Fakultät für Mathematik und Informatik
Ruprecht-Karls-Universität Heidelberg

Diplomarbeit

Über die maximale p-Erweiterung algebraischer Zahlkörper mit beschränkter Verzweigung und vorgegebener Zerlegung

Jochen Gärtner

Januar 2008

Betreuer:
Prof. Dr. Kay Wingberg

Inhaltsverzeichnis

1 Einleitung **1**

2 Kohomologie von pro-p-Gruppen **5**

2.1 Kohomologie pro-endlicher Gruppen 5
2.2 Kohomologische Dimension und Euler-Poincaré-Charakteristik . 5
2.3 Freie pro-p-Gruppen 6
2.4 Darstellungen von pro-p-Gruppen 7
2.5 Zulässige Darstellungen von pro-p-Gruppen 8
2.6 Pro-p-Gruppen vom Koch-Typ 9

3 Die maximale p-Erweiterung von $k_{\mathfrak{p}}$ **11**

3.1 Der Fall $\chi(\mathfrak{p}) \neq p$ 11
3.2 Der Fall $\chi(\mathfrak{p}) = p$ 12

4 Beschränkte Verzweigung und vorgegebene Zerlegung **15**

4.1 Das globale Normrestsymbol 15
4.2 Verallgemeinerte Idelklassen 16
4.3 Die Erweiterung $k_S^T|k$ 16
4.4 Verallgemeinerte Idealklassen 18

5 Der Erzeugerrang $h^1(G_S^T)$ **21**

5.1 Die Kummergruppen V_S^T und die exakte 5-Term-Sequenz 21
5.2 Berechnung des Erzeugerrangs von G_S^T 22

6 Der Relationenrang $h^2(G_S^T)$ **27**

6.1 Die Lokalisierungsabbildungen $\varphi_{S,T}^i$ 27
6.2 Berechnung des Relationenrangs von G_S^T 32
6.3 Eine Bedingung für $[k_S^T(p) : k] = \infty$ 34

7 Die Kummergruppen V_S^T **37**

7.1 Primstellenmengen mit $Б_S^T = 0$ 37
7.2 Der Fall $\delta = 1$ - Anwendung der Kummertheorie 40

8 Erzeuger und Relationen von G_S^T **43**

8.1 Ein kanonisches Erzeugendensystem von G_S^T 43
8.2 Bestimmung eines minimalen Erzeugendensystems 44
8.3 Relationen von G_S^T 45
8.4 Beispiele 47
8.5 Der Fall $k = \mathbb{Q}, |T| = 1$ - G_S^T vom Koch-Typ 49

Literaturverzeichnis **53**

1 Einleitung

Das Verzweigungsverhalten von Primstellen nimmt in der klassischen algebraischen Zahlentheorie eine zentrale Stellung ein. So ist beispielsweise von Interesse, welche Primstellen in einer gegebenen galoisschen Erweiterung algebraischer Zahlkörper unverzweigt oder gar voll zerlegt sind. Nach der *Hilbertschen Verzweigungstheorie* hängt diese Fragestellung eng mit dem Studium der zugehörigen Galoisgruppen zusammen.

Für abelsche Erweiterungen liefert die globale Klassenkörpertheorie schöne Resultate. Nach dem *Zerlegungsgesetz* spiegelt sich das Verzweigungsverhalten der Primstellen eines algebraischen Zahlkörpers k in einer endlichen abelschen Erweiterung $L|k$ direkt in der zugehörigen Normenuntergruppe $N_{L|k}C_L$ der Idelklassengruppe C_k wider. Möchte man sich jedoch von der Einschränkung, lediglich abelsche Erweiterungen zu betrachten, lösen, ist es ungleich schwieriger, analoge Fragestellungen zu beantworten.

Wir betrachten zunächst das folgende Problem der *beschränkten Verzweigung:* Sei k ein algebraischer Zahlkörper und S eine beliebige Menge von Primstellen von k. Es sollen Erweiterungen $L|k$ studiert werden, welche außerhalb der Menge S unverzweigt sind, also die Eigenschaft besitzen, dass alle Primstellen von k, die in L verzweigen, in S enthalten sind. Komposita und normale Hüllen solcher Erweiterungen haben wieder diese Eigenschaft und es existiert folglich eine *maximale außerhalb S unverzweigte Erweiterung k_S* von k. Diese ist galoissch und eine möglichst detaillierte Kenntnis ihrer Galoisgruppe $G(k_S|k)$ ist erstrebenswert. Eine Reihe wichtiger Fragen lassen sich jedoch erst dann zufriedenstellend beantworten, wenn man zum maximalen pro-p-Quotienten von $G(k_S|k)$ übergeht. Man betrachtet also nunmehr die *maximale außerhalb S unverzweigte p-Erweiterung $k_S(p)$* von k, wobei p eine beliebige Primzahl bezeichnet.

Erste Studien zu minimalen Darstellungen mit Erzeugern und Relationen der Gruppe $G_S = G(k_S(p)|k)$ gehen auf den russischen Mathematiker I.R. Šafarevič ([Saf]) zurück. H. Koch ([Ko]) gibt nicht nur eine übersichtliche Darstellung dieser Ergebnisse, sondern zeigt auch, dass sich die Relationen dieser Gruppe unter bestimmten Voraussetzungen explizit mit Kenntnis der *lokalen Relationen,* d.h. der Relationen der maximalen p-Erweiterung der lokalen Körper $k_\mathfrak{p}$ für Primstellen $\mathfrak{p} \in S$, bestimmen lassen. Als methodische Grundlage dient die *Kohomologie* pro-endlicher Gruppen, welche sich in der Zahlentheorie in vielerlei Hinsicht als nützlich und ergiebig erwiesen hat. Für den *Relationenrang* von G_S, d.h. der Kardinalität eines minimalen Relationensystems, kann hier zunächst lediglich eine obere Schranke angegeben werden. Enthält S jedoch die Menge S_∞ der unendlichen Primstellen und die Menge S_p aller über der

Primzahl p liegenden Primstellen, so kann für den Relationenrang unter Ausnutzung der tiefliegenden *Poitou-Tate-Dualität* sogar Gleichheit gezeigt werden (vgl. [NSW], Chap. VIII, §7).

Eine weitere wichtige Eigenschaft der pro-p-Gruppe G_S ist ihre *kohomologische Dimension.* Auch hier waren zufriedenstellende Ergebnisse zunächst nur für den Fall $S \supseteq S_p \cup S_\infty$ möglich (vgl. [NSW], Chap. VIII). Für den Fall, dass der betrachtete Grundkörper der Körper $\mathbb{Q}$ der rationalen Zahlen ist und die Menge S die Primzahl p nicht enthält, konnte J. Labute ([La1]) Voraussetzungen an die in S liegenden Primzahlen angeben, unter welchen G_S eine *milde* pro-p Gruppe von kohomologischer Dimension 2 ist. D. Vogel ([Vo]) konnte dies auf den Fall imaginär quadratischer Zahlkörper übertragen.

Bezeichne nun T eine weitere, zu S disjunkte, endliche Menge endlicher Primstellen von k. In der vorliegenden Arbeit betrachten wir Erweiterungen von k, welche außerhalb der Menge S unverzweigt und über der Menge T voll zerlegt sind. Mit k_S^T bezeichnen wir die *maximale außerhalb S unverzweigte, über T voll zerlegte Erweiterung von k* und mit G_S^T die Galoisgruppe der maximalen pro-p-Zwischenerweiterung $k_S^T(p)|k$.

$$\begin{tikzcd} k_S^T \arrow[d, dash] \\ k_S^T(p) \arrow[d, dash] \\ k \arrow[u, bend right, dash, "G_S^T"'] \end{tikzcd}$$

Im Zentrum unseres Interesses steht das Studium von minimalen Darstellungen der Gruppe G_S^T. Insbesondere soll nach dem Vorbild der Gruppen G_S unter entsprechenden Voraussetzungen eine explizite Darstellung von Erzeugern und Relationen angegeben werden.

