ASYMPTOTIK WILD VERZWEIGTER ABELSCHER FUNKTIONENKÖRPER

vorgelegt von
Diplom-Mathematiker

THORSTEN LAGEMANN

aus Siegen

Von der Fakultät II - Mathematik und Naturwissenschaften
der Technischen Universität Berlin
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
Dr. rer. nat.
genehmigte Dissertation

Promotionsausschuss:
Vorsitzender: Prof. Dr. Martin Skutella
Gutachter: Prof. Dr. Florian Heß
Gutachter: Prof. Dr. Jürgen Klüners
Gutachter: Prof. Dr. Michael E. Pohst
Tag der wissenschaftlichen Aussprache: 7. September 2010

Berlin 2010
D83

Meiner Frau Inken in Liebe gewidmet.

INHALT

KAPITEL 1

EINFÜHRUNG

Die Galoistheorie gehört für mich zu den faszinierendsten Theorien der Mathematik. Jeder algebraischen Gleichung über einem Körper K kann eine Galoisgruppe G zugewiesen werden, welche die Symmetrien ihrer Lösungen offenlegt. In der inversen Galoistheorie wird der Frage nachgegangen, ob es zu jedem Körper K und jeder Gruppe G eine Gleichung beziehungsweise einen Erweiterungskörper mit eben dieser Galoisgruppe G besitzt. In meiner hier vorliegenden Arbeit untersuche ich, wie oft eine vorgegebene Gruppe als Galoisgruppe auftritt. Die Verteilungsfunktion

$$Z(F, G; x) = |\{E/F : \mathrm{Gal}(E/F) \simeq G,\ \mathcal{N}\mathfrak{d}(E/F) \leq x\}|$$

misst, wieviele Körper mit Galoisgruppe G und beschränkter Diskriminante existieren. Gunter Malle hat in seinen Arbeiten von 2002 und 2004 für das asymptotische Verhalten dieser Funktion eine präzise Vermutung aufgestellt, welche die bekannten Ergebnisse über abelschen Gruppen von David Wright (1989) und einige kleineren Gruppen verallgemeinert. Ursprünglich nur für Zahlkörper formuliert, lässt sich seine Vermutung auch auf Funktionenkörper erweitern. Durch eine Heuristik von Jordan Ellenberg und Akshay Venkatesh (2005) über Hurwitzräume scheint es überzeugend, dass diese erweiterte Mallevermutung zumindest für Funktionenkörper, deren Charakteristik p teilerfremd zur Gruppenordnung $(G : 1)$ ist, zutreffen könnte. Es verbleibt der Fall, in dem die Charakteristik die Gruppenordnung teilt. Dies betrifft die globalen Funktionenkörper und ihre wild verzweigten Erweiterungen. Diese Fälle hat David Wright in seiner Arbeit (1989) über abelschen Gruppen ausgelassen, aber die Vermutung geäußert, dass in diesen Fällen keine anderen Ergebnisse zu erwarten seien.

In meiner Arbeit werde ich zeigen, dass die wild verzweigten Funktionenkörper zu Recht eine Sonderstellung inne haben. Für Funktionenkörper F mit Klassenzahl 1, das sind im Wesentlichen rationale Funktionenkörper, und nichtzyklische abelsche p-Gruppen G kann ich eine untere Schranke für $Z(F, G; x)$ angeben, welche über dem erwarteten Niveau liegt. Grund hierfür ist die Tatsache, dass bereits über einem lokalisierten Körper $F_{\mathfrak{p}}$ unendlich viele Erweiterungen mit Gruppe G existieren. Im Fall $p \nmid (G : 1)$ gibt es dieses Phänomen nicht. Hieraus entsteht auch die Fragestellung, welche Asymptotik die lokalen Erweiterungen, also die Funktionen $Z(F_{\mathfrak{p}}, G; x)$ besitzen. In dieser Arbeit weise ich den asymptotischen

Vergleich $Z(F_\mathfrak{p}, G; x) \sim c \cdot x^a$ für abelsche Gruppen G nach. Die a-Konstante hängt dabei nur vom Gruppentyp und der zu Grunde gelegten Charakteristik ab. Für zyklische p-Gruppen G kann ich auch für globale Funktionenkörper F den Asymptotiktyp von $Z(F, G; x)$ bestimmen. Interessanterweise hat die wilde Verzweigung in diesen Fällen keinen größeren Einfluss und die Asymptotik stimmt mit der erweiterten Mallevermutung überein. Als letztes Ergebnis gebe ich noch eine exakte Formel für die Asymptotik der einfachen zyklischen Gruppen G an und erreiche somit eine Verallgemeinerung der Arbeit von Cohen et al. (2002) über globale Zahlkörper auf globale Funktionen- und Zahlkörper.

Asymptotik von Galoisgruppen. — Eines der wichtigsten und umfangreichsten Resultate über die Asymptotik von Galoisgruppen wurde von David Wright für abelsche Erweiterungen von globalen Funktionen- oder Zahlkörper erzielt.

Satz 1.1 **(Wright, 1989)**. — *Es seien F ein globaler Körper der Charakteristik $p \geq 0$ und G eine abelsche Gruppe mit zu p teilerfremder Gruppenordnung und minimalem Primteiler $\ell \mid (G : 1)$. Des Weiteren seien $\tilde{F}$ die Erweiterung von F mit primitiven ℓ-ten Einheitswurzeln sowie*

$$a(G) = \frac{\ell}{(G:1)\cdot(\ell-1)} \qquad \text{und} \qquad b(F,G) = \frac{(G[\ell]:1)-1}{[\tilde{F}:F]}.$$

Dann gibt es eine positive Konstante $c(F, G)$ mit

$$Z(F, G; x) \sim c(F, G) \cdot x^{a(G)} \cdot \log(x)^{b(F,G)-1}.$$

Hierbei steht der Ausdruck $f(x) \sim g(x)$ für die asymptotische Äquivalenz von $f(x)$ und $g(x)$ und bedeutet, dass $f(x)$ und $g(x)$ den asymptotischen Quotienten $\lim\limits_{x\to\infty} f(x)/g(x) = 1$ besitzen. Teile von Wrights Beweismethode sind dem Anhangskapitel A gewidmet. Er untersucht im Wesentlichen die zu G gehörende Dirichletreihe

$$\Phi(F, G; s) = \sum_{\mathrm{Gal}(E/F)\simeq G} \mathcal{N}\mathfrak{d}(E/F)^{-s}$$

auf ihre Meromorphie. Die a-Konstante entspricht genau ihrer Konvergenzabszisse, die b-Konstante der Polordnung bei der Abszisse und die c-Konstante sowie obiges Resultat ergeben sich aus einem Taubersatz (siehe Kapitel D). Diesen analytischen Zugang der Asymptotikuntersuchung werde ich ebenfalls für fast die gesamte Arbeit beschreiten.

Basierend auf Wrights und anderen kleineren Ergebnissen hat Gunter Malle in seinen Arbeiten von 2002 und 2004 eine Vermutung für die Asymptotik von $Z(F, G; x)$ für allgemeine Gruppen aufgestellt. Seine Vermutung bezieht sich nur auf Zahlkörper, allerdings ist diese durch die Heuristik von Ellenberg und Venkatesh aus dem Jahre 2005 auf beliebige globale Körper der Charakteristik $p \nmid (G : 1)$ erweiterbar und daher möchte ich diese als erweiterte oder globale Mallevermutung bezeichnen. Ihrer nach soll die Form

$$Z(F, G; x) \sim c(F, G) \cdot x^{a(G)} \cdot \log(x)^{b(F,G)-1}$$

auch für allgemeine Gruppen gelten. Da sie für meine Arbeit irrelevant sind, verzichte ich auf die Angabe der Malleschen Formeln für die a- und b-Konstante und verweise den interessierten Leser auf die Originalarbeit. Ich beschäftige mich in dieser Arbeit nur mit der Asymptotik abelscher Gruppen und für diese Fälle reichen die gleichwertigen Wrightschen Formeln für $a(G)$ und $b(F,G)$ aus Satz 1.1 vollkommen aus. Anwendbar sind sie auch für den Fall $p \mid (G:1)$, wobei nur im Fall, in welchem die Charakteristik p und der minimale Primteiler ℓ der Gruppenordnung übereinstimmen, eine vermeintliche Lücke zu schließen ist. Im Fall $\ell = p$ ist nämlich zu beachten, dass es lediglich eine p-te Einheitswurzel gibt und es daher $\tilde{F} = F$ gilt.

Wild verzweigte Funktionenkörper. — Die Ausnahmefälle $p = \mathrm{char}(F) \mid (G:1)$ in Wrights Arbeit (1989) betreffen globale Funktionenkörper und ihre wild verzweigten Erweiterungen. Wright belässt es bei der Vermutung, dass sich ihre Asymptotik analog verhält. Für zyklische p-Erweiterungen trifft dies sogar zu. Dies werde ich im Kapitel 3 beweisen und erhalte folgendes Resultat.

Satz 3.1. — *Es seien F ein globaler Funktionenkörper der Charakteristik p und G eine zyklische p-Gruppe. Dann gibt es eine positive Konstante $c(F,G)$ mit*

$$Z(F,G;x) \sim c(F,G) \cdot x^{a(G)} \cdot \log(x)^{b(F,G)-1}.$$

Ist die Gruppe G zusätzlich einfach, so lässt sich $c(F,G)$ explizit berechnen.

Zunächst rechne ich dieses Ergebnis für die einfachen Erweiterungen mit Gruppe $G = Z_p$ nach. Es lässt sich fast ausschließlich mit klassenkörpertheoretischen und analytischen Methoden erreichen. Insbesondere ist hier ein schönes Lokal-Global-Prinzip gültig. Für zyklische p-Gruppen $G = Z_{p^n}$ höheren Grades nutze ich die Zerlegung von $\Phi(F,G;s)$ in eine alternierende Summe von Eulerprodukten nach Wright. Allerdings geht aus dieser Zerlegung nicht ihre Konvergenzabszisse hervor. Die benötigte untere Schranke erhalte ich via Einbettungsproblemen, die Jürgen Klüners in seiner Habilitationsschrift (2005) schon erfolgreich zur Untersuchung nilpotenter Erweiterungen von Zahlkörpern eingesetzt hat. Die Schärfe dieser Schranke ergibt sich dann aus der Analyse der Eulerfaktoren, welche in Wright (1989) allgemein für Gruppen mit durch p teilbarer Ordnung vollständig ausgespart ist.

Die Eulerfaktoren enthalten im Wesentlichen Informationen über die Erweiterungen der lokalisierten Körper $F_\mathfrak{p}$. Im Fall $p \nmid (G:1)$ gibt es, wenn überhaupt, nur endliche viele solcher Erweiterungen. Für abelsche p-Gruppen G allerdings gibt es unendlich viele G-Erweiterungen von $F_\mathfrak{p}$ und folglich haben diese eine nichttriviale Asymptotik. Im Kapitel 2 wird diese Asymptotik von abelschen p-Erweiterungen lokaler Funktionenkörper unter die Lupe genommen und ich erhalte folgendes Resultat.

Satz 2.1. — *Es seien $F_\mathfrak{p}$ ein lokaler Funktionenkörper der Charakteristik p und G eine abelsche p-Gruppe. Dann gibt es positive Konstanten $a_\mathfrak{p}(G)$ und $c(F_\mathfrak{p},G)$ mit*

$$Z(F_\mathfrak{p},G;x) \sim c(F,G) \cdot x^{a_\mathfrak{p}(G)}.$$

Für die Asymptotik der Erweiterungen eines globalen Funktionenkörper mit Klassenzahl 1 erhalte ich immerhin folgenden Satz.

Satz 2.2. — *Für die Asymptotik der abelschen p-Erweiterungen eines globalen Funktionenkörpers F der Charakteristik p und Klassenzahl* 1 *mit Galoisgruppe G gilt*

$$Z(F, G; x) \in \Omega\left(x^{a_{\mathfrak{p}}(G)}\right)$$

mit $a_{\mathfrak{p}}(G) > a(G)$ für nichtzyklische abelsche p-Gruppen G der Mindestgröße 10.

Dieses etwas überraschende Ergebnis widerlegt Wrights Einschätzung und ist das erste Gegenbeispiel zu der erweiterten Mallevermutung, in der die a-Konstante nicht die erwartete Größe hat. Für elementarabelsche 2-Gruppen werde ich diese Abschätzung sogar noch verbessern. Im Abschnitt 2.3 stelle ich Beispiele zur Verfügung, mit welchen die gefundenen Schranken mit $a(G)$ verglichen werden.

Zahm verzweigte einfache Funktionen- oder Zahlkörper. — Im letzten Kapitel widme ich mich der Konstante $c(F, G)$ für globale Funktionen- oder Zahlkörper F und einfachen zyklischen Gruppen G. Für Zahlkörper F gibt es bereits ein explizites Ergebnis von Cohen et al. (2002), welches hier nochmal bestätigt wird. Der Beweisumfang wird hier jedoch stark reduziert. Es ist nämlich lediglich erforderlich, die durch Wrights Zerlegung von $\Phi(F, G; s)$ gewonnenen Eulerfaktoren genau auszurechnen. Heraus kommt ein auch für Funktionenkörper mit zu $(G : 1)$ teilerfremden Charakteristik p gültiges Resultat. Die Konstante $c(F, Z_p)$ für wild verzweigte einfache Funktionenkörper passt sich diesem bis auf einen möglichen Faktor $(p-1)/p!$ in harmonischer Weise an.

Danksagungen. — *Diese Doktorarbeit wurde unterstützt durch ein dreijähriges Stipendium der* Berlin Mathematical School *im Rahmen der durch die Exzellenzinitiative zur Verfügung gestellten Mittel der deutschen Forschungsgesellschaft. Ich danke der Organisation der* Berlin Mathematical School *nicht nur für die Vergabe des Stipendiums sondern auch für das hervorragende Umfeld, in dem ich mich während meines Promotionsstudiums bewegen konnte. Meinem Doktorvater Prof. Dr. Florian Heß danke ich vielmals für die Vergabe und Betreuung dieses spannenden Themas und die zahlreichen intensiven und hilfreichen Gespräche. Ferner danke ich Prof. Dr. Jürgen Klüners und Prof. Dr. Michael E. Pohst für die Übernahme des Koreferats und ihre Unterstützung des Promotionsverfahren. Meinen ehemaligen und jetzigen Kollegen danke ich für ihre Unterstüzung und Freundschaft. Zu guter Letzt danke ich meiner Familie für den liebevollen Rückhalt.*

KAPITEL 2

ASYMPTOTIK ABELSCHER p-ERWEITERUNGEN

In diesem Kapitel wird die Asymptotik abelscher p-Erweiterungen lokaler Funktionenkörper von der Charakteristik p bestimmt. Diese liegt über dem durch die erweiterte Mallevermutung vorgegebenen Niveau und es gilt folgender Satz.

Satz 2.1. — *Es seien $F_\mathfrak{p}$ ein lokaler Funktionenkörper der Charakteristik p und G eine abelsche p-Gruppe vom Exponenten p^e und p^i-Rängen $g_i = \dim G[p^i]/G[p^{i-1}]$. Dann ist die Zählfunktion $Z(F_\mathfrak{p}, G; x)$ asymptotisch äquivalent zu*

$$Z(F_\mathfrak{p}, G; x) \sim c(F_\mathfrak{p}, G) \cdot x^{a_\mathfrak{p}(G)}$$

mit positiver Konstante $c(F_\mathfrak{p}, G)$ und

$$a_\mathfrak{p}(G) = \frac{(1-p^{-1}) \cdot \sum_{i=0}^{e-1} p^i \cdot g_{e-i}}{\sum_{i=0}^{e-1} p^i \cdot (1-p^{-g_{e-i}}) \cdot p^{g_e+\ldots+g_{e-i}}}.$$

Die Asymptotik lokaler Funktionenkörper wirkt sich auch auf die Asymptotik globaler Funktionenkörper mit Klassenzahl 1 aus, sodass die erweiterte Mallevermutung nicht für Gruppen mit $p \mid (G:1)$ standhält. Im Abschnitt 2.3 beweise ich folgende Schranken.

Satz 2.2. — *Für die Asymptotik der abelschen p-Erweiterungen eines globalen Funktionenkörpers F der Charakteristik p und Klassenzahl 1 mit Galoisgruppe G gelten folgende Aussagen.*

(a) *Es sei $\mathfrak{p}$ eine beliebige Stelle in F. Dann gilt*

$$Z(F, G; x) \geq Z(F_\mathfrak{p}, G; x) \in \Omega\left(x^{a_\mathfrak{p}(G)}\right)$$

und es ist $a_\mathfrak{p}(G) > a(G)$ für nichtzyklische abelsche p-Gruppen $G \neq Z_2^2, Z_3^2, Z_2^3$.

(b) *Es seien G eine elementarabelsche Gruppe vom Rang $r = \dim G[p]$ und*

$$a(F, G) = \frac{1+r}{2 \cdot (p^r - 1)} \geq \frac{1}{p^{r-1} \cdot (p-1)} = a(G).$$

Dann gilt

$$Z(F, G; x) \in \Omega\left(x^{a(F,G)}\right)$$

und es ist $a(F, G) > a(G)$ für $G \neq Z_p, Z_2^2$.

Schlachtplan. — Die Asymptotik von abelschen Erweiterungen eines lokalen Körpers $F_\mathfrak{p}$ der Charakteristik p mit vorgegebener Galoisgruppe G hängt nur von ihrer p-Sylowgruppe ab, da es nur endlich viele Erweiterungen von $F_\mathfrak{p}$ mit vorgegebenen und zu p teilerfremden Grad gibt. Folglich liefert die Asymptotikbestimmung der abelschen p-Erweiterungen schon ein vollständiges Bild. Die Relativdiskriminante einer endlichen abelschen Erweiterung des lokalen Körpers $F_\mathfrak{p}$ kann eindeutig durch ihre höhreren Verzweigungsgruppen und deren Sprungstellen konstruiert werden. Mein Ansatz zur Quantifizierung abelscher Erweiterungen von $F_\mathfrak{p}$ mit vorgegebener Gruppe ist es, die Erweiterungen mit vorgegebener Kette $\boldsymbol{G}$ von Verzweigungsgruppen und entsprechenden Sprungstellenlisten $\boldsymbol{m}$ gemäß Definition 2.3 zu zählen. Dabei soll $\boldsymbol{G}$ nur die Auflistung der Länge $l(\boldsymbol{G})$ der Faktorgruppen an den durch $\boldsymbol{m}$ vorgegebenen Sprungstellen sein. Ist $a(\boldsymbol{G},\boldsymbol{m})$ die Anzahl der Erweiterungen mit diesem Verzweigungsverhalten, so gilt

$$\Phi(F_\mathfrak{p},G;s)=\sum_{\mathrm{Gal}(E/F_\mathfrak{p})\simeq G}\mathcal{N}\mathfrak{d}(E/F)^{-s}=\sum_{\boldsymbol{G}}\sum_{\boldsymbol{m}}a(\boldsymbol{G},\boldsymbol{m})\cdot\prod_{i=0}^{l(\boldsymbol{G})}\mathcal{N}\mathfrak{p}^{-(m_i+1)\cdot t_i(\boldsymbol{G})\cdot s}$$

für die Dirichletreihe der G-Erweiterungen von $F_\mathfrak{p}$, wobei $t_i(\boldsymbol{G})=(G_i:1)-(G_{i-1}:1)$ eine von $\boldsymbol{G}$ abhängige Konstante ist. Die Zahl $a(\boldsymbol{G},\boldsymbol{m})$ ist mit Hilfe der lokalen Klassenkörpertheorie an Hand der kanonischen Filtration in der multiplikativen Gruppe $F_\mathfrak{p}^\times$ bestimmbar. Sie wächst exponentiell in den Sprungstellen und es gilt

$$a(\boldsymbol{G},\boldsymbol{m})=b(\boldsymbol{G},\mathcal{I})\cdot\prod_{i=1}^{l(\boldsymbol{G})}\mathcal{N}\mathfrak{p}^{r_i(\boldsymbol{G})\cdot(m_i-1-\lfloor\frac{m_i-1}{p}\rfloor)}$$

für eine von endlich vielen Konstanten $b(\boldsymbol{G},\mathcal{I})$ und nur von $\boldsymbol{G}$ abhängigen Zahl $r_i(\boldsymbol{G})$. Nach Gruppierung dieser Familien $\mathcal{I}$ gilt dann

$$\Phi(F_\mathfrak{p},G;s)=\sum_{\boldsymbol{G}}\sum_{\mathcal{I}}b(\boldsymbol{G},\mathcal{I})\sum_{\boldsymbol{m}\in\mathcal{I}}\prod_{i=0}^{l(\boldsymbol{G})}\mathcal{N}\mathfrak{p}^{r_i(\boldsymbol{G})\cdot(m_i-1-\lfloor\frac{m_i-1}{p}\rfloor)-(m_i+1)\cdot t_i(\boldsymbol{G})\cdot s}.$$

Eine Reihe dieser Gestalt entpuppt sich als rationale Funktion und das asymptotische Verhalten der Galoiserweiterungen mit Gruppe G kann durch einen Taubersatz gewonnen werden.

2.1. Arithmetische Zählung

Definition 2.3. — Es seien $F_\mathfrak{p}$ ein lokaler Körper mit Restklassencharakteristik $p=\mathrm{char}(\mathbb{F}_\mathfrak{p})$ und G eine endliche abelsche Gruppe. Dann bezeichne $\mathcal{F}_G$ die Menge aller Galoiserweiterungen $E/F_\mathfrak{p}$ mit Gruppe G innerhalb eines fest gewählten algebraischen Abschlusses von $F_\mathfrak{p}$ und $\mathcal{G}_G$ die Menge aller Paare $(\boldsymbol{G},\boldsymbol{m})$ mit den folgenden Eigenschaften.

(i) Es ist $\boldsymbol{G}=(G_{-1},G_0,G_1,\ldots,G_l)$ eine Auflistung einer Auflösung

$$G_{-1}\hookrightarrow G_0\hookrightarrow G_1\hookrightarrow\ldots\hookrightarrow G_l=G$$

von G, bei welcher die Faktoren G_i/G_{i-1} für $1\leq i\leq l$ als elementarabelsche Gruppe in $\mathbb{F}_\mathfrak{p}$ und für $i=0$ als zyklische Gruppe in $\mathbb{F}_\mathfrak{p}^\times$ einbettbar sind. Zudem ist auch G_{-1} zyklisch. Weiterer Bestandteil dieser Definition ist die Forderung $G_i\not\simeq G_{i-1}$ für die Indizes $1\leq i\leq l$.

(ii) Es ist $\boldsymbol{m} = (m_{-1}, m_0, m_1, \ldots, m_l)$ eine Auflistung gleicher Länge einer endlichen strikt montonen Folge ganzer Zahlen

$$-1 = m_{-1} < 0 = m_0 < m_1 < \ldots < m_l.$$

Hierbei ist ein Glied m_i nur dann durch p teilbar, wenn $m_i = p \cdot m_j$ für einen Index $0 \leq j \leq i$ gilt.

Für ein Paar $(\boldsymbol{G}, \boldsymbol{m})$ setze ich $l(\boldsymbol{G}) = l(\boldsymbol{m}) = l$.

Satz 2.4. — *Es seien $F_\mathfrak{p}$ ein lokaler Körper mit Restklassencharakteristik $p = \mathrm{char}(\mathbb{F}_\mathfrak{p})$ und G eine endliche abelsche Gruppe. Dann gibt es eine Abbildung*

$$\dagger : \mathcal{F}_G \to \mathcal{G}_G,\ E/F_\mathfrak{p} \mapsto (\boldsymbol{G}, \boldsymbol{m}),$$

sodass die Relativdiskriminante von E durch $\dagger(E/F_\mathfrak{p}) = (\boldsymbol{G}, \boldsymbol{m})$ berechenbar ist vermöge

$$\mathfrak{d}(E/F_\mathfrak{p}) = \prod_{i=0}^{l(\boldsymbol{G})} \mathfrak{p}^{(m_i+1)\cdot((G_i:1)-(G_{i-1}:1))}.$$

Beweis. — Es sei $E/F_\mathfrak{p} \in \mathcal{F}_G$ eine Galoiserweiterung von $F_\mathfrak{p}$ mit Gruppe G. Nach der lokalen Klassenkörpertheorie ist $E/F_\mathfrak{p}$ genau der offenen Untergruppe $U = \mathcal{N}_{E/F_\mathfrak{p}} E^\times$ der multiplikativen Gruppe $F_\mathfrak{p}^\times$ zugewiesen. Es seien

$$H_{-1} = F_\mathfrak{p}^\times / \langle U, \mathcal{O}_\mathfrak{p}^\times \rangle \qquad \text{und} \qquad H_m = F_\mathfrak{p}^\times / \langle U, 1 + \mathfrak{p}^{m+1} \rangle \qquad \text{für } m \geq 0$$

die Faktorgruppen von U entlang der Filtration

$$F_\mathfrak{p}^\times \rhd \mathcal{O}_\mathfrak{p}^\times \rhd 1 + \mathfrak{p} \rhd 1 + \mathfrak{p}^2 \rhd \ldots$$

offener Untergruppen in $F_\mathfrak{p}^\times$. Der Diskriminantenexponent berechnet sich nach Satz C.4 durch

$$d_\mathfrak{p}(E/F_\mathfrak{p}) = \sum_{m \geq 0} (m+1) \cdot ((H_m : 1) - (H_{m-1} : 1)).$$

Sind $m_{-1} = -1$ und $m_0 = 0$ sowie $m_1, \ldots, m_l$ die Sprungstellen m der Filtration mit $H_m \not\simeq H_{m-1}$ für $m \geq 1$, so berechnet sich dieser Exponent auch vermöge

$$d_\mathfrak{p}(E/F_\mathfrak{p}) = \sum_{i=0}^{l} (m_i + 1) \cdot ((H_{m_i} : 1) - (H_{m_i - 1} : 1)),$$

wobei hier beabsichtigt ist, dass der der zu $i = 0$ gehörende Summand auch verschwindend sein kann. Ich setze nun $\boldsymbol{G} = (H_{m_i})_{-1 \leq i \leq l}$, $\boldsymbol{m} = (m_i)_{-1 \leq i \leq l}$ und

$$\dagger(E/F_\mathfrak{p}) = (\boldsymbol{G}, \boldsymbol{m}).$$

Nun ist nur noch zu überprüfen, ob $\mathcal{G}_G$ tatsächlich der Bildraum dieser so gebildeten Abbildung $\dagger$ ist, d.h. für das Paar $(\boldsymbol{G}, \boldsymbol{m})$ sind die Eigenschaften (i) und (ii) aus Definition 2.3 nachzuweisen. Als Erstes zeige ich, dass $\boldsymbol{G}$ die geforderten Auflösungseigenschaften besitzt. Das bedeutet, G_{-1} muss zyklisch sein und es muss eine Kette von Einbettungen $G_{i-1} \hookrightarrow G_i$ geben, deren Kokerne für $1 \leq i \leq l$ in $\mathbb{F}_\mathfrak{p}$ und für $i = 0$ in $\mathbb{F}_\mathfrak{p}^\times$ einbettbar sind. Durch die kanonische exakte Sequenz

$$1 \to \mathbb{F}_\mathfrak{p} \to F_\mathfrak{p}^\times / \langle 1 + \mathfrak{p}^{m+1} \rangle \to F_\mathfrak{p}^\times / \langle 1 + \mathfrak{p}^m \rangle \to 1$$

wird eine Projektion $H_m \twoheadrightarrow H_{m-1}$ mit für $m \geq 1$ elementarabelschen Kern induziert. Gemäß Selbstdualität abelscher Gruppen gewinne ich hieraus eine Einbettung

$$G_{i-1} \simeq H_{m_{i-1}} \simeq H_{m_i-1} \simeq H^*_{m_i-1} \hookrightarrow H^*_{m_i} \simeq H_{m_i} \simeq G_i$$

mit für $1 \leq i \leq l$ elementarabelschen Kokern von $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$ nicht überschreitenden Rang. Für $i = 0$ verfahre ich analog, wobei ich mit der Sequenz

$$1 \to \mathbb{F}_\mathfrak{p}^\times \to F_\mathfrak{p}^\times/\langle 1+\mathfrak{p}\rangle \to F_\mathfrak{p}^\times/\mathcal{O}_\mathfrak{p}^\times \to 1$$

starte. Hieraus ist ebenfalls erkennbar, dass $G_{-1} = H_{-1}$ als endliches epimorphes Bild von $F_\mathfrak{p}^\times/\mathcal{O}_\mathfrak{p}^\times \simeq \mathbf{Z}$ zyklisch ist. Die nächste nachzuweisende Eigenschaft des Paares $(\boldsymbol{G}, \boldsymbol{m})$ ist, dass eine durch p teilbare Sprungstelle m_i das p-fache einer Sprungstelle m_j vom kleineren Index sein soll. Dazu nehme ich an, $m_i = p \cdot m$ sei eine durch p teilbare Sprungstelle und m selbst sei keine Sprungstelle. Dann gilt

$$\langle U, 1+\mathfrak{p}^{m+1}\rangle = \langle U, 1+\mathfrak{p}^m\rangle$$

und folglich enthält $\langle U, 1+\mathfrak{p}^{m+1}\rangle$ alle Elemente kongruent zu $1 + a \cdot t^m$ modulo $\langle 1+\mathfrak{p}^{m+1}\rangle$ für beliebige Konstanten $a \in \mathbb{F}_\mathfrak{p}$. Potenziere ich diese Elemente mit p, so erhalte ich

$$(1 + a \cdot t^m + b \cdot t^{m+1} + \ldots + \mathfrak{p}^{m_i+1})^p \equiv 1 + a^p \cdot t^{m_i} \pmod{\langle 1+\mathfrak{p}^{m_i+1}\rangle}.$$

Auf Grund der Surjektivität des Frobeniushomorphismus auf endlichen Körpern enthält $\langle U, 1+\mathfrak{p}^{m_i+1}\rangle$ somit auch alle Elemente kongruent zu $1 + a \cdot t^{m_i}$ modulo $\langle 1+\mathfrak{p}^{m_i+1}\rangle$ und es folgt daher

$$\langle U, 1+\mathfrak{p}^{m_i+1}\rangle = \langle U, 1+\mathfrak{p}^{m_i}\rangle$$

im Widerspruch zur Annahme, dass m_i eine Sprungstelle ist. □

Die im obigen Beweis gebildeten Gruppen H_m entsprechen den Faktorgruppen $G/G^m(E/F_\mathfrak{p})$ der Hilbertschen Verzweigungsgruppen mit oberer Nummerierung (vergleiche Neukirch (1992) Abschnitt 5.6). Durch die Parametrisierung der Galoiserweiterungen mit Gruppe G durch die Paare $(\boldsymbol{G}, \boldsymbol{m})$ ergibt sich unmittelbar die erste Zerlegung von $\Phi(F_\mathfrak{p}, G; s)$.

Korollar 2.5. — *Es sei $a(\boldsymbol{G}, \boldsymbol{m})$ die Faserstärke von $(\boldsymbol{G}, \boldsymbol{m})$ unter der Abbildung †. Dann gilt*

$$\Phi(F_\mathfrak{p}, G; s) = \sum_{\mathrm{Gal}(E/F_\mathfrak{p}) \simeq G} \mathcal{N}\mathfrak{d}(E/F_\mathfrak{p})^{-s} = \sum_{\boldsymbol{G}} \sum_{\boldsymbol{m}} a(\boldsymbol{G}, \boldsymbol{m}) \cdot \prod_{i=0}^{l(\boldsymbol{G})} \mathcal{N}\mathfrak{p}^{-(m_i+1)\cdot((G_i:1)-(G_{i-1}:1))\cdot s}.$$

Die Sprungstellenlisten $\boldsymbol{m}$ möchte ich im Folgenden zu Familien zusammenfassen, um eine feinere Zerlegung der Reihe zu gewinnen.

Definition 2.6. — Es sei $l \geq 0$ eine ganze Zahl und

$$\mathcal{N}^l = \{\boldsymbol{m} = (-1, 0, m_1, \ldots, m_l) : -1 < 0 < m_1 < \ldots < m_l\} \subset \{-1\} \times \{0\} \times \mathbf{Z}^l$$

eine Menge von endlichen strikt monotonen Folgen ganzer Zahlen. Für Indizes $1 \leq i \leq l$ und $0 \leq j < i$ setze ich

$$\mathcal{J}_{i,j}^{l} = \{\boldsymbol{m} \in \mathcal{N}^l : p \cdot m_j < m_i < p \cdot m_{j+1},\ p \nmid m_i\} \qquad \text{und} \qquad \mathcal{K}_{i,j}^{l} = \{\boldsymbol{m} \in \mathcal{N}^l : p \cdot m_j = m_i\}$$

und nenne diese Mengen Elementarfamilien. Zwei verschiedene Elementarfamilien zum Index i sind disjunkt. Einen nichtleeren Schnitt

$$\mathcal{I} = \mathcal{J}_1 \cap \ldots \cap \mathcal{J}_{l(\boldsymbol{G})} \qquad \text{mit} \qquad \mathcal{J}_i \in \{\mathcal{J}_{i,j}^{l}, \mathcal{K}_{i,j}^{l} : 0 \leq j < i\}$$

von l Elementarfamilien nenne ich zulässig und $\mathcal{J}_i$ die i-te Komponente oder i-te Elementarfamilie. Für die Projektion einer zulässigen Familie $\mathcal{I} \subset \mathcal{N}^l$ auf $\mathcal{N}^k$ verwende ich die Notation

$$\mathcal{I}^k = \{\boldsymbol{m}^k = (-1, 0, m_1, \ldots, m_k) : \boldsymbol{m} \in \mathcal{I}\} \subset \mathcal{N}^k.$$

Bemerkung 2.7. — *Es sei $(\boldsymbol{G}, \boldsymbol{m})$ ein Paar aus $\mathcal{G}_G$. Dann ist $\boldsymbol{m}$ in genau einer zulässigen Familie $\mathcal{I}$ enthalten.*

Beweis. — Die Eindeutigkeit folgt aus der Tatsache, dass zwei zulässige Familien mit unterschiedlicher i-ter Elementarfamilie disjunkt sind. Es ist also lediglich eine zuläsige Familie $\mathcal{I}$ mit $\boldsymbol{m} \in \mathcal{I}$ zu finden. Es seien $1 \leq i \leq l(\boldsymbol{G})$ ein beliebiger Index und $0 \leq j < i$ der zugehörige maximale Index mit $p \cdot m_j \leq m_i$. Ist m_i nicht durch p teilbar, so ist $p \cdot m_j < m_i < p \cdot m_{j+1}$ gültig und es folgt $\boldsymbol{m} \in \mathcal{J}_{i,j}^{l(\boldsymbol{G})}$. Ist m_i jedoch durch p teilbar, so fordert Definition 2.3 die Gleichheit $m_i = p \cdot m_j$ und es gilt $\boldsymbol{m} \in \mathcal{K}_{i,j}^{l(\boldsymbol{G})}$. Die gesuchte zulässige Familie $\mathcal{I}$ mit $\boldsymbol{m} \in \mathcal{I}$ ergibt sich schließlich als Schnitt der so gefundenen Mengen. □

Auf Grund von $\mathcal{K}_{i,0}^{l} = \emptyset$ ist die erste Elementarfamilie einer zulässigen Familie $\mathcal{I} = \mathcal{J}_1 \cap \ldots \cap \mathcal{J}_l$ stets $\mathcal{J}_1 = \mathcal{J}_{1,0}^{l}$ und es stehen zur Wahl der i-ten Elementarfamilie $\mathcal{J}_i \in \{\mathcal{J}_{i,j}^{l}, \mathcal{K}_{i,j}^{l} : 0 \leq j < i\}$ nicht mehr als $2i - 1$ Möglichkeiten offen. Insgesamt gibt es also nicht mehr als $\prod_{i=1}^{l}(2i-1)$ zulässige Familien $\mathcal{I}$ der Länge l. Da auch die Anzahl der Auflösungen $\boldsymbol{G}$ der endlichen Gruppe G endlich ist, ergibt sich folgende günstige Verfeinerung der Reihenzerlegung aus Korollar 2.5.

Korollar 2.8. — *Für eine Auflösung $\boldsymbol{G}$ gemäß Definition 2.3 (i) und eine zulässige Familie $\mathcal{I}$ sei*

$$\Phi(F_{\mathfrak{p}}, \boldsymbol{G}, \mathcal{I}; s) = \sum_{\boldsymbol{m} \in \mathcal{I}} a(\boldsymbol{G}, \boldsymbol{m}) \cdot \prod_{i=0}^{l(\boldsymbol{G})} \mathcal{N}\mathfrak{p}^{-(m_i+1)\cdot((G_i:1)-(G_{i-1}:1))\cdot s}.$$

Dann besitzt die Dirichletreihe $\Phi(F_{\mathfrak{p}}, G; s)$ die endliche Zerlegung

$$\Phi(F_{\mathfrak{p}}, G; s) = \sum_{\boldsymbol{G}} \sum_{\mathcal{I}} \Phi(F_{\mathfrak{p}}, \boldsymbol{G}, \mathcal{I}; s).$$

Nun komme ich zum Hauptergebnis über die arithmetische Zählung von Galoiserweiterungen mit vorgegebenem Verzweigungsverhalten.

Satz 2.9. — *Es seien $(\boldsymbol{G},\boldsymbol{m})$ ein beliebiges Paar aus $\mathcal{G}_G$ mit Faserstärke $a(\boldsymbol{G},\boldsymbol{m})$ unter der Abbildung $\dagger$ und $\mathcal{I}$ die zulässige Familie mit $\boldsymbol{m}\in\mathcal{I}$. Sind $r_i=\dim G_i/G_{i-1}$ die p-Ränge der elementarabelschen Faktoren G_i/G_{i-1} für $1\le i\le l(\boldsymbol{G})$, dann gibt es einen in $\mathcal{N}\mathfrak{p}$ polynomialen Ausdruck $b(\boldsymbol{G},\mathcal{I})=f(\mathcal{N}\mathfrak{p})$ mit $f(t)\in\mathbf{Q}[t]$ und*

$$a(\boldsymbol{G},\boldsymbol{m})=b(\boldsymbol{G},\mathcal{I})\cdot\prod_{i=1}^{l(\boldsymbol{G})}\mathcal{N}\mathfrak{p}^{r_i\cdot(m_i-1-\lfloor\frac{m_i-1}{p}\rfloor)}.$$

Das Polynom $f(t)$ ist entweder das Nullpolynom oder vom Grad $r(\mathcal{I})$. Der Grad $r(\mathcal{I})=\sum' r_i$ errechnet sich als Summe der r_i über alle Indizes $1\le i\le l(\boldsymbol{G})$ mit $p\nmid m_i$.

Unmittelbar hieraus ergibt sich die letzte und entscheidende Zerlegung von $\Phi(F_\mathfrak{p},G;s)$.

Korollar 2.10. — *Es seien $\boldsymbol{G}$ eine Auflösung gemäß Definition 2.3 (i) und $\mathcal{I}$ eine zulässige Familie. Des Weiteren seien $r_i=\dim G_i/G_{i-1}$ für $1\le i\le l(\boldsymbol{G})$ und $t_i=(G_i:1)-(G_{i-1}:1)$ für $0\le i\le l(\boldsymbol{G})$. Dann gilt*

$$\Phi(F_\mathfrak{p},\boldsymbol{G},\mathcal{I};s)=b(\boldsymbol{G},\mathcal{I})\cdot\mathcal{N}\mathfrak{p}^{-t_0\cdot s}\cdot\sum_{\boldsymbol{m}\in\mathcal{I}}\prod_{i=1}^{l(\boldsymbol{G})}\mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}$$

mit

$$\alpha_i(m_i;s)=r_i\cdot\left(m_i-1-\left\lfloor\frac{m_i-1}{p}\right\rfloor\right)-(m_i+1)\cdot t_i\cdot s.$$

Beweis. — Nach Korollar 2.8 und Satz 2.9 folgt

$$\begin{aligned}\Phi(F_\mathfrak{p},\boldsymbol{G},\mathcal{I};s)&=\sum_{\boldsymbol{m}\in\mathcal{I}}a(\boldsymbol{G},\boldsymbol{m})\cdot\prod_{i=0}^{l(\boldsymbol{G})}\mathcal{N}\mathfrak{p}^{-(m_i+1)\cdot t_i\cdot s}\\&=\sum_{\boldsymbol{m}\in\mathcal{I}}\left(b(\boldsymbol{G},\mathcal{I})\cdot\prod_{i=1}^{l(\boldsymbol{G})}\mathcal{N}\mathfrak{p}^{r_i\cdot(m_i-1-\lfloor\frac{m_i-1}{p}\rfloor)}\right)\cdot\prod_{i=0}^{l(\boldsymbol{G})}\mathcal{N}\mathfrak{p}^{-(m_i+1)\cdot t_i\cdot s}.\end{aligned}$$

Abschließend ist noch $m_0=0$ zu beachten. □

Für den Beweis von Satz 2.9 ist es völlig ausreichend, sich auf abelsche p-Gruppen zu beschränken. Da abelsche Gruppen direkte Produkte ihrer Sylowgruppen sind, verhält sich nämlich die Anzahl von Untergruppen mit bestimmter Faktorgruppe multiplikativ über die Sylowgruppen. Die Faktorgruppen von $F_\mathfrak{p}^\times$ mit zu p teilerfremder Ordnung sind überschaubar und ergeben sich schon aus den epimorphen Bildern von $F_\mathfrak{p}^\times/\langle 1+\mathfrak{p}\rangle\simeq\mathbf{Z}\times\mathbb{F}_\mathfrak{p}^\times$. Ist H das Komplement der p-Sylowgruppe $G[p^\infty]$ von G, so gilt insbesondere

$$a(\boldsymbol{G},\boldsymbol{m})=a((H_{-1},H),(-1,0))\cdot a(\tilde{\boldsymbol{G}},\boldsymbol{m})$$

mit den durch $\tilde{G}_i=G_i\cap G[p^\infty]$ und $H_i=G_i\cap H$ gebildeten Auflösungen. Als nächstes reduziere ich mein Zählproblem auf das Zählen in endlichen Gruppen. Ist nämlich ein Paar $(\boldsymbol{G},\boldsymbol{m})$ für eine abelsche p-Gruppe G mit Exponenten p^e vorgegeben, so müsste die Normgruppe $U=\mathcal{N}_{E/F_\mathfrak{p}}E^\times$ eines Urbilds $E/F_\mathfrak{p}$ unter $\dagger$ ungeachtet ihrer Existenz in jeden Fall die Untergruppe

$$p^e\mathbf{Z}\times\mathbb{F}_\mathfrak{p}^\times\times\langle 1+\mathfrak{p}^{m+1}\rangle\le U\le F_\mathfrak{p}^\times=\mathbf{Z}\times\mathbb{F}_\mathfrak{p}^\times\times\langle 1+\mathfrak{p}\rangle$$

mit $m = m_{l(\boldsymbol{G})}$ enthalten. Es reicht also, die entsprechenden Untergruppen in der endlichen abelschen p-Gruppe

$$X_m = F_{\mathfrak{p}}^{\times}/\langle p^e\mathbf{Z} \times \mathbb{F}_{\mathfrak{p}}^{\times} \times \langle 1+\mathfrak{p}^{m+1}\rangle\rangle \simeq Z_{p^e} \times \langle 1+\mathfrak{p}\rangle/\langle 1+\mathfrak{p}^{m+1}\rangle$$

ausfindig zu machen. Des Weiteren erscheint es mir bequemer, dieses Zählproblem zu dualisieren. Dabei können zu G isomorphen Untergruppen in $X_m^* \simeq X_m$ gezählt werden statt nach jenen in X_m mit zu G isomorpher Faktorgruppe. Ich betrachte $X_m^* = \mathrm{Hom}(X_m, \mathbf{Q}/\mathbf{Z})$ als Gruppe der Charaktere χ mit Modul $\mathfrak{p}^{m+1}$. Die Charaktergruppe X_n^* mit kleineren Erklärungsmodul $\mathfrak{p}^{n+1}$ ist vermöge des Pullbacks der kanonischen Projektion $X_m \twoheadrightarrow X_n = X_m/\langle 1+\mathfrak{p}^{n+1}\rangle$ in X_m^* eingebettet und ich betrachte

$$X_n^* \simeq \langle 1+\mathfrak{p}^{n+1}\rangle^{\perp} = \{\chi \in X_m^* : \chi(1+\mathfrak{p}^{n+1}) = 0\}$$

als Untergruppe von X_m^*.

Bemerkung 2.11. — *Die Faserstärke $a(\boldsymbol{G}, \boldsymbol{m})$ eines Paares $(\boldsymbol{G}, \boldsymbol{m})$ aus $\mathcal{G}_G$ unter der Abbildung † berechnet sich aus der Anzahl von zu G isomorphen Untergruppen $U^{\perp} \leq X^*_{m_{l(\boldsymbol{G})}}$ mit*

$$U^{\perp} \cap X^*_{m_i} \simeq G_i \qquad \textit{und} \qquad U^{\perp} \cap X^*_{m_i-1} \simeq G_{i-1} \qquad \textit{für } -1 \leq i \leq l(\boldsymbol{G}).$$

Beweis. — Es seien $l = l(\boldsymbol{G})$ und $m = m_l$. Nach der lokalen Klassenkörpertheorie ist die Faserstärke $a(\boldsymbol{G}, \boldsymbol{m})$ die Anzahl aller Untergruppen $U \leq X_m$ mit

$$X_m/\langle U, 1+\mathfrak{p}^{m_i+1}\rangle \simeq G_i \qquad \text{und} \qquad X_m/\langle U, 1+\mathfrak{p}^{m_i}\rangle \simeq G_{i-1} \qquad \text{für } 0 \leq i \leq l,$$

wobei ich hier $1+\mathfrak{p}^0 = \mathcal{O}_{\mathfrak{p}}^{\times}$ und $1+\mathfrak{p}^{-1} = F_{\mathfrak{p}}^{\times}$ setzen möchte. Nun weise ich einer solchen Gruppe U ihren orthogonalen Komplement $U^{\perp} = \{\chi \in X_m^* : \chi(U) = 0\}$ zu. Auf Grund der bidualen Relation $(U^{\perp})^{\perp} = U$ endlicher abelscher Gruppen ist diese Zuweisung bijektiv. Des Weiteren ist $U^{\perp}$ isomorph zu X_m/U und somit zu G. Auch ihre Untergruppen

$$U^{\perp} \cap X_n^* = \{\chi \in X_n^* : \chi(U) = 1\} = \{\chi \in X_m^* : \chi(\langle U, 1+\mathfrak{p}^{n+1}\rangle) = 0\}$$

sind isomorph zu $X_m/\langle U, 1+\mathfrak{p}^{n+1}\rangle$ und folglich zu jener Gruppe G_j mit $m_j \leq n < m_{j+1}$. □

Die Faserstärke $a(\boldsymbol{G}, \boldsymbol{m})$ soll nun induktiv berechnet werden. Ich nehme an, es gibt eine zu $H = G_{i-1}$ isomorphe Untergruppe $V = U_{i-1}^{\perp} \leq Y = X^*_{m_i-1}$. Dann ermittle ich die Anzahl der zu $G = G_i$ isomorphen Gruppen $U \leq X$ mit $U \cap Y = V$. Diese Situation ist im Diagramm

$$\begin{array}{ccccccccc}
1 & \longrightarrow & Y & \longrightarrow & X & \longrightarrow & Z & \longrightarrow & 1 \\
 & & \text{Injektionen}\uparrow & & ?\uparrow\ \#\ & & \uparrow & & \\
1 & \longrightarrow & H & \xrightarrow[\#]{?} & G & \longrightarrow & I & \longrightarrow & 1
\end{array}$$

Wieviele kommutierende Injektionen $H \hookrightarrow G \hookrightarrow X$ gibt es?

zusammengefasst und liefert die Motivation zu folgendem allgemeingültigen Lemma. Hier spielt die Anzahl

$$\begin{bmatrix} n \\ k \end{bmatrix}_p = \prod_{i=0}^{k-1} \frac{p^n - p^i}{p^k - p^i}$$

der k-dimensionalen Untervektorräume in einem n-dimensionalen Vektorraum über $\mathbb{F}_p$ eine große Rolle, da ich sehr oft mit elementarabelschen Gruppen vom Exponenten p hantieren muss. Man überlege sich hierbei, dass der Zähler die Anzahl der geordneten k-Tupel linear unabhängiger Vektoren in $\mathbb{F}_p^n$ und der Nenner die Anzahl der geordneten Basen eines zu $\mathbb{F}_p^k$ isomorphen Vektorraums angibt. Folglich ist der Zähler mit der Anzahl der Einbettungen von $\mathbb{F}_p^k$ in $\mathbb{F}_p^n$ und der Nenner mit der Anzahl der Automorphismen von $\mathbb{F}_p^k$ identisch.

Lemma 2.12. — *Es seien $X \geq Y$ und $G \geq H$ Erweiterungen abelscher p-Gruppen mit nichttrivialen elementarabelschen Quotienten $X/Y = Z$ und $G/H = I$. Die Gruppen X und Y erlauben eine gemeinsame Zerlegung*

$$X = \tilde{Y} \times \tilde{Z} \qquad \text{und} \qquad Y = \tilde{Y} \times p \cdot \tilde{Z} \qquad \text{mit} \qquad \tilde{Z} = Z_{p^\nu}^{\dim Z}.$$

Für eine zu H isomorphe Gruppe $V \leq Y$ bezeichne

$$c(V, G) = |\{U \leq X : U \cap Y = V,\ U \simeq G\}|$$

die Anzahl der zu G isomorphen Erweiterungen von V außerhalb von Y. Des Weiteren benutze ich folgende Notationen.

(i) *Es seien $g_i = \dim G[p^i]/G[p^{i-1}]$ und $h_i = \dim H[p^i]/H[p^{i-1}]$ die p^i-Ränge von G und H sowie $s_i = g_i - h_i$ ihre Differenz. Des Weiteren sei $r = s_1 + \ldots + s_e = \dim G/H$.*

(ii) *Mit $\sqrt{V} = \{y \in Y : p \cdot y \in V\}$ sei die maximale Hülle in Y, in welcher sich V elementarabelsch erweitern lässt, gekennzeichnet. Außerdem sei $d_i = \dim \sqrt{V}[p^i]/\langle \sqrt{V}[p^{i-1}], V[p^i] \rangle$ die Differenz der p^i-Ränge von $\sqrt{V}$ und V.*

(iii) *Entsprechend sei mit $\sqrt{V}^\circ = \{y \in X : p \cdot y \in V\}$ die maximale elementarabelsche Hülle in X gekennzeichnet und $d_i^\circ = \dim \sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle$.*

Dann ergeben sich folgende Formeln für $c(V, G)$.

(a) *Im Fall $\nu = 1$ gelten $X = Y \times Z$ und*

$$c(V,G) \;=\; (Y[p] : V[p])^r \;\cdot\; \prod_{i=2}^{e} \prod_{j=2}^{i-1} \prod_{k=0}^{s_i-1} p^{d_j} \cdot (p^{d_i} - p^k) \;\cdot\; \prod_{i=1}^{e} \begin{bmatrix} \dim Z - \sum_{j=1}^{i-1} s_j \\ s_i \end{bmatrix}_p.$$

(b) *Im Fall $\nu > 1$ gilt*

$$c(V,G) \;=\; (Y[p] : V[p])^r \;\cdot\; \prod_{i=2}^{e} \prod_{j=2}^{i-1} \prod_{k=0}^{s_i-1} p^{d_j} \cdot (p^{d_i} - p^k) \;\cdot\; \begin{bmatrix} 0 \\ s_1 \end{bmatrix}_p$$

$$\cdot \sum_{(t_2,\ldots,t_e)} \prod_{i=2}^{e} \begin{bmatrix} -s_1 + \sum_{j=2}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \cdot \begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \prod_{k=t_i}^{s_i-1} \frac{1}{p^{d_i} - p^k} \cdot \frac{p^{d_i} \cdot \prod_{j=2}^{i-1} p^{d_j^\circ - d_j}}{p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}},$$

wobei die Summe über alle Tupel $(t_2, \ldots, t_e)$ mit $0 \leq t_i \leq s_i$ läuft.

Dem technischen Beweis dieses Lemmas wird im Anhangskapitel G umfangreichen Raum gegegeben. Nun sind die gegebenen Formeln in der Situtation $X = X_m^*$ und $Y = X_{m-1}^*$ auszurechnen. Zur Berechnung der elementarabelschen Hüllen $\sqrt{V}$ und $\sqrt{V}^\circ$ einer Untergruppe $V \leq Y = X_{m-1}^*$ sind die durch p teilbaren Charaktere zu ermitteln.

