruppe, die trivial auf $K(X)$ (und damit auch X und X') wirkt, π die Projektion $G \to G/G_0$. Dann wirkt G durch π auf X und X', und nach Proposition 3.2.3 e) folgt $L(X, \chi) = L(X, \pi_*\chi)$ und $L(X', \chi) = L(X', \pi_*\chi)$. Insbesondere ist die offene Menge der Punkte von X, welche unverzweigt über Y sind, nichtleer; wir gehen daher zusätzlich oBdA davon aus, dass $X = \operatorname{Spec} B$ unverzweigt über $Y = \operatorname{Spec} A$ ist.

Wie oben bereits erwähnt, können wir annehmen, dass es einen endlichen dominanten Morphismus $Y \to \mathbb{A}^1_{Y'}$ gibt. Wir betten nun $\mathbb{A}^1_{Y'}$ in den projektiven Raum $\mathbb{P}^1_{Y'}$ ein und konstruieren dazu $\hat{Y}$ und $\hat{X}$ lokal als ganze Abschlüsse von

$\mathbb{P}^1_{Y'}$ in $K(Y)$ bzw. $K(X)$. Die lokal konstruierten affinen Teile lassen sich einfach verkleben, und das entstehende Schema $\hat{X}$ (bzw. $\hat{Y}$) enthält offenbar X (bzw. Y) als offenes (affines) Unterschema, jeweils als Urbild von $\mathbb{A}^1_{Y'}$. Zudem ersieht man aus der Konstruktion auch direkt die (zulässige) Wirkung von G auf $\hat{X}$; es gilt $\hat{X}/G = \hat{Y}$. Der Morphismus $\hat{Y} \to \mathbb{P}^1_{Y'}$ ist nach Proposition 2.2.3 endlich und per Konstruktion dominant.

Indem wir Y' und X' - falls nötig - weiter verkleinern, können wir nach dem Satz über generische Flachheit ([EGA IV_2, 6.9.1]) schließlich annehmen, dass $\hat{X}$ flach über X' und $\hat{Y}$ flach über Y' ist.

Damit haben wir alle Voraussetzungen von Lemma 3.6.2 erfüllt, wie man sich leicht vergewissert; die Behauptung folgt dann unmittelbar aus der Aussage des obigen Lemmas. □

Nach diesem doch etwas schweren Gefecht ist der Rest aber relativ leicht:

Theorem 3.6.5. *Sei X ein Schema vom endlichen Typ über $\mathbb{Z}$, G eine endliche Gruppe, die auf zulässige Weise auf X operiert, und χ ein Charakter von G. Dann lässt sich die L-Funktion $L(X, \chi; s)$ meromorph in die Halbebene* $\operatorname{Re} s > \dim X - \frac{1}{2}$ *fortsetzen.*

Beweis. Sei zunächst X ganz, $K(X)$ der zugehörige Funktionenkörper und k der Primkörper von $K(X)$. Wir führen den Beweis über $\operatorname{trdeg}(K(X)|k)$:

- $\operatorname{trdeg}(K(X)|k) = 0$: In diesem Fall lässt sich die L-Funktion sogar auf ganz $\mathbb{C}$ meromorph fortsetzen:

  Im Fall $\operatorname{char} k > 0$ gilt $X = \operatorname{Spec} l$, wobei l eine endliche Erweiterung von k ist. Nach dem Ausführungen im obigen Beweis von Proposition 3.6.4 können wir annehmen, dass G treu auf l wirkt; überdies können wir, da jede Darstellung in eine direkte Summe irreduzibler Darstellungen zerfällt, davon ausgehen, dass χ irreduzibel ist. In diesem Fall sind wir im Kontext von Beispiel 3.2.4; die Aussage ist daher trivial.

  Ist dagegen $k = \mathbb{Q}$, so können wir nach den Ausführungen des obigen Beweis zunächst oBdA davon ausgehen, dass $X = \operatorname{Spec} A$ affin und normal ist, als $A = \mathcal{O}_K$ für einen Zahlkörper K. Dieser Fall wurde aber schon in obigem Fakt 3.6.1 behandelt.

- $\operatorname{trdeg}(K(X)|k) = n > 0$:

  In diesem Fall suchen wir uns eine in $\mathcal{O}_X(X)$ gelegene Transzendenzbasis $T_1, \ldots, T_n$ von $K(X)|k$. Sei L der separabel-algebraische Abschluss von $k(T_1, \ldots, T_n)$ in $K(X)$, $A = L \cap \mathcal{O}_X(X)$. Zwar gilt nicht notwendigerweise $\operatorname{Quot} A = L$, aber zumindest ist $L|\operatorname{Quot} A$ endlich separabel, wird also erzeugt durch ein Element $a = \frac{b}{c}$ mit $b, c \in \mathcal{O}_X(X)$. Wenn wir uns auf eine kleinere Teilmenge von X einschränken, können wir sogar annehmen, dass

$c \in \mathcal{O}_X(X)^\times$, also $a \in \mathcal{O}_X(X)$, d.h. $\operatorname{Quot} A = L$. Dann erfüllt der durch die Inklusion $A \hookrightarrow \mathcal{O}_X(X)$ induzierte Morphismus $X \to X' = \operatorname{Spec} A$ aber alle Voraussetzungen von Proposition 3.6.4; wegen $\operatorname{trdeg}(L|k) = n - 1$ gilt die Behauptung nach Induktionsvoraussetzung für $\operatorname{Spec} A$, und wegen $\dim X = \dim X' + 1$ folgt sie dann für X.

Damit ist der Satz für alle ganzen und damit auch für alle irreduziblen Schemata X bewiesen. Nun handeln wir den Fall ab, dass Y irreduzibel ist. Dann hat X endlich viele irreduzible Komponenten $X_1, \ldots X_r$, auf denen G notwendigerweise transitiv wirkt. Die Menge $Z = \bigcup_{i<j} X_i \cap X_j$ ist abgeschlossen, G-stabil und hat kleinere Dimension als X. Daher können wir aus bekannten Gründen auf die Menge $X - Z$ übergehen, also oBdA annehmen, dass die irreduziblen Komponenten von X gleichzeitig Zusammenhangskomponenten sind. Ist H die Untergruppe von G, die X_1 auf sich selbst abbildet, $\imath : H \to G$ die Inklusionsabbildung, so folgt daher in der Sprechweise von Proposition 3.2.3 d): $X = X_1 \times_H G = \imath_* X_1$ und daher $L(X, \chi) = L(X_1, \imath^* \chi)$. Damit haben wir den Fall auf den bereits bekannten zurückgeführt.