Im zweiten Abschnitt führen wir die benötigten Notationen und Resultate aus der Kohomologietheorie der pro-p-Gruppen an. Nach einer kurzen Einführung in die Theorie der *freien* Darstellungen zitieren wir wichtige Ergebnisse aus der Theorie der *zulässigen* Darstellungen und der Darstellungen vom *Koch-Typ.* Im dritten Abschnitt betrachten wir die Galoisgruppen der maximalen p-Erweiterungen lokaler Zahlkörper und geben hierfür die expliziten Darstellungen von Erzeugern und Relationen an. Wir verzichten hierbei jeweils auf die Beweise und verweisen auf die bereits erwähnte Literatur.

Im vierten Abschnitt werden wir für die Gruppe $G_S^T[p]$, der Galoisgruppe der maximalen abelschen Erweiterung vom Exponenten p in $k_S^T(p)$, eine ideltheoretische Entsprechung formulieren. Diese bildet die Grundlage für die Berechnung des Erzeugerrangs der Gruppe G_S^T im fünften Abschnitt.

Der sechste Abschnitt ist dem Relationenrang von G_S^T gewidmet. Wir orientieren uns in unserer Vorgehensweise an der analogen Berechnung für die Gruppe G_S bei [Ko]. Eine entscheidende Größe bei der Berechnung von Erzeuger- und Relationenrängen bilden die *Kummergruppen* V_S^T. Insbesondere drängt sich die Frage auf, wann diese Gruppen verschwinden. Im siebten Abschnitt geben wir hierfür eine notwendige und hinreichende Bedingung an die Primstellenmengen S und T an. Für den Fall $k = \mathbb{Q}$ wenden wir dies auf erste Beispiele an. Enthält k die p-ten Einheitswurzeln, so liefert die *Kummertheorie* eine direkte Beschreibung der Gruppen V_S^T als Duale von Galoisgruppen von Kummererweiterungen über k.

Im siebten Abschnitt geben wir nun eine Beschreibung der Erzeuger und Relationen an. Für die explizite Bestimmung einer minimalen Darstellung von G_S^T ist das Verschwinden der Kummergruppen V_S^T entscheidend. In diesem Fall lassen sich die Relationen aus den lokalen Relationen gewinnen. Diese Darstellungen ausnützend, kann für den Fall $k = \mathbb{Q}, |T| = 1$ unter weiteren Voraussetzungen gezeigt werden, dass die Gruppe G_S^T vom *Koch-Typ* ist. Stehen die in S liegenden Primzahlen in bestimmten Relationen zueinander, ist die Gruppe G_S^T nach den Resultaten von Labute ([La1]) von kohomologischer Dimension 2.

Bei Herrn Prof. Dr. Wingberg, dessen Vorlesungen mein Interesse an der algebraischen Zahlentheorie geweckt haben und dessen Tür stets offen stand, möchte ich mich für das interessante Thema und die gute Betreuung beim Erstellen dieser Arbeit bedanken. Patrick Forré, Hauke Bracht und meinen Kommilitonen danke ich für die freundschaftliche Atmosphäre und viele hilfreiche Gespräche. Nicht zuletzt gilt mein Dank meinen Eltern für ihre stete Unterstützung.

2 Kohomologie von pro-p-Gruppen

In diesem Kapitel möchten wir zunächst einige grundlegende Resultate über die Kohomologie von pro-p-Gruppen angeben. Für die Beweise verweisen wir auf die entsprechende Literatur, etwa [NSW], [Ko] oder [Se].

2.1 Kohomologie pro-endlicher Gruppen

Sei G eine pro-endliche Gruppe und A ein G-Modul. Für die Definition der Kohomologiegruppen $H^n(G,A)$ für $n \geq 0$ und ihre grundlegenden Eigenschaften verweisen wir auf [NSW], Chap. I. An dieser Stelle sei lediglich das folgende wichtige Resultat über das Verhalten der Kohomologiegruppen bei Änderung der Gruppe G angegeben.

(2.1.1) Proposition. *Sei G eine pro-endliche Gruppe, H eine abgeschlossene normale Untergruppe von G und A ein G-Modul. Dann hat man die exakte Sequenz*

$$0 \longrightarrow H^1(G/H, A^H) \xrightarrow{inf} H^1(G,A) \xrightarrow{res} H^1(H,A)^{G/H}$$

$$\xrightarrow{tg} H^2(G/H, A^H) \xrightarrow{inf} H^2(G,A),$$

wobei wir mit inf, res und tg die Inflation, Restriktion und Verlagerung (vgl. etwa [NSW], Chap. I) bezeichnen.

2.2 Kohomologische Dimension und Euler-Poincaré-Charakteristik

Sei im Folgenden stets p eine Primzahl. Wir betrachten ***pro-p-Gruppen***, d.h. projektive Limiten endlicher p-Gruppen. Eine wichtige Eigenschaft von pro-p-Gruppen ist ihre kohomologische Dimension.

(2.2.1) Definition. *Sei G eine pro-p-Gruppe. Die* **kohomologische Dimension *cd G*** *(bzw.* **strikte kohomologische Dimension *scd G****) ist die kleinste ganze Zahl n, so dass*

$$H^q(G,A) = 0 \quad \textit{für alle } q > n$$

und alle Torsionsmoduln A (bzw. alle Moduln A).

(2.2.2) Proposition. *Sei G eine pro-p-Gruppe. Dann gilt*

$$cd\ G \leq scd\ G \leq cd\ G + 1.$$

(2.2.3) Proposition. *Für eine pro-p-Gruppe G sind die folgenden beiden Aussagen äquivalent:*

(i) *cd* $G \leq n$.

(ii) $H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0$.

(2.2.4) Notation. *Für eine pro-p-Gruppe G setzen wir abkürzend*

$$H^n(G) = H^n(G, \mathbb{Z}/p\mathbb{Z}).$$

Die Gruppen $H^n(G)$ sind in kanonischer Weise $\mathbb{F}_p$-Vektorräume und wir setzen

$$h^n(G) = \dim_{\mathbb{F}_p} H^n(G).$$

(2.2.5) Definition. *Sei G eine pro-p-Gruppe von endlicher kohomologischer Dimension, so dass die Gruppen $H^i(G)$ für $i \geq 0$ endlich sind. Die* **Euler-Poincaré-Charakteristik $\chi(G)$** *ist die alternierende Summe*

$$\chi(G) = \sum_{i=0}^{\infty} (-1)^i h^i(G).$$

Für pro-p-Gruppen G von nicht notwendig endlicher kohomologischer Dimension, so dass die Gruppen $H^i(G) = 0$ für alle $0 \leq i \leq n$ endlich sind, sei die **n-te partielle Euler-Poincaré-Charakteristik** *gegeben durch*

$$\chi_n(G) = \sum_{i=0}^{n} (-1)^i h^i(G).$$

(2.2.6) Satz. *Sei G eine pro-p-Gruppe, so dass die Gruppen $H^i(G) = 0$ für alle $0 \leq i \leq n$ endlich sind und $\mathfrak{U}$ eine Umgebungsbasis des Einselements von offenen Untergruppen von G. Dann sind die folgenden beiden Aussagen äquivalent:*

(i) $\chi_n(U) = (G : U)\chi_n(G)$ *für alle* $U \in \mathfrak{U}$.

(ii) *cd* $G \leq n$.

2.3 Freie pro-p-Gruppen

(2.3.1) Definition. *Sei X eine Menge und F_X die freie Gruppe über X. Die* **freie pro-p-Gruppe $F(X)$ über X** *ist der projektive Limes*

$$F(X) = \varprojlim_{N} F_X/N,$$

wobei N alle normalen Untergruppen von F_X durchläuft, die die folgenden Eigenschaften erfüllen:

(i) *N enthält fast alle Elemente von X.*

(ii) *$(F_X : N)$ ist eine p-Potenz.*

(2.3.2) Definition. *Sei $G_i, i \in I$ eine Familie von pro-p-Gruppen und*

$$\tilde{G} = \mathop{\ast}_{i \in I}^{diskr} G_i$$

das gewöhnliche freie Produkt der G_i. Das **freie pro-p-Produkt $G = \mathop{\ast}_{i \in I} G_i$** *der Gruppen $G_i, i \in I$ ist der projektive Limes*

$$G = \varprojlim_{N} \tilde{G}/N,$$

wobei N alle normalen Untergruppen von G durchläuft, die die folgenden Eigenschaften erfüllen:

(i) $N \subseteq G_i$ *für fast alle* $i \in I$.

(ii) $(G : N)$ *ist eine* p*-Potenz.*

(iii) $N \cap G_i$ *ist eine offene Untergruppe von* G_i.

