Inauguraldissertation

zur Erlangung

der Doktorwürde der

Naturwissenschaftlich-Mathematischen Gesamtfakultät

der

Ruprecht-Karls-Universität Heidelberg

vorgelegt durch

Diplommathematiker Johannes Bartels

aus Göttingen

Tag der mündlichen Prüfung:

Über die Verwirklichung auflösbarer Gruppen über Zahlkörpern

Gutachter: Prof. Dr. Kay Wingberg

____

1 Einleitung

1.1 Beschreibung der Ergebnisse

Gegenstand dieser Arbeit sind Einbettungsprobleme. Zunächst werden solche über unendlichen Galoiserweiterungen betrachtet. Zu einer vollständigen Klasse endlicher Gruppen $\mathfrak{c}$, einen gegebenen Zahlkörper k und einer Stellenmenge S dieses Zahlkörpers sei $k_S(\mathfrak{c})$ die größte außerhalb S unverzweigte pro-$\mathfrak{c}$-Erweiterung von k. Ist $\mathfrak{c}$ eine vollständige Klasse auflösbarer Gruppen, so erweist sich diese Definition als von besonderer Bedeutung.

1.1.1 Definition: *Es sei k ein globaler Zahlkörper und $\mathfrak{c}$ eine vollständige Klasse auflösbarer Gruppen. Dann heißt k* ***in bezug auf $\mathfrak{c}$ vollständig****, wenn für jedes prime p aus $S(\mathfrak{c})$ die Erweiterung $k(\zeta_p)/k$ über eine Galoisgruppe aus $\mathfrak{c}$ verfügt.*

Es gilt nun der folgende Satz.

1.1.2 Satz: *Ist der globale Zahlkörper k in bezug auf eine vollständige Klasse auflösbarer Gruppen $\mathfrak{c}$ vollständig und sind $S \subseteq T$ zwei Stellenmengen von k mit den Eigenschaften*

1. *Für die Dirichletdichte δ gilt $\delta(S) = 0$.*
2. *Es gibt eine endliche Erweiterung F/k in $k_S(\mathfrak{c})$, so daß die in F sich voll zerlegenden Stellen $cs(F/k)$ in T enthalten sind.*

Dann ist die Galoisgruppe

$$G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$$

zur freien pro-$\mathfrak{c}$-Gruppe $F_\omega(\mathfrak{c})$ von abzählbar unendlichem Rang isomorph.

Über $k_S(\mathfrak{c})$ ist dann jedes globale Einbettungsproblem mit Gruppen aus $\mathfrak{c}$ innerhalb von $k_T(\mathfrak{c})$ lösbar. Der Beweis dieses Satzes benutzt ein Argument Iwasawas, welcher ein ähnliches Ergebnis für unendliche abelsche Erweiterungen über einem Zahlkörper entwickelt hat. Im Unterschied zu ihm ist der hier behandelte Grundkörper $k_S(\mathfrak{c})$ nicht abelsch über k. Wichtig dabei ist, daß die kohomologische Dimension von $G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$ kleiner oder gleich 1 ist. Der Vergleich mit den lokalen Trägheitsgruppen aus $T \smallsetminus S$ liefert den nachstehenden Satz:

1.1.3 Satz: *Unter den Bedingungen des vorangegangenen Satzes liefert der Epimorphismus von dem freien Produkt der lokalen Trägheitsgruppen der Stellen aus $T \smallsetminus S$ auf $G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$*

$$\mathop{\ast}_{\mathfrak{p} \in T \smallsetminus S} T_{\mathfrak{p}}(\mathfrak{c}) \twoheadrightarrow G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$$

einen Isomorphismus auf den Abelisierungen.

Dies liefert ein Indiz dafür, daß unter Umständen einst eine pro-$\mathfrak{c}$-Version des Riemannschen Existenzsatzes erstellt werden kann (s. [NSW08], chap. X, §5). Ist der Grundkörper des Einbettungsproblem eine endliche Erweiterung von $\mathbb{Q}$, so wird die Sache erheblich komplizierter. Das nachstehende Diagramm wird die Lage veranschaulichen.

$$\begin{tikzcd} & & & G_k \arrow[dl, dotted, "\psi"'] \arrow[d, "\varphi"] & \\ 1 \arrow[r] & H \arrow[r] & G \arrow[r, "j"] & G(K/k) \arrow[r] & 1 \end{tikzcd}$$

Zentraler Punkt des Problems ist die (nach Möglichkeit affirmative) Beantwortung der Frage nach dem Vorhandensein einer epimorphen Anhebung ψ des Epimorphismus φ zu einem kommutativen Diagramm. Seit den 30-er Jahren des vergangenen Jahrhunderts wird an der Lösung dieses Themas gearbeitet und es ist seither eine Kaskade aufeinander aufbauender Arbeiten zu nennen, welche entscheidende Beiträge erbracht haben. Den Anfang bilden Grunwald/Wang auf der einen, Scholz und Reichardt auf der anderen Seite. Nach Grunwald/Wang gilt nämlich dieser Satz, welcher sich in [AT09], chap. X befindet.

1.1.4 Satz (Grunwald/Wang, 1935): *Wenn k ein globaler Körper und A eine abelsche Gruppe ist, und zu endlich vielen Vervollständigungen $k_{\mathfrak{p}}$ es abelsche Erweiterungen $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ mit $G(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \hookrightarrow A$ gibt, so ist A isomorph zu einer Galoisgruppe eines Körpers K über k, dessen Vervollständigung an den gegebenen Stellen $K_{\mathfrak{P}}$ ergibt.*

Scholz und Reichardt beschränken sich zwar nicht auf abelsche Gruppen, liefern nur geringe Auskünfte über das Zerlegungsverhalten der Primstellen, so sind die im Beweis konstruierten Erweiterungen ausnahmslos lokal zyklisch. Aus [Ser08], chap. 2 ist dieser Satz entnommen.

1.1.5 Satz: *Jede p-Gruppe $p \neq 2$ kann über $\mathbb{Q}$ verwirklicht werden, d.h. es gibt zu jedweder p-Gruppe G eine Erweiterung $k/\mathbb{Q}$, deren Galoisgruppe zu G isomorph ist.*

Diese Sätze sind die ersten bekannten Ergebnisse zum Einbettungsproblem. Der Satz von Scholz und Reichardt wurde von Schafarewitsch weitreichend verallgemeinert zu folgendem Theorem - siehe auch [NSW08], chap. IX, §6.

1.1.6 Theorem (Schafarewitsch, 1954): *Sind eine auflösbare Gruppe G und ein Zahlkörper k gegeben, dann gibt es eine Zahlkörpererweiterung K/k, deren Galoisgruppe zu G isomorph ist.*

Unter Berücksichtigung lokaler Vorgaben ist der Satz von Neukirch aus dem Artikel [Neu79], welcher in umfangreichem Maß auf die Arbeiten von Hasse, Hoechsmann und Schafarewitsch zurückgreift.

1.1.7 Theorem (Neukirch, 1979): *Ist k ein Zahlkörper, dessen Ordnung der Einheitswurzelgruppe $\mu(k)$ zu einer natürlichen Größe n teilerfremd ist, dann ist jede auflösbare Gruppe G vom Exponenten n unter Berücksichtigung endlich vieler Einbettungen lokaler Galoisgruppen $G(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \hookrightarrow G$ zu verwirklichen.*

In dieser Arbeit bekennt sich Neukirch zu zwei Prinzipien, derer die Konstruktion der auflösbaren Erweiterung unterliegt:

1. Durch das Lokal-Global-Prinzip ist die lokale Lösbarkeit des Einbettungsproblems notwendig. Daher muß zunächst die lokale Lage untersucht werden. Um dies auf so einfach wie mögliche Weise zu gestalten, sollten die lokalen Lösungen an möglichst vielen Stellen zyklisch sein. Im lokalen Fall sind zyklische zahm verzweigte Erweiterungen über $k_{\mathfrak{p}}$ vom Grad n allein dann vorhanden, wenn μ_n im Grundkörper $k_{\mathfrak{p}}$ enthalten ist. Mit anderen Worten: die Stelle $\mathfrak{p}$ zerlegt sich in $k(\zeta_n)/k$ voll.

2. Wenn ein durch eine Primzahl p annullierter $G(K/k)$-Modul A über der Erweiterung K/k verwirklicht werden soll und K nicht die $p^{\underline{ten}}$ Einheitswurzeln enthält, so ist die Lösbarkeit des globalen Problems gleichbedeutend mit der Lösbarkeit sämtlicher lokaler Probleme. Laut [Neu79] geht dieser Gedanke auf O. Neumann zurück.

Die beiden letzten Theoreme stellen die tiefliegendsten Ergebnisse zur Frage nach der Erstellbarkeit globaler Lösungen des Einbettungsproblems dar. Aufgrund des umständlichen Verfahrens, welches auf einem sogenannten Schrumpfverfahren fußt, fehlt dem Satz von Schafarewitsch jedoch bis auf eine Ausnahme die Möglichkeit einer konkreten Aussage über das Zerlegungsverhalten der Primstellen in dieser Erweiterung. In diesem Verfahren werden bei sukzessiver Verwirklichung der Subnormalquotienten der auflösbaren Gruppe in jedem Schritt auf lokaler Ebene Schwierigkeiten auftreten, die es nötig machen, die jeweils vorangegangenen Schritte erneut zu modifizieren. Die angesprochene Ausnahme geht auf A. Schmidt zurück und liest sich folgendermaßen: Die Erweiterung aus 1.1.6 kann derart gewählt werden, daß sich endlich viele gegebene Primstellen in ihr voll zerlegen und keine wilde Verzweigung auftritt (s. [NSW08], chap. IX, §6, Exercises). Neukirch kann aufgrund der Bedingung an die Einheitswurzeln auf das Schrumpfverfahren verzichten und somit endlich viele lokale Vorgaben erfüllen - muß sich aber beispielsweise einschränken auf Gruppen ungerader Ordnung. Beiden Ansätzen gemein ist bei der Verwirklichung der abelschen Subnormalquotienten der auflösbaren Gruppe G die Herannahme des Hasseschen Lokal-Global-Prinzips - stets wird zunächst sichergestellt, daß es keine lokalen Hindernisse gibt, bevor die globale Frage in Angriff genommen wird. Dabei kann Neukirch gewährleisten, daß auch im folgenden Schritt lokale Probleme von vorneherein vermieden werden, d.h. die neu entstehenden lokalen Probleme des nächsten Schritts sind ausnahmslos lösbar. Für Zahlkörper mit mehr Einheitswurzeln ist bis dato nichts bekannt, was über das Gesagte hinausgeht. In besonderem Maß gilt dies für die Gruppen gerader Ordnung. Einem wohlbekannten Beispiel zufolge, welches unter anderem in [NSW08] auf Seite 562 oder [Ser08], chap. I, §2, Theorem 4 zu finden ist, treten schnell Schwierigkeiten auf:

1.1.8 Beispiel: Ist k ein Körper, dessen Charakteristik nicht 2 ist, dann kann die quadratische Erweiterung $k(\sqrt{a})$ genau dann in eine zyklische Erweiterung vom Grad 4 eingebettet werden, wenn a die Summe zweier Quadrate ist.

Im Fall eines Zahlkörpers $k/\mathbb{Q}$ ist dies gleichbedeutend damit, daß a überall lokale Summe zweier Quadrate ist. Es gilt hier demnach ein Lokal-Global-Prinzip - das bedeutet: wenn a so gewählt wird, daß auch im nächsten Schritt keine lokalen Hindernisse entstehen, wird die globale Frage auch eine affirmative Antwort erhalten. Dieses Beispiel belegt, daß man sich auch in anderen Fällen als den bisher bekannten ähnliche Ergebnisse erhoffen kann.

Soll eine Gruppe G über einem endlichen Zahlkörper $k/\mathbb{Q}$ unter Berücksichtigung dieser Vorgaben verwirklicht werden, kann unter Umständen die Struktur der Gruppe G ausgenutzt werden, um mit dem Neukirchschen Verfahren die Verwirklichung einiger auflösbarer Gruppen zu erreichen.

Dabei wird auf sogenannte stark nicht-abelsche Gruppen zurückgegriffen, welche im 8. Kapitel folgendermaßen getauft werden.

1.1.9 Definition: *Eine endliche auflösbare Gruppe G heißt **stark nicht-abelsch**, wenn sie eine Zerlegung in Normalteiler*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{\iota\}$$

mit diesen Eigenschaften besitzt:

1. *$A_i := G_i/G_{i+1}$ ist abelsch und ein einfacher G/G_i–Modul, welcher von einer Primzahl p_i annulliert wird.*

2. *Für $i > 1$ ist der größte Normalteiler $N_i \lhd G/G_i$, welcher auf A_i trivial operiert, ein echter Normalteiler, das heißt $N_i \neq G/G_i$.*

3. *Es gibt für kein $i > 1$ einen Epimorphismus $N_i \to A_i$.*

4. *Ist A_i nicht zyklisch, dann ist $G \cong G_{i+1} \rtimes G/G_{i+1}$.*

Dieser Katalog von Eigenschaften läßt sich zwar nicht einschränkungsfrei auf Untergruppen oder Quotienten übertragen, wird aber beispielsweise sowohl von der symmetrischen Gruppe S_4 auch von der alternierenden Gruppe A_4 erfüllt, nicht jedoch durch die in ihr enthaltene Diedergruppe D_4. Nahezu rein gruppentheoretischen Erwägungen zufolge sind diese über vielen Zahlkörpern mit hinreichend vielen Einheitswurzeln bei einer endlichen Anzahl beliebiger Vorgaben zu verwirklichen. Es gilt das Folgende:

1.1.10 Theorem: *Ist k ein Zahlkörper und G eine stark nicht-abelsche Gruppe vom Exponenten m mit endlich vielen lokalen Vorgaben $\{\psi_\mathfrak{p} : G_{k_\mathfrak{p}} \to G \mid \mathfrak{p} \in T\}$, dann gibt es eine Galoiserweiterung K/k, welche diese verwirklicht, sobald die folgende Bedingung erfüllt ist:*

> *Es sei $S := cs(k(\mu_m)/k) \cup T$, dann ist $A_0 := G_0/G_1$ innerhalb von k_S mit den Vorgaben $\overline{\psi_\mathfrak{p}} : G_{k_\mathfrak{p}} \to A_0$ realisierbar.*

Insbesondere ist die Bedingung in diesem Satz leer, sobald die Einheitswurzeln aus μ_m in k enthalten sind. Dies liefert erste Beispiele für die Verwirklichung von Gruppen gerader Ordnung. Insbesondere sind stark nicht-abelsche Gruppen - zum Beispiel die Gruppen S_4, A_4 oder S_3 - bei endlich vielen lokalen Vorgaben über $k(\mu_m)$ unbedingt zu verwirklichen.

1.2 Danksagung

Meinem Doktorvater Prof. Dr. Kay Wingberg, durch welchen ich in den vergangenen Jahren bei der Universität Heidelberg Anstellung fand, gebührt herzlicher Dank für seine unschätzbare Unterstützung und sein in mich gesetztes Vertrauen in mein Können. Darüber hinaus ist meinen Mitstreitern Peter Barth und Jochen Gärtner für die vielen nützlichen Diskussionen bei der Entstehung dieser Arbeit zu danken. Desgleichen danke ich Dr. Jakob Stix für die langen Gespräche über meine Ideen und Vorstellungen. Ich habe in den vergangenen Jahren einen teilweise harten Kampf um die Vollendung dieser Dissertation geführt. Zwischen Zweifel und Optimismus setzte sich letzterer durch. Dazu beigetragen haben all jene, welche in dieser Zeit eine dieser Arbeit förderliche Atmosphäre um mich herum geschaffen haben. Da ohne sie selbige heute nicht vorläge, bin ich diesen zu tiefstem Dank verpflichtet. Allen voran sind dabei meine Familie resp. Eltern zu nennen. Ich freue mich nun, eine Arbeit vorstellen zu können, die meine Ideen zur Verwirklichung auflösbarer Gruppen darstellt. Abschließend allen Genannten und Gemeinten herzlicher Dank für ihre Unterstützung.

2 Inhaltsangaben

2.1 Résumé

Les resultats principaux de cet article sont les suivants.

Soit $\mathfrak{c}$ une classe complète de groupes finis, $S(\mathfrak{c})$ l'ensemble des nombres premiers p tel que $\mathbb{Z}/p \in \mathfrak{c}$ et $S(\mathfrak{c}) \subseteq S$ un ensemble contenant tous les diviseurs premiers $\mathfrak{p}|p$ tel que $p \in S(\mathfrak{c})$ dans un corps de nombres global k. L'extension pro-$\mathfrak{c}$ maximale ne ramifié qu'aux places de S est notée $k_S(\mathfrak{c})$. Si $S \subset T$ est un autre ensemble des places de k, tel qu'il y a une extension finie F/k dans $k_S(\mathfrak{c})$, tel que les premiers totalement decomposée dans cet extension sont presque tous contenu dans $T \smallsetminus S$ et si pour tout premier $p \in S(\mathfrak{c})$ l'extension de corps $k(\zeta_p)/k$ fournit une extension dont le groupe de Galois est dans $\mathfrak{c}$, alors $G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$ est un pro-$\mathfrak{c}$-groupe libre de rang infiniment denombrable et il y a un epimorphisme

$$\mathop{\ast}_{\mathfrak{p} \in T \smallsetminus S} T_{\mathfrak{p}}(\mathfrak{c}) \twoheadrightarrow G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$$

fournissant un isomorphisme aux groupes abelisés.

Soit $(K_{\mathfrak{P}}/k_{\mathfrak{p}})_{\mathfrak{p} \in S}$ un ensemble fini d'extensions locales de corps p-adiques, et soit k un corps globale dont les complétés en S sont isomorphes aux $k_{\mathfrak{p}}$. En outre, soient $G(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \hookrightarrow G$ des injections dans un groupe fini et résoluble G dont l'exposant est égal à $n \in \mathbb{N}$ pour les places $\mathfrak{p} \in S$. Soit

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{\iota\}$$

une suite des sous-groupes distingués de G dont les quotients $A_i = G_i/G_{i+1}$ sont des G/G_i-modules simples qui vérifient les propriétés suivantes.

1. Pour $i > 1$, le plus grand sous-groupe distingué $N_i \lhd G/G_i$ opérant trivialement sur A_i n'est pas égal à G/G_i.
2. Si $i > 1$, il n'y a pas d'épimorphisme $N_i \twoheadrightarrow A_i$.
3. Quand A_i n'est pas cyclique, on a $G \cong G_{i+1} \rtimes G/G_{i+1}$.

Selon cet article, il est maintenant possible de construire une extension résoluble de groupe de Galois G, tel que les groupes de decomposition s'injectent de la maniére préscrite, si le corps de base k possède les racines $n^{\underline{\text{ièmes}}}$ de l'unité μ_n.