Im allgemeinen Fall seien $Y_1, \ldots, Y_s$ die irreduziblen Komponenten von Y, $X_1, \ldots, X_s$ die Urbilder in X. Wie oben können wir oBdA wieder davon ausgehen, dass die X_i und damit auch die Y_i disjunkt sind. Die Aussage ergibt sich dann direkt aus $L(X, \chi) = \prod_{i=1}^n L(X_i, \chi)$. □

Das Verhalten der L-Funktionen bei $\dim X$ entnehmen wir dem folgenden Satz:

Satz 3.6.6. *Sei X ein irreduzibles Schema v.e.T. über $\mathbb{Z}$, auf dem eine endliche Gruppe G in zulässiger Weise operiert, χ sei ein Charakter von G. Dann ist die Ordnung von $L(X, \chi)$ bei $s = \dim X$ gerade $-(\chi, 1)$.*

Beweis. Wie wir dem Beweis von Satz 3.6.5 entnehmen können, reicht es, diese Aussage für $\operatorname{trdeg} K(X) = 0$ zu zeigen, genauer: für $X = \operatorname{Spec} l$ mit einem endlichen Körper l oder für $X = \operatorname{Spec} \mathcal{O}_K$ für einen Zahlkörper K. Ist $\pi : G \twoheadrightarrow G''$ eine Projektion, über die G auf X operiert, so gilt $L(X, \chi) = L(X, \pi_* \chi)$ und $(\pi_* \chi, 1_{G''}) = (\chi, \pi^* 1_{G''}) = (\chi, 1_G)$; daher können wir oBdA davon ausgehen, dass G treu auf $K(X)$ wirkt. Zudem reicht es offenbar, die Aussage für irreduzible χ nachzuweisen.

Zu zeigen ist daher: Sei $X = \operatorname{Spec} l$ oder $X = \operatorname{Spec} \mathcal{O}_K$ mit l, K wie oben; G wirke treu auf $K(X)$, χ sei ein irreduzibler Charakter von G. Dann hat $L(X, \chi)$ einen einfachen Pol bei $s = \dim X$, falls $\chi = 1_G$; andernfalls ist es dort holomorph und $\neq 0$. Für $X = \operatorname{Spec} l$ entnimmt man die Behauptung nun unmittelbar dem Beispiel 3.2.4, für $X = \operatorname{Spec} \mathcal{O}_K$ dem Fakt 3.6.1. □

3.7 Artin-Čebotarev's Dichtigkeitssatz

Endlich sind wir nun bereit, den Satz von Čebotarev zu beweisen. Dazu benötigen wir wieder den Begriff der Dichte.

Definition 3.7.1. *Sei X ein Schema, $M \subseteq \overline{X}$ eine Menge von abgeschlossenen Punkten in X. Existiert der Grenzwert*

$$d(M) = \lim_{s \to \dim X + 0} \frac{\sum_{x \in M} N(x)^{-s}}{\sum_{x \in \overline{X}} N(x)^{-s}},$$

so sagen wir, M hat die ***Dirichlet-Dichte*** *$d(M)$.*

Theorem 3.7.2 (Satz von Artin-Čebotarev). *Sei X ein normales Schema, auf dem eine endliche Gruppe G auf zulässige Weise operiert, sei $Y = X/G$; G operiere treu auf $K(X)|K(Y)$. Zu $\sigma \in \mathrm{Gal}(L|K)$ sei $\mathcal{C}(\sigma)$ die zugehörige Konjugationsklasse, $M_\sigma^{X|Y}$ die Menge der in X unverzweigten Punkte $y \in \overline{Y}$, für es ein $\overline{X}$ über y gibt mit $F_x = \sigma$. Dann hat $M_\sigma^{X|Y}$ eine Dichte, und es gilt:*

$$d(M_\sigma^{X|Y}) = \frac{\#\mathcal{C}(\sigma)}{[K(X) : K(Y)]} = \frac{\mathrm{card}(\mathcal{C}(\sigma))}{\mathrm{card}(G)}.$$

Beweis. Betrachten wir zunächst den abelschen Fall. Dann ist $M_\sigma := M_\sigma^{X|Y}$ offenbar gerade die Menge der in X unverzweigten abgeschlossenen Punkte in $\overline{Y}$, so dass für jeden Punkt $x \in \overline{X}$ über y gilt $F_x = \sigma$. Die verzweigten Punkte liegen in einem echten abgeschlossenen Unterschema und können daher aus bekannten Gründen vernachlässigt werden. Wir erhalten dann für jeden Charakter χ von G

$$\log L(X, \chi, s) \sim \sum_{\tau \in G} \sum_{y \in M_\tau} \sum_{m=1}^{\infty} \frac{\chi(\tau^m) N(y)^{-ms}}{m} \sim \sum_{\tau \in G} \sum_{y \in M_\tau} \frac{\chi(\tau)}{N(y)^s}.$$

Nun multiplizieren wir mit $\chi(\sigma^{-1})$ und summieren über alle irreduziblen Charaktere, so ergibt sich

$$\sum_\chi \chi(\sigma^{-1}) \log L(X, \chi, s) \sim \sum_\chi \sum_{\tau \in G} \chi(\tau\sigma^{-1}) \sum_{y \in M_\tau} \frac{1}{N(y)^s} = \mathrm{ord}\, G \sum_{y \in M_\sigma} N(y)^{-s},$$

da $r = \sum \chi$ der Charakter der regulären Darstellung ist (d.h. $r(\tau) = \mathrm{ord}\, G$, falls $\tau = 1$, $r(\tau) = 0$ für $\tau \neq 1$). Nach Satz 3.6.6 ist für jeden nichttrivialen irreduziblen Charakter $\log L(L|K, \chi, s)$ holomorph bei 1, folglich erhalten wir

$$\zeta(Y, s) = \log L(X, 1, s) \sim \sum_\chi \chi(\sigma^{-1}) \log L(X, \chi, s) \sim \mathrm{ord}\, G \cdot \sum_{y \in M_\sigma} N(y)^{-s}$$

und damit unmittelbar unsere Behauptung.

Der allgemeine Fall lässt sich nun auf bekannte Art auf den zyklischen (also insbesondere abelschen) Fall zurückführen:

$$d(M_\sigma^{X|X^\sigma}) = \frac{1}{[K(X):K(X^\sigma)]} \Leftrightarrow d(M_\sigma^{X|Y}) = \frac{\#\mathcal{C}(\sigma)}{[K(X):K(Y)]}$$

Betrachte dazu zu $y \in M_\sigma^{X|Y}$ die Menge $X_{\sigma,y} = \{x \in \pi^{-1}(y) | F_x = \sigma\}$. Bezeichnen wir wieder mit $Z(\sigma)$ den Zentralisator von σ, so erhalten wir $\#X_{\sigma,y} = \frac{\#Z(\sigma)}{\#D(x)} = \frac{\#G}{\#\mathcal{C}(\sigma)\#D(x)} = \frac{[K(X):K(Y)]}{\#\mathcal{C}(\sigma)\cdot[K(X):K(X^\sigma)]}$ und $\#X_{\sigma,x'} = 1$ für $x' \in M_\sigma^{X|X^\sigma}$. Es folgt

$$\sum_{x' \in M_\sigma^{X|X^\sigma}} N(x')^{-s} = \frac{[K(X):K(Y)]}{\#\mathcal{C}(\sigma)\cdot[K(X):K(X^\sigma)]} \sum_{y \in M_\sigma^{X|Y}} N(y)^{-s}$$

und damit obige Gleichung. □

3.8 Der Rest des Beweises

Bevor wir uns dem letzten Teil des Beweises zuwenden, müssen wir zunächst ein paar Notationen festhalten: Sei X ein irreduzibles Schema, M, N Teilmengen von $\overline{X}$. Wir definieren

$$\begin{aligned} M \dot{\subseteq} N \quad &:\Leftrightarrow \quad M - N \subseteq Z,\ Z \text{ echte abgeschlossene Teilmenge von} X, \\ M \subseteq_d N \quad &:\Leftrightarrow \quad d(M-N) = 0 \end{aligned}$$