Bemerkung 2.13. — *Es seien $X_m^* = \mathrm{Hom}(X_m, \mathbf{Q}/\mathbf{Z})$ die Gruppe von Charakteren auf X_m mit dem Erklärungsmodul $\mathfrak{p}^{m+1}$ und $n = \lfloor m/p \rfloor$ die größte ganze Zahl mit $p \cdot n \leq m$. Dann gilt*

$$X_n^* = p \cdot X_m^*.$$

Beweis. — Nach Hasses Einseinheitensatz C.1 ist X_m isomorph zum direkten Produkt

$$X_m \simeq \langle t \rangle / \langle t^{p^e} \rangle \times \prod_{x \in S_m} \langle x \rangle \qquad \text{mit} \qquad S_m = \{1 + b \cdot t^k + \mathfrak{p}^{m+1} : 1 \leq k \leq m,\ p \nmid k,\ b \in B\},$$

wobei B eine Basis von $\mathbb{F}_\mathfrak{p}$ über $\mathbb{F}_p$ ist. Entsprechend bilden die Charaktere $x^* \in X_m^*$ für $x \in S_m \cup \{\bar{t}\}$ mit

$$x^*(y) = \begin{cases} 1/(\langle x \rangle : 1) & y = x \\ 0 & x \neq y \in S_m \cup \{\bar{t}\} \end{cases}$$

ein minimales Erzeugendensystem von X_m^*, wobei ich die Notation $\bar{t} = t \cdot \langle t^{p^e} \rangle$ verwende. Für einen Erzeuger $x \neq \bar{t}$ mit $x = 1 + b \cdot t^k + \mathfrak{p}^{m+1}$ ist die Ordnung $(\langle x \rangle : 1) = p^\nu$ durch den maximalen Exponenten $\nu \geq 1$ mit $p^{\nu-1} \cdot k \leq m$ gegeben. Entsprechend gilt $x^*(x) = p^{-\nu}$. Es sei nun $\chi \in X_n^*$ ein Charakter mit Erklärungsmodul $\mathfrak{p}^{n+1}$. Dann ist χ eine Kombination $\sum_{x \in S_m \cup \{\bar{t}\}} a_x \cdot x^*$. Auf Grund von $\chi(1 + \mathfrak{p}^{n+1}) = 0$ folgen $\chi(x) = a_x \cdot x^*(x) \in \mathbf{Z}$ und somit $a_x = 0$ für $x = (1 + b \cdot t^k + \mathfrak{p}^{m+1}) \in S_m$ mit $k \geq n + 1$. Folglich wird X_n^* schon von den dualen Funktionen von $\bar{t}$ und $x = 1 + b \cdot t^k + \mathfrak{p}^{m+1}$ mit $k \leq n$ erzeugt. Es sei nun χ von der Form

$$\chi = a \cdot x^* \in \langle x^* \rangle \cap X_n^* \qquad \text{mit} \qquad x = 1 + b \cdot t^k + \mathfrak{p}^{m+1} \text{ und } k \leq n.$$

Ist ν maximal mit $p^{\nu-1} \cdot k \leq m$, so ist ν auch maximal mit $p^{\nu-2} \cdot k \leq n$. Dann folgen $x^{p^{\nu-1}} \in \langle 1 + \mathfrak{p}^{n+1} \rangle^\perp$ und

$$0 = \chi(x^{p^{\nu-1}}) = p^{\nu-1} \cdot \chi(x) = p^{\nu-1} \cdot a \cdot x^*(x) = a \cdot \frac{1}{p}.$$

Folglich muss auch a durch p teilbar sein und es folgen $\chi \in p \cdot X_m^*$ sowie $X_n^* \leq p \cdot X_m^*$. Für die umgekehrte Inklusion $p \cdot X_m^* \leq X_n^*$ betrachte ich einen beliebigen Charakter $\chi \in X_m^*$. Dann gilt

$$p \cdot \chi(1 + b \cdot t^k + \mathfrak{p}^{m+1}) = \chi(1 + b^p \cdot t^{k \cdot p} + \mathfrak{p}^{m+1}) \in \chi(1 + \mathfrak{p}^{m+1}) = 0$$

für $k \geq n + 1$ und somit $p \cdot \chi \in X_n^* = \langle 1 + \mathfrak{p}^{n+1} \rangle^\perp$. □

Bemerkung 2.14. — *Es seien $V \leq X_{m-1}^*$ eine Untergruppe mit den elementarabelschen Hüllen $\sqrt{V} \leq X_{m-1}^*$ und $\sqrt{V}^\circ \leq X_m^*$ sowie $n = \lfloor m/p \rfloor$ die größte ganze Zahl mit $p \cdot n \leq m$.*

(a) *Im Fall $p \nmid m$ gelten*

$$\sqrt{V}/\sqrt{V}[p] \simeq V \cap X_n^* \qquad \textit{und} \qquad \sqrt{V}^\circ/\sqrt{V}^\circ[p] \simeq V \cap X_n^*.$$

(b) *Im Fall $p \mid m$ gelten*

$$\sqrt{V}/\sqrt{V}[p] \simeq V \cap X_{n-1}^* \qquad \textit{und} \qquad \sqrt{V}^\circ/\sqrt{V}^\circ[p] \simeq V \cap X_n^*.$$

Beweis. — Um den Nachweis der Isomorphie von $\sqrt{V}/\sqrt{V}[p]$ auf die Fälle $m \neq p \cdot n$ und $m = p \cdot n$ zu vereinen, ersetze ich $n = \lfloor m/p \rfloor$ durch $\tilde{n} = \lfloor (m-1)/p \rfloor$. Dann gilt im ersten Fall $\tilde{n} = n$ und im zweiten Fall $\tilde{n} = n - 1$. Ich betrachte den Homomorphismus

(2.14.1) $$\psi : \sqrt{V}/\sqrt{V}[p] \to V \cap X_{\tilde{n}}^*,\ \chi \mapsto p \cdot \chi.$$

Zunächst gilt es, sich von der Wohldefiniertheit zu überzeugen. Für $\chi \in \sqrt{V}$ gelten $\psi(\chi) \in V$ und $\chi \in X_{m-1}^* = \langle 1 + \mathfrak{p}^m \rangle^\perp$. Auf Grund von $p \cdot (\tilde{n}+1) \geq m$ ist $x^p \in \langle 1 + \mathfrak{p}^m \rangle$ für $x \in \langle 1 + \mathfrak{p}^{\tilde{n}+1} \rangle$ und es folgt daher $(p \cdot \chi)(x) = \chi(x^p) = 0$. Das bedeutet, $\psi(\chi)$ hat den Erklärungsmodul $\mathfrak{p}^{\tilde{n}+1}$ und gehört damit zu $\langle 1 + \mathfrak{p}^{\tilde{n}+1} \rangle^\perp = X_{\tilde{n}}^*$. Das zeigt die Wohldefiniertheit von ψ. Des Weiteren ist ψ offensichtlich homomorph und injektiv. Nach Bemerkung 2.13 ist ψ auch surjektiv und es folgt die behauptete Isomorphie zwischen $\sqrt{V}/\sqrt{V}[p]$ und $V \cap X_{\tilde{n}}^*$. Es verbleibt nun noch die Isomorphie von $\sqrt{V}^\circ/\sqrt{V}^\circ[p]$ nachzuweisen. Analog zu der obigen Vorgehensweise betrachte ich nun

(2.14.2) $$\psi^\circ : \sqrt{V}^\circ/\sqrt{V}^\circ[p] \to V \cap X_n^*,\ \chi \mapsto p \cdot \chi.$$

Auf Grund von $p \cdot (n+1) \geq m+1$ ist $(p \cdot \chi)(1 + \mathfrak{p}^{n+1}) = 0$ und somit ist ψ° wohldefiniert. Auch hier folgen unmittelbar Homomorphie, Injektivität und Surjektivität gemäß Bemerkung 2.13. □

Satz 2.15. — *Für $m \geq 1$ seien $X = X_m^*$, $Y = X_{m-1}^*$ und $Z = \mathbb{F}_\mathfrak{p}$ sowie $V \leq Y$ eine zu H isomorphe Untergruppe. Ich setze zudem $r = \dim G/H = s_1 + \ldots + s_e$. Dann nehmen die p^i-Ränge d_i und d_i° folgende Werte an.*

(i) *Es ist*

$$d_1 = 1 - \dim H[p] + [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \cdot \left(m - 1 - \left\lfloor \frac{m-1}{p} \right\rfloor \right).$$

(ii) *Es seien $i \geq 2$ und $n = \lfloor m/p \rfloor$. Dann gilt im Fall $m \neq p \cdot n$*

$$d_i = \dim(V \cap X_n^*)[p^{i-1}]/\langle (V \cap X_n^*)[p^{i-2}], p \cdot V[p^i] \rangle$$

und im Fall $m = p \cdot n$

$$d_i = \dim(V \cap X_{n-1}^*)[p^{i-1}]/\langle (V \cap X_{n-1}^*)[p^{i-2}], p \cdot V[p^i] \rangle.$$

(iii) *Es seien $i \geq 2$ und $m = p \cdot n$. Dann gilt*

$$d_i^\circ = \dim(V \cap X_n^*)[p^{i-1}]/\langle (V \cap X_n^*)[p^{i-2}], p \cdot V[p^i] \rangle.$$

Insgesamt ergibt sich die Fortsetzungsanzahl $c(V, G)$ wie folgt.

(a) *Im Fall $p \nmid m$ gilt*

$$c(V,G) = \mathcal{N}\mathfrak{p}^{r \cdot (m-1-\lfloor \frac{m-1}{p} \rfloor)} \cdot \frac{\prod_{i=2}^{e} \prod_{j=2}^{i-1} \prod_{k=0}^{s_i-1} p^{d_j} \cdot (p^{d_i} - p^k) \cdot \prod_{i=1}^{e} \begin{bmatrix} [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] - \sum_{j=1}^{i-1} s_j \\ s_i \end{bmatrix}_p}{(H[p] : Z_p)^r}.$$

(b) *Im Fall $p \mid m$ und $p^{\nu-1} \mid\mid m$ gilt*

$$c(V,G) = \mathcal{N}\mathfrak{p}^{r\cdot(m-1-\lfloor\frac{m-1}{p}\rfloor)} \cdot \frac{\prod_{i=2}^{e}\prod_{j=2}^{i-1}\prod_{k=0}^{s_i-1} p^{d_j}\cdot(p^{d_i}-p^k)\cdot \begin{bmatrix} 0 \\ s_1 \end{bmatrix}_p}{(H[p]:Z_p)^r}$$
$$\cdot \sum_{(t_2,\dots,t_e)} \prod_{i=2}^{e} \begin{bmatrix} -s_1+\sum_{j=2}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \cdot \begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \prod_{k=t_i}^{s_i-1} \frac{1}{p^{d_i}-p^k} \cdot \frac{p^{d_i}\cdot\prod_{j=2}^{i-1} p^{d_j^\circ - d_j}}{p^{t_i}\cdot\prod_{j=1}^{i-1} p^{s_j}},$$

wobei die Summe über alle Tupel $(t_2,\dots,t_e)$ mit $0 \le t_i \le s_i$ läuft.

Beweis. — Zunächst zeige ich, dass die Fälle (a) und (b) genau zu den entsprechenden Fällen in Lemma 2.12 gehören. Die Formeln (a) und (b) ergeben sich dann unmittelbar aus jenen von Lemma 2.12 und

$$(Y[p]:V[p]) = p^{d_1} = p^{[\mathbb{F}_\mathfrak{p}:\mathbb{F}_p]\cdot(m-1-\lfloor\frac{m-1}{p}\rfloor)} \cdot \frac{p}{(H[p]:1)} = \mathcal{N}\mathfrak{p}^{m-1-\lfloor\frac{m-1}{p}\rfloor} \cdot \frac{1}{(H[p]:Z_p)}.$$

Abschließend sind noch die Formeln für die p^i-Ränge nachzuweisen.

(a) Im Fall $p \nmid m$ besitzt X_{m-1}^* ein Komplement in X_m^* und es gilt $X = Y \times \mathbb{F}_\mathfrak{p}$. Denn in diesem Fall ist $T_m = \{1 + b\cdot t^m + \mathfrak{p}^{m+1} : b \in B\}$ ein Teilsystem der Erzeuger $S_m \cup \{\bar{t}\}$ von X_m und es folgt

$$Y = X_{m-1}^* = \prod_{x\in\tilde{S}_m\cup\{\bar{t}\}} \langle x\rangle \qquad \text{und} \qquad X = X_m^* = X_{m-1}^* \times \prod_{x\in T_m}\langle x\rangle \tag{2.15.1}$$

mit $\tilde{S}_m = S_m \setminus T_m$. Das zeigt, dass in diesem Fall die Formel (a) aus Lemma 2.12 anwendbar ist.

(b) Im Fall $p \mid m$ besitzt X_{m-1}^* kein Komplement in X_m, da die oben betrachtete Familie T_m nicht in S_m enthalten ist. Ist jedoch k teilerfremd zu p mit $p^{\nu-1}\cdot k = m$, so ersetze ich T_m durch $T_m = \{1 + b\cdot t^k + \mathfrak{p}^{m+1} : b \in B\}$. Dies sind Erzeuger von X_m mit der Ordnung p^ν. Die von ihren dualen Funktionen erzeugte Gruppe $\tilde{Z}$ hat p-Rang $[\mathbb{F}_\mathfrak{p}:\mathbb{F}_p]$ und ihr Schnitt mit X_{m-1}^* ist in $p\cdot X_m^*$ enthalten. Die von der Komplementärmenge $\tilde{S}_m = S_m \setminus T_m$ und $\bar{t}$ erzeugte Gruppe $\tilde{Y}$ ist eine Untergruppe in X_m^* sowie in X_{m-1}^*. Zusammengefasst gelten also

$$\tilde{Z} = \prod_{x\in T_m}\langle x^*\rangle = Z_{p^\nu}^{[\mathbb{F}_\mathfrak{p}:\mathbb{F}_p]} \qquad \text{und} \qquad \tilde{Y} = \prod_{x\in\tilde{S}_m\cup\{\bar{t}\}}\langle x^*\rangle$$

sowie

$$Y = X_{m-1}^* = \tilde{Y}\times p\cdot\tilde{Z} \qquad \text{und} \qquad X = X_m^* = \tilde{Y}\times\tilde{Z}. \tag{2.15.2}$$

Folglich ist die Formel (b) aus Lemma 2.12 anwendbar.

(i) Es ist $d_1 = \dim \sqrt{V}[p]/V[p]$. Dabei stimmt der p-Rang von $\sqrt{V}$ mit dem von Y und jener von V mit dem von H überein. Ersterer ist durch Korollar C.2 gegeben vermöge

$$\dim\sqrt{V}[p] = \dim Y[p] = 1 + \dim(\langle 1+\mathfrak{p}\rangle/\langle 1+\mathfrak{p}^m\rangle)[p] = 1 + [\mathbb{F}_\mathfrak{p}:\mathbb{F}_p]\cdot\left(m-1-\left\lfloor\frac{m-1}{p}\right\rfloor\right).$$

Die behauptete Formel ergibt sich also aus $d_1 = \dim\sqrt{V}[p]/V[p] = \dim\sqrt{V}[p] - \dim H[p]$.

(ii) Nun sei $i \geq 2$. Definitionsgemäß ist $d_i = \dim \sqrt{V}[p^i]/\langle \sqrt{V}[p^{i-1}], V[p^i]\rangle$. Wieder möchte ich die Berechnung von d_i auf die Fälle $m \neq p \cdot n$ und $m = p \cdot n$ vereinen und ersetze $n = \lfloor m/p \rfloor$ durch $\tilde{n} = \lfloor (m-1)/p \rfloor$. Dann gilt im ersten Fall $\tilde{n} = n$ und im zweiten Fall $\tilde{n} = n - 1$. Nach `2.14.1` ist

$$\psi : \sqrt{V}/\sqrt{V}[p] \to V \cap X_{\tilde{n}}^*,\ \chi \mapsto p \cdot \chi$$

ein Isomorphismus. Folglich ist auch die Einschränkung

$$\psi_i : \sqrt{V}[p^i]/\sqrt{V}[p] \to (V \cap X_{\tilde{n}}^*)[p^{i-1}],\ \chi \mapsto p \cdot \chi$$

ein Isomorphismus. Für einen Isomorphismus $\alpha : A \to B$ gilt stets $A/C \simeq B/\alpha(C)$. Daher folgt die behauptete Formel auf Grund von $\psi_i(\sqrt{V}[p^{i-1}]) = (V \cap X_n^*)[p^{i-2}]$ sowie $\psi_i(V[p^i]) = p \cdot V[p^i]$.

(iii) Die Formel für d_i° im Fall $i \geq 2$ und $m = p \cdot n$ ergibt sich analog aus obiger Vorgehensweise. □

Ich wiederhole an dieser Stelle noch einmal die gewünschte Anwendung von Satz 2.15. Für eine Sprungstelle $m = m_i$ sei $V = U_{m_i-1}^\perp$ eine zu G_{i-1} isomorphe Untergruppe in $Y = X_{m_i-1}^*$ und $c(V, G) = c(U_{m_i-1}^\perp, G_i)$ die Anzahl der zu G_i isomorphen Gruppen $U = U_{m_i}^\perp$ in $X = X_{m_i}^*$ mit der Schnittbedingung $U \cap Y = V$. Durch sukzessive Anwendung kann hieraus tatsächlich die Faserstärke $a(\boldsymbol{G}, \boldsymbol{m})$ unter der Abbildung † berechnet werden.

Korollar 2.16. — *Es seien $E/F_\mathfrak{p} \in \mathcal{F}_G$ eine abelsche p-Erweiterung mit $\dagger(E/F_\mathfrak{p}) = (\boldsymbol{G}, \boldsymbol{m})$ und $m = m_{l(\boldsymbol{G})}$ der Führerexponent von $E/F_\mathfrak{p}$. Die Bildgruppen von $\langle \mathcal{N}_{E/F_\mathfrak{p}} E^\times, 1 + \mathfrak{p}^{n+1}\rangle$ unter der Projektion $F_\mathfrak{p}^\times \twoheadrightarrow X_m$ seien für $n \geq 0$ mit U_n und für $n = m$ mit $U = U_m$ gekennzeichnet. Dann hat die Faserstärke $a(\boldsymbol{G}, \boldsymbol{m})$ unter † die Faktorisierung*

$$a(\boldsymbol{G}, \boldsymbol{m}) = \prod_{i=1}^{l(\boldsymbol{G})} c(U_{m_i-1}^\perp, G_i).$$

Beweis. — Es sei $D/F_\mathfrak{p}$ ein beliebiges Urbild von $(\boldsymbol{G}, \boldsymbol{m})$ unter † mit entsprechender Filtration $W = W_m \leq W_n \leq X_m$. Dann sind die Faktorgruppen X_m/U_n und X_m/W_n und somit auch die dualen Gruppen isomorph vermöge

$$U^\perp \cap X_n^* = U_n^\perp \simeq X_m/U_n \simeq G_j \simeq X_m/W_n \simeq W_n^\perp = W^\perp \cap X_n^*,$$

wobei hier j der Index mit $m_j \leq n < m_{j+1}$ ist. Also hängen die in Satz 2.15 (i) - (iii) gebildeten Werte d_k und d_k° nur vom Isomorphietypen der Gruppen G_i aus der Auflösung $\boldsymbol{G}$ ab und es folgt

$$c(U_{m_i-1}^\perp, G_i) = c(W_{m_i-1}^\perp, G_i)$$

für $i \geq 1$. Da die Gruppe $X_0^* = X_{-1}^*$ zyklisch ist, besitzt sie genau eine zu $G_0 = G_{-1}$ isomorphe Untergruppe und es folgt $U_0^\perp = W_0^\perp$. Hieraus folgt

$$a(\boldsymbol{G}, \boldsymbol{m}) = \prod_{i=1}^{l(\boldsymbol{G})} c(U_{m_i-1}^\perp, G_i) = \prod_{i=1}^{l(\boldsymbol{G})} c(W_{m_i-1}^\perp, G_i).$$

□

Definition 2.17. — Es seien $(\boldsymbol{G},\boldsymbol{m})$ ein Paar aus $\mathcal{G}_G$ mit $m = m_{l(\boldsymbol{G})}$ und $\mathcal{I}$ die zulässige Familie mit $\boldsymbol{m} \in \mathcal{I}$. Des Weiteren sei $-1 \leq k < l(\boldsymbol{G})$ der maximale Index mit der folgenden Eigenschaft (i).

(i) Es gibt eine zu G_k isomorphe Untergruppe $U^\perp \leq X_m^*$ mit

$$U^\perp \cap X_{m_i}^* \simeq G_i \qquad \text{und} \qquad U^\perp \cap X_{m_i-1}^* \simeq G_{i-1} \qquad \text{für } 0 \leq i \leq k.$$

Dann definiere ich $b(\boldsymbol{G},\mathcal{I})$ als das Produkt

$$b(\boldsymbol{G},\mathcal{I}) = \prod_{i=1}^{k+1} c(U_{m_i-1}^\perp, G_i) \cdot \mathcal{N}\mathfrak{p}^{-r_i\cdot(m_i-1-\lfloor\frac{m_i-1}{p}\rfloor)}.$$

Die Zahl $c(U_{m_i-1}^\perp, G_i) \cdot \mathcal{N}\mathfrak{p}^{-r_i\cdot(m_i-1-\lfloor\frac{m_i-1}{p}\rfloor)}$ ist der in Satz 2.15 (a) bzw. (b) erscheinende Faktor nach der $\mathcal{N}\mathfrak{p}$-Potenz. Insbesondere gilt $b(\boldsymbol{G},\mathcal{I}) = 0$ für $k \neq l(\boldsymbol{G}) - 1$.

Für abelsche p-Gruppen ist der maximale Index k mindestens 1. Zunächst einmal sei daran erinnert, dass X_{-1} zyklisch mit dem gleichen Exponenten wie G ist und die p-Gruppe G_0/G_{-1} in $\mathbb{F}_\mathfrak{p}^\times$ einbettbar sein soll. Hieraus folgen $G_0 = G_{-1}$ und die Existenz einer zu G_{-1} isomorphen Untergruppe in $X_0^* = X_{-1}^*$. Des Weiteren ist m_1 nach Definition 2.3 nicht durch p teilbar und G_1/G_0 in $\mathbb{F}_\mathfrak{p}$ einbettbar. Hieraus folgt die Existenz der zu G_1 isomorphen Untergruppe $U^\perp \leq X_{m_1}^*$ mit $U^\perp \cap X_{m_1-1}^* \simeq G_0$.

Korollar 2.18. — *Die Konstante $b(\boldsymbol{G},\mathcal{I})$ ist unabhängig von der Wahl des Tupels $\boldsymbol{m} \in \mathcal{I}$.*

Beweis. — Es seien $\boldsymbol{m} \in \mathcal{I}$ ein beliebig gewähltes Tupel und $k-1 < l(\boldsymbol{G})$ ein Index mit der Eigenschaft 2.17 (i). Die gefundene zu G_{k-1} isomorphe Gruppe in X_m^* benenne ich hier mit V. Nach Satz 2.15 hängt $c(V,G_k)\cdot\mathcal{N}\mathfrak{p}^{-r_k\cdot(m_k-1-\lfloor\frac{m_k-1}{p}\rfloor)}$ nur von den p^i-Rängen d_i und d_i° mit $i \geq 2$ ab. Diese wiederum sind nur von den Isomorphietypen der Gruppen $G_{k-1} \simeq V$, $G_j \simeq V \cap X_n^*$ und im Fall $p \mid m$ auch $G_{j-1} \simeq V \cap X_{n-1}^*$ abhängig, wobei j der Index mit $p\cdot m_j \leq m_k < p\cdot m_{j+1}$ oder äquivalent $m_j \leq n = \lfloor m_k/p\rfloor < m_{j+1}$ ist. Als zulässige Familie ist $\mathcal{I}$ in der Elementarfamilie $\mathcal{J}_k \in \{\mathcal{J}_{k,j}^{l(\boldsymbol{G})}, \mathcal{K}_{k,j}^{l(\boldsymbol{G})}\}$ enthalten und folglich der zu k gehörende Index j mit $p\cdot m_j \leq m_k < p\cdot m_{j+1}$ invariant unter der Wahl eines Tupel $\boldsymbol{m}$. Hieraus folgt auch die Invarianz des Faktors $c(V,G_k)\cdot\mathcal{N}\mathfrak{p}^{-r_k\cdot(m_k-1-\lfloor\frac{m_k-1}{p}\rfloor)}$ und per Induktionsschluss auch die Invarianz von $b(\boldsymbol{G},\mathcal{I})$ unter der Wahl eines Tupels $\boldsymbol{m} \in \mathcal{I}$. □

Beweis von Satz 2.9. — Die Formel für $a(\boldsymbol{G},\boldsymbol{m})$ folgt unmittelbar aus den Korollaren 2.16 und 2.18. Es ist nur noch der Grad von $b(\boldsymbol{G},\mathcal{I})$ in $\mathcal{N}\mathfrak{p}$ zu untersuchen. Dieser wird von den Faktoren

$$\prod_{k=1}^{e}\left[\begin{matrix}[\mathbb{F}_\mathfrak{p}:\mathbb{F}_p] - \sum_{j=1}^{k-1} s_j \\ s_k\end{matrix}\right]_p = \prod_{k=1}^{e} \frac{1}{p^{s_1+\ldots+s_{k-1}}} \prod_{\nu=0}^{s_k-1} \frac{\mathcal{N}\mathfrak{p} - p^{s_1+\ldots+s_{k-1}+\nu}}{p^{s_k}-p^\nu},$$

mit Grad $r_i = s_1 + \ldots + s_e$ erzeugt, welche nur im Fall $p \nmid m_i$ auftreten. Alle restlichen Faktoren sind von $\mathfrak{p}$ invariante Gruppenkonstanten. □

Folgende Überlegungen erweist bei der Berechnung von $\Phi(F_\mathfrak{p}, G; s)$ als hilfreich.

Bemerkung 2.19. — *Es seien $\boldsymbol{G}$ eine Auflösung gemäß Definition 2.3 und $\mathcal{I}$ eine zulässige Familie mit Komponenten ausschließlich der Gestalt $\mathcal{J}_i = \mathcal{J}_{i,i-1}^l$. Dann ist $b(\boldsymbol{G},\mathcal{I}) \neq 0$.*

Beweis. — Auf Grund von $p \cdot m_{i-1} < m_i$ ist eine zu G_{i-1} isomorphe Gruppe $V \leq X^*_{m_i-1}$ nach Bemerkung 2.13 vollständig in $p \cdot X^*_{m_i-1}$ enthalten. Folglich ist jedes Element in V durch p teilbar und es kann eine gewünschte zu G_i isomorphe elementarabelsche Erweiterung von V gefunden werden. □

Bemerkung 2.20. — *Es seien $\boldsymbol{G}$ eine Auflösung gemäß Definition 2.3 und $\mathcal{I}$ eine zulässige Familie mit i-ter Komponente $\mathcal{J}_i \in \{\mathcal{J}^{l(\boldsymbol{G})}_{i,j}, \mathcal{K}^{l(\boldsymbol{G})}_{i,j}\}$. Für die zu $\boldsymbol{G}, \mathcal{I}$ gehörende Konstante gelte $b(\boldsymbol{G}, \mathcal{I}) \neq 0$. Dann ist G_i/G_j elementarabelsch.*

Beweis. — Es seien $\boldsymbol{m} \in \mathcal{I}$ und $U = \mathcal{N}_{E/F_\mathfrak{p}} E^\times$ die Normgruppe eines Urbildes $E/F_\mathfrak{p}$ von $(\boldsymbol{G}, \boldsymbol{m}) \in \mathcal{G}_G$ unter †. Für die dualen Gruppen gilt dann

$$W_i = U^\perp \cap X^*_{m_i} \simeq G_i \qquad \text{und} \qquad W_j = U^\perp \cap X^*_{m_j} \simeq G_j$$

und es ist $p \cdot W_i \leq W_j$ zu zeigen. Auf Grund der Vorgabe der i-ten Komponente $\mathcal{J}_i$ gilt $p \cdot m_j \leq m_i$. Wie im Beweis zu Bemerkung 2.13 folgt $p \cdot X^*_{m_i} \leq X_{m_j}$ und es ergibt sich wie gewünscht

$$p \cdot W_i = p \cdot \left(U^\perp \cap X^*_{m_i}\right) \leq U^\perp \cap X^*_{m_j} = W_j.$$

Das zeigt, dass W_i/W_j und somit auch G_i/G_j den Exponenten p besitzen. □

Mit den folgenden drei Beispielen soll der Leser dieser Arbeit etwas Übung mit den eingeführten Konstanten erfahren. Außerdem wird einer alternativen Fragestellung nachgegangen.

Beispiel 2.21. — Es sei $G = Z_{p^n}$ eine zyklische Gruppe der Ordnung p^n. Die möglichen Auflösungen von G mit elementarabelschen Faktoren gemäß Definition 2.3 sind genau

$$\boldsymbol{G} = (1, 1, G_1, \ldots, G_n) \qquad \text{und} \qquad \boldsymbol{H} = (H_0, H_0, H_1, \ldots, H_{n-1})$$

mit $G_i = Z_{p^i}$ und $H_i = Z_{p^{i+1}}$ von der Länge $l \in \{n, n-1\}$. Als zulässige Familien $\mathcal{I}$ mit $b(\boldsymbol{G}, \mathcal{I}) \neq 0$ bzw. $b(\boldsymbol{H}, \mathcal{I}) \neq 0$ kommen nur solche mit

$$\mathcal{I} = \mathcal{J}_1 \cap \ldots \cap \mathcal{J}_l \qquad \text{und} \qquad \mathcal{J}_i \in \{\mathcal{J}^l_{i,i-1}, \mathcal{K}^l_{i,i-1}\}$$

in Frage. Dies möchte ich im Folgenden demonstrieren. Dabei reicht es zu zeigen, dass die Sprungstellen m_i einer beliebigen G-Erweiterung $E/F_\mathfrak{p}$ die Ungleichung $m_i \geq p \cdot m_{i-1}$ für $1 \leq i \leq l$ erfüllen. Es seien also $E/F_\mathfrak{p}$ eine Erweiterung mit Galoisgruppe G und Führerexponenten $m+1$ sowie $U_i^\perp \leq X^*_m$ die dualen Gruppen zu den Normgruppen $U_i = \langle \mathcal{N}_{E/F_\mathfrak{p}} E^\times, 1 + \mathfrak{p}^{m_i+1} \rangle$ an den Sprungstellen. Für einen Charakter χ aus $U_i^\perp$ verschwindet $p \cdot \chi$ auf $\langle 1 + \mathfrak{p}^{n+1} \rangle$ mit $n = \lfloor m_i/p \rfloor$ und somit hat χ^p den Erklärungsmodul $\mathfrak{p}^{n+1}$. Des Weiteren ist $p \cdot \chi$ in $U_{i-1}^\perp$ enthalten und umgekehrt gilt $U_{i-1}^\perp = (U_i^\perp)^p$, da $U_i^\perp$ als zu G_i bzw. zu H_i isomorphe Gruppe zyklisch ist. Also hat auch $U_{i-1}^\perp$ den Erklärungsmodul $\mathfrak{p}^{n+1}$ und für den Führerexponenten $m_{i-1} + 1$ gilt $m_{i-1} \leq n$. Das zeigt wie behauptet $m_i \geq p \cdot m_{i-1}$. Da der Koeffizient m_1 eines eines Tupels $\boldsymbol{m}$ in einer zulässigen Menge stets zu p teilerfremd frei wählbar ist, gilt $\mathcal{J}_1 = \mathcal{J}^l_{1,0}$ und es gibt genau 2^{l-1} zulässige Mengen $\mathcal{I}$ mit $b(\boldsymbol{G}, \mathcal{I}) \neq 0$ bzw. $b(\boldsymbol{H}, \mathcal{I}) \neq 0$.

Nun ermittle ich die Form dieser $b(\boldsymbol{G},\mathcal{I})$ nach Satz 2.15. Es sei $G_{i-1} \simeq V \leq X^*_{m_i-1}$ eine Untergruppe mit den Sprungstellen $m_1,\dots,m_{i-1}$. Es ist $s_\nu = \delta_{i,\nu}$ das Kroneckersymbol für $1 \leq \nu \leq n$ und es gelten

$$d_1 = (\mathbb{F}_\mathfrak{p} : \mathbb{F}_p) \cdot \left(m_i - 1 - \left\lfloor \frac{m_i - 1}{p} \right\rfloor \right) + \delta_{1,i} \qquad \text{und} \qquad d_\nu = \delta_{\nu,i}$$

für $2 \leq \nu \leq l = n$. Das Kroneckersymbol für d_1 entspringt auf Grund $G_0 = 1$ und jenes für d_ν kommt auf Grund $p \cdot V[p^\nu] \leq V[p^{i-1}]$ zur Erscheinung. Somit gilt im Fall $\mathcal{J}_i = \mathcal{J}^n_{i,i-1}$ nach Satz 2.15 (a)

$$\begin{aligned} c(V,G_i) &= \mathcal{N}\mathfrak{p}^{m_i-1-\lfloor\frac{m_i-1}{p}\rfloor} \cdot \begin{bmatrix} [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \\ 1 \end{bmatrix}_p \cdot \prod_{\nu=2}^{l} \prod_{j=2}^{\nu-1} \prod_{k=0}^{s_\nu-1} p^{s_\nu \cdot d_j} \cdot (p^{d_\nu} - 1) \\ &= \mathcal{N}\mathfrak{p}^{m_i-1-\lfloor\frac{m_i-1}{p}\rfloor} \cdot \begin{bmatrix} [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \\ 1 \end{bmatrix}_p \cdot (p-1)^{1-\delta_{1,i}}. \end{aligned}$$

Im Fall $\mathcal{J}_i = \mathcal{K}^l_{i,i-1}$ ist $d^\circ_i = 1$ sowie $i \neq 1$ und es gilt nach (b)

$$c(V,G_i) = \mathcal{N}\mathfrak{p}^{m_i-1-\lfloor\frac{m_i-1}{p}\rfloor} \cdot \left(\prod_{j=2}^{i-1} p^{d_j} \right) \cdot \begin{bmatrix} 1 \\ 1 \end{bmatrix}_p \cdot p^{d_i} = \mathcal{N}\mathfrak{p}^{m_i-1-\lfloor\frac{m_i-1}{p}\rfloor}.$$

Ist $r(\mathcal{I}) \geq 1$ die Summe aller Indizes $1 \leq i \leq l$ mit $\mathcal{J}_i = \mathcal{J}^l_{i,i-1}$, so gilt zusammengefasst

$$b(\boldsymbol{G},\mathcal{I}) = p \cdot \prod_{\mathcal{J}_i = \mathcal{J}^l_{i,i-1}} \begin{bmatrix} [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \\ 1 \end{bmatrix}_p \cdot (p-1)^{1-\delta_{1,i}} = \frac{p}{p-1} \cdot (Np-1)^{r(\mathcal{I})}.$$

Folglich hat die von $\boldsymbol{G}$ erzeugte Teilreihe von $\Phi(F_\mathfrak{p}, G; s)$ nach den Korollaren 2.8 und 2.10 die Gestalt

$$\sum_{b(\boldsymbol{G},\mathcal{I})\neq 0} \Phi(F_\mathfrak{p}, \boldsymbol{G}, \mathcal{I}; s) = \sum_{b(\boldsymbol{G},\mathcal{I})\neq 0} \frac{p}{p-1} \cdot (Np-1)^{r(\mathcal{I})} \cdot \sum_{\boldsymbol{m}\in\mathcal{I}} \prod_{i=1}^{n} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}. \tag{2.21.1}$$

Die von $\boldsymbol{H}$ erzeugte Teilreihe berechnet sich analog. Hier ist $H_i \simeq G_{i+1}$ und die Substitution von $l = n$ mit $l = n-1$ zu beachten. Das heißt, es gelten $s_\nu = \delta_{\nu,i+1}$ für $1 \leq \nu \leq l = n-1$ sowie $d_\nu = \delta_{\nu,i+1}$ für $2 \leq \nu \leq l = n-1$. Die Zahl d_1 hat die gleiche Gestalt abzüglich $\delta_{1,i}$. Zusammengefasst gilt also

$$b(\boldsymbol{H},\mathcal{I}) = (Np-1)^{r(\mathcal{I})}$$

und $\Phi(F_\mathfrak{p}, G; s)$ hat die Form

$$\sum_{b(\boldsymbol{G},\mathcal{I})\neq 0} \frac{p}{p-1} \cdot (Np-1)^{r(\mathcal{I})} \cdot \sum_{\boldsymbol{m}\in\mathcal{I}} \prod_{i=1}^{n} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)} + \sum_{b(\boldsymbol{H},\mathcal{I})\neq 0} (Np-1)^{r(\mathcal{I})} \cdot \sum_{\boldsymbol{m}\in\mathcal{I}} \prod_{i=1}^{n-1} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}.$$

Der Analyse der Reihen über $\boldsymbol{m} \in \mathcal{I}$ wird mit den Methoden aus dem nächsten Abschnitt ermöglicht.

Beispiel 2.22. — Im Abschnitt 3.4 ist für eine zyklische p-Gruppe G die lokale Reihe

$$\Phi(\mathcal{O}^\times_\mathfrak{p}, G; s) = \sum_{\mathcal{O}^\times_\mathfrak{p}/U \simeq G} \mathcal{N}\mathfrak{d}(U)^{-s}$$

der G-Erweiterungen $E/F_\mathfrak{p}$ mit Normgruppenvorgabe $U = \mathcal{N}_{E/F_\mathfrak{p}} E^\times \leq \mathcal{O}_\mathfrak{p}^\times$ zu berechnen. Dies ist nur eine leichte Variation der in diesem Kapitel untersuchten Aufgabenstellung, daher ist hier ein geeigneter Platz für ihre Abhandlung gefunden. Auf Grund von

$$F_\mathfrak{p}^\times = \mathbf{Z} \times \mathcal{O}_\mathfrak{p}^\times = \mathbf{Z} \times \mathbb{F}_\mathfrak{p}^\times \times \langle 1 + \mathfrak{p} \rangle$$

entsprechen die Untergruppen $U \leq \mathcal{O}_\mathfrak{p}^\times$ mit Faktorgruppe G genau jenen in der Einseinheitengruppe. Diese lassen sich auch mit den gleichen Methoden berechnen. Statt $X_m = F_\mathfrak{p}^\times / \langle p^e \mathbf{Z} \times \mathbb{F}_\mathfrak{p}^\times \times \langle 1 + \mathfrak{p}^{m+1} \rangle \rangle$ wähle ich hierfür $X_m = \langle 1+\mathfrak{p} \rangle / \langle 1+\mathfrak{p}^{m+1} \rangle$. Diese Gruppen besitzen einen um genau 1 reduzierten p-Rang, was sich im Lemma 2.12 mit

$$d_1 = [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \cdot \left(m - 1 - \left\lfloor \frac{m-1}{p} \right\rfloor \right) - \dim H[p]$$

auswirkt. Alle anderen Konstanten haben die gleiche Gestalt wie in Satz 2.15 angegeben. Die Reihe $\Phi(F_\mathfrak{p}, G; s)$ hat also die selbe Zerlegung

$$\Phi(\mathcal{O}_\mathfrak{p}^\times, G; s) = \sum_{\mathcal{I}} b'(\boldsymbol{G}, \mathcal{I}) \cdot \sum_{\boldsymbol{m} \in \mathcal{I}} \prod_{i=1}^{n} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}$$

wie die Reihe `2.21.1` aus obigen Beispiel mit den variierten Konstanten

$$b'(\boldsymbol{G}, \mathcal{I}) = \frac{b(\boldsymbol{G}, \mathcal{I})}{p} = \frac{(\mathcal{N}\mathfrak{p} - 1)^{r(\mathcal{I})}}{p - 1}.$$

Insbesondere besteht die Reihe für $G = Z_p$ lediglich aus dem zu $\mathcal{I} = \mathcal{J}_{1,0}^1$ gehörenden Summanden und es gilt

$$\Phi(\mathcal{O}_\mathfrak{p}^\times, Z_p; s) = \frac{\mathcal{N}\mathfrak{p} - 1}{p - 1} \cdot \sum_{\boldsymbol{m} \in \mathcal{I}} \mathcal{N}\mathfrak{p}^{\alpha_1(m_1;s)} = \frac{\mathcal{N}\mathfrak{p} - 1}{p - 1} \cdot \sum_{p \nmid m} \mathcal{N}\mathfrak{p}^{m-1-\lfloor \frac{m-1}{p} \rfloor - (m+1)\cdot(p-1)\cdot s}.$$

Beispiel 2.23. — Es sei $G = G[p]$ eine elementarabelsche Gruppe der Ordnung p^r. Dann entsprechen die Auflösungen $\boldsymbol{G}$ von G den geordneten Partionen $(r_1, \ldots, r_l)$ von r oder $r-1$, je nachdem ob eine unverzweigte Teilerweiterung (in Form von $G_{-1} = G_0 = Z_p$) erwünscht ist oder nicht. Eine Einschränkung hierbei ist der Restklassengrad $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$, d.h. es gilt $r_i \leq [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$ für $1 \leq i \leq l$. Die zulässigen Familien $\mathcal{I}$ mit $b(\boldsymbol{G}, \mathcal{I}) \neq 0$ werden ausschließlich von $\mathcal{J}_{i,j}^l$ mit $1 \leq i \leq l$ und $1 \leq j < i$ erzeugt. Übersichtlich ist immerhin die Berechnung der $b(\boldsymbol{G}, \mathcal{I})$, da nur der Fall (a) aus Satz 2.15 zum Tragen kommt und es gilt

$$c(V, G_i) = \mathcal{N}\mathfrak{p}^{r_i \cdot (m_i - 1 - \lfloor \frac{m_i}{p} \rfloor)} \cdot \begin{bmatrix} [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \\ r_i \end{bmatrix}_p \cdot (G_{i-1} : Z_p)^{-r_i}.$$

Auch hier ist die Notwendigkeit von $r_i \leq [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$ erkennbar. Insgesamt gilt also

$$b(\boldsymbol{G}, \mathcal{I}) = \begin{cases} (G : 1) \cdot \prod_{i=1}^{l} \begin{bmatrix} [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \\ r_i \end{bmatrix}_p \cdot p^{-r_i \cdot \bar{r}_{i-1}} & G_{-1} = 1 \\ (G : Z_p) \cdot \prod_{i=1}^{l} \begin{bmatrix} [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \\ r_i \end{bmatrix}_p \cdot p^{-r_i \cdot \bar{r}_{i-1}} & G_{-1} = Z_p \end{cases}$$

mit $\bar{r}_j = r_1 + \ldots + r_j$ und $\bar{r}_0 = \dim G_{-1}$.

2.2. Analyse der Dirichletreihe $\Phi(F_\mathfrak{p}, G; s)$

Nun habe ich alle Werkzeuge für die analytische Zählung zur Verfügung und widme ich mich gänzlich der Dirichletreihe

$$\Phi(F_\mathfrak{p}, G; s) = \sum_{\mathrm{Gal}(E/F_\mathfrak{p}) \simeq G} \mathcal{N}\mathfrak{d}(E/F)^{-s} = \sum_{F_\mathfrak{p}^\times / U \simeq G} \mathcal{N}\mathfrak{d}(U)^{-s}.$$

Ich nenne eine Dirichletreihe $\Psi(s)$ einen direkten Summanden der Dirichletreihe $\Phi(s)$, wenn $\Phi(s) - \Psi(s)$ keine negativen Koeffizienten besitzt. Da $\Phi(F_\mathfrak{p}, G; s)$ ausschließlich nichtnegative Koeffizienten hat, ergibt sich ihre Konvergenzabszisse aus der maximalen Abszisse sämtlicher direkter Summanden, da Pole direkter Summanden nicht ausgelöscht werden können. Mit dem in Bemerkung 2.25 beschriebenen direkten Summanden in Gestalt einer geometrischen Reihe erhalte ich bereits eine scharfe untere Schranke für die Abszisse von $\Phi(F_\mathfrak{p}, G; s)$ sowie der Asymptotik von G-Erweiterungen. Dazu betrachte ich folgende Maximalauflösung.

Definition 2.24. — Es sei G eine abelsche p-Gruppe vom Exponenten p^e und den p^i-Rängen $g_i = \dim G[p^i]/G[p^{i-1}]$. Dann hat G die Elementarteilerzerlegung

$$G = Z_{p^e}^{g_e} \times Z_{p^{e-1}}^{g_{e-1}-g_e} \times \ldots \times Z_{p^{e-j}}^{g_{e-j}-g_{e-j+1}} \times \ldots \times Z_{p^2}^{g_2-g_3} \times Z_p^{g_1-g_2}.$$

Die Auflösung $\boldsymbol{G} = (1, 1, G_1, \ldots, G_e)$ von G mit den Komponenten

$$G_i = Z_{p^i}^{g_e} \times Z_{p^{i-1}}^{g_{e-1}-g_e} \times \ldots \times Z_{p^{i-j}}^{g_{e-j}-g_{e-j+1}} \times \ldots \times Z_{p^2}^{g_{e-i+2}-g_{e-i+3}} \times Z_p^{g_{e-i+1}-g_{e-i+2}}$$

nenne ich Maximalauflösung mit elementarabelschen Faktoren. Dabei sei G_{i-1} in G_i vermöge der Abbildung

$$G_{i-1} \hookrightarrow G_i,\ (\sigma_{i-1}, \ldots, \sigma_1) \mapsto (\sigma_{i-1}^p, \ldots, \sigma_1^p, 1)$$

eingebettet. Die Faktoren G_i/G_{i-1} sind vom p-Rang $r_i = \dim G_i/G_{i-1} = g_{e-i+1}$. Insbesondere ist G_e/G_{e-1} vom Rang g_1 und es ist hier zu beachten, dass die Maximalauflösung nur im Fall $g_1 \geq [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$ eine Auflösung von G im Sinne der Definition 2.3 ist. Des Weiteren definiere ich an dieser Stelle

$$a_\mathfrak{p}(G) = \frac{(p-1) \cdot \sum_{i=0}^{e-1} p^i \cdot g_{e-i}}{p \cdot \sum_{i=0}^{e-1} p^i \cdot (1 - p^{-g_{e-i}}) \cdot p^{g_e + \ldots + g_{e-i}}}.$$

Mit $r_i = \dim G_i/G_{i-1} = g_{e-i+1}$ und $t_i = (G_i : 1) - (G_{i-1} : 1) = (p^{r_i} - 1) \cdot p^{r_1 + \ldots + r_{i-1}}$ ist hierbei

$$a_\mathfrak{p}(G) = \frac{(p-1) \cdot \sum_{i=1}^{e} p^i \cdot r_i}{p \cdot \sum_{i=1}^{e} p^i \cdot t_i} = \frac{(p-1) \cdot \sum_{i=1}^{e} p^i \cdot r_i}{p \cdot \sum_{i=1}^{e} p^i \cdot (p^{r_i} - 1) \cdot p^{r_1 + \ldots + r_{i-1}}}$$

Bemerkung 2.25. — *Es sei G eine abelsche p-Gruppe. Dann gilt für die lokale Verteilung $Z(F_\mathfrak{p}, G; x)$ der asymptotische Vergleich*

$$Z(F_\mathfrak{p}, G; x) \in \Omega\left(x^{a_\mathfrak{p}(G)}\right).$$

Beweis. — Für diese Abschätzung werde ich nur einen Teil der Erweiterungen $E/F_\mathfrak{p}$ mit Gruppe G zählen. Dazu konstruiere ich einen direkten Summanden von $\Phi(F_\mathfrak{p}, G; s)$, dessen Konvergenzabszisse die gewünschte untere Schranke liefert. Zunächst gebe ich einen Beweis für den Fall $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \geq g_1$ an und verallgemeinere im Anschluß für beliebige Restklassengrade. Es seien $\boldsymbol{G} = (1, 1, G_1, \ldots, G_e)$ die

Maximalauflösung aus Definition 2.24 und $\mathcal{I}$ die durch $\mathcal{I} = \mathcal{J}_1 \cap \ldots \cap \mathcal{J}_e$ mit $\mathcal{J}_i = \mathcal{J}_{i,i-1}^e$ gegebene zulässige Familie. Der vom Paar $(\boldsymbol{G}, \mathcal{I})$ erzeugte Summand $\Phi(F_\mathfrak{p}, \boldsymbol{G}, \mathcal{I}; s)$ von $\Phi(F_\mathfrak{p}, G; s)$ hat nach Korollar 2.10 die Gestalt

$$\Phi(F, \boldsymbol{G}, \mathcal{I}; s) = b(\boldsymbol{G}, \mathcal{I}) \cdot \sum_{\boldsymbol{m} \in \mathcal{I}} \prod_{i=1}^{e} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i; s)}$$

und nach Bemerkung 2.19 ist $b(\boldsymbol{G}, \mathcal{I}) \neq 0$. Aus dieser Reihe gewinne ich einen kritischen direkten Summanden

$$\Phi(s) = \sum_{\boldsymbol{m} \in \mathcal{J}} \prod_{i=1}^{e} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i; s)}$$

durch Einschränkung auf die im Folgenden beschriebene Teilfamilie

$$\mathcal{J} = \{\boldsymbol{m}_x : x \in \mathbf{Z},\ x \geq 0\} \subset \mathcal{I}.$$

Für eine ganze Zahl $x \geq 0$ sei dabei $\boldsymbol{m}_x = (-1, 0, m_1, \ldots, m_e)$ mit

$$m_i = \begin{cases} p \cdot x + 1 & i = 1 \\ p \cdot m_{i-1} + 1 & 2 \leq i \leq e. \end{cases}$$

Durch sukzessives Einsetzen erhalte ich nur von i abhängige Konstanten $f_i = (p^{i-1} - 1)/(p-1)$, sodass

$$m_i = p^i \cdot x + p \cdot f_i + 1 \qquad \text{für} \qquad 1 \leq i \leq e$$

erfüllt ist. Für $\boldsymbol{m}_x \in \mathcal{J}$ erhalte ich insbesondere

$$\alpha_i(m_i; s) = r_i \cdot \left(m_i - 1 - \left\lfloor \frac{m_i - 1}{p} \right\rfloor \right) - (m_i + 1) \cdot t_i \cdot s = (x \cdot p^{i-1} + f_i) \cdot \beta_i(s) - 2 \cdot \delta_i(s)$$

mit

$$\beta_i(s) = r_i \cdot (p-1) - t_i \cdot p \cdot s \qquad \text{und} \qquad \delta_i(s) = t_i \cdot s.$$

Die von $\mathcal{J}$ erzeugte Teilreihe $\Phi(s)$ besitzt also statt e Summationsvariablen $m_1, \ldots, m_e$ nur noch eine und es gilt

$$\Phi(s) = \sum_{\boldsymbol{m} \in \mathcal{J}} \prod_{i=1}^{e} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i; s)} = \prod_{i=1}^{e} \mathcal{N}\mathfrak{p}^{f_i \cdot \beta_i(s) - 2 \cdot \delta_i(s)} \sum_{x \geq 0} \prod_{i=1}^{e} \mathcal{N}\mathfrak{p}^{x \cdot p^{i-1} \cdot \beta_i(s)}.$$

Diese Reihe ist offensichtlich rational auf die gesamte komplexe Ebene fortsetzbar durch

$$\Phi(s) = \left(1 - \mathcal{N}\mathfrak{p}^{\bar{\beta}_1(s)}\right)^{-1} \cdot \mathcal{N}\mathfrak{p}^{-2 \cdot ((G:1) - 1) \cdot s} \cdot \prod_{i=1}^{e} \mathcal{N}\mathfrak{p}^{f_i \cdot \beta_i(s)}$$

mit einzigem Pol in der Nullstelle $a_\mathfrak{p}(G)$ der linearen Funktion

$$\bar{\beta}_1(s) = \sum_{i=1}^{e} p^{i-1} \cdot \beta_i(s) = \sum_{i=1}^{e} (p-1) \cdot p^{i-1} \cdot r_i - p \cdot p^{i-1} \cdot t_i \cdot s. \tag{2.25.1}$$

Nach dem Taubersatz D.5 haben also die hier gezählten Erweiterungen die asymptotische Äquivalenzklasse $x^{a_\mathfrak{p}(G)}$ und somit ergibt sich die behauptete untere Abschätzung für den Fall $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \geq g_1$.