(2.3.3) Bemerkung. Die freie pro-p-Gruppe $F(X)$ über eine Menge X ist gerade das freie pro-p-Produkt

$$F(X) = \mathop{\ast}_{x \in X} \mathbb{Z}_p.$$

2.4 Darstellungen von pro-p-Gruppen

Sei G eine pro-p-Gruppe.

(2.4.1) Definition. *Eine Teilmenge $S \subseteq G$ heißt* **konvergent***, falls jede offene Untergruppe von G fast alle Elemente von S enthält. Eine konvergente Teilmenge $S \subseteq G$ heißt* **Erzeugendensystem***, falls sie G als topologische Gruppe erzeugt. Ein Erzeugendensystem heißt* **minimal***, falls keine echte Teilmenge ein Erzeugendensystem ist. Mit $d(G)$ bezeichnen wir den* **Rang** *von G, d.h. das Infimum der Kardinalitäten von minimalen Erzeugendensystemen von G.*

(2.4.2) Definition. *Mit $[G, G]$ bezeichnen wir die abgeschlossene, von den Kommutatoren*

$$[x, y] = xyx^{-1}y^{-1}, \quad x, y \in G$$

erzeugte Untergruppe von G. Ferner bezeichnen wir mit $Fr(G)$ die **Frattini-Untergruppe** *von G, also die abgeschlossene, von den Kommutatoren und p-Potenzen erzeugte Untergruppe von G:*

$$\mathrm{Fr}(G) = [G, G]G^p.$$

Wir formulieren nun den ***Burnsideschen Basissatz***:

(2.4.3) Satz. *Eine konvergente Teilmenge $S \subseteq G$ ist genau dann ein Erzeugendensystem von G, wenn die Menge $\overline{S} = \{s \operatorname{Fr}(G) | s \in S\}$ der Restklassen modulo $\operatorname{Fr}(G)$ die Gruppe $G/\operatorname{Fr}(G)$ erzeugt. S ist genau dann ein minimales Erzeugendensystem von G, falls $\overline{S}$ ein minimales Erzeugendensystem von $G/\operatorname{Fr}(G)$ ist. Alle minimalen Erzeugendensysteme haben die Kardinalität $d(G)$ und es gilt*

$$d(G) = h^1(G).$$

(2.4.4) Definition. *Sei G eine pro-p-Gruppe, S ein Erzeugendensystem von G und $F = F(S)$ die freie pro-p-Gruppe über S. Dann hat man eine exakte Sequenz*

$$1 \longrightarrow R \longrightarrow F \longrightarrow G \longrightarrow 1 .$$

Eine konvergente Teilmenge E von R heißt Relationensystem von G bezüglich S, falls R die kleinste abgeschlossene normale Untergruppe von F ist, die E enthält. Ist S ein minimales Erzeugendensystem von G, so heißt E **minimal***, falls keine echte Teilmenge von E ein Relationensystem von G bezüglich S ist. Die exakte Sequenz $1 \to R \to F \to G \to 1$ heißt dann auch* **minimale Darstellung** *von G und mit $S = \{x_i, i \in I\}, E = \{w_j, j \in J\}$ schreiben wir abkürzend*

$$G = < x_i, i \in I | w_j, j \in J > .$$

Mit $r(G)$ bezeichnen wir den **Relationenrang** *von G, d.h. die Kardinalität eines minimalen Relationensystems von G.*

(2.4.5) Proposition. *Für eine pro-p-Gruppe G gilt*

$$r(G) = h^2(G).$$

Ist $G \neq 1$, dann ist G genau dann frei, falls cd $G \leq 1$.

Wir zitieren nun den berühmten Satz von E.S. Golod und I.R. Šafarevič, der eine notwendige Bedingung für die Endlichkeit einer pro-p-Gruppe G liefert.

(2.4.6) Satz. *Für eine endliche p-Gruppe $G \neq 1$ gilt*

$$h^2(G) > \frac{1}{4} h^1(G)^2.$$

Beweis. Für den Beweis verweisen wir auf [NSW], Chap. III, (3.9.7) bzw. [Se], Chap. I, §4, Theorem 1. □

2.5 Zulässige Darstellungen von pro-p-Gruppen

(2.5.1) Definition. *Sei $G_i, i \in I$ eine Familie von pro-p-Gruppen und für jedes $i \in I$ sei T_i eine Untergruppe von G_i. Eine Familie von Homomorphismen $\varphi_i : G_i \to G$, $i \in I$, wobei G eine weitere pro-p-Gruppe bezeichnet, heißt* **zulässig bezüglich $\{T_i, i \in I\}$***, falls $U \subseteq \varphi_i(T_i)$ für fast alle $i \in I$ und jede offene normale Untergruppe U von G.*

(2.5.2) Satz. *Sei $G_i, i \in I$ eine Familie von pro-p-Gruppen und für jedes $i \in I$ sei T_i eine abgeschlossene normale Untergruppe von G_i, so dass*

$$H^2(G_i/T_i) = 0 \quad \text{für alle } i \in I.$$

Sei G eine weitere pro-p-Gruppe und $\varphi_i : G_i \to G, i \in I$ zulässig bezüglich $\{T_i, i \in I\}$.

Für jedes $i \in I$ sei ferner $1 \to R_i \to F_i \xrightarrow{\psi_i} G_i \to 1$ eine minimale Darstellung von G_i und $1 \to R \to F \to G \to 1$ eine minimale Darstellung von G. Dann existieren Homomorphismen $\chi_i : F_i \to F$, die zulässig bezüglich $\{R_i, i \in I\}$ sind, mit Einschränkungen

$$\chi_i' = (\chi_i)_{|R_i} : \quad R_i \longrightarrow R,$$

so dass das Diagramm

$$\begin{tikzcd} 1 \arrow[r] & R_i \arrow[r] \arrow[d, "\chi_i'"] & F_i \arrow[r, "\psi_i"] \arrow[d, "\chi_i"] & G_i \arrow[r] \arrow[d, "\varphi_i"] & 1 \\ 1 \arrow[r] & R \arrow[r] & F \arrow[r] & G \arrow[r] & 1 \end{tikzcd}$$

kommutiert. Die Gruppe R wird genau dann von den Untergruppen $\chi_i(R_i), i \in I$ erzeugt, wenn der durch die Homomorphismen $\chi_i, i \in I$ induzierte Homomorphismus

$$H^2(G) \longrightarrow \prod_{i \in I} H^2(G_i),$$

dessen Bild bereits in $\bigoplus_{i \in I} H^2(G_i)$ enthalten ist, injektiv ist.

2.6 Pro-p-Gruppen vom Koch-Typ

In diesem Abschnitt betrachten wir pro-p-Gruppen, deren Relationen in einer minimalen freien Darstellung eine bestimmte Gestalt haben und geben einige Eigenschaften dieser Gruppen an.

(2.6.1) Definition. *Eine pro-p-Gruppe G heißt* **Schur-Gruppe**, *falls ihr Erzeugerrang gleich ihrem Relationenrang ist, d.h. falls*

$$h^1(G) = h^2(G).$$

(2.6.2) Definition. *Sei G eine pro-p-Gruppe und $q = p^m$ eine p-Potenz. Die* **absteigende q-Zentralreihe** *$\{G_{(n,q)}\}_{n \in \mathbb{N}}$ von G ist induktiv wie folgt definiert:*

(i)

$$G_{(1,q)} = G.$$

(ii) Für $n \geq 1$ *ist* $G_{(n+1,q)}$ *die abgeschlossene, von den Kommutatoren*

$$[x,y] = xyx^{-1}y^{-1}, \quad x \in G_{(n,1)}, y \in G$$

und den q*-ten Potenzen erzeugte Untergruppe von* G*, also*

$$G_{(n+1,q)} = (G_{(n,q)})^q[G_{(n,q)}, G].$$

Ferner setzen wir

$$G_n = G_{(n,p)}.$$

(2.6.3) Definition. *Sei* G *eine pro-*p*-Gruppe und* $< x_1, \ldots, x_d | w_1, \ldots, w_r >$ *eine minimale Darstellung von* G*. Wir nennen die Darstellung vom* **Koch-Typ***, falls* $r \leq d$ *und*

$$w_i \equiv x_i^{pa_i} \prod_{i \neq j} [x_i, x_j]^{a_{ij}} \mod F_3$$

mit Koeffizienten $a_i, a_{ij} \in \mathbb{Z}$*.* G *heißt vom* **Koch-Typ***, falls* G *eine Darstellung vom Koch-Typ besitzt.*

Sei nun G eine pro-p-Gruppe vom Koch-Typ und $< x_1, \ldots, x_d | w_1, \ldots, w_r >$ wie oben eine Darstellung vom Koch-Typ. Wir setzen $S = \{x_1, \ldots, x_d\}$. $\Gamma_S(p)$ bezeichne den gerichteten Graphen mit Ecken in S und gerichteten Kanten $x_i x_j$ von x_i nach x_j, falls

$$l(x_i, x_j) := a_{ij} \neq 0 \bmod p.$$

Der Graph $\Gamma_S(p)$ zusammen mit den $l(x_i, x_j) \in \mathbb{Z}/p\mathbb{Z}, i, j \leq d$ heißt ***Verbindungsdiagramm*** von (G, S).