Man beachte, dass $\dot{\subseteq}$ hier also nicht mehr bedeutet, dass $M-N$ endlich ist (außer in Dimension 1). Entsprechend seien $\doteq$ und $=_d$ definiert. Es gilt offenbar

$$M \subseteq N \Rightarrow M \dot{\subseteq} N \Rightarrow M \subseteq_d N$$

Definition 3.8.1. *Sei $g : X \to Y$ eine endliche Überlagerung von normalen Schemata. Dazu definieren wir zwei Mengen:*

- *die* ***Kroneckermenge***

$$D(X|Y) := \{y \in \overline{Y} | f(y|x) = 1 \text{ für ein } x \in \overline{X}, x \mapsto y\};$$

- *und die* ***Zerlegungsmenge***

$$S(X|Y) := \{y \in \overline{Y} |\ \forall\, x \in g^{-1}(y) \text{ ist } f(y|x) = 1 \text{ und } g \text{ unverzweigt in } x\}.$$

Bemerkung 3.8.2. *Sei $X \to Y$ eine endliche Überlagerung von normalen Schemata, $\tilde{X}$ der separable Abschluss von Y in X. Wie man den Ausführungen aus Abschnitt 2.3 entnimmt, gilt dann $D(X|Y) = D(\tilde{X}|Y)$. Der Begriff der Zerlegungsmenge ist aufgrund der Forderung nach Unverzweigtheit nur bei separablen Überlagerungen wirklich sinnvoll.*

Proposition 3.8.3. *Es gilt* $S(X|Y) \doteq \{y \in Y | \#g^{-1}(y) = [K(X) : K(Y)]\}$

Beweis. Seien oBdA $X = \operatorname{Spec} B$ und $Y = \operatorname{Spec} A$ affin, $n = [K(X) : K(Y)]$, $y = \mathfrak{p}$ ein maximales Ideal in A, $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ die darüberliegenden maximalen Ideale von B. Nach dem Grothendiecks Lemma über generische Freiheit [Ei99, 14.4] können wir nach Lokalisieren annehmen, dass B ein freier A-Modul ist. Nach dieser Einschränkung gilt sogar die strikte Gleichheit (ohne Punkt). Sei $\omega_1, \ldots, \omega_n$ eine Basis von $B|A$ (und damit $K(X)|K(Y)$). Dann ist offenbar $\bar{\omega}_1, \ldots, \bar{\omega}_n$ eine Basis des $k(\mathfrak{p})$-Vektorraums $B/\mathfrak{p}B$.

Zunächst „$\supseteq$": Wegen $\mathfrak{p}B \subseteq \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$ und des chinesischen Restsatzes gilt

$$n = \dim_{k(\mathfrak{p})} B/\mathfrak{p}B \geq \dim_{k(\mathfrak{p})} B/(\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r) = \sum_{i=1}^{r} \dim_{k(\mathfrak{p})} B/\mathfrak{q}_i = \sum_{i=1}^{r} f(\mathfrak{q}_i|\mathfrak{p}).$$

Für $r = n$ folgt also $f(\mathfrak{q}_i|\mathfrak{p}) = 1 \ \forall\, i$ und $\mathfrak{p}B = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r$. Somit erhalten wir (dank Primvermeidung) $\mathfrak{p}B_{\mathfrak{q}_i} = \mathfrak{q}_i B_{\mathfrak{q}_i} \ \forall\, i$, d.h. alle $\mathfrak{q}_i|\mathfrak{p}$ sind unverzweigt.

„$\subseteq$": Nach weiterem Lokalisieren an $A \backslash \mathfrak{p}$ können wir davon ausgehen, dass $(A, \mathfrak{p})$ lokal ist und $\mathfrak{q}_i$ gerade die maximalen Ideale von B sind. Insbesondere gilt $\bigcap_{i=1}^r \mathfrak{p}B_{\mathfrak{q}_i} = \mathfrak{p}B$ (denn zu $b \in \bigcap_{i=1}^r \mathfrak{p}B_{\mathfrak{q}_i}$ sei $\mathfrak{b} = \{s \in B | bs \in \mathfrak{p}B\}$; wegen $\mathfrak{b} \not\subseteq \mathfrak{q}_i$ $\forall\, i$ folgt dann $\mathfrak{b} = (1)$). Sind alle $\mathfrak{q}_i$ unverzweigt über $\mathfrak{p}$, d.h. $\mathfrak{p}B_{\mathfrak{q}_i} = \mathfrak{q}_i B_{\mathfrak{q}_i}$, so ergibt sich $\bigcap_{i=1}^r \mathfrak{q}_i \subseteq \bigcap_{i=1}^r \mathfrak{q}_i B_{\mathfrak{q}_i} = \bigcap_{i=1}^r \mathfrak{p}B_{\mathfrak{q}_i} = \mathfrak{p}B$, also $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r = \mathfrak{p}B$. Damit gilt $n = \sum_{i=1}^r f(\mathfrak{q}_i|\mathfrak{p})$, für $f(\mathfrak{q}_i|\mathfrak{p}) = 1 \ \forall\, i$ also $r = n$. □

Die nicht vollkommene Gleichheit zwischen den beiden Mengen in der vorangegangenen Proposition ist das Einzige, was winzige Unterschiede zwischen den folgenden Aussagen und den analogen Aussagen für den Zahlkörperfall (siehe 1.3.7 ff.) bewirkt. Die Beweise sind ansonsten identisch und werden daher weggelassen. Man beachte allerdings, dass es nicht immer notwendig ist, die Separabilität des Morphismus zu fordern; dies sieht man dann jeweils leicht mit den Argumenten aus Abschnitt 2.3.

Lemma 3.8.4. *Sei W ein normales Schema, G eine endliche Gruppe, die zulässig auf W und treu auf $K(W)$ wirke. Sei H eine Untergruppe von G, $X = W/H$, $Y = W/G$. Für $w \in \overline{W}$, y das Bild in Y bezeichnen wir unter Mißbrauch der Notation mit F_w statt dem Frobenius in* $\operatorname{Gal}(k(w)|k(y))$ *das Urbild in $D(w) \subseteq G$. Dann gilt*

$$\begin{aligned} D(X|Y) &= \{y \in \overline{Y} | F_w \cap H^G \neq \emptyset \text{ für ein (jedes) } w \in \overline{W}, w \mapsto y\} \\ S(X|Y) &\doteq \{y \in \overline{Y} | F_w \subseteq H_G \text{ für ein (jedes) } w \in \overline{W}, w \mapsto y\} \end{aligned}$$

Korollar 3.8.5. *Im obigen Kontext gilt*

$$D(X|Y) \doteq \dot{\bigcup}_{\mathcal{C}(\sigma) \subseteq H^G} M_\sigma^{W|Y} \tag{48}$$

Korollar 3.8.6. *Sei $X \to Y$ eine endliche Überlagerung von normalen Schemata. Dann hat $D(X|Y)$ eine Dichte*

$$d(D(X|Y)) \geq \frac{1}{[K(X) : K(Y)]}.$$

Gleichheit gilt genau dann, wenn $X|Y$ eine Galoisüberlagerung ist.