Für allgemeine Restklassengrade kann die Auflösung verfeinert werden, um ein analoges Resultat zu erhalten. Sofern nicht explizit geändert behalte ich obige Bezeichnungen bei und wähle irgendeine Verfeinerung $\boldsymbol{H}$ von $\boldsymbol{G}$ der Gestalt

$$1 = G_0 = H_0 \lhd H_1 \lhd \ldots \lhd H_{r_1} = G_1 \lhd \ldots \lhd H_{r_1+\ldots+r_i} = G_i \lhd \ldots \lhd H_l = G_e = G$$

mit einfachen Faktoren $H_i/H_{i-1} \simeq Z_p$. Die Summen $r_1 + \ldots + r_i$ bezeichne ich fortan mit $\bar{r}_i$ und setze $\bar{r}_0 = 0$. Insbesondere hat $\boldsymbol{H}$ die Länge $l(\boldsymbol{H}) = l = \bar{r}_e$. Als zulässige Familie wähle ich $\mathcal{I} = \mathcal{J}_1 \cap \ldots \cap \mathcal{J}_l$ mit $\mathcal{J}_i = \mathcal{J}^l_{i,\bar{r}_j}$ für $\bar{r}_j < i \leq \bar{r}_{j+1}$. Dann gilt $b(\boldsymbol{H}, \mathcal{I}) \neq 0$. Dies ist wie folgt einzusehen. Es seien $\bar{r}_j < i \leq \bar{r}_{j+1}$ und $G_j \simeq V \leq X^*_{m_{\bar{r}_j}}$. Dann ist V nach Bemerkung 2.13 in $X^*_{m_i}$ durch p teilbar, d.h. es gilt $V \leq p \cdot X^*_{m_i}$. Folglich gibt es mindestens eine Untergruppe $H_i \simeq U \leq X^*_{m_i}$ mit $U \cap X^*_{m_{\bar{r}_j}}$ und $H_k \simeq U \cap X^*_{m_k}$ und es folgt $b(\boldsymbol{H}, \mathcal{I}) \neq 0$ nach Bemerkung 2.18. Nach Korollar 2.10 ist dann

$$\Phi(F_\mathfrak{p}, \boldsymbol{H}, \mathcal{I}; s) = b(\boldsymbol{H}, \mathcal{I}) \cdot \sum_{\boldsymbol{m} \in \mathcal{I}} \prod_{i=1}^{l} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}$$

mit entsprechend angepassten Funktionen $\alpha_i(m_i; s)$. Die Teilfamilie $\mathcal{J} = \{\boldsymbol{m}_x : x \in \mathbf{Z},\ x \geq 0\} \subset \mathcal{I}$ gestalte ich hier mit Tupel $\boldsymbol{m}_x$ der Form

$$m_i = \begin{cases} p \cdot x + 1 & i = 1 \\ p \cdot m_{i-1} + 1 & i = \bar{r}_j + 1 \text{ und } 1 \leq j < e \\ m_{i-1} + p & \text{sonst.} \end{cases}$$

Auch hier gibt es nur von i abhängige Konstanten f_i, sodass m_i die Gestalt $m_i = p^{j+1} \cdot x + p \cdot f_i + 1$ für einen Index $0 \leq j < e$ mit $\bar{r}_j < i \leq \bar{r}_{j+1}$ aufweist. Insbesondere gilt

$$\begin{aligned} \sum_{i=\bar{r}_j+1}^{\bar{r}_{j+1}} \alpha_i(m_i; s) &= \sum_{i=\bar{r}_j+1}^{\bar{r}_{j+1}} m_i - 1 - \left\lfloor \frac{m_i - 1}{p} \right\rfloor - (m_i + 1) \cdot (p^i - p^{i-1}) \cdot s \\ &= x \cdot p^j \cdot \beta_{j+1}(s) - 2 \cdot \delta_{j+1}(s) + \sum_{i=\bar{r}_j+1}^{\bar{r}_{j+1}} f_i \cdot ((p-1) - p \cdot (p^i - p^{i-1}) \cdot s) \end{aligned}$$

und es gibt eine lineare von x unabhängige Funktion $f(s)$ mit

$$\sum_{i=1}^{l} \alpha_i(m_i; s) = x \cdot \sum_{j=0}^{e-1} p^j \cdot \beta_{j+1}(s) + f(s) = x \cdot \bar{\beta}_1(s) + f(s).$$

Der von $\mathcal{J}$ erzeugte direkte Summand

$$\Phi(s) = \sum_{\boldsymbol{m} \in \mathcal{J}} \prod_{i=1}^{l} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}$$

von der Reihe $\Phi(F_\mathfrak{p}, \boldsymbol{H}, \mathcal{I}; s)$ ist also im Wesentlichen eine geometrische Reihe mit gleichem Pol wie die oben berechnete Reihe und folglich kann die Behauptung für beliebige Restklassengrade analog geschlossen werden. □

Nachdem nun $a_{\mathfrak{p}}(G)$ als untere Schranke für die Abszisse von $\Phi(F_{\mathfrak{p}}, G; s)$ etabliert ist, widme ich mich nun dem Nachweis, dass diese Schranke auch tatsächlich scharf ist. Zudem muss die Frage nach der meromorphen Fortsetzbarkeit über die Konvergenzlinie hinaus beantwortet werden. Nach den Korollaren 2.8 und 2.10 ist die Reihe der G-Erweiterungen direkt zerlegbar in

$$\Phi(F_{\mathfrak{p}}, G; s) = \sum_{\boldsymbol{G}} \sum_{\mathcal{I}} \Phi(F_{\mathfrak{p}}, \boldsymbol{G}, \mathcal{I}; s).$$

Da es nur endlich viele direkten Summanden $\Phi(F_{\mathfrak{p}}, \boldsymbol{G}, \mathcal{I}; s)$ gibt, reicht es aus, $a_{\mathfrak{p}}(G)$ als obere Schranke dieser Reihen zu realisieren. Das Interesse ist also gänzlich auf die Dirichletreihen

$$\Phi(s) = \frac{\Phi(F_{\mathfrak{p}}, \boldsymbol{G}, \mathcal{I}; s)}{b(\boldsymbol{G}, \mathcal{I})} = \sum_{\boldsymbol{m} \in \mathcal{I}} \prod_{i=1}^{l(\mathcal{G})} \mathcal{N}\mathfrak{p}^{r_i \cdot (m_i - 1 - \lfloor \frac{m_i - 1}{p} \rfloor) - t_i \cdot (m_i + 1) \cdot s} \tag{2.2.1}$$

mit $b(\boldsymbol{G}, \mathcal{I}) \neq 0$ gerichtet. Das nun folgende Lemma liefert eine sukzessive Zerlegung nach geometrischen Reihen und legt die Rationalität von $\Phi(F_{\mathfrak{p}}, G; s)$ offen.

Lemma 2.26. — *Es seien $\alpha_i(m; s), \beta_i(s), \gamma_i(s), \delta_i(s)$ in s lineare und fallende Funktionen mit*

$$\alpha_i(m; s) = \begin{cases} x \cdot \beta_i(s) + y \cdot \gamma_i(s) - 2 \cdot \delta_i(s) & m = xp + y + 1,\ 0 \leq y \leq p - 2 \\ x \cdot \beta_i(s) - \delta_i(s) & m = xp. \end{cases}$$

Des Weiteren sei $\Phi(s)$ eine Dirichletreihe der Form

$$\Phi(s) = \sum_{\boldsymbol{m} \in \mathcal{I}} \prod_{i=1}^{l} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i; s)}$$

mit einer zulässigen Familie $\mathcal{I} = \mathcal{J}_1 \cap \ldots \cap \mathcal{J}_l$ und $f_i(s), g_i(s)$ in $\mathcal{N}\mathfrak{p}^{-s}$ polynomiale Ausdrücke mit

$$f_i(s) = \sum_{y=0}^{p-2} \mathcal{N}\mathfrak{p}^{y \cdot \gamma_i(s)} \qquad \text{und} \qquad g_i(s) = \mathcal{N}\mathfrak{p}^{-\delta_i(s)}.$$

Dann gelten folgende Aussagen.

(a) *Sind $\mathcal{J}_l = \mathcal{J}^l_{l,j}$ und $\mathcal{J}_{l-1} \neq \mathcal{J}^l_{l-1,j}$ für ein $0 \leq j < i$, so hat $\Phi(s)$ die Gestalt*

$$\Phi(s) = f_l(s) \cdot g_l(s)^2 \cdot \left(1 - \mathcal{N}\mathfrak{p}^{\beta_l(s)}\right)^{-1} \cdot \sum_{\boldsymbol{m} \in \mathcal{I}^{l-1}} \left(\mathcal{N}\mathfrak{p}^{m_j \cdot \beta_l(s)} - \mathcal{N}\mathfrak{p}^{m_{j+1} \cdot \beta_l(s)}\right) \cdot \prod_{i=1}^{l-1} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i; s)}.$$

Im Fall $j + 1 < l$ ist die hier auftretende Singularität bei der Nullstelle von $\beta_l(s)$ hebbar.

(b) *Gilt im Fall (a) die Bedingung $j + 1 = l$, so folgt*

$$\Phi(s) = f_l(s) \cdot g_l(s)^2 \cdot \left(1 - \mathcal{N}\mathfrak{p}^{\beta_l(s)}\right)^{-1} \cdot \sum_{\boldsymbol{m} \in \mathcal{I}^{l-1}} \mathcal{N}\mathfrak{p}^{m_j \cdot \beta_l(s)} \cdot \prod_{i=1}^{l-1} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i; s)}.$$

Diese Reihe besitzt in der Nullstelle von $\beta_l(s)$ einen Pol.

(c) *Ist $\mathcal{J}_l = \mathcal{K}^l_{l,j}$ für ein $0 \leq j < i$, so gilt $m_l = p \cdot m_j$ und $\Phi(s)$ hat die Gestalt*

$$\Phi(s) = g_l(s) \cdot \sum_{\boldsymbol{m} \in \mathcal{I}^{l-1}} \mathcal{N}\mathfrak{p}^{m_j \cdot \beta_l(s)} \cdot \prod_{i=1}^{l-1} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i; s)}.$$

(d) *Im Fall* $\mathcal{J}_l = \mathcal{J}_{l,j}^l$ *und* $\mathcal{J}_{l-1} = \mathcal{J}_{l-1,j}^l$ *für ein* $0 \leq j < i$ *ist die Reihe* $\Phi(s)$ *von der Gestalt*

$$\Phi(s) \;=\; g_l(s)^2 \cdot \sum_{\boldsymbol{m}\in\mathcal{I}^{l-1}} \sum_{y=y_{l-1}+1}^{p-2} \mathcal{N}\mathfrak{p}^{y\cdot\gamma_l(s)} \cdot \mathcal{N}\mathfrak{p}^{x_{l-1}\cdot\beta_l(s)} \cdot \prod_{i=1}^{l-1} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}$$

$$+\; f_l(s)\cdot g_l(s)^2 \cdot \left(1-\mathcal{N}\mathfrak{p}^{\beta_l(s)}\right)^{-1} \cdot \sum_{\boldsymbol{m}\in\mathcal{I}_{l-1}} \left(\mathcal{N}\mathfrak{p}^{(x_{l-1}+1)\cdot\beta_l(s)} - \mathcal{N}\mathfrak{p}^{m_{j+1}\cdot\beta_l(s)}\right) \cdot \prod_{i=1}^{l-1} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}$$

mit implizit durch $m_{l-1} = x_{l-1}p + y_{l-1} + 1$ *und* $0 \leq y_{l-1} \leq p-2$ *gegebenen Variablen* x_{l-1}, y_{l-1}. *Die hier auftretende Singularität in der Nullstelle von* $\beta_l(s)$ *ist hebbar.*

Beweis. — Für den Beweis dieses Lemmas ist lediglich der abspaltenden Faktor der Zerlegung

$$\Phi(s) = \sum_{\boldsymbol{m}\in\mathcal{I}} \prod_{i=1}^{l} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)} = \sum_{\boldsymbol{m}\in\mathcal{I}^{l-1}} \left(\prod_{i=1}^{l-1} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}\right) \cdot \sum_{(\boldsymbol{m},m)\in\mathcal{I}} \mathcal{N}\mathfrak{p}^{\alpha_l(m;s)}$$

auszurechnen. Für Teil (c) ist dies am einfachsten und es gilt

$$\sum_{(\boldsymbol{m},m)\in\mathcal{I}} \mathcal{N}\mathfrak{p}^{\alpha_l(m;s)} \;=\; \mathcal{N}\mathfrak{p}^{\alpha_l(p\cdot m_j;s)} \;=\; \mathcal{N}\mathfrak{p}^{m_j\cdot\beta_l(s)-\delta_l(s)} \;=\; g_l(s)\cdot\mathcal{N}\mathfrak{p}^{m_j\cdot\beta_l(s)}.$$

Die Teile (a) und (b) ergeben sich aus

$$\sum_{(\boldsymbol{m},m)\in\mathcal{I}} \mathcal{N}\mathfrak{p}^{\alpha_l(m;s)} \;=\; \sum_{x=m_j}^{\bar{v}-1} \sum_{y=0}^{p-2} \mathcal{N}\mathfrak{p}^{\alpha_l(xp+y+1;s)} \;=\; \sum_{y=0}^{p-2} \mathcal{N}\mathfrak{p}^{y\cdot\gamma_l(s)-2\cdot\delta_l(s)} \cdot \sum_{x=m_j}^{\bar{v}-1} \mathcal{N}\mathfrak{p}^{x\cdot\beta_l(s)}$$

$$=\; f_l(s)\cdot g_l(s)^2 \cdot \sum_{x=m_j}^{\bar{v}-1} \mathcal{N}\mathfrak{p}^{x\cdot\beta_l(s)} \;=\; f_l(s)\cdot g_l(s)^2 \cdot \left(\mathcal{N}\mathfrak{p}^{m_j\cdot\beta_l(s)} - \mathcal{N}\mathfrak{p}^{\bar{v}\cdot\beta_l(s)}\right) \cdot \left(1-\mathcal{N}\mathfrak{p}^{\beta_l(s)}\right)^{-1}$$

mit $\bar{v} = m_{j+1}$ oder $\bar{v} = \infty$, wobei der letzte Schritt für $\bar{v} = \infty$ in dieser Allgemeinheit zunächst einmal nicht ausführbar ist. Die Reihe $\sum_{x=0}^{\infty} \mathcal{N}\mathfrak{p}^{\beta_l(s)}$ besitzt allerdings die holomorphe Fortsetzung $\left(1-\mathcal{N}\mathfrak{p}^{\beta_l(s)}\right)^{-1}$ auf die ganze Ebene. Für Teil (d) wird die Zerlegung noch weiter verfeinert gemäß

$$\sum_{(\boldsymbol{m},m)\in\mathcal{I}} \mathcal{N}\mathfrak{p}^{\alpha_l(m;s)} \;=\; \sum_{m=m_{l-1}+1}^{p\cdot(x_{l-1}+1)} \mathcal{N}\mathfrak{p}^{\alpha_l(m;s)} + \sum_{x=x_{l-1}+1}^{m_{j+1}-1} \sum_{y=0}^{p-2} \mathcal{N}\mathfrak{p}^{\alpha_l(xp+y+1;s)}$$

sowie

$$\sum_{m=m_{l-1}+1}^{p\cdot(x_{l-1}+1)} \mathcal{N}\mathfrak{p}^{\alpha_l(m;s)} \;= \mathcal{N}\mathfrak{p}^{x_{l-1}\cdot\beta_l(s)-2\cdot\delta_l(s)} \cdot \sum_{y=y_{l-1}+1}^{p-2} \mathcal{N}\mathfrak{p}^{y\cdot\gamma_l(s)}$$

und entsprechend analog ausgerechnet. □

Im Folgenden nenne ich eine Funktion $\alpha_i(m;s)$ quasilinear in m, wenn sie von der Lemma 2.26 angegebenen Form ist. Sie ist stückweise linear und weist nur in $m \equiv 0 \pmod{p}$ eine Sprungstelle auf.

Korollar 2.27. — *Eine Dirichletreihe* $\Phi(s)$ *von der speziellen Form*

$$\Phi(s) = \sum_{\boldsymbol{m}\in\mathcal{I}} \prod_{i=1}^{l} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)}$$

mit in m *quasilinearen und in* s *linear fallenden Funktionen* $\alpha_i(m;s)$ *ist rational in* $\mathcal{N}\mathfrak{p}^{-s}$.

Beweis. — Diesen Beweis führe ich induktiv über l. Für $l = 1$ ist $\Phi(s)$ gemäß ihrer Zerlegung nach Lemma 2.26 offensichtlich rational. Für $l > 1$ ergeben sich nach Lemma 2.26 entsprechend des vorliegenden Falles die Aufteilungen

$$\Phi(s) = \begin{cases} f_l(s) \cdot g_l(s)^2 \cdot \left(1 - \mathcal{N}\mathfrak{p}^{\beta_l(s)}\right)^{-1} \cdot \Big(\Phi_1(s) - \Phi_2(s)\Big) & \text{Fall (a)} \\ f_l(s) \cdot g_l(s)^2 \cdot \left(1 - \mathcal{N}\mathfrak{p}^{\beta_l(s)}\right)^{-1} \cdot \Phi_1(s) & \text{Fall (b)} \\ g_l(s) \cdot \Phi_1(s) & \text{Fall (c)} \\ g_l(s)^2 \cdot \Psi(s) + f_l(s) \cdot g_l(s)^2 \cdot \left(1 - \mathcal{N}\mathfrak{p}^{\beta_l(s)}\right)^{-1} \cdot \Big(\Phi_3(s) - \Phi_2(s)\Big) & \text{Fall (d)} \end{cases}$$

mit Dirichletreihen $\Phi_k(s)$ von der Gestalt

$$\Phi_k(s) = \sum_{\boldsymbol{m} \in \mathcal{I}^{l-1}} \prod_{i=1}^{l-1} \mathcal{N}\mathfrak{p}^{\alpha_{i,k}(m_i;s)}$$

und den Exponentenfunktionen

$$\alpha_{i,k}(m;s) = \begin{cases} \alpha_i(m;s) & (i,k) \neq (j,1), (j+1,2), (l-1,3) \\ \alpha_j(m;s) + m \cdot \beta_l(s) & (i,k) = (j,1) \\ \alpha_{j+1}(m;s) + m \cdot \beta_l(s) & (i,k) = (j+1,2) \\ \alpha_{l-1}(m;s) + x \cdot \beta_l(s) & (i,k) = (l-1,3),\ m = xp + y + 2,\ 0 \leq y \leq p-1. \end{cases}$$

Auch diese Exponentenfunktionen sind quasilinear in m und linear fallend in s und hiermit ergibt sich die Rationalität von $\Phi(s)$ in den Fällen (a), (b) und (c) induktiv. Für den Fall (d) verbleibt nur noch der Nachweis der Rationalität von

$$\begin{aligned} \Psi(s) &= \sum_{\boldsymbol{m} \in \mathcal{I}^{l-1}} \sum_{y=y_{l-1}+1}^{p-2} \mathcal{N}\mathfrak{p}^{y \cdot \gamma_l(s)} \cdot \mathcal{N}\mathfrak{p}^{x_{l-1} \cdot \beta_l(s)} \cdot \prod_{i=1}^{l-1} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)} \\ &= \sum_{\boldsymbol{m} \in \mathcal{I}^{l-2}} \left(\prod_{i=1}^{l-2} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)} \right) \cdot \sum_{(\boldsymbol{m}, m_{l-1}) \in \mathcal{I}^{l-1}} \mathcal{N}\mathfrak{p}^{\alpha_{l-1,3}(m_{l-1};s)} \cdot \sum_{y=y_{l-1}+1}^{p-2} \mathcal{N}\mathfrak{p}^{y \cdot \gamma_l(s)} \end{aligned}$$

zu erbringen. Dazu definiere ich zunächst die rationale Funktion

$$h_{l-k}(s) = \sum_{y_k=0}^{p-2} \cdots \sum_{y_1=y_2+1}^{p-2} \sum_{y_0=y_1+1}^{p-2} \prod_{\nu=0}^{k} \mathcal{N}\mathfrak{p}^{y_\nu \cdot \gamma_{l-\nu}(s)}.$$

Erfüllt die $(l-2)$-te Komponente $\mathcal{J}_{l-2} \neq \mathcal{J}^l_{l-2,j}$, so folgt die Rationalität von $\Psi(s)$ aus der Identität

$$\begin{aligned} \Upsilon(\boldsymbol{m};s) &= \sum_{(\boldsymbol{m}, m_{l-1}) \in \mathcal{I}^{l-1}} \mathcal{N}\mathfrak{p}^{\alpha_{l-1,3}(m_{l-1};s)} \cdot \sum_{y=y_{l-1}+1}^{p-2} \mathcal{N}\mathfrak{p}^{y \cdot \gamma_l(s)} \\ &= g_{l-1}(s)^2 \cdot \sum_{x_{l-1}=m_j}^{m_{j+1}-1} \sum_{y_{l-1}=0}^{p-2} \mathcal{N}\mathfrak{p}^{x_{l-1} \cdot \tilde{\beta}_{l-1}(s)} \cdot \mathcal{N}\mathfrak{p}^{y_{l-1} \cdot \gamma_{l-1}(s)} \cdot \sum_{y=y_{l-1}+1}^{p-2} \mathcal{N}\mathfrak{p}^{y \cdot \gamma_l(s)} \\ &= g_{l-1}(s)^2 \cdot h_{l-1}(s) \cdot \left(1 - \mathcal{N}\mathfrak{p}^{\tilde{\beta}_{l-1}(s)}\right)^{-1} \cdot \left(\mathcal{N}\mathfrak{p}^{m_j \cdot \tilde{\beta}_{l-1}(s)} - \mathcal{N}\mathfrak{p}^{m_{j+1} \cdot \tilde{\beta}_{l-1}(s)}\right) \end{aligned}$$

mit $\tilde{\beta}_{l-1}(s) = \beta_{l-1}(s) + \beta_l(s)$, wobei die erste Gleichung lediglich eine Notationsetzung ist. Andernfalls gilt $\mathcal{J}_{l-2} = \mathcal{J}^l_{l-2,j}$ und es ist

$$\begin{aligned}(2.27.1) \qquad \Upsilon(\boldsymbol{m}; s) \;=\; & g_{l-1}(s)^2 \cdot \mathcal{N}\mathfrak{p}^{x_{l-2}\cdot\tilde{\beta}_{l-1}(s)} \cdot \sum_{y_{l-1}=y_{l-2}+1}^{p-2} \sum_{y_l=y_{l-1}+1}^{p-2} \prod_{\nu=0}^{1} \mathcal{N}\mathfrak{p}^{y_{l-\nu}\cdot\gamma_{l-\nu}(s)} \\ & + \; g_{l-1}(s)^2 \cdot h_{l-1}(s) \cdot \left(1 - \mathcal{N}\mathfrak{p}^{\tilde{\beta}_{l-1}(s)}\right)^{-1} \cdot \left(\mathcal{N}\mathfrak{p}^{(x_{l-2}+1)\cdot\tilde{\beta}_{l-1}(s)} - \mathcal{N}\mathfrak{p}^{m_{j+1}\cdot\tilde{\beta}_{l-1}(s)}\right)\end{aligned}$$

für $m_{l-2} = x_{l-2}p + y_{l-2} + 1$ mit $0 \leq y_{l-2} \leq p-2$. Durch sukzessiver Zerlegung dieser Art ergibt sich die Rationalität von $\Psi(s)$ auch allgemein im Fall (d). Ist k maximal mit $\mathcal{J}_{l-k} = \mathcal{J}^l_{l-k}$, so hat $\Psi(s)$ insbesondere einen direkten Summanden der Gestalt

$$\mathcal{N}\mathfrak{p}^{m_j\cdot\tilde{\beta}_{l-k}(s)} \cdot h_{l-k}(s) \cdot \prod_{\nu=1}^{k} g_{l-\nu}(s)^2 \qquad \text{mit} \qquad \tilde{\beta}_{l-k}(s) = \sum_{\nu=0}^{k} \beta_{l-k}(s).$$

Dieser entsteht sukzessive aus dem ersten Summanden gemäß der Zerlegung 2.27.1. □

Zur Bestimmung der Konvergenzabszisse von $\Phi(s)$ ist nun lediglich der höchste Pol zu ermitteln. Dazu ist bei der sukzessiven Anwendung von Lemma 2.26 die Neukonfiguration der β_i zu beobachten, da sich deren Nullstellen für die Pole verantwortlich zeichnen.Konkret spaltet sich $\Phi(s)$ nach Anwendung des Fall (a) in zwei Reihen baugleich zur Ursprungsreihe auf, bei der eine Reihe durch die Ersetzung

$$\tilde{\beta}_i(s) = \beta_i(s) \qquad \text{und} \qquad \tilde{\beta}_j(s) = \beta_j(s) + p \cdot \beta_l(s) \qquad \text{für} \qquad 1 \leq i \leq l-1, i \neq j$$

entsteht und die zweite Reihe entsprechend für den Index $j+1$ statt j gebildet wird. Genauso ergibt sich nach Anwendung der Fälle (b) und (c) die Neukonfiguration

$$\tilde{\beta}_i(s) = \beta_i(s) \qquad \text{und} \qquad \tilde{\beta}_{l-1}(s) = \beta_{l-1}(s) + p \cdot \beta_l(s) \qquad \text{für} \qquad 1 \leq i \leq l-2.$$

Im Fall (d) ergeben sich sogar drei neue Reihen mit analogen Ersetzungen. Ein interessanter Unterschied hierbei ist, dass bei zweien von diesen sogar die Ersetzung

$$\tilde{\beta}_{l-1}(s) = \beta_{l-1}(s) + \beta_l(s)$$

vorgenommen wird. Nach der letztmöglichen Zerlegung via Lemma 2.26 erhalte ich ich aus der Ursprungskonfiguration die Funktionen

$$(2.27.2) \qquad \bar{\beta}_i(s) = \beta_i(s) + p^{e_i(i+1)} \cdot \bar{\beta}_{i+1}(s) = \sum_{j=i}^{l} p^{e_i(j)} \cdot \beta_j(s),$$

wobei e_i ein angepasste Treppenfunktion mit $e_i(j) \in \{e_i(j-1), e_i(j-1)+1\}$ ist. Ist $\mathcal{I}$ beispielsweise von der Gestalt $\mathcal{I} = \mathcal{J}_1 \cap \ldots \mathcal{J}_l$ mit $\mathcal{J}_i \in \{\mathcal{J}^l_{i,i-1}, \mathcal{K}^l_{i,i-1}\}$, so kommen nur die Fälle (b) und (c) zum Tragen und diese Funktionen haben die Formel

$$\bar{\beta}_i(s) = \sum_{j=i}^{l} p^{j-i} \cdot \beta_j(s).$$

Im Folgenden untersuche ich, welche der Nullstellen dieser Funktionen $\bar{\beta}_i$ als Konvergenzabszisse zu $\Phi(s)$ in Frage kommen.

Lemma 2.28. — *Es seien a_0, a_1, b_0, b_1 positive reelle Zahlen und $\alpha(s) = a_0 - a_1 \cdot s$ und $\beta(s) = b_0 - b_1 \cdot s$ zwei lineare Funktionen mit Nullstellen a bzw. b und es gelte $a < b$. Dann besitzt ihre Summenfunktion $\gamma(s) = \alpha(s) + \beta(s)$ eine reelle Nullstelle c mit $a < c < b$.*

Beweis. — Die Annahme, c wäre zugleich größer (bzw. kleiner) als a und b führte zu $\alpha(c), \beta(c) < 0$ (bzw. $\alpha(c), \beta(c) > 0$) im Widerspruch zu $\gamma(c) = \alpha(c) + \beta(c) = 0$. □

Nun betrachte ich bzgl. der Reihe $\Phi(s)$ der konkreten Gestalt `2.2.1` die Funktionen

$$\alpha_i(m_i; s) = r_i \cdot \left(m_i - 1 - \left\lfloor \frac{m_i - 1}{p} \right\rfloor \right) - t_i \cdot (m_i + 1) \cdot s,$$

die sich wie in Lemma 2.26 als Quasilinearkombination der Funktionen

$$\beta_i(s) = r_i \cdot (p-1) - t_i \cdot p \cdot s, \qquad \gamma_i(s) = r_i - t_i \cdot s, \qquad \delta_i(s) = t_i \cdot s$$

schreiben lässt. Die Nullstellen a_i der $\beta_i(s)$ bilden eine absteigende Kette $a_1 > \ldots > a_{l(\boldsymbol{G})}$ von rationalen Zahlen und folglich bilden auch die Nullstellen der Funktionen $\bar{\beta}_i(s)$ eine echt absteigende Kette und die maximale Nullstelle unter den $\bar{\beta}_i(s)$ gehört genau zu $i = 1$. Erstere Aussage kann dabei mit der faktorweisen Ungleichung

$$r_i \cdot p^{r_i} \cdot (p^{r_{i+1}} - 1) \geq p^{r_i} \cdot (p^{r_{i+1}} - 1) > (p^{r_i} - 1) \cdot r_{i+1}$$

und der hieraus folgenden Abschätzung

$$a_i = \frac{(p-1) \cdot r_i}{p \cdot t_i} = \frac{(1 - p^{-1}) \cdot r_i}{(p^{r_i} - 1) \cdot (G_{i-1} : 1)} > \frac{(1 - p^{-1}) \cdot r_{i+1}}{(p^{r_{i+1}} - 1) \cdot p^{r_i} \cdot (G_{i-1} : 1)} = \frac{(p-1) \cdot r_{i+1}}{p \cdot t_{i+1}} = a_{i+1}$$

belegt werden und die zweite Aussage folgt aus obigem Lemma 2.28. Die Konvergenzabszisse der meromorphen Fortsetzung von $\Phi(s)$ ergibt sich also aus der Nullstelle von $\bar{\beta}_1(s)$. Der Formel `2.27.2` für diese Funktion zu Folge hat diese Nullstelle die Gestalt

$$\frac{(p-1) \cdot \sum_{i=1}^{l} p^{e_1(i)} \cdot r_i}{p \cdot \sum_{i=1}^{l} p^{e_1(i)} \cdot t_i} = \frac{(p-1) \cdot \sum_{k=0}^{\tilde{l}} p^k \cdot \tilde{r}_k}{p \cdot \sum_{k=0}^{\tilde{l}} p^k \cdot \tilde{t}_k}$$

mit $\tilde{r}_k = \sum_{e_1(i)=k} r_i$ und $\tilde{t}_k = \sum_{e_1(i)=k} t_i$. Die Zahlen $\tilde{r}_k$ und $\tilde{t}_k$ gehören zu einer gröberen Auflösung $\tilde{\boldsymbol{G}}$ mit elementarabelschen Faktoren vom Rang $\tilde{r}_k$. Der Exponent der Faktoren ergibt sich dabei aus dem notwendigen Kriterium 2.20, da das Interesse nur auf Reihen $\Phi(s) = \Phi(F_{\mathfrak{p}}, \boldsymbol{G}, \mathcal{I}; s)$ mit $b(\boldsymbol{G}, \mathcal{I}) \neq 0$ eingegrenzt ist. Die Brüche obiger Gestalt werden nun auf ihren Maximalwert untersucht.

Lemma 2.29. — *Es seien $\boldsymbol{r} = (r_1, \ldots, r_l)$ ein Tupel ganzer Zahlen mit $0 \leq r_i \leq [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_p]$ und*

$$a_{\mathfrak{p}}(\boldsymbol{r}) = \frac{(p-1) \cdot \sum_{i=1}^{l} p^i \cdot r_i}{p \cdot \sum_{i=1}^{l} p^i \cdot (p^{r_i} - 1) \cdot p^{r_1 + \ldots + r_{i-1}}}.$$

Dann gelten die folgende Aussagen.

(a) (Verkürzen) *Es sei k mit $r_k + r_{k+1} \leq [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$. Dann gilt*

$$a_\mathfrak{p}(\boldsymbol{s}) > a_\mathfrak{p}(\boldsymbol{r}) \qquad \textit{mit} \qquad s_i = \begin{cases} r_i & 1 \leq i \leq k-1 \\ r_k + r_{k+1} & i = k \\ r_{i+1} & k+1 \leq i \leq l \end{cases}$$

und der künstlichen Setzung $s_l = r_{l+1} = 0$.

(b) (Aufteilen) *Es sei k mit $\max_{1 \leq i \leq k}(r_i) = r_k$ und $2 \leq r_k \leq r_{k+1} < [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$. Dann gilt*

$$a_\mathfrak{p}(\boldsymbol{s}) > a_\mathfrak{p}(\boldsymbol{r}) \qquad \textit{mit} \qquad s_i = \begin{cases} r_i & i \neq k, k+1 \\ r_k - 1 & i = k \\ r_{k+1} + 1 & i = k+1. \end{cases}$$

(c) (Tauschen) *Es sei k minimal mit $r_k > r_{k+1}$. Dann gilt*

$$a_\mathfrak{p}(\boldsymbol{s}) > a_\mathfrak{p}(\boldsymbol{r}) \qquad \textit{mit} \qquad s_i = r_{\tau(i)}$$

für die Permutation $\tau = (k \ k+1)$ mit Ausnahme in den Fällen $\boldsymbol{r} = (1, \ldots, 1, 2, \ldots, 2, 1)$ oder $\boldsymbol{r} = (2, \ldots, 2, 1)$ bei $p = 2$.

(d) (Sortieren) *In den Ausnahmefällen aus (c) gilt*

$$a_\mathfrak{p}(\boldsymbol{s}) > a_\mathfrak{p}(\boldsymbol{r}) \qquad \textit{mit} \qquad s_i = r_{\sigma(i)}$$

für die Permutation $\sigma = (1 \ l)$.

Der Beweis dieses vom Rest dieses Kapitels unabhängigen Lemmas kann im Anhangskapitel F nachvollzogen werden. Hier nun folgt das Hauptresultat der Asymptotikuntersuchung lokaler Galoiserweiterungen mit abelscher p-Gruppe.

Satz 2.30. — *Für die Zählfunktion $Z(F_\mathfrak{p}, G; x)$ gilt der asymptotische Vergleich*

$$Z(F_\mathfrak{p}, G; x) \sim c(F_\mathfrak{p}, G) \cdot x^{a_\mathfrak{p}(G)}.$$

Beweis. — Nach Korollar 2.27 ist bereits bekannt, dass $\Phi(F_\mathfrak{p}, G; s)$ als endliche Summe von rationalen Funktionen ebenfalls rational ist. Eine untere Abschätzung der Konvergenzabszisse ist mit 2.25 durch $a_\mathfrak{p}(G)$ gegeben. Ich bleibe also noch den Nachweis schuldig, dass $a_\mathfrak{p}(G)$ auch eine obere Abschätzung der Abszisse ist. Sämtliche Kandidaten haben nach den Überlegungen zwischen Korollar 2.27 und Lemma 2.29 die Gestalt $a_\mathfrak{p}(\boldsymbol{r})$, wobei $a_\mathfrak{p}(\boldsymbol{r})$ die in Lemma 2.29 vorgestellte multivariate Funktion und $\boldsymbol{r} = (\dim G_i/G_{i-1})_{1 \leq i \leq l(\boldsymbol{G})}$ die Auflistung von den Rängen der Faktoren einer Auflösung von G mit elementarabelschen Faktoren (nicht notwendigerweise in $\mathbb{F}_\mathfrak{p}$ einbettbar) ist. Diese Abszisse bezeichne ich fortan mit $a_\mathfrak{p}(\boldsymbol{G})$. Nach wiederholter Anwendung von obigen Lemma 2.29 ist erkennbar, dass genau eine Auflösung die größte Abszisse liefert, nämlich jene mit revers lexikographisch größtem Erweiterungstupel $\boldsymbol{r}$. Anders ausgedrückt, für jene Auflösung $\boldsymbol{G}$, bei der startend von G mit jeweils maximal möglichen elementarabelschen Faktor aufgelöst wird. Dies ist die Maximalauflösung $\boldsymbol{G}$ aus Definition 2.24 und für

jene habe ich in Bemerkung 2.25 bereits $a_{\mathfrak{p}}(\boldsymbol{G}) = a_{\mathfrak{p}}(G)$ festgestellt. Folglich ist $\Phi(F_{\mathfrak{p}}, G; s)$ eine rationale Funktion mit Konvergenzabszisse $a_{\mathfrak{p}}(G)$. Das behauptete Resultat gewinne ich schließlich aus dem Taubersatz D.5 und seinem Korollar D.6. □

Beispiel 2.31. — Ich setze nun die Untersuchung der zyklischen p-Gruppen aus Bespiel 2.21 fort. Es sei $\prod'$ das Produkt über alle Indizes $1 \leq i \leq l$ mit $\mathcal{J}_i = \mathcal{J}_{i,i-1}^l$. Dann gilt nach Lemma 2.26

$$\sum_{\boldsymbol{m}\in\mathcal{I}} \prod_{i=1}^{l} \mathcal{N}\mathfrak{p}^{\alpha_i(m_i;s)} = \mathcal{N}\mathfrak{p}^{-(t_l-t_0)\cdot s} \cdot \prod{}' \left((1-\mathcal{N}\mathfrak{p}^{\bar{\beta}_i(s)})^{-1} \cdot \mathcal{N}\mathfrak{p}^{-t_i\cdot s+\bar{\beta}_{i+1}(s)} \cdot \sum_{y=0}^{p-2} \mathcal{N}\mathfrak{p}^{y\cdot\bar{\gamma}_i(s)} \right)$$

mit $t_j = p^j - p^{j-1}$ für die Auflösung $\boldsymbol{G}$ und $t_j = p^{j+1} - p^j$ für die Auflösung $\boldsymbol{H}$. Wiederum betrachte ich nur die zulässigen Familien $\mathcal{I} \subset \mathcal{N}^l$ mit nichtverschwindenden Konstante $b(\boldsymbol{G}, \mathcal{I})$ bzw. $b(\boldsymbol{H}, \mathcal{I})$. Diese erfüllen allesamt die Eigenschaft $m_i \geq p \cdot m_{i-1}$ für $1 \leq i \leq l$ und somit haben die Funktionen $\bar{\beta}_i(s)$ und $\bar{\gamma}_i(s)$ unabhängig von der Wahl der Familie $\mathcal{I}$ die Gestalt

$$\bar{\beta}_i(s) = \sum_{j=i}^{l} p^{j-i} \cdot \beta_i(s) = \sum_{j=i}^{l} p^{j-i} \cdot (r_j \cdot (p-1) - t_j \cdot p \cdot s) = \sum_{j=i}^{l} p^{j-i} \cdot ((p-1) - t_j \cdot p \cdot s)$$

sowie

$$\bar{\gamma}_i(s) = \gamma_i(s) + \bar{\beta}_{i+1}(s) = 1 - t_i \cdot s + \bar{\beta}_{i+1}(s).$$

Insgesamt lassen die Funktionen $\Phi(F_{\mathfrak{p}}, \boldsymbol{G}, \mathcal{I}; s)$ zerlegen in eine rationale Funktion der Gestalt

$$\Phi(F_{\mathfrak{p}}, \boldsymbol{G}, \mathcal{I}; s) = \frac{g(\boldsymbol{G}, \mathcal{I}; s)}{f(\boldsymbol{G}; s)}$$

mit den in $\mathcal{N}\mathfrak{p}^{-s}$ polynomialen Ausdrücken

$$f(\boldsymbol{G}; s) = \prod_{i=1}^{l} (1 - \mathcal{N}\mathfrak{p}^{\bar{\beta}_i(s)})$$

und

$$g(\boldsymbol{G}, \mathcal{I}; s) = b(\boldsymbol{G}, \mathcal{I}) \cdot \mathcal{N}\mathfrak{p}^{-(t_l-t_0)\cdot s} \cdot \prod{}' \left(\mathcal{N}\mathfrak{p}^{-t_i\cdot s+\bar{\beta}_{i+1}(s)} \cdot \sum_{y=0}^{p-2} \mathcal{N}\mathfrak{p}^{y\cdot\bar{\gamma}_i(s)} \right) \cdot \prod{}'' (1 - \mathcal{N}\mathfrak{p}^{\bar{\beta}_i(s)}).$$

Hierbei ist $\prod''$ das Komplementärprodukt zu $\prod'$ und läuft dementsprechend über alle Indizes $1 \leq i \leq l$ mit Elementarfamilie $\mathcal{J}_i = \mathcal{K}_{i,i-1}^l$. Diese Zerlegung ist selbstverständlich auch für $\Phi(F_{\mathfrak{p}}, \boldsymbol{H}, \mathcal{I}; s)$ möglich und hierfür ist in den vorliegenden Formeln lediglich $\boldsymbol{G}$ durch $\boldsymbol{H}$ zu ersetzen.

Beispiel 2.32. — Das entsprechende Ergebnis für die Reihe $\Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, G; s)$ aus Beispiel 2.22 sei hier für den späteren Zugriff etwas genauer untersucht. Es ist zunächst

$$\Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, G; s) = \sum_{b(\boldsymbol{G},\mathcal{I})\neq 0} \frac{\Phi(F_{\mathfrak{p}}, \boldsymbol{G}, \mathcal{I}; s)}{p} = f(\boldsymbol{G}; s)^{-1} \cdot \sum_{b(\boldsymbol{G},\mathcal{I})\neq 0} \frac{g(\boldsymbol{G}, \mathcal{I}; s)}{p}$$

festzuhalten. Im Einzelnen sind die Polynome von der Gestalt

$$f(\boldsymbol{G}; s) = \prod_{i=1}^{n} (1 - \mathcal{N}\mathfrak{p}^{\bar{\beta}_i(s)})$$

und

$$\frac{g(\boldsymbol{G},\mathcal{I};s)}{p} = \frac{(\mathcal{N}\mathfrak{p}-1)^{r(\mathcal{I})}}{p-1}\cdot\mathcal{N}\mathfrak{p}^{-(p^n-1)\cdot s}\cdot\prod{}'\left(\mathcal{N}\mathfrak{p}^{-p^{i-1}(p-1)\cdot s+\bar{\beta}_{i+1}(s)}\cdot\sum_{y=0}^{p-1}\mathcal{N}\mathfrak{p}^{y\cdot\bar{\gamma}_i(s)}\right)$$
$$\cdot\prod{}''(1-\mathcal{N}\mathfrak{p}^{\bar{\beta}_i(s)}).$$

Da die erste Elementarfamilie einer zulässigen Familie stets $\mathcal{J}_1 = \mathcal{J}_{1,0}^n$ ist, gilt insbesondere für $G = Z_p$ die Identität

$$\Phi(\mathcal{O}_\mathfrak{p}^\times, Z_p; s) = \frac{\mathcal{N}\mathfrak{p}-1}{p-1}\cdot\left(1-\mathcal{N}\mathfrak{p}^{(p-1)(1-p\cdot s)}\right)^{-1}\cdot\mathcal{N}\mathfrak{p}^{-2(p-1)\cdot s}\cdot\sum_{y=0}^{p-2}\mathcal{N}\mathfrak{p}^{y\cdot(1-(p-1)\cdot s)}.$$

2.3. Asymptotik globaler abelscher Funktionenkörper

In diesem Abschnitt werden die Auswirkungen der lokalen Erweiterungen auf die Verteilung der globalen Erweiterungen untersucht. Bei globalen Körpern der Klassenzahl 1 kann jede lokale Erweiterung auch global realisiert werden. Die beiden im Folgenden vorgestellten Schranken für $Z(F,G;x)$ erreiche ich, indem ich zum Einen nur in einer einzigen Stelle verzweigten Erweiterungen und zum Anderen nur elementarabelsche Erweiterungen mit quadratischem Führer zähle. Beide Schranken erweisen sich in verschiedenen Fällen als zweckmäßig.

Satz 2.33. — *Für die Asymptotik der abelschen p-Erweiterungen eines globalen Funktionenkörpers F der Charakteristik p und Klassenzahl 1 mit Galoisgruppe G gelten folgende Aussagen.*

(a) *Es sei $\mathfrak{p}$ eine beliebige Stelle in F. Dann gilt*

$$Z(F,G;x) \geq Z(F_\mathfrak{p},G;x) \in \Omega\left(x^{a_\mathfrak{p}(G)}\right)$$

und es ist $a_\mathfrak{p}(G) > a(G)$ für abelsche nichtzyklische p-Gruppen $G \neq Z_2^2, Z_3^2, Z_2^3$.

(b) *Es seien G eine elementarabelsche Gruppe vom Rang $r = \dim G[p]$ und*

$$a(F,G) = \frac{1+r}{2\cdot(p^r-1)} \geq \frac{1}{(G:Z_p)\cdot(p-1)} = a(G).$$

Dann gilt

$$Z(F,G;x) \in \Omega\left(x^{a(F,G)}\right)$$

und es ist $a(F,G) > a(G)$ für $G \neq Z_p, Z_2^2$.

Beweis. — Aus der klassenkörpertheoretischen exakten Sequenz

$$1 \to K^\times \to F^{\mathfrak{p}^m}/F_{\mathfrak{p}^m} \to \mathcal{C}\ell_{\mathfrak{p}^m} \to \mathcal{C}\ell \to 1$$

gewinne ich mit $\mathcal{C}\ell = \mathbf{Z}$ und $F^{\mathfrak{p}^m}/F_{\mathfrak{p}^m} = \mathcal{O}_\mathfrak{p}^\times/\langle 1+\mathfrak{p}^m\rangle$ die exakte Sequenz

$$1 \to K^\times \to \mathcal{O}_\mathfrak{p}^\times/\langle 1+\mathfrak{p}^m\rangle \to \mathcal{C}\ell_{\mathfrak{p}^m}/\mathbf{Z} \to 1.$$

Folglich ist die p-Sylowgruppe von $\mathcal{C}\ell_{\mathfrak{p}^m}$ isomorph zu jener von $\mathcal{O}_\mathfrak{p}^\times/\langle 1+\mathfrak{p}^m\rangle$, was die bijektive Beziehung zwischen lokalen G-Erweiterungen und globalen nur in $\mathfrak{p}$ verzweigten G-Erweiterungen belegt. Hieraus

folgt unmittelbar die Schranke für $Z(F,G;x)$ aus Teil (a). Die Abschätzung der a-Konstanten erfolgt elementar aus

$$\sum_{i=0}^{e-1} p^i \cdot \left(g_{e-i} \cdot (G:1) \cdot (1-p^{-1})^2 - p^{g_e+\ldots+g_{e-i}} \cdot (1-p^{-g_{e-i}})\right) > 0.$$

Nach einem Vergleich der p-Potenzen ist erkennbar, dass es einen Index k gibt, sodass der Ausdruck in der großen Klammer für $i \leq k$ positiv ist. Es reicht hier somit, den $(e-1)$-ten Ausdruck zu begutachten. Dieser ist genau dann positiv wenn

$$f(x) = x \cdot (1-p^{-1})^2 - (1-p^{-x})$$

positiv ist. Hier habe ich $x = g_1$ gesetzt. Diese Funktion ist monoton steigend, da ihre Ableitung $(1-p^{-1})^2 - \log(p) \cdot p^{-x}$ von für $x \geq 2$ nicht negativ ist. Außerdem gelten

$$f(2) = \frac{p^2 - 4 \cdot p + 3}{p^2},\ f(3) = \frac{2 \cdot p^3 - 6 \cdot p^2 + 3 \cdot p + 1}{p^3} \text{ und } f(4) = \frac{3 \cdot p^4 - 8 \cdot p^3 + 4 \cdot p^2 + 1}{p^4}.$$

Somit ist $f(x)$ für $p \geq 5$ oder $x \geq 4$ positiv. Die Ausnahmefälle sind $(p,x) = (2,2), (2,3)$ und $(3,2)$. Hierzu kann ein Blick ins Beispielmaterial am Ende des Abschnittes geworfen werden.

Aussage (b) bezieht sich nur auf elementarabelsche Gruppen $G = G[p]$. Dazu zähle ich lediglich die Erweiterungen mit quadratischem Führer $\mathfrak{m}^2$, deren Anzahl ich mit $a(G,\mathfrak{m}^2)$ bezeichne. Die Gruppenparameter bezeichne ich hier mit $r = g_1$ und $t = (G:1) - 1 = p^r - 1$. Damit ist $a(F,G) = (1+r)/2t$. Nach Satz 2.15 gibt es $\begin{bmatrix} [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \\ r \end{bmatrix}_p$ Erweiterungen von $F_\mathfrak{p}$ und folglich auch von F mit Gruppe G und Diskriminante $\mathfrak{p}^{2t}$. Zu jeweils zwei Erweiterungen E_1/F und E_2/F mit Gruppe G und teilerfremden Diskriminanten gibt es mindestens eine weitere Erweiterung E/F mit Gruppe G und Diskriminante $\mathfrak{d}(E/F) \mid \mathfrak{d}(E_1/F) \cdot \mathfrak{d}(E_2/F)$. Hieraus folgen $\mathcal{N}\mathfrak{d}(E/F)^{-s} \geq \mathcal{N}\mathfrak{d}(E_1/F)^{-s} \cdot \mathcal{N}\mathfrak{d}(E_2/F)^{-s}$ und

$$\Phi(F,G;s) \quad \geq \quad \sum_{\mu(\mathfrak{m}) \neq 0} a(G,\mathfrak{m}^2) \cdot \mathcal{N}\mathfrak{m}^{-2t\cdot s} \quad \geq \quad \prod_\mathfrak{p} \left(1 + \begin{bmatrix} [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p] \\ r \end{bmatrix}_p \cdot \mathcal{N}\mathfrak{p}^{-2t\cdot s}\right)$$

für positive $s \in \mathbf{R}$. Der Binomialkoeffizient ist ein Polynom in $\mathcal{N}\mathfrak{p}$ vom Grad r und bezeichnet b seinen Leitkoeffizienten, so hat das Eulerprodukt die Form

$$\prod_\mathfrak{p} \left(1 + b \cdot \mathcal{N}\mathfrak{p}^{r-2t\cdot s} + o(\mathcal{N}\mathfrak{p}^{-s/a(F,G)})\right)$$

für $s \geq a(F,G)$ und besitzt einen Pol in $s = a(F,G)$. Somit ist $a(F,G)$ eine untere Schranke für die Konvergenzabszisse von $\Phi(F,G;s)$.

Auch hier ist der Vergleich der a-Konstanten elementar gewinnbar. Für nichtzyklische Gruppen ist $a(F,G)$ genau dann größer als $a(G)$, wenn

$$g(x) = (1+x) \cdot (p^x - p^{x-1}) - 2 \cdot (p^x - 1)$$

positiv ist. Es sind $g(1) = 0$, $g(2) = p^2 - 3 \cdot p + 2$ und

$$\frac{g(x) - 2}{p^{x-1}} = (x+1) \cdot (p-1) - 2 \cdot p = (x-1) \cdot (p-1) - 2.$$

Somit ist $g(x)$ nicht negativ und nur im Fall $x = 1$ oder $(p,x) = (2,2)$ nicht positiv. □

Dieser Satz stellt klar, dass die Mallevermutung nicht einfach auf den Fall wild verzweigter Funktionenkörper übertragen werden kann. Interessant gegenüber anderen Gegenbeispielen zur Mallevermutung (siehe Klüners 2005a), in welchen der logarithmische Exponent höher als erwartet ausfällt, ist hier der a-Exponent betroffen. In den folgenden Beispielen und Bemerkungen sollen die a-Konstanten $a(G)$, $a_{\mathfrak{p}}(G)$ und $a(F,G)$ verglichen werden.