(2.6.4) Definition. *Sei* $G =< x_1, \ldots, x_d, w_1, \ldots, w_r >$ *eine pro-*p*-Gruppe vom Koch-Typ und* $\Gamma_S(p)$ *das Verbindungsdiagramm von* (G, S)*.* $\Gamma_S(p)$ *heißt* **strikter Kreis***, falls es eine Anordnung* $S = \{v_1, \ldots, v_d\}$ *von* S *gibt, so dass die folgenden Bedingungen erfüllt sind:*

(i) Die Ecken $v_1, \ldots, v_d$ *von* $\Gamma_S(p)$ *bilden einen Kreis* $v_1 v_2 \ldots v_d v_1$*.*

(ii) Sind i *und* j *beide ungerade, so ist* $v_i v_j$ *keine Kante von* $\Gamma_S(p)$*.*

(iii) Mit $l_{ij} = l(v_i, v_j)$ *gilt*

$$l_{12} l_{23} \cdots l_{d-1,d} l_{d1} - l_{1d} l_{21} l_{32} \cdots l_{d,d-1} \neq 0.$$

(2.6.5) Bemerkung. Die Bedingung (ii) in obiger Definition impliziert, dass d gerade und $d \geq 4$ ist. Bedingung (iii) ist erfüllt, falls es eine Kante $v_i v_j$ des Kreises $v_1, v_2, \ldots, v_d v_1$ gibt, so dass $v_j v_i$ keine Kante von $\Gamma_S(p)$ ist. Ferner kann gezeigt werden, dass unter obigen Voraussetzungen notwendig $h^1(G) = h^2(G)$ folgt, d.h. G ist eine Schur-Gruppe.

Abschließend zitieren wir den folgenden Satz

(2.6.6) Satz. *Ist* G *eine pro-*p*-Gruppe vom Koch-Typ mit minimalem Erzeugendensystem* S*. Ist* $\Gamma_S(p)$ *ein strikter Kreis, dann gilt*

$$cd\ G = 2.$$

3 Die maximale p-Erweiterung von $k_{\mathfrak{p}}$

In diesem Kapitel sollen einige Resultate über die maximale p-Erweiterung von lokalen Körpern der Charakteristik 0 angegeben werden. Sei hierzu im Folgenden k ein algebraischer Zahlkörper und $\mathfrak{p}$ eine endliche Primstelle von k. Sei $k_{\mathfrak{p}}(p)$ die maximale p-Erweiterung des lokalen Zahlkörpers $k_{\mathfrak{p}}(p)$, $\mathcal{G}_{\mathfrak{p}} = \mathrm{Gal}(k_{\mathfrak{p}}(p)|k_{\mathfrak{p}})$ ihre Galoisgruppe und $\mathcal{T}_{\mathfrak{p}}$ die Trägheitsuntergruppe von $\mathcal{G}_p$, d.h.

$$\mathcal{T}_{\mathfrak{p}} = \mathrm{Gal}(k_{\mathfrak{p}}(p)|k_{\mathfrak{p}}^{nr}(p)),$$

wobei $k_{\mathfrak{p}}^{nr}(p)$ die maximale unverzweigte Erweiterung von $k_{\mathfrak{p}}$ in $k_{\mathfrak{p}}(p)$ bezeichnet. Die Galoisgruppe $\mathrm{Gal}\, k_{\mathfrak{p}}^{nr}(p)|k = \mathcal{G}_{\mathfrak{p}}/\mathcal{T}_{\mathfrak{p}}$ wird kanonisch durch den ***Frobenius-Automorphismus*** $\sigma_{\mathfrak{p}}$ erzeugt und wir haben die Isomorphie

$$\mathcal{G}_{\mathfrak{p}}/\mathcal{T}_{\mathfrak{p}} \cong \mathbb{Z}_p.$$

Mit $\chi(\mathfrak{p})$ bezeichnen wir die unter $\mathfrak{p}$ liegende Primzahl, d.h. $\chi(\mathfrak{p})$ ist gerade die Restkörpercharakteristik von $k_{\mathfrak{p}}$. $U_{\mathfrak{p}} \subseteq k_{\mathfrak{p}}^{\times}$ bezeichne die Einheitengruppe. Weiter setzen wir

$$\delta_{\mathfrak{p}} := \begin{cases} 1, & \text{falls } \mu_p \subseteq k_{\mathfrak{p}}, \\ 0, & \text{falls } \mu_p \not\subseteq k_{\mathfrak{p}}. \end{cases}$$

Für eine endliche Primstelle $\mathfrak{p}$ von k mit $\chi(p) \neq p$ ist damit $\delta_{\mathfrak{p}} = 1$ genau dann, wenn für die Norm $\mathfrak{N}(\mathfrak{p})$ die Gleichung

$$\mathfrak{N}(\mathfrak{p}) \equiv 1 \mod p$$

gilt. Wir möchten nun einige Resultate über die Erzeuger und Relationen von $\mathcal{G}_{\mathfrak{p}}$ angeben. Für die Beweise verweisen wir auf [Ko], Chap. 10.

3.1 Der Fall $\chi(\mathfrak{p}) \neq p$

Zunächst betrachten wir Primstellen $\mathfrak{p}$, die nicht über p liegen.

(3.1.1) Satz. *Ist $\chi(\mathfrak{p}) \neq p$ und $\delta_{\mathfrak{p}} = 0$, so ist $\mathcal{G}_{\mathfrak{p}} \cong \mathbb{Z}_p$ und $\mathcal{T}_{\mathfrak{p}} = 1$.*

(3.1.2) Satz. *Ist $\chi(\mathfrak{p}) \neq p$ und $\delta_{\mathfrak{p}} = 1$, dann gilt*

$$h^1(\mathcal{G}_{\mathfrak{p}}) = 2 \quad \textit{und} \quad h^2(\mathcal{G}_{\mathfrak{p}}) = 1.$$

Ferner ist $\mathcal{T}_{\mathfrak{p}} \cong \mathbb{Z}_p$. Bezeichne $\sigma \in \mathcal{G}_{\mathfrak{p}}$ einen Lift von $\sigma_{\mathfrak{p}}$ und τ einen Erzeuger von $\mathcal{T}_{\mathfrak{p}}$, so wird $\mathcal{G}_{\mathfrak{p}}$ durch σ und τ erzeugt und diese erfüllen die Relation

$$\tau^{\mathfrak{N}(\mathfrak{p})-1}[\tau, \sigma] = 1.$$

Es gilt

$$cd\ \mathcal{G}_{\mathfrak{p}} = 2.$$

Nach (3.1.1) und (3.1.2) gilt $\mathcal{T}_{\mathfrak{p}} \neq 1$ im Falle $\chi(\mathfrak{p}) \neq p$ genau dann, wenn $\delta_{\mathfrak{p}} = 1$ gilt. Hieraus erhalten wir das folgende

(3.1.3) Korollar. *Ist $\mathfrak{p}$ eine endliche Primstelle von k mit $\chi(\mathfrak{p}) \neq p$, so ist $\mathfrak{p}$ in der maximalen p-Erweiterung $k(p)$ von k unverzweigt.*

3.2 Der Fall $\chi(\mathfrak{p}) = p$

Wir betrachten nun die über p liegenden Primstellen. Für $\chi_{\mathfrak{p}}$ setzen wir $n_{\mathfrak{p}} = [k_{\mathfrak{p}} : \mathbb{Q}_p]$.