Korollar 3.8.7. *Sei $X \to Y$ eine endliche separable Überlagerung normaler Schemata, W die normale Hülle von $X \to Y$. Dann gilt $S(X|Y) \doteq S(W|Y)$.*

Satz 3.8.8. *Sei $X \to Y$ ein endliche separable Überlagerung normaler Schemata. Dann ist $X \to Y$ genau dann eine Galoisüberlagerung, wenn $D(X|Y) \doteq S(X|Y)$ gilt.*

Damit haben wir offenbar gerade die Rückrichtung unseres Hauptsatzes 2.1.3 bzw. 2.2.7 gezeigt. Dies war der letzte verbleibende Schritt in unserem Beweis; der Satz ist hiermit also bewiesen.

4 Folgerungen und Anwendungen

Im folgenden wollen wir einige Anwendungen unseres Satzes beziehungsweise der Beweisschritte, die dorthin geführt haben, anschauen. Wir orientieren uns dabei im wesentlichen an [Kl98].

Weiterhin seien alle Schemata vom endlichen Typ über $\mathbb{Z}$. Auch sonst übernehmen wir die Bezeichnungen aus dem letzten Abschnitt.

4.1 Kronecker-Äquivalenz

Die Mittel, die wir uns im letzten Abschnitt erarbeitet haben, können auch dazu dienen, zwei verschiedene Überlagerungen eines normalen Schemas zu vergleichen. Man betrachte dazu folgende

Proposition 4.1.1. *Sei W ein Schema mit einer endlichen zulässigen Gruppenwirkung G, G wirke treu auf $K(W)$. Seien H, H' Untergruppen von G, $X = W/H$, $X' = W/H'$, $Y = W/G$. Dann sind folgende Aussagen äquivalent:*

(i) $D(X|Y) \subseteq_d D(X'|Y)$.

(ii) $D(X|Y) \subseteq D(X'|Y)$.

(iii) $H^G \subseteq H'^G$.

Beweis. $(ii) \Rightarrow (i)$ ist klar, $(iii) \Rightarrow (ii)$ folgt unmittelbar aus Lemma 3.8.4. Um $(i) \Rightarrow (iii)$ zu zeigen, verwenden wir Korollar 3.8.5: Mit Hilfe von (48) folgt dann $\dot\bigcup_{\mathcal{C}(\sigma)\subseteq H^G} M_\sigma^{W|Y} \subseteq_d \dot\bigcup_{\mathcal{C}(\sigma)\subseteq H'^G} M_\sigma^{W|Y}$, also nach dem Čebotarevschen Dichtigkeitssatz

$$0 = d\left(\dot\bigcup_{\mathcal{C}(\sigma)\subseteq H^G\setminus H'^G} M_\sigma^{W|Y}\right) = \sum_{\mathcal{C}(\sigma)\subseteq H^G\setminus H'^G} d(M_\sigma^{W|Y}) = \frac{\#(H^G\setminus H'^G)}{\#G}.$$

Damit folgt wie behauptet $H^G \subseteq H'^G$. □

Diese Proposition hat zwei wichtige Konsequenzen. Die erste ist folgender Satz, der im Original (also im Zahlkörperfall) auf M. Bauer zurückgeht:

Satz 4.1.2. *a) Sei $W|Y$ eine Galoisüberlagerung von normalen Schemata, $X|Y$ eine beliebige endliche Überlagerung von normalen Schemata. Dann sind folgende Aussagen äquivalent:*

- $D(X|Y) \subseteq_d D(W|Y)$.
- $D(X|Y) \subseteq D(W|Y)$.
- *Es gibt einen endlichen dominanten Morphismus $X \to W$.*

b) Sind $W|Y$ und $W'|Y$ zwei Galoisüberlagerungen von normalen Schemata, so sind folgende Aussagen äquivalent:

- $D(W|Y) =_d D(W'|Y)$.
- $D(W|Y) = D(W'|Y)$.
- $W \cong W'$.

Beweis. Die einzige Sache, die wirklich zu beweisen sind, ist die Folgerung $D(X|Y) \subseteq_d D(W|Y) \Rightarrow \exists\ X \to W$. Nach Übergang zum separablen Abschluss von Y in X können wir dabei oBdA annehmen, dass $K(X)|K(Y)$ separabel ist. Entsprechend Bemerkung 2.2.6 gibt es eine Galoisüberlagerung Z von Y mit Galoisgruppe G und zwei Untergruppen H, H', so dass $Z/H = X$, $Z/H' = W$. Da W selbst schon eine Galoisüberlagerung ist, ist H' normal. Aus obiger Proposition folgt daher $H \subseteq H^G \subseteq H'^G = H'$. Daraus ergibt sich der erwünschte endliche Morphismus $X = Z/H \to Z/H' = W$. □

Insbesondere sind Galoisüberlagerungen von normalen Schemata durch ihre Kroneckermengen bis auf Isomorphien eindeutig festgelegt. Allgemeiner definiert man

Definition 4.1.3. *Eine Überlagerung normaler Schemata $X \to Y$ heißt **Bauersch**, falls es zu jeder weiteren Überlagerung X' von Y mit $D(X'|Y) \subseteq_d D(X|Y)$ einen endlichen dominanten Morphismus $X' \to X$ gibt.*

Aus dem Satz von Bauer 4.1.2 ergibt sich unmittelbar das folgende

Korollar 4.1.4. *Galoisüberlagerungen sind Bauersch.*

Eine Bauersche Überlagerung ist automatisch separabel. Weitere Beispiele für Bauersche Überlagerungen sind separable Überlagerungen $X \to Y$ vom Grad $[K(X) : K(Y)] \leq 4$ (zu diesem oder ähnlichen Beispielen vgl. [Kl98, II.1.9]).

Die zweite Anwendung der obigen Proposition 4.1.1 beruht auf folgender

Definition 4.1.5. *Zwei Überlagerungen X, X' von einem normalen Schema Y heißen **Kronecker-äquivalent**, in Zeichen*

$$X \sim_Y X',$$

genau dann, wenn $D(X|Y) \doteq D(X'|Y)$.

Aus Proposition 4.1.1 ergibt sich nun unmittelbar das folgende

Korollar 4.1.6. *Seien X, X' separable Überlagerungen eines normalen Schemas Y, (W,G) eine Galoisüberlagerung von Y, die auch endliche dominante Morphismen $W \to X$ und $W \to X'$ zulässt, und seien $H = \mathrm{Gal}(K(W)|K(X))$, $H' = \mathrm{Gal}(K(W)|K(X'))$ (vgl. Bemerkung 2.2.6). Dann sind folgende Aussagen äquivalent:*

(i) $X \sim_Y X'$.

(ii) $D(X|Y) =_d D(X'|Y)$.

(iii) $D(X|Y) = D(X'|Y)$.

(iv) $H^G = H'^G$.

Bemerkung 4.1.7. *a) Wie wir bereits eingesehen haben, sind zwei zueinander Kronecker-äquivalente Galoisüberlagerungen über einem normalen Schema notwendigerweise isomorph.*

b) Eine endliche Überlagerung X über einem normalen Schema Y ist über selbigem Kronecker-äquivalent zu dem separablen Abschluss $\tilde{X}$ von Y in X.

c) Sind zwei endliche Überlagerungen X, X' eines normalen Schemas Y Kronecker-äquivalent über Y und existiert gleichzeitig ein endlicher dominanter Morphismus $X \to X'$, so ist auch jedes normale Schema X'', über das dieser Morphismus faktorisiert, Kronecker-äquivalent zu X. Dies folgt unmittelbar aus der Multiplizität der Trägheitsgrade.

d) Gilt $X \sim_Y X'$ und ist $Y \to Y'$ ein endlicher dominanter Morphismus, so gilt auch $X \sim_{Y'} X'$. Dies erhält man unmittelbar aus der Darstellung

$$D(X|Y') = \{y' \in D(Y|Y')| \exists\, y \in D(X|Y), y \mapsto y'\},$$

die wiederum aus der Multiplizität der Trägheitsgrade folgt.