2.2 Abstract

The central results of this thesis are the following ones:

Let $\mathfrak{c}$ be a full class of finite groups, $S(\mathfrak{c})$ shall describe the set of prime numbers p such that $\mathbb{Z}/p \in \mathfrak{c}$ and let $S(\mathfrak{c}) \subseteq S$ be a set of primes of a global number field k containing all prime divisors of p contained in $S(\mathfrak{c})$. The maximal pro-$\mathfrak{c}$-extension of k unramified outside S will be denoted by $k_S(\mathfrak{c})$. Assume that the Galois group of $k(\zeta_p)/k$ is contained

in $\mathfrak{c}$ for all $p \in S(\mathfrak{c})$. If S is contained in another set of primes T such that there exists a finite subextension F/k of $k_S(\mathfrak{c})$ with $T \underset{\sim}{\subset} cs(F/k)$, then the Galois group $G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$ of $k_T(\mathfrak{c})/k_S(\mathfrak{c})$ is a free pro-$\mathfrak{c}$-group of countable infinite rank and there is an epimorphism

$$\mathop{\ast}_{\mathfrak{p} \in T \smallsetminus S} T_{\mathfrak{p}}(\mathfrak{c}) \twoheadrightarrow G(k_T(\mathfrak{c})/k_S(\mathfrak{c})),$$

which yields an isomorphism on the abelianizations of these groups.

Let $(K_{\mathfrak{P}}/k_{\mathfrak{p}})_{\mathfrak{p} \in S}$ be a finite family of local extensions of p-adic fields and k a global field whose completions in the places of S are the fields $k_{\mathfrak{p}}$. Furthermore, for the places of S let $G(K_{\mathfrak{P}}/k_{\mathfrak{p}}) \hookrightarrow G$ be injections in a finite solvable group G whose exponent is equal to $n \in \mathbb{N}$. Assume that there is a sequence

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{\iota\}$$

of normal subgroups of G where for each i the quotient $A_i = G_i/G_{i+1}$ is a simple G/G_i-module such that the following properties are satisfied:

1. For $i > 1$, the biggest normal subgroup $N_i \triangleleft G/G_i$ which operates trivially on A_i is not equal to G/G_i itself.
2. If $i > 1$, there is no epimorphism $N_i \twoheadrightarrow A_i$.
3. Whenever A_i is not cyclic, one has the equality $G \cong G_{i+1} \rtimes G/G_{i+1}$.

Then it will be shown that it is possible to construct a solvable extension of k with Galois group G realizing the extensions $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ if all $n^{\underline{th}}$ roots of unity are contained in the base field k.

Inhaltsverzeichnis

3 Einbettungsprobleme

3.1 Allgemeines

Ist $\mathfrak{G}$ eine proendliche Gruppe, dann besteht ein ***Einbettungsproblem*** $\mathcal{E}(\mathfrak{G}) = \mathcal{E}(\mathfrak{G}, \Gamma, G)$ für die Gruppe $\mathfrak{G}$ aus einem Diagramm

$$\begin{tikzcd}
 & & & \mathfrak{G} \arrow[dl, dotted, "\psi"'] \arrow[d, "\varphi"] & \\
1 \arrow[r] & H \arrow[r] & G \arrow[r, "j"] & \Gamma \arrow[r] & 1
\end{tikzcd}$$

mit endlichen Gruppen H, G und Γ, einer exakten Zeile und einem Epimorphismus φ sowie der Frage nach dem Vorhandensein eines (surjektiven) Homomorphismus $\psi : \mathfrak{G} \to G$ mit der Eigenschaft, daß $\varphi = j \circ \psi$ gilt.

Von dem arithmetischen Standpunkt her ist der Spezialfall dieses Problems, welcher durch eine Galoisgruppe $\mathfrak{G}$, etwa $\mathfrak{G} = G_S$ für eine beliebige Primstellenmenge S eines Zahlkörpers k gegeben ist, von besonderem Interesse. Ist k ein Zahlkörper, dann sei ab nun mit $\overline{k}$ stets ein fest gewählter separabler algebraischer Abschluß und mit k_S die größte außerhalb einer gegebenen Primstellenmenge S unverzweigte Teilerweiterung gemeint. In diesem Fall beschreibt der Epimorphismus φ eine endliche Teilerweiterung $k_S/K/k$ von k, deren Galoisgruppe durch $G(K/k)$ gegeben ist. Ein surjektiver Homomorphimus $\psi : \mathfrak{G} \to G$ verwirklicht dann eine Erweiterung N/k in k_S/k, welche in $G = G(N/k)$ ihre Galoisgruppe hat und in K/k eine galoissche Teilerweiterung findet.

Wenn ein solches Einbettungsproblem über einem globalen Zahlkörper k in Verbindung mit den zugehörigen lokalen Einbettungsproblemen betrachtet wird, reicht es nicht, zwei verschiedene Lösungen $\psi_{1,2}$ des Einbettungsproblems $\mathcal{E}(\mathfrak{G})$ für äquivalent zu halten, sobald ihre Kerne und somit deren Fixkörper übereinstimmen. Vielmehr ist gemäß [Neu73a] die folgende Festlegung angemessen:

3.1.1 Definition: *Zwei Homomorphismen $\psi', \psi : \mathfrak{G} \to G$ mit $j \circ \psi' = j \circ \psi = \varphi$ heißen* ***äquivalent****, wenn*

$$\psi'(\sigma) = a\psi(\sigma)a^{-1} \text{ für jedwedes } \sigma \in \mathfrak{G} \text{ bei festem } a \in A \text{ gilt.}$$

Unter einer ***Lösung*** *des Einbettungsproblems wird fortan eine solche Äquivalenzklasse $[\psi]$ verstanden. In ihrer Gesamtheit bilden die Lösungen $[\psi]$ des Einbettungsproblems den sogenannten* ***Lösungsraum*** $\mathcal{L}_{\mathcal{E}(\mathfrak{G})} = \mathcal{L}_{\mathcal{E}(\mathfrak{G},\Gamma,G)}$ *und ein Element aus selbigem ist definitionsgemäß eine* ***eigentliche*** *Lösung, sobald die Homomorphismen dieser Klasse surjektiv sind.*

Ist $\mathfrak{G}'$ durch $\mathfrak{G}' \hookrightarrow \mathfrak{G}$ eine Untergruppe von $\mathfrak{G}$, dann entsteht aus dem Diagramm

$$\begin{tikzcd}
 & & & \mathfrak{G} \arrow[dl, dotted, "\psi"'] \arrow[d, "\varphi"] & \\
1 \arrow[r] & H \arrow[r] & G \arrow[r, "j"] & \Gamma \arrow[r] & 1
\end{tikzcd}$$

ein Weiteres, welches durch die Gruppen $\Gamma' := \varphi(\mathfrak{G}') \subseteq \Gamma$ und $G' \subseteq G$ mit $G' := j^{-1}(\Gamma')$ beschrieben wird:

$$\begin{tikzcd} & & & \mathfrak{G}' \arrow[dl, dotted, "\psi"'] \arrow[d, "\varphi|_{\mathfrak{G}'}"] & \\ 1 \arrow[r] & H \arrow[r] & G' \arrow[r, "j|_{G'}"] & \Gamma' \arrow[r] & 1. \end{tikzcd}$$

Dieses Einbettungsproblem $\mathcal{E}(\mathfrak{G}') = \mathcal{E}(\mathfrak{G}', \Gamma', G')$ werde im weiteren Verlauf ***Verlagerung*** des ursprünglichen $\mathcal{E}(\mathfrak{G})$ auf die Untergruppe $\mathfrak{G}'$ genannt.

> Für eine Galoisgruppe $\mathfrak{G}$ zum Grundkörper k entspricht dies einem auf den Fixkörper k' von $\mathfrak{G}'$ verschobenen Einbettungsproblem.

Nach gleicher Art wird aus einer Lösung $[\psi] \in \mathcal{L}_{\mathcal{E}(\mathfrak{G})}$ des ursprünglichen Problems durch Verlagerung mittels Ersatz von $[\psi]$ durch $[\psi|_{\mathfrak{G}'}]$ eine Lösung des Neuen. Für einen nichtleeren Lösungsraum $\mathcal{L}_{\mathcal{E}(\mathfrak{G})}$ ergibt sich daraus die Einschränkungsabbildung

$$res : \mathcal{L}_{\mathcal{E}(\mathfrak{G})} \to \mathcal{L}_{\mathcal{E}(\mathfrak{G}')}$$

auf natürliche Weise.
Von besonderem Interesse ist die Frage, inwieweit eine Lösung

$$[\overline{\psi}] \in \mathcal{L}_{\mathcal{E}(\mathfrak{G}')} \text{ eine Lösung } [\psi] \in \mathcal{L}_{\mathcal{E}(\mathfrak{G})}$$

nach sich zieht, resp. ob $[\overline{\psi}]$ im Bild der obigen Einschränkungsabbildung liegt oder nicht.

> Im Hinblick auf den körpertheoretischen Hintergrund dieser Fragestellung, d.h. auf die Verwirklichung komplizierterer Gruppen - etwa auflösbarer - ist der Fall eines abelschen Kerns $A := H$ von hervorgehobener Bedeutung, da dieser unter Umständen durch die Methode des schrittweisen Aufstiegs zielführend ist. In diesem Fall darf A als $\mathfrak{G}$–Modul verstanden werden, dessen Operation mit Hilfe von φ definiert wird. Wird das Einbettungsproblem um $\mathfrak{G}_0$ zu einem mit exakter Spalte erweitert
>
> $$\begin{tikzcd} & & & \mathfrak{G}_0 \arrow[d] \arrow[ddll, dotted, "\psi_0"'] & \\ & & & \mathfrak{G} \arrow[dl, dotted, "\psi"'] \arrow[d, "\varphi"] & \\ 1 \arrow[r] & A \arrow[r] & G \arrow[r, "j"] & \Gamma \arrow[r] & 1, \end{tikzcd}$$
>
> dann findet ein solches Einbettungsproblem in der Hochschild-Serre-Sequenz
>
> $$0 \to H^1(\Gamma, A) \to H^1(\mathfrak{G}, A) \to H^1(\mathfrak{G}_0, A)^{\Gamma} \to H^2(\Gamma, A) \to H^2(\mathfrak{G}, A)$$
>
> seine kohomologische Formulierung, und zwar gilt gemäß Hoechsmann [Hoe68]:

3.1.2 Satz (Hoechsmann): *Beschreibt* $\epsilon \in H^2(\Gamma, A)$ *die Gruppenerweiterung*

$$1 \to A \to G \to \Gamma \to 1,$$

so hat das Einbettungsproblem $\mathcal{E}(\mathfrak{G})$ *genau dann eine Lösung, wenn für dessen Inflation*

$$inf(\epsilon) = 1$$

gilt, d.h. genau dann, wenn ϵ *über ein* Γ*−invariantes Urbild* $\psi_0 : \mathfrak{G}_0 \to A$ *aus* $H^1(\mathfrak{G}_0, A)$ *unter der Transgression verfügt.*

Beweis. s. [Neu73a], §1, Satz 2 oder [NSW08], chap. III, §5, Proposition 9. ◊

3.2 Lokale Vorgaben

Es sei $\mathcal{E}(\mathfrak{G})$ ein Einbettungsproblem für $\mathfrak{G} = G(k_S/k)$ über dem globalen Zahlkörper k. Es bezeichnet $\mathcal{P}_k$ die Gesamtheit der Primstellen $\mathfrak{p}$ von k. Für jedes Element $\mathfrak{p} \in \mathcal{P}_k$ sei $\mathfrak{G}_\mathfrak{p} \subseteq \mathfrak{G}$ eine fest gewählte Zerlegungsgruppe über der Stelle $\mathfrak{p}$. Die Verlagerungen $\mathcal{E}(\mathfrak{G}_\mathfrak{p})$ von $\mathcal{E}(\mathfrak{G})$ auf die Untergruppen $\mathfrak{G}_\mathfrak{p} \subseteq \mathfrak{G}$ heißen die zum globalen Einbettungsproblem $\mathcal{E}(\mathfrak{G})$ gehörigen ***lokalen Einbettungsprobleme***. Unter einer ***unverzweigten Lösung*** $[\psi]$ von $\mathcal{E}(\mathfrak{G})$ wird gemeinhin ein Homomorphismus

$$\psi_\mathfrak{p} : \mathfrak{G}_\mathfrak{p} \to E_\mathfrak{p} \text{ aus } \mathcal{L}_{\mathcal{E}(\mathfrak{G}_\mathfrak{p})}$$

verstanden, welcher entlang der Trägheitsgruppe $\mathfrak{T}_\mathfrak{p}$ faktorisiert, d.h. einen Homomorphismus auf $\mathfrak{G}_\mathfrak{p}/\mathfrak{T}_\mathfrak{p}$ definiert. Eine globale Lösung $[\psi]$ ist in $\mathfrak{p}$ per definitionem ***unverzweigt***, wenn ihre Verlagerung $[\psi_\mathfrak{p}]$ es ist. Die Gesamtheit der Verlagerungen einer Lösung $[\psi]$ nach den Stellen $\mathfrak{p} \in \mathcal{P}_k$ werden als ***lokale Komponenten*** derselben bezeichnet. Ist A abelsch, so ist A ein endlicher $\mathfrak{G}$−Modul und es lassen sich die Kohomologiegruppen $H^i(\mathfrak{G}, A)$ resp. $H^i(\mathfrak{G}_\mathfrak{p}, A)$ bilden.

3.2.1 Definition: *Es sei*

$$H^i_{nr}(\mathfrak{G}_\mathfrak{p}, A) := \mathit{Bild}(H^i(\mathfrak{G}_\mathfrak{p}/\mathfrak{T}_\mathfrak{p}, A^{\mathfrak{T}_\mathfrak{p}}) \overset{inf^i}{\to} H^i(\mathfrak{G}_\mathfrak{p}, A))$$

und bezeichnet diese Gruppe als den ***unverzweigten*** *Anteil von* $H^i(\mathfrak{G}_\mathfrak{p}, A)$. *Die Menge*

$$\mathcal{L}^{nr}_{\mathcal{E}(\mathfrak{G}_\mathfrak{p})} := \{[\psi_\mathfrak{p}] \in \mathcal{L}_{\mathcal{E}(\mathfrak{G}_\mathfrak{p})} | [\psi_\mathfrak{p}] \textit{ ist eine unverzweigte Lösung.}\}$$

heißt ***unverzweigter*** *Anteil des Lösungsraums* $\mathcal{L}_{\mathcal{E}(\mathfrak{G})}$.

Die beschränkten Produkte

$$\prod_{\mathfrak{p} \in \mathcal{P}_k} \mathcal{L}_{\mathcal{E}(\mathfrak{G})} \text{ und } \prod_{\mathfrak{p} \in \mathcal{P}_k} H^i(\mathfrak{G}_\mathfrak{p}, A)$$

jeweils bezüglich ihrer unverzweigten Anteile liefern die Abbildungen

$$\mathcal{L}_{\mathcal{E}(\mathfrak{G})} \to \prod_{\mathfrak{p} \in \mathcal{P}_k} \mathcal{L}_{\mathcal{E}(\mathfrak{G}_\mathfrak{p})}$$

und

$$H^i(\mathfrak{G}, A) \to \prod_{\mathfrak{p} \in \mathcal{P}_k} H^i(\mathfrak{G}_\mathfrak{p}, A).$$

3.2.2 Bemerkung: Über der Gruppe $\prod_{\mathfrak{p}} H^1(\mathfrak{G}_{\mathfrak{p}}, A)$ ist $\prod_{\mathfrak{p}} \mathcal{L}_{\mathcal{E}(\mathfrak{G}_{\mathfrak{p}})}$ ein prinzipal-homogener Raum, desgleichen ist es $\mathcal{L}_{\mathcal{E}(\mathfrak{G})}$ über $H^1(\mathfrak{G}, A)$.

Darunter wird das Folgende verstanden:

3.2.3 Definition: *Ein topologischer Raum X, auf dem eine Gruppe Γ stetig und einfach transitiv operiert, heißt* ***prinzipal homogener Raum*** *über Γ. Wirkt eine Untergruppe Γ_0 auf einem abgeschlossenen Unterraum $Y \subseteq X$ einfach transitiv, wird von einem* ***homogenen Unterraum*** *gesprochen.*

In der Absicht, auflösbare Gruppen G mit lokaler Vorgabe schrittweise zu verwirklichen, ist die kohomologische Sichtweise im folgenden Diagramm konkretisiert:

$$\begin{tikzcd}
H^1(k,A) \arrow[r, "res"] \arrow[d, "res"] & H^1(K,A)^{\Gamma} \arrow[r, "tg"] \arrow[d, "res"] & H^2(\Gamma,A) \arrow[r, "inf"] \arrow[d, "res"] & H^2(k,A) \arrow[d, "res"] \\
\bigoplus_{\mathfrak{p}} H^1(k_{\mathfrak{p}},A) \arrow[r, "res_{\mathfrak{p}}"] & \bigoplus_{\mathfrak{p}} \bigoplus_{\mathfrak{P}|\mathfrak{p}} H^1(K_{\mathfrak{P}},A)^{\Gamma_{\mathfrak{P}}} \arrow[r, "tg_{\mathfrak{p}}"] & \bigoplus_{\mathfrak{p}} H^2(\Gamma_{\mathfrak{p}},A) \arrow[r, "inf_{\mathfrak{p}}"] & \bigoplus_{\mathfrak{p}} H^2(k_{\mathfrak{p}},A).
\end{tikzcd}$$

Im Fall $K \subset k_S$ gibt es zusätzlich das folgende Diagramm:

$$\begin{tikzcd}
H^1(k_S/k,A) \arrow[r, "res"] \arrow[d, "res"] & H^1(k_S/K,A)^{\Gamma} \arrow[r, "tg"] \arrow[d, "res"] & H^2(\Gamma,A) \arrow[r, "inf"] \arrow[d, "res"] & H^2(k_S/k,A) \arrow[d, "res"] \\
\bigoplus_{\mathfrak{p}} H^1(k_{\mathfrak{p}},A) \arrow[r, "res_{\mathfrak{p}}"] & \bigoplus_{\mathfrak{p}} \bigoplus_{\mathfrak{P}|\mathfrak{p}} H^1(K_{\mathfrak{P}},A)^{\Gamma_{\mathfrak{P}}} \arrow[r, "tg_{\mathfrak{p}}"] & \bigoplus_{\mathfrak{p}} H^2(\Gamma_{\mathfrak{p}},A) \arrow[r, "inf_{\mathfrak{p}}"] & \bigoplus_{\mathfrak{p}} H^2(k_{\mathfrak{p}},A).
\end{tikzcd}$$

Zur konkreten Lösbarkeit ist der folgende Satz bekannt:

3.2.4 Satz: *Ist ein Einbettungsproblem $\mathcal{E}(\mathfrak{G})$ mit abelschem Kern A gegeben und die Restriktionsabbildung*

$$res^2 : H^2(\mathfrak{G}, A) \to \prod_{\mathfrak{p} \in \mathcal{P}_k} H^2(\mathfrak{G}_{\mathfrak{p}}, A)$$

ein Monomorphismus, dann ist das globale Problem genau dann lösbar, wenn sämtliche zu diesem Problem gehörigen lokalen Probleme es sind.