Beispiel 2.34. — Im Fall der Charakteristik $p = 2$ gilt für elementarabelsche p-Gruppen G

$$\max\{a(G), a_{\mathfrak{p}}(G), a(F,G)\} = a(F,G).$$

Bezeichnet $r = \dim G$ den p-Rang von G, so hat der Quotient von $a(F,G)$ und $a(G)$ den Wert

$$1 \leq \frac{a(F,G)}{a(G)} = \frac{(r+1)\cdot 2^r}{4\cdot(2^r-1)} \overset{r\to\infty}{\longrightarrow} \infty$$

mit über alle Grenzen wachsenden Limes. In folgender Tabelle sind einige Werte für elementarabelsche Gruppen eingetragen.

r	1	2	3	4	5	...	1000
$a(F,Z_2^r)$	1	$\frac{1}{2}$	$\frac{2}{7}$	$\frac{1}{6}$	$\frac{3}{31}$		$1.955\cdot 2^{-992}$
$a_{\mathfrak{p}}(Z_2^r)$	$\frac{1}{2}$	$\frac{1}{3}$	$\frac{3}{14}$	$\frac{2}{15}$	$\frac{5}{62}$		$1.953\cdot 2^{-992}$
$a(Z_2^r)$	1	$\frac{1}{2}$	$\frac{1}{4}$	$\frac{1}{8}$	$\frac{1}{16}$		2^{-999}
$\frac{a(F,Z_2^r)}{a(Z_2^r)}$	1	1	$\frac{8}{7}$	$\frac{4}{3}$	$\frac{48}{31}$		$1.955\cdot 2^7$

Beweis. — Nach Satz 2.33 reicht der Nachweis von $a(F,G) > a_{\mathfrak{p}}(G)$ und es gilt

$$a(F,G) = a_{\mathfrak{p}}(G) + \frac{1}{2\cdot(2^r-1)}.$$

□

Beispiel 2.35. — Im Fall der Charakteristik $p \neq 2$ gilt für elementarabelsche p-Gruppen G vom Rang r die Relation

$$\max\{a(G), a_{\mathfrak{p}}(G), a(F,G)\} = \begin{cases} a(F,G) & r = 1 \text{ oder } (p,r) = (3,2) \\ a_{\mathfrak{p}}(G) & \text{sonst.} \end{cases}$$

Der Quotient von $a_{\mathfrak{p}}(G)$ und $a(G)$ wächst bei nichtzyklischen Gruppen mit steigender Ordnung über alle Grenzen. Die folgenden Tabellen enthalten konkrete Werte für $p = 3, 5, 103$.

r	1	2	3	4	5	...	1000
$a_{\mathfrak{p}}(Z_3^r)$	$\frac{1}{3}$	$\frac{1}{6}$	$\frac{1}{13}$	$\frac{1}{30}$	$\frac{5}{363}$		$2.743\cdot 3^{-995}$
$a(F,Z_3^r)$	$\frac{1}{2}$	$\frac{3}{16}$	$\frac{1}{13}$	$\frac{1}{32}$	$\frac{3}{242}$		$2.059\cdot 3^{-995}$
$a(Z_3^r)$	$\frac{1}{2}$	$\frac{1}{6}$	$\frac{1}{18}$	$\frac{1}{54}$	$\frac{1}{162}$		$0.5\cdot 3^{-999}$
$\frac{a_{\mathfrak{p}}(Z_3^r)}{a(Z_3^r)}$	$\frac{2}{3}$	1	$\frac{18}{13}$	$\frac{9}{5}$	$\frac{270}{121}$		$5.486\cdot 3^4$

r	1	2	3	4	5	...	1000
$a_{\mathfrak{p}}(Z_5^r)$	$\frac{1}{5}$	$\frac{1}{15}$	$\frac{3}{155}$	$\frac{1}{195}$	$\frac{1}{781}$		$1.280 \cdot 5^{-996}$
$a(F, Z_5^r)$	$\frac{1}{4}$	$\frac{1}{16}$	$\frac{1}{62}$	$\frac{5}{1248}$	$\frac{3}{3124}$		$0.800 \cdot 5^{-996}$
$a(Z_5^r)$	$\frac{1}{4}$	$\frac{1}{20}$	$\frac{1}{100}$	$\frac{1}{500}$	$\frac{1}{2500}$		$0.25 \cdot 5^{-999}$
$\frac{a_{\mathfrak{p}}(Z_5^r)}{a(Z_5^r)}$	$\frac{4}{5}$	$\frac{4}{3}$	$\frac{60}{31}$	$\frac{100}{39}$	$\frac{2500}{781}$		$5.120 \cdot 5^3$

r	1	2	3	4	5	...	1000
$a_{\mathfrak{p}}(Z_{103}^r)$	$\frac{1}{103}$	$\frac{1}{5356}$	$\frac{1}{367813}$	$\frac{1}{28413580}$	$\frac{5}{11706395063}$		$9.614 \cdot 103^{-999}$
$a(F, Z_{103}^r)$	$\frac{1}{102}$	$\frac{1}{7072}$	$\frac{1}{546363}$	$\frac{1}{45020352}$	$\frac{5}{19321234570}$		$4.859 \cdot 103^{-999}$
$a(Z_{103}^r)$	$\frac{1}{102}$	$\frac{1}{10506}$	$\frac{1}{1082118}$	$\frac{1}{111458154}$	$\frac{1}{11480189862}$		$0.009 \cdot 103^{-999}$
$\frac{a_{\mathfrak{p}}(Z_{103}^r)}{a(Z_{103}^r)}$	$\frac{102}{103}$	$\frac{51}{26}$	$\frac{10506}{3571}$	$\frac{541059}{137930}$	$\frac{557290770}{113654321}$		$9.521 \cdot 103$

Beweis. — Die Ungleichung

$$\frac{(p-1) \cdot r}{p \cdot (p^r - 1)} = a_{\mathfrak{p}}(G) > a(F, G) = \frac{1 + r}{2 \cdot (p^r - 1)}$$

ist äquivalent zu

$$(r-1) \cdot p > 2 \cdot r,$$

was für $r \geq 2$ und $(p, r) \neq (3, 2)$ zutreffend ist. □

KAPITEL 3

ASYMPTOTIK ZYKLISCHER p-ERWEITERUNGEN

In diesem Kapitel gebe ich die exakte Asymptotik zyklischer p-Erweiterungen globaler Funktionenkörper der Charakteristik p an. Im Gegensatz zu den nichtzyklischen p-Gruppen erfüllt die Asymptotik dieses Gruppentyps das erwartete Verhalten, welches nach dem Satz von Wright und der Asymptotikvermutung von Malle nahegelegt werden könnte.

Satz 3.1. — *Es seien F ein globaler Funktionenkörper der Charakteristik p und G eine zyklische p-Gruppe. Dann gibt es eine positive Konstante $c(F,G)$, sodass die Zählfunktion $Z(F,G;x)$ asymptotisch äquivalent ist zu*

$$Z(F,G;x) \sim c(F,G) \cdot x^{a(G)} \cdot \log(x)^{b(F,G)-1}$$

mit $a(G) = ((G : Z_p) \cdot (p-1))^{-1}$ und $b(F,G) = p-1$.

Zusatz 3.2. — *Es sei d der Grenzwert der Folge $d_m = \sum_{n \leq m} q^{(n-m)/(p-1)}(n/m)^{p-2}$. Dann hat die reelle Konstante $c(F,Z_p)$ für $p \neq 2$ die Gestalt*

$$c(F,Z_p) = \frac{d \cdot \log(q) \cdot \mathrm{Res}_{s=1}(\zeta_F(s))^{p-1}}{(p-1)! \cdot (p-2)! \cdot (p-1)^{p-1}} \cdot \prod_{\mathfrak{p}} (1 + (p-1) \cdot \mathcal{N}\mathfrak{p}^{-1}) \cdot (1 - \mathcal{N}\mathfrak{p}^{-1})^{p-1}$$

und für $p = 2$ die Formel

$$c(F,Z_2) = 2 \cdot d \cdot \log(q) \cdot \frac{\mathrm{Res}_{s=1}(\zeta_F(s))}{\zeta_F(2)}.$$

Schlachtplan. — Die Berechnung der Asymptotik zyklischer p-Erweiterungen erfolgt in drei Schritten. Zunächst berechne ich die exakte Asymptotik einfacher Erweiterungen vom Grad p, den Artin-Schreier-Erweiterungen. Der globalen Klassenkörpertheorie zu Folge entsprechen die Artin-Schreier-Erweiterungen mit Führer $\mathfrak{f} \mid \mathfrak{m}$ genau den Untergruppen der Strahlklassengruppe $\mathcal{C}\ell_{\mathfrak{m}}$ vom Index p. Bei der exakten Ermittlung des p-Ranges tritt der Störfaktor $S_{p,\mathfrak{m}}$ auf. Diese Gruppe besteht aus aus den p-Selmerelementen, die einen Vertreter im Strahl $F_{\mathfrak{m}}$ besitzen. Ihre exakte Berechnung ist im Allgemeinen kaum möglich (siehe Cohen et al. (2002)). Allerdings kann ich hier im vorliegenden Fall ihre Isomorphie zu einer Untergruppe von ganzen Differentialen ausnutzen und so nachweisen, dass sie für eine asymptotisch dominante Familie von relevanten Moduln $\mathfrak{m}$ trivial ist. Es ergibt sich ein schönes Lokal-Global-Prinzip, da sich die Anzahl der Artin-Schreier-Erweiterungen mit jenen Führer $\mathfrak{m}$ multiplikativ verhält. Dieses Prinzip kann

ich ausnutzen, um die Dirichletreihe $\Phi(F,G;s)$ in ein Eulerprodukt und einer gut kontrollierbaren rationalen Funktion zu zerlegen. Mit dem Taubersatz gewinne ich schließlich das asymptotische Verhalten der Artin-Schreier-Erweiterungen, welches in Harmonie mit der Malleschen Vermutung steht.

Dies trifft auch für beliebige zyklische p-Gruppen zu. Ihre Analyse ist leider nicht so leicht zugänglich wie jene der Artin-Schreier-Erweiterungen. Hier nutze ich die Ergebnisse von Wright (1989) und Klüners (2005). Zunächst erhalte ich mit der Methodik der zentralen Einbettungen eine untere Schranke für die Konvergenzabszisse der Reihe $\Phi(F,G;s)$. Mit Wrights Zerlegung von $\Phi(F,G;s)$ kann ich die am weitesten rechts liegende Singularität von $\Phi(F,G;s)$ lokalisieren und diese stimmt mit der bereits erhaltenen unteren Abschätzung der Abszisse überein. Es ist schließlich noch die Polordnung und analytische Fortsetzbarkeit zu überprüfen, um schließlich wiederum mit dem Taubersatz die behauptete Asymptotik zu verifizieren.

3.1. Strahlklassengruppen

In diesem Abschnitt taucht die p-Selmergruppe $S_p = \{x \in F^\times : (x) = \mathfrak{b}^p\}/F^p$ der Funktionen mit Divisor zur p-Potenz auf. Die Selmerstrahlgruppe $S_{p,\mathfrak{m}} = \{x \cdot F^p \in S_p : x \in F_\mathfrak{m}\}$ besteht aus jenen Selmerklassen, die einen Repräsentanten im Strahl $F_\mathfrak{m}$ besitzen.

Bemerkung 3.3. — *Es gilt die exakte Sequenz von abelschen p-Gruppen*

$$1 \to S_{p,\mathfrak{m}} \to S_p \to (F^\mathfrak{m}/F_\mathfrak{m})/(F^\mathfrak{m}/F_\mathfrak{m})^p \to \mathcal{C}\ell_\mathfrak{m}/\mathcal{C}\ell_\mathfrak{m}^p \to \mathcal{C}\ell/\mathcal{C}\ell^p \to 1.$$

Beweis. — Die aus der Klassenkörpertheorie bekannte Sequenz

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

bleibt unter Tensorierung mit Z_p rechtsexakt, d.h. es gilt

$$U_\mathfrak{m} = (F^\mathfrak{m}/F_\mathfrak{m})/(F^\mathfrak{m}/F_\mathfrak{m})^p \to \mathcal{C}\ell_\mathfrak{m}/\mathcal{C}\ell_\mathfrak{m}^p \to \mathcal{C}\ell/\mathcal{C}\ell^p \to 1.$$

Der Kern U der Abbildung $U_\mathfrak{m} \to \mathcal{C}\ell_\mathfrak{m}/\mathcal{C}\ell_\mathfrak{m}^p$ wird erzeugt von Funktionen $x \in F^\mathfrak{m}$ mit Divisor $(x) = (y)\cdot\mathfrak{a}^p$, wobei y aus dem Strahl $F_\mathfrak{m}$ stammt. Folglich enthält jede Klasse $x\cdot F_\mathfrak{m} = xy^{-1}\cdot F_\mathfrak{m}$ in U ein Selmerelement $z = xy^{-1}$. Umgekehrt ist nach dem Approximationssatz jede Klasse $z \cdot F^p$ von Selmerelementen in U abbildbar und jene Abbildung besitzt den Kern $S_{p,\mathfrak{m}}$. □

Bemerkung 3.4. — *Der p-Rang der Strahlklassengruppe $\mathcal{C}\ell_\mathfrak{m}$ ergibt sich aus*

$$(\mathcal{C}\ell_\mathfrak{m} : \mathcal{C}\ell_\mathfrak{m}^p) = p \cdot (S_{p,\mathfrak{m}} : 1) \cdot \prod_{\mathfrak{p}^m || \mathfrak{m}} \mathcal{N}\mathfrak{p}^{m-1-\lfloor \frac{m-1}{p} \rfloor}.$$

Beweis. — Nach Bemerkung 3.3 gilt die Indexformel

$$(\mathcal{C}\ell_\mathfrak{m} : \mathcal{C}\ell_\mathfrak{m}^p) = (S_{p,\mathfrak{m}} : 1) \cdot (S_p : 1)^{-1} \cdot (U_\mathfrak{m} : 1) \cdot (\mathcal{C}\ell : \mathcal{C}\ell^p).$$

Die Selmergruppe S_p ist isomorph zur p-Torsionsgruppe der Nullklassen in $\mathcal{C}\ell$ vermöge der wie folgt beschriebenen Abbildung. Für eine Selmerklasse $x \cdot F^p$ gibt es einen Divisor $\mathfrak{b}$ mit $(x) = \mathfrak{b}^p$ und dieser

ist eindeutig bis auf Multiplikation mit der Hauptklasse. Somit ist $x \cdot F^p \mapsto [\mathfrak{b}]$ eine wohldefinierte und offensichtlich auch bijektive Abbildung von S_p auf $\mathcal{C}\ell[p]$. Auf Grund von $\mathcal{C}\ell/\mathcal{C}\ell^p \simeq Z_p \times \mathcal{C}\ell[p]$ hat dies

$$(\mathcal{C}\ell_{\mathfrak{m}} : \mathcal{C}\ell_{\mathfrak{m}}^p) = (S_{p,\mathfrak{m}} : 1) \cdot (U_{\mathfrak{m}} : 1) \cdot p$$

zur Folge. Die p-Sylowgruppe von $F^{\mathfrak{m}}/F_{\mathfrak{m}}$ ist isomorph zum direkten Produkt der Einseinheitengruppen $\langle 1 + \mathfrak{p} \rangle / \langle 1 + \mathfrak{p}^m \rangle$ und die behauptete Größe von $U_{\mathfrak{m}}$ ergibt sich aus Korollar C.2. □

Der p-Rang von Strahlklassengruppen verhält sich also bis auf den Störfaktor $S_{p,\mathfrak{m}}$ multiplikativ. Mit den beiden folgenden Bemerkungen untersuche ich diesen und gebe ein hinreichendes Kriterium für $S_{p,\mathfrak{m}} = 1$ an. Dabei bezeichne g_F das Geschlecht des Funktionenkörpers F.

Bemerkung 3.5. — *Es seien* $\mathfrak{m} = \mathfrak{n}\mathfrak{p}$ *ein Modul und* $\mathfrak{p}$ *eine zu* $\mathfrak{n}$ *teilerfremde Stelle. Dann gelten* $(\mathcal{C}\ell_{\mathfrak{m}} : \mathcal{C}\ell_{\mathfrak{m}}^p) = (\mathcal{C}\ell_{\mathfrak{n}} : \mathcal{C}\ell_{\mathfrak{n}}^p)$ *und* $(S_{p,\mathfrak{m}} : 1) = (S_{p,\mathfrak{n}} : 1)$.

Beweis. — Da eine verzweigte p-Erweiterung des lokalen Körpers $F_{\mathfrak{p}}$ stets wild verzweigt, kann der Führer jener Erweiterung nicht quadratfrei sein. Folglich gibt es keine in $\mathfrak{p}$ verzweigte p-Erweiterung von F mit Modul $\mathfrak{m}$. Hieraus folgt $(\mathcal{C}\ell_{\mathfrak{m}} : \mathcal{C}\ell_{\mathfrak{m}}^p) = (\mathcal{C}\ell_{\mathfrak{n}} : \mathcal{C}\ell_{\mathfrak{n}}^p)$. Außerdem gilt $(U_{\mathfrak{m}} : 1) = (U_{\mathfrak{n}} : 1)$ und somit ergibt sich die Restbehauptung aus Bemerkung 3.4. □

Bemerkung 3.6. — *Die Selmerstrahlgruppe* $S_{p,\mathfrak{m}}$ *ist trivial für Moduln* $\mathfrak{m}$ *mit*

$$\sum_{\mathfrak{p}^m || \mathfrak{m}} (m-1) \cdot \deg \mathfrak{p} > 2g_F - 2.$$

Beweis. — Die multiplikative Selmerstrahlgruppe $S_{p,\mathfrak{m}}$ ist isomorph zu einer additiven Untergruppe von ganzen logarithmischen Differentialen. Dies geht aus der Abbildung

$$S_{p,\mathfrak{m}} \to \Omega_F, \quad x \cdot F^p \mapsto \frac{dx}{x}$$

hervor. Die Wohldefiniertheit und Homomorphie dieser Abbildung folgen aus der wohlbekannten Produktregel vermöge

$$\frac{d(xy)}{xy} = \frac{ydx + xdy}{xy} = \frac{dx}{x} + \frac{dy}{y} \qquad \text{und} \qquad \frac{dz^p}{z^p} = p \cdot \frac{dz}{z} = 0$$

für $x, y, z \in F^\times$. Des Weiteren ist das Differential einer Funktion x genau dann trivial, wenn x kein separierendes Element von F und somit von der Gestalt $x = z^p$ ist.[(1)] Also ist die Abbildung injektiv. Die zu einer beliebigen Stelle $\mathfrak{p}$ mit Primelement t gehörende Laurententwicklung des Selmerelementes x hat die Gestalt $x = a \cdot t^{np} + b \cdot t^{np+1} + \mathfrak{p}^{np+2}$. Somit ergeben sich aus der Kettenregel die Identität

$$\frac{dx}{x} = \frac{dx}{dt} \cdot \frac{dt}{x} = \frac{np \cdot a \cdot t^{np-1} + (np+1) \cdot b \cdot t^{np} + \mathfrak{p}^{np+1}}{a \cdot t^{np} + b \cdot t^{np+1} + \mathfrak{p}^{np+2}} \cdot dt = (ba^{-1} + \mathfrak{p}) \cdot dt$$

(1) Dieser Sachverhalt ist in Stichtenoth (2008) Proposition 4.1.8 (c) auf Seite 160 nachzulesen. Die Gestalt von nichtseparierenden Elementen ist aus Proposition 3.10.2 (d) auf Seite 144 zu entnehmen.

und folglich auch die Ganzheit von dx/x. Der Divisorgrad eines beliebigen Differentials beträgt $2g_F - 2$ und ich gewinne aus der Ganzheit die Ungleichung

$$2g_F - 2 = \deg(dx/x) \geq \sum_{\mathfrak{p}|\mathfrak{m}} \mathrm{ord}_{\mathfrak{p}}(dx/x) \cdot \deg \mathfrak{p}.$$

Da x weiterhin auch aus dem Strahl $F_{\mathfrak{m}}$ gewählt werden kann, hat die Funktion bei den Trägerstellen $\mathfrak{p}$ von $\mathfrak{m}$ sogar eine lokale Entwicklung der Gestalt $x = 1 + \mathfrak{p}^m$, woraus sich $\mathrm{ord}_{\mathfrak{p}}(dx/x) \geq m - 1$ und

$$2g_F - 2 \geq \sum_{\mathfrak{p}^m||\mathfrak{m}} (m-1) \cdot \deg \mathfrak{p}$$

ergeben. Für einen Modul $\mathfrak{m}$, welcher diese Ungleichung verletzt, ist also das Bild von $S_{p,\mathfrak{m}}$ und somit die Selmerstrahlgruppe selbst trivial. □

Es bezeichne $\mathcal{M}$ die endliche Menge aller nirgends quadratfreien Moduln mit Trägerstellen $\mathfrak{p}$ ausschließlich vom Grad $\deg \mathfrak{p} \leq 2g_F - 2$ und Ordnung $2 \leq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}) \leq 2g_F - 1$.

Satz 3.7. — *Es sei $a(Z_p, \mathfrak{m})$ die Anzahl der Artin-Schreier-Erweiterungen von F mit Führer $\mathfrak{m}$. Dann gelten folgende Aussagen.*

(a) *Für den trivialen Modul $\mathfrak{m} = \mathfrak{1}$ gilt*

$$a(Z_p, \mathfrak{m}) = \frac{(\mathcal{C}\ell : \mathcal{C}\ell^p) - 1}{p-1}.$$

(b) *Besitzt $\mathfrak{m}$ einen einfachen Teiler, so ist $a(Z_p, \mathfrak{m}) = 0$.*

(c) *Es seien $\mathfrak{m}_0 \in \mathcal{M}$, $\mathfrak{m}_1$ ein quadratfreier Modul mit Trägerstellen $\mathfrak{p}$ ausschließlich vom Grad $\deg \mathfrak{p} > 2g_F - 2$ und $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_1^2$. Dann gilt*

$$a(Z_p, \mathfrak{m}) = \frac{p}{p-1} \cdot \prod_{\mathfrak{p}^m||\mathfrak{m}} \left(\mathcal{N}\mathfrak{p}^{m-1-\lfloor \frac{m-1}{p} \rfloor} - \mathcal{N}\mathfrak{p}^{m-2-\lfloor \frac{m-2}{p} \rfloor} \right) + \mu(\mathfrak{m}_1) \cdot \tilde{a}(Z_p, \mathfrak{m}_0)$$

mit Korrektursummand

$$\tilde{a}(Z_p, \mathfrak{m}_0) = a(Z_p, \mathfrak{m}_0) - \frac{p}{p-1} \cdot \prod_{\mathfrak{p}^m||\mathfrak{m}_0} \left(\mathcal{N}\mathfrak{p}^{m-1-\lfloor \frac{m-1}{p} \rfloor} - \mathcal{N}\mathfrak{p}^{m-2-\lfloor \frac{m-2}{p} \rfloor} \right).$$

(d) *Für alle restlichen Moduln $\mathfrak{m}$ gilt*

$$a(Z_p, \mathfrak{m}) = \frac{p}{p-1} \cdot \prod_{\mathfrak{p}^m||\mathfrak{m}} \left(\mathcal{N}\mathfrak{p}^{m-1-\lfloor \frac{m-1}{p} \rfloor} - \mathcal{N}\mathfrak{p}^{m-2-\lfloor \frac{m-2}{p} \rfloor} \right).$$

Beweis. — Die Aussage für den trivialen Modul folgt aus der Tatsache, dass die unverzweigten Erweiterungen mit den Untergruppen von $\mathcal{C}\ell$ korrespondieren. Besitzt $\mathfrak{m} = \mathfrak{n}\mathfrak{p}$ den einfachen Teiler $\mathfrak{p}$, so gilt $(\mathcal{C}\ell_{\mathfrak{m}} : \mathcal{C}\ell_{\mathfrak{m}}^p) = (\mathcal{C}\ell_{\mathfrak{n}} : \mathcal{C}\ell_{\mathfrak{n}}^p)$ und folglich gibt es keine Artin-Schreier-Erweiterungen mit Führer $\mathfrak{m}$. Somit sind die Aussagen (a) und (b) nachgewiesen. Die Anzahl aller Artin-Schreier-Erweiterungen mit einem $\mathfrak{m}$ teilenden Führer summiert sich zu

$$\frac{(\mathcal{C}\ell_{\mathfrak{m}} : \mathcal{C}\ell_{\mathfrak{m}}^p) - 1}{p-1} = \sum_{\mathfrak{n}|\mathfrak{m}} a(Z_p, \mathfrak{n}).$$

Nach der Möbiusschen Umkehrformel und der Indexformel für $(\mathcal{C}\ell_{\mathfrak{n}} : \mathcal{C}\ell_{\mathfrak{n}}^{p})$ gemäß Bemerkung 3.3 lässt sich $a(Z_p, \mathfrak{m})$ für nichttrivale Moduln $\mathfrak{m}$ via

$$a(Z_p, \mathfrak{m}) = \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1}) \cdot \frac{(\mathcal{C}\ell_{\mathfrak{n}} : \mathcal{C}\ell_{\mathfrak{n}}^{p}) - 1}{p-1} = \frac{p}{p-1} \cdot \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1}) \cdot (U_{\mathfrak{n}} : 1) \cdot (S_{p,\mathfrak{n}} : 1)$$

berechnen, da die Differenz der letzten Gleichung durch die verschwindende Summe $\sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{n})$ teilbar ist. Besitzt $\mathfrak{m}$ einen dreifachen Teiler $\mathfrak{p}$ vom Grad $\deg \mathfrak{p} > 2g_F - 2$, so ist $a(Z_p, \mathfrak{m})$ gleichwertig mit

$$a(Z_p, \mathfrak{m}) = \frac{p}{p-1} \cdot \sum_{\mathfrak{n}|\mathfrak{m}} \mu(\mathfrak{m}\mathfrak{n}^{-1}) \cdot (U_{\mathfrak{n}} : 1),$$

da $\mathfrak{n}$ im Fall $\mu(\mathfrak{m}\mathfrak{n}^{-1}) \neq 0$ durch $\mathfrak{p}^2$ teilbar und seine Selmergruppe $S_{p,\mathfrak{n}}$ nach Bemerkung 3.6 trivial ist. Die Funktion $\mu(\mathfrak{m}\mathfrak{n}^{-1}) \cdot (U_{\mathfrak{n}} : 1)$ ist multiplikativ und somit ergibt sich $a(Z_p, \mathfrak{m})$ als Produkt

$$a(Z_p, \mathfrak{m}) = \frac{p}{p-1} \cdot \prod_{\mathfrak{p}^m || \mathfrak{m}} \sum_{n=0}^{m} \mu(\mathfrak{p}^{m-n}) \cdot (U_{\mathfrak{p}^n} : 1) = \frac{p}{p-1} \cdot \prod_{\mathfrak{p}^m || \mathfrak{m}} \left((U_{\mathfrak{p}^m} : 1) - (U_{\mathfrak{p}^{m-1}} : 1) \right).$$

Dies zeigt Aussage (d) und es verbleibt nur noch der Nachweis der Aussage (c). In diesem Fall sind in der Möbiusschen Umkehrformel höchstens die Teiler $\mathfrak{n}$ von der Form $\mathfrak{n} = \mathfrak{n}_0\mathfrak{m}_1\mathfrak{n}_1$ mit $\mathfrak{n}_0 \mid \mathfrak{m}_0$ und $\mathfrak{n}_1 \mid \mathfrak{m}_1$ von Relevanz, da andernfalls $\mathfrak{m}\mathfrak{n}^{-1}$ einen quadratischen Teiler besäße. Folglich gilt

$$a(Z_p, \mathfrak{m}) = \frac{p}{p-1} \cdot \sum_{\mathfrak{n}_0|\mathfrak{m}_0} \mu(\mathfrak{m}_0\mathfrak{n}_0^{-1}) \cdot (U_{\mathfrak{n}_0} : 1) \cdot \left(\sum_{\mathfrak{n}_1|\mathfrak{m}_1} \mu(\mathfrak{m}_1\mathfrak{n}_1^{-1}) \cdot (U_{\mathfrak{m}_1\mathfrak{n}_1} : 1) \cdot (S_{p,\mathfrak{n}_0\mathfrak{m}_1\mathfrak{n}_1} : 1) \right).$$

Auf Grund von $(S_{p,\mathfrak{m}_1\mathfrak{n}_0} : 1) = (S_{p,\mathfrak{n}_0} : 1)$ und $U_{\mathfrak{m}_1} = 1$ hat der Teilsummand für $\mathfrak{n}_1 = \mathfrak{1}$ hat die Gestalt

$$\frac{p}{p-1} \cdot \sum_{\mathfrak{n}_0|\mathfrak{m}_0} \mu(\mathfrak{m}_0\mathfrak{n}_0^{-1}) \cdot (U_{\mathfrak{n}_0} : 1) \cdot \mu(\mathfrak{m}_1) \cdot (S_{p,\mathfrak{n}_0} : 1) = \mu(\mathfrak{m}_1) \cdot a(Z_p, \mathfrak{m}_0).$$

Im Restsummanden entfallen die Selmerstrahlgruppen, da ihr jeweiliger Modul $\mathfrak{n}_0\mathfrak{m}_1\mathfrak{n}_1$ mindestens einen quadratischen Teiler $\mathfrak{p}^2$ mit $\deg \mathfrak{p} > 2g_F - 2$ hat, und er besitzt die Formel

$$\begin{aligned}
&\frac{p}{p-1} \cdot \sum_{\mathfrak{n}_0|\mathfrak{m}_0} \mu(\mathfrak{m}_0\mathfrak{n}_0^{-1}) \cdot (U_{\mathfrak{n}_0} : 1) \cdot \sum_{\mathfrak{1} \neq \mathfrak{n}_1|\mathfrak{m}_1} \mu(\mathfrak{m}_1\mathfrak{n}_1^{-1}) \cdot (U_{\mathfrak{m}_1\mathfrak{n}_1} : 1) \\
&= \frac{p}{p-1} \cdot \left(\sum_{\mathfrak{n}_0|\mathfrak{m}_0} \sum_{\mathfrak{n}_1|\mathfrak{m}_1} \mu(\mathfrak{m}\mathfrak{n}_0^{-1}\mathfrak{m}_1^{-1}\mathfrak{n}_1^{-1}) \cdot (U_{\mathfrak{n}_0\mathfrak{m}_1\mathfrak{n}_1} : 1) - \sum_{\mathfrak{n}_0|\mathfrak{m}_0} \mu(\mathfrak{m}\mathfrak{n}_0^{-1}\mathfrak{m}_1^{-1}) \cdot (U_{\mathfrak{n}_0} : 1) \cdot (U_{\mathfrak{m}_1} : 1) \right) \\
&= \frac{p}{p-1} \cdot \left(\prod_{\mathfrak{p}^m || \mathfrak{m}} \Big((U_{\mathfrak{p}^m} : 1) - (U_{\mathfrak{p}^{m-1}} : 1) \Big) - \mu(\mathfrak{m}_1) \cdot \prod_{\mathfrak{p}^m || \mathfrak{m}_0} \Big((U_{\mathfrak{p}^m} : 1) - (U_{\mathfrak{p}^{m-1}} : 1) \Big) \right),
\end{aligned}$$

wobei in der letzten Gleichung $(U_{\mathfrak{m}_1} : 1) = 1$ und die Multiplikativität der Summanden ausgenutzt werden. Zusammen mit der obigen Formel für den Teilsummanden im Fall $\mathfrak{n}_1 = \mathfrak{1}$ ergibt sich hieraus schließlich auch die Behauptung für Teil (c). □

Die Multiplikativität der Koeffizienten $a(Z_p, \mathfrak{m})$ liefert ein einfaches Lokal-Global-Prinzip für Artin-Schreier-Erweiterungen vom Grad p, welches in einem Eulerprodukt für die Dirichletreihe

$$\Phi(F, Z_p; s) = \sum_{\mathrm{Gal}(E/F) \simeq Z_p} \mathcal{N}\mathfrak{d}(E/F)^{-s}$$

codiert werden kann.

Korollar 3.8. — *Die Dirichletreihe $\Phi(F, Z_p; s)$ der zyklischen Artin-Schreier-Erweiterungen von F hat die Summenzerlegung*

$$\Phi(F, Z_p; s) = \frac{p}{p-1} \cdot \Phi(s) + \Upsilon(s)$$

in ein Eulerprodukt $\Phi(s) = \prod_{\mathfrak{p}} \Phi_{\mathfrak{p}}(s)$ mit

$$\Phi_{\mathfrak{p}}(s) = 1 + \sum_{m \geq 1} \left(\mathcal{N}\mathfrak{p}^{m - \lfloor \frac{m}{p} \rfloor} - \mathcal{N}\mathfrak{p}^{m-1-\lfloor \frac{m-1}{p} \rfloor} \right) \cdot \mathcal{N}\mathfrak{p}^{-(m+1)\cdot(p-1)\cdot s}$$

und einer in q^{-s} rationalen Funktion $\Upsilon(s)$ mit Konvergenzabszisse $a(Z_p)/4$.

Beweis. — Nach der Führerdiskriminantenformel hat eine Artin-Schreier-Erweiterung mit Führer $\mathfrak{m}$ die Diskriminante $\mathfrak{m}^{p-1}$ und daher lässt sich $\Phi(F, Z_p; s)$ schreiben als

$$\Phi(F, Z_p; s) = \sum_{\mathfrak{m}} a(Z_p, \mathfrak{m}) \cdot \mathcal{N}\mathfrak{m}^{-(p-1)\cdot s}.$$

Nach Bemerkung 3.7 kann diese Reihe auf nirgends quadratfreie Moduln $\mathfrak{m}$ sowie den trivialen Modul eingeschränkt werden. Diese Einschränkung für $\mathfrak{m}$ möchte ich für diesen Beweis annehmen. Dann hat das Eulerprodukt $\Phi(s)$ die Gestalt

$$\Phi(s) = \sum_{\mathfrak{m}} \prod_{\mathfrak{p}^m || \mathfrak{m}} \left(\mathcal{N}\mathfrak{p}^{m-1-\lfloor \frac{m-1}{p} \rfloor} - \mathcal{N}\mathfrak{p}^{m-2-\lfloor \frac{m-2}{p} \rfloor} \right) \cdot \mathcal{N}\mathfrak{m}^{-(p-1)\cdot s}$$

und die Differenz $\Upsilon(s)$ von $\Phi(F, Z_p; s)$ und $\Phi(s) \cdot p/(p-1)$ ist von der Form

$$\Upsilon(s) = \sum_{\mathfrak{m}} \left(a(Z_p, \mathfrak{m}) - \frac{p}{p-1} \cdot \prod_{\mathfrak{p}^m || \mathfrak{m}} \left(\mathcal{N}\mathfrak{p}^{m-1-\lfloor \frac{m-1}{p} \rfloor} - \mathcal{N}\mathfrak{p}^{m-2-\lfloor \frac{m-2}{p} \rfloor} \right) \right) \cdot \mathcal{N}\mathfrak{m}^{-(p-1)\cdot s}.$$

Diese Reihe wird ausschließlich von den Ausnahmemoduln aus Fall (c) in Bemerkung 3.7 sowie dem trivialen Modul $\mathfrak{m} = \mathfrak{1}$ erzeugt und es gilt

$$\Upsilon(s) = \frac{(\mathcal{C}\ell : \mathcal{C}\ell^p) - p}{p-1} + \sum_{\mathfrak{m}_0 \in \mathcal{M}} \tilde{a}(Z_p, \mathfrak{m}_0) \cdot \mathcal{N}\mathfrak{m}_0^{-(p-1)\cdot s} \cdot \prod_{\deg \mathfrak{p} > 2g_F - 2} (1 - \mathcal{N}\mathfrak{p}^{-2\cdot(p-1)\cdot s}).$$

Da $\mathcal{M}$ eine endliche Elementzahl hat, ist die Summe über ihre Elemente ein Polynom $f(q^{-s})$ in q^{-s}. Genauso gibt es nur endlich viele Stellen vom Grad $\deg \mathfrak{p} \leq 2g_F - 2$ und das Produkt $g(q^{-s})$ über ihre Eulerfaktoren $(1 - \mathcal{N}\mathfrak{p}^{-s})$ ist ebenfalls ein Polynom. Folglich ist die Reihe $\Upsilon(s)$ rational in q^{-s} vermöge

$$\Upsilon(s) = \frac{(\mathcal{C}\ell : \mathcal{C}\ell^p) - p}{p-1} + \frac{f(q^{-s})}{g(q^{-2(p-1)s})} \cdot \zeta_F(2(p-1)s)^{-1}.$$

Die Pole befinden sich auf den Imaginärachsen $\Re(s) = 0$ und $\Re(s) = 1/(4(p-1)) = a(Z_p)/4$. □

3.2. Asymptotik einfacher zyklischer p-Erweiterungen

In diesem Abschnitt untersuche ich die Dirichletreihe $\Phi(F, Z_p; s)$ auf ihre Konvergenzabszisse a, der zugehörenden Polordnung b in $s = a$ sowie dem Grenzwert $c = \lim_{s \to a}(s-a)^b \cdot \Phi(F, Z_p; s)$, woraus sich Satz 3.1 im Fall $G = Z_p$ und Zusatz 3.2 ergeben. Die Korrekturreihe $\Upsilon(s)$ ist bereits hinreichend genau untersucht und auf Grund ihrer strikt kleineren Abszisse als $a(Z_p)$ wird sie, sobald die Abszisse von

$\Phi(s)$ festgestellt ist, in der Asymptotikuntersuchung keine weitere Rolle mehr spielen. Zunächst gilt es Kontrolle über die Eulerfaktoren von $\Phi(s)$ zu gewinnen.

Bemerkung 3.9. — *Die Eulerfaktoren von $\Phi(s)$ sind meromorph auf die gesamte Ebene fortsetzbar durch*

$$\Phi_{\mathfrak{p}}(s) = \Psi_{\mathfrak{p}}(s) \cdot (1 - \mathcal{N}\mathfrak{p}^{\beta(s)})^{-1} \cdot (1 - \mathcal{N}\mathfrak{p}^{-(p-1)\cdot s}) \cdot \prod_{y=0}^{p-2} (1 - \mathcal{N}\mathfrak{p}^{y\cdot\gamma(s)-(p-1)\cdot s})^{-1}$$

mit $\beta(s) = (p-1)\cdot(1-p\cdot s)$ und $\gamma(s) = 1-(p-1)\cdot s$. Das Eulerprodukt $\Psi(s) = \prod_{\mathfrak{p}} \Psi_{\mathfrak{p}}(s)$ ist hierbei über $s = a(Z_p)$ hinaus holomorph fortsetzbar mit dem Funktionswert

$$\Psi(a(Z_p)) = \prod_{\mathfrak{p}} \Psi_{\mathfrak{p}}(a(Z_p)) = \prod_{\mathfrak{p}} (1 + (p-1)\cdot\mathcal{N}\mathfrak{p}^{-1}) \cdot (1 - \mathcal{N}\mathfrak{p}^{-1})^{p-1}.$$

Beweis. — Die Eulerfaktoren besitzen nach Bemerkung 3.8 die Reihengestalt

$$\Phi_{\mathfrak{p}}(s) = 1 + \sum_{p\nmid m} (\mathcal{N}\mathfrak{p}-1)\cdot\mathcal{N}\mathfrak{p}^{m-1-\lfloor\frac{m-1}{p}\rfloor-(m+1)\cdot(p-1)\cdot s}.$$

Reihen dieser Form sind nach Lemma 2.26 berechenbar, aber diese Zerlegung ist hier schneller manuell nachvollzogen als das Blättern dauern würde. Für $m = xp+y+1$ mit $0 \le y \le p-2$ besitzt nämlich der Exponent die Aufteilung

$$m - 1 - \left\lfloor \frac{m-1}{p} \right\rfloor - (m+1)\cdot(p-1)\cdot s = x\cdot\beta(s) + y\cdot\gamma(s) - 2\cdot(p-1)\cdot s$$

und hieraus folgt die Formel

$$\Phi_{\mathfrak{p}}(s) = 1 + (\mathcal{N}\mathfrak{p}-1)\cdot\mathcal{N}\mathfrak{p}^{-2\cdot(p-1)\cdot s} \cdot \sum_{x\ge 0} \mathcal{N}\mathfrak{p}^{x\cdot\beta(s)} \cdot \sum_{y=0}^{p-2} \mathcal{N}\mathfrak{p}^{y\cdot\gamma(s)}.$$

Diese Reihe hat die Konvergenzabszisse in der Nullstelle $1/p$ von $\beta(s)$ und ist über ihre Abszisse hinaus meromorph fortsetzbar mit

$$\Phi_{\mathfrak{p}}(s) = (1-\mathcal{N}\mathfrak{p}^{\beta(s)})^{-1} \cdot \left(1 - \mathcal{N}\mathfrak{p}^{\beta(s)} + (\mathcal{N}\mathfrak{p}-1)\cdot\mathcal{N}\mathfrak{p}^{-2\cdot(p-1)\cdot s} \cdot \sum_{y=0}^{p-2} \mathcal{N}\mathfrak{p}^{y\cdot\gamma(s)}\right).$$

Der besseren Übersicht wegen verwende ich für den Rest dieses Beweis die vereinfachenden Notationen $u = \mathcal{N}\mathfrak{p}^{-(p-1)\cdot s}$, $v = \mathcal{N}\mathfrak{p}^{1-(p-1)\cdot s}$ sowie $w = 1+v+\ldots+v^{p-2}$. Insbesondere gelten $\mathcal{N}\mathfrak{p}^{\beta(s)} = uv^{p-1}$ und $\mathcal{N}\mathfrak{p} = u^{-1}v$. So umgeschrieben besitzt $\Phi_{\mathfrak{p}}(s)$ die Gleichung

$$\Phi_{\mathfrak{p}}(s) = (1-uv^{p-1})^{-1}\cdot(1-uv^{p-1}+uw(v-u)).$$

Letzterer Faktor ist identisch mit

$$1 - uv^{p-1} + uw(v-u) = 1 + u(v+\ldots+v^{p-2}) - u^2w = 1 + u(w-1) - u^2w = (1+uw)\cdot(1-u).$$

Mit $(1-uv^{p-1})^{-1}\cdot(1-u)$ sind somit bereits zwei der Faktoren von $\Phi_{\mathfrak{p}}(s)$ bestätigt. Des Weiteren spaltet $1+uw$ die Faktoren $(1-u)^{-1}\cdots(1-uv^{p-2})^{-1}$ ab, d.h. die behauptete Formel ist wahr mit

$$\Psi_{\mathfrak{p}}(s) = (1+uw)\cdot\prod_{y=0}^{p-2}(1-uv^y) = 1-(uw)^2+(1+uw)\cdot z \tag{3.9.1}$$

und

$$z = \prod_{y=0}^{p-2}(1-uv^y) - (1-uw) = \sum_{k=2}^{p-2}(-u)^k \cdot \sum_{0\le y_1<\ldots<y_k\le p-2} v^{y_1+\ldots+y_k}.$$

Für $s = a(G)$ gelten $u = \mathcal{N}\mathfrak{p}^{-1}$, $v = 1$ sowie $w = p-1$ und $\Psi(a(Z_p))$ hat tatsächlich den angegebenen Wert. Für den Nachweis der Holomorphie von $\Psi(s)$ in einer $a(Z_p)$ umfassenden Halbebene ist nach Lemma E.1 nur ein $\varepsilon > 0$ zu finden, sodass die $\mathcal{N}\mathfrak{p}$-Potenzen von $\Psi_\mathfrak{p}(s)$ in $\Re(s) > a(Z_p) - \varepsilon$ einen strikt kleineren Exponenten als -1 haben. Ich transformiere nun s in die Gestalt $s = (1-\varepsilon)/(p-1)$. Für solche s gelten $u = \mathcal{N}\mathfrak{p}^{\varepsilon-1}$, $v = \mathcal{N}\mathfrak{p}^{\varepsilon}$ und die größte $\mathcal{N}\mathfrak{p}$-Potenz in w ist $\mathcal{N}\mathfrak{p}^{(p-2)\cdot\varepsilon}$. Die in $\Psi_\mathfrak{p}(s)$ auftretenden Exponenten sind dann von der Gestalt $(y_1+y_2+2)\varepsilon - 2$, nämlich jene in $(uw)^2$, oder aber $(y_1+\ldots+y_k+k)\varepsilon - k$ als solche in z sowie $(1+y+y_1+\ldots+y_k+k)\varepsilon - (1+k)$ als Exponenten in uwz. Dies liefert endlich viele Ungleichungen mit Unbekannter ε und es kann tatsächlich ein positives $\varepsilon > 0$ gefunden werden, sodass jene Exponenten allesamt strikt kleiner als -1 sind, beispielsweise im Intervall $1/2(p-1) > \varepsilon > 0$. □

Korollar 3.10. — *Für die Dirichletreihe $\Phi(F, Z_p; s)$ gilt*

$$\Phi(F, Z_p; s) = \frac{p}{p-1} \cdot \Psi(s) \cdot \prod_{l=2}^{p} \zeta_F\big(1 - l\cdot\gamma(s)\big) + \Upsilon(s).$$

Insbesondere ergibt sich im Fall der Charakteristik $p = 2$ die Gleichung

$$\Phi(F, Z_2; s) = 2\cdot\zeta_F(2s)^{-1}\cdot\zeta_F(2s-1) + \Upsilon(s).$$

Beweis. — Nach Korollar 3.8 ist $\Phi(F, Z_p; s)$ die Summe von $\Phi(s)\cdot p/(p-1)$ und $\Upsilon(s)$ und des Weiteren gilt nach Bemerkung 3.9

$$\Phi(s) = \Psi(s)\cdot\zeta_F(-\beta(s))\cdot\zeta_F((p-1)\cdot s)^{-1}\cdot\prod_{y=0}^{p-2}\zeta_F\big((p-1)\cdot s - y\cdot\gamma(s)\big).$$

Für die behauptete Identität ist der zu $y = 0$ gehörenden ζ-Faktor mit seinem Reziprok auszulöschen, die Gleichungen $\beta(s) = (p-1)\cdot(\gamma(s) - s)$ und $(p-1)\cdot s - y\cdot\gamma(s) = 1 - (y+1)\cdot\gamma(s)$ auszunutzen und die verbleibenden Faktoren als Produkt über $l = y+1$ zusammenzufassen. Für den Fall $p = 2$ ist noch $\Psi(s) = \zeta_F(2s)^{-1}$ zu zeigen. Dies ist ersichtlich an Hand von

$$\Psi_\mathfrak{p}(s) = (1+uw)(1-u) = (1+\mathcal{N}\mathfrak{p}^{-s})(1-\mathcal{N}\mathfrak{p}^{-s}) = 1 - \mathcal{N}\mathfrak{p}^{-2s}$$

vermöge der Formel `3.9.1`. □

Satz 3.11. — *Die Artin-Schreier-Erweiterungen über F haben die Asymptotik*

$$Z(F, Z_p; x) \sim c(F, Z_p)\cdot x^{a(Z_p)}\cdot\log(x)^{b(F,Z_p)-1}$$

mit der in Zusatz 3.2 angegebenen Konstante $c(F, Z_p)$.

Beweis. — Die Konvergenzabszisse von $\Phi(F, Z_p; s)$ ist nach den Korollaren 3.8 und 3.10 tatsächlich $a = a(Z_p) = 1/(p-1)$. Daher ist der Korrektursummand $\Upsilon(s)$ wie angekündigt unerheblich für die Asymptotik der Artin-Schreier-Erweiterungen und die a, b, c-Konstanten gemäß des Taubersatzes der Reihen $\Phi(F, Z_p; s)$ und $\Phi(s) \cdot p/(p-1)$ stimmen überein. Ich betrachte nun für $p \neq 2$ die Dirichletreihe

$$\begin{aligned}\tilde{\Phi}(s) &= \frac{p}{p-1} \cdot \Phi(a \cdot s) = \sum_{n \geq 0} a_n q^{-n \cdot a \cdot s} = \sum_{n \geq 0} \tilde{a}_n q^{-n \cdot s} \\ &= \frac{p}{p-1} \cdot \Psi(a \cdot s) \cdot \prod_{l=2}^{p} \zeta_F\big(1 + l \cdot (s-1)\big)\end{aligned}$$

mit Koeffizienten $\tilde{a}_n = a_{n/a}$, wobei a_n die Koeffizienten von $\Phi(s)$ seien. Die Reihe $\tilde{\Phi}(s)$ hat die Periode $v = 2\pi i/\log(q)$ und ist in einer Halbebene $\Re(s) > 1 - \varepsilon$ über ihre Abszisse $\tilde{a} = 1$ hinaus meromorph mit einzigen Polen auf der Konvergenzlinie $\Re(s) = 1$. Im Grundstreifen C ihrer Periode befinden sich die Pole bei $1 \pm kv/l$ für $2 \leq l \leq p$ und $0 \leq k < l$. Nur der Pol bei $s = 1$ ist von der Maximalordnung $b = b(F, Z_p) = p - 1$ und alle anderen sind einfach. Für diese Eigenschaft ist $p \neq 2$ wesentlich. Nach dem Taubersatz D.5 hat die Koeffizientensumme von $\tilde{\Phi}(s)$ die Asymptotik

$$\tilde{Z}(x) = \sum_{q^n \leq x} \tilde{a}_n \sim \frac{c(\tilde{\Phi}) \cdot d \cdot \log(q)}{(b-1)!} \cdot x \cdot \log(x)^{b-1}$$

mit

$$\begin{aligned}c(\tilde{\Phi}) &= \lim_{s \to 1} (s-1)^b \cdot \tilde{\Phi}(s) = \frac{p \cdot \Psi(a)}{p-1} \cdot \prod_{l=2}^{p} \mathrm{Res}_{s=1}\big(\zeta_F\big(1 + l(s-1)\big)\big) \\ &= \frac{p \cdot \Psi(a)}{p-1} \cdot \prod_{l=2}^{p} \frac{\mathrm{Res}_{s=1}(\zeta_F(s))}{l} = \frac{\Psi(a)}{p-1} \cdot \frac{\mathrm{Res}_{s=1}(\zeta_F(s))^{p-1}}{(p-1)!}.\end{aligned}$$

Es ist $Z(F, Z_p; x) \sim \tilde{Z}(x^a)$ und hieraus folgt nach Korollar D.6

$$Z(F, Z_p; x) \sim \frac{d \cdot \log(q)}{(p-2)!} \cdot \frac{\mathrm{Res}_{s=1}(\zeta_F(s))^{p-1} \cdot \Psi(a)}{(p-1)! \cdot (p-1)^{p-1}} \cdot x^a \cdot \log(x)^{b-1}.$$

Nun ist noch der Sonderfall $p = 2$ abzuhandeln. Hier hat $\Phi(s)$ nach Korollar 3.10 die Periode $\pi i/\log(q) \cdot \mathbf{Z}$ und ich betrachte die Reihe

$$\tilde{\Phi}(s) = \Phi(F, Z_2; s/2) - \Upsilon(s/2) = 2 \cdot \Phi(s/2) = 2 \cdot \zeta_F(s-1) \cdot \zeta_F(s)^{-1}$$

mit den Koeffizienten $\tilde{a}_n = a_{2n}$. Diese Funktion hat die Kovergenzabszisse 2 und es folgt nach dem Taubersatz

$$\tilde{Z}(x) = \sum_{q^n \leq x} \tilde{a}_n \sim d \cdot \log(q) \cdot \frac{2 \cdot \mathrm{Res}_{s=1}(\zeta_F(s))}{\zeta_F(2)} \cdot x^2.$$

In diesem Fall ändert die Variablentransformation nichts an der c-Konstante, denn es gilt $b = 1$ und

$$Z(F, Z_2; x) = \tilde{Z}(\sqrt{x}) \sim 2 \cdot d \cdot \log(q) \cdot \frac{\mathrm{Res}_{s=1}(\zeta_F(s))}{\zeta_F(2)} \cdot x$$

ergibt sich aus Korollar D.6. □

3.3. Einbettungsprobleme

Bemerkung 3.12. — *Das durch die zentrale Gruppenerweiterung $1 \to Z_p \to G \to H \to 1$ und der Galoiserweiterung F_H/F mit Gruppe H gegebene Einbettungsproblem besitze mindestens eine Lösung. Dann gilt*

$$Z(F,G;x) \in \Omega(Z(F,Z_p;x^{1/(H:1)})).$$

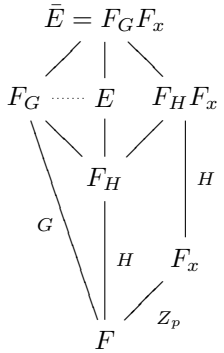
Insbesondere gilt für zyklische p-Gruppen G der asymptotische Vergleich

$$Z(F,G;x) \in \Omega(x^{a(G)} \cdot \log(x)^{b(F,G)-1}).$$

Beweis. — Es sei F_G/F eine Lösung des Einbettungsproblems mit Teilkörper F_H. Da F_G/F_H eine Artin-Schreier-Erweiterung ist, gibt es eine Funktion $y \in F_H$ mit $F_G = F_H(\wp^{-1}y)$. Nach Satz B.1 entsprechen sämtliche Lösungen des Einbettungsproblems genau den Körpern $E = F_H(\wp^{-1}(x+y))$ mit $x \in F/\wp F$. Ihre Diskriminantennorm kann ich in gleicher Weise wie Klüners und Malle (2004) mit Hilfe der Kompositionsformel

$$\mathcal{N}\mathfrak{d}(E/F)^p \cdot \mathcal{N}\mathfrak{d}(\bar{E}/E) = \mathcal{N}\mathfrak{d}(F_x/F)^{(G:1)} \cdot \mathcal{N}\mathfrak{d}(F_HF_x/F_x)^p \cdot \mathcal{N}\mathfrak{d}(\bar{E}/F_HF_x)$$

mit $F_x = F(\wp^{-1}x)$ und $\bar{E} = F_GF_x$ abschätzen.



Sowohl $\bar{E}/E$ als auch $\bar{E}/F_HF_x$ besitzen wie F_G/F_H das primitive Element $\wp^{-1}y$, wonach sich ihre Diskriminantennormen nach unten durch 1 und nach oben durch $\mathcal{N}\mathfrak{d}(F_G/F_H)^p$ abschätzen lassen.[(2)] Ebenso besitzen F_HF_x/F_H und F_x/F das gleiche primitive Element $\wp^{-1}x$ und $\mathcal{N}\mathfrak{d}(F_HF_x/F_H)$ ist durch 1 und $\mathcal{N}\mathfrak{d}(F_x/F)^{(H:1)}$ beschränkt.

Für die Norm $\mathcal{N}\mathfrak{d}(F_HF_x/F_x)$ ergeben sich hieraus die Schranken mit abermaliger Anwendung der Kompositionsformel durch

$$1 \le \mathcal{N}\mathfrak{d}(F_HF_x/F_x) = \mathcal{N}\mathfrak{d}(F_x/F)^{-(H:1)} \cdot \mathcal{N}\mathfrak{d}(F_H/F)^p \cdot \mathcal{N}\mathfrak{d}(F_HF_x/F_H) \le \mathcal{N}\mathfrak{d}(F_H/F)^p.$$

Folglich gibt es zwei nur von F_G abhängige Konstanten $c_1(F_G)$ und $c_2(F_G)$ mit

$$c_1(F_G) \cdot \mathcal{N}\mathfrak{d}(F_x/F)^{(G:1)} \le \mathcal{N}\mathfrak{d}(E/F)^p \le c_2(F_G) \cdot \mathcal{N}\mathfrak{d}(F_x/F)^{(G:1)}.$$

[(2)] Dies wird beispielsweise durch Stichtenoth (2008) Proposition 3.7.8 und Lemma 3.7.7 ersichtlich.