Proposition 4.1.8. *Keine nichttriviale endliche separable Überlagerung $X \to Y$ ist über Y Kronecker-äquivalent zu Y:*

$$X \sim_Y Y \Rightarrow X \cong Y$$

Beweis. Sei W die galoissche Hülle von X über Y, $G = G(K(W)|K(Y))$ und $H = G(K(W)|K(X))$. Aus $X \sim_Y Y$ folgt nach Korollar 4.1.6 direkt $H^G = G$. Für $H \neq G$ kann dies aber aus Abzählargumenten nicht stimmen: Denn H^G ist die Vereinigung der höchstens $(G : H)$ Konjugierten von H, und diese sind offenbar nicht disjunkt; daher folgt $\#H^G < (G : H)\#H = \#G$. Somit gilt $G = H$, also $X \cong Y$. □

Man sollte allerdings nicht denken, dass, wenn wir uns auf separable Überlagerungen beschränken, die Kroneckerklasse von $X \to Y$ die Isomorphieklasse von X über Y oder auch nur den Grad der Körpererweiterung $[K(X) : K(Y)]$ bestimmt. Bevor wir aber ein passendes Beispiel bringen, müssen wir einen kleinen Ausflug in die Welt der Körpertheorie machen (vgl. [FJ86, Kapitel 11 & 12]):

Definition 4.1.9. *Sei K ein Körper, $f_1(\boldsymbol{T}, \boldsymbol{X}), \ldots, f_m(\boldsymbol{T}, \boldsymbol{X})$ irreduzible Polynome in $K(\boldsymbol{T})[\boldsymbol{X}] = K(T_1, \ldots, T_r)[X_1, \ldots, X_n]$. Für jedes von 0 verschiedene Polynom $g \in K[T]$ definiere man die* ***Hilbertmenge***

$$H_K(f_1, \ldots, f_m; g) = \left\{ \boldsymbol{a} = (a_1, \ldots, a_r) \in K^r \middle| \begin{array}{l} g(\boldsymbol{a}) \neq 0 \textit{ und } f_1(\boldsymbol{a}, \boldsymbol{X}), \ldots, f_m(\boldsymbol{a}, \boldsymbol{X}) \\ \textit{wohldefiniert und irreduzibel in } K[\boldsymbol{X}] \end{array} \right\}.$$

K heißt ***Hilbertsch****, wenn alle Hilbertmengen nichtleer sind.*

Die Definition ist auf den ersten Blick etwas verwirrend, aber für uns auch nicht weiter wichtig. Entscheidend sind folgende Aussagen, die hier ohne Beweis zu einem Fakt zusammengefasst werden:

Fakt 4.1.10.

1. *Ist K Hilbertsch, so müssen alle Hilbertmengen unendlich sein, also insbesondere auch K selbst.*
2. *Globale Körper sind Hilbertsch ([FJ86, 12.8]).*
3. *Jede endlich erzeugte Körpererweiterung eines Hilbertschen Körpers ist Hilbertsch ([FJ86, 11.11]).*
4. *Ist K ein Hilbertscher Körper, $n \in \mathbb{N}$, so hat K unendlich viele paarweise linear disjunkte Galoiserweiterungen mit Galoisgruppe $\mathfrak{S}_n$ ([FJ86, 15.9]).*

Mit diesen Aussagen bewaffnet lässt sich nun folgendes Beispiel konstruieren:

Beispiel 4.1.11. *Sei Z ein normales Schema von Dimension ≥ 1, W eine Galoisüberlagerung mit $G = \mathrm{Gal}(K(W)|K(Z)) = \mathfrak{A}_4$ (die Existenz einer solchen ist durch obigen Fakt sichergestellt). Betrachte*

$$H' = \{\mathrm{id}, (12)(34)\} \subset H = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}.$$

Dann gilt offenbar $H'^G = H^G$; für $X = W/H'$, $Y = W/H$ gilt also $X \sim_Z Y$, obwohl X eine zweifache Überlagerung von Y ist.

Die Äquivalenzklassen der endlichen Überlagerungen unter der Kronecker-Äquivalenz bezeichnet man als *Kroneckerklassen*. Die Kroneckermengen aller Überlagerungen in einer solchen Kroneckerklasse $\mathcal{K}$ haben alle die gleiche Dirichletdichte; daher sprechen wir von der *Dirichletdichte* $\delta(\mathcal{K})$ von $\mathcal{K}$.

Enthält eine Kroneckerklasse eine Galoisüberlagerung, so ist diese eindeutig bestimmt. Betrachten wir die Kroneckerklasse als Kategorie (mit endlichen dominanten Morphismen), so ist die Galoisüberlagerung das Endobjekt. Dies folgt aus Satz 4.1.2.

Was nutzt uns diese Einteilung in Kroneckerklassen? Wir wollen nur kurz eine Anwendung zeigen.

Satz 4.1.12. *Für eine Kroneckerklasse $\mathcal{K}$ über einem normalen Schema Y sei $m(\mathcal{K}) = \min\{[K(X) : K(Y)] | X \in \mathcal{K}\}$. Sei $X \in \mathcal{K}$, bezeichne mit $\operatorname{Aut}(X|Y)$ die Gruppe der Decktransformationen von $X|Y$. Dann gilt:*

(i) $\# \operatorname{Aut}(X|Y) \leq \frac{1}{\delta(\mathcal{K})} \leq m(\mathcal{K})$;

(ii) $\# \operatorname{Aut}(X|Y) = \frac{1}{\delta(\mathcal{K})} \Leftrightarrow \# \operatorname{Aut}(X|Y) = m(\mathcal{K}) \Leftrightarrow X|Y$ *ist normal.*

(iii) $\frac{1}{\delta(\mathcal{K})} = m(\mathcal{K}) \Leftrightarrow \mathcal{K}$ *enthält eine Galoisüberlagerung von Y.*

Beweis. Zunächst erinnern wir uns an Korollar 3.8.6. In obige Schreibweise übersetzt, bedeutet es nichts anderes als $\frac{1}{\delta(\mathcal{K})} \leq [K(X) : K(Y)]$, mit Gleichheit genau dann, wenn X eine Galoisüberlagerung von Y ist. Damit haben wir die Gleichung $\frac{1}{\delta(\mathcal{K})} \leq m(\mathcal{K})$ und (iii) bereits erledigt.