Beweis. s. [Neu73a], §2, Satz 2. ◊

3.2.5 Definition: *Ist $\Gamma_{\mathfrak{p}}$ zyklisch, so bezeichne*

$$\mathcal{L}^{zykl}_{\mathcal{E}(G_{k_{\mathfrak{p}}}, \Gamma_{\mathfrak{p}}, G_{\mathfrak{p}})}$$

die (evtl. leere) Menge aller Klassen $[\psi]$, deren Vertreter Homomorphismen mit zyklischem Bild sind. Diese Menge werde ***zyklischer Anteil der Lösungsmenge*** *genannt. Wird eine* *globale Lösung aus $\mathcal{L}_{\mathcal{E}(G_k,\Gamma,G)}$ unter der Einschränkungsabbildung in ein Tupel zyklischer Lösungen übergeführt, wird von einer* ***lokal zyklischen*** *Lösung gesprochen. Mit anderen Worten: die Zerlegungsgruppen des verwirklichten Körpers über k sind ausnahmslos zyklische Gruppen. Die Menge aller solchen Lösungen wird mit*

$$\mathcal{L}^{lok\ zykl}_{\mathcal{E}(G_k,\Gamma,G)} \textit{ bezeichnet.}$$

4 Auflösbare Gruppen

4.1 Kohomologische Dimensionen

Ziel dieses Abschnitts ist es, Aussagen für die pro-$\mathfrak{c}$-Quotienten der absoluten Galoisgruppen bei beschränkter, durch zwei Stellenmengen S, T gegebener Verzweigung zu machen. Allem voran sei die folgende Definition gestellt.

4.1.1 Definition:

1. *Unter einer* ***vollständigen*** *Klasse $\mathfrak{c}$ endlicher Gruppen wird eine Klasse endlicher Gruppen verstanden, welche bzgl. Untergruppenbildung, homomorpher Bilder und Gruppenerweiterungen abgeschlossen ist. Die Klasse der auflösbaren Gruppen wird mit $(solv)$ bezeichnet.*

2. *Ist $\mathfrak{c}$ eine vollständige Klasse endlicher Gruppen, dann ist eine* ***pro-$\mathfrak{c}$-Gruppe*** *ein projektiver Limes von Gruppen aus $\mathfrak{c}$.*

3. *$S(\mathfrak{c})$ ist die Menge aller primen Größen p, so daß $\mathbb{Z}/p \in \mathfrak{c}$ gilt. Ist S eine Menge von Primzahlen, dann ist $\mathfrak{c}(S)$ die Klasse aller endlichen Gruppen deren Ordnung nur durch Primzahlen p aus S teilbar ist.*

4. *$\mathbb{N}(S)$ sei die Menge aller natürlichen Zahlen, welche nur durch Primzahlen p teilbar sind, deren Stellenmenge S_p gänzlich in S enthalten ist.*

5. *Ist K/k eine Zahlkörpererweiterung, so bezeichne $cs(K/k)$ die sich in dieser Erweiterung voll zerlegenden Stellen aus $\mathcal{P}_k$. Ist die Erweiterung trivial, so bezeichne sie $\mathcal{P}_k$ selbst.*

6. *Zu Erweiterung von Zahlkörpern K/k sei $Ram(K/k)$ die Menge aller verzweigten Primstellen aus $\mathcal{P}_k$.*

Es sei $\mathfrak{c}$ eine vollständige Klasse auflösbarer Gruppen.

4.1.2 Satz: *Es sei eine pro-$\mathfrak{c}$-Gruppe G mit $\mathfrak{c} \subseteq (solv)$ gegeben. Dann sind gleichbedeutend*

1. *G ist eine abgeschlossene Untergruppe einer freien Gruppe $F_X(\mathfrak{c})$ mit normalem Komplement: $F_X(\mathfrak{c}) = R \rtimes_\phi G$.*

2. *G ist ein projektives Objekt in der Kategorie der pro-$\mathfrak{c}$-Gruppen.*

Beweis. klar. ◊

Es sei eine Primstellenmenge S gegeben. Aus [NSW08] ist der folgende Satz über die kohomologische Dimension des pro-$\mathfrak{c}$-Quotienten bekannt.

4.1.3 Satz: *Wenn $S(\mathfrak{c}) \subseteq S$ gilt, ist*

$$cd(G_S(\mathfrak{c})) \leq 2.$$

Beweis. Dies ist eine Folgerung der Aussagen von [NSW08], chap. X, §4, Corollary 9 und chap. VIII, §3, Proposition 18. ◊

Allgemein gibt es die Projektion

$$G_{k_{\mathfrak{p}}}(\mathfrak{c}) \to G_S(\mathfrak{c})_{\mathfrak{p}}.$$

Da für $p \in S(\mathfrak{c})$ und $\mathfrak{p}|p$ die Gruppe $G_S(\mathfrak{c})_{\mathfrak{p}}$ die Zerlegungsgruppe einer endlichen Stelle $\mathfrak{p}$ ist, welche eine abgeschlossene Untergruppe von $G_S(\mathfrak{c})$ ist, gilt:

4.1.4 Satz: *Wenn $S(\mathfrak{c}) \subseteq S$ ist und $\mathfrak{p}|p$ mit $p \in S(\mathfrak{c})$ gilt, so ist*

$$cd_p(G_S(\mathfrak{c})_{\mathfrak{p}}) \leq 2.$$

Beweis. Klar. ◊

4.1.5 Satz: *Es sei L/K eine pro-auflösbare galoissche Körpererweiterung mit $S(\mathfrak{c}) \subseteq S$ und den Eigenschaften*

1. *L ist $\mathfrak{c} - S$-abgeschlossen.*
2. *K ist $\mathfrak{c} - (S_p \cup S_\infty)$-abgeschlossen.*

Dann gilt für $p \in S(\mathfrak{c})$

$$H^2(G(L/K), \mathbb{Z}/p) = 0.$$

Beweis. Der Beweis verläuft analog zu [NSW08], chap. X, §4, Theorem 2. ◊

4.1.6 Satz: *Es sei k ein Körper mit $Char(k) \neq p$, $S_p \cup S_\infty \subseteq S$ eine Primstellenmenge aus k und n eine natürliche Größe. Dann sind die folgenden Aussagen gleichwertig:*

1. *$cd_p(k_S/k) \leq n$.*
2. *$H^{n+1}(G(k_S/K), \mathcal{O}_S^*)(p) = 0$ und $H^n(G(k_S/K), \mathcal{O}_S^*)$ ist $p-$divisibel für jede endliche separable Erweiterung K/k.*

Beweis. Analog zu [NSW08], chap. VI, §5, Proposition 11. ◊

4.1.7 Satz: *Es seien ein globaler Zahlkörper k und Stellenmengen $S(\mathfrak{c}) \subseteq S \subseteq T$ mit $cs(F/k) \subsetneqq T$ mit einer endlichen Erweiterung F/k, so daß $F \subseteq k_S(\mathfrak{c})$ erfüllt ist, gegeben. Dann gilt*

$$cd(G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))) \leq 1.$$

Beweis. Es sei $G_p \leq G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$ eine $p-$Sylowgruppe, deren Fixkörper mit L bezeichnet werde. Aus der Hochschild-Serre-Sequenz folgt: $H^2(G_p, \mathbb{Z}/p\mathbb{Z}) \hookrightarrow H^2(G(k_T/L), \mathbb{Z}/p\mathbb{Z})$ und es ist $H^2(G(k_T/L), \mathbb{Z}/p\mathbb{Z}) = 0$, weil

$$H^2(G(k_T/L), \mathcal{O}_T^*)(p) \hookrightarrow H^2(G(k_T/L), I_T)(p) = \bigoplus_{\mathfrak{p} \in T} Br(L_{\mathfrak{p}})(p) = 0$$

nach [NSW08], chap. VII, §1, Theorem 8 und $H^1(G(k_T/L), \mathcal{O}_T^*)(p) = 0$ gilt. Letztere Gruppe verschwindet nach dem Hauptidealsatz, da L wegen $\delta_K(T) = 1$ für Erweiterungen K/F keine p-Erweiterung besitzt, die an allen Stellen aus T voll zerlegt ist. ◊

Mit Hilfe des Riemannschen Existenzsatzes (s. [NSW08], chap. X, §5, Satz 1 oder [Win84]) läßt sich diese schärfere Aussage nachweisen:

4.1.8 Satz: *Es seien die Voraussetzungen wie oben außer der Aussage über die Größe der Stellenmenge T. Dann ist wiederum*

$$cd_p(G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))) \leq 1 \text{ für jedes prime } p \text{ aus } S(\mathfrak{c}).$$

Beweis. Daß für jeden p–primären $G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$-Modul A die Gruppen

$$H^i(G(k_T(\mathfrak{c})/k_S(\mathfrak{c})), A) \to H^i(G(k_T/k_S(\mathfrak{c})), A)$$

zueinander isomorph sind, folgt aus [NSW08], chap. X, §4, Corollary 8. Die rechte Seite verschwindet jedoch aufgrund von [NSW08], chap. X, §5, Corollary 4 für $i = 2$. ◊

4.1.9 Bemerkung: Dank globaler Klassenkörpertheorie läßt sich nun $G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))^{ab}$ berechnen. Dazu ist das Diagramm des Lemma 13 aus [NSW08], chap. X, §3 durch das Produkt mehrerer verschiedener Kopien desselben folgendermaßen zu ändern:

4.1.10 Hilfssatz: *Für Stellenmengen $S_p \cup S_\infty, T \subseteq S$ und einen Zahlkörper K ist das kanonische Diagramm*

$$\begin{tikzcd}
H_2(G_S, \widehat{\mathbb{Z}}(\mathfrak{c})) \arrow[r, hook] \arrow[d, equal] & \mathcal{O}^\times_{K,T} \otimes \widehat{\mathbb{Z}}(\mathfrak{c}) \arrow[r] \arrow[d, hook] & \prod_{\mathfrak{p} \in S \smallsetminus T} \widehat{U_\mathfrak{p}} \times \prod_{\mathfrak{p} \in T} \widehat{K^*_\mathfrak{p}} \arrow[r] \arrow[d, hook] & G_S^{ab}(\mathfrak{c}) \arrow[r, two heads] \arrow[d, equal] & Cl_T(K)(\mathfrak{c}) \arrow[d, two heads] \\
H_2(G_S, \widehat{\mathbb{Z}}(\mathfrak{c})) \arrow[r, hook] & \mathcal{O}^\times_{K,S} \otimes \widehat{\mathbb{Z}}(\mathfrak{c}) \arrow[r] & \prod_{\mathfrak{p} \in S} \widehat{K^*_\mathfrak{p}} \arrow[r] & G_S^{ab}(\mathfrak{c}) \arrow[r, two heads] & Cl_S(K)(\mathfrak{c})
\end{tikzcd}$$

kommutativ und besteht aus exakten Zeilen. Hierbei bezeichnet das Symbol $\widehat{\ }$ *die* $\mathfrak{c}$*-Vervollständigung der Gruppe.*

Beweis. Der Beweis erfolgt analog zu [NSW08], chap. X, §3, Lemma 13, ausgehend von dem Herzstück der Poitou-Tate-Sequenz

$$0 \to Ш^2(G_S, \mathbb{Z}/n)^\vee \to H^1(G_S, \mu_n) \to \bigoplus_{\mathfrak{p} \in S} H^1(K_\mathfrak{p}, \mu_n) \to H_1(G_S, \mathbb{Z}/n) \to Ш^1(G_S, \mathbb{Z}/n)^\vee \to 0$$

mit $n \in \mathbb{N}(S(\mathfrak{c}))$ wird ein Grenzübergang wie in [NSW08] an erwähnter Stelle vollzogen. ◊

Aus zwei Kopien der oberen Zeile dieses Diagramms wird durch Verwendung verschiedener Stellenmengen $S \subseteq T$ für $k' \subseteq k_S(\mathfrak{c})$ dieses Diagramm:

$$\begin{tikzcd}
H_2(G_T(k'), \widehat{\mathbb{Z}}(\mathfrak{c})) \arrow[r, hook] \arrow[d, equal] & \mathcal{O}^\times_{k'} \otimes \widehat{\mathbb{Z}}(\mathfrak{c}) \arrow[r] \arrow[d, hook] & \prod_{\mathfrak{p} \in T(k')} \widehat{U_\mathfrak{p}} \arrow[r] \arrow[d, hook] & G_T(k')^{ab}(\mathfrak{c}) \arrow[r, two heads] \arrow[d, equal] & Cl_T(k')(\mathfrak{c}) \arrow[d, two heads] \\
H_2(G_S(k'), \widehat{\mathbb{Z}}(\mathfrak{c})) \arrow[r, hook] & \mathcal{O}^\times_{k'} \otimes \widehat{\mathbb{Z}}(\mathfrak{c}) \arrow[r] & \prod_{\mathfrak{p} \in S(k')} \widehat{U_\mathfrak{p}} \arrow[r] & G_S(k')^{ab}(\mathfrak{c}) \arrow[r, two heads] & Cl_S(k')(\mathfrak{c})
\end{tikzcd}$$

Bei Grenzübergang über sämtliche $k' \subseteq k_S(\mathfrak{c})$ entfallen nach 4.1.5 die Terme

$$H_2(G_T(k_S(\mathfrak{c})), \widehat{\mathbb{Z}}(\mathfrak{c})) \text{ und } H_2(G_S(k_S(\mathfrak{c})), \widehat{\mathbb{Z}}(\mathfrak{c})).$$

Dasselbe gilt für $H_1(G_S(k_S(\mathfrak{c})), \widehat{\mathbb{Z}}(\mathfrak{c}))$, weil $k_S(\mathfrak{c})$ eine $\mathfrak{c} - S$-abgeschlossene Erweiterung ist. Schließlich verschwindet der Limes

$$\varprojlim_{k_S(\mathfrak{c})/k'/k} Cl(k')(\mathfrak{c}),$$

da $k_S(\mathfrak{c})$ die größte außerhalb S unverzweigte pro-$\mathfrak{c}$-Erweiterung von k ist. Dies ergibt das Diagramm

$$\begin{tikzcd}
\varprojlim_{k_S(\mathfrak{c})/k'/k} \mathcal{O}_{k'} \otimes \widehat{\mathbb{Z}}(\mathfrak{c}) \arrow[r, hook] \arrow[d, equal] & \varprojlim_{k_S(\mathfrak{c})/k'/k} \prod_{\mathfrak{p} \in T(k')} \widehat{U_{\mathfrak{p}}} \arrow[r, two heads] \arrow[d, two heads] & G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))^{ab} \\
\varprojlim_{k_S(\mathfrak{c})/k'/k} \mathcal{O}_{k'} \otimes \widehat{\mathbb{Z}}(\mathfrak{c}) \arrow[r, "\sim"] & \varprojlim_{k_S(\mathfrak{c})/k'/k} \prod_{\mathfrak{p} \in S(k')} \widehat{U_{\mathfrak{p}}} &
\end{tikzcd}$$

und daher die Isomorphie

$$G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))^{ab} \cong \varprojlim_{k_S(\mathfrak{c})/k'/k} \prod_{\mathfrak{p} \in T \setminus S(k')} \widehat{U_{\mathfrak{p}}},$$

wobei $\widehat{U_{\mathfrak{p}}}$ die pro-$\mathfrak{c}$-Vervollständigung der Einheitengruppe $U_{\mathfrak{p}}$ des lokalen Körpers $k'_{\mathfrak{p}}$ sei.

4.2 Freie pro-$\mathfrak{c}$-Gruppen

4.2.1 Definition:

1. *Es sei k ein globaler Zahlkörper und $\mathfrak{c}$ eine Klasse auflösbarer Gruppen. Dann heißt k* ***in bezug auf $\mathfrak{c}$ vollständig****, wenn für jedes prime p aus $S(\mathfrak{c})$ die Erweiterung $k(\zeta_p)/k$ über eine Galoisgruppe aus $\mathfrak{c}$ verfügt.*

2. *Eine (nicht unbedingt endliche) Erweiterung globaler Körper K/k heiße* ***$\mathfrak{c}$-potent****, sobald diese Eigenschaft zutrifft:*

   I. *Zu einer endlichen $\mathfrak{c}$-Gruppe E und einer endlichen separablen Erweiterung K'/K gibt es stets hinreichend viele Primstellen $\mathfrak{P}_1, ..., \mathfrak{P}_s$ aus K, welche sich in K' voll zerlegen und deren größte lokale pro-$\mathfrak{c}$-Erweiterungen über $K_{\mathfrak{P}}$ Homomorphismen*

   $$G(K_{\mathfrak{P}_i}(\mathfrak{c})/K_{\mathfrak{P}_i}) \longrightarrow E,\ i = 1, ..., s$$

   liefern, deren Bild die Gruppe E erzeugt.

   Ist $\mathfrak{c}$ die Klasse aller endlichen Gruppen, so heißt dieser Körper K ***potent****.*

4.2.2 Bemerkung: Ist eine Körpererweiterung K/k potent, so ist sie auch $\mathfrak{c}$–potent.

4.2.3 Beispiel: Es sei $S = \{3,7\}$ und $\mathfrak{c} = \mathfrak{c}(S)$, dann ist $\mathbb{Q}(\sqrt{-3}, \sqrt{-7})$ ein in bezug auf $\mathfrak{c}$ vollständiger Körper.

4.2.4 Generalvoraussetzung: Für den Rest dieses Abschnitts mögen diese Generalvoraussetzungen zutreffen:

$\mathfrak{c}$	sei eine Klasse auflösbarer Gruppen.
S	sei eine Stellenmenge, welche alle über $S(\mathfrak{c})$ liegenden enthalte.

4.2.5 Satz: *Ist k endlicher Zahlkörper, so gilt für $p \in S(\mathfrak{c})$ stets*

$$cd_p(G_{k_S(\mathfrak{c})}) \leq 1.$$

Beweis. Für $\mathfrak{q} \in \mathcal{P}_k$ und $p \in S(\mathfrak{c})$ ist

$$([k(\zeta_{p^n})_{\mathfrak{Q}} : k_{\mathfrak{q}}])_{n \in \mathbb{N}}$$

eine monoton bis ins Unendliche wachsende Folge, welche wegen $(\mathbb{Z}/p^n)^* \cong \mathbb{Z}/(p-1) \times \mathbb{Z}/p^{n-1}$ einen immer größer werdenden p–Quotienten enthält, dessen zugehöriger Körper in $k_S(\mathfrak{c})$ enthalten ist. [NSW08], chap. VIII, §1, Corollary 18 erlaubt den Schluß. ◊

Im Folgenden sind die Beweise dem Artikel [Neu73a] entlehnt. Die dortigen Aussagen beinhalten jedoch keinerlei arithmetische Information, wie die auf den Nächsten folgenden Sätze.