(3.2.1) Satz. *Ist $\chi(\mathfrak{p}) = p$ und $\delta_{\mathfrak{p}} = 0$, so ist $\mathcal{G}_{\mathfrak{p}}$ eine freie pro-p-Gruppe vom Rang*

$$h^1(\mathcal{G}_{\mathfrak{p}}) = n_{\mathfrak{p}} + 1.$$

$\mathcal{G}_{\mathfrak{p}}$ besitzt ein minimales Erzeugendensystem der Form $\{\sigma, \tau_1, \ldots, \tau_{n_{\mathfrak{p}}}\}$, wobei $\sigma \in \mathcal{G}_{\mathfrak{p}}$ einen Lift von $\sigma_{\mathfrak{p}}$ bezeichnet und $\tau_i \in \mathcal{T}_{\mathfrak{p}}, i = 1, \ldots, n_{\mathfrak{p}}$.

Wir wenden uns wieder dem Fall $\delta_{\mathfrak{p}} = 1$ zu, d.h. $k_{\mathfrak{p}}$ enthalte die p-ten Einheitswurzeln. Genauer bezeichne q die maximale Potenz von p, so dass $k_{\mathfrak{p}}$ die q-ten Einheitswurzeln enthält. Weiter sei $\hat{q}$ die maximale Potenz von p, so dass $k_{\mathfrak{p}}^{nr}(p)$ die $\hat{q}$-ten Einheitswurzeln enthält.

(3.2.2) Notation. *Das* **Normrestsymbol zur p-ten Potenz (,)** *definieren wir für $\alpha, \beta \in k_{\mathfrak{p}}^{\times}$ durch die Gleichung*

$$(\beta, k(\sqrt[p]{\alpha})|k)\sqrt[p]{\alpha} = (\alpha, \beta)\sqrt[p]{\alpha},$$

wobei $(\ , k(\sqrt[p]{\alpha})|k)$ das gewöhnliche lokale Normrestsymbol bezeichnet.

(3.2.3) Proposition. *Es gelte $\chi(\mathfrak{p}) = p$ und $\delta = 1$. Sei $\zeta_q \in k_{\mathfrak{p}}$ eine primitive q-te Einheitswurzel und q' die maximale p-Potenz, so dass die Erweiterung $k_{\mathfrak{p}}(\sqrt[q']{\zeta_q})|k_{\mathfrak{p}}$ unverzweigt ist. Ferner sei $g \in \mathbb{Z}$, so dass die Operation des Frobenius-Automorphimus σ von $k_{\mathfrak{p}}(\sqrt[q']{\zeta_q})|k_{\mathfrak{p}}$ durch*

$$\sigma\sqrt[q']{\zeta_q} = \sqrt[q']{\zeta_q}^{\,g}.$$

Dann gilt notwendig $g \equiv 1 \bmod q$ und es existiert eine Basis $\{\pi, \alpha_0, \ldots, \alpha_{n_{\mathfrak{p}}}\}$ von $k_{\mathfrak{p}}^{\times}/k_{\mathfrak{p}}^{\times q}$, so dass die folgenden Bedingungen erfüllt sind:

(i) *π ist Primelement von $k_{\mathfrak{p}}$.*

(ii) *Die Erweiterung $k_{\mathfrak{p}}(\sqrt[q]{\alpha_0})|k_{\mathfrak{p}}$ ist unverzweigt.*

(iii) *Es gilt $\alpha_i \in U_{\mathfrak{p}}$ für $1 \leq i \leq n_{\mathfrak{p}}$. Ist $n_{\mathfrak{p}} \equiv 1 \bmod 2$, so ist ferner $\alpha_0 \in U_{\mathfrak{p}}$.*

(iv) *Ist $n_{\mathfrak{q}} \equiv 0 \bmod 2$, so gilt*

$$\begin{aligned} (\alpha_0, \pi) &= \zeta_q, \\ (\alpha_{2i-1}, \alpha_{2i}) &= \zeta_q, \quad i = 1, \ldots, n_{\mathfrak{p}}/2 \end{aligned}$$

und $(x, y) = 1$ für alle anderen Paare von Basiselementen x und y. Ist $n_\mathfrak{p} \equiv 1 \bmod 2$, so gilt

$$\begin{aligned} (\alpha_0, \pi) = (\alpha_1, \pi) &= \zeta_q, \\ (\alpha_{2i}, \alpha_{2i+1}) &= \zeta_q, \quad i = 1, \ldots, (n_\mathfrak{p} - 1)/2 \end{aligned}$$

und $(x, y) = 1$ für alle anderen Paare von Basiselementen x und y.

(v) $\sigma \sqrt[q]{\alpha_0} = \zeta_q \sqrt[q]{\alpha_0}$.

(vi) $\zeta_q = \alpha_0^{(g-1)/q} \alpha_1^{q'}$.

(3.2.4) Bemerkung. Ist $n_\mathfrak{p} \equiv 1 \bmod 2$, so gilt im Fall $\chi(\mathfrak{p}) = p, \delta_\mathfrak{p} = 1$ notwendig $p = 2$ und mit den obigen Bezeichnungen haben wir

$$q = \hat{q} = 2, \quad \zeta_q = -1 \quad \text{und} \quad q' = g = 1.$$

Wir können nun für den Fall $\chi(\mathfrak{p}) = p, \delta = 1$ wieder hinreichend explizite Darstellungen für die Erzeuger und Relationen von $\mathcal{G}_\mathfrak{p}$ angeben.

(3.2.5) Satz. *Es gelte $\chi(\mathfrak{p}) = p$ und $\delta = 1$. Dann ist*

$$h^1(\mathcal{G}_\mathfrak{p}) = n_\mathfrak{p} + 2, \quad h^2(\mathcal{G}_\mathfrak{p}) = 1.$$

und

$$cd\ \mathcal{G}_\mathfrak{p} = 2.$$

Sei ζ_q bzw. $\zeta_{\hat{q}}$ eine primitive q-te bzw. eine primitive $\hat{q}$-te Einheitswurzel, so dass $\zeta_q = \zeta_{\hat{q}}^{\hat{q}q^{-1}}$. Ferner sei die ganze Zahl g gegeben durch

$$\sigma_\mathfrak{p} \zeta_{\hat{q}} = \zeta_{\hat{q}}^g.$$

Weiter sei $\{\pi, \alpha_0, \ldots, \alpha_{n_\mathfrak{p}}\}$ eine Basis von $k_\mathfrak{p}^\times / k_\mathfrak{p}^{\times q}$, die den Bedingungen von (3.2.3) genügt. Wir bezeichnen mit $\sigma \in \mathcal{G}_\mathfrak{p}$ einen Lift von $\sigma_\mathfrak{p}$ dessen Restklasse in $\mathcal{G}_\mathfrak{p}^{ab}$ durch $(\pi, k_\mathfrak{p}(p)^{ab}|k)$ gegeben ist. Für $i = 0, \ldots, n_\mathfrak{p}$ sei $\tau_i \in \mathcal{G}_\mathfrak{p}$ ein Lift von $(\alpha_i, k_\mathfrak{p}(p)^{ab}|k)$.

Dann gilt $\tau_i \in \mathcal{T}_\mathfrak{p}, i = 0, \ldots, n_\mathfrak{p}$ und die Menge $\{\sigma, \tau_0, \ldots, \tau_{n_\mathfrak{p}}\}$ bildet ein minimales Erzeugendensystem von $\mathcal{G}_\mathfrak{p}$. Ist

$$1 \longrightarrow R \longrightarrow F \longrightarrow \mathcal{G}_\mathfrak{p} \longrightarrow 1$$

eine minimale Darstellung von $\mathcal{G}_\mathfrak{p}$ und sind $s, t_0, \ldots, t_{n_\mathfrak{p}} \in F$ Urbilder von $\sigma, \tau_0, \ldots, \tau_{n_\mathfrak{p}}$, so kann die erzeugende Relation $r \in R$ von der Form

$$r = t_0^{g-1} t_1^{\hat{q}} [t_0, s][t_1, t_2] \cdots [t_{n_\mathfrak{p}-1}, t_{n_\mathfrak{p}}] r'$$

mit $r' \in F_{(3,q)} \cap [F, F]$ gewählt werden.