Für das weitere nehme man zunächst an, $K(X)|K(Y)$ sei separabel. Sei $\bar{X}$ der Galoisabschluss von $X|Y$, $G = \operatorname{Gal}(K(\bar{X})|K(Y)), H = \operatorname{Gal}(K(\bar{X})|K(X))$. Dann gilt $\delta(\mathcal{K}) = d(D(X|Y)) = \frac{\# H^G}{\# G}$ (vgl. den Beweis von Korollar 1.3.9). Sei nun $N_G(H)$ der Normalisator von H in G. Dann gibt es genau $(G : N_G(H))$ Konjugierte von H; es gilt daher $\# H^G \leq (G : N_G(H)) \# H$, also

$$\frac{1}{\delta(\mathcal{K})} = \frac{\# G}{\# H^G} \geq (N_G(H) : H).$$

Nun ist $(N_G(H) : H)$ aber offenbar die Anzahl der Automorphismen der Körpererweiterung $K(X)|K(Y)$; jeder Automorphismus entspricht eineindeutig einer Decktransformation von $X|Y$. Damit haben wir die zweite Abschätzung gezeigt. Gleichheit gilt nur dann, wenn H normal ist, also $X|Y$ galoissch. Damit ist im separablen Fall alles bewiesen.

Im allgemeinen Fall beachte man, dass nach Proposition 2.3.3 jede Decktransformation von X automatisch eindeutig eine Decktransformation des separablen Abschlusses $\tilde{X}$ von Y in X induziert. Daher gilt $\# \operatorname{Aut}(X|Y) \leq \# \operatorname{Aut}(\tilde{X}|Y)$; wegen $\mathcal{K}(X) = \mathcal{K}(\tilde{X})$ folgt damit zumindest die (i). Für den Beweis der (ii) im allgemeinen Fall beachte man, dass gilt:

$$(*) \qquad X|Y \text{ normal } \Leftrightarrow \tilde{X}|Y \text{ galoissch und } \# \operatorname{Aut}(X|Y) = \# \operatorname{Aut}(\tilde{X}|Y).$$

Mit dieser Aussage sind die meisten Implikationen aus (ii) dann klar; wirklich zu zeigen ist nur noch $\# \operatorname{Aut}(X|Y) = \frac{1}{\delta(\mathcal{K})} \Rightarrow X|Y$ normal. Aus $\# \operatorname{Aut}(\tilde{X}|Y) = \frac{1}{\delta(\mathcal{K})}$

folgt aber mit $\mathcal{K}(X) = \mathcal{K}(\tilde{X})$ und dem bisher Gezeigten die Ungleichungskette $\frac{1}{\delta(\mathcal{K})} = \#\mathrm{Aut}(\tilde{X}|Y) \leq \#\mathrm{Aut}(X|Y) \leq \frac{1}{\delta(\mathcal{K})}$, also $\#\mathrm{Aut}(\tilde{X}|Y) = \#\mathrm{Aut}(X|Y) = \frac{1}{\delta(\mathcal{K})}$. Damit ist dann aber $\tilde{X}|Y$ galoissch, nach $(*)$ also $X|Y$ normal.

Zu $(*)$: Nach einer der vielen möglichen Definitionen der Normalität ist eine algebraische Erweiterung L eines Körpers K genau dann normal, wenn die Anzahl der Einbettungen von L in einen algebraischen Abschluss $\bar{K}$ von K gleich der Anzahl der Automorphismen von $L|K$ ist. Andererseits ist bei einer rein inseparablen Überlagerung $L|\tilde{L}$ jeder Körpermorphismus auf L eindeutig durch seine Werte auf $\tilde{L}$ bestimmt. Aus diesen beiden Aussagen lässt sich $(*)$ leicht folgern. $\square$

Damit ist uns nun tatsächlich ein (weitgehend) arithmetische Charakterisierung von normalen Überlagerung von Schemata gelungen, die auch im inseparablen Fall ihre Gültigkeit hat.

4.2 Arithmetische Äquivalenz

Kronecker-Äquivalenz ist eine relativ schwache Aussage über Überlagerungen von Schemata, da - wie wir gesehen haben - nicht einmal bei separablen Überlagerungen der Grad der Überlagerungen übereinstimmen muss.

Auf der Suche nach einer stärkeren Äquivalenzrelation rücken die Trägheitsgrade wieder stärker ins Visier:

Definition 4.2.1. *Sei $X \to Y$ eine endliche Überlagerung von normalen Schemata.*

a) Zu einem abgeschlossenen Punkt $y \in \overline{Y}$ definiert man den ***Zerlegungstyp*** *von y in X als Tupel*

$$A_{X|Y}(y) = (f_1, \ldots, f_r),$$

bestehend aus den Trägheitsgraden $f_i = f(x_i|y)$ aller Punkte $x_i \in \overline{X}$ über y in aufsteigender Reihenfolge: $f_1 \leq f_2 \leq \ldots \leq f_r$.

b) Für ein Tupel $A = (f_1, \ldots, f_r)$ von natürlichen Zahlen in aufsteigender Reihenfolge definiert man die Menge

$$P_A(X|Y) = \{y \in \overline{Y} |\, A_{X|Y}(y) = A\}$$

aller Punkte in $\overline{Y}$ mit diesem Zerlegungstyp.

c) Zwei Überlagerungen $X \to Y$, $X' \to Y$ heißen ***arithmetisch äquivalent*** *(in Zeichen $X \approx_Y X'$), wenn für fast alle abgeschlossenen Punkte in Y die Zerlegungstypen in X und X' übereinstimmen:*

$$X \approx_Y X' \Leftrightarrow \exists U \subseteq Y \text{ offen, nichtleer}: A_{X|Y}(y) = A_{X'|Y}(y)\ \forall\, y \in \bar{U}.$$

Aus der Definition wird unmittelbar klar:

Fakt 4.2.2. *Arithmetische Äquivalenz impliziert Kronecker-Äquivalenz:*

$$X \approx_Y X' \Rightarrow X \sim_Y X' \tag{49}$$

Auch arithmetische Äquivalenz wollen wir auf mehrere Arten charakterisieren. Dazu brauchen wir noch den Begriff der *semilokalen Zetafunktionen* von X über Y:

$$\zeta_X^{(y)}(s) := \prod_{x \in \overline{X}, x \mapsto y} \frac{1}{1 - N(x)^{-s}} = \zeta(X_y, s) \quad \text{für jedes } y \in \overline{Y}. \tag{50}$$

Hat nun ein Punkt $y \in \overline{Y}$ mit Norm q den Zerlegungstyp $(f_1, \ldots, f_r)$, so gilt für die zugehörige semilokale Zetafunktion:

$$\log \zeta_X^{(y)}(s) = -\sum_{i=1}^{r} \log(1 - q^{-f_i s}) = \sum_{i=1}^{r} \sum_{k=1}^{\infty} \frac{q^{-kf_i s}}{k} = \sum_{n=1}^{\infty} \left(\sum_{f_i | n} f_i \right) \frac{q^{-ns}}{n}.$$

Der Zerlegungstyp bestimmt also die semilokale Zetafunktion; umgekehrt läst sich aus der semilokalen Zetafunktion auch der Zerlegungstyp ablesen: Die Funktion bestimmt zunächst einmal für jedes $n \in \mathbb{N}$ die Summe $\sum_{f_i|n} f_i$; aus diesem lassen sich dann nach und nach die Zahlen $\#\{x \in \overline{X} | x \mapsto y, f(x|y) = n\}$ und damit der Zerlegungstyp bestimmen.

Satz 4.2.3. *Sei X, X' zwei endliche separable Überlagerungen eines normalen Schemas Y, (W, G) eine Galoisüberlagerung von Y, die auch endliche dominante Morphismen $W \to X$ und $W \to X'$ zulässt, und seien $H = \mathrm{Gal}(K(W)|K(X))$, $H' = \mathrm{Gal}(K(W)|K(X'))$. Dann sind folgende Aussagen äquivalent:*

(i) X und X' sind über Y arithmetisch äquivalent: $X \approx_Y X'$.