4.2.6 Satz: *Jede abelsche (nicht notwendig endliche) Erweiterung K/k eines globalen in bezug auf $\mathfrak{c}$ vollständigen Körpers ist $\mathfrak{c}$-potent, insbesondere auch k selbst.*

Beweis. Wenn die Erweiterung K/k potent ist, dann ist sie auch $\mathfrak{c}$–potent. Somit ist dieser Satz eine Folgerung von [NSW08], chap. IX, §5, Proposition 2. ◊

4.2.7 Satz: *Es sei $S(\mathfrak{c}) \subseteq S$ und k ein in bezug auf eine auflösbare Klasse $\mathfrak{c}$ vollständiger globaler Körper. Wenn für die Dirichletdichte δ die Gleichung $\delta(S) = 0$ gilt, dann ist*

$$k_S(\mathfrak{c}) \text{ ein } \mathfrak{c}\text{-potenter Körper.}$$

Beweis. Es sei E eine endliche $\mathfrak{c}$–Gruppe und n ihr Exponent. Da k ein $\mathfrak{c}$–vollständiger Körper ist, gehört die Galoisgruppe von $k(\zeta_n)/k$ der Klasse $\mathfrak{c}$ an. Es sei nun K' eine endliche separable Erweiterung von $k_S(\mathfrak{c})$. Die Erweiterung $k(\zeta_n)/k$ ist in $k_S(\mathfrak{c})/k$ enthalten. Es beschreibe $\overline{K}/k(\zeta_n)$ eine endliche Erweiterung, deren Kompositum mit $k_S(\mathfrak{c})$ den Körper K' ergibt. Tschebotareffs Satz hat das Vorhandensein beliebig vieler sich in $\overline{K}/k(\zeta_n)$ voll zerlegender Stellen, welche nicht über Stellen aus S liegen zur Folge, weil $\delta(S) = 0$ ist. Darüber hinaus ist jede in $k_S(\mathfrak{c})$ über einer solchen Stelle definierte Stelle $\mathfrak{P}$ in K' voll zerlegt. Der Quotient der Trägheitsgruppe $T_{\mathfrak{P}}(\mathfrak{c})$ einer solchen Stelle hat den Quotienten $\mathbb{Z}/n$. Damit ist gezeigt, was zu zeigen war. ◊

4.2.8 Bemerkung: Die Bedingung $\delta(S) = 0$ in obigem Satz könnte durch $\delta(S \cap cs(F/k)) = 0$ ersetzt werden, wenn $F \subseteq k_S(\mathfrak{c})$ gilt und F/k endlich ist.

4.2.9 Theorem: *Es seien $S \subseteq T$ Primstellenmengen eines in bezug auf $\mathfrak{c}$ potenten Zahlkörpers k und es gebe eine Teilerweiterung F/k in $k_S(\mathfrak{c})$ mit $cs(F/k) \underset{\sim}{\subset} T \setminus S$. Dann ist $G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$ zur freien pro-$\mathfrak{c}$-Gruppe $F_\omega(\mathfrak{c})$ von abzählbar unendlichem Rang isomorph, das heißt*

$$F_\omega(\mathfrak{c}) \cong G(k_T(\mathfrak{c})/k_S(\mathfrak{c})).$$

Beweis. Ist E eine endliche $\mathfrak{c}$-Gruppe, so ist zu zeigen, daß das Einbettungsproblem

$$\mathcal{E}(G(k_T(\mathfrak{c})/k_S(\mathfrak{c})), \overline{G}, E)$$

bei beliebigem endlichen Quotienten $\varphi : G(k_T(\mathfrak{c})/k_S(\mathfrak{c})) \twoheadrightarrow \overline{G}$, welches durch das Diagramm

$$\begin{tikzcd}
 & & & G(k_T(\mathfrak{c})/k_S(\mathfrak{c})) \arrow[d, "\varphi"] \arrow[dl, dotted, "\psi"'] & \\
1 \arrow[r] & A \arrow[r] & E \arrow[r, "j"] & \overline{G} \arrow[r] & 1
\end{tikzcd}$$

beschrieben wird, eine eigentliche Lösung hat. O.B.d.A. sei A abelsch und ein einfacher $\overline{G}$–Modul, welcher durch die Primzahl p annulliert werde. Aus $H^2(G(k_T(\mathfrak{c})/k_S(\mathfrak{c})), A) = 0$ (s. 4.1.7) läßt sich eine Lösung

$$\psi : G_{k_S(\mathfrak{c})} \to E \text{ ableiten,}$$

deren Einschränkung auf den Kern von φ entweder ganz A oder 0 zum Bilde hat. Im zweiten Fall sei $k(A)/k_S(\mathfrak{c})$ eine trivialisierende Erweiterung, welche auf endlichem Niveau durch die Erweiterung k_0'/k_0 beschrieben werde, d.h. $k_0 \subseteq k_S(\mathfrak{c})$, $k_0' k_S(\mathfrak{c}) = k(A)$ und $G(k_0'/k_0) \cong G(k(A)/k_S(\mathfrak{c}))$. Da $k_S(\mathfrak{c})$ ein $\mathfrak{c}$–potenter Körper ist, gibt es in $k(A)$ voll zerfallende Stellen aus $T \setminus S(k_S(\mathfrak{c}))$, die mit $\mathfrak{P}_1, ..., \mathfrak{P}_s$ bezeichnet werden möchten und Gruppenhomomorphismen

$$\varphi_i : G(\overline{K}_{\mathfrak{P}_i}(\mathfrak{c})/K_{\mathfrak{P}_i}) \to A,$$

deren Bilder ganz A erzeugen. O.B.d.A. möge die Erweiterung k_0'/k_0 in den Stellen unter den $\mathfrak{P}_i$; $i = 1, ..., s$ voll zerfallen. Im Fall verschiedener Charakteristik $p \neq char(k)$, liefert [NSW08], chap. IX, §2, Theorem 3 (v) -spätestens nach Austausch von k durch F - die Surjektivität der Einschränkung

$$H^1(k_T/k, A) \to \prod_{i=1}^{s} H^1(k_{\mathfrak{P}_i}, A).$$

Im anderen Fall $p = char(k)$ liefert [NSW08], chap. IX, §2, Theorem 5 dieselbe Aussage. Der Grenzübergang über sämtliche endliche Teilerweiterungen liefert den Epimorphismus

$$H^1(K, A) \to \prod_{i=1}^{s} H^1(K_{\mathfrak{P}_i}, A).$$

Aus diesem ergibt sich das Vorhandensein einer Klasse $[x] \in H^1(K, A)$, welche durch res_i auf

$$\varphi_i \in Hom(G(\overline{K}_{\mathfrak{P}_i}(\mathfrak{c})/K_{\mathfrak{P}_i}), A) = H^1(K_{\mathfrak{P}_i}, A)$$

abgebildet wird. Die um x manipulierte Lösung $\psi' := \psi^x \in Hom(G_K, E)$ liefert eine eigentliche Lösung des Einbettungsproblems. ◊

4.2.10 Beispiel: Es sei $\mathfrak{c} = \mathfrak{c}(S)$ mit der Menge $S = \{p_1, ..., p_r\}$ als der Menge der ersten r ungeraden Primzahlen, $n = \prod_{i=1}^{r} p_i$ und n_2 die höchste in $\#(\mathbb{Z}/n)^*$ aufgehende Potenz der 2. Wenn ζ_{n_2} eine primitive $n_2\underline{^{te}}$ Einheitswurzel beschreibt, dann ist $k = \mathbb{Q}(\zeta_{n_2})$ und jede endliche Erweiterung davon sowohl $\mathfrak{c}$-potent als auch in bezug auf $\mathfrak{c}$ vollständig. Ist T eine Stellenmenge der Dirichletdichte 1, dann ist $G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$ eine freie pro-$\mathfrak{c}$-Gruppe vom Rang ω, d.h. der Rang ist abzählbar unendlich.

4.2.11 Theorem: *Wenn $S(\mathfrak{c}) \subseteq S \subseteq T$ gilt und k ein $\mathfrak{c}$−vollständiger Körper ist, dann kann im Fall des Vorhandenseins einer Erweiterung F/k innerhalb $k_S(\mathfrak{c})$ mit $cs(F/k) \subsetneqq T \smallsetminus S$, ein Epimorphismus*

$$\mathop{\ast}_{\mathfrak{p} \in T \smallsetminus S} T_{\mathfrak{p}}(\mathfrak{c}) \longrightarrow G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))$$

abgeleitet werden, dessen Bild frei ist und auf den Abelisierungen zu einem Isomorphismus wird:

$$\left(\mathop{\ast}_{\mathfrak{p} \in T \smallsetminus S} T_{\mathfrak{p}}(\mathfrak{c})\right)^{ab} \xrightarrow{\sim} \left(G(k_T(\mathfrak{c})/k_S(\mathfrak{c}))\right)^{ab}.$$

Beweis. Dies folgt aus den in 4.1 vorangegangenen Ausführungen und 4.2.9. ◊

5 Lokale Galoisgruppen

5.1 Die p–Quotienten der absoluten lokalen Galoisgruppe

Ziel dieses Abschnitts ist es, ein paar bekannte Tatsachen in bezug auf lokale Galoisgruppen zusammenzutragen und drei Konsequenzen daraus zu erörtern.

5.1.1 Definition: *Es sei G eine pro-p-Gruppe und $q = p^n$, dann sei $\{G^i\}_{i\geq 1}$ die absteigende q–Zentralreihe. Für $x, y \in G$ werden die Kommutatoren (x, y) durch $(x, y) := x^{-1}y^{-1}xy$ definiert.*

5.1.2 Bemerkung: Zur Definition dieser Filtrierung s. [NSW08], chap. III, §8, Definition 1.

5.1.3 Satz (Iwasawa)**:** *Die Galoisgruppe G^{tr} der größten zahm verzweigten Erweiterung eines lokalen Körpers k^{tr}/k ist isomorph zur pro-endlichen Gruppe $\mathcal{G}$ mit zwei Erzeugern σ, τ, welche nur durch die Relation*

$$\sigma\tau\sigma^{-1} = \tau^q$$

miteinander in Beziehung stehen. Dabei ist $q = p^n$ die Restklassenkörperordnung von k. Mit anderen Worten:

$$1 \to \hat{\mathbb{Z}}^{(p')} \to G^{tr} \to \hat{\mathbb{Z}} \to 1$$

ist exakt und beschreibt ein semidirektes Produkt.

Beweis. Siehe [Iwa55] oder [NSW08], chap. VII, §5, Theorem 3. ◊

5.1.4 Folgerung: *Ist k ein lokaler Körper und $\mu_l \subseteq k$, dann ist $G_k(l) \cong \mathbb{Z}_l \rtimes \mathbb{Z}_l$, wenn l nicht die Restklassenkörperordnung q von k teilt. Die Gruppe entspricht der durch zwei Elemente σ, τ erzeugten pro-l-Gruppe mit der einzigen Relation*

$$\sigma\tau\sigma^{-1} = \tau^q.$$

Für deren Abelisierung gilt:

$$G_k(l)^{ab} \cong \mathbb{Z}_l \times \mathbb{Z}/l^i, \text{ wobei } l^i \text{ die größte in } q-1 \text{ aufgehende } l-\text{Potenz ist.}$$

5.1.5 Satz (Demuškin)**:** *Wenn k ein p–adischer Zahlkörper vom Grad $N = [k : \mathbb{Q}_p]$ ist, p^s die größtmögliche p–Potenz, deren Einheitswurzeln μ_{p^s} in k enthalten sind, dann gilt für $p^s > 2$, daß $G_k(p)$ die von $N+2$ Elementen erzeugte pro-p-Gruppe ist, welche allein durch die Relation*

$$x_1^{p^s}(x_1, x_2)(x_3, x_4)\cdots(x_{N+1}, x_{N+2}) = \iota$$

in Beziehung zueinander stehen. Dessen Abelisierung ist isomorph zu

$$\mathbb{Z}/p^s \times \prod_{i=1}^{N+1} \mathbb{Z}_p.$$

Beweis. Siehe [Dem61] oder [NSW08], chap. VII, §5, Theorem 12. ◊

5.1.6 Bemerkung: Ist $p^s = 2$, dann muß nach [Lab67] und [Ser64] folgendermaßen unterschieden werden:
Für ungerades $N := [k : \mathbb{Q}_2]$ ist $G_k(p)$ die durch $N + 2$ Erzeuger $x_1, ..., x_{N+2}$ definierte freie Gruppe modulo einer einzigen Relation, welche diese Gestalt hat:

$$\rho = x_1^2 x_2^4 (x_2, x_3) \cdots (x_{N+1}, x_{N+2}).$$

Wenn N jedoch gerade ist, muß der zyklotomische Charakter $\chi : G_k \to \mathbb{Z}_2^\times$ hinzugezogen werden. Selbiger ist durch die Wirkung von G_k auf μ_{2^∞}, resp. dem dadurch gelieferten Homomorphismus $G_k \to Aut(\mu_{2^\infty}) \cong \mathbb{Z}_2^\times$ gegeben. Ist $-1 + 2^f$ $(f \geq 2)$ ein Erzeuger des Bildes von χ, wird $G_k(2)$ als pro-2-Gruppe durch die Erzeuger $x_1, ..., x_{N+2}$ und die Relation

$$\rho = x_1^{2+2^f} (x_1, x_2) \cdots (x_{N+1}, x_{N+2})$$

vollständig beschrieben. Das bedeutet, daß $k \cap \mathbb{Q}_2(\mu_{2^\infty})$ unter dem Automorphismus, welcher von der komplexen Konjugation induziert wird, nicht invariant ist.
Entspricht jedoch $Bild(\chi)$ dem Erzeugnis von -1 und $1 + 2^f$ $(f \geq 2)$, so kann die zu diesen Erzeugern gehörige Relation durch die Gleichung

$$x_2^2 (x_1, x_2) x_3^{2^f} (x_3, x_4) \cdots (x_{N+1}, x_{N+2}) = \iota$$

dargestellt werden. Dieser Fall tritt genau dann auf, wenn $k \cap \mathbb{Q}_2(\mu_{2^\infty}) = \mathbb{Q}_2(\zeta_{2^n} + \zeta_{2^n}^{-1})$ für ein $n \in \mathbb{N}$ ist. Die Abelisierung dieser Gruppen ist in allen drei Fällen isomorph zu

$$\mathbb{Z}/2 \times \prod_{i=1}^{N+1} \mathbb{Z}_2.$$

5.2 Die gruppentheoretische Beschreibung des Cupprodukts

Es sei F die freie pro-p-Gruppe vom Rang n und die exakte Sequenz

$$1 \to R \to F \to G \to 1$$

beschreibe eine minimale Darstellung der Gruppe G. Als Normalteiler $R \lhd F$ werde durch ein Element ρ erzeugt: $R =< \rho >$. Wird die obige Sequenz abelisiert, so wird aus G^{ab} entweder

$$G^{ab} \cong \mathbb{Z}_p^n \text{ oder } G^{ab} \cong \mathbb{Z}/p^f \times \mathbb{Z}_p^{n-1}.$$

Im zweiten Fall sei $q := p^f$ und $k := \mathbb{Z}/q$, ansonsten sei $q := 0$ und $k = \mathbb{Z}_p$.

5.2.1 Satz (Labute)**:** *Durch die exakte Sequenz*

$$1 \to R \to F \to G \to 1$$

sei eine minimale Darstellung einer endlich erzeugten pro-p-Gruppe G gegeben.

1. *Jede Basis $x_1, ..., x_n \in F$ von F definiert in $H^1(F, k) = H^1(G, k)$ eine duale Basis $\chi_1, ..., \chi_n \in H^1(G, k)$ mit $\chi_i(x_j) = \delta_{ij}$.*

2. *Ist ein Element $\rho \in R$ gegeben, so liefert es eine Bilinearform, welche mit dem Cupprodukt definiert wird:*
$$H^1(G,k) \times H^1(G,k) \longrightarrow H^2(G,k) \overset{tr_\rho}{\to} k$$
ist genau dann nicht entartet, wenn die Paarung nach Austausch von k mit $\mathbb{Z}/p\mathbb{Z}$ nicht entartet ist. In diesem Fall ist tr_ρ surjektiv.

3. *Wenn G allein durch eine Relation $\rho \in R$ beschrieben wird und R als Normalteiler von ρ erzeugt wird, dann ist tr_ρ injektiv.*

Beweis. Siehe [Lab67] oder [NSW08], chap. III, §9, Proposition 12. ◊

5.2.2 Satz: *Ist*
$$1 \to R \to F \to G \to 1$$
eine minimale Darstellung einer endlich erzeugten pro-p-Gruppe G und $x_1, ..., x_n \in F$ eine Basis von F sowie $\chi_1, ..., \chi_n$ eine k-Basis von $H^1(G,k)$, dann gilt:

1. *Jedes Element $\rho \in F^2$ hat eine Darstellung*
$$\rho = \prod_{j=1}^{n} x_j^{qa_j} \prod_{1\le k<l\le n} (x_k, x_l)^{a_{kl}} \rho',\ \rho' \in F^3, a_j, a_{kl} \in k.$$
Dabei sind die a_{kl} durch ρ in eindeutiger Weise festgelegt und wenn $q \neq 0$ gilt, dann sind es auch die Koeffizienten a_j.

2. *Wenn $\mathcal{R} = \{\rho_i | i \in I\}$ ein minimales Erzeugendensystem definierender Relationen von G sind und*
$$\rho_i = \prod_{j=1}^{n} x_j^{qa_j^i} \prod_{1\le k<l\le n} (x_k, x_l)^{a_{kl}^i} \rho_i',\ \rho_i' \in F^3, a_j^i, a_{kl}^j \in k,\ i \in I$$
ist, dann wird die Paarung
$$H^1(G,k) \times H^1(G,k) \overset{\cup}{\longrightarrow} H^2(G,k) \overset{tr_{\rho_i}}{\to} k$$
durch die folgende antisymmetrische Matrix $B_i = (b_{kl}^i)$ in bezug auf die Basis $\chi_1, ..., \chi_n$ gegeben:
$$b_{kl}^i = \begin{cases} -a_{kl}^i & wenn \quad k < l \\ -\binom{q}{2} a_k^i & wenn \quad k = l \\ a_{lk}^i & wenn \quad k > l. \end{cases}$$

Beweis. Siehe [NSW08], chap. III, §9, Proposition 13. ◊

5.2.3 Hilfssatz: *Es sei G eine Gruppe und $x, y, z \in G$, dann gilt:*

1. $(x, yz) = (x, z)z^{-1}(x, y)z = (x, z)(x, y)((x, y), z)$

2. $(xy, z) = y^{-1}(x, z)y(y, z) = (x, z)((x, z), y)(y, z)$.

Beweis. siehe [Ser65], chap. II, §1, Proposition 1. ◊

5.3 Explizite Folgerungen

5.3.1 Bemerkung: Es sei $q \equiv 1 \mod p$ und G die durch $< \sigma, \tau | \tau^{q-1}[\tau, \sigma] = \iota >$ definierte pro-p-Gruppe. Wegen 5.2.3 ist $[\tau, \sigma] = (\tau^{-1}, \sigma^{-1}) \equiv (\tau, \sigma) \equiv (\sigma, \tau)^{-1} \mod G^3$. Wenn $q - 1 = m.p^i$ mit $(m, p) = 1$ ist, dann hat die Matrix B aus 5.2.2 diese Gestalt:

$$B \equiv \begin{pmatrix} 0 & 1 \\ -1 & -\binom{p^i}{2}m \end{pmatrix} \mod p^i.$$

p^i ist hierbei die höchste p–Potenz, deren Einheitswurzeln μ_{p^i} gänzlich in k enthalten sind. Ist $p \neq 2$, dann gilt allgemein $\binom{p^i}{2} \equiv 0 \mod p^i$ und für $p = 2$, aber $p^i \neq 2$ gilt: $\binom{p^i}{2} \equiv 0 \mod p$, für $p^i = 2$ ist $\binom{p^i}{2} \equiv 1 \mod 2$.

5.3.2 Bemerkung: Für eine Gruppe wie in 5.1.5 wird die Paarung des Cupprodukts der 1. Kohomologiegruppen mit Koeffizienten in $\mathbb{Z}/p^s$ durch die Matrix

$$B = \begin{pmatrix} -\binom{p^s}{2} & 1 & & & \\ -1 & -\binom{p^s}{2} & \ddots & 0 & \\ & \ddots & \ddots & \ddots & \\ & 0 & \ddots & -\binom{p^s}{2} & 1 \\ & & & -1 & -\binom{p^s}{2} \end{pmatrix}$$

beschrieben. Ist p^s keine Potenz der 2, so gilt $\binom{p^s}{2} \equiv 0 \mod p^s$.