Mit der oberen Abschätzung erhalte ich für reelle s die Ungleichung

$$\Phi(s) = \sum_{\substack{\mathrm{Gal}(E/F)\simeq G,\\ E\geq F_H}} \mathcal{N}\mathfrak{d}(E/F)^{-s} \geq c_2(F_G)^{-s/p} \cdot \sum_{x\in F/\wp F} \mathcal{N}\mathfrak{d}(F_x/F)^{-(H:1)\cdot s}$$

von Dirichletreihen, wobei die linke Seite eine Teilreihe von $\Phi(F,G;s)$ und die rechte Seite ein Vielfaches der Reihe $\Phi(F,Z_p;s)$ ist. Folglich besitzt $\Phi(s)$ in $s=a(Z_p)/(H:1)$ einen Pol der Ordnung $b(F,Z_p)$ und es ergibt sich die behauptete Abschätzung für die Zählfunktion $Z(F,G;x)$. Ist G eine zyklische Gruppe, so folgt die zusätzliche Aussage aus $a(G)=a(Z_p)/(H:1)$ und $b(F,G)=b(F,Z_p)$. □

3.4. Asymptotik zyklischer p-Erweiterungen

In diesem Abschnitt sei G eine beliebige zyklische p-Gruppe der Ordnung p^n. Zunächst werde ich die lokale Dirichletreihe $\Phi(F_\mathfrak{p},G;s)$ auf ihre $\mathcal{N}\mathfrak{p}$-Potenzen untersuchen und mich auf die Resultate des Abschnittes 2.2 stützen. Genauer brauche ich Ergebnisse über den in Beispiel 2.22 definierten direkten Summanden $\Phi(\mathcal{O}_\mathfrak{p}^\times,G;s)$, um Aussagen über die Meromorphie der globalen Reihe $\Phi(F;G;s)$ zu gewinnen. Ich benutze den Ausdruck $o(\mathcal{N}\mathfrak{p}^{-1})$ für endliche Summen von $\mathcal{N}\mathfrak{p}$-Potenzen mit Exponenten echt kleiner als -1 und nicht von $\mathfrak{p}$ abhängigen Koeffizienten.

Bemerkung 3.13. — *Die lokale Reihe $\Phi(\mathcal{O}_\mathfrak{p}^\times,G;s)$ kann für reelle Argumente $s\geq a(G)$ durch*

$$\Phi(\mathcal{O}_\mathfrak{p}^\times,G;s) \leq 2^n \cdot o\left(\mathcal{N}\mathfrak{p}^{-1}\right) = o\left(\mathcal{N}\mathfrak{p}^{-1}\right)$$

abgeschätzt werden mit der einzigen Ausnahme

$$\Phi(\mathcal{O}_\mathfrak{p}^\times,Z_p;a(Z_p)) = \mathcal{N}\mathfrak{p}^{-1}.$$

Beweis. — Der Beweis dieser Aussage verwendet die Vorleistung in den Beispielen 2.22 und 2.32, in denen $\Phi(\mathcal{O}_\mathfrak{p}^\times,G;s)$ als rationale Funktion der Form

$$\Phi(\mathcal{O}_\mathfrak{p}^\times,G;s) = \sum_{b(\boldsymbol{G},\mathcal{I})\neq 0} \frac{\Phi(F_\mathfrak{p},\boldsymbol{G},\mathcal{I};s)}{p} = f(\boldsymbol{G};s)^{-1}\cdot \sum_{b(\boldsymbol{G},\mathcal{I})\neq 0} \frac{g(\boldsymbol{G},\mathcal{I};s)}{p} \tag{3.13.1}$$

zerlegt wird. Insbesondere ist

$$\Phi(\mathcal{O}_\mathfrak{p}^\times,Z_p;s) = \frac{\mathcal{N}\mathfrak{p}-1}{p-1}\cdot\left(1-\mathcal{N}\mathfrak{p}^{(p-1)(1-p\cdot s)}\right)^{-1}\cdot\mathcal{N}\mathfrak{p}^{-2(p-1)\cdot s}\cdot\sum_{y=0}^{p-2}\mathcal{N}\mathfrak{p}^{y\cdot(1-(p-1)\cdot s)}.$$

Hiermit kann bereits der Ausnahmefall bestätigt werden, denn im Fall $G=Z_p$ und $s=a(Z_p)$ gilt

$$\Phi(\mathcal{O}_\mathfrak{p}^\times,Z_p;a(Z_p)) = \frac{\mathcal{N}\mathfrak{p}-1}{p-1}\cdot\left(1-\mathcal{N}\mathfrak{p}^{-1}\right)^{-1}\cdot\mathcal{N}\mathfrak{p}^{-2}\cdot\sum_{y=0}^{p-2}1 = \mathcal{N}\mathfrak{p}^{-1}.$$

Für alle anderen Fälle ist entweder $G\neq Z_p$ oder $s>a(G)$. Ich untersuche die Funktionen $f(\boldsymbol{G};s)$ und $g(\boldsymbol{G},\mathcal{I};s)$ auf ihre $\mathcal{N}\mathfrak{p}$-Exponenten. Nach Beispiel 2.32 gelten

$$f(\boldsymbol{G};s) = \prod_{i=1}^{n}(1-\mathcal{N}\mathfrak{p}^{\bar{\beta}_i(s)})$$

und

$$\frac{g(\boldsymbol{G},\mathcal{I};s)}{p} = \frac{(\mathcal{N}\mathfrak{p}-1)^{r(\mathcal{I})}}{p-1}\cdot\mathcal{N}\mathfrak{p}^{-(p^n-1)\cdot s}\cdot\prod{}'\left(\mathcal{N}\mathfrak{p}^{-p^{i-1}(p-1)\cdot s+\bar\beta_{i+1}(s)}\cdot\sum_{y=0}^{p-1}\mathcal{N}\mathfrak{p}^{y\cdot\bar\gamma_i(s)}\right)$$
$$\cdot\prod{}''(1-\mathcal{N}\mathfrak{p}^{\bar\beta_i(s)}),$$

wobei das Produkt $\prod'$ über alle Indizes $1\le i\le n$ mit Elementarfamilie $\mathcal{J}_i=\mathcal{J}^n_{i,i-1}$ und das Produkt $\prod''$ über alle Indizes $1\le i\le n$ mit Elementarfamilie $\mathcal{J}_i=\mathcal{K}^n_{i,i-1}$ läuft. Nach Beispiel 2.31 gilt

$$\bar\beta_i(s)=\sum_{j=i}^{n}p^{j-i}\cdot((p-1)-(p^j-p^{j-1})\cdot p\cdot s)=(p-1)\cdot\sum_{j=i}^{n}p^{j-i}\cdot(1-p^j\cdot s)$$
$$=(p-1)\cdot\sum_{k=0}^{n-i}p^k-(p-1)\cdot p^i\cdot\sum_{k=0}^{n-i}p^{2k}\cdot s=-1+p^{n-i+1}-p^i\cdot\sum_{j=0}^{n-i}p^{2j}\cdot(p-1)\cdot s$$

und somit ist diese Funktion linear fallend. Der Wertebereich für $s>a(G)=1/(p^n-p^{n-1})=p^{1-n}/(p-1)$ ist also durch $\bar\beta_i(a(G))$ strikt nach oben beschränkt und es gelten

$$\bar\beta_n(a(G))=-1+p-p^n\cdot(p-1)\cdot(p^n-p^{n-1})^{-1}=-1$$

sowie

$$\bar\beta_i(a(G))=-1+p^{n-i+1}-p^i\cdot\sum_{j=0}^{n-i}p^{2j}\cdot p^{1-n}=-1-p^i\cdot\sum_{j=0}^{n-i-1}p^{2j}\cdot p^{1-n}<-1$$

im Fall $i\ne n$. Die Funktionen $\bar\gamma_i(s)$ sind ebenfalls linear fallend und es gilt nach Beispiel 2.31

$$\bar\gamma_i(a(G))=1-(p^i-p^{i-1})\cdot a(G)+\bar\beta_{i+1}(a(G))<-(p^i-p^{i-1})\cdot a(G)<0$$

für $i\ne n$. Für $i=n$ ist zubeachten, dass $\bar\beta_{n+1}(s)$ nicht definiert ist und durch 0 zu ersetzen ist. Dann ist

$$\bar\gamma_n(a(G))=1-(p^n-p^{n-1})\cdot a(G)=0$$

ersichtlich. Folglich hat der höchste $\mathcal{N}\mathfrak{p}$-Exponent $e_\mathfrak{p}(s)$ von $g(\boldsymbol{G},\mathcal{I};s)$ die Gestalt

$$e_\mathfrak{p}(s)=r(\mathcal{I})-(p^n-1)\cdot s+\sum{}'\left(\bar\beta_{i+1}(s)-(p^i-p^{i-1})\cdot s\right)$$

und dieser ist ebenfalls linear fallend. Hierbei ist in der Summe $\sum'$ die Einschränkung des Laufindex wie in $\prod'$ gegeben. Definitionsgemäß ist $r(\mathcal{I})=\sum' r_i=\sum' 1$, wie mit Satz 2.9 oder Beispiel 2.21 abgeglichen werden kann. Somit gilt

$$e_\mathfrak{p}(s)\le e_\mathfrak{p}(a(G))=-(p^n-1)\cdot a(G)+\sum{}'\left(1+\bar\beta_{i+1}(a(G))-(p^i-p^{i-1})\cdot a(G)\right). \tag{3.13.2}$$

Da der Fall $G=Z_p$ und $s=a(Z_p)=1/(p-1)$ bereits oben abgehandelt ist, kann dieser ignoriert werden. Folglich ist der erste Summand von $e_\mathfrak{p}(a(G))$ stets strikt kleiner als -1. Für den zweiten Summanden von 3.13.2 gilt

$$\sum{}'\left(1+\bar\beta_{i+1}(a(G))-(p^i-p^{i-1})\cdot a(G)\right)\le\sum_{i\ne n}{}'(1+\bar\beta_{i+1}(a(G)))+\sum_{i=n}{}'(1-(p^n-p^{n-1})\cdot a(G)),$$

wobei die Summen $\sum'$ auf der rechten Seite noch weiter auf die angezeigten Indizes eingeschränkt seien. Der Abschätzung $\bar{\beta}_i(a(G)) \leq -1$ zufolge ist der zweite Summand von `3.13.2` also nicht positiv und es gelten

$$e_{\mathfrak{p}}(s) \leq e_{\mathfrak{p}}(a(G)) < -1 \qquad \text{und} \qquad \frac{g(\boldsymbol{G}, \mathcal{I}; s)}{p} = o\left(\mathcal{N}\mathfrak{p}^{-1}\right).$$

Die Funktion $f(\boldsymbol{G}, s)^{-1}$ ist das Produkt von nicht mehr als n Ausdrücken der Gestalt

$$\frac{1}{1 - \mathcal{N}\mathfrak{p}^{\bar{\beta}_i(s)}} \leq \frac{1}{1 - \mathcal{N}\mathfrak{p}^{-1}} = \frac{\mathcal{N}\mathfrak{p}}{\mathcal{N}\mathfrak{p} - 1} \leq 2.$$

Zusammengefasst gilt nach `3.13.1` die Abschätzung

$$\Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, G; s) = f(\boldsymbol{G}; s)^{-1} \cdot \sum_{b(\boldsymbol{G}, \mathcal{I}) \neq 0} \frac{g(\boldsymbol{G}, \mathcal{I}; s)}{p} = f(\boldsymbol{G}; s)^{-1} \cdot o\left(\mathcal{N}\mathfrak{p}^{-1}\right) \leq 2^n \cdot o\left(\mathcal{N}\mathfrak{p}^{-1}\right) = o\left(\mathcal{N}\mathfrak{p}^{-1}\right)$$

für $s \geq a(G)$ mit dem bereits abgehandelten Ausnahmefall $G = Z_p$ und $s = a(Z_p)$. □

Korollar 3.14. — *Die globale Dirichletreihe $\Phi(F, G; s)$ besitzt Konvergenzabszisse $a(G)$ und ist über ihrem Pol in $s = a(G)$ der Ordnung $b(F, G)$ hinaus holomorph fortsetzbar.*

Beweis. — Nach Bemerkung 3.12 folgt, dass die Konvergenzabszisse von $\Phi(F, G; s)$ von unten durch $a(G)$ abschätzbar ist. Es reicht also, $a(G)$ auch als obere Schranke zu realisieren. Nach Bemerkung A.3 ist $\Phi(F, G; s)$ in eine alternierende endliche Summe der Eulerprodukte $\Psi(F, H, S; (G : H) \cdot s; e)$ für $H \leq G$ zerlegbar. Die maximale ihrer Konvergenzabszissen wird also die gewünschte obere Schranke liefern. Wegen $|\Psi(F, G, S; s; e)| \leq |\Psi(F, G, S; s; 1)|$ reicht die Abszissenberechnung zu den Reihen $\Psi(F, G, S; s; 1)$. Da F und S für diesen Beweis nicht von Relevanz sein werden, nutze ich die abkürzenden Notationen

$$\Psi(G; s) = \Psi(F, G, S; s; 1) = \prod_{\mathfrak{p}} \Psi_{\mathfrak{p}}(G; s) \qquad \text{und} \qquad \Psi_{\mathfrak{p}}(G; s) = \Psi_{\mathfrak{p}}(F, G, S; s; 1)$$

für die Eulerfaktoren. Diese haben fast alle, nämlich außerhalb der endlichen Stellenmenge S, die Gestalt

$$\begin{aligned}
\Psi_{\mathfrak{p}}(G; s) &= 1 + \sum_{1 \neq H \leq G} \sum_{\mathcal{O}_{\mathfrak{p}}^{\times}/U \simeq H} \tau_{\mathfrak{p}}(U; 1) \cdot \mathcal{N}\mathfrak{d}(U)^{-(G:H) \cdot s} \\
&= 1 + \sum_{1 \neq H \leq G} \sum_{\mathcal{O}_{\mathfrak{p}}^{\times}/U \simeq H} (H : 1) \cdot (1 - p^{-1}) \cdot \mathcal{N}\mathfrak{d}(U)^{-(G:H) \cdot s} \\
&= 1 + \sum_{1 \neq H \leq G} (H : 1) \cdot (1 - p^{-1}) \cdot \Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, H; (G : H) \cdot s).
\end{aligned}$$

Da die endlich vielen Eulerfaktoren $\Psi_{\mathfrak{p}}(G; s)$ für $\mathfrak{p} \in S$ keinen Einfluß auf das Konvergenzverhalten in der Abszisse haben, werde ich im Folgenden die obige Gestalt für alle $\mathfrak{p}$ annehmen. Nun möchte ich nachweisen, dass $\Psi(G; s) = \prod_{\mathfrak{p}} \Psi_{\mathfrak{p}}(G; s)$ in $\Re(s) > a(G)$ konvergent ist. Als unendliches Produkt konvergiert die Funktion genau dann in s, wenn die unendliche Reihe

$$\begin{aligned}
&\sum_{\mathfrak{p}} \sum_{1 \neq H \leq G} (H : 1) \cdot (1 - p^{-1}) \cdot \Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, H; (G : H) \cdot s) \\
= &\sum_{1 \neq H \leq G} (H : 1) \cdot (1 - p^{-1}) \cdot \sum_{\mathfrak{p}} \Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, H; (G : H) \cdot s)
\end{aligned}$$

konvergiert. Nach Bemerkung 3.13 besitzt jeder der endlich vielen Teilsummanden die Abschätzung

$$\sum_{\mathfrak{p}} \Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, H; (G:H)\cdot s) \leq \sum_{\mathfrak{p}} o\left(\mathcal{N}\mathfrak{p}^{-1}\right) < \infty$$

für $s > a(G)$. Folglich hat $\Psi(G;s)$ eine $a(G)$ nicht überschreitende Abszisse und dies trifft somit auch auf $\Phi(F,G;s)$ zu. Mit der bereits bekannten unteren Schranke ist $a(G)$ also tatsächlich die Konvergenzabszisse von $\Phi(F,G;s)$.

Als letzten Schritt ist die Frage nach der meromorphen Fortsetzbarkeit von $\Phi(F,G;s)$ zu beantworten. Dazu weise ich zunächst nach, dass $\Upsilon(G;s) = \Psi(G;s)\cdot\Psi(Z_p;(G:Z_p)\cdot s)^{-1}$ holomorph in einem $\Re(s) \geq a(G)$ umfassenden Gebiet ist, woraus die Holomorphie von $\Phi(F,G;s)\cdot\Psi(Z_p;(G:Z_p)\cdot s)^{-1}$ in einem solchen folgt. Denn ist $\Upsilon(G;S)$ konvergent, so auch

$$\left|\frac{\Psi(F,G,S;s;e)}{\Psi(F,Z_p;s)}\right| = \frac{|\Psi(F,G,S;s;e)|}{|\Psi(F,Z_p;s)|} \leq \frac{|\Psi(F,G,S;s;1)|}{|\Psi(F,Z_p;s)|} = |\Upsilon(G;s)|$$

für die endlichen vielen Summanden $\Psi(F,G,S;s;e)$ von $\Phi(F,G;s)$. Wegen $a(G) = a(H)/(G:H)$ haben die Eulerfaktoren $\Psi_{\mathfrak{p}}(G;a(G))$ die Gestalt

$$\Psi_{\mathfrak{p}}(a(G)) = 1 + \sum_{1\neq H\leq G} (H:1)\cdot(1-p^{-1})\cdot\Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, H; a(H)).$$

Weiter folgt nach Bemerkung 3.13

$$\Psi_{\mathfrak{p}}(G;a(G)) = 1 + (p-1)\cdot\mathcal{N}\mathfrak{p}^{-1} + \sum_{1,Z_p\neq H\leq G} (H:1)\cdot(1-p^{-1})\cdot\Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, H; a(H)).$$

Hieraus ergeben sich für die Eulerfaktoren $\Upsilon_{\mathfrak{p}}(s)$ der fraglichen Funktion

$$\begin{aligned}\Upsilon_{\mathfrak{p}}(a(G)) &= \frac{\Psi_{\mathfrak{p}}(G;a(G))}{\Psi_{\mathfrak{p}}(Z_p;a(Z_p))} = 1 + \sum_{1,Z_p\neq H\leq G} \frac{(H:1)\cdot(1-p^{-1})\cdot\Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, H; a(H))}{1+(p-1)\cdot\mathcal{N}\mathfrak{p}^{-1}} \\ &= 1 + \frac{o\left(\mathcal{N}\mathfrak{p}^{-1}\right)}{1+(p-1)\cdot\mathcal{N}\mathfrak{p}^{-1}}.\end{aligned}$$

Hier ist $1/(1+(p-1)\cdot\mathcal{N}\mathfrak{p}^{-1}) = \mathcal{N}\mathfrak{p}/(\mathcal{N}\mathfrak{p}+p-1)$ nach oben durch 1 abschätzbar und folglich ist das Eulerprodukt $\Upsilon(s) = \prod_{\mathfrak{p}}\Upsilon_{\mathfrak{p}}(s)$ konvergent in $s = a(G)$. Damit hat $\Upsilon(s)$ eine Abszisse strikt kleiner als $a(G)$ und ist folglich holomorph in einem $\Re(s) \geq a(G)$ umfassendem Gebiet. Auf Grund der Identität

$$\Psi_{\mathfrak{p}}(Z_p;s) = 1 + (p-1)\cdot\Phi(\mathcal{O}_{\mathfrak{p}}^{\times}, Z_p; s) = 1 + (\mathcal{N}\mathfrak{p}-1)\cdot\sum_{p\nmid m}\mathcal{N}\mathfrak{p}^{m-1-\lfloor\frac{m-1}{p}\rfloor-(m+1)\cdot(p-1)\cdot s} = \Phi_{\mathfrak{p}}(s)$$

mit dem Eulerfaktor $\Phi_{\mathfrak{p}}(s)$ der Funktion $\Phi(s) = \prod_{\mathfrak{p}}\Phi_{\mathfrak{p}}(s)$ aus Korollar 3.8 hat $\Psi(Z_p;(G:Z_p)\cdot s)$ in $s = a(G)$ einen Pol der Ordnung $p-1 = b(F,G)$. Somit ist dies auch für $\Phi(F,G;s)$ der Fall. □

KAPITEL 4

ASYMPTOTIK EINFACHER ZYKLISCHER ERWEITERUNGEN

In diesem Kapitel berechne ich die Konstante $c(F,G)$ einfacher zyklischer Erweiterungen beliebiger globaler Körper, deren Charakteristik $p \geq 0$ nicht mit der Gruppenordnung $\ell = (G:1)$ übereinstimmt. Ein auf Zahlkörper eingeschränktes Resultat wurde hierfür bereits von Cohen et al. (2002) präsentiert. Ihre Methodik der arithmetischen und expliziten Kummertheorie lässt sich für den Fall $p \neq \ell$ ohne Weiteres auch auf Funktionenkörper übertragen und im Gegensatz zur Originalarbeit entfallen dabei die klassenkörpertheoretischen Berechnungen. In den folgenden Zeilen stelle ich aber einen erheblich kürzeren Beweisweg vor, der im Wesentlichen die bekannten Ergebnisse von Wright (1989) und ihre spezielle Anwendung ausnutzt. Für Funktionenkörper mit Charakteristik $p = \ell$ habe ich den Wert $c(F,Z_p)$ in Zusatz 3.2 bereits separat berechnet und bis auf kleinere Fallunterscheidungen kann diese in Analogie mit der Allgemeinheit angesehen werden.

Satz 4.1. — *Es seien F ein beliebiger globaler Körper der Charakteristik $p \geq 0$ und ℓ eine Primzahl. Des Weiteren seien $\tilde{F}$ die Erweiterung von F mit primitiven ℓ-ten Einheitswurzeln*[(1)] *und $\tilde{F}_d$ dessen Teilkörper vom Index $d = [\tilde{F} : \tilde{F}_d]$. Der Erweiterungsgrad $[\tilde{F} : F]$ sei mit n und der Komplementärgrad $(\ell-1)/n$ mit b angegeben. Die Mengen V und Z seien die Mengen der in $\tilde{F}/F$ verzweigten bzw. vollständig zerlegten Stellen. Die Gruppe $G = Z_\ell$ hat über F die Verteilung*

$$Z(F,G;x) \sim c(F,G) \cdot x^{a(G)} \cdot \log(x)^{b-1}$$

mit einer explizit berechenbaren Konstante $c(F,G)$ der Form

$$c(F,G) = \frac{\ell \cdot (F^\times[\ell] : 1)^{-1}}{(\ell-1) \cdot (b-1)! \cdot (\ell-1)^b} \cdot t_p \cdot c_{p,\ell} \cdot c_\ell \cdot c_\infty \cdot \lim_{s \to 1} (s-1)^b \cdot \prod_{\mathfrak{p} \in Z} (1 + (\ell-1) \cdot \mathcal{N}\mathfrak{p}^{-s}).$$

(1) Für $\ell = p$ ist hier die Interpretation der 1 als primitive p-te Einheitswurzel und die Gleichsetzung $\tilde{F} = F$ sinnvoll.

Die Bedeutung des Ausdrucks $t_p \cdot c_{p,\ell} \cdot c_\ell \cdot c_\infty$ sowie seiner unterschiedlichen Werte für Funktionen- und Zahlkörpern ist in den folgenden Aussagen (a) und (b) entschlüsselt. Der auftretende Grenzwert ist

$$\left(\operatorname{Res}_{s=1}(\zeta_{\tilde{F}}(s)) \cdot \prod_{1\neq d|n} \zeta_{\tilde{F}_d}(d)^{\mu(d)}\right)^b \cdot \prod_{\mathfrak{p}\in Z}(1+(\ell-1)\cdot \mathcal{N}\mathfrak{p}^{-1}) \prod_{d|n}(1-\mathcal{N}\mathfrak{p}^{-d})^{\mu(d)(\ell-1)/d}$$
$$\cdot \prod_{\mathfrak{p}\in V}\prod_{d|n}\prod_{\mathfrak{p}_d|\mathfrak{p}}(1-\mathcal{N}\mathfrak{p}_d^{-d})^{-\mu(d)b}.$$

(a) *Für Funktionenkörper mit Konstantengröße q gelten $c_\ell = c_\infty = 1$ und $t_p = d\cdot\log(q)$. Hierbei ist d der Grenzwert der Folge $d_m = \sum_{k\leq m} q^{(k-m)/(\ell-1)}(k/m)^b$ und* log *der natürliche Logarithmus. Des Weiteren ist $c_{p,\ell} = 1/((p-2)!\cdot p)$ für $p = \ell \neq 2$ und $c_{p,\ell} = 1$ sonst.*

(b) *Für Zahlkörper mit Signatur (r_1, r_2) gelten im Einzelnen $t_p = c_{p,\ell} = 1$ sowie $c_\infty = 2^{-r_2}$ für $\ell = 2$ und $c_\infty = \ell^{-(r_1+r_2)}$ sonst. Die Konstante c_ℓ ist durch*

$$c_\ell = \prod_{\mathfrak{p}|\ell,\mathfrak{p}\notin Z}\left(1+(\ell-1)\cdot\mathcal{N}\mathfrak{p}^{-1} - \frac{\ell-1-r_\mathfrak{p}\cdot(1-\mathcal{N}\mathfrak{p}^{-1})}{\mathcal{N}\mathfrak{p}^{e_\mathfrak{p}+1}}\right)$$

mit $e(\mathfrak{p}|\ell) = e_\mathfrak{p}\cdot(\ell-1)+r_\mathfrak{p}$ und $0\leq r_\mathfrak{p}\leq \ell-2$ gegeben.

Insbesondere ergibt sich hieraus folgendes schöne klassische Resultat.

Korollar 4.2. — *Die Verteilung der quadratischen Erweiterungen eines globales Körpers ist*

$$Z(F, Z_2; x) \sim \frac{\operatorname{Res}_{s=1}(\zeta_F(s))}{\zeta_F(2)} \cdot t_p \cdot c_\infty \cdot x.$$

Beweis. — In diesem Fall ist $n = [\tilde{F} : F] = 1 = n/(\ell-1) = b$ und $c_{p,\ell} = 1$. Die Stellenmenge Z stimmt mit der Gesamtmenge von Stellen in F überein und daher ist auch $c_2 = 1$ und es folgt

$$c(F, Z_2) = t_p \cdot c_\infty \cdot \lim_{s\to 1}(s-1)\cdot\prod_\mathfrak{p}(1+\mathcal{N}\mathfrak{p}^{-s}).$$

Das Eulerprodukt stimmt mit $\zeta_F(s)/\zeta_F(2s)$ überein und hieraus ergibt sich die behauptete Formel. □

Schlachtplan. — Für den Fall $\ell = p$ habe ich dieses Ergebnis bereits in Kapitel 3 bewiesen. Für $\ell \neq p$ wird im Folgenden die Dirichletreihe $\Phi(F, G; s)$ genau untersucht. Die Lage $s = a(G)$ und Ordnung $b = b(F, G)$ des Pols in ihrer Konvergenzabszisse ergibt sich nebenbei. Entscheidend ist der Grenzwert $c(\Phi(F, G; s)) = \lim_{s\to a}(s-a)^b\cdot\Phi(F, G; s)$, mit welchem die Konstante $c(F, G)$ nach dem Taubersatz bestimmt werden kann. Durch die Zerlegung von $\Phi(F, G; s)$ nach Wright ergibt sich der Grenzwert durch ein einziges Eulerprodukt $\Psi(F, G, S; s; \bar{1})$, dessen lokalen Faktoren berechnet werden müssen.

4.1. Asymptotik einfacher zyklischer Erweiterungen globaler Körper

Nach Bemerkung A.3 ist $\Phi(F, G; s)$ in

$$\Phi(F, G; s) = \frac{1}{\ell-1}\cdot(\Psi(F, G; s) - \Psi(F, 1; \ell\cdot s)) = \frac{1}{\ell-1}\cdot(\Psi(F, G; s) - 1)$$

zerlegbar. Es sei nun S eine endliche Stellenmenge inklusive aller archimedischen Stellen S_∞ mit $\langle \mathcal{A}_S^\times, F^\times \rangle = \mathcal{A}_F^\times$, d.h. S ist groß genug, um die Klassengruppe zu erzeugen. Zur Vermeidung müßiger Fallunterscheidungen nehme ich zusätzlich an, dass S keine Trägerstellen von ℓ enthält. Dann gilt weiter nach Bemerkung A.3

$$\begin{aligned}\Psi(F,G;s) &= (\mathcal{O}_S^\times : \mathcal{O}_S^\ell)^{-1} \cdot \sum_{\bar{z}\in\mathcal{O}_S^\times/\mathcal{O}_S^\ell} \sum_{\chi\in C(\mathcal{A}_S^\times)[\ell]} \chi(\bar{z}) \cdot \mathcal{N}\mathfrak{f}_G(\chi)^{-s} \\ &= (\mathcal{O}_S^\times : \mathcal{O}_S^\ell)^{-1} \cdot \sum_{\bar{z}\in\mathcal{O}_S^\times/\mathcal{O}_S^\ell} \Psi(F,G,S;s;\bar{z}).\end{aligned}$$

Der Faktor $(\mathcal{O}_S^\times : \mathcal{O}_S^\ell)$ hat nach Dirichlets Einheitensatz den Wert

$$(\mathcal{O}_S^\times : \mathcal{O}_S^\ell) = (F^\times[\ell] : 1) \cdot \ell^{|S\setminus S_\infty|+r_1+r_2-1}$$

und es ergibt sich

$$\Phi(F,G;s) = -\frac{1}{\ell-1} + \frac{\ell\cdot(F^\times[\ell]:1)^{-1}}{\ell-1} \cdot \sum_{\bar{z}\in\mathcal{O}_S^\times/\mathcal{O}_S^\ell} \ell^{-(r_1+r_2)} \cdot \ell^{-|S\setminus S_\infty|} \cdot \Psi(F,G,S;s;\bar{z}).$$

Die Funktion $\Psi(F,G,S;s;\bar{z})$ ist weiter nach Bemerkung A.3 ein Eulerprodukt

$$\Psi(F,G,S;s;\bar{z}) = \prod_{\mathfrak{p}} \Psi_{\mathfrak{p}}(F,G,S;s;\bar{z})$$

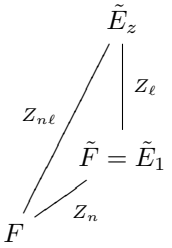
mit Eulerfaktoren

(4.1.1) $$\Psi_{\mathfrak{p}}(F,G,S;s;\bar{z}) = 1 + \sum_{X_{\mathfrak{p}}/U\simeq G} \tau_{\mathfrak{p}}(U;\bar{z}) \cdot \mathcal{N}\mathfrak{d}(U)^{-s}$$

und Koeffizienten

(4.1.2) $$\tau_{\mathfrak{p}}(U;\bar{z}) = \begin{cases} -1 & z_{\mathfrak{p}} \notin U \\ \ell-1 & z_{\mathfrak{p}} \in U. \end{cases}$$

Die Wahl der $\mathfrak{p}$-Komponente $z_{\mathfrak{p}} \in F_{\mathfrak{p}}^\times$ der S-Einheitenklasse $\bar{z} \in \mathcal{O}_S^\times/\mathcal{O}_S^\ell$ ist hierbei nicht von Relevanz. Nach Wright (1989, Prop. 4.2.) hängt der von $\tau_{\mathfrak{p}}(U;\bar{z})$ angenommene Wert nur vom Artinsymbol $(\tilde{E}_z/F,\mathfrak{p})$ der Erweiterung $\tilde{E}_z = \tilde{F}(\sqrt[\ell]{z})$ über F ab. Diese Erweiterung ist zyklisch vom Grad $n\ell$ für $\bar{z} \neq \bar{1}$ und vom Grad n für $\bar{z} = \bar{1}$. Im Folgenden möchte ich mit $T_k(\bar{z})$ die Menge der Stellen mit Artinsymbol von der Ordnung k bezeichnen. Zudem sei $T(\bar{z})$ die Vereinigung aller $T_k(\bar{z})$ mit $k \neq 1, \ell$.



Körperdiagramm für $\tilde{E}_z/F$ bei $\bar{z} \neq \bar{1}$

Bemerkung 4.3. — (a) *Die zu den nichtarchimedischen Stellen $\mathfrak{p} \nmid \ell$ gehörenden Eulerfaktoren von $\Psi(F, G, S; s; \bar{z})$ haben die Gestalt*

$$\Psi_{\mathfrak{p}}(F, G, S; s; \bar{z}) = \begin{cases} 0 & \mathfrak{p} \in S,\ \operatorname{ord}_{\mathfrak{p}}(z_{\mathfrak{p}}) \not\equiv 0 \pmod{\ell} \\ (1 + \tau_{\mathfrak{p}}(\bar{z}) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s}) \cdot \ell & \mathfrak{p} \in S,\ \operatorname{ord}_{\mathfrak{p}}(z_{\mathfrak{p}}) \equiv 0 \pmod{\ell} \\ (1 + \tau_{\mathfrak{p}}(\bar{z}) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s}) & \mathfrak{p} \notin S \end{cases}$$

mit Koeffizienten

$$\tau_{\mathfrak{p}}(\bar{z}) = \begin{cases} 0 & \mathfrak{p} \in T(\bar{z}) \\ -1 & \mathfrak{p} \in T_{\ell}(\bar{z}) \\ \ell - 1 & \mathfrak{p} \in T_1(\bar{z}). \end{cases}$$

(b) *Für die über ℓ liegenden Stellen $\mathfrak{p}$ gibt es eine in $\Re(s) \geq a(G)$ holomorphe Funktion $g(s; \bar{z})$ mit $g(a(G); \bar{1}) = 1$, sodass das Produkt der $\Psi_{\mathfrak{p}}(F, G, S; s; \bar{z})$ über alle Stellen $\mathfrak{p} \mid \ell$ die Gestalt*

$$\prod_{\mathfrak{p}|\ell} \Psi_{\mathfrak{p}}(F, G, S; s; \bar{z}) = \prod_{\mathfrak{p}|\ell, \mathfrak{p} \in Z} (1 + (\ell - 1) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s}) \cdot c_{\ell} \cdot g(s; \bar{z})$$

besitzt.

(c) *Es seien $\bar{z} = \bar{1}$ die triviale S-Einheitenklasse und r_1 die Anzahl der reellen Bewertungen von F. Dann gilt für das endliche Produkt der $\Psi_{\mathfrak{p}}(F, G, S; s; \bar{z})$ über allen archimedischen Bewertungen*

$$\prod_{\mathfrak{p}|\infty} \Psi_{\mathfrak{p}}(F, G, S; s; \bar{1}) = c_{\infty} \cdot \ell^{r_1 + r_2} = \begin{cases} 2^{r_1} & \ell = 2 \\ 1 & \textit{sonst.} \end{cases}$$

Beweis. — (a) Zunächst sei $\mathfrak{p} \nmid \ell$ stets aus dem Komplement zu S gewählt. Dann ist $X_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}}^{\times}$ und höchstens die Gruppe $U = \mathbb{F}_{\mathfrak{p}}^{\ell} \times \langle 1 + \mathfrak{p} \rangle$ hat Kokern G. Im Fall $\mathfrak{p} \in T(\bar{z})$ ist $\mathfrak{p}$ nicht vollständig zerlegt in $\tilde{F}/F$ und folglich ist $\mathbb{F}_{\mathfrak{p}}^{\times}$ nicht im Besitz primitiver ℓ-ter Einheitswurzeln und es gilt $\mathbb{F}_{\mathfrak{p}}^{\ell} = \mathbb{F}_{\mathfrak{p}}^{\times}$. Hieraus ergibt sich $\mathcal{O}_{\mathfrak{p}}^{\times}/U \simeq 1$ und wie behauptet $\Psi_{\mathfrak{p}}(F, G, S; s; \bar{z}) = 1$ für $\mathfrak{p} \in T(\bar{z})$ und $\mathfrak{p} \notin S$, d.h. es gilt $\tau_{\mathfrak{p}}(\bar{z}) = 0$ für $\mathfrak{p} \in T(\bar{z}) \setminus S$. Im Fall $\mathfrak{p} \in T_1(\bar{z}) \cup T_{\ell}(\bar{z})$ ist $\mathfrak{p}$ hingegen vollständig zerlegt in $\tilde{F}/F$ und U besitzt auf Grund $\mathbb{F}_{\mathfrak{p}}^{\ell} \neq \mathbb{F}_{\mathfrak{p}}$ tatsächlich Faktorgruppe G. Die Diskriminante von U ist $\mathfrak{d}(U) = \mathfrak{p}^{\ell-1}$ und es gilt nach `4.1.1`

$$\Psi_{\mathfrak{p}}(F, G, S; s; \bar{z}) = 1 + \tau_{\mathfrak{p}}(U, \bar{z}) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s}.$$

Nun ist noch $\tau_{\mathfrak{p}}(U; \bar{z}) = \tau_{\mathfrak{p}}(\bar{z})$ zu zeigen. Die Komponente $z_{\mathfrak{p}}$ ist genau dann in $U \leq \mathcal{O}_{\mathfrak{p}}^{\ell}$ enthalten, wenn $z_{\mathfrak{p}}$ eine ℓ-te Potenz ist. Diese Bedingung ist gleichbedeutend mit der vollständigen Zerlegung auch in $\tilde{E}_z/\tilde{F}$ und somit zur Zugehörigkeit zu $T_1(\bar{z})$. Hieraus ergeben sich $\tau_{\mathfrak{p}}(U; \bar{z}) = \tau_{\mathfrak{p}}(\bar{z})$ aus `4.1.2` und $\tau_{\mathfrak{p}}(\bar{z}) = \ell - 1$ für $\mathfrak{p} \in T_1(\bar{z}) \setminus S$ sowie $\tau_{\mathfrak{p}}(\bar{z}) = -1$ für $\mathfrak{p} \in T_{\ell}(\bar{z}) \setminus S$. Damit ist der Beweis für den Fall $\mathfrak{p} \notin S$ vervollständigt.

Nun sei $\mathfrak{p} \nmid \ell$ stets aus S gewählt. Dann ist $X_{\mathfrak{p}} = F_{\mathfrak{p}}^{\times} \simeq \mathbf{Z} \times \mathcal{O}_{\mathfrak{p}}^{\times}$ und alle Untergruppen $U \leq F_{\mathfrak{p}}^{\times}$ vom Index ℓ enthalten die offene Gruppe $W = \ell\mathbf{Z} \times \mathbb{F}_{\mathfrak{p}}^{\ell} \times \langle 1 + \mathfrak{p} \rangle$. Unter diesen korrespondiert die Gruppe $V = \ell\mathbf{Z} \times \mathcal{O}_{\mathfrak{p}}^{\times}$ zu der unverzweigten Erweiterung von $F_{\mathfrak{p}}$ mit Grad ℓ und $z_{\mathfrak{p}}$ ist genau dann in V enthalten, wenn $\operatorname{ord}_{\mathfrak{p}}(z) \equiv 0 \pmod{\ell}$ gilt. Ist $\mathfrak{p}$ eine Stelle aus $T(\bar{z})$, gibt es keine weiteren Untergruppen vom Index

ℓ und es gilt $\Psi_{\mathfrak{p}}(F,G,S;s;\bar{z}) = 1+\tau_{\mathfrak{p}}(V;\bar{z}) \in \{0,\ell\}$ in Abhängigkeit nur von $\mathrm{ord}_{\mathfrak{p}}(z) \pmod{\ell}$. Das zeigt also $\tau_{\mathfrak{p}}(\bar{z}) = 0$ auch für $\mathfrak{p} \in T(\bar{z}) \cap S$. Ist $\mathfrak{p}$ in $T_1(\bar{z})$ oder $T_\ell(\bar{z})$ enthalten, so gibt es ℓ weitere Untergruppen von $F_{\mathfrak{p}}^{\times}$ mit Index ℓ und Diskriminante $\mathfrak{p}^{\ell-1}$. Im Fall $\mathfrak{p} \in T_1(\bar{z})$ ist $z_{\mathfrak{p}}$ als ℓ-Potenz in W und somit in allen Untergruppen vom Index ℓ enthalten und es gilt nach `4.1.1`

$$\Psi_{\mathfrak{p}}(F,G,S;s;\bar{z}) = 1+(\ell-1)\cdot\mathcal{N}\mathfrak{p}^0+\ell\cdot(\ell-1)\cdot\mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s} = \ell\cdot(1+(\ell-1)\cdot\mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s}).$$

Das zeigt insbesondere $\tau_{\mathfrak{p}}(\bar{z}) = \ell-1$ für $\mathfrak{p} \in T_1(\bar{z}) \cap S$. Im Fall $\mathfrak{p} \in T_\ell(\bar{z})$ ist $z_{\mathfrak{p}}$ keine ℓ-te Potenz. Es gilt also $z_{\mathfrak{p}} \notin W$ und folglich gibt es genau eine Untergruppe U mit $z_{\mathfrak{p}} \in U$. Ist diese genau V, so ist $\mathrm{ord}_{\mathfrak{p}}(z_{\mathfrak{p}}) \equiv 0 \pmod{\ell}$ und es gilt

$$\Psi_{\mathfrak{p}}(F,G,S;s;\bar{z}) = 1+(\ell-1)\cdot\mathcal{N}\mathfrak{p}^0+\ell\cdot(-1)\cdot\mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s} = \ell\cdot(1-\mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s}).$$

Ist U jedoch ungleich V, so gelten $\mathrm{ord}_{\mathfrak{p}}(z_{\mathfrak{p}}) \not\equiv 0 \pmod{\ell}$ und

$$\Psi_{\mathfrak{p}}(F,G,S;s;\bar{z}) = 1-1\cdot\mathcal{N}\mathfrak{p}^0+(\ell-1)\cdot\mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s}+(\ell-1)\cdot(-1)\cdot\mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s} = 0.$$

Das zeigt insbesondere $\tau_{\mathfrak{p}}(\bar{z}) = -1$ für $\mathfrak{p} \in T_\ell(\bar{z}) \cap S$.

(b) Es seien nun $\mathfrak{p}$ eine Stelle über ℓ und $X_m = \mathcal{O}_{\mathfrak{p}}^{\times}/\langle \mathbb{F}_{\mathfrak{p}}^{\times}, 1+\mathfrak{p}^{m+1}\rangle$. Nach Hasses Einseinheitensatz ist der ℓ-Rang dieser Gruppen bei steigendem m stationär und es gilt nach Korollar C.3 Fall (b)

$$a_m = (X_m : X_m^{\ell}) = \begin{cases} \mathcal{N}\mathfrak{p}^{m-\lfloor \frac{m}{\ell} \rfloor} & 0 \le m < e(\mathfrak{p}|\ell)+e_{\mathfrak{p}} \\ \mathcal{N}\mathfrak{p}^{e(\mathfrak{p}|\ell)}\cdot(F_{\mathfrak{p}}^{\times}[\ell]:1) & m \ge e(\mathfrak{p}|\ell)+e_{\mathfrak{p}}. \end{cases}$$

Die Anzahl der Untergruppen in $U \le X_m$ mit Diskriminante $\mathcal{N}\mathfrak{d}(U) = \mathcal{N}\mathfrak{p}^{(m+1)\cdot(\ell-1)}$ beträgt genau $(a_m - a_{m-1})/(\ell-1)$ und alle solche Untergruppen besitzen den Koeffizienten $\tau_{\mathfrak{p}}(U;\bar{1}) = (\ell-1)$. Folglich besitzt der Eulerfaktor zu $\mathfrak{p}$ die Gestalt[(2)]

$$\Psi_{\mathfrak{p}}(F,G,S;s;\bar{1}) = 1+\sum_{m=1}^{e+e_{\mathfrak{p}}}(a_m-a_{m-1})\cdot\mathcal{N}\mathfrak{p}^{-(m+1)\cdot(\ell-1)\cdot s}.$$

Diese Funktion ist offensichtlich ganz und folglich ist für den Nachweis der behaupteten Gestalt lediglich der Wert bei $s = a(G)$ auszurechnen. Analog zu den lokalen Reihen von p-Erweiterungen in positiver Charakteristik kann dieser Eulerfaktor mit Hilfe des Lemma 2.26 auf eine angenehmere Form gebracht werden. Mit den linearen Funktionen $\beta(s) = (\ell-1)\cdot(1-\ell\cdot s)$ und $\gamma(s) = 1-(\ell-1)\cdot s$ ergibt sich hier unter Beachtung von $e+e_{\mathfrak{p}} = \ell\cdot e_{\mathfrak{p}}+r_{\mathfrak{p}}$ die Umformung

$$\begin{aligned}\Psi_{\mathfrak{p}}(F,G,S;s;\bar{1}) = 1 &+ (\mathcal{N}\mathfrak{p}-1)\cdot\sum_{x=0}^{e_{\mathfrak{p}}-1}\mathcal{N}\mathfrak{p}^{x\cdot\beta(s)}\sum_{y=0}^{\ell-2}\mathcal{N}\mathfrak{p}^{y\cdot\gamma(s)}\cdot\mathcal{N}\mathfrak{p}^{-2\cdot(\ell-1)\cdot s} \\ &+ (\mathcal{N}\mathfrak{p}-1)\cdot\mathcal{N}\mathfrak{p}^{e_{\mathfrak{p}}\cdot\beta(s)}\cdot\sum_{y=0}^{r_{\mathfrak{p}}-2}\mathcal{N}\mathfrak{p}^{y\cdot\gamma(s)}\cdot\mathcal{N}\mathfrak{p}^{-2\cdot(\ell-1)\cdot s} \\ &+ (a_{e+e_{\mathfrak{p}}}-a_{e+e_{\mathfrak{p}}-1})\cdot\mathcal{N}\mathfrak{p}^{-(e+e_{\mathfrak{p}}+1)\cdot(\ell-1)\cdot s},\end{aligned}$$

[(2)] Ich verwende hier e als abkürzenden Ausdruck für $e(\mathfrak{p}|\ell)$. Es gilt dann $e+e_{\mathfrak{p}} = \ell\cdot e_{\mathfrak{p}}+r_{\mathfrak{p}}$.

wobei die mittlere Summe bei $r_\mathfrak{p} = 0, 1$ durch den Wert 0 ersetzt sei. Eine Stelle $\mathfrak{p} \mid \ell$ ist genau dann in Z enthalten, wenn $(F_\mathfrak{p}^\times[\ell] : 1) = \ell$ und somit $r_\mathfrak{p} = 0$ gelten. Hieraus folgen $a_{e+e_\mathfrak{p}} - a_{e+e_\mathfrak{p}-1} = (\ell-1) \cdot \mathcal{N}\mathfrak{p}^e$ und

$$\Psi_\mathfrak{p}(F, G, S; a(G); \bar{1}) = 1 + (1 - \mathcal{N}\mathfrak{p}^{-e_\mathfrak{p}}) \cdot (\ell-1) \cdot \mathcal{N}\mathfrak{p}^{-1} + (\ell-1) \cdot \mathcal{N}\mathfrak{p}^{-e_\mathfrak{p}-1} = 1 + (\ell-1) \cdot \mathcal{N}\mathfrak{p}^{-1}.$$

Für die Stellen $\mathfrak{p}$ außerhalb Z ist hingegen $(F_\mathfrak{p}^\times[\ell] : 1) = 1$ und entweder $a_{e+e_\mathfrak{p}} = a_{e+e_\mathfrak{p}-1}$ im Fall $r_\mathfrak{p} = 0$ oder $a_{e+e_\mathfrak{p}} = a_{e+e_\mathfrak{p}-1} \cdot \mathcal{N}\mathfrak{p}$ erfüllt und es ergibt sich der Funktionswert

$$\begin{aligned}\Psi_\mathfrak{p}(F, G, S; a(G); \bar{1}) &= 1 + (\ell-1) \cdot (1 - \mathcal{N}\mathfrak{p}^{-e_\mathfrak{p}}) \cdot \mathcal{N}\mathfrak{p}^{-1} + (\mathcal{N}\mathfrak{p} - 1) \cdot \mathcal{N}\mathfrak{p}^{-e_\mathfrak{p}} \cdot r_\mathfrak{p} \cdot \mathcal{N}\mathfrak{p}^{-2} \\ &= 1 + (\ell-1) \cdot \mathcal{N}\mathfrak{p}^{-1} - \mathcal{N}\mathfrak{p}^{-e_\mathfrak{p}-1} \cdot ((\ell-1) - (1 - \mathcal{N}\mathfrak{p}^{-1}) \cdot r_\mathfrak{p}).\end{aligned}$$

Das Produkt dieser Werte ist identisch mit der im Hauptsatz definierten Konstanten c_ℓ, d.h. es gilt

$$c_\ell = \prod_{\mathfrak{p} \mid \ell, \mathfrak{p} \notin Z} \Psi_\mathfrak{p}(F, G, S; a(G); \bar{1}).$$

Nun setze ich

$$g(s; \bar{z}) = c_\ell^{-1} \cdot \prod_{\mathfrak{p} \mid \ell, \mathfrak{p} \in Z} (1 + (\ell-1) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1) \cdot s})^{-1} \cdot \prod_{\mathfrak{p} \mid \ell} \Psi_\mathfrak{p}(F, G, S; s; \bar{z}).$$

Mit dieser Funktion gelten wie behauptet

$$\prod_{\mathfrak{p} \mid \ell} \Psi_\mathfrak{p}(F, G, S; s; \bar{z}) = \prod_{\mathfrak{p} \mid \ell, \mathfrak{p} \in Z} (1 + (\ell-1) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1) \cdot s}) \cdot c_\ell \cdot g(s)$$

und $g(a(G), \bar{1}) = 1$. Die Funktion $g(s; \bar{z})$ ist als endliches Produkt rationaler Funktionen selbst rational und konvergent in einer Halbebene über $\Re(s) \geq a(G)$ hinaus.