(ii) $A_{X|Y}(y) = A_{X'|Y}(y) \ \forall\, y \in \overline{Y}$.

(iii) $P_A(X|Y) =_d P_A(X'|Y) \ \forall\, r \ \forall\, A = (f_1, \ldots f_r) \in \mathbb{N}^r, f_1 \leq \ldots \leq f_r$.

(iv) Für jede Konjugationsklasse $\mathcal{C}$ von G gilt $\#(\mathcal{C} \cap H) = \#(\mathcal{C} \cap H')$.

(v) Die durch die trivialen Charaktere 1_H bzw. $1_{H'}$ von H bzw. H' auf G induzierten Charaktere 1_H^G und $1_{H'}^G$ stimmen überein.

(vi) Die semilokalen Zetafunktionen stimmen für alle $y \in \overline{Y}$ überein.

Beweis. Die Äquivalenz von (ii) und (vi) haben wir oben schon gezeigt; die Implikationen $(ii) \Rightarrow (i) \Rightarrow (iii)$ sind klar.
$(iii) \Rightarrow (iv)$: Zunächst einmal entnehmen wir dem Beweis von Proposition 3.8.3, dass eine offene nichtleere Menge $U \subseteq X$ existiert, so dass für jede Menge $A_{X|Y}(y) = (f_1, \ldots, f_r)$ mit $y \in \bar{U}$ gilt $\sum_{i=1}^{r} f_i \leq [K(X) : K(Y)]$; insbesondere folgt $r, f_r \leq [K(X) : K(Y)]$. Für $r > [K(X) : K(Y)]$ oder $f_r > [K(X) : K(Y)]$ gilt also $P_A(X|Y) \cap U = \emptyset$; somit ist die Menge der Punkte y, in denen die Gleichung aus (ii) nicht gilt, eine *endliche* Vereinigung von Dirichlet-Nullmengen (schließlich ist auch $Y - U$ eine solche) und hat daher selbst Dirichlet-Dichte Null. Nach dem Satz von Čebotarev existiert daher zu jedem $\sigma \in G$ ein (in W unverzweigter) Punkt $y \in \overline{Y}$, der nicht in der oben beschriebenen Dirichlet-Nullmenge liegt und über dem ein Punkt $w \in \overline{W}$ liegt mit $F_w = \sigma$. Für diesen gilt dann $A_{X|Y}(y) = A_{X'|Y}(y)$. Nun betrachten wir die Menge aller Elemente $\tau \in G$, für die $\tau\sigma\tau^{-1}$ in H liegt und zählen die Anzahl dieser Elemente auf zwei Arten. Einerseits beträgt ihre Anzahl offensichtlich gerade $\#Z_G(\sigma) \cdot \#(\mathcal{C}(\sigma) \cap H)$, wobei $Z_G(\sigma)$ der Zentralisator von σ und $\mathcal{C}(\sigma)$ die Konjugationsklasse von σ darstellt. Andererseits liegt mit τ offenbar auch jedes Element aus $H\tau$ in dieser Menge; daher können wir die Menge auch in Rechtsnebenklassen von H aufteilen. Sei nun $H\tau$ eine solche. Dann gilt $F_{\tau w} = \tau\sigma\tau^{-1}$, d.h. der Frobenius von τw lässt den Restklassenkörper $k(x_{H\tau})$ des Bildes von τw in X fest, also $f(x_{H\tau}|y) = 1$. Da sich diese Argumentation auch umdrehen lässt, beträgt die Kardinalität der obigen Menge also $\#H \cdot \#\{i|f_i = 1\}$. Nun folgern wir

$$\frac{\#(\mathcal{C}(\sigma) \cap H)}{\#H} = \frac{\#\{i|f_i = 1\}}{\#Z_G(\sigma)} = \frac{\#\{i|f_i' = 1\}}{\#Z_G(\sigma)} = \frac{\#(\mathcal{C}(\sigma) \cap H')}{\#H'} \tag{51}$$

Für $\sigma = \mathrm{id}$ gilt $\mathcal{C}(\mathrm{id}) = \{\mathrm{id}\} = \mathcal{C}(\mathrm{id}) \cap H = \mathcal{C}(\mathrm{id}) \cap H'$, also folgt aus obiger Gleichung $\#H = \#H'$; daraus wiederum ergibt sich mit (51) die Behauptung.
$(iv) \Rightarrow (v)$: Ist $\imath : H \hookrightarrow G$ die Inklusion, so gilt für den Charakter 1_H^G:

$$1_H^G(\sigma) = \imath_* 1_H(\sigma) = \frac{1}{\#H} \sum_{\tau \in G:\, \tau\sigma\tau^{-1} \in H} 1 = \frac{\#Z_G(\sigma) \cdot \#(\mathcal{C}(\sigma) \cap H)}{\#H}$$

Aus $\#(\mathcal{C} \cap H) = \#(\mathcal{C} \cap H')$ für alle Konjugationsklassen $\mathcal{C}$ folgt unmittelbar auch $\#H = \sum_{\mathcal{C}} \#(\mathcal{C} \cap H) = \sum_{\mathcal{C}} \#(\mathcal{C} \cap H') = \#H'$ und damit $1_H^G = 1_{H'}^G$.
$(v) \Rightarrow (vi)$: Wir betrachten dazu zu einem beliebigen Punkt $y \in \overline{Y}$ das Schema $(W_y)_{red} = \mathrm{Spec}\left(\bigoplus_j k(w_j)\right)$; dabei seien w_j gerade die Punkte von $\overline{W}$ über y. Man sieht leicht ein, dass die Wirkung von G auf W auch eine zulässige Wirkung von G auf $(W_y)_{red}$ induziert und dass für die Quotienten gilt: $(W_y)_{red}/G = \mathrm{Spec}\, k(y)$ sowie $(W_y)_{red}/H = (X_y)_{red}$ und $(W_y)_{red}/H' = (X_y')_{red}$. Nun gilt nach Proposition 3.2.3 e) und f) und Bemerkung 3.1.10

$$L((W_y)_{red}, 1_H^G) = L((W_y)_{red}, 1_H) = \zeta((W_y)_{red}/H) = \zeta((X_y)_{red}) = \zeta(X_y) = \zeta_X^{(y)}.$$

Damit ist auch diese Implikation bewiesen und der Beweis vollständig. □

Dem obigen Satz entnehmen wir unmittelbar das folgende

Korollar 4.2.4. *Seien X, X' zwei arithmetisch äquivalente endliche separable Überlagerungen eines normalen Schemas Y. Dann stimmen die Grade der Überlagerungen und die Zetafunktionen überein: $[K(X) : K(Y)] = [K(X') : K(Y)]$ und $\zeta(X, s) = \zeta(X', s)$.*

Es ließen sich noch mehr Invarianten aufstellen, doch die obigen sollen zur Verdeutlichung der Stärke der arithmetischen Äquivalenz ausreichen. Doch obwohl diese Äquivalenz eine deutlich stärkere Eigenschaft als Kronecker-Äquivalenz ist, müssen zwei arithmetisch äquivalente Schemata dennoch nicht unbedingt konjugiert sein. Wir betrachten dazu folgendes