5.3.3 Bemerkung: Dies hat in beiden Bemerkungen zur Folge, daß für zwei Elemente $x, y \in H^1(G, \mathbb{Z}/p^s)$ mit $Kern(x) \subseteq Kern(y)$ das folgende gilt:

$$x \cup y = 0,$$

es sei denn, es ist $p = 2$. Der Grund dafür liegt darin, daß $Hom(G/Kern(x), \mathbb{Z}/p^s)$ ein $\mathbb{Z}/p^s$-Modul vom Rang 1 ist und die Inklusion der Kerne zur Folge hat, daß y ein Vielfaches von x ist. Da die Paarung in diesen Fällen symplektisch ist, folgt das Verschwinden des Cupprodukts. Im zahm verzweigten Fall aus 5.3.1 ist für $p^i \neq 2$ die Matrix nicht-ausgeartet und für festes $x \in H^1(G, \mathbb{Z}/p^s)$ der Ordnung p^s sind die Vielfachen von x der Kern der Abbildung

$$x \cup \_ : H^1(G, \mathbb{Z}/p^s) \to \mathbb{Z}/p^s, y \mapsto x \cup y.$$

Dasselbe gilt für die Reduktion der Paarung modulo p. In diesem Fall kann daher aus $x \cup y$ gefolgert werden, daß die Kerne einander enthalten. Ist $p = 2$, dann gilt $\binom{p^s}{2} \equiv -p^{s-1} \mod p^s$ und für $Kern(x) \subseteq Kern(y)$ gilt $x \cup y \equiv 0 \mod 2$, sobald $s > 1$ ist, d.h. $\zeta_4 = i$ liegt in k.

5.3.4 Bemerkung: Die Gruppen aus 5.1.6 werden von $N + 2$ Elementen erzeugt und sind durch eine Relation ρ vollständig beschrieben. In diesem Fall ist die Matrix B modulo 2 für die Relation

$$\rho = x_1^2 x_2^4 (x_2, x_3) \cdots (x_{N+1}, x_{N+2})$$

durch

$$\begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \ddots & \vdots \\ 0 & 1 & 0 & 1 & 0 \\ \vdots & \ddots & 1 & 0 & 1 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix},$$

für

$$\rho = x_1^{2+2^f}(x_1,x_2)\cdots(x_{N+1},x_{N+2})$$

durch

$$\begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 1 & 0 & 1 & \ddots & \vdots \\ 0 & 1 & 0 & 1 & 0 \\ \vdots & \ddots & 1 & 0 & 1 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

und schließlich für

$$\rho = x_2^2(x_1,x_2)x_3^{2^f}(x_3,x_4)\cdots(x_{N+1},x_{N+2})\ (f \geq 2)$$

durch

$$\begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 1 & \ddots & \vdots \\ 0 & 1 & 0 & 1 & 0 \\ \vdots & \ddots & 1 & 0 & 1 \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix} \text{gegeben.}$$

Keine dieser Matrizen liefert eine entartete Paarung, jedoch ist nicht länger $x^{tr}Bx \equiv 0 \mod 2$ für jeden Vektor $x \in H^1(G,\mathbb{Z}/2)$ gegeben. Definitionsgemäß bilden diese Elemente den Kern K des Diagonalhomomorphismus

$$H^1(G,\mathbb{Z}/2) \to H^2(G,\mathbb{Z}/2), x \mapsto x \cup x.$$

6 Dualität

Unter μ_n resp. μ werden im folgenden die $n^{\underline{ten}}$ resp. alle Einheitswurzeln verstanden. Ist A ein $\mathfrak{G}$-Modul, so wird jede Galoissche Erweiterung K/k eine A ***trivialisierende Erweiterung*** genannt, sobald die zu K gehörige Untergruppe von $\mathfrak{G}$ auf A trivial operiert; in diesem Fall wird A auch als $G(K/k)$-Modul aufgefaßt. Es sei

$$\mathfrak{G}_A := \{\sigma \in \mathfrak{G} | a^\sigma = a \text{ für jedes } a \in A.\}$$

und

$$k(A) := \bigcap_{K/k \text{ trivialisierend}} K$$

die ***durch A erzeugte Erweiterung*** von k, was die exakte Zeile

$$1 \to \mathfrak{G}_A \to \mathfrak{G} \to G(k(A)/k) \to 1 \text{ ergibt.}$$

6.1 Die lokale Lage

Für $\mathfrak{p}$–adische Körper ist durch Tate und Poitou (s. [Tat62] und [Poi67]) dieser Satz bekannt:

6.1.1 Satz (lokaler Dualitätssatz): *Es sei A ein endlicher $\mathfrak{G}_\mathfrak{p}$–Modul und $A' := Hom(A, \mu)$ der dazugehörige duale Modul. Dann gibt es für $0 \leq q \leq 2$ eine kanonische nicht-ausgeartete Paarung endlicher Gruppen*

$$H^q(k_\mathfrak{p}, A') \times H^{2-q}(k_\mathfrak{p}, A) \xrightarrow{\cup} H^2(k_\mathfrak{p}, \overline{k}^*) \overset{inv}{\to} \mathbb{Q}/\mathbb{Z}.$$

Die unverzweigten Anteile sind zueinander orthogonale Komplemente, wobei im Fall $q = 1$ vorausgesetzt werden muß, daß die Restklassenkörpercharakteristik zur Ordnung von A teilerfremd ist.

Beweis. s. [NSW08], chap. VII, §2, Theoreme 6 und 15. ◊

Ist $A = \mathbb{Z}/p$, so ist $A' = \mu_p$ und die Kummersequenz gestattet die Identifizierung der Gruppe $H^1(k_\mathfrak{p}, A')$ mit $k_\mathfrak{p}^*/k_\mathfrak{p}^{*^p}$, wenn die Gruppe μ_p in $k_\mathfrak{p}$ enthalten ist. Die durch das Cupprodukt beschriebene Paarung ist dann durch die Paarung

$$\begin{array}{ccccc} H^1(k_\mathfrak{p}, \mathbb{Z}/p) & \times & H^1(k_\mathfrak{p}, \mu_p) & \longrightarrow & \mu_p \\ & & & & \\ & & (\chi, x) & \longmapsto & \chi(a, K_\mathfrak{p}/k_\mathfrak{p}) \end{array}$$

gegeben, wenn $a \in k_\mathfrak{p}^*$dem Element $x \in H^1(k_\mathfrak{p}, \mu_p)$ via der Kummer-Zuordnung entspricht. $(\ \ , K_\mathfrak{p}/k_\mathfrak{p})$ steht hier für das Normrestsymbol der durch den Charakter $\chi : \mathfrak{G}_\mathfrak{p} \to \mathbb{Z}/p$ definierten Erweiterung $K_\mathfrak{p}/k_\mathfrak{p}$. Befinden sich die $p^{\underline{ten}}$ Einheitswurzeln bereits im Grundkörper $k_\mathfrak{p}$, so kann $\mathbb{Z}/p$ auch als $\mathfrak{G}_\mathfrak{p}$–Modul mit μ_p (nicht-kanonisch) identifiziert werden. Selbiges gilt für die Gruppe $H^1(k_\mathfrak{p}, \mathbb{Z}/p)$, welche nach Festlegung eines Isomorphismus $\mu_p \cong \mathbb{Z}/p$ zu $k_\mathfrak{p}^*/k_\mathfrak{p}^{*^p}$ isomorph ist. Werden somit obige Argumente ersetzt, so entspricht die Paarung der Bilinearform, welche durch das klassische Hilbertsymbol

$$\left(\frac{\ ,\ }{\mathfrak{p}}\right) : k_\mathfrak{p}^*/k_\mathfrak{p}^{*^p} \times k_\mathfrak{p}^*/k_\mathfrak{p}^{*^p} \longrightarrow \mu_p$$

gegeben ist.

6.2 Die globale Lage

Ist k ein endlicher Zahlkörper, $\mathfrak{G}$ dessen absolute Galoisgruppe und $k_{\mathfrak{p}}$ seine Vervollständigung bezüglich der Stelle $\mathfrak{p}$. Zu jeder solchen Primstelle $\mathfrak{p}$ von k kann eine Zerlegungsgruppe $\mathfrak{G}_{\mathfrak{p}} \subseteq \mathfrak{G}$ fixiert werden, was der Wahl einer Bewertungsfortsetzung auf den algebraischen Abschluß gleichkommt.

6.2.1 Definition: *Für eine Stellenmengen T eines Zahlkörpers k und eine Erweiterung L/k bezeichne $Ш^q(L/k, T, A)$ den Kern der Einschränkungsabbildung*

$$res^q(L/k, T, A) : H^q(L/k, A) \to \prod_{\mathfrak{p} \in T} H^q(k_{\mathfrak{p}}, A).$$

*Ist für $T \subseteq S$ die Erweiterung $L = k_S$, so mag diese Gruppe genauso mit $Ш^q(k_S, T, A)$ resp. $Ш^q(S, T, A)$ bezeichnet werden. Sie wird **Tate-Schafarewitsch-Gruppe** genannt und - stimmen S und T überein -, so wird sie im Folgenden durch $Ш^q(S, A)$ abgekürzt.*

Auf Poitou und Tate [Poi67] geht der folgende Satz zurück:

6.2.2 Satz (globaler Dualitätssatz)**:** *Ist A ein endlicher $\mathfrak{G}$–Modul und $A' := Hom(A, \mu)$ der zu A duale Modul, so gilt:*
Die Bilder von $H^q(k, A)$ und $H^{2-q}(k, A')$ sind für $0 \le q \le 2$ unter der Paarung

$$\prod_{\mathfrak{p}} H^q(k_{\mathfrak{p}}, A) \times \prod_{\mathfrak{p}} H^{2-q}(k_{\mathfrak{p}}, A') \to \mathbb{Q}/\mathbb{Z}$$

gegenseitige orthogonale Komplemente, d.h. für $x \in H^q(k, A)$ und $y \in H^{2-q}(k, A')$ gilt

$$\sum_{\mathfrak{p}} inv_{\mathfrak{p}}(res_{\mathfrak{p}}(x) \cup res_{\mathfrak{p}}(y)) = 0.$$

Darüber hinaus sind die Moduln

$$Ш^1(\overline{k}/k, A) \text{ und } Ш^2(\overline{k}/k, A')$$

zueinander dual.

Beweis. s. [Neu73a], §4, Satz 2. ◊

6.3 Pro-$\mathfrak{c}$-Varianten

Es sei $\mathfrak{c}$ eine beliebige Klasse endlicher Gruppen, k ein in bezug auf $\mathfrak{c}$ vollständiger Zahlkörper über $\mathbb{Q}$. S sei eine $S(\mathfrak{c})$ umfassende Primstellenmenge und A eine endliche abelsche $\mathfrak{c}$-Gruppe, welche gleichzeitig einen $G_S(\mathfrak{c})$–Modul darstellt. Die Erweiterung $k(A)/k$ ist eine Galoiserweiterung mit einer Automorphismengruppe aus $\mathfrak{c}$, weil diese Abbildung über $G_S(\mathfrak{c})$ faktorisiert. Da k in bezug auf $\mathfrak{c}$ vollständig ist, ist mit A auch der duale Modul $A' = Hom(A,\mu)$ ein $G_S(\mathfrak{c})$–Modul. Der Übersichtlichkeit wegen sollen an dieser Stelle ein paar Bezeichnungen eingeführt werden:

6.3.1 Definition: *Es sei*

$$\begin{aligned}
S(\mathfrak{c}) &\subseteq S\\
\mathcal{O}_{K,S} &= \{a \in K \mid v_{\mathfrak{P}}(a) \geq 0 \textit{ für sämtliche } \mathfrak{P} \notin S.\}\\
U_{k,S} &= \prod_{\mathfrak{p}\in S}\{1\} \times \prod_{\mathfrak{p}\notin S} U_{\mathfrak{p}}.\\
U_{S,\mathfrak{c}} &= \varinjlim_{K/k\subseteq k_S(\mathfrak{c})/k} U_{K,S}.\\
C_{K,S} &= I_{K,S}/\mathcal{O}^*_{K,S}\\
C_S(K) &= C_K/U_{K,S}\\
C_K^0 &= Kern(C_K \to \mathbb{R}^\times_+, \overline{a} \mapsto \prod_{\mathfrak{p}} |a_{\mathfrak{p}}|_{\mathfrak{p}}).\\
C_S^0(K) &= C_K^0/U_{K,S}.\\
\mathcal{O}_{S,\mathfrak{c}} &= \varinjlim_{K/k\subseteq k_S(\mathfrak{c})/k} \mathcal{O}_{K,S} \textit{ die } S\textit{-Einheiten von } k_S(\mathfrak{c}).\\
I_{S,\mathfrak{c}} &= \varinjlim_{K/k\subseteq k_S(\mathfrak{c})/k} I_{K,S} \textit{ die } S\textit{-Idelgruppe des Körpers } k_S(\mathfrak{c}).\\
C_{S,\mathfrak{c}} &= \varinjlim_{K/k\subseteq k_S(\mathfrak{c})/k} C_{K,S}.\\
C^0_{S,\mathfrak{c}} &= \varinjlim_{K/k\subseteq k_S(\mathfrak{c})/k} C_S^0(K) = C^0(k_S(\mathfrak{c}))/U_{S,\mathfrak{c}}\\
A &\quad \textit{ein endlicher } G_S(\mathfrak{c}) - \textit{Modul, dessen Ordnung}\\
&\quad \textit{nur durch Primzahlen } p \in S(\mathfrak{c}) \textit{ teilbar ist.}\\
I_{S,\mathfrak{c}}(A) &= Hom(A, I_{S,\mathfrak{c}}).\\
C_{S,\mathfrak{c}}(A) &= Hom(A, C_{S,\mathfrak{c}}).\\
C^0_{S,\mathfrak{c}}(A) &= Hom(A, C^0_{S,\mathfrak{c}}).
\end{aligned}$$

6.3.2 Bemerkung: Aus der exakten Sequenz auf endlichem Niveau

$$0 \to C_{K,S} \to C_S(K) \to Cl_S(K) \to 1$$

kann durch Grenzübergang ***nicht*** die Gleichheit von

$$C_{S,\mathfrak{c}} \text{ mit } C_S(k_S(\mathfrak{c})),$$

abgeleitet werden, da der Limes über der S–Idealklassengruppe im Allgemeinen nicht verschwindet - jedoch stimmen des Hauptidealsatzes wegen für $p \in S(\mathfrak{c})$ die p–primären Anteile dieser Gruppen überein. Daher ist $Hom(A, C_{S,\mathfrak{c}}) \cong Hom(A, C_S(k_S(\mathfrak{c})))$ und somit $C_{S,\mathfrak{c}}(A) \cong C_S(k_S(\mathfrak{c}))(A)$.

Es entsteht aus der exakten Sequenz

$$1 \to \mathcal{O}^*_{S,\mathfrak{c}} \to I_{S,\mathfrak{c}} \to C_{S,\mathfrak{c}} \to 1$$

die exakte Sequenz von $G_S(\mathfrak{c})$–Moduln

$$0 \to A' \to I_{S,\mathfrak{c}}(A) \to C_{S,\mathfrak{c}}(A) \to 0.$$

Die Exaktheit ergibt sich, weil $\mathcal{O}^*_{S,\mathfrak{c}}$ für jedes $p \in S(\mathfrak{c})$ p–divisibel ist.

6.3.3 Hilfssatz: *Es sei $K/k \subseteq k_S(\mathfrak{c})/k$ eine endliche galoissche Teilerweiterung, dann gilt*

$$(C_S(k_S(\mathfrak{c})))^{G(k_S(\mathfrak{c})/K)} = C_S(K).$$

Beweis. Klar. ◊

6.3.4 Hilfssatz: *Das Paar $(G_S(\mathfrak{c}), C_S(k_S(\mathfrak{c})))$ ist eine Klassenformation.*

Beweis. Für eine endliche galoissche Erweiterung K/k ist der $G(K/k)$-Modul $U_{K,S}$ kohomologisch trivial, weswegen $H^i(K/k, C_S(K)) = H^i(K/k, C_K)$ gilt. Mit dieser Gleichheit vererben sich die nötigen Eigenschaften von $C = \varinjlim_{K/k} C_K$ auf $C_S(k_S(\mathfrak{c}))$. ◊

6.3.5 Hilfssatz: *Die Sequenz*

$$1 \to N_{k_S(\mathfrak{c})/k} C_S(k_S(\mathfrak{c})) \to C_S(k) \to G_S^{ab}(\mathfrak{c}) \to 1$$

ist exakt und $N_{k_S(\mathfrak{c})/k} C_S(k_S(\mathfrak{c}))$ ist für $p \in S(\mathfrak{c})$ p-divisibel.

Beweis. Die linke Seite kann aus dem Reziprozitätsgesetz auf endlichem Niveau direkt durch Grenzübergang abgeleitet werden. Die Surjektivität ergibt sich aus der Beobachtung, daß die kompakte Untergruppe C_K^0 über dasselbe Bild verfügt, da der Quotient $C_K/C_K^0 \cong \mathbb{R}_+^*$ keinen nichttrivialen endlichen Quotienten hat. Demnach ist das Bild unter dem Normrestsymbol ebenfalls kompakt und dicht in $G_S(\mathfrak{c})^{ab}$, was die Surjektivität der rechten Abbildung liefert. Aus der Sequenz

$$1 \to \Big(\bigcap_{\substack{K/k \subseteq k_S/k \\ \text{galoissch}}} N_{K/k} C_K\Big) U_{k,S}/U_{k,S} \to C_S(k) \to G_S^{ab} \to 1$$

des Theorems 13 aus [NSW08], chap. VIII, §3 ergibt sich durch eine Diagrammjagd in

$$\begin{tikzcd}
 & N_{k_S(\mathfrak{c})/k} C_S(k_S(\mathfrak{c})) \arrow[dr, dotted] & & G(k_S^{ab}/k_S^{ab}(\mathfrak{c})) \arrow[d] & \\
1 \arrow[r] & (N_{\overline{k}/k} C) U_{k,S}/U_{k,S} \arrow[r] & C_S(k) \arrow[r, "(\ \ ,k_S/k)"] \arrow[dr, dotted, "(\ \ ,k_S(\mathfrak{c})/k)"'] & G_S^{ab}(\mathfrak{c}) \arrow[r] \arrow[d, two heads, "\pi"] & 1 \\
 & & & G_S^{ab}(\mathfrak{c}) &
\end{tikzcd}$$

und dem Umstand, daß $G(k_S^{ab}/k_S^{ab}(\mathfrak{c}))$ für $p \in S(\mathfrak{c})$ p-divisibel ist, die Divisibilität der universellen $\mathfrak{c}$–Normgruppe für die primen Größen aus $S(\mathfrak{c})$. ◇

6.3.6 Satz: *Der $G_S(\mathfrak{c})$–Modul $C_S^0(k_S(\mathfrak{c}))$ ist ein level-kompakter Formationsmodul und für $p \in S(\mathfrak{c})$ ist die universelle Normgruppe $N_{k_S(\mathfrak{c})/k}(C_S^0(k_S(\mathfrak{c})))$ eine p-divisible Gruppe.*

Beweis. Mit $U_{K,S}$ für galoissches K/k ist auch $U_S^{\mathfrak{c}}$ kohomologisch trivial, daher ist

$$1 \to U_{K,S} \to C_K^0 \to (C_S^0(k_S(\mathfrak{c})))^{G(k_S(\mathfrak{c})/K)} \to 1$$

exakt und

$$(C_S^0(k_S(\mathfrak{c})))^{G(k_S(\mathfrak{c})/K)} = C_K^0/U_{K,S} = C_S^0(K).$$

Mit C_K^0 ist auch $C_S^0(K)$ kompakt und daher ist $C_S^0(k_S(\mathfrak{c}))$ level-kompakt. Die Divisibilität der Normgruppe von $C_S^0(k_S(\mathfrak{c}))$ ergibt sich aus der Divisibilität derer von $C_S(k_S(\mathfrak{c}))$. ◇

Unter Verwendung dieser Gleichheit und [NSW08], chap. VIII, §4, Proposition 2 kann der sich anschließende Satz aus [NSW08], chap. III, §1, Theorem 11 abgeleitet werden

6.3.7 Satz: *Es gilt für diskrete endliche $G_S(\mathfrak{c})$-Moduln A aus $\mathfrak{c}$, daß die Paarung*

$$\hat{H}^i(G_S(\mathfrak{c}), C_S^0(k_S(\mathfrak{c}))(A)) \times \hat{H}^{2-i}(G_S(\mathfrak{c}), A) \overset{\cup}{\to} H^2(G_S(\mathfrak{c}), C_S^0(k_S(\mathfrak{c}))) \to \frac{1}{\#G_S(\mathfrak{c})}\mathbb{Z}/\mathbb{Z}$$

einen topologischen Isomorphismus

$$\hat{H}^i(G_S(\mathfrak{c}), Hom(A, C_S^0(k_S(\mathfrak{c})))) \cong \hat{H}^{2-i}(G_S(\mathfrak{c}), A)^{\vee} \text{ für } i \leq 0.$$

hervorruft, wenn $p \in S(\mathfrak{c})$ Exponent der Gruppe A ist.