(c) Für $\ell \neq 2$ gibt es keine offenen Untergruppen von $\mathbf{R}^\times$ oder $\mathbf{C}^\times$ vom Index ℓ. Im Fall $\ell = 2$ entspricht das angegebene Produkt genau dem Ausdruck (4.6) aus Wright (1989), welcher durch die dort folgende Berechnung mit 2^{r_1} beziffert wird. □

Bemerkung 4.4. — (a) *Es sei $\bar{z} = \bar{1}$ die triviale S-Einheitenklasse. Dann besitzt $\Psi(F, G, S; s; \bar{1})$ in $s = a(G)$ einen Pol der Ordnung b.*

(b) *Die Reihen $\Psi(F, G, S; s; \bar{z})$ sind für nichttriviale S-Einheitenklassen $\bar{z}$ holomorph in $s = a(G)$.*

Beweis. — Die Reihe $\Psi(F, G, S; s; \bar{z})$ ist genau dann ungleich 0, wenn global $\mathrm{ord}_\mathfrak{p}(z) \equiv 0 \pmod{\ell}$ erfüllt ist und in diesem Fall hat sie die Gestalt

$$\Psi(s; \bar{z}) = \Psi(F, G, S; s; \bar{z}) = \prod_{\mathfrak{p} \in T_1(\bar{z})} (1 + (\ell-1) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1) \cdot s}) \cdot \prod_{\mathfrak{p} \in T_\ell(\bar{z})} (1 - \mathcal{N}\mathfrak{p}^{-(\ell-1) \cdot s}) \cdot f(s; \bar{z})$$

wobei $f(s; \bar{z})$ eine in $\Re(s) \geq a(G)$ holomorphe Funktion mit dem für $\bar{z} = \bar{1}$ und $s = a(G)$ expliziten Wert

$$f(a(G); \bar{1}) = c_\ell \cdot c_\infty \cdot \ell^{r_1 + r_2} \cdot \ell^{|S \setminus S_\infty|}$$

ist. Für die triviale Klasse $\bar{z} = \bar{1}$ ist $T_\ell(\bar{z})$ leer und $T_1(\bar{z})$ stimmt mit den in $\tilde{F}/F$ vollständig zerlegten Stellen überein, d.h. es gilt $T_1(\bar{1}) = Z$. Dann hat $\Psi(s; \bar{1})$ nach Bemerkung E.3 einen Pol in $s =$

$a(G)$ von der Ordnung b und ist meromorph über die Abszissenachse fortsetzbar. Für nichttriviale S-Einheitenklassen $\bar{z}$ ist $\tilde{E}_z/\tilde{F}$ galoissch vom Grad ℓ. Ein Charakter χ von der Galoisgruppe $\mathrm{Gal}(\tilde{E}_z/\tilde{F})$ kann via dem Artinsymbol auf den Stellen aus $\tilde{F}$ definiert werden vermöge $\chi(\tilde{\mathfrak{p}}) = \chi((\tilde{E}_z/\tilde{F}, \tilde{\mathfrak{p}}))$. Ich betrachte nun das Produkt

$$L(s) = \prod_{\chi \neq 1} L(s;\chi) = \prod_{\tilde{\mathfrak{p}}} \prod_{\chi \neq 1} (1 + \chi(\tilde{\mathfrak{p}}) \cdot \mathcal{N}\tilde{\mathfrak{p}}^{-s}) = \prod_{\tilde{\mathfrak{p}}} \left(1 + \sum_{\chi \neq 1} \chi(\tilde{\mathfrak{p}}) \cdot \mathcal{N}\tilde{\mathfrak{p}}^{-s} + O\left(\mathcal{N}\tilde{\mathfrak{p}}^{-2\cdot s}\right) \right)$$

der L-Reihen nichttrivialer Charaktere χ von $\mathrm{Gal}(\tilde{E}_z/\tilde{F})$ über $\tilde{F}$. Es ist wohlbekannt, dass ein solches Produkt holomorph über die ganze komplexe Ebene ist. Nach der Orthogonalitätsrelation von Gruppen haben die Eulerfaktoren die Gestalt

$$L_{\tilde{\mathfrak{p}}}(s) = \begin{cases} (1 + (\ell - 1) \cdot \mathcal{N}\tilde{\mathfrak{p}}^{-s} + O\left(\mathcal{N}\tilde{\mathfrak{p}}^{-2\cdot s}\right)) & (\tilde{E}_z/\tilde{F}, \tilde{\mathfrak{p}}) = 1 \\ (1 - \mathcal{N}\tilde{\mathfrak{p}}^{-s} + O\left(\mathcal{N}\tilde{\mathfrak{p}}^{-2\cdot s}\right)) & \text{sonst.} \end{cases}$$

Da $\tilde{E}_z/F$ galoissch ist, besitzen alle Fortsetzungen $\tilde{\mathfrak{p}} \mid \mathfrak{p}$ von Stellen aus F das gleiche Artinsymbol $(\tilde{E}_z/\tilde{F}, \tilde{\mathfrak{p}})$ und es gilt

$$L_{\mathfrak{p}}(s) = \prod_{\tilde{\mathfrak{p}} \mid \mathfrak{p}} L_{\tilde{\mathfrak{p}}}(s) = \begin{cases} (1 + (\ell - 1) \cdot \mathcal{N}\mathfrak{p}^{-s} + O\left(\mathcal{N}\mathfrak{p}^{-2\cdot s}\right))^n & \mathfrak{p} \in T_1(\bar{z}) \subseteq Z \\ (1 - \mathcal{N}\mathfrak{p}^{-s} + O\left(\mathcal{N}\mathfrak{p}^{-2\cdot s}\right))^n & \mathfrak{p} \in T_\ell(\bar{z}) \subseteq Z \\ (1 + O\left(\mathcal{N}\mathfrak{p}^{-2\cdot s}\right)) & \text{sonst.} \end{cases}$$

Ist nämlich $\mathfrak{p}$ in $\tilde{F}/F$ nicht vollständig zerlegt, so besitzt $\mathfrak{p}$ den Trägheitsgrad $f_{\mathfrak{p}} \geq 2$ und es gilt $\mathcal{N}\tilde{\mathfrak{p}} = \mathcal{N}\mathfrak{p}^{f_{\mathfrak{p}}}$ für $\tilde{\mathfrak{p}} \mid \mathfrak{p}$. Das Produkt über diese trägen Stellen ist also konvergent und somit holomorph im Gebiet $\Re(s) > 1/2$ und auf Grund der Ganzheit von L trifft das selbe auch für das Produkt über Z zu, d.h.

$$L_Z(s) = \prod_{\mathfrak{p} \in Z} L_{\mathfrak{p}}(s) = L(s) \cdot \prod_{\mathfrak{p} \notin Z} L_{\mathfrak{p}}(s)^{-1}$$

ist holomorph für $\Re(s) > 1/2$. Hieraus ist die behauptete Holomorphie von $\Psi(s;\bar{z})$ ersichtlich. Für die Eulerfaktoren bzgl. $\mathfrak{p} \in Z$ von $\Psi(s;\bar{z})^n$ und $L_Z(s)$ gilt

$$\Psi_{\mathfrak{p}}(s;\bar{z})^n = L_{\mathfrak{p}}(s) \cdot \frac{(1 + (\ell - 1) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s})^n}{L_{\mathfrak{p}}(s)} = L_{\mathfrak{p}}(s) \cdot \left(1 + O\left(\mathcal{N}\mathfrak{p}^{-2(\ell-1)\cdot s}\right)\right)^{-n}$$

für $\mathfrak{p} \in T_1(\bar{z})$ und für $\mathfrak{p} \in T_\ell(\bar{z})$ die entsprechende Form. Die Konvergenzabszissen von $\Psi(s;\bar{z})$ und $\Psi(s;\bar{z})^n$ sind identisch und diese ist vermöge

$$\Psi(s;\bar{z})^n = L_Z((\ell - 1) \cdot s) \cdot \prod_{\mathfrak{p} \in Z} \left(1 + O\left(\mathcal{N}\mathfrak{p}^{-2(\ell-1)\cdot s}\right)\right)^{-n} \cdot f(s;\bar{z})^n$$

von der Größe $a(G)/2$ oder kleiner. □

Beweis von Satz 4.1. — Der Grenzwert von $\Phi(F, G; s)$ in $s = a(G)$ ist also nach obiger Bemerkung nur vom Eulerprodukt $\Psi(F, G, S; s; \bar{1})$ abhängig und es gilt

$$\Phi(F, G; s) = \frac{\ell \cdot (F^\times[\ell] : 1)^{-1}}{\ell - 1} \cdot c_\ell \cdot c_\infty \cdot \prod_{\mathfrak{p} \in Z} (1 + (\ell - 1) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s}) + h(s)$$

mit in $s = a(G)$ holomorpher Funktion $h(s)$. Der Grenzwert dieses Eulerprodukts ist auf Grund

$$\lim_{s \to a(G)} (s - a(G))^b \cdot \prod_{\mathfrak{p} \in Z} (1 + (\ell - 1) \cdot \mathcal{N}\mathfrak{p}^{-(\ell-1)\cdot s}) = \frac{1}{(\ell-1)^b} \cdot \lim_{s \to 1} (s-1)^b \cdot \prod_{\mathfrak{p} \in Z} (1 + (\ell - 1) \cdot \mathcal{N}\mathfrak{p}^{-s})$$

nach Bemerkung E.3 genau bekannt. Mit Hilfe der Taubersätze ergibt sich nun Satz 4.1. □

APPENDIX A

ASYMPTOTIK ABELSCHER ERWEITERUNGEN

In diesem Kapitel möchte ich eine kurze Zusammenfassung jener Resultate des Artikels DISTRIBUTION OF DISCRIMINANTS OF ABELIAN EXTENSIONS (1989) von David Wright geben, für die ich in meiner Arbeit Verwendung finde. Insbesondere kann die Dirichletreihe $\Phi(F, G; s)$ in eine alternierende Summe von Eulerprodukten zerlegt werden, wodurch ein brauchbares Lokal-Global-Prinzip zur Verfügung gestellt wird.

Notationen und Hilfssätze. — Alle in den beiden folgenden Abschnitten getroffenen Aussagen geben stark reduziert und in leicht variierter Notation den Sachverhalt aus den Abschnitten 2 bis 4 in Wrights Artikel wieder.

***Lemma A.1* (Delsartes Umkehrformel).** — *Es seien A eine endliche abelsche Gruppe, τ eine Funktion auf ihren Untergruppen $B \leq A$ sowie*

$$\bar{\tau}(B) = \sum_{C \leq B} \tau(C)$$

die zugehörige summatorische Funktion. Des Weiteren sei μ durch

$$\mu(A) = \prod_p \mu(A[p^\infty]) \qquad \textit{und} \qquad \mu(A[p^\infty]) = \begin{cases} (-1)^r \cdot p^{\frac{r\cdot(r-1)}{2}} & A[p^\infty] = Z_p^r \\ 0 & \textit{sonst} \end{cases}$$

das gruppentheoretische Analogon der Möbiusfunktion gegeben. Dann lässt sich τ durch die Formel

$$\tau(B) = \sum_{C \leq B} \mu(B/C) \cdot \bar{\tau}(C)$$

berechnen. Insbesondere besitzt μ die summatorische Funktion

$$\bar{\mu}(B) = \sum_{C \leq B} \mu(C) = \begin{cases} 1 & B = 1 \\ 0 & \textit{sonst.} \end{cases}$$

Es seien A eine endliche abelsche Gruppe mit Elementarteilern $n_r \mid \ldots \mid n_1$ und X eine beliebige abelsche Gruppe. Die Charaktergruppe von X bezeichne ich mit $C(X)$ und ihre n-Torsionsgruppe mit $C(X)[n]$. Das direkte Produkt der n_j-Torsionsgruppen sei mit

$$C(X)[A] = \prod_{i=1}^{r} C(X)[n_i] \leq C(\prod_{i=1}^{r} X) \qquad \text{bei} \qquad A = \prod_{i=1}^{r} Z_{n_i}$$

notiert. Für ein Charaktertupel $\boldsymbol{\chi} = (\chi_1, \ldots, \chi_r) \in C(X)[A]$ sei

$$U_{\boldsymbol{\chi}} = \bigcap_{j=1}^{r} \mathrm{Kern}\chi_j$$

der gemeinsame Kern aller χ_j, den ich im Folgenden als Kern von $\boldsymbol{\chi}$ bezeichnen werde. Die Anzahl der Tupel $\boldsymbol{\chi} \in C(X)[A]$ mit Kern $U_{\boldsymbol{\chi}} = U$ entspricht genau der Anzahl $\sum_{X/U \simeq B \leq A} (\mathrm{Aut}(B) : 1)$ der surjektiven Homomorphismen $A \twoheadrightarrow X/U$. Es sei τ eine Abbildung auf den von $C(X)[A]$ gebildeten Kernen. Vom Interesse ist die Summe $\sum_{X/U \simeq A} \tau(U)$, welche im Folgenden als $\Phi(F, A; s)$ mit $X = \mathcal{A}_F^\times / F^\times$ und $\tau(U) = \mathcal{N}\mathfrak{d}(U)^{-s}$ zum Ausdruck kommt. Sie tritt in der Formel

$$\sum_{\boldsymbol{\chi} \in C(X)[A]} \tau(\chi) = \sum_{B \leq A} (\mathrm{Aut}(B) : 1) \cdot \sum_{X/U \simeq B} \tau(U)$$

auf, wobei hier $\tau(\boldsymbol{\chi})$ mit $\tau(U_{\boldsymbol{\chi}})$ gleichgesetzt wird. Dann folgt aus Delsartes Umkehrformel

$$\sum_{X/U \simeq A} \tau(U) = \frac{1}{(\mathrm{Aut}(A) : 1)} \cdot \sum_{B \leq A} \mu(A/B) \cdot \sum_{\boldsymbol{\chi} \in C(X)[A]} \tau(\boldsymbol{\chi}).$$

Nun sei $X = \mathcal{C}_F = \mathcal{A}_F^\times / F^\times$ die Idelklassengruppe von F und wir wenden uns der Frage zu, welche Charaktertupel $\boldsymbol{\chi}$ von Charaktergruppe $C(\mathcal{A}_S^\times)[A]$ der S-Idelklassengruppe $\mathcal{A}_S^\times$ in $C(\mathcal{A}_F^\times / F^\times)[A]$ gehoben werden können.

Lemma A.2. — *Es seien S eine endliche Menge von Stellen mit $\langle \mathcal{A}_S^\times, F^\times \rangle = \mathcal{A}_F^\times$ und $\mathcal{O}_S^\times = \mathcal{A}_S^\times \cap F^\times$ die S-Einheitengruppe in F. Sind $n_r \mid \ldots \mid n_1$ die Elementarteiler von A, so setze ich weiter*

$$\mathcal{E}_S[A] = \mathcal{O}_S^\times / \mathcal{O}_S^{n_1} \times \ldots \times \mathcal{O}_S^\times / \mathcal{O}_S^{n_r}.$$

Ein Charaktertupel $\boldsymbol{\chi} \in C(\mathcal{A}_S^\times)[A]$ kann genau dann in $C(\mathcal{A}_F^\times / F^\times)[A]$ gehoben werden, wenn $\boldsymbol{\chi}$ auf $\mathcal{E}_S[A]$ trivial ist. In diesem Fall liefert $\boldsymbol{\chi}$ bei der $\{0,1\}$-wertigen Orthogonalrelation

$$\prod_{j=1}^{r} \frac{1}{(\mathcal{O}_S^\times : \mathcal{O}_S^{n_j})} \cdot \sum_{\boldsymbol{e} \in \mathcal{E}_S[A]} \boldsymbol{\chi}(\boldsymbol{e})$$

den Wert 1.

Zerlegungen von $\Phi(F, G; s)$. — Mit folgender Bemerkung wird die Diskriminantenreihe einer abelschen Gruppe

$$\Phi(F, G; s) = \sum_{\mathrm{Gal}(E/F) \simeq G} \mathcal{N}\mathfrak{d}(E/F)^{-s} = \sum_{\mathcal{C}_F / U \simeq G} \mathcal{N}\mathfrak{d}(U)^{-s}$$

in eine Summe von Führerreihen

$$\Psi(F,G;s)=\sum_{\boldsymbol{\chi}\in C(\mathcal{C}_F)[G]}\prod_{a_1=1}^{n_1}\cdots\prod_{a_r=1}^{n_r}\mathcal{N}\mathfrak{f}(\mathrm{Kern}(\chi_1^{a_1}\cdot\chi_r^{a_r}))^{-s}=\sum_{\boldsymbol{\chi}\in C(\mathcal{C}_F)[G]}\mathcal{N}\mathfrak{f}_G(\boldsymbol{\chi})^{-s}$$

umgeformt, welche ihrerseits in eine Summe von Eulerprodukten zerlegt werden können.

Bemerkung A.3. — *Die Dirichletreihe $\Phi(F,G;s)$ besitzt die folgenden Zerlegungen.*

(a)
$$\Phi(F,G;s)=\frac{1}{(\mathrm{Aut}(G):1)}\cdot\sum_{H\leq G}\mu(G/H)\cdot\Psi(F,H;(G:H)\cdot s)$$

(b)
$$\Psi(F,G;s)=\prod_{j=1}^{r}\frac{1}{(\mathcal{O}_S^\times:\mathcal{O}_S^{n_j})}\cdot\sum_{\boldsymbol{e}\in\mathcal{E}_S[G]}\sum_{\boldsymbol{\chi}\in C(\mathcal{A}_S^\times)[G]}\boldsymbol{\chi}(\boldsymbol{e})\cdot\mathcal{N}\mathfrak{f}_G(\chi)^{-s}$$

(c)
$$\Psi(F,G,S;s;\boldsymbol{e})=\sum_{\boldsymbol{\chi}\in C(\mathcal{A}_S^\times)[G]}\boldsymbol{\chi}(\boldsymbol{e})\cdot\mathcal{N}\mathfrak{f}_G(\chi)^{-s}=\prod_{\mathfrak{p}}\sum_{\boldsymbol{\chi}\in C(X_\mathfrak{p})[G]}\boldsymbol{\chi}(\boldsymbol{e}_\mathfrak{p})\cdot\mathcal{N}\mathfrak{f}_G(\boldsymbol{\chi})^{-s}$$

Hierbei ist $X_\mathfrak{p}$ die lokale Gruppe $F_\mathfrak{p}^\times$ für $\mathfrak{p}\in S$ und $X_\mathfrak{p}=\mathcal{O}_\mathfrak{p}^\times$ für $\mathfrak{p}\notin S$.

(d)
$$\Psi_\mathfrak{p}(F,G,S;s;\boldsymbol{e})=\sum_{\boldsymbol{\chi}\in C(X_\mathfrak{p})[G]}\boldsymbol{\chi}(\boldsymbol{e}_\mathfrak{p})\cdot\mathcal{N}\mathfrak{f}_G(\boldsymbol{\chi})^{-s}=\sum_{H\leq G}{}'\sum_{X_\mathfrak{p}/U\simeq H}\tau_\mathfrak{p}(U;\boldsymbol{e})\cdot\mathcal{N}\mathfrak{d}(U)^{-(G:H)\cdot s}$$

Hierbei läuft die Summe über die Isomorphieklassen von Untergruppen $H\leq G$.

(e)
$$\tau_\mathfrak{p}(U;\boldsymbol{e})=\sum_{\boldsymbol{\chi}\in C(X_\mathfrak{p})[G],U_{\boldsymbol{\chi}}=U}\boldsymbol{\chi}(\boldsymbol{e})=\sum_{U\leq V\leq X_\mathfrak{p}}\mu(V/U)\cdot\bar{\tau}_\mathfrak{p}(U;\boldsymbol{e})$$

Beweis. — Die erste Zerlegung ergibt sich aus Delsartes Umkehrformel mit der Wahl

$$X=\mathcal{C}_F\qquad\text{und}\qquad\tau(\boldsymbol{\chi})=\mathcal{N}\mathfrak{f}_G(\chi)^{-s}=\prod_{a_1=1}^{n_1}\cdots\prod_{a_r=1}^{n_r}\mathcal{N}\mathfrak{f}(\mathrm{Kern}(\chi_1^{a_1}\cdot\chi_r^{a_r}))^{-s}$$

und der Führerdiskriminantenformel

$$\mathcal{N}\mathfrak{d}(U_{\boldsymbol{\chi}})^{-(G:H)\cdot s}=\mathcal{N}\mathfrak{f}_G(\boldsymbol{\chi})$$

mit $\mathcal{C}_F/U_{\boldsymbol{\chi}}\simeq H$. In der zweiten Zerlegung wird die Orthogonalitätsrelation aus Lemma A.2 verarbeitet. Die Faktorisierung in ein Eulerprodukt folgt aus jener von

$$\boldsymbol{\chi}(\boldsymbol{e})=\prod_{\mathfrak{p}}\boldsymbol{\chi}_\mathfrak{p}(\boldsymbol{e}_\mathfrak{p})\qquad\text{und}\qquad\mathcal{N}\mathfrak{f}_G(\boldsymbol{\chi})=\prod_{\mathfrak{p}}\mathcal{N}\mathfrak{f}_G(\boldsymbol{\chi}_\mathfrak{p}).$$

Bei der vierten Zerlegung wird die Reihe nach den Faktorgruppen von den Kernen der Charaktertupel zerlegt und die Führerdiskriminantenformel wieder rückgängig gemacht. Der Wert $\tau_\mathfrak{p}(U;\boldsymbol{e})$ lässt sich schließlich wie in (e) angegeben mit Hilfe der Delsarte Umkehrformel berechnen. □

APPENDIX B

EINBETTUNGSPROBLEME

Zentrale Einbettungsprobleme. — In diesem Abschnitt fasse ich die benötigten Ergebnisse über Einbettungsprobleme zusammen. Dabei folge ich im Wesentlichen den Ausführungen von Klüners in seiner Habilitationsschrift (2005). Die zugehörigen Beweise können dort nachgeschlagen werden.

Es seien F ein beliebiger Körper und $\bar{F}$ ein fest gewählter seperabler Abschluss. Ein Einbettungsproblem wird durch zwei Epimorphismen $\bar{\varphi} : \mathrm{Gal}(\bar{F}/F) \to H$ und $\pi : G \to H$ gestellt und gesucht wird ein Epimorphismus $\varphi : \mathrm{Gal}(\bar{F}/F) \to G$ mit $\bar{\varphi} = \pi \circ \varphi$. Die Abbildung φ wird dann Lösung des Einbettungsproblem genannt.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I & \longrightarrow & G & \xrightarrow{\pi} & H & \longrightarrow & 1 \\ & & & & & \nwarrow^{\varphi} & \uparrow{\scriptstyle \bar{\varphi}} & & \\ & & & & & & \mathrm{Gal}(\bar{F}/F) & & \end{array}$$

Das Einbettungsproblem wird weiter zentral genannt, wenn der Kern von π im Zentrum von G liegt. Beispielsweise können nilpotente Erweiterungen von F sukzessiv durch Lösungen zentraler Einbettungsprobleme mit einfachem zyklischen Kern I konstruiert werden. Für jene Lösungen gibt es eine einfache Parametrisierung durch die Erweiterungen von F mit Gruppe I.

Satz B.1. — *Es seien F_H/F eine galoissche Erweiterung von Körpern der Charakteristik p mit Gruppe H und G eine zentrale Gruppenerweiterung*

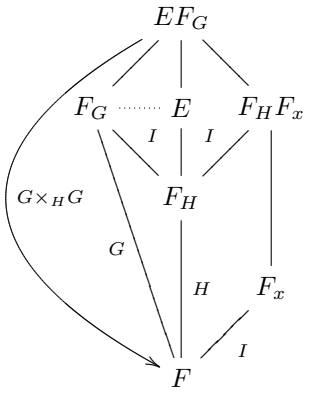
$$1 \to I \to G \to H \to 1$$

von einer einfachen zyklischen Gruppe $I = Z_\ell$ mit H sowie $F_G \geq F_H$ eine Lösung des vorliegenden Einbettungsproblems. Dann sind alle Lösungen des Einbettungsproblems parametrisierbar durch die Erweiterungen von F mit Gruppe I wie folgt.

(a) *Im Fall $p = \ell$ gibt es ein Element $y \in F_H$ mit $F_G = F_H(\wp^{-1}y)$, wobei $\wp(z) = z^p - z$ der Artin-Schreier-Operator ist. Dann lassen sich sämtliche Lösungen des Einbettungsproblem durch die Gestalt $E = F_H(\wp^{-1}(x + y))$ mit $x \in F/\wp F$ angeben.*

(b) *Es sei $p \neq \ell$ und F enthalte die primitiven ℓ-ten Einheitswurzeln. Dann gibt es ein Element $y \in F_H$ mit $F_G = F_H(\sqrt[\ell]{y})$. Sämtliche Lösungen des Einbettungsproblem lassen durch die Gestalt $E = F_H(\sqrt[\ell]{xy})$ mit $x \in F/F^\ell$ angeben.*

Beweisskizze. — Ich beweise hier nur den Fall (a), für Fall (b) kann analog verfahren oder die Theorie der Brauer Einbettungsprobleme herangezogen werden.[(1)] Sämtliche Beweismittel finden sich in den Kapiteln 4.2 und 4.3 in Klüners Habilitationsschrift (2005), wie auch folgendes schönes Diagramm, und im Anhangskapitel A.1 *The 'Seen one, seen them all' Lemma* von Jensen et al. (2002).



Es sei $E \geq F_H$ eine Lösung des Einbettungsproblems. Dann ist EF_G/F galoissch mit dem Faserprodukt $G \times_H G$, welches isomorph zum Faserprodukt $G \times_H (I \times H)$ ist. Dieses enthält genau $p+1$ Untergruppen der Ordnung p, die zu den Teilkörpern von EF_G/F_H korrespondieren. Genau eine jener Untergruppen besitzt die Faktorgruppe $I \times H$, alle restlichen Untergruppen von der Ordnung p besitzen die Faktorgruppe G. Also enthält EF_G/F_H einen Zwischenkörper E' mit Galoisgruppe $I \times H$ über F. Zur Untergruppe H korrespondiert der Teilkörper $F_x = F(\wp^{-1}x)$ von E', der somit die Gestalt $E' = F_HF_x$ hat. Also ist $EF_G = F_H(\wp^{-1}\{x, y\})$ eine elementarabelsche Erweiterung von F_H und alle Teilkörper sind von der Gestalt $F_H(\wp^{-1}(ax + by))$ mit $a, b \in \mathbb{F}_p$, die allesamt mit Ausnahme für $a \neq 0 = b$ die Galoisgruppe G über F besitzen.

Umgekehrt ist ein Körper der Gestalt $E = F_H(\wp^{-1}(x+y))$ eine Teilerweiterung von F_GF_x/F_H. Wieder hat F_GF_x/F die Galoisgruppe $G \times_H G$ und F_HF_x korrespondiert zu der Untergruppe mit Ordnung p und Faktorgruppe $I \times H$. Somit ist E/F galoissch mit Gruppe G. □

(1) z.B. im Kapitel IV.7. Malle und Matzat (1999)

APPENDIX C

KLASSENKÖRPERTHEORIE

Lokale Klassenkörpertheorie. —

***Satz C.1* (Einseinheitensatz von Hasse).** — *Für einen lokalen Körper $F_\mathfrak{p}$ mit Restklassenkörper $\mathbb{F}_\mathfrak{p}$ der Charakteristik p gilt*

$$F_\mathfrak{p}^\times \simeq \mathbf{Z} \times \mathcal{O}_\mathfrak{p}^\times \simeq \mathbf{Z} \times \mathbb{F}_\mathfrak{p}^\times \times \langle 1+\mathfrak{p} \rangle.$$

Die Einseinheitengruppe $\langle 1+\mathfrak{p} \rangle$ ist ein $\mathbf{Z}_p$-Modul mit in den Punkten (a) und (b) beschriebener Basis. Dazu sei t ein Primelement von $\mathfrak{p}$ und $B = \{b_1, \ldots, b_{[\mathbb{F}_\mathfrak{p}:\mathbb{F}_p]}\}$ ein Repräsentantensystem einer Basis von $\mathbb{F}_\mathfrak{p}$ über $\mathbb{F}_p$.

(a) *Ist $F_\mathfrak{p}$ ein lokaler Funktionenkörper, so ist $\langle 1+\mathfrak{p} \rangle$ ein freier $\mathbf{Z}_p$-Modul mit Basis*

$$\{1 + b_i \cdot t^m : m \in \mathbf{N},\ (m,p) = 1,\ 1 \leq i \leq [\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]\}.$$

(b) *Ist $F_\mathfrak{p}$ ein lokaler Zahlkörper, so ist $\langle 1+\mathfrak{p} \rangle$ das direkte Produkt von $F_\mathfrak{p}^\times[p^\infty]$ und einem freien $\mathbf{Z}_p$-Modul mit Basis*

$$C \cup \{1 + b_i \cdot t^m : m \in \mathbf{N},\ 1 \leq m < e(\mathfrak{p}|p) + e_\mathfrak{p},\ (m,p) = 1,\ 1 \leq i \leq \deg \mathfrak{p}\}$$

für ein geeignet angepasstes Repräsentantensystem B und $C = \{1 + c \cdot t^{pe_\mathfrak{p}}\}$ für ein bestimmtes $c \in F_\mathfrak{p}$, falls $F_\mathfrak{p}$ primitive p-te Einheitswurzeln enthält und $C = \emptyset$ sonst. Die Zahl $e(\mathfrak{p}|p) = e_\mathfrak{p} \cdot (p-1) + r_\mathfrak{p}$ mit $0 \leq r_\mathfrak{p} \leq p-2$ ist hier der absolute Verzweigungsindex von $\mathfrak{p}$.

Beweis. — Diese Aussagen folgen nach Hasse (1980). Für Funktionenkörper wie auch Zahlkörper findet sich eine kompakte Einführung in Fesenko und Vostokov (1993) Kapitel I.6, Proposition 6.2 auf Seite 15. □

Auf $F_\mathfrak{p}^\times$ wird eine Topologie durch die aus den Untergruppen $\langle 1+\mathfrak{p}^m \rangle$ bestehende Umgebungsbasis erklärt. Sie bildet eine Filtration

$$\langle 1+\mathfrak{p} \rangle \geq \langle 1+\mathfrak{p}^2 \rangle \geq \ldots \geq \langle 1+\mathfrak{p}^m \rangle \geq \langle 1+\mathfrak{p}^{m+1} \rangle \geq \ldots$$

und eine Untergruppe $U \leq F_\mathfrak{p}^\times$ ist genau dann offen, wenn es ein m mit $U \geq \langle 1+\mathfrak{p}^m \rangle$ gibt.

Korollar C.2. — *Für die Einseinheitengruppe $X_m := \langle 1+\mathfrak{p} \rangle / \langle 1+\mathfrak{p}^{m+1} \rangle$ ergeben sich folgende Aussagen.*

(a) *Für einen Funktionenkörper gilt*

$$(X_m : X_m^p) = \mathcal{N}\mathfrak{p}^{m-\lfloor \frac{m}{p} \rfloor}.$$

(b) *Für einen Zahlkörper gilt*

$$(X_m : X_m^p) = \begin{cases} \mathcal{N}\mathfrak{p}^{m-\lfloor \frac{m}{p} \rfloor} & 0 \leq m < e(\mathfrak{p}|p) + e_\mathfrak{p} \\ \mathcal{N}\mathfrak{p}^{e(\mathfrak{p}|p)} \cdot (F_\mathfrak{p}^\times[p] : 1) & m \geq e(\mathfrak{p}|p) + e_\mathfrak{p}. \end{cases}$$

Beweis. — Für Funktionenkörper findet sich in Auer (1999) mit Proposition 6.2 auf Seite 39 ein konstruktiver Beweis. Eine Übersicht für Zahlkörper kann beispielsweise in Nakagoshi (1979) eingesehen werden. □

***Satz C.3* (Lokales Reziprozitätsgesetz).** — *Die Zuordnung*

$$E \mapsto U = \mathcal{N}_{E/F_\mathfrak{p}}(E^\times)$$

liefert eine bijektive Zuordnung zwischen den endlichen abelschen Erweiterungen $E/F_\mathfrak{p}$ eines lokalen Körpers $F_\mathfrak{p}$ und den offenen Untergruppen $U \leq F_\mathfrak{p}^\times$ vom endlichen Index seiner multiplikativen Gruppe.

Beweis. — Ein Beweis befindet sich beispielsweise in Fesenko und Vostokov (1993) Kapitel IV.6, Theorem 6.2 auf Seite 124. □

***Satz C.4* (Diskriminanten abelscher Erweiterungen).** — *Es seien $E/F_\mathfrak{p}$ eine endliche abelsche Erweiterung und $U \leq F_\mathfrak{p}^\times$ die zugehörende multiplikative offene Untergruppe. Dann besitzt $E/F_\mathfrak{p}$ den Diskriminantenexponenten*

$$d_\mathfrak{p}(E/F_\mathfrak{p}) = d_\mathfrak{p}(U) = \sum_{m \geq 0} (m+1) \cdot \left((F_\mathfrak{p}^\times : \langle U, 1 + \mathfrak{p}^{m+1} \rangle) - (F_\mathfrak{p}^\times : \langle U, 1 + \mathfrak{p}^m \rangle) \right).$$

Diese Summe ist auf Grund $\langle 1 + \mathfrak{p}^m \rangle \leq U$ für $m \gg 0$ endlich.

Beweis. — Ist a_m die Anzahl der irreduziblen Charaktere von $F_\mathfrak{p}^\times / U$ mit Führerexponenten $m+1$, so gilt nach der Führerdiskriminantenformel $d_\mathfrak{p} = \sum_{m \geq 0} (m+1) \cdot a_m$. Die Führerdiskriminantenformel kann beispielsweise in Neukirch (1992) Kapitel VII.11 Satz 11.9 auf Seite 557 eingesehen werden. □

Globale Klassenkörpertheorie. —

***Satz C.5* (Globales Reziprozitätsgesetz).** — *Die Zuordnung*

$$E \mapsto \mathcal{N}_{E/F}(\mathcal{A}_E^\times)/F^\times$$

liefert eine bijektive Zuordnung zwischen den endlichen abelschen Erweiterungen E/F eines globalen Körpers F und den offenen Untergruppen $\prod_\mathfrak{p} U_\mathfrak{p} \leq \mathcal{A}_F^\times / F^\times$ vom endlichen Index seiner Idelklassengruppe.

Beweis. — Für Zahlkörper findet sich ein Beweis in Lang (1994) Kapitel X.3, Theorem 5 auf Seite 208 und für Funktionkörper eine Formulierung des Reziprozitätsgesetz in Villa Salvador (2006) Kapitel 11.6 Seite 411. □

***Satz C.6* (Strahlklassengruppe).** — *Für die Strahlklassengruppe $\mathcal{C}\ell_{\mathfrak{m}}$ eines globalen Funktionenkörpers F mit Konstantenkörper K gilt die exakte Sequenz*

$$1 \to K^\times \to F^{\mathfrak{m}}/F_{\mathfrak{m}} \to \mathcal{C}\ell_{\mathfrak{m}} \to \mathcal{C}\ell \to 1.$$

Des Weiteren gilt

$$F^{\mathfrak{m}}/F_{\mathfrak{m}} \simeq \prod_{\mathfrak{p}^m || \mathfrak{m}} \mathcal{O}_{\mathfrak{p}}^\times/\mathfrak{p}^m \simeq \prod_{\mathfrak{p}^m || \mathfrak{m}} \mathbb{F}_{\mathfrak{p}}^\times \times \langle 1+\mathfrak{p}\rangle/\langle 1+\mathfrak{p}^m\rangle.$$

Beweis. — Eine Abhandlung dieses Sachverhalts findet sich beispielsweise in Hess et al. (2003). □

***Satz C.7* (Diskriminanten abelscher Erweiterungen).** — *Es seien E/F eine endliche abelsche Erweiterung und $U = \prod_{\mathfrak{p}} U_{\mathfrak{p}} \leq \mathcal{A}_F^\times$ die zugehörende Idelgruppe. Dann besitzt E/F die Diskriminante*

$$\mathfrak{d}(E/F) = \mathfrak{d}(U) = \prod_{\mathfrak{p}} \prod_{\mathfrak{q}|\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}(E_{\mathfrak{q}}/F_{\mathfrak{p}})}.$$

Beweis. — Diese Formel folgt aus dem Lokal-Global-Prinzip. □

APPENDIX D

DIRICHLETREIHEN

Eigenschaften. — Eine allgemeine Dirichletreihe ist eine Reihe der Gestalt

$$\Phi(s) = \sum_{n \geq 1} a_n n^{-s}.$$

Diese Reihe besitzt eine **Konvergenzabszisse** $a \in \mathbf{R} \cup \{\pm\infty\}$, sodass $\Phi(s)$ divergent für $\Re(s) < a$ und konvergent für $\Re(s) > a$ ist. Im Gebiet $\Re(s) > a$ ist $\Phi(s)$ eine holomorphe Funktion. Zwei Dirichletreihen beschreiben genau dann eine gleiche Funktion, wenn ihre Koeffizienten gleich sind. Ich verwende an manchen Stellen die Redewendung **holomorph in** $\Re(s) \geq a$. Diese soll für die Holomorphie in $\Re(s) > a - \varepsilon$ mit einem hinreichend kleinen $\varepsilon > 0$ stehen.

Periodizität. — Die in dieser Arbeit bezüglich Funktionenkörper untersuchten Dirichletreihen haben die Gestalt

$$\Phi(s) = \sum_{n \geq 0} a_n q^{-ns},$$

wobei q die Elementanzahl des Konstantenkörpers angibt. Bei der Analyse von $\Phi(s)$ ist es oft einfacher, diese Reihe als Potenzreihe

$$F(t) = \sum_{n \geq 0} a_n t^n$$

in $t = q^{-s}$ zu betrachten. Trotzdem habe ich mich entschlossen, Dirichletreihen in der Unbestimmten s anzugeben und zu behandeln, um eine Analogie zu Zahlkörpern zu wahren. Dirichletreihen bezüglich Funktionenkörpern besitzen die Periode $v \cdot \mathbf{Z}$ mit $v = 2\pi i / \log(q)$. Deswegen werde ich periodische Dirichletreihen stillschweigend auf Argumente s im Gebietsstreifen

$$C = \{s \in \mathbf{C} : -\pi / \log(q) \leq \Im(s) < \pi / \log(q)\}$$

einschränken. Innerhalb dieses Streifen können die Reihen selbstverständlich immer noch eine Periode besitzen.

Bemerkung D.1. — *Es sei $F(t) = \sum_{n \geq 0} a_n t^n$ eine Potenzreihe mit positivem Konvergenzradius und $w = \mathrm{ggT}(n : a_n \neq 0)$. Dann gilt $F(\xi t) = F(t)$ genau dann, wenn ξ eine w-te Einheitswurzel ist.*

Beweis. — Es sei ξ eine komplexe Einheitswurzel mit $\xi^w = 1$. Da w der größte gemeinsame Teiler aller Indizes nichttrivialer Koeffizienten ist, gilt

$$F(t) = \sum_{n\geq 0} a_{nw} t^{nw} = \sum_{n\geq 0} a_{nw} (\xi t)^{nw} = F(\xi t).$$

Ist umgekehrt ξ eine komplexe Zahl mit $F(\xi t) = F(t)$, so gilt nach dem Residuensatz

$$0 \neq a_w = \frac{1}{2\pi i} \oint_\gamma \frac{F(t)}{t^{w+1}} dt = \frac{1}{2\pi i} \oint_\gamma \frac{F(\xi t)}{t^{w+1}} dt = a_w \xi^w$$

für einen hinreichend kleinen Kreisweg γ um $t = 0$ und somit $\xi^w = 1$. □

Ist also w der größte gemeinsame Teiler aller Indizes n mit $a_n \neq 0$, so hat die Dirichletreihe $\Phi(s) = \sum_{n\geq 0} a_n q^{-ns}$ die Periode $vw^{-1} \cdot \mathbf{Z}$. Alle Informationen über die Funktion stecken somit bereits im Gebietsstreifen

$$C_w = \{s \in \mathbf{C} : -\pi/(w \cdot \log(q)) \leq \Im(s) < \pi/(w \cdot \log(q))\}.$$

Taubersätze. — Mit Hilfe von Taubersätzen lassen sich Aussagen über die Koeffizienten a_n einer Dirichletreihe $\Phi(s)$ oder deren Summation gewinnen. Dazu muss $\Phi(s)$ über ihre Konvergenzabszisse a hinaus in $\Re(s) \geq a$ meromorph fortsetzbar sein. Dann liefern Taubersätze Aussagen über das asymptotische Wachstum der Koeffizienten. Der Ausdruck $f(x) \sim g(x)$ steht dabei für $f(x)$ **asymptotisch äquivalent zu** $g(x)$ und bedeutet $\lim_{x\to\infty} f(x)/g(x) = 1$.

Eine einfache Abschätzung der Summationsfunktion von Koeffizienten ergibt sich wie folgt.

Lemma D.2. — *Es sei $\Phi(s) = \sum_{n\geq 1} a_n n^{-s}$ eine für $\Re(s) > a$ holomorphe Dirichletreihe mit nichtnegativen Koeffizienten. Dann gilt für die Summation ihrer Koeffizienten und alle $\varepsilon > 0$ die Schranke*

$$\sum_{n\leq x} a_n \in O\left(x^{a+\varepsilon}\right)$$

Beweis. — Diese Aussage folgt aus

$$\sum_{n\leq x} a_n \leq \sum_{n\leq x} a_n \cdot (x \cdot n^{-1})^s = \left(\sum_{n\leq x} a_n n^{-s}\right) \cdot x^s \leq \Phi(s) \cdot x^s$$

für $s > a$. □

Zunächst entwickle ich einen Taubersatz für Dirichletreihen über Funktionenkörper. Grundversionen dieses Satzes befinden sich beispielsweise in Rosen (2002) Kapitel 17, welche mit Einschränkungen zur Lage der Konvergenzabszisse und der Anzahl der Pole versehen sind. Hier wird die Anwendung des Residuensatzes noch etwas intensiver ausgearbeitet.

Satz D.3. — *Es sei $F(t) = \sum_{n\geq 0} a_n t^n$ eine Potenzreihe mit positivem Konvergenzradius r. Auf dem Konvergenzkreis besitze $F(t)$ die endliche Menge P von isolierten Polen und sei über den Konvergenzkreis hinaus auf $|t| \leq r + \delta$, $t \notin P$ holomorph fortsetzbar. Die Hauptteile von $F(t)$ an den Polen $u \in P$ seien von der Gestalt $H_u((t-u)^{-1}) = \sum_{k=1}^{b_u} c_{u,k}(t-u)^{-k}$. Hierbei sei b_u die jeweilige Ordnung der Pole $u \in P$*

und b ihr Maximum. Dann sind die die Koeffizienten a_n von der Größenordnung $O\left(r^{-n}n^{b-1}\right)$ und es gilt

$$a_n = \sum_{u\in P}\left(\sum_{k=1}^{b_u}\binom{n+k-1}{k-1}\cdot c_{u,k}\cdot(-u)^{-k}\right)\cdot u^{-n} + o\left(r^{-n}\right).$$

Beweis. — Nach der Voraussetzung kann ich annehmen, dass $F(t)$ eine auf dem gelochten Bereich $\{t \in \mathbf{C} : |t| \leq r+\delta,\ t \notin P\}$ holomorphe Funktion ist. Den Koeffizienten a_n erhalte ich nun aus dem Kurvenintegral

$$a_n = \mathrm{Res}_{t=0}\frac{F(t)}{t^{n+1}} = -\frac{1}{2\pi i}\oint_{\gamma_\varepsilon}\frac{F(t)}{t^{n+1}}dt$$

längs eines kleinen nach dem Uhrzeigersinn orientierten Weges γ_ε um den Nullpunkt. Im Folgenden wird dieses Integral mit den Residuen in P in Relation gesetzt. Dazu sei γ der Kreisweg entgegen des Uhrzeigersinns um den Nullpunkt mit Radius $r+\delta$. Das Kurvenintegral

$$\frac{1}{2\pi i}\oint_{\gamma_\varepsilon+\gamma}\frac{F(t)}{t^{n+1}}dt = \frac{1}{2\pi i}\oint_{\gamma}\frac{F(t)}{t^{n+1}}dt + \frac{1}{2\pi i}\oint_{\gamma_\varepsilon}\frac{F(t)}{t^{n+1}}dt$$

berechnet sich aus der Summe der Residuen im eingeschlossen Bereich des Weges $\gamma_\varepsilon+\gamma$ und somit erhalte ich für a_n die Gleichheit

$$a_n = -\sum_{u\in P}\mathrm{Res}_{t=u}\frac{F(t)}{t^{n+1}} + \frac{1}{2\pi i}\oint_{\gamma}\frac{F(t)}{t^{n+1}}dt = -\sum_{u\in P}\mathrm{Res}_{t=u}\frac{F(t)}{t^{n+1}} + O\left((r+\delta)^{-n}\right).$$

Die O-Abschätzung des hier auftretenden Integrals gewinne ich aus dem Maximum von $|F(t)/t^{n+1}|$ längs des kompakten Weges γ und kann auch durch $o\left(r^{-n}\right)$ ersetzt werden. Es verbleiben nun lediglich die Residuen zu bestimmen. Die Funktion $d(t) = 1/t^{n+1}$ ist für $t \neq 0$ holomorph und ihre Taylorreihe um $t = u \in P$ besitzt die Koeffizienten

$$d_{u,m} = \frac{d^{(m)}(u)}{m!} = \frac{(-1)^m}{u^{n+1+m}}\cdot\prod_{l=1}^{m}\frac{n+l}{l} = -(-1)^{m+1}\cdot\binom{n+m}{m}\cdot u^{-(n+m+1)}.$$

Der Hauptteil von $F(t)$ um $t = u$ hat die Koeffizienten $c_{u,k}$ und das Residuum von $F(t)/t^{n+1}$ errechnet sich via

$$-\mathrm{Res}_{t=u}\frac{F(t)}{t^{n+1}} = -\sum_{k+m=-1}c_{u,k}\cdot d_{u,m} = \sum_{k=1}^{b_u}\binom{n+k-1}{k-1}\cdot(-1)^k\cdot u^{-(n+k)}\cdot c_{u,k}.$$

Der Binomialkoeffizient ist ein Polynom in n mit Leitterm $n^{k-1}/(k-1)!$ und für hinreichend große n gehört der betragsmäßig größte Term zu $k = b_u$. Mit der Residuenformel für a_n gewinne ich nun wie behauptet

$$a_n = \sum_{u\in P}\left(\sum_{k=1}^{b_u}\binom{n+k-1}{k-1}\cdot c_{u,k}\cdot(-u)^{-k}\right)\cdot u^{-n} + o\left(r^{-n}\right)$$

und

$$|a_n| \in O\left(r^{-n}n^{b-1}\right)$$

für $b = \max\{b_u : u \in P\}$. □

Korollar D.4. — *In der Sitution von Satz D.3 enthalte die Polstellenmenge P den reellen Pol $u = r$ von der Ordnung b. Des Weiteren seien alle anderen Pole $u \neq r$ von strikt kleinerer Ordnung. Bezeichnet $c = c_{r,b}$ den Grenzwert $\lim_{t\to r} F(t) \cdot (t-r)^b$, so gilt*

$$a_n \sim \frac{(-1)^b \cdot c}{r^b \cdot (b-1)!} \cdot r^{-n} n^{b-1}.$$

Es seien weiter $r < 1$ und d der Grenzwert der Summen $d_m = \sum_{n\leq m} r^{m-n}(n/m)^{b-1}$. Dann gilt

$$\sum_{n\leq m} a_n \sim \frac{(-1)^b \cdot c \cdot d}{r^b \cdot (b-1)!} \cdot r^{-m} m^{b-1}.$$

Beweis. — Ich knüpfe hier an dem Beweis obigen Satzes an. Der Leitterm von a_n als Polynom in n gehört zu den Polen von der Ordnung b, also in diesem Fall ausschließlich zu $u = r$. Daraus folgt

$$a_n = \frac{(-1)^b \cdot c}{r^b \cdot (b-1)!} \cdot r^{-n} n^{b-1} + o\left(r^{-n} n^{b-1}\right)$$

und somit die behauptete asymptotische Äquivalenz von a_n. Die asymptotische Äquivalenzklasse der Summation ergibt sich aus

$$\sum_{n\leq m} a_n = \frac{(-1)^b \cdot c}{r^b \cdot (b-1)!} \cdot d_m \cdot r^{-m} m^{b-1} + o\left(r^{-m} m^{b-1}\right).$$

Es ist nur noch die Konvergenz der Folge $(d_m)_{m\geq 1}$ nachzuweisen. Diese ist auf Grund von $r < 1$ beschränkt durch $1 \leq d_m \leq 1/(1-r)$ und monoton steigend vermöge

$$d_{m+1} - d_m = \sum_{n\leq m} r^n \cdot \left(\left(\frac{m+1-n}{m+1}\right)^{b-1} - \left(\frac{m-n}{m}\right)^{b-1}\right) \geq 0.$$

In dieser Summe ist keiner der Summanden negativ. Somit ist die Existenz des Grenzwertes d gesichert. □

Aus diesem Korollar ergibt sich folgender Taubersatz für Funktionenkörper.

***Satz D.5* (Taubersatz für Funktionenkörper)**. — *Die Dirichletreihe $\Phi(s) = \sum_{n\geq 0} a_n q^{-ns}$ habe die positive Konvergenzabszisse a und sei in $\Re(s) \geq a$ meromorph fortsetzbar mit Pol in $s = a$ von der Ordnung b und endlich vielen weiteren Polen auf $\Re(s) = a$ mit strikt kleinerer Ordnung. Bezeichnet $c(\Phi)$ den Grenzwert $lim_{s\to a}(s-a)^b \cdot \Phi(s)$ und d den Grenzwert von $\sum_{n\leq m} q^{a(n-m)}(n/m)^{b-1}$, so gilt für die Koeffizienten die asymptotische Äquivalenz*

$$a_n \sim \frac{c(\Phi) \cdot \log(q)^b}{(b-1)!} \cdot q^{an} n^{b-1}$$

und ihre Summationsfunktion in $x = q^m$ hat die asymptotische Äquivalenzklasse

$$\sum_{q^n\leq x} a_n \sim \frac{c(\Phi) \cdot d \cdot \log(q)}{(b-1)!} \cdot x^a \log(x)^{b-1}.$$

Beweis. — Die Dirichletreihe $\Phi(s)$ bildet eine Potenzreihe $F(t) = \sum_{n\geq 0} a_n t^n$ in $t = q^{-s}$ mit den Konvergenzradius $r = q^{-a}$. Der Grenzwert an $t = r$ ist vermöge der Regel von l'Hôpital durch

$$c = \lim_{t\to r}(t-r)^b F(t) = \lim_{s\to a}\left(\frac{q^{-s}-q^{-a}}{s-a}\right)^b (s-a)^b\Phi(s) = (-\log(q)q^{-a})^b c(\Phi)$$

gegeben. Nach Korollar D.4 gelten also

$$a_n \sim \frac{c(\Phi)\cdot\log(q)^b}{(b-1)!}\cdot q^{an} n^{b-1}$$

und

$$\sum_{n\leq m} a_n \sim \frac{c(\Phi)\cdot d\cdot\log(q)^b}{(b-1)!}\cdot q^{am} m^{b-1}.$$

Für $x = q^m$ ist $m = \log(x)/\log(q)$ und es folgt

$$q^{am}\cdot m^{b-1} = \frac{1}{\log(q)^{b-1}}\cdot x^a \log(x)^{b-1},$$

woraus sich die Reduktion der Logarithmuspotenz im Leitkoeffizienten erklärt. □

Korollar D.6. — *Es seien $\Phi(s) = \sum_{n\geq 0} a_n q^{-ns}$ eine Dirichletreihe mit positiver Konvergenzabszisse a und w der größte gemeinsame Teiler aller Indizes nichttrivialer Koeffizienten. Des Weiteren besitzen die Koeffizienten $\tilde{a}_n = a_{wn}$ die Asymptotik*

$$\tilde{Z}(x) = \sum_{q^n\leq x}\tilde{a}_n \sim \tilde{c}\cdot x^{aw}\log(x)^{b-1}.$$

Dann hat die Koffizientensumme der a_n die asymptotische Äquivalenzklasse

$$Z(x) = \sum_{q^n\leq x} a_n \sim \frac{\tilde{c}}{w^{b-1}}\cdot x^a\log(x)^{b-1}.$$

Beweis. — Nach Voraussetzung ist $\tilde{Z}(x) = Z(x^w)$. Dann folgt die Behauptung aus

$$Z(x) = \tilde{Z}(x^{1/w}) \sim \tilde{c}\cdot x^a\log(x^{1/w})^{b-1} = \tilde{c}\cdot(1/w)^{b-1}\cdot x^a\log(x)^{b-1}.$$

□

Für Zahlkörper beziehe ich mich auf folgenden Taubersatz. Er ist samt Beweis in Narkiewicz (1983) als Korollar im Abschnitt III.3 auf Seite 121 zu finden. Auch hier ist das oben beobachte Transformationsverhalten gültig und folgt analog aus $\tilde{Z}(x) = Z(x^w)$.

***Satz D.7* (Taubersatz nach Delange)**. — *Es sei $\Phi(s) = \sum_{n\geq 1} a_n n^{-s}$ eine Dirichletreihe mit nichtnegativen Konstanten $a_n \geq 0$ und Konvergenzabszisse $a > 0$. Des Weiteren sei $\Phi(s)$ auf $\Re(s) \geq a$ holomorph mit einziger Ausnahme in $s = a$. Zu $b \in \mathbf{R}$ existiere der positive Grenzwert*

$$c(\Phi) = \lim_{s\to a}(s-a)^b\cdot\Phi(s) > 0.$$

Dann gilt

$$\sum_{n\leq x} a_n \sim \frac{c(\Phi)}{a\cdot\Gamma(b)}\cdot x^a\log(x)^{b-1}.$$

Korollar D.8. — *Es sei zusätzlich* $\tilde{\Phi}(s) = \Phi(s/w)$ *ebenfalls eine Dirichletreihe. Deren Koeffizienten* $\tilde{a}_n = a_{n^w}$ *seien in der asymptotischen Äquivalenzklasse*

$$\tilde{Z}(x) = \sum_{n \leq x} \tilde{a}_n \sim \tilde{c} \cdot x^{aw} \log(x)^{b-1}.$$

Dann gilt für die Asymptotik der Koffizientensumme über a_n

$$Z(x) = \sum_{n \leq x} a_n \sim \frac{\tilde{c}}{w^{b-1}} \cdot x^a \log(x)^{b-1}.$$

APPENDIX E

EULERPRODUKTE

In diesem Kapitel werden die Meromorphieeigenschaften allgemeiner und spezieller Eulerprodukte offengelegt.

Lemma E.1. — *Es seien $h(t) \in \mathbf{Q}[t]$ ein Polynom mit ganzahligem positiven Absolutkoeffizienten $b \geq 1$ und $f(t) = t^a \cdot h(t)$ ebenfalls ein Polynom mit $a \geq 1$. Dann ist das Eulerprodukt*

$$\Phi(s) = \prod_{\mathfrak{p}} (1 + f(\mathcal{N}\mathfrak{p}^{-s}))$$

meromorph in $\Re(s) \geq 1/a$ mit einzigem Pol in $s = 1/a$ der Ordnung b.