Beispiel 4.2.5 (Gaßmann). *Sei Y ein normales Schema der Dimension ≥ 1, W eine Galoisüberlagerung mit $G = \mathrm{Gal}(K(W)|K(Y)) = \mathfrak{S}_6$ (zur Existenz siehe Fakt 4.1.10). In dieser Gruppe betrachten wir die Untergruppen*

$$\begin{aligned} H &:= \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}, \\ H' &:= \{\mathrm{id}, (12)(34), (12)(56), (34)(56)\}. \end{aligned}$$

Die beiden Gruppen sind offensichtlich nicht zueinander konjugiert, da die eine Gruppe Fixpunkte bei Operation auf G hat, die andere nicht. Betrachten wir nun eine beliebige Konjugationsklasse $\mathcal{C} \subset G$. Jede Konjugationsklasse besteht aus allen Elementen von G mit der gleichen Zykelstruktur, und da sowohl H als auch H' neben der Identität genau drei Produkte von zwei Transpositionen enthalten, gilt $\#(\mathcal{C} \cap H) = \#(\mathcal{C} \cap H')$, nach Satz 4.2.3 also $X := W/H \approx_Y W/H' =: X'$.

Auch beim Thema arithmetische Äquivalenz ist der Zahlkörperfall besser erforscht, zum einen natürlich, weil sie dort zuerst definiert wurde, zum anderen aber auch, weil man in diesem Fall viel mehr Invarianten findet, so zum Beispiel das Produkt aus Klassenzahl h_K und Regulator R_K. Zu einer umfangreichen Aufstellung der Invarianten lese man [Kl98, III.1.4].

Zum Abschluss wollen wir den Kreis schließen und zum Zahlkörperfall zurückkehren: Dort lässt sich arithmetische Äquivalenz (zumindest über $\mathbb{Q}$) auch analytisch definieren. Denn es gilt:

Proposition 4.2.6. *Zwei endliche Erweiterungen K, L von $\mathbb{Q}$ sind genau dann arithmetisch äquivalent, wenn ihre Zetafunktionen übereinstimmen.*

Beweis. Zu zeigen ist dazu nur noch, dass sich aus der (globalen) Zetafunktion alle semilokalen Zetafunktionen direkt ablesen lassen. Dazu schreibe man ζ_K und die $\zeta_K^{(p)}$ als Dirichletreihen:

$$\begin{aligned} \zeta_K(s) &= \sum_{n=1}^{\infty} \frac{a_n}{n^s} \\ \zeta_K^{(p)}(s) &= \sum_{n=1}^{\infty} \frac{a_{p^n}^{(p)}}{p^{ns}} \end{aligned}$$

Wegen $k^s \sum_{n=k}^{\infty} \frac{a_n}{n^s} = \sum_{n=k}^{\infty} \frac{a_n}{(n/k)^s} \longrightarrow a_k$ für $s \to \infty$ kann man aus der Zetafunktion nach und nach die Koeffizienten a_k der zugehörigen Dirichletreihe ablesen; darüber hinaus überlegt man sich leicht, dass wegen der Produktdarstellung $\zeta_K(s) = \prod_p \zeta_K^{(p)}(s)$ und der Eindeutigkeit der Dirichletreihe gelten muss: $a_{p^n}^{(p)} = a_{p^n}$. Daher kann man wie behauptet aus der Zetafunktion auf die semilokalen Zetafunktionen schließen. $\square$

Literatur

[Ar23] ARTIN, EMIL: *Über eine neue Art von L-Reihen*, Abhandlungen des Mathematischen Seminars Hamburg (1923), 89-108.

[CF67] CASSELS, J.W.S.; FRÖHLICH, A. (ED.): *Algebraic Number Theory*, Proceedings of an instructional conference organized by the London Mathematical Society, Thompson Book Company Inc., Washington D.C. (1967).

[De74] DELIGNE, PIERRE: *La conjecture de Weil: I*, Publications Mathématiques de l'IHES **43** (1974), 273-307.

[Dw60] DWORK, BERNARD M.: *On the rationality of the zeta function of an algebraic variety*, American Journal of Mathematics **82** (1960), 631-648.

[EGA II] GROTHENDIECK, ALEXANDER: *Éléments de Géométrie Algébrique: II Étude globale élémentaire de quelques classes de morphismes*, Publications Mathématiques de l'IHES **8** (1961).

[EGA IV_2] GROTHENDIECK, ALEXANDER: *Éléments de Géométrie Algébrique: IV Étude locale des schémas et des morphismes de schémas, Seconde partie*, Publications Mathématiques de l'IHES **24** (1965).

[EGA IV_3] GROTHENDIECK, ALEXANDER: *Éléments de Géométrie Algébrique: IV Étude locale des schémas et des morphismes de schémas, Troisième partie*, Publications Mathématiques de l'IHES **28** (1966).

[EGA IV_4] GROTHENDIECK, ALEXANDER: *Éléments de Géométrie Algébrique: IV Étude locale des schémas et des morphismes de schémas, Quatrième partie*, Publications Mathématiques de l'IHES **32** (1967).

[Ei99] EISENBUD, DAVIS: *Commutative Algebra with a View towards Algebraic Geometry*, Springer GTM **150** (1999).

[FJ86] FRIED, MICHEAL D.; JARDEN, MOSHE: *Field Arithmetic*, Band 11 der *Ergebnisse der Mathematik und ihrer Grenzgebiete*, Springer-Verlag (1986).

[Gr65] GROTHENDIECK, ALEXANDER: *Formule de Lefschetz et rationalité des fonctions L*, Séminaire Bourbaki **279** (1965).

[Ha77] HARTSHORNE, ROBIN: *Algebraic Geometry*, GTM **52**, Springer-Verlag, New York (1977).

[Kl98] KLINGEN, NORBERT: *Arithmetical Similarities: Prime Decomposition and Finite Group Theory*, Oxford University Press (1998).

[Ko97] KOCH, HELMUT: *Zahlentheorie: Algebraische Zahlen und Funktionen*, Vieweg, Braunschweig/Wiesbaden (1997).

[La94] LANG, SERGE: *Algebraic Number Theory*, Second Edition, GTM **110**, Springer-Verlag, New York (1994).

[Ma86] MATSUMURA, HIDEYUKI: *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics 8, Cambridge University Press (1986).

[Mu99] MUMFORD, DAVID: *The Red Book of Varieties and Schemes*, LNM **1358**, Springer-Verlag, Berlin (1999).

[Ne92] NEUKIRCH, JÜRGEN: *Algebraische Zahlentheorie*, Springer-Verlag (1992).

[Sch31] SCHMIDT, FRIEDRICH KARL: *Analytische Zahlentheorie in Körpern der Charakteristik* p, Mathematische Zeitschriften **33** (1931), 1-32.

[SGA 1] GROTHENDIECK, ALEXANDER ET AL.: *Revêtements étales et Groupe Fondamental (SGA 1)*, Springer LNM **224** (1971).

[Se65] SERRE, JEAN PIERRE: *Zeta and L Functions*, in *Algebraic Arithmetic Geometry* (Schilling, ed.), Harper & Row, New York (1965), 82-92.

[We48] WEIL, ANDRÉ : *Sur les courbes algébriques et les variétés qui s'en deduisent*, Actualités scientifiques et industrielles **1041**, Hermann, Paris (1948).