Beweis. In [NSW08], chap. VIII, §4, Theorem 4 darf nach obigem $\hat{H}^0(G_k, C_{\overline{k}}(A))$ durch $\hat{H}^0(G_k(\mathfrak{c}), C_{\mathfrak{c}}(A)))$ ersetzt werden. Darüber hinaus gilt $H^2(G_k(\mathfrak{c}), A) \cong H^2(G_k, A)$ mit Hilfe der Hochschild-Serre-Sequenz. ◇

6.3.8 Definition: *Die Gruppen $P^i(G_S(\mathfrak{c}), A)$ seien gegeben durch*

$$\begin{aligned}
P^0(G_S(\mathfrak{c}), A) &= \prod_{\mathfrak{p} \text{ endl.}} H^0(G_{k_\mathfrak{p}}(\mathfrak{c}), A) \times \prod_{\mathfrak{p}|\infty} \hat{H}^0(G_{k_\mathfrak{p}}(\mathfrak{c}), A)\\
P^1(G_S(\mathfrak{c}), A) &= \prod_{\mathfrak{p}}(H^1(G_{k_\mathfrak{p}}(\mathfrak{c}), A), H^1_{nr}(G_{k_\mathfrak{p}}(\mathfrak{c}), A))\\
P^2(G_S(\mathfrak{c}), A) &= \bigoplus_{\mathfrak{p}} H^2(G_{k_\mathfrak{p}}(\mathfrak{c}), A)\\
P^i(G_S(\mathfrak{c}), A) &= \bigoplus_{\mathfrak{p}|\infty} H^i(G_{k_\mathfrak{p}}(\mathfrak{c}), A)
\end{aligned}$$

6.3.9 Satz: *Ist $S_\infty \cup S(\mathfrak{c}) \subseteq S$ eine nichtleere Stellenmenge eines $\mathfrak{c}$-vollständigen Zahlkörpers k, dann ist für endliche $G_S(k)$–Moduln A, deren Kardinalität nur durch Primzahlen aus $S(\mathfrak{c})$ teilbar ist, diese Sequenz exakt:*

$$\begin{tikzcd}
0 \arrow[r] & H^0(G_S(\mathfrak{c}),A) \arrow[r] & P^0(G_S(\mathfrak{c}),A) \arrow[r] & H^2(G_S(\mathfrak{c}),A')^\vee \arrow[dll, bend left] \\
H^1(G_S(\mathfrak{c}),A')^\vee \arrow[d, bend right] & P^1(G_S(\mathfrak{c}),A) \arrow[l] & H^1(G_S(\mathfrak{c}),A) \arrow[l] & \\
H^2(G_S(\mathfrak{c}),A) \arrow[r] & P^2(G_S(\mathfrak{c}),A) \arrow[r] & H^0(G_S(\mathfrak{c}),A')^\vee \arrow[r] & 0
\end{tikzcd}$$

Beweis. Analog zur langen exakten Sequenz von Poitou-Tate in [NSW08], chap. VIII, §6 oder mit Hilfe der Isomorphien $H^i(G_S(\mathfrak{c}),A) \cong H^i(G_S,A)$. ◊

Genauso wie in [NSW08], chap. VIII, §6, Theorem 7 kann das Folgende gezeigt werden:

6.3.10 Satz: *Es sei k ein $\mathfrak{c}$−vollständiger Körper, A ein endlicher $G_S(\mathfrak{c})$−Modul mit $\#tor(A) \in \mathbb{N}(S)$ und $S(\mathfrak{c}) \cup S_\infty \subseteq S$, dann gilt:*

$$Ш^1(k_S(\mathfrak{c})/k,A') \times Ш^2(k_S(\mathfrak{c})/k,A) \xrightarrow{\cup} H^2(G_S(\mathfrak{c}),C_S(k_S(\mathfrak{c}))) \to \mathbb{Q}/\mathbb{Z}$$

ist eine perfekte Paarung.

6.3.11 Bemerkung: Ihre zentrale Bedeutung für die Bestimmung der Lösungen globaler Einbettungsprobleme bekommen diese Dualitätssätze durch die exakte Sequenz aus 7.1.4. Aus ihr ergeben sich dann mittels 3.2.2 Möglichkeiten der Steuerung gefundener globaler Lösungen hin zu anderen, welche gegebene lokale Eigenschaften hat.

7 Zur Tate-Schafarewitsch-Gruppe

7.1 Vorbemerkungen

7.1.1 Definition: *Es seien S, T Primstellenmengen eines Zahlkörpers k. Dann bedeute*

$$S \underset{\sim}{\subseteq} T, \text{ daß } \delta(S \smallsetminus T) = 0 \text{ sei.}$$

Aus [NSW08] ist dieser Satz entnommen:

7.1.2 Satz: *Ist die von einem einfachen G_k–Modul A erzeugte Erweiterung $k(A)$ auflösbar, dann gilt*

$$H^i(G(k(A)/k), A) = 0 \text{ für alle } i \geq 1.$$

Beweis. s. [NSW08], chap. IX, §1, Proposition 14. $\diamond$

7.1.3 Definition: *Der Kokern der Einschränkungsabbildung*

$$H^1(k_S/k, A) \longrightarrow \prod_T H^1(k_{\mathfrak{P}}, A)$$

bei endlicher Stellenmenge T, welche in einer weiteren S enthalten sei, wird allgemein mit $\boldsymbol{Kokern^1(S, T, A)}$ *bezeichnet.*

Darüber hinaus gilt nach [NSW08], chap. IX, §2, Lemma 2:

7.1.4 Satz: *Eine nicht-leere Primstellenmenge S, welche im Zahlkörperfall die unendlichen Stellen mit beinhalte, sei mitsamt einer endlichen Teilmenge T gegeben. Ist A ein endlicher $G_S(k)$–Modul, für den $\#A \in \mathbb{N}(S)$ gilt, dann ist die Sequenz*

$$0 \to Ш^1(k_S, A') \to Ш^1(k_S, S \smallsetminus T, A') \to Kokern(S, T, A)^\vee \to 0$$

eine exakte.

Beweis. Dies ist die unmittelbare Folge des aus den Dualitätssätzen hervorgehenden exakten Diagramms

$$\begin{tikzcd}
 & & 0 & \\
\text{Ш}^1(k_S/k, S \setminus T, A') \arrow[r, hook] & H^1(k_S/k, A') \arrow[r] & \prod_{S \setminus T} H^1(k_{\mathfrak{P}}, A') \arrow[u] & \\
\text{Ш}^1(k_S/k, S, A') \arrow[u, hook] \arrow[r, hook] & H^1(k_S/k, A') \arrow[u, equal] \arrow[r] & \prod_S H^1(k_{\mathfrak{P}}, A') \arrow[u] \arrow[r] & H^1(k_S/k, A)^\vee \\
 & & \prod_T H^1(k_{\mathfrak{P}}, A') \arrow[u] \arrow[r, "\sim"] & \prod_T H^1(k_{\mathfrak{P}}, A)^\vee \arrow[u] \\
 & & 0 \arrow[u] & Kokern^1(S, T, A)^\vee \arrow[u] \\
 & & & 0, \arrow[u]
\end{tikzcd}$$

dessen Isomorphimus in der vierten Zeile die komponentenweise Anwendung des lokalen Dualitätssatzes ist. ◇

7.1.5 Satz: *Es sei k ein globaler Körper, $T \subseteq S$ Primstellenmengen aus k, wobei T endlich gewählt sein möge und $S_\infty \subseteq S$ gelte, sobald k ein Zahlkörper ist. Ist A ein endlicher $G_S(k)$–Modul mit $\#A \in \mathbb{N}(S)$, dann ist der kanonischer Homomorphismus*

$$res^1(S, T, A) : H^1(k_S/k, A) \longrightarrow \bigoplus_{\mathfrak{p} \in T} H^1(k_{\mathfrak{P}}, A)$$

in den folgenden Fällen surjektiv.

1. *A' ist ein trivialer $G_S(k)$–Modul und $\delta_k(S) > \frac{1}{p}$, wobei p der kleinste Primteiler der Ordnung von A sei.*

2. *$A = \mathbb{Z}/m$ mit $m = \prod_{i=1,\dots,n} p_i^{r_i}$ mit paarweise verschiedenen Primzahlen $p_1, \dots, p_n$ aus $\mathbb{N}(S)$ und*
$$\delta_k(cs(k(\mu_{p_i^{r_i}})/k) \cap S) > \frac{1}{p_i[k(\mu_{p_i^{r_i}}) : k]}$$
für $i = 1, \dots, n$ - es sei denn, es liegt der Wangsche Sonderfall mit den Parametern $(k, m, S \setminus T)$ vor. Ist dieser gegeben, so hat der Kokern die Ordnung höchstens 2.

3. *$cs(k(A')/k) \mathrel{\substack{\subset\\\sim}} S$ und $\#G(k(A')/k) = kgV\{\#G(k(A')_{\mathfrak{P}}/k_{\mathfrak{P}}) | \mathfrak{p} \in S \setminus T\}$.*

4. *A ist einfach, $G(k(A')/k)$ auflösbar und $cs(k(A')/k) \mathrel{\substack{\subset\\\sim}} S$.*

5. *A ist einfach, $G(k(A)/k)$ auflösbar und $cs(k(A)/k) \mathrel{\substack{\subset\\\sim}} S$.*

6. *A ist einfach, $pA = 0$ für eine Primzahl $p \in \mathbb{N}(S)$ und es gibt endliche Galoiserweiterungen $K \subseteq \Omega$ innerhalb k_S, so daß $p \nmid [\Omega : K]$,*

$$\mu_p \notin K \text{ und } k(A) \subseteq K$$
$$\mu_p \subseteq \Omega \text{ und } cs(\Omega/k) \stackrel{\subset}{\sim} S.$$

Beweis. s. [NSW08], chap. IX, §2, Theorem 3. ◊

7.1.6 Satz: *Es sei $\mu_p \subseteq k$, (und wenn $p = 2$ gilt, auch $\mu_4 \subseteq k$) und K/k eine elementar-abelsche Erweiterung vom Grad p^2. Darüber hinaus sei $\mathfrak{p}$ eine Stelle aus k, welche nicht über p liegt. Ist die Erweiterung in allen Stellen aus $\mathcal{P}_k \setminus \{\mathfrak{p}\}$ zyklisch, dann auch in $\mathfrak{p}$ selbst.*

Beweis. Es sei K das Kompositum der $\mathbb{Z}/p$–Erweiterungen K' und K'', welche duch $x', x'' \in H^1(k, \mathbb{Z}/p)$ beschrieben werden. Der globale Dualitätssatz 6.2.2 besagt, daß

$$\sum_{\mathfrak{p}} inv_{\mathfrak{p}}(res_{\mathfrak{p}}(x') \cup res_{\mathfrak{p}}(x'')) = 0$$

gilt. Darüber hinaus ist für $\mathfrak{q} \in \mathcal{P}_k \setminus \{\mathfrak{p}\}$

$$res_{\mathfrak{q}}(x') \cup res_{\mathfrak{q}}(x'') = 0$$

nach der Bemerkung 5.3.3. Weil die Invariantenabbildung ein Isomorphismus ist, folgt

$$res_{\mathfrak{p}}(x') \cup res_{\mathfrak{p}}(x'') = 0$$

und daraus, daß der Kern des einen lokalen Elements im Kern des anderen enthalten ist, da die Paarung des Cupprodukts im zahm verzweigten Fall nicht ausgeartet ist. ◊

Dies ist im Wesentlichen eine Umformulierung der Geschlossenheitsrelation der globalen Hilbertsymbole. Desgleichen verhält es sich mit dem folgenden Satz.

7.1.7 Satz: *Sei k ein endlicher Zahlkörper mit $\mu(k)(2) = \mu_2$ und K/k eine V_4-Erweiterung und $\mathfrak{p} \nmid (2)$ eine Primstelle. Ist jede Zerlegungsgruppe für Stellen aus $\mathcal{P} \setminus \{\mathfrak{p}\}$ zyklisch und gilt für die Stellen $\mathfrak{q} \mid 2$, daß $K_{\mathfrak{q}}/k_{\mathfrak{q}}$ Teilkörper einer zyklischen Erweiterung vom Grad 4 über $k_{\mathfrak{q}}$ ist, dann ist die Zerlegungsgruppe von $\mathfrak{p}$ ebenfalls zyklisch.*

Beweis. K sei das Kompositum zweier quadratischer Erweiterungen K_i/k $(i = 1, 2)$. Es definiere $x_i \in H^1(G_k, \mathbb{Z}/2)$ für $i = 1, 2$ den Körper K_i. Für $\mathfrak{q} \mid 2$ gilt, daß jedes Paar $res_{\mathfrak{q}}(x_i) \in Hom(G_{k_{\mathfrak{q}}}, \mathbb{Z}/2)$ $(i = 1, 2)$ sich im Cupprodukt auslöscht, d.h. $res_{\mathfrak{q}}(x_1) \cup res_{\mathfrak{q}}(x_2) = 0$, wie man anhand der Matrices aus 5.3.4 erkennen kann. Restliches verläuft analog zum vorangegangenen Satz. ◊

7.2 Das Verschwinden von Ш^1 und Ш^2

Die exakte Zeile aus 7.1.4 erlaubt es, das Bild der Einschränkung

$$H^1(k_S/k, A) \to \prod_T H^1(k_{\mathfrak{p}}, A)$$

als Lösung eines homogenen „Gleichungssystems“ zu verstehen:

7.2.1 Bemerkung: Die Menge $\{\overline{x}_1, \overline{x}_2, ..., \overline{x}_n\}$ beschreibe ein Erzeugendensystem des Kokerns $Kokern^1(S, T, A)$. Dann ist für $y = (y_\mathfrak{p})_{\mathfrak{p}\in T} \in \prod_T H^1(k_\mathfrak{p}, A)$ die Bedingung

$$\sum_{\mathfrak{p}\in T} inv_\mathfrak{p}\left(res_\mathfrak{p}(\overline{x_i}) \cup y_\mathfrak{p}\right) = 0 \text{ für } i = 1, ..., n$$

sowohl notwendig als auch hinreichend dafür, daß das Element y in $H^1(k_S/k, A)$ über ein Urbild x verfügt. Jedes Element x aus $Ш^1(k_S/k, S \setminus T, A)$ wird nämlich in dem Diagramm aus dem Beweis zu 7.1.4 durch die dort aufgeführten Homomorphismen auf das Element

$$\prod_{\mathfrak{p}\in T} res_\mathfrak{p}(x) \in \prod_{\mathfrak{p}\in T} H^1(k_\mathfrak{p}, A')$$

abgebildet, was durch den lokalen Dualitätssatz als ein Element

$$(\prod_{\mathfrak{p}\in T} res_\mathfrak{p}(x) \cup \_) : \prod_{\mathfrak{p}\in T} H^1(k_\mathfrak{p}, A) \to \mathbb{Q}/\mathbb{Z}; (y_\mathfrak{p})_{\mathfrak{p}\in T} \mapsto \sum_{\mathfrak{p}\in T} inv_\mathfrak{p}(res_\mathfrak{p}(x) \cup y_\mathfrak{p})$$

in

$$\left(\prod_{\mathfrak{p}\in T} H^1(k_\mathfrak{p}, A)\right)^\vee$$

verstanden wird. Das orthogonale Komplement des Bilds besteht nach 6.2.2 gerade aus den Elementen $\{\overline{x}_1, \overline{x}_2, ..., \overline{x}_n\}$, die nach 7.1.4 in der Tate-Schafarewitsch-Gruppe $Ш^1(k_S/k, S \setminus T, A)$ ein globales Urbild haben. Diese Beobachtung ist im Wesentlichen eine Umformulierung des Satzes 4 aus [Neu73a], §8.

Eine Anhebung eines solchen Erzeugendensystems im Fall $pA = 0$ läßt sich zu einer Basis des $\mathbb{Z}/p$–Vektorraums $Ш^1(k_S, S \setminus T, A')$ ergänzen. Vor der Verwertung dieser Tatsachen seien diese Annahmen für den Rest dieses Abschnitts stets gültig.

7.2.2 Generalvoraussetzung: Für den Rest dieses Abschnitts mögen diese Generalvoraussetzungen zutreffen:

k	sei ein globaler Körper.
S	sei eine Primstellenmenge von k.
Ω/k	sei eine endliche auflösbare Erweiterung mit $cs(\Omega/k) \stackrel{\subset}{\sim} S$.
A	sei ein endlicher $G_S(k)$ – Modul, welcher durch die Primzahl $p \in \mathbb{N}(S)$ annulliert werde. und die Erweiterung $k(A)/k$ in Ω/k erzeuge.
T	sei eine Teilmenge von S.