4 Beschränkte Verzweigung und vorgegebene Zerlegung

Sei k ein algebraischer Zahlkörper. Wir werden in den folgenden Kapiteln k stets als fest gewählten Grundkörper betrachten und daher darauf verzichten, die zugehörigen Idelgruppen und Idelklassengruppen stets mit k zu indizieren.

4.1 Das globale Normrestsymbol

Wir wollen zunächst einige Resultate der globalen Klassenkörpertheorie angeben. Für die Beweise verweisen wir auf die einschlägige Literatur, vgl. etwa [Ne1], oder [AT].

(4.1.1) Definition. *Die* **Idelgruppe** *I von k ist das restringierte Produkt*

$$I := \prod_{\mathfrak{p}} k_{\mathfrak{p}}^{\times},$$

wobei $\mathfrak{p}$ alle (endlichen und unendlichen) Primstellen von k durchläuft und das restringierte Produkt bezüglich der Einheitengruppen $U_{\mathfrak{p}} \subseteq k_{\mathfrak{p}}^{\times}$ gebildet ist. Die **Idelklassengruppe** *von k ist der Quotient*

$$C := I/k^{\times},$$

wobei wir die multiplikative Gruppe $k^{\times}$ als diagonal in I eingebettet betrachten.

Die Gruppe I ist in kanonischer Weise eine lokal kompakte topologische Gruppe. Eine Umgebungsbasis des Einselements ist gegeben durch

$$\prod_{\mathfrak{p} \in P} W_{\mathfrak{p}} \times \prod_{\mathfrak{p} \notin P} U_{\mathfrak{p}} \subseteq I,$$

wenn P alle endlichen, die unendlichen Stellen enthaltenden, Primstellenmengen und $W_{\mathfrak{p}}$ eine Umgebungsbasis von $1 \in k_{\mathfrak{p}}^{\times}$ durchläuft. Die multiplikative Gruppe $k^{\times}$ ist eine diskrete (und damit insbesondere abgeschlossene) Untergruppe von I. Folglich ist C eine lokal kompakte Hausdorffsche Gruppe.

Wir bezeichnen mit k^{ab} die maximale abelsche Erweiterung von k und setzen $G^{ab} := \mathrm{Gal}(k^{ab}|k)$. Nach Klassenkörpertheorie haben wir das ***universelle Normrestsymbol***

$$(\ ,k^{ab}|k):\ C \twoheadrightarrow G^{ab}.$$

Dieses ist surjektiv und stetig. Sei $D := \ker(\ ,k^{ab}|k)$ die ***Gruppe der universellen Normen von k***. Dann gilt

(i) D ist die Gruppe unendlich divisiblen Elemente von C, d.h.

$$D = \bigcap_{n \in \mathbb{N}} C^n.$$

(ii) D ist die Zusammenhangskomponente des Einselements in C.

Für eine Primstelle $\mathfrak{p}$ von k induziert die natürliche Inklusion $k_{\mathfrak{p}}^{\times} \hookrightarrow I$ eine topologische Einbettung $k_{\mathfrak{p}}^{\times} \hookrightarrow C$ und es gilt das folgende Zerlegungsgesetz:

(4.1.2) Proposition. *Für jede Primstelle $\mathfrak{p}$ von k bildet das Normrestsymbol $(\ ,k^{ab}|k)$ die Gruppe $k_{\mathfrak{p}}^{\times}$ surjektiv auf die Zerlegungsgruppe von G^{ab} bezüglich $\mathfrak{p}$ und die Einheitengruppe $U_{\mathfrak{p}}$ surjektiv auf die Trägheitsgruppe von G^{ab} bezüglich $\mathfrak{p}$ ab.*

4.2 Verallgemeinerte Idelklassen

(4.2.1) Definition. *Seien S und T zwei disjunkte Primstellen von k. T sei zudem endlich. Wir setzen*

$$I_S^T := \prod_{\mathfrak{p}\in S}\{1\} \times \prod_{\mathfrak{p}\in T} k_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p}\notin S\cup T} U_{\mathfrak{p}} \subseteq I$$

und

$$C_S^T := I/I_S^T k^{\times}.$$

Ist $S \neq \varnothing$, dann gilt $I_S^T \cap k^{\times} = 1$ und wir können I_S^T als Untergruppe von C auffassen und haben $C_S^T = C/I_S^T$.

4.3 Die Erweiterung $k_S^T|k$

Seien S und T Primstellenmengen von k, T sei endlich. Wir betrachten Erweiterungen von k, die außerhalb der Menge S unverzweigt und über der Menge T voll zerlegt sind. Komposita und normale Hüllen solcher Erweiterungen haben wieder diese Eigenschaft. Folglich existiert eine maximale außerhalb S unverzweigte, über T voll zerlegte Erweiterung k_S^T von k. Diese ist galoissch und wir setzen

$$\mathcal{G}_S^T := \mathrm{Gal}(k_S^T|k).$$

Ferner sei p eine fest gewählte Primzahl. Mit $k_S^T(p) \subseteq k_S^T$ bezeichnen wir die maximale außerhalb S unverzweigte, über T voll zerlegte pro-p-Erweiterung von k. Wir setzen

$$G_S^T(p) := \mathrm{Gal}(k_S^T(p)|k).$$

In den folgenden Abschnitten werden wir uns überwiegend auf das Studium von pro-p-Erweiterungen beschränken und wir schreiben daher abkürzend

$$G_S^T := G_S^T(p).$$

Weiter bezeichne $k_S^T[p]$ die maximale abelsche Zwischenerweiterung vom Exponenten p in $k_S^T(p)$ und $G_S^T[p]$ ihre Galoisgruppe über k. Es ist also

$$G_S^T[p] = G_S^T/\,\mathrm{Fr}(G_S^T),$$

wobei $\mathrm{Fr}(G_S^T) = [G_S^T, G_S^T](G_S^T)^p$ wieder die Frattini-Untergruppe von G_S^T bezeichnet.

(4.3.1) Definition. *Mit S_∞ bezeichnen wir die Menge der unendlichen Primstellen von k. Mit $S_\mathbb{R}$ bzw. $S_\mathbb{C}$ bezeichnen wir die Menge der reellen bzw. komplexen Primstellen von k und wir setzen*

$$r := |S_\infty|, \quad r_\mathbb{R} := |S_\mathbb{R}|, \quad r_\mathbb{C} := |S_\mathbb{C}|.$$

Für reelle Primstellen treffen wir die folgende Konvention: Die Erweiterung $\mathbb{C}|\mathbb{R}$ sehen wir als verzweigt an, d.h. eine reelle Primstelle $\mathfrak{p}$ ist in einer Erweiterung $L|k$ genau dann unverzweigt, wenn sie voll zerlegt ist, d.h. wenn $L_\mathfrak{p} = k_\mathfrak{p} = \mathbb{R}$. Wir können daher ferner ohne Einschränkung annehmen, dass die Menge T nur endliche Primstellen enthält.

In einer Erweiterung $L|k$ sind voll zerlegte Primstellen insbesondere unverzweigt und wir können daher ohne Einschränkung annehmen, dass die Primstellenmengen S und T disjunkt sind.

(4.3.2) Notation. *Für zwei Primstellenmengen S und T schreiben wir,* ***S* und *T* haben die Eigenschaft ($*$)***, falls folgende Bedingungen erfüllt sind:*

(i) $|T| < \infty$,

(ii) $S \cap T = \varnothing$,

(iii) $T \cap S_\infty = \varnothing$.

(4.3.3) Notation. *Für $T = \varnothing$ setzen wir*

$$k_S = k_S^\varnothing,\ \mathcal{G}_S = \mathcal{G}_S^\varnothing,\ G_S = G_S^\varnothing,\ I_S = I_S^\varnothing \quad \textit{und} \quad C_S = C_S^\varnothing.$$

Wir bezeichnen mit D_S die Zusammenhangskomponente des Einselements in C_S. Für den Fall $S \supseteq S_\infty$ haben wir die folgende

(4.3.4) Proposition. *Sei S eine Primstellenmenge von k, die die unendlichen Stellen enthält. Dann gilt*

(i) $D_S = DI_S/I_S$.