Beweis. — Das erweitertete Eulerprodukt

$$\begin{aligned} g(s) &= \prod_{\mathfrak{p}} (1 - \mathcal{N}\mathfrak{p}^{-as})^b \cdot (1 + f(\mathcal{N}\mathfrak{p}^{-s})) \\ &= \prod_{\mathfrak{p}} (1 - b \cdot \mathcal{N}\mathfrak{p}^{-as} + O\left(\mathcal{N}\mathfrak{p}^{-2as}\right)) \cdot (1 + b \cdot \mathcal{N}\mathfrak{p}^{-as} + O\left(\mathcal{N}\mathfrak{p}^{-(a+1)s}\right)) \\ &= \prod_{\mathfrak{p}} (1 + O\left(\mathcal{N}\mathfrak{p}^{-(a+1)s}\right)) \end{aligned}$$

ist konvergent und somit holomorph für $\Re(s) > 1/(a+1)$. Daher ist

$$\Phi(s) = \zeta(as)^b \cdot g(s)$$

meromorph in $\Re(s) > 1/(a+1)$ mit Pol in $s = 1/a$ der Ordnung b. □

Grenzwerte zyklotomischer Eulerprodukte. — Es sei ℓ eine Primzahl und $\tilde{F}$ die Erweiterung eines globalen Körpers F mit primitiven ℓ-ten Einheitswurzeln vom Grad $n = [\tilde{F} : F]$. Im Fall $\ell = \mathrm{char}(F)$ ist dabei $\tilde{F} = F$. Im Folgenden bezeichnet $\tilde{F}_d$ den Zwischenkörper von $\tilde{F}/F$ vom Index $[\tilde{F} : \tilde{F}_d] = d$. Eine Stelle aus diesem Zwischenkörper wird mit dem entsprechenden Index gekennzeichnet, d.h. ich schreibe $\mathfrak{p}_d$ für eine Erweiterung der Stelle $\mathfrak{p} \in \mathbb{P}_F$ in $\tilde{F}_d$ und $\tilde{\mathfrak{p}} = \mathfrak{p}_1$ für die Erweiterung in $\tilde{F}$. Die folgenden beiden Bemerkungen wurden aus Abschnitt 2.4 der Arbeit von Cohen et al. (2002) entnommen.

***Bemerkung E.2* (Cohen et al, 2002, Satz 2.16).** — *Es seien V und Z die Mengen der in $\tilde{F}/F$ verzweigten bzw. vollständig zerlegten Stellen aus F. Insbesondere enthalte Z alle Stellen von F im Fall $\tilde{F} = F$. Dann gilt*

$$\prod_{d|n} \zeta_{\tilde{F}_d}(ds)^{\mu(d)} = \prod_{d|n} \prod_{\mathfrak{p}\in Z} (1 - \mathcal{N}\mathfrak{p}^{-ds})^{-\mu(d)n/d} \cdot \prod_{\mathfrak{p}\in V} \prod_{\mathfrak{p}_d|\mathfrak{p}} (1 - \mathcal{N}\mathfrak{p}_d^{-ds})^{-\mu(d)}.$$

Beweis. — Die behauptete Identität wird lokal an den Stellen $\mathfrak{p}$ aus F nachgewiesen. Deren Eulerfaktor zu $\zeta_{\tilde{F}_d}$ auf der linken Seite ist

$$\prod_{\mathfrak{p}_d|\mathfrak{p}} (1 - \mathcal{N}\mathfrak{p}_d^{-d\cdot s})^{-\mu(d)} = (1 - \mathcal{N}\mathfrak{p}^{-d\cdot f_d\cdot s})^{-\mu(d)\cdot n/(d\cdot f_d\cdot e_d)},$$

wobei $e_d = e(\mathfrak{p}_d|\mathfrak{p})$ den Verzweigungs- und $f_d = f(\mathfrak{p}_d|\mathfrak{p})$ den Trägheitsgrad von $\mathfrak{p}_d$ angibt. Für die Eulerfaktoren der verzweigten Stellen $\mathfrak{p} \in V$ ist dies genau die angegebene Formel, für die vollständig zerlegten Stellen $\mathfrak{p} \in Z$ stimmt die behauptete Formel auf Grund $e_d = f_d = 1$. Es bleibt also die Untersuchung der Faktoren

$$L_\mathfrak{p} = \prod_{d|n} (1 - \mathcal{N}\mathfrak{p}^{-d\cdot f_d\cdot s})^{-\mu(d)\cdot n/(d\cdot f_d)}$$

für die Stellen $\mathfrak{p} \notin V \cup Z$. Der Behauptung zu Folge soll $L_\mathfrak{p} = 1$ gelten. Zunächst wird gezeigt, dass der Trägheitsgrad f_d durch den Quotienten $f/(d, f)$ mit $f = f_1 = f(\tilde{\mathfrak{p}}|\mathfrak{p})$ gegeben ist. Nach Stichtenoth (1993), Lemma V.1.9. gilt

$$f_d \cdot (n/d, \deg(\mathfrak{p})) = n/d.$$

Somit ist behauptete Gleichung $f_d = f/(d, f)$ äquivalent zu

$$d \cdot (n/d, \deg(\mathfrak{p})) = (n, \deg(\mathfrak{p})) \cdot (d, n/(n, \deg(\mathfrak{p}))).$$

Diese elementare Gleichung lässt sich zum Beispiel unter Gebrauch einer Fallunterscheidung nachweisen. Es gilt also

$$L_\mathfrak{p} = \prod_{d|n} (1 - t^{d\cdot f/(d,f)})^{-\mu(d)\cdot n\cdot (d,f)/(d\cdot f)}$$

mit $t = \mathcal{N}\mathfrak{p}^{-s}$. Jeder einzelne Faktor lässt sich gemäß $t^{n_d} - 1 = \prod_{m|n_d} \Phi_m(t)$ noch weiter in Produkte von Kreisteilungspolynomen $\Phi_m(t)$ zerlegen und es gilt

$$L_\mathfrak{p} = \pm \prod_{d|n} \prod_{m|n_d} \Phi_m(t)^{-\mu(d)\cdot n/n_d} = \pm \prod_{m|n} \Phi_m(t)^{h_m}$$

mit $n_d = d \cdot f/(d, f)$ und

$$h_m = -n \sum_{d|n} \sum_{m|n_d} \mu(d)/n_d = -n \sum_{\tilde{n}|n} \frac{\#\{m : m|\tilde{n}\}}{\tilde{n}} \sum_{n_d=\tilde{n}} \mu(d).$$

Die innere Summe verschwindet, wenn f kein Teiler von $\tilde{n}$ ist, da n_d das kleinste gemeinsame Vielfache von d und f angibt. Ist f ein Teiler von $\tilde{n}$, so sind sämtliche d mit $n_d = \tilde{n}$ ein Vielfaches von

$$\tilde{d} = \prod_{v_p(f)<v_p(\tilde{n})} p^{v_p(\tilde{n})}$$

mit einem Quotienten $d/\tilde{d} \mid f/(\tilde{d},f)$. Der Fall $f/(\tilde{d},f)=1$ kann nicht eintreten, da dies sonst $f=1$ oder $\tilde{d}=\tilde{n}$ zur Folge hätte. Somit ist die innere Summe stets durch

$$\sum_{a\mid f/(\tilde{d},f)} \mu(\tilde{d}a) = \mu(\tilde{d}) \sum_{a\mid f/(\tilde{d},f)} \mu(a) = 0$$

gegeben. Folglich gelten $h_m = 0$ und $L_{\mathfrak{p}} = \pm 1$. Als Polynom in t besitzt $L_{\mathfrak{p}}$ den Absolutkoeffizienten 1 und somit folgt schließlich wie gewünscht $L_{\mathfrak{p}} = 1$. □

***Bemerkung E.3* (Cohen et al., 2002, Korollar 2.17).** — *Das auf Z eingeschränkte Eulerprodukt $\Phi(s) = \prod_{\mathfrak{p}\in Z}(1+(\ell-1)\mathcal{N}\mathfrak{p}^{-s})$ ist meromorph in $\Re(s)\geq 1$ mit einzigem Pol in $s=1$ der Ordnung $b=(\ell-1)/n$. Für den Grenzwert $c(\Phi)=\lim_{s\to 1}(s-1)^b\cdot\Phi(s)$ gilt*

$$c(\Phi) = \left(\mathrm{Res}_{s=1}(\zeta_{\tilde{F}}(s))\cdot \prod_{1\neq d\mid n} \zeta_{\tilde{F}_d}(d)^{\mu(d)}\right)^b \cdot \prod_{\mathfrak{p}\in Z}(1+(\ell-1)\cdot\mathcal{N}\mathfrak{p}^{-1}) \prod_{d\mid n}(1-\mathcal{N}\mathfrak{p}^{-d})^{\mu(d)(\ell-1)/d}$$
$$\cdot \prod_{\mathfrak{p}\in V}\prod_{d\mid n}\prod_{\mathfrak{p}_d\mid\mathfrak{p}}(1-\mathcal{N}\mathfrak{p}_d^{-d})^{-\mu(d)b}$$

Beweis. — Für die in Bemerkung E.2 betrachtete Funktion

$$\Upsilon(s) = \prod_{d\mid n}\zeta_{\tilde{F}_d}(ds)^{\mu(d)}$$

gilt die Identität

$$\frac{\Phi(s)}{\Upsilon(s)^b} = \prod_{\mathfrak{p}\in Z}\left((1+(\ell-1)\mathcal{N}\mathfrak{p}^{-s})\cdot\prod_{d\mid n}(1-\mathcal{N}\mathfrak{p}^{-ds})^{\mu(d)(\ell-1)/d}\right)\cdot\prod_{\mathfrak{p}\in V}\prod_{d\mid n}\prod_{\mathfrak{p}_d\mid\mathfrak{p}}(1-\mathcal{N}\mathfrak{p}_d^{-ds})^{\mu(d)b}.$$

Dieser Quotient ist als konvergentes unendliches Produkt über $\Re(s)=1$ hinaus holomorph. Das Produkt über die Verzweigungsstellen $\mathfrak{p}\in V$ ist endlich und für jenes über die Zerlegungsstellen $\mathfrak{p}\in Z$ gilt

$$\prod_{\mathfrak{p}\in Z}\left((1+(\ell-1)\mathcal{N}\mathfrak{p}^{-s})\cdot\prod_{d\mid n}(1-\mathcal{N}\mathfrak{p}^{-ds})^{\mu(d)(\ell-1)/d}\right) = \prod_{\mathfrak{p}\in Z}\frac{1+O\left(\mathcal{N}\mathfrak{p}^{-2s}\right)}{1+O\left(\mathcal{N}\mathfrak{p}^{-2s}\right)}.$$

Hieraus ergeben sich die Meromorphieeigenschaften von $\Phi(s)$ und der Grenzwert $c(\Phi)$. □

APPENDIX F

FUNKTIONSWACHSTUM VON $a_{\mathfrak{p}}(\boldsymbol{r})$

In diesem Kapitel wird der Beweis von Lemma 2.29 geliefert. Hier sei p eine Primzahl und

$$a_{\mathfrak{p}}(\boldsymbol{r}) = \frac{(p-1)\cdot\sum_{i=1}^{l} p^i \cdot r_i}{p\cdot\sum_{i=1}^{l} p^i\cdot(p^{r_i}-1)\cdot p^{r_1+\ldots+r_{i-1}}}$$

eine Funktion von Tupeln $\boldsymbol{r} = (r_1,\ldots,r_l)$ mit der Beschränkung $0 \le r_i \le m$. Tupel $\boldsymbol{r}$ mit der gleichen Quersumme $\sum_{i=1}^{l} r_i$ können gemäß der revers lexikographischen Ordnung verglichen werden, d.h. es gilt $\boldsymbol{s} > \boldsymbol{r}$ genau dann wenn es einen Index $1 \le i \le l$ gibt mit $s_i > r_i$ und $s_j = r_j$ für $i < j \le l$. Ziel des Lemmas ist der Nachweis, dass $a_{\mathfrak{p}}(\boldsymbol{r})$ unter Tupeln $\boldsymbol{r}$ mit fest vorgegebener Quersumme $a = \sum_{i=1}^{l} r_i$ maximal für das maximale Tupel unter der revers lexikographischen Ordnung ist.

Lemma F.1. — *Es sei $\boldsymbol{r} = (r_1,\ldots,r_l)$ ein Tupel ganzer Zahlen mit $0 \le r_i \le m$. Dann gelten die folgende Aussagen.*

(a) (Verkürzen) *Es sei k mit $r_k + r_{k+1} \le m$. Dann gilt*

$$a_{\mathfrak{p}}(\boldsymbol{s}) > a_{\mathfrak{p}}(\boldsymbol{r}) \qquad \textit{mit} \qquad s_i = \begin{cases} r_i & 1 \le i \le k-1 \\ r_k + r_{k+1} & i = k \\ r_{i+1} & k+1 \le i \le l \end{cases}$$

und der künstlichen Setzung $s_l = r_{l+1} = 0$.

(b) (Aufteilen) *Es sei k mit $\max_{1\le i\le k}(r_i) = r_k$ und $2 \le r_k \le r_{k+1} < m$. Dann gilt*

$$a_{\mathfrak{p}}(\boldsymbol{s}) > a_{\mathfrak{p}}(\boldsymbol{r}) \qquad \textit{mit} \qquad s_i = \begin{cases} r_i & i \ne k, k+1 \\ r_k - 1 & i = k \\ r_{k+1} + 1 & i = k+1. \end{cases}$$

(c) (Tauschen) *Es sei k minimal mit $r_k > r_{k+1}$. Dann gilt*

$$a_{\mathfrak{p}}(\boldsymbol{s}) > a_{\mathfrak{p}}(\boldsymbol{r}) \qquad \textit{mit} \qquad s_i = r_{\tau(i)}$$

für die Permutation $\tau = (k\ k+1)$ mit Ausnahme in den Fällen $\boldsymbol{r} = (1,\ldots,1,2,\ldots,2,1)$ oder $\boldsymbol{r} = (2,\ldots,2,1)$ bei $p = 2$.

(d) (Sortieren) *In den Ausnahmefällen aus (c) gilt*

$$a_{\mathfrak{p}}(\boldsymbol{s}) > a_{\mathfrak{p}}(\boldsymbol{r}) \qquad \textit{mit} \qquad s_i = r_{\sigma(i)}$$

für die Permutation $\sigma = (1\ l)$.

Beweis. — (a) Für den Beweis dieser Aussage setze ich $r = \sum_{i=1}^{k} p^i \cdot r_i$ und $s = \sum_{i=k+1}^{l} p^{i-1} \cdot r_i$ sowie $t = \sum_{i=1}^{k} p^i \cdot (p^{r_i} - 1) \cdot p^{r_1+\ldots+r_{i-1}}$ und $u = \sum_{i=k+1}^{l} p^{i-1} \cdot (p^{r_i} - 1) \cdot p^{r_1+\ldots+r_{i-1}}$. Dann gelten nach Voraussetzung

$$a_{\mathfrak{p}}(\boldsymbol{s}) = \frac{p-1}{p} \cdot \frac{r+s}{t+u} \qquad \text{und} \qquad a_{\mathfrak{p}}(\boldsymbol{r}) = \frac{p-1}{p} \cdot \frac{r+ps}{t+pu}$$

und die Behauptung $a_{\mathfrak{p}}(\boldsymbol{s}) > a_{\mathfrak{p}}(\boldsymbol{r})$ ist äquivalent zur Ungleichung

$$(r+s)(t+pu) > (r+ps)(t+u).$$

Nach Abzug von $rt + psu$, Zusammenführen der verbleibenden Vielfache von ru und st sowie der Multiplikation mit $p/(p-1)$ erhalte ich die äquivalente Abschätzung

$$pru = \sum_{i=1}^{k} \sum_{j=k+1}^{l} p^{i+j} \cdot r_i \cdot (p^{r_j} - 1) \cdot p^{r_1+\ldots+r_{j-1}} > \sum_{i=1}^{k} \sum_{j=k+1}^{l} p^{i+j} \cdot r_j \cdot (p^{r_i} - 1) \cdot p^{r_1+\ldots+r_{i-1}} = pst.$$

Die Gültigkeit dieser Ungleichung ist schon summandenweise ersichtlich. Die zu (i,j) gehörenden Summanden beider Seiten haben nach Division mit $p^{i+j+r_1+\ldots+r_i}$ die Gestalt

$$r_i \cdot (p^{r_j} - 1) \cdot p^{r_{i+1}+\ldots+r_{j-1}} \geq p^{r_j} - 1 \geq r_j > r_j \cdot \frac{p^{r_i} - 1}{p^{r_i}}.$$

(b) Für den Nachweis dieser Ungleichung verwende ich die Bezeichnungen $a = r_k$, $b = r_{k+1}$ und $c = r_1 + \ldots + r_{k-1}$ sowie $r = \sum_{i=1}^{k+1} p^{i-k} \cdot r_i$ und $s = \sum_{i=k+2}^{l} p^{i-k} \cdot r_i$ als Zählerkomponenten und $t = \sum_{i=1}^{k+1} p^{i-k} \cdot (p^{r_i} - 1) \cdot p^{r_1+\ldots+r_{i-1}}$ und $u = \sum_{i=k+2}^{l} p^{i-k} \cdot (p^{r_i} - 1) \cdot p^{c+r_k+\ldots+r_{i-1}}$ als Nennerkomponenten. Dann gelten nach Voraussetzung

$$a_{\mathfrak{p}}(\boldsymbol{s}) = \frac{p-1}{p} \cdot \frac{r + (p-1) + s}{t + (p^{a+c} - p^{a-1+c})(p-1) + u} \qquad \text{und} \qquad a_{\mathfrak{p}}(\boldsymbol{r}) = \frac{p-1}{p} \cdot \frac{r+s}{t+u}$$

und die behauptete Ungleichung $a_{\mathfrak{p}}(\boldsymbol{s}) > a_{\mathfrak{p}}(\boldsymbol{r})$ ist äquivalent mit

$$(r + (p-1) + s)(t+u) > (r+s)(t + (p^{a+c} - p^{a-1+c})(p-1) + u).$$

Ich starte mit den für natürliche Zahlen a, b gültigen Ungleichung

$$p^{b+1} - (2b+1)(p-1) \geq 1,$$

welche durch den Test für $b = 0$ und einen Wachstumsvergleich ersichtlich ist, und ihrer offensichtlichen Implikation

$$p^a \cdot (p^{b+1} - (2b+1)(p-1)) \geq p^a \geq 1.$$

Hieraus ergeben sich

$$p^{a+b+1} - p^a(p-1) - 1 \geq 2b(p-1)p^a = 2bp(p^a - p^{a-1})$$

und auf Grund von $pb \geq pb/(p-1) > b(p^k-1)/(p^k-p^{k-1}) = \sum_{i=1}^{k} p^{i-k}b$ und $b \geq r_i$ für $1 \leq i \leq k$ auch

$$p^{a+b+1} - p^a(p-1) - 1 \geq 2bp(p^a - p^{a-1}) > \left(\frac{p^k-1}{p^k-p^{k-1}} \cdot b + pb\right)(p^a - p^{a-1}) > r(p^a - p^{a-1}).$$

Die linke Seite dieser Ungleichung ist nach oben durch

$$tp^{-c} = \sum_{i=1}^{k-1} p^{i-k} \cdot (p^{r_i} - 1) \cdot p^{r_1+\ldots+r_{i-1}-c} + (p^a - 1) + p^a(p^b - 1)$$

abschätzbar und ich ersetze sie durch diesen Ausdruck. Nach Multiplikation mit $p^c(p-1)$ und Addition von rt ergibt sich hieraus

$$(r + (p-1))t > r(t + (p^{a+c} - p^{a-1+c})(p-1)).$$

Diese Ungleichung addiere ich nun mit der folgenden

$$(p-1)u \geq (p-1)p^{a+b+c} \sum_{i=k+2}^{l} p^{i-k}(p^{r_i} - 1) \geq (p-1)(p^{a+c} - p^{a-1+c})s$$

samt des Terms $ru + s(t+u)$ und erhalte wie gewünscht

$$(r + (p-1) + s)(t+u) > (r+s)(t + (p^{a+c} - p^{a-1+c})(p-1) + u).$$

(c) Mit den im Beweis zu (b) eingeführten Bezeichnungen gelten

$$a_{\mathfrak{p}}(\boldsymbol{s}) = \frac{p-1}{p} \cdot \frac{r + (a-b)(p-1) + s}{t + (p^a - p^b)p^c(p-1) + u} \qquad \text{und} \qquad a_{\mathfrak{p}}(\boldsymbol{r}) = \frac{p-1}{p} \cdot \frac{r+s}{t+u}$$

und die behauptete Ungleichung $a_{\mathfrak{p}}(\boldsymbol{s}) > a_{\mathfrak{p}}(\boldsymbol{r})$ ist äquivalent mit

(c.1) $$(r + (a-b)(p-1) + s)(t+u) > (r+s)(t + (p^a - p^b)p^c(p-1) + u).$$

Leider ist der Beweis hierfür via Fallunterscheidung zu führen. Für positive ganzzahlige Zahlen $x, b \geq 1$ gilt

$$x \cdot p^b - \frac{p}{p-1} \cdot (b+x) \geq p^b - \frac{p}{p-1} \cdot (b+1) \geq p\left(1 - \frac{2}{p-1}\right)$$

und daher ist die linke Seite mit Ausnahme der Fälle $(b,x) = (1,1), (2,1)$ für $p = 2$ nicht negativ. Für alle anderen Fälle gilt also

$$x \cdot (p^b - x) \geq \frac{p}{p-1} \cdot (b+x) - x = \left(\frac{b+x}{p-1} + b\right)$$

und ich kann für $x = a - b$ mit der umgeformten und mit p^{a+c+1} multiplizierten Ungleichung

$$(a-b) \cdot p^c \cdot p^{a+1} \cdot \left(p^b - 1\right) \geq p^c \cdot p^a \cdot \left(\frac{pa}{p-1} + pb\right)$$

starten. Dann gebe ich der linken Seite etwas dazu und ziehe der rechten Seite etwas ab und erhalte somit die echte Ungleichung

$$(a-b) \cdot p^c \cdot \left(p^{a+1} \cdot \left(p^b - 1\right) + (p^a - 1)\right) > \left(\frac{pa}{p-1} + pb\right) \cdot p^c \cdot (p^a - p^b).$$

An dieser Stelle kann ich bereits den Fall $(b,x) = (2,1)$ bei $p = 2$ mit einbeziehen. Dabei ist $(a,b) = (3,2)$ und diese Ungleichung ergibt $55 \cdot 2^c > 40 \cdot 2^c$. Für $(a,b,p) = (2,1,2)$ ist diese Ungleichung immer noch

zu unscharf. Die linke Seite kann leicht gemäß $t \geq p^c(p^{a+b+1} - p^a(p-1) - 1)$ erweitert werden. Für die rechte Seite nutze ich die Maximalbedingung an $a = r_k \geq r_i$ für $1 \leq i \leq k$ und erhalte

$$r = \sum_{i=1}^{k+1} p^{i-k} r_i = \sum_{i=1}^{k} p^{i-k} r_i + pb \leq \frac{p^k - 1}{p^k - p^{k-1}} \cdot a + pb < \frac{pa}{p-1} + pb.$$

Hiermit ergibt sich

$$(a-b) \cdot t > r \cdot p^c \cdot (p^a - p^b). \tag{c.2}$$

Aus dieser Ungleichung folgt nach Multiplikation mit $(p-1)$ und Addition von $r(t+u)$ die Abschätzung

$$(r + (a-b)(p-1))t + ru > r(t + p^c(p^a - p^b) + u)$$

und nach Addition mit $s(t+u)$ die Ungleichung

$$(r + (a-b)(p-1) + s)(t+u) - (a-b)(p-1)u > (r+s)(t + (p^a - p^b)p^c(p-1) + u) - s(p^a - p^b)p^c(p-1).$$

Ist einer der Subtrahenten ungleich 0 so auch der andere und jener der linken Seite ist größer als der auf der rechten Seite befindliche vermöge

$$u \geq p^{a+b+c} \cdot \sum_{i=k+2}^{l} p^{i-k}(p^{r_i} - 1) > (p^a - p^b)p^c \cdot s.$$

Hieraus folgt die gewünschte Ungleichung `c.1`. Nun ist noch der verbliebende Ausnahmefall $(a, b, p) = (2, 1, 2)$ abzuhandeln. Für $l = k+1$ ergibt das Tauschen der letzten beiden Glieder sogar einen schwächeren Wert. Für $l \neq k+1$ hingegen reicht es schon aus, das Glied $r_{k+2} = d$ mit einzubeziehen. Dabei gilt mit Einsetzen von $a = 2$, $b = 1$ und $p = 2$

$$t + p^2 p^{a+b+c}(p^d - 1) \geq p^{a+b+c+1} - p^{a+c}(p-1) - 1 + p^2 p^{a+b+c}(p^d - 1) = 2^c(11 + 32(2^d - 1))$$
$$> 2^c(12 + 8d) = p(a + b + pd)p^c(p^a - p^b) \geq (r + p^2 d)p^c(p^a - p^b).$$

Hieraus folgt die Ungleichung `c.1` auch für $l \neq k+1$.

(d) In der beschriebenen Situation muss im Fall $l = k+1$ hingegen r_l an den Anfang geschoben werden, um einen größeren Wert zu erzielen. Das Gegenbeispiel $\boldsymbol{r} = (2, 2, 2, 1)$ mit minimaler Länge zeigt, dass einfaches Tauschen nicht notwendigerweise zum Wachstum führt. Grund ist hierfür das etwas dynamischere Verhalten des binären Stellensystems bei Überträgen. Es sei x die Anzahl der Einsen und y die Anzahl der Zweien in $\boldsymbol{r}$. Dann hat der Zähler von $a_{\mathfrak{p}}(\boldsymbol{r})$ die Gestalt

$$\sum_{i=1}^{x-1} 2^i \cdot 1 + \sum_{i=x}^{x+y-1} 2^i \cdot 2 + 2^{x+y} \cdot 1 = (2^x - 2) + 2 \cdot (2^{x+y} - 2^x) + 2^{x+y} = 2^x \cdot (3 \cdot 2^y - 1) - 2$$

und die Hälfte des Nenners die Form

$$\begin{aligned}
&\sum_{i=1}^{x-1} 2^i \cdot (2^1-1) \cdot 2^{i-1} + \sum_{i=x}^{x+y-1} 2^i \cdot (2^2-1) \cdot 2^{1(x-1)+2(i-x)} + 2^{x+y} \cdot 2^{1(x-1)+2y} \cdot (2^1-1) \\
&= \frac{2}{3} \cdot (4^{x-1}-1) + 3 \cdot 2^{2x-1} \cdot \sum_{i=x}^{x+y-1} 2^{3(i-x)} + \frac{1}{2} \cdot 4^x 8^y \\
&= \frac{2}{3} \cdot (4^{x-1}-1) + \frac{3 \cdot 2 \cdot 4^{x-1}}{7} \cdot (8^y-1) + \frac{1}{2} \cdot 4^x 8^y \\
&= \frac{5}{7} \cdot 4^x 8^y - \frac{1}{21} \cdot 4^x - \frac{2}{3} \;=\; \frac{1}{21} \cdot (15 \cdot 4^x 8^y - 4^x - 14).
\end{aligned}$$

Für $a_{\mathfrak{p}}(\boldsymbol{s})$ sind Zähler und Nennerhälfte von der Gestalt

$$\sum_{i=1}^{x} 2^i \cdot 1 + \sum_{i=x+1}^{x+y} 2^i \cdot 2 = (2^{x+1}-2) + 2 \cdot (2^{x+y+1} - 2^{x+1}) = 2^x \cdot (4 \cdot 2^y - 2) - 2$$

und

$$\begin{aligned}
&\sum_{i=1}^{x} 2^i \cdot 2^{i-1} + \sum_{i=x+1}^{x+y} 2^i \cdot 3 \cdot 2^{2(i-(x+1))+x} \;=\; \frac{2}{3} \cdot (4^x - 1) + \frac{3 \cdot 2 \cdot 4^x}{7} \cdot (8^y - 1) \\
&= \frac{6}{7} \cdot 4^x 8^y - \frac{4}{21} \cdot 4^x - \frac{2}{3} \;=\; \frac{1}{21} \cdot (18 \cdot 4^x 8^y - 4 \cdot 4^x - 14).
\end{aligned}$$

Nach Voraussetzung ist also

$$a_{\mathfrak{p}}(\boldsymbol{s}) = \frac{21}{2} \cdot \frac{2^x \cdot (4 \cdot 2^y - 2) - 2}{18 \cdot 4^x 8^y - 4 \cdot 4^x - 14} \qquad \text{und} \qquad a_{\mathfrak{p}}(\boldsymbol{r}) = \frac{21}{2} \cdot \frac{2^x \cdot (3 \cdot 2^y - 1) - 2}{15 \cdot 4^x 8^y - 4^x - 14}$$

und meine Behauptung ist äquivalent mit

(d.1) $$(2^x \cdot (4 \cdot 2^y - 2) - 2) \cdot (15 \cdot 4^x 8^y - 4^x - 14) \;>\; (2^x \cdot (3 \cdot 2^y - 1) - 2) \cdot (18 \cdot 4^x 8^y - 4 \cdot 4^x - 14)$$

für $x, y \geq 1$. Ich starte mit der offensichtlich richtigen Ungleichung

$$3 \cdot 2^x \cdot (8^y - 1) \geq 6 \cdot (8^y - 1) > 7 \cdot (2^y - 1)$$

und ergänze die linke Seite zu

$$3 \cdot (2^y - 2) \cdot 4^x 8^y + (4 \cdot 2^y - 1) \cdot 4^x + 3 \cdot 2^x \cdot (8^y - 1) > 7 \cdot (2^y - 1).$$

Diese Ungleichung wird mit 2^{x+1} multipliziert und es ergibt sich

$$2^x \cdot ((6 \cdot 2^y - 12) \cdot 4^x 8^y + (8 \cdot 2^y - 2) \cdot 4^x + 6 \cdot 2^x \cdot (8^y - 1)) > 14 \cdot 2^x \cdot (2^y - 1).$$

Nach Abzug von $14 \cdot 2^x \cdot (4 \cdot 2^y - 2)$ erhalte ich

$$\begin{aligned}
&2^x \cdot ((6 \cdot 2^y - 12) \cdot 4^x 8^y + (8 \cdot 2^y - 2) \cdot 4^x + 6 \cdot 2^x \cdot (8^y - 1) - 14 \cdot (4 \cdot 2^y - 2)) \\
&> \; -14 \cdot 2^x \cdot (3 \cdot 2^y - 1).
\end{aligned}$$

Nun addiere ich $2^x \cdot (54 \cdot 2^y - 18) \cdot 4^x 8^y = 2^x \cdot (3 \cdot 2^y - 1) \cdot (18 \cdot 4^x 8^y)$ und erhalte

$$\begin{aligned}
&2^x \cdot ((60 \cdot 2^y - 30) \cdot 4^x 8^y + (8 \cdot 2^y - 2) \cdot 4^x - 14 \cdot (4 \cdot 2^y - 2) + 6 \cdot 2^x \cdot (8^y - 1)) \\
&> 2^x \cdot (3 \cdot 2^y - 1) \cdot (18 \cdot 4^x 8^y - 14).
\end{aligned}$$

Anschließend subtrahiere ich mit $2^x \cdot (12 \cdot 2^y - 4) \cdot 4^x = 2^x \cdot (3 \cdot 2^y - 1) \cdot (4 \cdot 4^x)$ und durch

$$\begin{aligned} & 2^x \cdot ((60 \cdot 2^y - 30) \cdot 4^x 8^y - (4 \cdot 2^y - 2) \cdot 4^x - 14 \cdot (4 \cdot 2^y - 2) + 6 \cdot 2^x \cdot (8^y - 1)) \\ > \; & 2^x \cdot (3 \cdot 2^y - 1) \cdot (18 \cdot 4^x 8^y - 4 \cdot 4^x - 14) \end{aligned}$$

ist das erklärte Ziel schon langsam vom Hochmast erkennbar. Auf der rechten Seite fehlt noch der Term $-2 \cdot (18 \cdot 4^x 8^y - 4 \cdot 4^x - 14)$, dessen Addition die gewünschten Ausdrücke

$$(2^x \cdot (3 \cdot 2^y - 1) - 2) \cdot (18 \cdot 4^x 8^y - 4 \cdot 4^x - 14)$$

auf der rechten und

$$\begin{aligned} & 2^x \cdot (4 \cdot 2^y - 2) \cdot (15 \cdot 4^x 8^y - 4^x - 14) + 6 \cdot 4^x \cdot (8^y - 1) - 2 \cdot (18 \cdot 4^x 8^y - 4 \cdot 4^x - 14) \\ = \; & 2^x \cdot (4 \cdot 2^y - 2) \cdot (15 \cdot 4^x 8^y - 4^x - 14) - 2 \cdot (15 \cdot 4^x 8^y - 4^x - 14) \\ = \; & (2^x \cdot (4 \cdot 2^y - 2) - 2) \cdot (15 \cdot 4^x 8^y - 4^x - 14) \end{aligned}$$

auf der linken Seite ergibt. Hieraus folgt schließlich die Abschätzung `d.1`. □

APPENDIX G

GRUPPENERWEITERUNGEN

In diesem Anhangskapitel wird ein Beweis von Lemma 2.12 demonstriert. Die Voraussetzungen und das Resultat werden im folgenden Abschnitt dargelegt.

Gruppenerweiterungen mit Schnittbedingung. — Es seien $X \geq Y$ und $G \geq H$ Erweiterungen abelscher p-Gruppen mit nichttrivialen elementarabelschen Quotienten $X/Y = Z$ und $G/H = I$. Die Gruppen X und Y erlauben eine gemeinsame Zerlegung

$$X = \tilde{Y} \times \tilde{Z} \qquad \text{und} \qquad Y = \tilde{Y} \times p \cdot \tilde{Z} \qquad \text{mit} \qquad \tilde{Z} = Z_{p^\nu}^{\dim Z}.$$

Des Weiteren benutze ich folgende Notationen.

(i) Es seien $g_i = \dim G[p^i]/G[p^{i-1}]$ und $h_i = \dim H[p^i]/H[p^{i-1}]$ die p^i-Ränge von G und H sowie $s_i = g_i - h_i$ ihre Differenz. Des Weiteren sei $r = s_1 + \ldots + s_e = \dim G/H$.

(ii) Mit $\sqrt{V} = \{y \in Y : p \cdot y \in V\}$ sei die maximale Hülle in Y, in welcher sich V elementarabelsch erweitern lässt, gekennzeichnet. Außerdem sei $d_i = \dim \sqrt{V}[p^i]/\langle \sqrt{V}[p^{i-1}], V[p^i]\rangle$ die Differenz der p^i-Ränge von $\sqrt{V}$ und V.

(iii) Entsprechend sei mit $\sqrt{V}^\circ = \{y \in X : p \cdot y \in V\}$ die maximale Hülle in X gekennzeichnet und $d_i^\circ = \dim \sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$.

Für eine zu H isomorphe Gruppe $V \leq Y$ bezeichne

$$\mathcal{U}_G = \{U \leq X : U \cap Y = V,\ U \simeq G\}$$

die Menge aller gesuchten Untergruppen und

$$c(V, G) = |\mathcal{U}_G| = |\{U \leq X : U \cap Y = V,\ U \simeq G\}|$$

ihre Anzahl. Dann ergeben sich folgende Formeln für $c(V, G)$.

Lemma G.1. — (a) *Im Fall $\nu = 1$ gelten $X = Y \times Z$ und*

$$c(V, G) = (Y[p] : V[p])^r \cdot \prod_{i=1}^{e} \begin{bmatrix} \dim Z - \sum_{j=1}^{i-1} s_j \\ s_i \end{bmatrix}_p \cdot \prod_{i=2}^{e} \prod_{j=2}^{i-1} \prod_{k=0}^{s_i - 1} p^{d_j} \cdot (p^{d_i} - p^k).$$

(b) *Im Fall* $\nu > 1$ *gilt*

$$c(V,G) = (Y[p] : V[p])^r \cdot \begin{bmatrix} 0 \\ s_1 \end{bmatrix}_p \cdot \prod_{i=2}^{e} \prod_{j=2}^{i-1} \prod_{k=0}^{s_i-1} p^{d_j} \cdot (p^{d_i} - p^k)$$

$$\cdot \sum_{(t_2,\ldots,t_e)} \prod_{i=2}^{e} \begin{bmatrix} -s_1 + \sum_{j=2}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \cdot \begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \prod_{k=t_i}^{s_i-1} \frac{1}{p^{d_i} - p^k} \cdot \frac{p^{d_i} \cdot \prod_{j=2}^{i-1} p^{d_j^\circ - d_j}}{p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}},$$

wobei die Summe über alle Tupel $(t_2, \ldots, t_e)$ *mit* $0 \leq t_i \leq s_i$ *läuft.*

Erzeugendensysteme. — In diesem Abschnitt werden Gruppen $U = \langle S, V \rangle$ untersucht, welche über V durch ein System S von Elementen aus der Hülle $\sqrt{V}^\circ$ erzeugt werden. Solche Systeme führen zu direkten Produkten $U = \langle S \rangle \times W$ mit $W \leq V = p \cdot \langle S \rangle \times W$.

Bemerkung G.2. — *Es seien* $E_1, \ldots, E_e$ *minimale Erzeugendensysteme mit der Eigenschaft*

$$\sqrt{V}^\circ[p^i] = \langle E_i, \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle.$$

Dann hat die von $E = E_1 \cup \ldots \cup E_e$ *erzeugte Gruppe* $\langle E \rangle$ *ein Komplement in* $\sqrt{V}^\circ$ *und es gilt*

$$\sqrt{V}^\circ \simeq \langle E \rangle \times \sqrt{V}^\circ / \langle E \rangle \simeq \langle E_1 \rangle \times \ldots \times \langle E_e \rangle \times \sqrt{V}^\circ / \langle E \rangle \qquad \text{mit} \qquad \langle E_i \rangle \simeq Z_{p^i}^{|E_i|}.$$

Beweis. — Zunächst zeige ich, dass die Erzeugendensysteme zu direkten Produkten führen und starte mit dem Nachweis der Isomorphie zwischen $\langle E_i \rangle$ und $Z_{p^i}^{e_i}$ mit $e_i = |E_i|$. Offensichtlich besteht E_i nur aus Elementen der Ordnung p^i. Sind $u_1, \ldots, u_{e_i}$ die Elemente von E_i, so ist

$$Z_{p^i}^{e_i} \twoheadrightarrow \langle E_i \rangle, \ (a_1, \ldots, a_{e_i}) \mapsto \sum_{j=1}^{e_i} a_j \cdot u_j$$

ein surjektiver Homomorphismus. Ich nehme an, es gebe eine Kombination

$$u = \sum_{j=1}^{e_i} a_j \cdot u_j = 0 \qquad \text{mit} \qquad 1 \leq a_j \leq p^i.$$

Es sei $m \leq i$ das Supremum aller natürlichen Zahlen $n \in \mathbf{N}$ mit $p^n \mid a_j$. Dann haben die Koeffizienten der Kombination u die Gestalt $a_j = p^m b_j$ und

$$y = p^{-m} \cdot u = \sum_{j=1}^{e_i} b_j \cdot u_j \in \langle E_i \rangle$$

ist in der Torsionsgruppe $\sqrt{V}^\circ[p^m]$ enthalten. Des Weiteren ist y linear unabhängig im $\mathbb{F}_p$-Vektorraum $\sqrt{V}^\circ[p^i] / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle$, da mindestens ein Koeffizient b_j zu p teilerfremd ist und die Restklassen von $u_1, \ldots, u_{e_i}$ eine Basis bilden. Somit hat y Ordnung p^i. Das zeigt $i \leq m$ und $a_j = p^i$ für $1 \leq j \leq e_i$. Hieraus folgt

$$\langle E_i \rangle = \prod_{j=1}^{e_i} \langle u_j \rangle \simeq Z_{p^i}^{e_i}.$$

Insbesondere ist jedes Element in $\langle E_i\rangle$ ein Vielfaches $a \cdot u$ eines Elements $u \in \langle E_i\rangle \setminus \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$ der Ordnung p^i. Nun zeige ich entsprechend, dass die kanonische Abbildung

$$\langle E_1\rangle \times \ldots \times \langle E_e\rangle \twoheadrightarrow \langle E_1, \ldots, E_e\rangle$$

ein Isomorphismus ist. Eine Kombination $\sum_{i=1}^e x_i = 0$ von $x_i \in \langle E_i\rangle$ sei im Kern enthalten. Dann gibt es Elemente $u_i \in \langle E_i\rangle \setminus \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$ der Ordnung p^i und ganze Zahlen $0 \leq a_i < p^i$ mit $x_i = a_i \cdot u_i$, sodass die Relation $\sum_{i=1}^e a_i \cdot u_i = 0$ erfüllt ist. Es ist $a_i = 0$ für $1 \leq i \leq e$ zu zeigen. Dazu nehme ich an, es gebe mindestens ein Index i mit $a_i \neq 0$. Das Supremum m aller natürlichen Zahlen $n \in \mathbf{N}$ mit der Eigenschaft $p^n \mid a_i$ für $1 \leq i \leq e$ ist dann endlich und es gibt einen maximalen Index $1 \leq k \leq e$ mit $p^m \mid\mid a_k$. Auf Grund der Voraussetzung $a_k < p^k$ ist die Relation zwischen diesen beiden Zahlen $m < k$. Die Koeffizienten a_i können in der Form $a_i = p^m b_i$ angeben werden und ich betrachte nun die folgenden Elemente

$$x = \sum_{i=1}^{e} b_i \cdot u_i = y + z \qquad \text{mit} \qquad y = \sum_{i \leq k} b_i \cdot u_i \qquad \text{und} \qquad z = \sum_{i > k} b_i \cdot u_i,$$

welche von $\langle E_1, \ldots, E_e\rangle$ erzeugt und somit in der elementarabelschen Hülle $\sqrt{V}^\circ$ enthalten sind. Auf Grund der Identität $p^m \cdot x = 0$ ist x Element der Torsionsgruppe $\sqrt{V}^\circ[p^m]$. Die Ordnung von y ist exakt p^k, da y wegen der Relationen $p \nmid b_k$ und

$$y = b_k \cdot u_k + \sum_{i<k} b_i \cdot u_i \in b_k \cdot u_k + \sqrt{V}^\circ[p^{k-1}]$$

linear unabhängig im $\mathbb{F}_p$-Vektorraum $\sqrt{V}^\circ[p^k]/\langle \sqrt{V}^\circ[p^{k-1}], V[p^k]\rangle$ ist. Auf Grund der Ungleichung $m < k$ gilt $z = x - y \in \sqrt{V}^\circ[p^k]$. Des Weiteren ist z auch in V enthalten. Denn k ist das Maximum der Indizes $1 \leq i \leq e$ mit $p \nmid a_i$ und somit folgen $p \mid b_i$ und $b_i \cdot u_i \in V$ für $i > k$. Folglich ist auch

$$x = y + z \in y + V[p^k]$$

linear unabhängig im $\mathbb{F}_p$-Vektorraum $\sqrt{V}^\circ[p^k]/\langle \sqrt{V}^\circ[p^{k-1}], V[p^k]\rangle$ und als ein solches Element von der Ordnung p^k. Dies steht im Widerspruch zu $x \in \sqrt{V}^\circ[p^m]$ und es folgt $a_i = 0$ für $1 \leq i \leq e$.

Als Letztes ist die Existenz eines Komplements nachzuweisen. Dazu zeige ich, dass $E = E_1 \cup \ldots \cup E_e$ zu einem minimalen Erzeugendensystem von $\sqrt{V}^\circ$ ergänzt werden kann. Es sei $F = \{x_1, \ldots, x_s\}$ ein Erzeugendensystem von $\sqrt{V}^\circ$ und $u \in E_i$ von der Gestalt $\sum a_j \cdot x_j$. Es sei v die Teilsumme $\sum' a_j \cdot x_j$ über alle Indizes j mit $p \mid a_j$ und w die Teilsumme $\sum'' a_j \cdot x_j$ der restlichen Indizes mit $(\langle x_j\rangle : 1) < p^i = (\langle u\rangle : 1)$ und x der Restsummand, d.h. es gilt $u = x + v + w$. Folglich besteht x nur aus Summanden $a_j \cdot x_j$ mit $(\langle x_j\rangle : 1) = p^i$ und $p \nmid a_j$. Diese Summe ist nicht leer, denn es sind v in V und w in $\sqrt{V}^\circ[p^{i-1}]$ enthalten und es folgt $u = x + \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$. Da $u \in E_i$ in $\sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$ linear unabhängig ist, trifft dies auch auf x zu. Folglich kann ich irgendeinen Summanden $x_j \in F$ von x durch das Element $u \in E_i$ ersetzen und F bleibt nach diesem Tausch ein Erzeugendensystem von $\sqrt{V}^\circ$. Durch sukzessives Fortfahren kann eine Teilmenge von F durch E ausgetauscht werden und es folgt die Existenz eines Komplements zu $\langle E\rangle$. □

Korollar G.3. — *Es seien $S_i \subset \sqrt{V}^\circ[p^i]$ linear unabhängige Systeme über $\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$, d.h. es gilt $|S_i| = \dim\langle S_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$. Dann gilt für die von $S = S_1 \cup \ldots \cup S_e$ über V erzeugte Gruppe*

$$\langle S, V\rangle \simeq \langle S_1\rangle \times \ldots \times \langle S_e\rangle \times V/(p \cdot \langle S\rangle) \qquad \text{mit} \qquad \langle S_i\rangle \simeq Z_{p^i}^{s_i}.$$

Beweis. — Die Systeme S_i können zu einem Erzeugendensystem E_i von $\sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$ ergänzt werden und besitzen somit nach Bemerkung G.2 die Eigenschaft

$$\sqrt{V}^\circ \simeq \langle S_1\rangle \times \ldots \times \langle S_e\rangle \times \sqrt{V}^\circ/\langle S\rangle \qquad \text{mit} \qquad \langle S_i\rangle \simeq Z_{p^i}^{s_i}.$$

Nach Schnittbildung mit der Gruppe $\langle S, V\rangle$ erhalte ich die gewünschte Zerlegung in ein direktes Produkt. Denn für Gruppen $A \geq B \geq C$ mit $A = C \times D$ ist mit dem Element $b = (c, d) \in B$ auch das Element $b - (c, 0) = (0, d) \in \langle B, C\rangle = B$ enthalten und folglich ist $D \cap B$ ein Komplement von C in B. Somit gilt

$$\langle S, V\rangle \simeq \langle S_1\rangle \times \ldots \times \langle S_e\rangle \times \langle S, V\rangle/\langle S\rangle \qquad \text{mit} \qquad \langle S_i\rangle \simeq Z_{p^i}^{s_i}.$$

Nun ist noch der Nachweis zu erbringen, dass das Komplement auch als Untergruppe von V zu realisieren ist. Komponentenweise gilt $\langle S_i\rangle \cap Y = p \cdot \langle S_i\rangle$, da sonst die lineare Unabhängigkeit von S_i in $\sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$ verletzt wäre. Somit folgen

$$\langle S\rangle \cap V = p \cdot \langle S\rangle$$

und

$$\langle S, V\rangle/\langle S\rangle \simeq V/(V \cap \langle S\rangle) = V/(p \cdot \langle S\rangle).$$

Somit besitzen $\langle S, V\rangle$ und V einen gemeinsamen direkten Faktor. □

Gruppenerweiterungen ohne Schnittbedingung. — In der nächsten Bemerkung gebe ich einen Überblick über die Gesamtheit der zu G isomorphen Erweiterungen U von V innerhalb der elementarabelsche Hülle $\sqrt{V}^\circ$.

Bemerkung G.4. — *Für die zu G isomorphen Gruppen U mit $V \leq U \leq \sqrt{V}^\circ$ gilt folgende Charakterisierung.*

(a) *Es seien U isomorph zu G mit $V \leq U \leq \sqrt{V}^\circ$ und S_i minimale Erzeugendensysteme mit der Eigenschaft $U[p^i] = \langle S_i, U[p^{i-1}], V[p^i]\rangle$. Dann gilt $U = \langle S_1, \ldots, S_e, V\rangle$ und die Systeme S_i haben die Länge und Dimension*

$$|S_i| = s_i = \dim\langle S_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle.$$

(b) *Es seien $S_i \subset \sqrt{V}^\circ[p^i]$ Systeme der Länge und Dimension*

$$|S_i| = s_i = \dim\langle S_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle.$$

Dann ist die von den Systemen S_i über V erzeugte Gruppe $U = \langle S_1, \ldots, S_e, V\rangle$ isomorph zu G mit $V \leq U \leq \sqrt{V}^\circ$.

Beweis. — (a) Selbstverständlich wird U von $S = S_1 \cup \ldots \cup S_e$ über V erzeugt, denn jedes Element von U ist in einer der Torsionsgruppen $U[p^i]$ enthalten. Die Länge der Systeme S_i ergibt sich aus

$$|S_i| = \dim U[p^i]/\langle U[p^{i-1}], V[p^i]\rangle = \dim G[p^i]/G[p^{i-1}] - \dim H[p^i]/H[p^{i-1}] = g_i - h_i = s_i.$$

Des Weiteren ergibt sich aus der Inklusion $U \leq \sqrt{V}^\circ$ die kanonische Einbettung

$$U[p^i]/\langle U[p^{i-1}], V[p^i]\rangle \hookrightarrow \sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle. \tag{G.4.1}$$

Hieraus folgt $s_i = \dim\langle S_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$.

(b) Die Eigenschaft $V \leq U \leq \sqrt{V}^\circ$ ergibt sich aus der Konstruktion von $U = \langle S, V\rangle$. Vermöge der exakten Sequenz

$$1 \to H[p^i]/H[p^{i-1}] \simeq V[p^i]/V[p^{i-1}] \to U[p^i]/U[p^{i-1}] \to U[p^i]/\langle U[p^{i-1}], V[p^i]\rangle \to 1$$

hat U die p^i-Ränge $\dim U[p^i]/U[p^{i-1}] = h_i + s_i = g_i = \dim G[p^i]/G[p^{i-1}]$. Somit besitzt U die gleichen Elementarteiler wie G und ist daher zu G isomorph. □

Bemerkung G.5. — *Für die Anzahl der zu G isomorphen Gruppen U mit $V \leq U \leq \sqrt{V}^\circ$ gilt*

$$|\{U \leq \sqrt{V}^\circ : V \leq U \simeq G\}| = \prod_{i=1}^{e} \begin{bmatrix} d_i^\circ \\ s_i \end{bmatrix}_p \cdot \left(\frac{(\sqrt{V}^\circ[p^{i-1}] : V[p^{i-1}])}{\prod_{j=1}^{i-1} p^{s_j}} \right)^{s_i}.$$

Beweis. — Nach Bemerkung G.4 werden die gesuchten Gruppen U von den Systemen $S_i \subset \sqrt{V}^\circ[p^i]$ der Länge und Dimension $|S_i| = s_i = \dim\langle S_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$ erzeugt. Gemäß der Einbettung G.4.1 sind die Räume $\langle U[p^i], \sqrt{V}^\circ[p^{i-1}]\rangle/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$ Invarianten der Gruppe U und somit unabhängig von der Auswahl der Erzeugendensysteme S_i. Für die Wahl eines s_i-dimensionalen Raum W_i in $\sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$ als Invariante stehen dazu

$$\begin{bmatrix} \dim \sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle \\ s_i \end{bmatrix}_p = \begin{bmatrix} d_i^\circ \\ s_i \end{bmatrix}_p$$

Möglichkeiten offen. Für eine fest gewählte Basis $[y_{i1}], \ldots, [y_{is_i}]$ von Restklassen gibt es dann modulo Vielfacher aus V genau

$$(\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle : V[p^i])^{s_i} = (\sqrt{V}^\circ[p^{i-1}] : V[p^{i-1}])^{s_i}$$

Optionen, Vertreter $y_{i1}, \ldots, y_{is_i}$ der Klassen auszuwählen. Die von den Systemen $S_i = \{y_{i1}, \ldots, y_{is_i}\}$ über V erzeugte Gruppe $U = \langle S, V\rangle$ mit $S = S_1 \cup \ldots \cup S_e$ ist isomorph zu G und erfüllt die Inklusionskette $V \leq U \leq \sqrt{V}^\circ$. Hier führen genau die Systeme S und $\tilde{S}$ zu der gleiche Gruppe $U = \langle S, V\rangle = \langle \tilde{S}, V\rangle$, wenn sich die Vertreter y_{ij} und $\tilde{y}_{ij}$ nur durch Elemente aus $\langle S_1, \ldots, S_{i-1}, V\rangle = \langle \tilde{S}_1, \ldots, \tilde{S}_{i-1}, V\rangle$ unterscheiden. Da Elemente aus V bereits bei der Auswahl der Repräsentanten ignoriert wurde, ist die Zahl der gefundenen Erzeugendensysteme S_i noch durch

$$(\langle S_1, \ldots, S_{i-1}, V[p^{i-1}]\rangle : V[p^{i-1}])^{s_i} = (\langle S_1, \ldots, S_{i-1}\rangle : \langle S_1, \ldots, S_{i-1}\rangle \cap V[p^{i-1}])^{s_i} = p^{(s_1+\ldots+s_{i-1})\cdot s_i}$$

zu teilen. Die letzte Gleichung folgt auf Grund von $\langle S_j\rangle \cap V = p \cdot \langle S_j\rangle$ gemäß der Basiseigenschaft der Systeme S_j und $\langle S_1, \ldots, S_{i-1}\rangle = \langle S_1\rangle \times \ldots \times \langle S_{i-1}\rangle$. □

Gruppenerweiterungen mit Schnittbedingung. — Im folgenden Abschnitt werden die zu G isomorphen Erweiterungen U von V mit der zusätzlichen Schnittbedingung $U \cap Y = V$ strukturell untersucht und gezählt. Die Gesamtheit dieser Gruppen U ist wie bekannt mit

$$\mathcal{U}_G = \{U \subset X : U \cap Y = V,\ U \simeq G\} = \{U \subset \sqrt{V}^\circ : U \cap Y = V,\ U \simeq G\}$$

gekennzeichnet. Letztere Gleichung folgt hierbei aus $p \cdot X \leq Y$. Nach dem vorhergehenden Abschnitt können die zu G isomorphen Erweiterungen $U = \langle S_1, \ldots, S_e, V\rangle$ von V innerhalb der elementarabelschen Hülle $\sqrt{V}^\circ$ durch Erzeugendensysteme $S_i \subset \sqrt{V}^\circ[p^i]$ der Länge und Dimension s_i konstruiert werden. Die naheliegende Intuition, dass die Schnittbedingung $U \cap Y = V$ äquivalent zu $S_i \subset \sqrt{V}^\circ[p^i]/\sqrt{V}[p^i]$ sein müsste, belege ich mit der folgenden Bemerkung.