7.2.3 Satz: *Es sei* $cs(\Omega/k) \stackrel{\subset}{\sim} T$ *und* $cs(\Omega/k) \subseteq S$, *dann ist*

$$Ш^1(k_S, T, A) = 0,$$

wenn es für jede Teilerweiterung $k(A) \subseteq K$ *vom Grad* p *in* Ω *ein Element* $\mathfrak{p} \in T \smallsetminus cs(K/k(A))$ *gibt und eine der beiden Bedingungen erfüllt ist:*

1. $k = k(A)$.
2. *A ist ein einfacher Modul vom Exponenten p.*

Beweis. In dem Diagramm

$$\begin{tikzcd}
H^1(k_S/\Omega, A) \arrow[r, hook] & \bigoplus_T H^1(\Omega_{\mathfrak{P}}, A) \\
H^1(k_S/k, A) \arrow[u] \arrow[r] & \bigoplus_T H^1(k_{\mathfrak{P}}, A) \arrow[u] \\
H^1(\Omega/k, A) \arrow[u] \arrow[r] & \bigoplus_T H^1(\Omega_{\mathfrak{P}}/k_{\mathfrak{P}}, A) \arrow[u]
\end{tikzcd}$$

ist in beiden Fällen die untere horizontale Abbildung injektiv. Im ersten direkt, im zweiten aufgrund des Umstands, daß nach 7.1.2 in beiden Fällen $H^1(k(A)/k, A) = 0$ gilt. Die obere horizontale Abbildung ist es ebenso, wegen $cs(\Omega/k) \stackrel{\subset}{\sim} S$ und des 1. Punkts aus Satz 7.1.5. Der Schluß erfolgt dann über die Hochschild-Serre Sequenz. ◇

Aus 7.1.4 kann dieses Ergebnis gewonnen werden:

7.2.4 Folgerung: *Unter den Bedingungen wie in 7.2.3 mit endlicher Menge* $S \smallsetminus T$ *ist die Abbildung*

$$res^1(S, T, A) : H^1(k_S/k, A') \to \bigoplus_{S \smallsetminus T} H^1(k_{\mathfrak{P}}, A')$$

surjektiv.

7.2.5 Hilfssatz: *Es sei G eine Gruppe und A ein einfacher G–Modul, welcher von einer Primzahl p annulliert werde. Dann gilt:*
Ist A einfacher G–Modul, so auch $Hom(A, \mathbb{Z}/p)$. *Insbesondere ist* $G_A = G_{Hom(A,\mathbb{Z}/p)}$.

Beweis. Wäre $H \triangleleft Hom(A, \mathbb{Z}/p)$ ein echter Untermodul, dann gäbe es nach Dualisierung dieser Inklusion einen G–Epimorphismus $Hom(Hom(A, \mathbb{Z}/p), \mathbb{Z}/p) \twoheadrightarrow Hom(H, \mathbb{Z}/p)$ mit nichttrivialem Kern, was der kanonischen Isomorphie zum Doppeldual

$$Hom(Hom(A, \mathbb{Z}/p), \mathbb{Z}/p) \cong A$$

widerspräche. Der Rest ist klar. ◊

7.2.6 Satz: *Ist A ein einfacher $G(k_S/k)$–Modul und $S = cs(\Omega/k) \cup T$ für eine endliche Stellenmenge T, dann ist*

$$Ш^1(k_S/k, S \smallsetminus T, A) = 0,$$

wenn $k(A) \subseteq \Omega$ gilt und es keine Galoiserweiterung $k(A) \subseteq K \subseteq \Omega$ gibt, deren Galoisgruppe $G(K/k(A))$ zu A als $G(k(A)/k)$–Modul isomorph ist.

Beweis. Ein $x \neq 0$ aus $Ш^1(k_S/k, S \smallsetminus T, A)$ wird unter der Einbettung

$$H^1(k, A) \to H^1(k(A), A)$$

auf ein Element $\tilde{x} := res_k^{k(A)}(x) \neq 0$ aus $H^1(k(A), A)^{G(k(A)/k)}$ abgebildet. Das Bild von $\tilde{x}$ ist wegen

$$\sigma(\tilde{x}(g)) = \sigma(\tilde{x}(\sigma^{-1}\sigma(g))) = (\sigma\tilde{x})(\sigma g) = \tilde{x}(\sigma g) \text{ für } g \in G_{k(A)} \text{ und } \sigma \in G(k(A)/k)$$

ein $G(k(A)/k)$–Untermodul von A und definiert somit wegen der Einfachheit von A eine Teilerweiterung $K/k(A)$ innerhalb $\Omega/k(A)$ mit Galoisgruppe $G(K/k) \cong A$, die es nicht gibt. ◊

7.2.7 Satz: *Umfaßt die Menge S die unendlichen Stellen S_∞ und S_p und ist A ein einfacher $G_S(k)$–Modul, dann ist der kanonische Homomorphismus*

$$H^2(k_S/k, A') \longrightarrow \bigoplus_S H^2(k_{\mathfrak{P}}, A')$$

ein Monomorphismus, wenn es eine auflösbare Erweiterung $\Omega/k(A)/k$ gibt, so daß für die Menge $cs(\Omega/k) \subseteq S$ gilt und es zu jeder Teilerweiterung $K/k(A)$ vom Grad p über $k(A)$ eine Stelle $\mathfrak{p}$ aus $S \smallsetminus cs(K/k(A))$ gibt.

Beweis. Poitou-Tate-Dualität, [NSW08], chap. IX, §2, Lemma 2 und 7.2.3. ◊

8 Stark nicht-abelsche Gruppen

8.1 Der Begriff einer stark nicht-abelschen Gruppe

Zu einer endlichen auflösbaren Gruppe G gibt es stets eine Normalreihe

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{\iota\}$$

mit abelschen Quotienten $A_i := G_i/G_{i+1}$, welche gleichzeitig einfache von einer Primzahl p_i annullierte G/G_i-Moduln sind.

8.1.1 Definition: *Eine endliche auflösbare Gruppe G mit einer Normalreihe wie oben heißt* ***stark nicht-abelsch****, wenn diese Zerlegung in Normalteiler*

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{\iota\}$$

diese Eigenschaften besitzt:

1. *Für $i > 1$ ist der größte Normalteiler $N_i \lhd G/G_i$, welcher auf A_i trivial wirkt, ein echter Normalteiler, das heißt $N_i \neq G/G_i$.*
2. *Es gibt für kein $i > 1$ einen Epimorphismus $N_i \to A_i$.*
3. *Ist A_i nicht zyklisch, dann ist $G \cong G_{i+1} \rtimes G/G_{i+1}$.*

8.1.2 Beispiel: Es sei eine Primzahl q gegeben und dazu eine streng monoton steigende Folge von Primzahlen $p_1, ..., p_n$ mit n Gliedern, für die stets $p_i \equiv 1 \mod q$ gilt. Dann können nichttriviale Homomorphismen $\varphi_i : \mathbb{Z}/q \to Aut(\mathbb{Z}/p_i)$ gefunden werden. Mit diesen läßt sich das iterierte semidirekte Produkt

$$\mathbb{Z}/p_n \rtimes_{\varphi_n} (\mathbb{Z}/p_{n-1} \rtimes_{\varphi_{n-1}} \cdots \rtimes_{\varphi_2} (\mathbb{Z}/p_1 \rtimes_{\varphi_1} \mathbb{Z}/q))$$

definieren, wobei die φ_i der Kürze wegen für $\varphi_i \circ \pi$ stehen. Dabei ist π die Projektion auf den Quotienten $\mathbb{Z}/q$. Dies ist selbstverständlich eine stark nicht-abelsche Gruppe, da die Kardinalität der Subnormalquotienten monoton wächst.

8.1.3 Bemerkung: Ist $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = \{\iota\}$ eine stark nicht-abelsche Gruppe, so ist es auch G/G_i für $i \leq n$. Ansonsten beschreibt die Bezeichnung „stark nicht-abelsch“ einen alles andere als gutartigen Katalog technischer Eigenschaften. Beispielsweise ist sie nicht abgeschlossen hinsichtlich von Gruppenerweiterungen und dem Übergang auf Untergruppen. Der Begriff schuldet seine Daseinsberechtigung allein der Tatsache, daß eine Reihe bekannter auflösbarer Gruppen geringer Kardinalität von ihm abgedeckt wird.

8.2 Stark nicht-abelsche Gruppen über endlichen Zahlkörpern

8.2.1 Theorem: *Ist k ein Zahlkörper und G eine stark nicht-abelsche Gruppe vom Exponenten m mit einer Filtrierung $\{G_i\}_{i\leq n}$ wie in 8.1.1 und endlich vielen lokalen Vorgaben $\{\psi_{\mathfrak{P}} : G_{k_{\mathfrak{P}}} \to G \mid \mathfrak{p} \in T\}$, dann gibt es eine Galoiserweiterung K/k mit $G(K/k) \cong G$, welche die lokalen Vorgaben verwirklicht, sobald die folgende Bedingung erfüllt ist:*

> *Es sei $\underline{S} := cs(k(\mu_m)/k) \cup T$, dann ist $A_0 = G/G_1$ innerhalb von k_S mit den Vorgaben $\overline{\psi_{\mathfrak{P}}} : G_{k_{\mathfrak{P}}} \to A_0$ realisierbar.*

Der Beweis wird nachgeliefert.

8.2.2 Folgerung: *Ist $\mu_m \subset k$, dann ist die Bedingung mit Hilfe des Satzes von Grunwald und Wang leer.*

8.2.3 Satz: *Ist A der Kern eines Epimorphismus $f : G \to \Gamma = G(K/k)$ mit auflösbarem Bild, welcher gleichzeitig ein von p annullierter einfacher $\Gamma-$Modul sei, dann gilt*

$$\mathcal{L}_{\mathcal{E}(G_k,\Gamma,G)} \neq \varnothing \Leftrightarrow \prod_{\mathfrak{p}} \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}},\Gamma_\mathfrak{p},G_\mathfrak{p})} \neq \varnothing.$$

Beweis. Ausgangspunkt des Beweises ist das folgende Diagramm.

$$\begin{tikzcd} H^2(G_k, A) \arrow[rr] & & \bigoplus_\mathfrak{p} H^2(G_{k_\mathfrak{p}}, A) \\ & H^2(\Gamma, A) \arrow[ul, "\varphi^*"] \arrow[ur, "(\varphi_\mathfrak{p}^*)_\mathfrak{p}"'] & \end{tikzcd}$$

Die horizontale Abbildung ist nach [NSW08], chap. IX, § 1, Corollary 16 (i) injektiv. Es sei $x \in H^2(\Gamma, A)$ die zur Gruppenerweiterung $1 \to A \to G \to \Gamma \to 1$ gehörige Klasse. Nach [NSW08], chap. III, §5, Proposition 9 bzw. 3.1.2 gilt nun:

$$\begin{aligned} \mathcal{L}_{\mathcal{E}(G_k,\Gamma,G)} \neq \varnothing &\Leftrightarrow \varphi^*(x) = 0 \\ &\Leftrightarrow \varphi_\mathfrak{p}^*(x) = 0 \text{ für sämtliche } \mathfrak{p} \\ &\Leftrightarrow \prod_{\mathfrak{p}} \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}},\Gamma_\mathfrak{p},G_\mathfrak{p})} \neq \varnothing. \end{aligned}$$

◊

In der Absicht 8.2.1 zu beweisen, muß ein Satz entwickelt werden, der garantiert, daß die Methode des sukzessiven Aufstiegs, d.h. der schrittweisen Verwirklichung der abelschen Subquotienten einer stark nicht-abelschen Gruppe gelingt. Dies gewährleistet der nun folgende Satz. Alles in Allem orientiert sich die Vorgehensweise stark an Neukirchs Arbeiten über nilpotente resp. auflösbare Gruppen aus [Neu73a] und [Neu79].

8.2.4 Satz: *Durch $\pi : E \twoheadrightarrow G$ werde ein Epimorphismus auflösbarer Gruppen gegeben, dessen Bild G die Erweiterung einer Galoisgruppe Γ einer endlichen Erweiterung K/k globaler Zahlkörper um einen einfachen, durch die Primzahl p annullierten Γ-Modul A sei. Für diesen Modul möge gelten:*

1. *Der größte Normalteiler $N \lhd \Gamma$, welcher auf A trivial wirkt, sei von Γ verschieden.*
2. *Es gebe keinen Epimorphismus $N \twoheadrightarrow A$.*
3. *Wenn A nicht zyklisch ist, so sei $E \cong Kern(\pi) \rtimes G$.*

Dazu sei T eine beliebige endliche Primstellenmenge des globalen Körpers k und

$$(\#E, \#\mu(k)) = (\#E, \#\mu(K)).$$

Wenn

$$\prod_{\mathfrak{p}} \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}},\Gamma_\mathfrak{p},G_\mathfrak{p})} \neq \varnothing \textit{ gilt,}$$

dann gibt es ein surjektives Element $[\psi] \in \mathcal{L}_{\mathcal{E}(G_k,\Gamma,G)}$, welches diese Eigenschaften hat:

1. $[\psi]$ *verwirklicht gegebene Elemente* $[\psi_{\mathfrak{p}}] \in \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}},\Gamma_\mathfrak{p},G_\mathfrak{p})}$ *für* $\mathfrak{p} \in T$.

2. *Ist* $\mathfrak{p} \notin T$ *in* K/k *unverzweigt, dann ist* $\mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}},G_\mathfrak{p},E_\mathfrak{p})} \neq \varnothing$.

3. *Für den durch* $G_k \to G$ *definierten Körper* N *gilt* $(\#E, \#\mu(K)) = (\#E, \#\mu(N))$.

Beweis. Ist μ_p nicht in k enthalten, dann ist dies ein Satz von Neukirch und wird im Main Lemma aus [NSW08], chap. IX, §5 gefunden. Ansonsten ist folgendermaßen zu verfahren: Zunächst ist festzuhalten: Wird T um endlich viele Stellen zu T' vergrößert, so ist die Aussage gezeigt, wenn sie für T' gezeigt wird. Dies ist offensichtlich, weil für unverzweigtes $\mathfrak{p} \in T' \setminus T$ eine unverzweigte Vorgabe $[\psi_\mathfrak{p}]$ definiert werden kann, die sich der Freiheit von $\widehat{\mathbb{Z}}$ wegen zu einem Homomorphismus nach E anheben läßt. Daher kann o.B.d.A. angenommen werden, daß die Menge T die Menge

$$Ram(K/k) \cup S_p \cup S_\infty \text{ beinhaltet.}$$

Darüber hinaus ist es erlaubt, davon auszugehen, daß die Bilder der lokalen Vorgaben $[\psi_\mathfrak{p}]$ ganz G erzeugen: für in K/k voll zerlegte Stellen $\mathfrak{p}$ kann der unverzweigte Quotient

$$G_{k_\mathfrak{p}}/T_{k_\mathfrak{p}} \twoheadrightarrow < a >,\ a \in A$$

epimorph auf eine beliebige zyklische Gruppe $< a > \subseteq A$ abgebildet werden und dieser Homomorphismus kann zu den lokalen Vorgaben aus T hinzugenommen werden.
Als nächstes ist zu bemerken, daß die Erfüllung der letzten Bedingung durch geeignete Wahl von Vorgaben $\mathfrak{p} \in T$ bei abermaliger Vergrößerung der Menge T gewährleistet werden kann. Es sei $m := \#E$. Dazu können in K/k voll zerlegte Stellen $\mathfrak{q}_i$, $i = 1, ..., s$ gewählt werden, deren Frobeniuselemente die Gruppe $G(K(\zeta_m)/K)$ erzeugen mit den zugehörigen trivialen Homomorphismen

$$\psi_{\mathfrak{q}_i} : G_{k_{\mathfrak{q}_i}} \to \{\iota\} \subseteq G,$$

welche lokale Klassen in

$$\mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}},\Gamma_\mathfrak{p},G_\mathfrak{p})} \text{ definieren.}$$

Diese sind zu den Vorgaben aus T hinzuzunehmen. Nach 8.2.3 gibt es ein $[\psi_0] \in \mathcal{L}_{\mathcal{E}(G_k,\Gamma,G)}$, weil A nach Definition ein einfacher Modul ist. Es seien

$$[\psi_{1,\mathfrak{p}}] \in \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}},\Gamma_\mathfrak{p},G_\mathfrak{p})}$$

die lokalen Vorgaben aus T und $\mathfrak{p}_1, ..., \mathfrak{p}_r$ die Stellen außerhalb von T, in denen ψ_0 verzweigt. Letztere verzweigen wegen $Ram(K/k) \subseteq T$ nicht in K/k und können somit auch zu einem unverzweigten $\psi_{1,\mathfrak{p}_i} : G_{k_{\mathfrak{p}_i}} \to G$ angehoben werden. Ist $T^* := T \cup \{\mathfrak{p}_1, ..., \mathfrak{p}_r\}$, so kann nach 3.2.2 für jedwedes $\mathfrak{p} \in T^*$ ein $y_\mathfrak{p} \in H^1(k_\mathfrak{p}, A)$ mit

$$[\psi_{1,\mathfrak{p}}] = [\psi_{0,\mathfrak{p}}]^{y_\mathfrak{p}} \text{ gefunden werden.}$$

N_0/K sei die durch ψ_0 definierte abelsche Erweiterung von K; es läßt sich nun ein Element $x \in H^1(k_S/k, A)$ mit

$$S = cs(K(\zeta_{p^{v_p(m)}})/K) \cup T^* \text{ finden,}$$

welches die obigen $y_\mathfrak{p}$ für $\mathfrak{p} \in T^*$ verwirklicht, d.h. $res_\mathfrak{p}(x) = y_\mathfrak{p}$. Dies kann gefolgert werden, da die Voraussetzungen von 7.2.6 erfüllt sind: Die Erweiterungen

$$\begin{tikzcd}
k(A)(\zeta_{p^{v_p(m)}}) \arrow[dr, dash] & & K \arrow[dl, dash] \\
& \mu_p \subseteq k(A) &
\end{tikzcd}$$

sind über $k(A)$ sind linear disjunkt. In K/k gibt es keine Teilerweiterung über $k(A)$ mit Galoisgruppe A, da G stark nicht-abelsch ist. Gäbe es eine Erweiterung

$$L/k(A) \text{ in } K(\zeta_{p^{v_p(m)}})/k(A)$$

mit zu A isomorpher Galoisgruppe, dann würde $\mu(L)(p) \neq \mu(k(A))(p)$ gelten und da die Erweiterung $k(A)(\zeta_{p^l})/k$ galoissch ist, wäre $L = k(A)(\zeta_{p^l})$ für ein geeignetes l die Erweiterung vom Grad p im Körper aller $p^{\underline{ten}}$ Einheitswurzeln. $G(k(A)/k)$ wirkte dann jedoch auf $G(L/k(A))$ trivial, was einen Widerspruch liefert. Aus diesem Grund gilt nach 7.2.6, daß $Ш^1(k_S, S \setminus T^*, A') = 0$ ist. Ein solches x manipuliert ψ_0 demnach so, daß $[\psi_0]^x$ den obigen Anforderungen genüge trägt:
Es verwirklicht nach Wahl von x die lokalen Vorgaben in $\mathfrak{p} \in T^*$.
Ist $\mathfrak{p} \in T^* \setminus T$, dann ist $[\psi_{1,\mathfrak{p}}]$ unverzweigt und somit zu einem Homomorphismus nach E anzuheben. Ist $\mathfrak{p} \notin T^*$, so ist im unverzweigten Fall die Lage klar. Verzweigt jedoch $[\psi_{1,\mathfrak{p}}]$, so passiert dies allein aufgrund des Umstands, daß $x_\mathfrak{p}$ in $\mathfrak{p}$ verzweigt, da $Ram(N_0/k) \subseteq T^*$ gilt. $x_\mathfrak{p}$ verzweigt jedoch nur in Stellen, welche in N_0/k und $k(\zeta_{p^{v_p(m)}})/k$ voll zerlegt sind. Ist $x_\mathfrak{p}$ verzweigt und nicht zyklisch, so entspricht E nach Voraussetzung dem semidirekten Produkt $Kern(\pi) \rtimes G$, d.h. es gibt einen Schnitt $G \to E$ von π und somit ist auch in diesem Fall $\mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, G_\mathfrak{p}, E_\mathfrak{p})} \neq \emptyset$. $\diamond$

Mit diesem Ergebnis ist es jetzt möglich, den zentralen Teil dieses Abschnitts nachzuweisen.