(ii) *D_S ist divisibel.*

(iii) *Wir haben die exakte Sequenz topologischer Gruppen*

$$0 \longrightarrow D_S \longrightarrow C_S \xrightarrow{(\ ,(k_S)^{ab}|k)} (\mathcal{G}_S)^{ab} \longrightarrow 0,$$

wobei $(\ ,(k_S)^{ab}|k)$ *durch* $C \xrightarrow{(\ ,k^{ab}|k)} G^{ab} \twoheadrightarrow (\mathcal{G}_S)^{ab}$ *induziert wird.*

Beweis. Für den Beweis verweisen wir auf [NSW], Chap. VIII, (8.3.12). □

(4.3.5) Satz. *Für beliebige Primstellenmengen S, T mit Eigenschaft ($*$) hat man den algebraischen wie topologischen Isomorphismus*

$$G_S^T/\operatorname{Fr}(G_S^T) \cong I/I_S^T I^p k^\times.$$

Beweis. Wir betrachten zunächst den Fall $S \supseteq S_\infty, T = \varnothing$. Nach (4.3.4) (iii) haben wir den Isomorphismus topologischer Gruppen

$$(\mathcal{G}_S)^{ab} \cong C_S/D_S.$$

Ferner ist D_S nach (4.3.4) (ii) divisibel und folglich

$$(\mathcal{G}_S)^{ab}/((\mathcal{G}_S)^{ab})^p \cong C_S/D_S(C_S)^p = C_S/(C_S)^p = I/I_S I^p k^\times.$$

Die Behauptung folgt nun wegen $G_S/\operatorname{Fr}(G_S) = (\mathcal{G}_S)^{ab}/((\mathcal{G}_S)^{ab})^p$.

Seien nun S und T beliebig mit Eigenschaft $(*)$. Wir setzen

$$H = \operatorname{Gal}(k_{S\cup S_\infty}[p]|k_S^T[p]).$$

Für jede Primstelle $\mathfrak{p}$ von k wählen wir eine über $\mathfrak{p}$ liegende Primstelle $\mathfrak{P}$ von $k_{S\cup S_\infty}[p]$. Ferner sei $T' = T \cup (S_\mathbb{R} \setminus S)$. H ist damit gerade die von den Zerlegungsuntergruppen $H_\mathfrak{P}, \mathfrak{p} \in T'$ erzeugte Untergruppe von $G^T_{S\cup S_\infty}[p] = G^T_{S\cup S_\infty}/\operatorname{Fr}(G^T_{S\cup S_\infty})$. Nach (4.1.2) haben wir den surjektiven stetigen Homomorphismus

$$\varphi:\ I_S^T \twoheadrightarrow \prod_{\mathfrak{p}\in T'} k_\mathfrak{p}^\times \twoheadrightarrow H,$$

Die Verträglichkeit des globalen Normrestsymbols mit den lokalen Normrestsymbolen (vgl. etwa [Ne1], Kap. III, (6.15)) impliziert die Kommutativität des exakten Diagramms topologischer Gruppen

$$\begin{tikzcd}
 & I_S^T \arrow[r] \arrow[d] & I/I_{S\cup S_\infty} I^p k^\times \arrow[r] \arrow[d, "\wr"] & I/I_S^T I^p k^\times \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & H \arrow[r] & G_{S\cup S_\infty}/\operatorname{Fr}(G_{S\cup S_\infty}) \arrow[r] & G_S^T/\operatorname{Fr}(G_S^T) \arrow[r] & 1.
\end{tikzcd}$$

Das Schlangenlemma liefert die Behauptung. □

4.4 Verallgemeinerte Idealklassen

In den folgenden Kapiteln werden wir die Resultate aus der Klassenkörpertheorie sämtlich ideltheoretisch formulieren. An dieser Stelle sei jedoch für die Gruppe $I/I_S^T I^p k^\times$ die idealtheoretische Entsprechung angegeben. Ein ausführliches Kalkül mit verallgemeinerten Idealklassengruppen findet sich beispielsweise in [Gr].

(4.4.1) Definition. *Ein* **Modul** $\mathfrak{m}$ *ist ein formales Produkt*

$$\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{n_\mathfrak{p}}, \quad n_\mathfrak{p} \in \mathbb{N}_0,$$

wobei $\mathfrak{p}$ *alle Primstellen von* k *durchläuft,* $n_\mathfrak{p} = 0$ *für fast alle* $\mathfrak{p}$ *gilt und* $n_\mathfrak{p} \in \{0,1\}$ *für* $\mathfrak{p} \in S_\infty$. *Wir schreiben*

$$\mathfrak{m} \in \langle S\rangle,$$

falls $n_\mathfrak{p} = 0$ *für alle* $\mathfrak{p} \notin S$.

(4.4.2) Definition. *Für einen Modul* $\mathfrak{m} = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}} \in \langle S \rangle$ *setzen wir*

$$I_{\mathfrak{m}}^T := \prod_{\mathfrak{p}|\mathfrak{m}} U_{\mathfrak{p}}^{n_{\mathfrak{p}}} \times \prod_{\mathfrak{p}\in T} k_{\mathfrak{p}}^{\times} \times \prod_{\mathfrak{p}\nmid\mathfrak{m},\mathfrak{p}\notin T} U_{\mathfrak{p}},$$

wobei wir für endliche Primstellen mit $U_{\mathfrak{p}}^{n_{\mathfrak{p}}}$ *die höheren Einseinheitengruppen bezeichnen und für unendliche Primstellen setzen:*

$$U_{\mathfrak{p}}^{m_{\mathfrak{p}}} = \begin{cases} \mathbb{R}_+^{\times}, & \textit{falls } \mathfrak{p} \textit{ reell und } m_{\mathfrak{p}} = 1, \\ \mathbb{R}^{\times}, & \textit{falls } \mathfrak{p} \textit{ reell und } m_{\mathfrak{p}} = 0, \\ \mathbb{C}^{\times}, & \textit{falls } \mathfrak{p} \textit{ komplex ist.} \end{cases}$$

Für $x \in k^{\times}$ *schreiben wir ferner*

$$x \equiv 1 \bmod \mathfrak{m} :\Longleftrightarrow x \in U_{\mathfrak{p}}^{n_{\mathfrak{p}}} \textit{ für alle } \mathfrak{p}.$$

(4.4.3) Satz.

$$I/I_S^T I^p k^{\times} = \varprojlim_{\mathfrak{m}\in\langle S\rangle} Cl_{\mathfrak{m}}^T/(Cl_{\mathfrak{m}}^T)^p.$$

Beweis. Wir betrachten zunächst einen festen Modul $\mathfrak{m} \in \langle S \rangle$ und setzen

$$Cl_{\mathfrak{m}}^T := \mathcal{I}_{\mathfrak{m}}/\mathcal{H}_{\mathfrak{m}}\langle T \rangle.$$

Hierbei bezeichnet $\mathcal{I}_{\mathfrak{m}}$ die Gruppe der zu $\mathfrak{m}$ teilerfremden (gebrochenen) Ideale von k, $\langle T \rangle$ die von den Primidealen $\mathfrak{p} \in T$ erzeugte Untergruppe und

$$\mathcal{H}_{\mathfrak{m}} := \big\{(x) | x \in k^{\times},\ x \equiv 1 \bmod \mathfrak{m}\big\}.$$

Sei nun $I^{\langle\mathfrak{m}\rangle} := \{\mathfrak{a} \in I | \mathfrak{a}_{\mathfrak{p}} = 1 \text{ für alle } \mathfrak{p}|\mathfrak{m}\}$. Wir betrachten den Homomorphismus

$$\begin{aligned} \varphi : I^{\langle\mathfrak{m}\rangle} &\longrightarrow Cl_{\mathfrak{m}}^T, \\ \mathfrak{a} &\longmapsto \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{v_{\mathfrak{p}}(\mathfrak{a}_{\mathfrak{p}})}. \end{aligned}$$

φ ist offensichtlich surjektiv. Es ist $\mathfrak{a} \in \ker\varphi \subseteq I^{\langle\mathfrak{m}\rangle}$ genau dann, wenn ein $x \in \mathcal{H}_{\mathfrak{m}}$ existiert mit $x^{-1}\varphi(\mathfrak{a}) \in \langle T \rangle$ und damit

$$x^{-1}\mathfrak{a} \in I_{\varnothing}^T = \big\{\mathfrak{b} \in I | \mathfrak{b}_{\mathfrak{p}} \in U_{\mathfrak{p}}, \mathfrak{p} \notin T\big\}.$$