Bemerkung G.6. — *Für die Gruppen $U \in \mathcal{U}_G$ gilt die folgende Charakterisierung.*

(a) *Für eine Gruppe $U \in \mathcal{U}_G$ seien $S_i \subset \sqrt{V}^\circ[p^i]$ minimale Erzeugendensysteme mit der Eigenschaft $U[p^i] = \langle S_i, U[p^{i-1}], V[p^i]\rangle$. Dann gilt $S_i \subset \sqrt{V}^\circ[p^i] \setminus \sqrt{V}[p^i]$.*

(b) *Es seien $S_i \subset \sqrt{V}^\circ[p^i] \setminus \sqrt{V}[p^i]$ Systeme der Länge und Dimension*

$$|S_i| = s_i = \dim\langle S_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle/\langle\sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle.$$

Dann gilt $U \in \mathcal{U}_G$ für $U = \langle S_1, \ldots, S_e, V\rangle$.

Beweis. — (a) Für ein Element $y \in S_i \cap \sqrt{V}[p^i]$ folgte $\langle V, y\rangle \leq U \cap Y = V$ und daher $y \in V$ im Widerspruch zur Minimalität von S_i.

(b) Es sei $U = \langle S_1, \ldots, S_e, V\rangle$. Dann ergibt sich aus Bemerkung G.4 die Isomorphie $U \simeq G$ und es gilt offensichtlich $U \cap Y \geq V$. Des Weiteren ist U nach Korollar G.3 isomorph zum direkten Produkt

$$U \simeq \langle S_1\rangle \times \ldots \times \langle S_e\rangle \times V/(p \cdot \langle S_1, \ldots, S_e\rangle) \qquad \text{mit} \qquad \langle S_i\rangle \simeq Z_{p^i}^{s_i}.$$

Folglich ist die gewünschte Inklusion $U \cap Y \leq V$ schon via $\langle x\rangle \cap Y \leq V$ für $x \in S_i$ überprüfbar. Es sei also $x \in S_i$ beliebig vorgegeben. Definitionsgemäß sind x in $X \setminus Y$ und $p \cdot x$ in V enthalten. Hieraus folgt

$$\langle x\rangle \cap Y = \langle p \cdot x\rangle \leq V$$

und somit zusammenfassend $U \cap Y = V$. □

Ein naiver Ansatz, die Erzeugendensystem S_i aus den Räumen $\sqrt{V}^\circ[p^i]/\langle\sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle$ zu gewinnen, ist zum Scheitern verurteilt. Beispielsweise gilt

$$\sqrt{V}^\circ[p^i] = \langle\sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle$$

im Fall $X = Y \times Z$ und $i \geq 2$. Abhilfe dieser Problematik kann aus folgender Unterteilung der Systeme $S_i = T_i \cup S_i \setminus T_i$ gewonnen werden.

Bemerkung G.7. — *Für die Gruppen $U \in \mathcal{U}_G$ gilt die folgende Charakterisierung.*

(a) *Für $U \in \mathcal{U}_G$ gibt es Erzeugendensysteme $S_i \subset \sqrt{V}^\circ[p^i] \setminus \sqrt{V}[p^i]$ der Länge s_i mit der Eigenschaft $U[p^i] = \langle S_i, U[p^{i-1}], V[p^i]\rangle$ und ein Teilsystem $T_i = S_i \cap \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle$ der Länge und Dimension*

$$|T_i| = \dim\langle T_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$$

und

$$|S_i \setminus T_i| = \dim\langle S_i \setminus T_i, \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle.$$

(b) *Es seien $S_i \subset \sqrt{V}^\circ[p^i] \setminus \sqrt{V}[p^i]$ Systeme der Länge s_i mit den jeweiligen Teilsystemen $T_i = S_i \cap \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle$ der Länge und Dimension*

$$|T_i| = \dim\langle T_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$$

und

$$|S_i \setminus T_i| = \dim\langle S_i \setminus T_i, \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle.$$

Dann gilt $U \in \mathcal{U}_G$ für $U = \langle S_1, \ldots, S_e, V\rangle$.

Beweis. — (a) Es seien $T_i \subset \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle$ ein Repräsentantensystem einer Basis des Kerns der surjektiven Abbildung

$$\psi : U_i = U[p^i]/\langle U[p^{i-1}], V[p^i]\rangle \twoheadrightarrow U[p^i]/\left(U[p^i] \cap \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle\right)$$

und $S_i \supseteq T_i$ ein zu einer Basis von U_i ergänztes System. Dann hat S_i nach Bemerkung G.4 die Länge und Dimension s_i und nach Bemerkung G.6 gilt $S_i \subset \sqrt{V}^\circ[p^i] \setminus \sqrt{V}[p^i]$. Auf Grund von $U[p^{i-1}] \leq \sqrt{V}^\circ[p^{i-1}]$ folgt aus dem Isomorphiesatz

$$|T_i| = \dim\langle T_i, U[p^{i-1}], V[p^i]\rangle / \langle U[p^{i-1}], V[p^i]\rangle = \dim\langle T_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle.$$

Offensichtlich ist $S_i \setminus T_i$ eine Basis des Bildes $\psi(U_i)$ und es gilt wiederum nach dem Isomorphiesatz

$$|S_i \setminus T_i| = \dim\langle S_i \setminus T_i, \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle.$$

(b) Es sei $U = \langle S_1, \ldots, S_e, V\rangle$. Dann erfüllt U nach Bemerkung G.6 die gewünschte Schnittbedingung $U \cap Y = V$. Für die Isomorphie von U mit G ist nach Bemerkung G.4 lediglich zu zeigen, dass S_i die Dimension

$$s_i = \dim\langle S_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$$

besitzt. Dies folgt direkt aus der Dimensionsformel der linearen Abbildung

$$\langle S_i, \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle \twoheadrightarrow \langle S_i, \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle / \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle,$$

für welche voraussetzungsgemäß $|T_i|$ die Dimension des Kerns und $|S_i \setminus T_i|$ jene des Bilds angibt. □

Bemerkung G.8. — *Es seien $U \in \mathcal{U}_G$ mit den Erzeugendensystemen $S_i \supseteq T_i$ von der in Bemerkung G.7 beschriebenen Form und $t_i = |T_i|$. Dann beträgt die Anzahl solcher geordneten Systeme $S_1, \dots, S_e$ modulo Vielfacher aus V genau*

$$\prod_{i=1}^{e} \Big(\prod_{k=0}^{t_i-1} (p^{t_i} - p^k) \Big) \cdot \Big(\prod_{k=0}^{s_i-t_i-1} (p^{s_i-t_i} - p^k) \Big) \cdot \Big(p^{t_i \cdot (s_i - t_i)} \cdot \prod_{j=1}^{i-1} p^{s_j \cdot s_i} \Big)$$

Beweis. — Nach Bemerkung G.7 setzen sich die Systeme S_i mit $U[p^i] = \langle S_i, U[p^{i-1}], V[p^i] \rangle$ aus einem Repräsentantensystem T_i einer Basis des t_i-dimensionalen Raums

$$A_i = U[p^i] \cap \langle \sqrt{V}^{\circ}[p^{i-1}], \sqrt{V}[p^i] \rangle / \langle U[p^{i-1}], V[p^i] \rangle$$

und einem Repräsentantensystem $S_i \setminus T_i$ einer Basis des $(s_i - t_i)$-dimensionalen Raums

$$B_i = U[p^i]/U[p^i] \cap \langle \sqrt{V}^{\circ}[p^{i-1}], \sqrt{V}[p^i] \rangle$$

zusammen. Die Wahlmöglichkeiten für eine geordnete Basis $([x_{i1}], \dots, [x_{it_i}])$ von A_i beträgt

$$\prod_{k=0}^{t_i-1} \big(|A_i| - p^k \big) = (p^{t_i} - 1) \cdots (p^{t_i} - p^{t_i - 1}).$$

Die Repräsentantenanzahl einer Restklasse $[x_{ij}]$ modulo Vielfacher aus V beträgt dann

$$(\langle U[p^{i-1}], V[p^i] \rangle : V[p^i]) = (U[p^{i-1}] : V[p^{i-1}]) = (G[p^{i-1}] : H[p^{i-1}]) = \prod_{j=1}^{i-1} p^{s_j}.$$

Insgesamt stehen also zur Wahl des geordneten Systems T_i genau

$$\prod_{k=0}^{t_i-1} (p^{t_i} - p^k) \cdot \prod_{j=1}^{i-1} p^{s_j} = \Big(\prod_{k=0}^{t_i-1} (p^{t_i} - p^k) \Big) \cdot \prod_{j=1}^{i-1} p^{s_j \cdot t_i} \tag{G.8.1}$$

Möglichkeiten zur Verfügung. Entsprechend ist die Anzahl aller geordneten Basen $([x_{i(t_i+1)}], \dots, [x_{is_i}])$ von B_i durch

$$\prod_{k=0}^{s_i-t_i-1} (|B_i| - p^k) = (p^{s_i-t_i} - 1) \cdots (p^{s_i-t_i} - p^{s_i-t_i-1})$$

und die Anzahl der möglichen Repräsentanten von $[x_{ij}]$ modulo Vielfacher aus V durch

$$(\Big(U[p^i] \cap \langle \sqrt{V}^{\circ}[p^{i-1}], \sqrt{V}[p^i] \rangle \Big) : V[p^i]) = p^{t_i} \cdot (U[p^{i-1}] : V[p^{i-1}]) = p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}$$

gegeben. Zusammengefasst beträgt die Zahl der möglichen Ergänzungen eines Systems T_i zu S_i genau

$$\prod_{k=0}^{s_i-t_i-1} (p^{s_i-t_i} - p^k) \cdot p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j} = \Big(\prod_{k=0}^{s_i-t_i-1} (p^{s_i-t_i} - p^k) \Big) \cdot \Big(p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j} \Big)^{s_i-t_i}. \tag{G.8.2}$$

In Kombination ergibt sich nun die Behauptung aus G.8.1 und G.8.2. □

Für die Zählung der Systeme $T_i \subset S_i$ erweist sich folgende strukturelle Untersuchung als hilfreich.

Bemerkung G.9. — *Es sei $T = \{x_1, \dots, x_t\} \subset \sqrt{V}^\circ[p^i] \setminus \sqrt{V}[p^i]$ ein System der Länge t mit der Eigenschaft $T \subset \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle$. Des Weiteren seien $y_j \in \sqrt{V}[p^i]$ und $z_j \in \sqrt{V}^\circ[p^{i-1}]$ die Summanden von $x_j = y_j + z_j$. Dann ist T genau dann linear unabhängig in $\sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle$, wenn $\{y_1, \dots, y_t\}$ in $\sqrt{V}[p^i]/\langle \sqrt{V}[p^{i-1}], V[p^i] \rangle$ und $\{z_1, \dots, z_t\}$ in $\sqrt{V}^\circ[p^{i-1}]/\sqrt{V}[p^{i-1}]$ linear unabhängig sind.*

Beweis. — Zunächst nehme ich an, T sei linear unabhängig in $\sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle$. Es seien a_j ganze Zahlen mit $\sum a_j \cdot y_j \in \langle \sqrt{V}[p^{i-1}], V[p^i] \rangle$. Dann ist $\sum a_j \cdot x_j$ in $\langle \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle$ enthalten und es folgt $p \mid a_j$ aus der linearen Unabhängigkeit von T. Somit ist $\{y_1, \dots, y_t\}$ linear unabhängig. Sind a_j ganze Zahlen mit $\sum a_j \cdot z_j \in \sqrt{V}[p^{i-1}]$, so folgt $x = \sum a_j \cdot x_j \in \sqrt{V}[p^i]$. Nach Korollar G.3 gilt $\langle T \rangle \simeq Z_{p^i}^t$ und auf Grund $T \subset \sqrt{V}^\circ[p^i] \setminus \sqrt{V}[p^i]$ folgt $\langle T \rangle \cap Y = p \cdot \langle T \rangle$. Somit ist x als Element von Y in $p \cdot \langle T \rangle$ enthalten und es gilt $p \mid a_j$. Hieraus ergibt sich die lineare Unabhängigkeit von $\{z_1, \dots, z_t\}$.

Es seien nun umgekehrt $\{y_1, \dots, y_t\}$ und $\{z_1, \dots, z_t\}$ in den jeweils beschrieben Räumen linear unabhängig. Für eine Kombination $\sum a_j \cdot x_j \in \langle \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle$ ist $\sum a_j \cdot y_j$ in $\langle \sqrt{V}[p^{i-1}], V[p^i] \rangle$ enthalten. Hieraus folgt wie gewünscht $p \mid a_j$ und somit die lineare Unabhängigkeit von T. □

Bemerkung G.10. — *Für die Anzahl der Gruppen $U \in \mathcal{U}_G$ gilt*

$$c(V,G) = |\mathcal{U}_G| = \sum_{(t_1,\dots,t_e)} \prod_{i=1}^{e} \begin{bmatrix} \sum_{j=1}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \cdot (\sqrt{V}[p^{i-1}] : V[p^{i-1}])^{t_i} \cdot \prod_{k=0}^{t_i-1} (p^{d_i} - p^k) \cdot \begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \left(\frac{(\langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle : V[p^i])}{p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}} \right)^{s_i - t_i},$$

wobei die Summe über die Tupel $(t_1, \dots, t_e)$ mit $0 \le t_i \le s_i$ läuft.

Beweis. — Die Dimension t_i des Unterraums

$$\left(U[p^i] \cap \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle \right) / \langle U[p^{i-1}], V[p^i] \rangle \le U[p^i]/\langle U[p^{i-1}], V[p^i] \rangle$$

ist eine Invariante von $U \in \mathcal{U}_G$ und nach dieser möchte ich im Folgenden zählen. Dazu seien $t_1, \dots, t_e$ mit $0 \le t_i \le s_i$ vorgegeben und gesucht sind die geordneten Erzeugendensysteme T_i der Länge t_i und $S_i \supseteq T_i$ der Länge s_i mit den wie folgt gelisteten Eigenschaften gemäß Bemerkung G.7 (b).

(i) Es gilt $S_i \subset \sqrt{V}^\circ[p^i] \setminus \sqrt{V}[p^i]$.
(ii) Es gilt $T_i \subset \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle$.
(iii) Es gilt $|T_i| = t_i = \dim \langle T_i, \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle$.
(iv) Es gilt $|S_i \setminus T_i| = s_i - t_i = \dim \langle S_i \setminus T_i, \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle / \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle$.

Für die Zählung der möglichen Systeme S_i zum Index i gehe ich davon aus, dass $S_1, \dots, S_{i-1}$ schon bereits gewählt sind. Nach Bemerkung G.9 setzt sich $T_i = \{x_{i1}, \dots, x_{it_i}\}$ aus jeweils linear unabhängigen Systemen $\{y_{i1}, \dots, y_{it_i}\}$ aus $\sqrt{V}[p^i]/\langle \sqrt{V}[p^{i-1}], V[p^i] \rangle$ und $\{z_{i1}, \dots, z_{it_i}\}$ aus $\sqrt{V}^\circ[p^{i-1}]/\sqrt{V}[p^{i-1}]$ zusammen. Im Folgenden werde ich also die Paare $((y_{i1}, \dots, y_{it_i}), (z_{i1}, \dots, z_{it_i}))$ geordneter Systeme modulo Vielfacher aus V zählen und anschließend die Anzahl der sich aus diesen Paaren ergebenen geordneten Systemen $T_i = (x_{i1}, \dots, x_{it_i})$ mit $x_{ij} = y_{ij} + z_{ij}$ ermitteln.

Für die Wahl eines linear unabhängigen Systems $([y_{i1}],\dots,[y_{it_i}])$ in $\sqrt{V}[p^i]/\langle\sqrt{V}[p^{i-1}],V[p^i]\rangle$ der Länge t_i stehen

$$\prod_{k=0}^{t_i-1}\Big((\sqrt{V}[p^i]:\langle\sqrt{V}[p^{i-1}],V[p^i]\rangle)-p^k\Big)=(p^{d_i}-1)\cdots(p^{d_i}-p^{t_i-1})=\begin{bmatrix}d_i\\t_i\end{bmatrix}_p\cdot\prod_{k=0}^{t_i-1}(p^{t_i}-p^k)$$

Möglichkeiten offen. Die Anzahl der wählbaren Repräsentanten $y_{i1},\dots,y_{it_i}$ modulo Vielfacher aus V beträgt dabei

$$(\langle\sqrt{V}[p^{i-1}],V[p^i]\rangle:V[p^i])^{t_i}=(\sqrt{V}[p^{i-1}]:V[p^{i-1}])^{t_i}.$$

Für die Wahl eines linear unabhängigen Systems $([z_{i1}],\dots,[z_{it_i}])$ im Raum $\sqrt{V}^\circ[p^{i-1}]/\sqrt{V}[p^{i-1}]$ ist die Einschränkung zu beachten, dass keine Kombination bereits in $S_1\cup\ldots\cup S_{i-1}\subset\sqrt{V}^\circ[p^{i-1}]$ gewählter Elemente verwendet werden darf, weil sonst die Schnittbedingung $U\cap Y=V$ verletzt wäre. Folglich ist aus dem Raum $\sqrt{V}^\circ[p^{i-1}]/\langle\sqrt{V}[p^{i-1}],S_1,\dots,S_{i-1}\rangle$ zu wählen und für das System $([z_{i1}],\dots,[z_{it_i}])$ stehen somit genau

$$\prod_{k=0}^{t_i-1}\Big(\frac{(\sqrt{V}^\circ[p^{i-1}]:\sqrt{V}[p^{i-1}])}{\prod_{j=1}^{i-1}p^{s_j}}-p^k\Big)=\begin{bmatrix}\sum_{j=1}^{i-1}d_j^\circ-d_j-s_j\\t_i\end{bmatrix}_p\cdot\prod_{k=0}^{t_i-1}(p^{t_i}-p^k)$$

Möglichkeiten zur Wahl. Die Anzahl der Repräsentanten $z_{i1},\dots,z_{it_i}$ modulo Vielfacher aus V beträgt

$$(\langle\sqrt{V}[p^{i-1}],S_1,\dots,S_{i-1}\rangle:V[p^{i-1}])^{t_i}=(\sqrt{V}[p^{i-1}]:V[p^{i-1}])^{t_i}\cdot\prod_{j=1}^{i-1}p^{s_j\cdot t_i}.$$

Folglich gibt es also

$$\begin{bmatrix}\sum_{j=1}^{i-1}d_j^\circ-d_j-s_j\\t_i\end{bmatrix}_p\cdot\Big(\prod_{k=0}^{t_i-1}(p^{d_i}-p^k)\cdot(p^{t_i}-p^k)\Big)\cdot(\sqrt{V}[p^{i-1}]:V[p^{i-1}])^{2\cdot t_i}\cdot\prod_{j=1}^{i-1}p^{s_j\cdot t_i}\tag{G.10.1}$$

verschiedene Paare $((y_{i1},\dots,y_{it_i}),(z_{i1},\dots,z_{it_i}))$ modulo Vielfacher aus V. Die zusammengesetzten Systeme $(x_{i1},\dots,x_{it_i})$ mit $x_{ij}=y_{ij1}+z_{ij}$ sind allerdings nicht allesamt verschieden. Zwei zusammengesetzte Systeme (x_{ij}) und $(\tilde{x}_{ij})$ sind genau dann gleich, wenn $x_{ij}=\tilde{x}_{ij}$ bzw. $y_{ij}-\tilde{y}_{ij}=\tilde{z}_{ij}-z_{ij}$ gilt. Dies ist ein Element aus $\sqrt{V}[p^i]\cap\sqrt{V}^\circ[p^{i-1}]=\sqrt{V}[p^{i-1}]$. Somit führen also von den in G.10.1 gezählten Paaren genau $(\sqrt{V}[p^{i-1}]:V[p^{i-1}])^{t_i}$ zu einem gleichen zusammengesetzten geordneten System T_i. Insgesamt beläuft sich die Anzahl der geordneten Systeme T_i also auf

$$\begin{bmatrix}\sum_{j=1}^{i-1}d_j^\circ-d_j-s_j\\t_i\end{bmatrix}_p\cdot\Big(\prod_{k=0}^{t_i-1}(p^{d_i}-p^k)\cdot(p^{t_i}-p^k)\Big)\cdot(\sqrt{V}[p^{i-1}]:V[p^{i-1}])^{t_i}\cdot\prod_{j=1}^{i-1}p^{s_j\cdot t_i}.\tag{G.10.2}$$

Der von $S_i\setminus T_i$ aufgespannte Unterraum $W_i=\langle U[p^i],\sqrt{V}^\circ[p^{i-1}],\sqrt{V}[p^i]\rangle/\langle\sqrt{V}^\circ[p^{i-1}],\sqrt{V}[p^i]\rangle$ von $W=\sqrt{V}^\circ[p^i]/\langle\sqrt{V}^\circ[p^{i-1}],\sqrt{V}[p^i]\rangle$ der Dimension s_i-t_i ist eine Invariante der Gruppe $U\in\mathcal{U}_G$. Die Dimension von W ergibt sich vermöge

$$1\to\sqrt{V}[p^i]/\langle\sqrt{V}[p^{i-1}],\sqrt{V}[p^i]\rangle\to\sqrt{V}^\circ[p^i]/\langle\sqrt{V}^\circ[p^{i-1}],V[p^i]\rangle\to\sqrt{V}^\circ[p^i]/\langle\sqrt{V}^\circ[p^{i-1}],\sqrt{V}[p^i]\rangle\to1$$

durch $d_i^\circ-d_i$ und folglich stehen für die Auswahl der Invariante $W_i\le W$ genau

$$\begin{bmatrix}d_i^\circ-d_i\\s_i-t_i\end{bmatrix}_p$$

Möglichkeiten offen. Die Anzahl der möglichen geordneten Basen $([x_{i(s_i+1)}], \ldots, [x_{is_i}])$ von W_i ist dann

$$\begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \prod_{k=0}^{s_i-t_i-1} (p^{s_i-t_i} - p^k)$$

und für die Wahl der Repräsentanten $x_{i(s_i+1)}, \ldots, x_{is_i}$ modulo Vielfacher aus V stehen exakt

$$(\langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle : V[p^i])^{s_i-t_i}$$

Optionen zur Verfügung. Insgesamt ist der Anzahl der wählbaren Systeme $S_i \setminus T_i$ mit der vorgegebenen Länge $s_i - t_i$ genau

$$\begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \Big(\prod_{k=0}^{s_i-t_i-1} (p^{s_i-t_i} - p^k) \Big) \cdot (\langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle : V[p^i])^{s_i-t_i}. \tag{G.10.3}$$

Sind also die Invarianten $t_1, \ldots, t_e$ gewählt, so ergibt sich für die Anzahl der möglichen Erzeugendensysteme $T_i \subseteq S_i$ mit den Eigenschaften (i)-(iv) modulo Vielfacher aus V mit den Formeln G.10.2 und G.10.3 insgesamt

$$\begin{aligned} &\begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \begin{bmatrix} \sum_{j=1}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \\ &\cdot \Big(\prod_{k=0}^{t_i-1} (p^{d_i} - p^k) \cdot (p^{t_i} - p^k) \Big) \cdot (\sqrt{V}[p^{i-1}] : V[p^{i-1}])^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j \cdot t_i} \\ &\cdot \Big(\prod_{k=0}^{s_i-t_i-1} (p^{s_i-t_i} - p^k) \Big) \cdot (\langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle : V[p^i])^{s_i-t_i}. \end{aligned} \tag{G.10.4}$$

Zum Schluß ist noch durch die in Bemerkung G.8 ermittelte Zahl von Erzeugendensysteme zu teilen, welche zu einer gleichen Gruppe führen und es ergibt sich

$$\begin{aligned} \prod_{i=1}^{e} &\begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \begin{bmatrix} \sum_{j=1}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \\ &\cdot \Big(\prod_{k=0}^{t_i-1} (p^{d_i} - p^k) \Big) \cdot (\sqrt{V}[p^{i-1}] : V[p^{i-1}])^{t_i} \cdot p^{-t_i \cdot (s_i-t_i)} \cdot \prod_{j=1}^{i-1} p^{-s_j \cdot (s_i-t_i)} \\ &\cdot (\langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i] \rangle : V[p^i])^{s_i-t_i}. \end{aligned} \tag{G.10.5}$$

Hieraus folgt die behauptete Formel. □

Gruppenindizes. — Bevor nun die in Lemma G.1 behaupteten Formeln nachgewiesen werden können sind die in Bemerkung G.10 auftauchenden Gruppenindizes auszurechnen.

Bemerkung G.11. — *Für $1 \leq i \leq e$ gilt die Gruppenindexformel*

$$(\langle \sqrt{V}[p^i], V[p^{i+1}] \rangle : V[p^{i+1}]) = (\sqrt{V}[p^i] : V[p^i]) = \prod_{j=1}^{i} p^{d_j}.$$

Beweis. — Der erste Gleichung ergibt sich aus dem Isomorphiesatz vermöge $\sqrt{V}[p^i] \cap V[p^{i+1}] = V[p^i]$. Die zweite Gleichung ist für $i = 1$ gültig, denn definitionsgemäß ist $d_i = \dim \sqrt{V}[p^i]/\langle \sqrt{V}[p^{i-1}], V[p^i]\rangle$ und somit $d_1 = \dim \sqrt{V}[p]/V[p]$. Mit der ersten Gleichung ergibt sich vermöge

$$(\sqrt{V}[p^i] : V[p^i]) = (\sqrt{V}[p^i] : \langle \sqrt{V}[p^{i-1}], V[p^i]\rangle) \cdot (\langle \sqrt{V}[p^{i-1}], V[p^i]\rangle : V[p^i]) = p^{d_i} \cdot \prod_{j=1}^{i-1} p^{d_j}$$

eine Induktionsgleichung für $i > 1$. □

Bemerkung G.12. — *Für $1 \leq i \leq e$ gilt die Gruppenindexformel*

$$(\langle \sqrt{V}^\circ[p^i], \sqrt{V}[p^{i+1}]\rangle : V[p^{i+1}]) = p^{d_{i+1}} \cdot \prod_{j=1}^{i} p^{d_j^\circ}.$$

Beweis. — Diese Formel folgt aus der Zerlegung

$$\begin{aligned}(\langle \sqrt{V}^\circ[p^i], \sqrt{V}[p^{i+1}]\rangle : V[p^{i+1}]) &= (\langle \sqrt{V}^\circ[p^i], \sqrt{V}[p^{i+1}]\rangle : \sqrt{V}[p^{i+1}]) \cdot (\sqrt{V}[p^{i+1}] : V[p^{i+1}]) \\ &= (\sqrt{V}^\circ[p^i] : \sqrt{V}[p^i]) \cdot (\sqrt{V}[p^{i+1}] : V[p^{i+1}]).\end{aligned}$$

Der letzte Faktor hat nach Bemerkung G.11 den Wert

$$(\sqrt{V}[p^{i+1}] : V[p^{i+1}]) = \prod_{j=1}^{i+1} p^{d_j}.$$

Der erste Faktor läßt sich induktiv vermöge

$$\begin{aligned}(\sqrt{V}^\circ[p^i] : \sqrt{V}[p^i]) &= (\sqrt{V}^\circ[p^i] : \langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle) \cdot (\langle \sqrt{V}^\circ[p^{i-1}], \sqrt{V}[p^i]\rangle : \sqrt{V}[p^i]) \\ &= p^{d_i^\circ - d_i} \cdot (\sqrt{V}^\circ[p^{i-1}] : \sqrt{V}[p^{i-1}]) = \prod_{j=1}^{i} p^{d_j^\circ - d_j}\end{aligned}$$

berechnen. Hieraus folgt die Behauptung. □

Beweis von Lemma G.1. — Aus Bemerkung G.10 ergibt sich mit den obigen Berechnungen der Gruppenindizes

$$c(V, G) = \sum_{(t_1,\ldots,t_e)} \prod_{i=1}^{e} c(t_i)$$

mit

$$\texttt{(I)}\quad c(t_i) = \begin{bmatrix} \sum_{j=1}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \cdot \begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \Big(\prod_{k=0}^{t_i-1} (p^{d_i} - p^k) \Big) \cdot \Big(\prod_{j=1}^{i-1} p^{d_j} \Big)^{t_i} \cdot \left(\frac{p^{d_i} \cdot \prod_{j=1}^{i-1} p^{d_j^\circ}}{p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}} \right)^{s_i - t_i}.$$

Wie an Hand des ersten Faktors festgestellt werden kann, liefert nur $t_1 = 0$ einen nichtverschwindenden Wert für $c(t_1)$. Hieraus folgt

$$c(V, G) = p^{s_1 \cdot d_1} \cdot \begin{bmatrix} d_1^\circ - d_1 \\ s_1 \end{bmatrix}_p \cdot \sum_{(t_2,\ldots,t_e)} \prod_{i=2}^{e} c(t_i).$$

Für $i \geq 2$ erweist sich die Ersetzung

$$\Big(\prod_{j=1}^{i-1} p^{d_j}\Big)^{t_i} \cdot \left(\frac{p^{d_i} \cdot \prod_{j=1}^{i-1} p^{d_j^\circ}}{p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}}\right)^{s_i - t_i} \;=\; \Big(\prod_{j=1}^{i-1} p^{s_i \cdot d_j}\Big) \cdot \left(\frac{p^{d_i} \cdot \prod_{j=1}^{i-1} p^{d_j^\circ - d_j}}{p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}}\right)^{s_i - t_i}$$

als relevant und folglich ist $c(t_i)$ für $i \geq 2$ identisch mit

$$c(t_i) = \Big(\prod_{j=1}^{i-1} p^{s_i \cdot d_j}\Big) \cdot \begin{bmatrix} \sum_{j=1}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \cdot \begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \Big(\prod_{k=0}^{t_i - 1} (p^{d_i} - p^k)\Big) \cdot \left(\frac{p^{d_i} \cdot \prod_{j=1}^{i-1} p^{d_j^\circ - d_j}}{p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}}\right)^{s_i - t_i}.$$

Nach der Ausklammerung sämtlicher von t_i unabhängigen Faktoren und der Zusammenfassung der zu d_1 gehörenden Faktoren $s_i \cdot d_1$ zu $r \cdot d_1$ gilt also

$$\begin{aligned} c(V,G) \quad &= \quad p^{r \cdot d_1} \cdot \begin{bmatrix} d_1^\circ - d_1 \\ s_1 \end{bmatrix}_p \cdot \prod_{i=2}^{e} \prod_{j=2}^{i-1} p^{s_i \cdot d_j} \\ \cdot \sum_{(t_2,\ldots,t_e)} \prod_{i=2}^{e} &\begin{bmatrix} \sum_{j=1}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \cdot \begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \Big(\prod_{k=0}^{t_i - 1} (p^{d_i} - p^k)\Big) \cdot \left(\frac{p^{d_i} \cdot \prod_{j=1}^{i-1} p^{d_j^\circ - d_j}}{p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}}\right)^{s_i - t_i}. \end{aligned}$$

Abschließend ersetze ich den Faktor $p^{d_1} = (\sqrt{V}[p] : V[p])$ durch $(Y[p] : V[p])$, ziehe ein Produkt über k vor die Summe und erhalte

$$\begin{aligned} \texttt{(II)} \qquad c(V,G) \quad &= \quad (Y[p] : V[p])^r \cdot \begin{bmatrix} d_1^\circ - d_1 \\ s_1 \end{bmatrix}_p \cdot \prod_{i=2}^{e} \prod_{j=2}^{i-1} \prod_{k=0}^{s_i - 1} p^{d_j} \cdot (p^{d_i} - p^k) \\ \cdot \sum_{(t_2,\ldots,t_e)} \prod_{i=2}^{e} &\begin{bmatrix} \sum_{j=1}^{i-1} d_j^\circ - d_j - s_j \\ t_i \end{bmatrix}_p \cdot \begin{bmatrix} d_i^\circ - d_i \\ s_i - t_i \end{bmatrix}_p \cdot \prod_{k=t_i}^{s_i - 1} \frac{1}{p^{d_i} - p^k} \cdot \frac{p^{d_i} \cdot \prod_{j=1}^{i-1} p^{d_j^\circ - d_j}}{p^{t_i} \cdot \prod_{j=1}^{i-1} p^{s_j}}. \end{aligned}$$

(a) In diesem Fall ist $X = Y \times Z$. Dann erfüllt die elementarabelsche Hülle $\sqrt{V}^\circ$ von V die Identität $\sqrt{V}^\circ = \langle \sqrt{V}, Z \rangle$ und es gilt für ihre p^i-Torsionsfaktorräume

$$\sqrt{V}^\circ[p^i] / \langle \sqrt{V}^\circ[p^{i-1}], V[p^i] \rangle \simeq \begin{cases} \langle \sqrt{V}[p], Z \rangle / V[p] & i = 1 \\ \sqrt{V}[p^i] / \langle \sqrt{V}[p^{i-1}], V[p^i] \rangle & i \geq 2. \end{cases}$$

Für ihre Dimension ergibt sich also

$$d_i^\circ = \begin{cases} d_1 + \dim Z & i = 1 \\ d_i & i \geq 2. \end{cases}$$

Wie an Hand des zweiten Faktors in `I` überprüfbar ist $c(t_i)$ für $i \geq 2$ höchstens im Fall $t_i = s_i$ nichtverschwindend und die Formel `II` kann somit zu

$$c(V,G) = (Y[p] : V[p])^r \cdot \begin{bmatrix} \dim Z \\ s_1 \end{bmatrix}_p \cdot \prod_{i=2}^{e} \prod_{j=2}^{i-1} \prod_{k=0}^{s_i - 1} p^{d_j} \cdot (p^{d_i} - p^k) \cdot \prod_{i=2}^{e} \begin{bmatrix} \dim Z - \sum_{j=1}^{i-1} s_j \\ s_i \end{bmatrix}_p$$

vereinfacht werden.

(b) Für diesen Fall ist die Formel für $c(V,G)$ bereits wie behauptet aufgestellt und es ist nur noch $d_1^\circ = d_1$ zu beachten. Dies ergibt sich auf Grund von $\nu > 1$ aus $\sqrt{V}^\circ[p] = \sqrt{V}[p]$. □

Ein alternativer Beweis von Lemma G.1 im Fall $X = Y \times Z$. — Dieser Beweis ist auch ohne die Resultate aus dem Abschnitt *Gruppenerweiterungen mit Schnittbedingung* funktionstüchtig und sei hier um seiner selbst willen angefügt. Es sei also $X = Y \times Z$. Dann hat die elementarabelsche Hülle $\sqrt{V}^\circ$ von V die Identität $\sqrt{V}^\circ = \langle \sqrt{V}, Z\rangle$ und es gilt für ihre p^i-Torsionsfaktorräume

$$\sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle \simeq \begin{cases} \langle \sqrt{V}[p], Z\rangle/V[p] & i = 1 \\ \sqrt{V}[p^i]/\langle \sqrt{V}[p^{i-1}], V[p^i]\rangle & i \geq 2. \end{cases}$$

Nach Bemerkung G.4 wird eine Gruppe $U \in \mathcal{U}_G$ von Systemen $S_i \subset \sqrt{V}^\circ[p^i]$ der Länge und Dimension $s_i = \dim \sqrt{V}^\circ[p^i]/\langle \sqrt{V}^\circ[p^{i-1}], V[p^i]\rangle$ erzeugt. Für die Elemente x_{ij} von S_i ergibt sich die Komponentenzerlegung $x_{ij} = (y_{ij}, z_{ij})$ mit $y_{ij} \in \sqrt{V}[p^i]$ und $z_{ij} \in Z$. Die Z-Komponenten sind linear unabhängig über $\mathbb{F}_p$. Um dies zu demonstrieren, nehme ich an, es bestünde eine lineare Abhängigkeit der Gestalt $\sum a_{ij} \cdot z_{ij} = 0$ mit ganzen Zahlen a_{ij}. Dann ist $x = \sum a_{ij} \cdot x_{ij}$ ein Element aus Y und es gilt $V = U \cap Y \geq \langle x, V\rangle$. Dies ist nur möglich, wenn x in V enthalten ist und somit alle Koeffizienten a_{ij} durch p teilbar sind. Somit erzeugen die Familien $\{z_{i1}, \ldots, z_{is_i}\}$ jeweils s_i-dimensionale Unterräume W_i in Z, deren direkte Summe $W = W_1 \oplus \ldots \oplus W_e$ die Dimension $r = \dim G/H$ besitzt. Dabei sind die Unterräume $W_1 \oplus \ldots \oplus W_i$ für $1 \leq i \leq e$ die Projektionen der Untergruppen $U[p^i]$ auf Z und somit invariant unter der Auswahl der Erzeugendensysteme $S_1 \cup \ldots \cup S_i$. Denn für u aus $U[p^i]$ gibt es ganze Zahlen $1 \leq a_{kl} \leq p^i$ und ein Element $v \in V$ mit

$$u = \sum_{k=1}^{i} \sum_{l=1}^{s_k} a_{kl} \cdot x_{kl} + \sum_{k=i+1}^{e} p^{k-i} \cdot a_{kl} \cdot x_{kl} + v = (y, z) \qquad \text{mit} \qquad z = \sum_{k=1}^{i} \sum_{l=1}^{s_k} a_{kl} \cdot z_{kl}.$$

Somit sind die Z-Komponenten von W_i nur eindeutig modulo $W_1 \cup \ldots \cup W_{i-1}$. Des Weiteren ist es eine einfache Überlegung, dass unter sämtlichen Gruppen $U \in \mathcal{U}_G$, sofern es überhaupt eine gibt, jede Projektionen $W = W_1 \oplus \ldots \oplus W_e$ auf Z möglich ist, sodass $U[p^i]$ auf $W_1 \oplus \ldots \oplus W_i$ projiziert wird. Dies ist beispielsweise durch manuellen Austausch der Z-Komponenten ersichtlich. Folglich gibt es genau

(a.1) $$\begin{bmatrix} \dim Z \\ s_1 \end{bmatrix}_p \cdot \begin{bmatrix} \dim Z - s_1 \\ s_2 \end{bmatrix}_p \cdots \begin{bmatrix} \dim Z - s_1 - \ldots - s_{e-1} \\ s_e \end{bmatrix}_p$$

solcher geordneten Projektionen $W = W_1 \oplus \ldots \oplus W_e$ auf Z. Dabei steht der erste Faktor für die Anzahl der s_1-dimensionalen Räume W_1 in Z, der zweite für die s_2-dimensionalen Räume $[W_2]$ in Z/W_1 und so weiter.

Nun ist zu zählen, wie viele Untergruppen $U \in \mathcal{U}_G$ die gleichen Invarianten $W_1 \oplus \ldots \oplus W_i$ besitzen. Für jede Komponente W_i wird eine fest geordnete Basis $z_{i1}, \ldots, z_{is_i}$ gewählt. Für $i \neq 1$ wird jedem Basiselement z_{ij} wird dann eine Klasse $[y_{ij}] \in \sqrt{V}[p^i]/\langle \sqrt{V}[p^{i-1}], V[p^i]\rangle$ zugewiesen, sodass $[y_{i1}], \ldots, [y_{is_i}]$ linear unabhängig über $\mathbb{F}_p$ sind. Für die Wahl dieser geordneten Familie von Klassen stehen

$$(p^{d_i} - 1) \cdot (p^{d_i} - p) \cdots (p^{d_i} - p^{s_i - 1})$$

Möglichkeiten zur Verfügung. Die Anzahl der Repräsentanten dieser Klassen modulo Vielfacher aus V ist dabei

$$(\langle\sqrt{V}[p^{i-1}], V[p^i]\rangle : V[p^i])^{s_i} = \prod_{j=1}^{i-1} p^{s_i \cdot d_j},$$

wobei ich die Formel G.11 für die Auswertung dieses Gruppenindexes herangezogen habe. Ist nun ein geordnetes Repräsentantensystem $y_{i1}, \ldots, y_{is_i}$ gewählt, so setze ich

$$S_i = \{(y_{i1}, z_{i1}), \ldots, (y_{is_i}, z_{is_i})\}.$$

Zusammengefasst gibt es also für jede Auswahl von Invarianten $W_1 \oplus \ldots \oplus W_i$ $(1 \leq i \leq e)$ genau

$$\prod_{i=2}^{e} \prod_{j=1}^{i-1} p^{s_i \cdot d_j} \cdot \prod_{k=0}^{s_i-1} (p^{d_i} - p^k) \tag{a.2}$$

Möglichkeiten zur Wahl der Erzeugendensysteme $S_2, \ldots, S_e$. Für das System S_1 müssen die Y-Komponenten $y_{11}, \ldots, y_{1s_1}$ nicht zwangsläufig einen s_1-dimensionalen Unterraum erzeugen, daher stehen für die Wahl von S_1 exakt

$$(\sqrt{V}[p] : V[p])^{s_1} = p^{s_1 \cdot d_1} \tag{a.3}$$

Möglichkeiten offen. Mit den Formeln a.1, a.2 und a.3 ergibt sich nun die Formel

$$c(V,G) = \prod_{i=1}^{e} \begin{bmatrix} \dim Z - \sum_{j=1}^{i-1} s_j \\ s_i \end{bmatrix}_p \cdot p^{s_1 \cdot d_1} \cdot \prod_{i=2}^{e} \prod_{j=1}^{i-1} p^{s_i \cdot d_j} \cdot \prod_{k=0}^{s_i-1} (p^{d_i} - p^k).$$

Ich fasse ich alle zu d_1 gehörenden Exponenten zusammen zu $(s_1 + \ldots + s_e) \cdot d_1 = r \cdot d_1$ und ich erhalte

$$c(V,G) = p^{r \cdot d_1} \cdot \prod_{i=1}^{e} \begin{bmatrix} \dim Z - \sum_{j=1}^{i-1} s_j \\ s_i \end{bmatrix}_p \cdot \prod_{i=2}^{e} \prod_{j=2}^{i-1} p^{s_i \cdot d_j} \cdot \prod_{k=0}^{s_i-1} (p^{d_i} - p^k).$$

Abschließend nehme ich die Faktoren p^{d_j} von der Anzahl s_i in das Produkt über $0 \leq k \leq s_i - 1$ auf und es ergibt sich wie behauptet

$$c(V,G) = p^{r \cdot d_1} \cdot \prod_{i=1}^{e} \begin{bmatrix} \dim Z - \sum_{j=1}^{i-1} s_j \\ s_i \end{bmatrix}_p \cdot \prod_{i=2}^{e} \prod_{j=2}^{i-1} \prod_{k=0}^{s_i-1} p^{d_j} \cdot (p^{d_i} - p^k).$$

□

NOTATIONSVERZEICHNIS

$a(G), b(F,G)$		(s. Kap. 1)
$a_{\mathfrak{p}}(G)$		(s. Satz 2.1)
$a(F,G)$		(s. Satz 2.2)
$\mathcal{C}\ell_F$, $\mathcal{C}\ell$	Klassengruppe zu F	
$\mathcal{C}\ell_{\mathfrak{m}}$	Strahlklassengruppe zu $\mathfrak{m}$	(s. Kap. C)
$\mathfrak{d}(E/F)$	Diskriminante der Körpererweiterung E/F	
$d_{\mathfrak{p}}(E/F)$	$d_{\mathfrak{p}}(E/F) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{d}(E/F))$, Diskriminantenexponent von $\mathfrak{p}$	(s. Kap. C)
$\dim G$	p-Rang einer elementarabelsche p-Gruppe G, Dimension als $\mathbb{F}_p$-Vektorraum	
F	Globaler Funktionenkörper mit Konstantenkörper $K = \mathbb{F}_q$ oder Zahlkörper (im Kap. 4)	
$F_{\mathfrak{p}}$	Lokaler Funktionenkörper mit maximalem Ideal $\mathfrak{p}$ oder Zahlkörper (im Kap. 4)	
$F^{\mathfrak{m}}$	Elemente von $F^\times$ mit zu $\mathfrak{m}$ teilerfremden Divisor	
$F_{\mathfrak{m}}$	Strahl modulo $\mathfrak{m}$	
$\mathbb{F}_q$	Endlicher Körper mit q Elementen	
$\mathbb{F}_{\mathfrak{p}}$	Restklassenkörper $\mathcal{O}_{\mathfrak{p}}/\mathfrak{p}$ bzgl. Stelle $\mathfrak{p}$	
$\mathrm{Gal}(E/F)$	Galoisgruppe der galoischen Hülle von E/F	
G	endliche Gruppe	
$G[n], G[p^\infty]$	$G[n] = \{\sigma \in G : \sigma^n = 1\}$ und $G[p^\infty] = \{\sigma \in G : \sigma^{p^r} = 1$ für ein $r \geq 0\}$	
g_i	$g_i = \dim G[p^i]/G[p^{i-1}]$ bzw. $p^{g_i} = (G[p^i] : G[p^{i-1}])$	
$(G : Z_\ell)$	$(G : Z_\ell) = (G : H)$ für eine zu Z_ℓ isomorphe Untergruppe $H \leq G$	
$\boldsymbol{G}$	Auflistung einer Auflösung	(s. Definition 2.3)
$\mathcal{I}$	zulässige Familie von Sprungstellenlisten	(s. Definition 2.6)

$\begin{bmatrix} n \\ k \end{bmatrix}_p$	$\begin{bmatrix} n \\ k \end{bmatrix}_p = \prod_{i=0}^{k-1} \frac{p^n - p^i}{p^k - p^i}$ Anzahl der k-dimensionalen Unterräume in $\mathbb{F}_p^n$	
$\mathcal{N}\mathfrak{m}$	Divisornorm $\mathcal{N}\mathfrak{m} = \prod_{\mathfrak{p}^m \| \mathfrak{m}} \mathcal{N}\mathfrak{p}^m = \prod_{\mathfrak{p}^m \| \mathfrak{m}} (\mathbb{F}_\mathfrak{p} : 1)^m$.	
$\mathfrak{p}$	Stelle mit Bewertungsring $\mathcal{O}_\mathfrak{p}$	
$\mathfrak{p} \mid \mathfrak{m},\ \mathfrak{p}^m \mid\mid \mathfrak{m}$	Teilerrelationen, letztere bedeutet $\mathrm{ord}_\mathfrak{p}(m) = m$	
S_p	Selmerklassengruppe $S_p = \{x \in F^\times : (x) = \mathfrak{b}^p\}/F^p$	
Z_ℓ	$Z_\ell = \mathbf{Z}/\ell\mathbf{Z}$, zyklische Gruppe	
	Verschiedene Dirichletreihen	
$\Phi(F, G; s)$	$\Phi(F, G; s) = \sum_{\mathrm{Gal}(E/F) \simeq G} \mathcal{N}\mathfrak{d}(E/F)^{-s}$	
$\Phi(F_\mathfrak{p}, \mathcal{G}, \mathcal{I}; s)$	$\Phi(F_\mathfrak{p}, G; s) = \sum_{\mathcal{G}, \mathcal{I}} b(\mathcal{G}, \mathcal{I}) \cdot \Phi(F, \mathcal{G}, \mathcal{I}; s)$	(s. Abs. 2.2)
$\Phi(F_\mathfrak{p}^\times, G; s)$	$\Phi(F_\mathfrak{p}^\times, G; s) = \sum_{\mathcal{G}, G_0 = 1} \sum_{\mathcal{I}} b(\mathcal{G}, \mathcal{I}) \cdot \Phi(F_\mathfrak{p}, \mathcal{G}, \mathcal{I}; s)$	(s. Abs. 3.4)
$\Psi(F, G; s)$		(s. Kap. A)
$\Psi(F, G, S; s; \boldsymbol{e})$		(s. Bem. A.3)
$\zeta_F(s)$	Zetafunktion zu F	
	Landaunotationen	
$f(x) \in o\,(g(x))$	$0 = \lim_{x \to \infty} f(x)/g(x)$	
$f(x) \in O\,(g(x))$	$0 \leq \limsup_{x \to \infty} f(x)/g(x) < \infty$	
$f(x) \sim g(x)$	$\lim_{x \to \infty} f(x)/g(x) = 1$	(s. Kap. D)
$f(x) \in \Omega\,(g(x))$	$0 < \liminf_{x \to \infty} f(x)/g(x) \leq \infty$	
$f(x) \in \omega\,(g(x))$	$\lim_{x \to \infty} f(x)/g(x) = \infty$	

LITERATURVERZEICHNIS

[Auer, 1999] Auer, R. (1999). Ray Class Fields of Global Function Fields with Many Rational Places. Doktorarbeit, Universität Oldenburg.

[Cohen et al., 2002] Cohen, H., y Diaz, F. D., and Olivier, M. (2002). On the density of discriminants of cyclic extensions of prime degree. *J. reine angew. Math.*, 550:169–209.

[Ellenberg and Venkatesh, 2005] Ellenberg, J. S. and Venkatesh, A. (2005). Counting extensions of function fields with specified Galois group and bounded discriminant. *Geometric Methods in Algebra and Number Theory*, 235:151–168.

[Fesenko and Vostokov, 1993] Fesenko, I. B. and Vostokov, S. V. (1993). *Local Fields and Their Extensions*. AMS.

[Hasse, 1980] Hasse, H. (1980). *Number Theory*. Springer.

[Hess et al., 2003] Hess, F., Pauli, S., and Pohst, M. E. (2003). Computing the multiplicative group of residue class rings. *Math. Comput.*, 72(243):1531–1548.

[Jensen et al., 2002] Jensen, C. U., Ledet, A., and Yui, N. (2002). *Generic Polynomials*. Cambridge University Press.

[Klüners, 2005a] Klüners, J. (2005a). A Counter Example to Malle's Conjecture on the Asymptotics of Discriminants. *C. R. Math. Acad. Sci. Paris*, Ser. I 340:411–414.

[Klüners, 2005b] Klüners, J. (2005b). Über die Asymptotik von Zahlkörpern mit vorgegebener Galoisgruppe. Habilitationsschrift, Universität Kassel.

[Klüners and Malle, 2004] Klüners, J. and Malle, G. (2004). Counting nilpotent Galois extensions. *J. reine angew. Math.*, 572:1–16.

[Lang, 1994] Lang, S. (1994). *Algebraic Number Theory*. Springer, 2nd edition.

[Lang, 2002] Lang, S. (2002). *Algebra*. Springer, 3rd edition.

[Malle, 2002] Malle, G. (2002). On the Distribution of Galois Groups. *J. Number Theory*, 92:315–329.

[Malle, 2004] Malle, G. (2004). On the Distribution of Galois Groups, II. *Exper. Math.*, 13(2):129–135.

[Malle and Matzat, 1999] Malle, G. and Matzat, B. (1999). *Inverse Galois Theory*. Springer.

[Nakagoshi, 1979] Nakagoshi, N. (1979). The structure of the multiplicative group of residue classes modulo $\mathfrak{p}^{N+1}$. *Nagoya Math. J.*, 73:41–60.

[Narkiewicz, 1983] Narkiewicz, W. (1983). *Number Theory*. World Scientific.

[Narkiewicz, 1989] Narkiewicz, W. (1989). *Elementary and Analytic Theory of Algebraic Numbers*. Springer.

[Neukirch, 1992] Neukirch, J. (1992). *Algebraische Zahlentheorie*. Springer.

[Rosen, 2002] Rosen, M. (2002). *Number Theory in Function Fields*. Springer.

[Stichtenoth, 2008] Stichtenoth, H. (2008). *Algebraic Function Fields and Codes*. Springer, 2nd edition.

[Villa Salvador, 2006] Villa Salvador, G. D. (2006). *Topics in the Theory of Algebraic Function Fields*. Birkhäuser.

[Wright, 1989] Wright, D. J. (1989). Distribution of discriminants of abelian extensions. *Proc. London Math. Soc. (3)*, 58:17–50.