Beweis. (von 8.2.1): Es sei

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = \{\iota\}.$$

Dann darf von einer Lage ausgegangen werden, die durch das folgende Diagramm beschrieben wird

$$\begin{tikzcd}
& & & G_k \arrow[dl, dotted, "\psi"'] \arrow[d, "\varphi"] & \\
1 \arrow[r] & G_1 \arrow[r] & G \arrow[r, two heads] & G/G_1 = A_0 \arrow[r] & 1,
\end{tikzcd}$$

da der Voraussetzung zufolge die Gruppe G/G_1 so erhalten werden kann, daß an allen lokalen Stellen Anhebungen vorhanden sind und dabei gegebene lokale Vorgaben an den Stellen aus T verwirklicht werden. Um ein $\psi \in \mathcal{L}_{\mathcal{E}(G_k, A_0, G)}$ zu erhalten, welches den lokalen Vorgaben $\psi_\mathfrak{p} \in \mathcal{L}_{\mathcal{E}(G_k, A_{0,\mathfrak{p}}, G_\mathfrak{p})}$ für $\mathfrak{p} \in T$ Rechnung trägt, ist schrittweise vorzugehen wie es das nächste Diagramm veranschaulicht:

$$\begin{tikzcd}
 & & & G_k \arrow[d, two heads, "\varphi"] \arrow[ddl, dotted, "\psi_i"'] \arrow[dddl, dotted, "\psi_{i-1}"] & \\
1 \arrow[r] & G_1 \arrow[r, hook] \arrow[d, two heads] & G \arrow[r, two heads] \arrow[d, two heads] & G/G_1 \arrow[r] \arrow[d, equal] & 1 \\
 & G_1/G_i \arrow[r, hook] \arrow[d, two heads] & G/G_i \arrow[r, two heads, "\pi_i"] \arrow[d, two heads] & G/G_1 \arrow[d, equal] & \\
 & G_1/G_{i-1} \arrow[r, hook] & G/G_{i-1} \arrow[r, two heads] & G/G_1. &
\end{tikzcd}$$

Behauptung Es gibt eine Folge von Lösungen $\psi_i : G_k \to G/G_i$ $i = 1, ..., n$ aus $\mathcal{L}_{\mathcal{E}(G_k, G/G_{i-1}, G/G_i)}$ für $i = 1, ..., n$ des obigen Einbettungsproblems, welche diesen Bedingungen genüge leistet:

1. $$\psi_{i-1} = \pi_i \cdot \psi_i \text{ für } i = 1, ..., n.$$

2. $$[\psi_i|_{G_{k_\mathfrak{p}}}] = [\psi_{\mathfrak{p}_i}] \in \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, (G/G_{i-1})_\mathfrak{p}, (G/G_i)_\mathfrak{p})} \text{ für } \mathfrak{p} \in T.$$

3. Wird durch ψ_i der Körper K_i definiert, dann gilt für selbigen:
$$(\#G, \#\mu(K_{i-1})) = (\#G, \#\mu(K_i)).$$

4. $$\prod_{\mathfrak{p}} \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, (G/G_i)_\mathfrak{p}, G_\mathfrak{p})} \neq \varnothing.$$

Beweis. (obiger Behauptung):
Für ψ_0 kann die Verwirklichung von A_0 genommen werden, welche in der Voraussetzung des Satzes enthalten ist.
Da A_0 ein einfacher Modul mit trivialer Operation ist, ist er zyklisch und in $\mathfrak{p} \in T$ nach Voraussetzung auf G fortsetzbar. Alle unverzweigten Stellen sind ebenso fortsetzbar und $Ram(K_0/k) \subseteq cs(k(\mu_m)/k) \cup T$ garantiert auch die Fortsetzbarkeit der verzweigten Stellen. Ist der Homomorphismus $\psi_{i-1} : G_k \to G/G_{i-1}$ bereits konstruiert, so kann
$$T_{i-1} := T \cup Ram(K_{i-1}/k)$$
gesetzt werden und zu $\mathfrak{p} \in T_{i-1} \setminus T$ eine Lösung $\psi_\mathfrak{p} : G_{k_\mathfrak{p}} \to G \to G/G_i$ des lokalen Problems gewählt werden. Ihr Dasein wird durch die 4. Eigenschaft der Behauptung gewährleistet. Selbige garantiert darüber hinaus, daß
$$\prod_{\mathfrak{p}} \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, (G/G_{i-1})_\mathfrak{p}, (G/G_i)_\mathfrak{p})} \neq \varnothing$$
gilt und deshalb Satz 8.2.4 sogar nach Austausch von sowohl T durch T_{i-1}, als auch $E \twoheadrightarrow G$ durch $G \twoheadrightarrow G/G_i$ und φ durch ψ_{i-1} anwendbar ist. Als Ergebnis

wird ein epimorphes Element $[\psi_i]$ aus $\mathcal{L}_{\mathcal{E}(G_k, G/G_{i-1}, G/G_i)}$ erhalten, welches diese Eigenschaften hat:

1. $[\psi_i|_{G_{k_\mathfrak{p}}}] = [\psi_{\mathfrak{p},i}]$ in $\mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, (G/G_{i-1})_\mathfrak{p}, (G/G_i)_\mathfrak{p})}$ für $\mathfrak{p} \in T_{i-1}$.
2. $\mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, (G/G_i)_\mathfrak{p}, G)} \neq \varnothing$ für jedes $\mathfrak{p} \notin T_{i-1}$.
3. $(\#G, \#\mu(K_i)) = (\#G, \#\mu(K_{i-1}))$.

Ist ψ_i ein Vertreter von $[\psi_i]$, so ist ψ_i surjektiv und genügt den Bedingungen 1-4 diesen Überlegungen zufolge: Die 1. Bedingung ist wegen $[\psi_i] \in \mathcal{L}_{\mathcal{E}(G_k, (G/G_{i-1})_\mathfrak{p}, (G/G_i)_\mathfrak{p})}$ selbstverständlich erfüllt. Der 1. Eigenschaft von 8.2.4 zufolge sind die Elemente $\psi_i|_{G_{k_\mathfrak{p}}}$ und $\psi_{\mathfrak{p}i}$ für $\mathfrak{p} \in T_{i-1}$ durch ein Element aus A_i zueinander konjugiert. A_i selbst ist jedoch in G_1/G_i enthalten, was dem Kern der Projektion $G/G_i \twoheadrightarrow G/G_1$ entspricht. Daher gilt auch die 2. Bedingung der Behauptung. Die 3. Eigenschaft liefert die 3. Bedingung unmittelbar und die 4. ist die Folge des Umstands, daß für $\mathfrak{p} \in T_{i-1}$ die Aussage

$$[\psi_\mathfrak{p}] \in \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, (G/G_i)_\mathfrak{p}, G_\mathfrak{p})}$$

gilt. Damit ist die Behauptung verifiziert. ◊

Nun ist $[\psi_n]$ die gesuchte Klasse $[\psi]$ welche durch die Einschränkungsabbildung auf ein gegebenes Element aus $\prod_{\mathfrak{p}\in T} \mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, (A_0)_\mathfrak{p}, G_\mathfrak{p})}$ abgebildet wird. ◊

8.3 Abelsche Erweiterungen

Es verbleibt die Frage nach der Möglichkeit der Verwirklichung abelscher Erweiterungen, welche ausbaufähig sind, d.h. deren lokale Komponenten sämtlich Projektionen einer nichtabelschen Erweiterung sind, deren Galoisgruppen in eine auflösbare Gruppe G einzubetten sind. Für $\mu_p \notin k$ kann auf die Arbeit von Neukirch [Neu79], resp. [NSW08], chap. IX, §5 zurückgegriffen werden.

8.3.1 Satz: *Es seien natürliche Zahlen $m, e \in \mathbb{N}$ und eine endliche Stellenmenge T eines globalen Zahlkörpers k mit lokal zyklischen Vorgaben $L_\mathfrak{P}/k_\mathfrak{p}$, deren Grade Teiler von m seien, gegeben. Ist nun K/k eine endliche lokal zyklische Erweiterung, so daß für $\mathfrak{p} \in T$ die Erweiterungen $K_\mathfrak{P} L_\mathfrak{P}(\mu_{me})/k_\mathfrak{p}$ zyklisch sind, so gibt es eine zyklische Körpererweiterung L vom Grad m über k mit diesen Eigenschaften:*

1. *L und K sind über k linear disjunkt.*
2. *Für jede Gruppe $E \twoheadrightarrow G(KL/k)$, deren Exponent das Produkt me teilt, gilt*

$$\mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, G(KL_\mathfrak{P}/k_\mathfrak{p}), E_\mathfrak{p})} \neq \varnothing.$$

Beweis. Ohne Beschränkung der Allgemeinheit darf davon ausgegangen werden, daß $m = p^j$ und $e = p^l$ Potenzen einer Primzahl p sind. Im Fall $\mu_p \notin k$ ist dies ein Spezialfall von Neukirchs Satz, wie er sich in [NSW08], chap. IX unter §5, Theorem 5 befindet. Es darf also von $\mu_p \subseteq k$ ausgegangen werden. Sei $A = \mathbb{Z}/m$ und für jedes $\mathfrak{p} \in T$ sei eine Einbettung $y_\mathfrak{p} : G(L_\mathfrak{P}/k_\mathfrak{p}) \hookrightarrow A$ gegeben. Wenn

$$S = cs(K(\mu_{p^{j+l}})/k) \cup Ram(K(\mu_{p^{j+l}})/k)$$

ist, liegt 7.2.1 zufolge das Tupel $(y_\mathfrak{p})_{\mathfrak{p}\in T}$ im Kokern der Abbildung

$$H^1(k_S/k, A) \to \prod_{\mathfrak{p}\in T} H^1(k_\mathfrak{p}, A),$$

wenn für jedes Element $x \in Ш^1(k_S, S \setminus T, A')$ die folgende Relation gilt:

$$\sum_{\mathfrak{p}\in T} inv_\mathfrak{p}(x_\mathfrak{p} \cup y_\mathfrak{p}) = 0.$$

Es kann nun gezeigt werden, daß jeder Summand obiger Summe 0 ist, denn: Ist die Erweiterung

$$K_\mathfrak{P} L_\mathfrak{P}(\mu_{p^{j+l}})/k_\mathfrak{p}$$

zyklisch, so ist sie für $\mathfrak{p} \nmid p$ entweder rein zahm verzweigt oder unverzweigt. Im unverzweigten Fall sind sowohl $x_\mathfrak{p}$ als auch $y_\mathfrak{p}$ unverzweigt und annullieren sich daher dem Dualitätssatz 6.1.1 zufolge im Cupprodukt. Im anderen Fall gilt: $\mu_{p^{j+l}} \subseteq k_\mathfrak{p}$ und damit ist A' ein $G_{k_\mathfrak{p}}$–Modul mit trivialer Wirkung. Das Cupprodukt wird dann durch die Matrix aus 5.3.1 beschrieben. Da sowohl $x_\mathfrak{p}$ als auch $y_\mathfrak{p}$ über denselben zyklischen Quotienten faktorisieren, annullieren sie sich in dieser Paarung. Es verbleibt die Erläuterung des rein verzweigten Falls $\mathfrak{p} \mid p$: Ist $\mu_{p^{j+l}} \subseteq k_\mathfrak{p}$, so ist A' abermals ein trivialer Modul und 5.3.2 liefert das gewünschte Ergebnis. Ist $k_\mathfrak{p}(\mu_{p^{j+l}})/k_\mathfrak{p}$ eine echte Erweiterung, so läßt sie sich nach lokaler Klassenkörpertheorie nur auf eine Weise zu einer zyklischen Erweiterung vom Grad m anheben, und zwar durch Adjunktion weiterer Einheitswurzeln. Dies impliziert, daß sowohl $L_\mathfrak{P}$ als auch $K_\mathfrak{P}$ rein wild verzweigte Einheitswurzelerweiterungen sind. Damit faktorisiert das Cupprodukt über $H^2(G(k_\mathfrak{p}(\mu_{p^\infty})/k_\mathfrak{p}), \mu_{p^m})$. Diese Kohomologiegruppe verschwindet jedoch, da die Galoisgruppe zu $\mathbb{Z}_p$ isomorph ist und demnach kohomologische Dimension 1 hat. Dem Verschwinden obiger Summe zufolge ist nun das Tupel $(y_\mathfrak{p})_{\mathfrak{p}\in T}$ in allen Fällen im Bild des obigen Einschränkungshomomorphismus enthalten und daher gibt es eine Klasse $x \in H^1(k_S/k, A)$, welche diese Erweiterungen verwirklicht. An allen Primstellen werden also lokale Erweiterungen verwirklicht, bei denen die Projektion der absoluten Galoisgruppe $G_{k_\mathfrak{p}} \twoheadrightarrow G(LK/k)$ über einen zyklischen Quotienten der Ordnung p^{j+l} faktorisiert und daher ist $\mathcal{L}_{\mathcal{E}(G_{k_\mathfrak{p}}, G_\mathfrak{p}(LK/k), E_\mathfrak{p})}$ niemals leer. ◊

8.3.2 Beispiel: Mit Satz 8.2.1 und 8.3.1 kann nun festgehalten werden:

1. Die symmetrische Gruppe S_3 ist über jeder endlichen Erweiterung k von $\mathbb{Q}(\zeta_3)$ realisierbar, wobei beliebige lokale Vorgaben $K_\mathfrak{P}/k_\mathfrak{p}$ mit $G(K_\mathfrak{P}/k_\mathfrak{p}) \hookrightarrow S_3$ verwirklicht werden können, solange die Gesamtzahl der Vorgaben endlich ist.

2. Die alternierende Gruppe A_4 und die symmetrische Gruppe S_4 sind über jeder endlichen Erweiterung k von $\mathbb{Q}(\zeta_{12})$ so zu verwirklichen, daß sie eine endliche Menge lokaler Vorgaben realisieren. Diese Vorgaben unterliegen keiner weiteren Einschränkung.

3. Die obigen Körper k können auch anders gewählt werden: Unter Benutzung des Satzes 8.3.1 können dann hinreichende Einschränkungen für die lokalen Vorgaben formuliert werden:

   I. Wenn k den Körper $\mathbb{Q}(\zeta_3)$ nicht umfaßt, dann können für $\mathfrak{p} \in cs(k(\zeta_3)/k)$ beliebige Vorgaben gewählt werden, im Fall $\mathfrak{p} \notin cs(k(\zeta_3)/k)$ muß $K_\mathfrak{P}/k_\mathfrak{p}$ entweder die dritten Einheitswurzeln enthalten oder eine Erweiterung vom Grad 3 sein, wenn die S_3 realisiert werden soll.

II. Enthält k nicht den Körper $\mathbb{Q}(\zeta_{12})$, dann können bei der Realisierung von A_4 oder S_4 für $\mathfrak{p} \in cs(k(\zeta_{12})/k)$ beliebige Vorgaben gewählt werden, im Fall $\mathfrak{p} \notin cs(k(\zeta_{12})/k)$ können Erweiterungen verwirklicht werden, die das Element ζ_{12} einschließen: $K_{\mathfrak{P}}(\zeta_{12}) = K_{\mathfrak{P}}$.

4. Die in Beispiel 8.1.2 erwähnten iterierten semidirekten Produkte G können über jeder endlichen Erweiterung k von $\mathbb{Q}(\zeta_n)$ mit jeder endlichen Menge an lokalen Vorgaben verwirklicht werden. Hierbei sei n der Exponent der Gruppe.

Die Ergebnisse dieses Abschnitts stehen in Verbindung mit Satz 2 aus Neukirchs Arbeit [Neu73b], §8. Er besagt das Folgende:

8.3.3 Satz: *Zu jedem über einem endlichen algebraischen Zahlkörper K definierten Einbettungsproblem $\mathcal{E}(G_K, \Gamma, G)$ mit lokaler Vorgabe an endlich vielen Stellen $\mathfrak{p}$ und mit auflösbarem Kern A gibt es eine endliche Kreiskörpererweiterung K'/K, derart daß die Verlagerung auf K' eigentlich lösbar wird.*

Obigem Ergebnis zufolge läge es nun nahe davon auszugehen, daß jedwede auflösbare Gruppe vom Exponenten n über jeder Erweiterung von $\mathbb{Q}(\zeta_n)$ unter Berücksichtigung einer beliebigen endlichen Menge lokaler Vorgaben verwirklicht werden kann. Ob dies jedoch gelingt, bleibt eine offene Frage.

9 Literatur

[AT09] Artin, E. and Tate,J. *Class Field Theory.* AMS Chelsea Publishing, 2009.

[Dem61] S. P. Demuškin. Die Gruppe der maximalen p-Erweiterung eines lokalen Körpers. *Izv. Akad. Nauk. UdSSR Ser. Mathem. 25.3*, Seiten 329–346, 1961. (russisch).

[Hoe68] K. Hoechsmann. Zum Einbettungsproblem. *Journal f. reine und angewandte Mathematik 229*, Seiten 81–106, 1968.

[Iwa55] K. Iwasawa. On Galois Groups of Local Fields. *Trans. AMS 80*, Seiten 448–469, 1955.

[Lab67] J.-P. Labute. Classification of Demuškin groups. *Can. J. Math. 19*, Seiten 106–132, 1967.

[Neu73a] J. Neukirch. Über das Einbettungsproblem der algebraischen Zahlentheorie. *Inventiones Math. 21*, Seiten 59–116, 1973.

[Neu73b] J. Neukirch. Einbettungsprobleme mit lokaler Vorgabe. *Journal für reine und angewandte Mathematik 259*, Seiten 1–47, 1973.

[Neu79] J. Neukirch. On solvable Number Fields. *Inventiones Math. 53*, Seiten 135–164, 1979.

[NSW08] Neukirch, J., Schmidt, A., and Wingberg, K. *Cohomology of Number Fields.* Springer Verlag, 2. Auflage, 2008.

[Poi67] G. Poitou. *Cohomologie Galoisienne des modules finis.* Editions Dunod, 1967.

[Ser65] J.-P. Serre. *Lie Algebras and Lie Groups.* Benjamin, 1965.

[Ser64] J.-P. Serre. Structure de certains pro-p-groupes. *Séminaire Nicolas Bourbaki, exp. n^o 252*, Seiten 145–155, 1962-64.

[Ser08] J.-P. Serre. *Topics in Galois Theory.* A. K. Peters, Ltd., 2008.

[Tat62] J. Tate. Duality theorems in galois cohomology over number fields. *Proc. Int. Congress Math. Stockholm*, Seiten 288–295, 1962.

[Win84] K. Wingberg. Ein Analogon zur Fundamentalgruppe einer Riemannschen Fläche im Zahlkörperfall. *Inventiones Math. 77*, Seiten 557–584, 1984.