Folglich ist kern $\varphi = I_{\varnothing}^T \mathcal{H}_{\mathfrak{m}} \cap I^{\langle\mathfrak{m}\rangle}$ und man rechnet leicht nach, dass

$$I^T \mathcal{H}_{\mathfrak{m}} \cap I^{\langle\mathfrak{m}\rangle} = I_{\mathfrak{m}}^T k^{\times} \cap I^{\langle\mathfrak{m}\rangle}.$$

Wir haben also den Isomorphismus

$$I^{\langle\mathfrak{m}\rangle}/I_{\mathfrak{m}}^T k^{\times} \cap I^{\langle\mathfrak{m}\rangle} \cong I^{\langle\mathfrak{m}\rangle} I_{\mathfrak{m}}^T k^{\times}/I_{\mathfrak{m}}^T k^{\times} \cong Cl_{\mathfrak{m}}^T.$$

Wir zeigen nun die Gleichung $I^{\langle\mathfrak{m}\rangle} I^T_{\mathfrak{m}} k^\times = I$. Sei hierfür $\mathfrak{b} \in I$. Nach dem Approximationssatz existiert ein $y \in k^\times$ mit $y\mathfrak{b}_{\mathfrak{p}}^{-1} \in U_{\mathfrak{p}}^{m_{\mathfrak{p}}}$ für alle $\mathfrak{p} \mid \mathfrak{m}$. Seien die beiden Idele $\mathfrak{b}_1, \mathfrak{b}_2$ gegeben durch

$$(\mathfrak{b}_1)_{\mathfrak{p}} = 1,\ (\mathfrak{b}_2)_{\mathfrak{p}} = y^{-1}\mathfrak{b}_{\mathfrak{p}}, \quad \text{für } \mathfrak{p} \mid \mathfrak{m} \text{ bzw.}$$
$$(\mathfrak{b}_1)_{\mathfrak{p}} = y^{-1}\mathfrak{b}_{\mathfrak{p}},\ (\mathfrak{b}_2)_{\mathfrak{p}} = 1, \quad \text{für } \mathfrak{p} \nmid \mathfrak{m}.$$

Offensichtlich gilt dann $\mathfrak{b}_1 \in I^{\langle\mathfrak{m}\rangle}$, $\mathfrak{b}_2 \in I_{\mathfrak{m}} \subseteq I^T_{\mathfrak{m}}$ und $y\mathfrak{b}_1\mathfrak{b}_2 = \mathfrak{b}$. Zusammenfassend erhalten wir also den Isomorphismus $I/I^T_{\mathfrak{m}} k^\times \cong Cl^T_{\mathfrak{m}}$ und damit

$$I/I^T_{\mathfrak{m}} I^p k^\times \cong Cl^T_{\mathfrak{m}}/(Cl^T_{\mathfrak{m}})^p.$$

Der Existenzsatz der globalen Klassenkörpertheorie (vgl. etwa [Ne1], Kap. III, (7.9)) liefert $I/I^T_S I^p k^\times \cong \varprojlim_{\mathfrak{m}\in\langle S\rangle} I/I^T_{\mathfrak{m}} I^p k^\times$ und wir erhalten die Behauptung. □

5 Der Erzeugerrang $h^1(G_S^T)$

Sei p eine Primzahl. Seien k ein algebraischer Zahlkörper und S, T zwei Primstellenmengen von k mit Eigenschaft $(*)$. Für eine pro-p-Gruppe G setzen wir gemäß (2.2.4)

$$H^i(G) = H^i(G, \mathbb{Z}/p\mathbb{Z}) \text{ und } h^i(G) = \dim_{\mathbb{F}_p} H^i(G), \quad i \geq 0.$$

Im Folgenden soll der Erzeugerrang $h^1(G_S^T)$ der Gruppe G_S^T berechnet werden.

Nun gilt aber $H^1(G_S^T) = H^1(G_S^T/\operatorname{Fr}(G_S^T))$ und folglich nach (4.3.5)

$$H^1(G_S^T) = H^1(I/I_S^T I^p k^\times).$$

Nach (3.1.3) können folgende Primstellen in einer p-Erweiterung nicht verzweigen:

(i) komplexe Primstellen,

(ii) reelle Primstellen, falls $p \neq 2$,

(iii) endliche Primstellen $\mathfrak{p} \nmid p$ mit $\mathfrak{N}(\mathfrak{p}) \not\equiv 1 \bmod p$.

Entfernt man diese Primstellen aus S, so erhält man eine Primstellenmenge $S_{\min} \subseteq S$ mit $k_{S_{\min}}^T(p) = k_S^T(p)$ und folglich $G_{S_{\min}}^T = G_S^T$. Wir nehmen daher im Folgenden an, dass $S = S_{\min}$.

5.1 Die Kummergruppen V_S^T und die exakte 5-Term-Sequenz

(5.1.1) Definition. *Wir setzen*

$$\delta := \begin{cases} 1, & \text{falls } \mu_p \subseteq k, \\ 0, & \text{falls } \mu_p \not\subseteq k \end{cases} \qquad \text{und} \quad \delta_{\mathfrak{p}} := \begin{cases} 1, & \text{falls } \mu_p \subseteq k_{\mathfrak{p}}, \\ 0, & \text{falls } \mu_p \not\subseteq k_{\mathfrak{p}} \end{cases}$$

für eine Primstelle $\mathfrak{p}$ von k.

S_p bezeichne die Menge der über p liegenden Primstellen von k. Wir orientieren uns an der Berechnung des Erzeugerrangs der Gruppe G_S, der Galoisgruppe der maximalen außerhalb S unverzweigten p-Erweiterung von k, vgl. [Ko], Chap. 11.

(5.1.2) Definition. *Wir definieren die* **Kummergruppen** V_S^T *durch*

$$V_S^T = U_S^T/k^{\times p},$$

wobei

$$\begin{aligned} U_S^T &= \{a \in k^\times | a \in k_{\mathfrak{p}}^{\times p} \text{ für } \mathfrak{p} \in S \text{ und } a \in U_{\mathfrak{p}} k_{\mathfrak{p}}^{\times p} \text{ für } \mathfrak{p} \notin S \cup T\} \\ &= k^\times \cap (I_S^T I^p). \end{aligned}$$

Ferner setzen wir

$$Б_S^T = (V_S^T)^* = \operatorname{Hom}(V_S^T, \mathbb{Z}/p\mathbb{Z}).$$

(5.1.3) Proposition. *Man hat eine exakte Sequenz*

$$\begin{tikzcd} 1 \arrow[r] & V_S^T \arrow[r] & V_\varnothing^T \arrow[r, "\varphi_1"] & I_\varnothing^T/I_S^T I_\varnothing^p \arrow[d, "\varphi_2"] \\ & 1 & I/I_\varnothing^T I^p k^\times \arrow[l] & I/I_S^T I^p k^\times \arrow[l, "\varphi_3"'] \end{tikzcd}$$

Beweis. Nach Definition ist $U_S^T = k^\times \cap (I_S^T I^p)$ und der kanonische Homomorphismus $V_S^T \to V_\varnothing^T$ ist injektiv. Der Homomorphismus φ_1 ist wie folgt gegeben: Sei $xk^{\times p} \in V_\varnothing^T$, $x = \mathfrak{a}\mathfrak{b} \in k^\times$ mit $\mathfrak{a} \in I_\varnothing^T$, $\mathfrak{b} \in I^p$. Dann liefert $\varphi_1(xk^{\times p}) := \mathfrak{a} I_S^T I_\varnothing^p$ einen wohldefinierten Homomorphismus $\varphi_1 : V_\varnothing^T \to I_\varnothing^T/I_S^T I_\varnothing^p$ mit Kern V_S^T. Man rechnet weiter leicht nach, dass $\ker(\varphi_2) = (I_\varnothing^T \cap k^\times I^p) I_S^T I_\varnothing^p / I_S^T I_\varnothing^p = \mathrm{im}(\varphi_1)$ und $\ker(\varphi_3) = I_\varnothing^T I^p k^\times / I_S^T I^p k^\times = \mathrm{im}(\varphi_3)$. Die Surjektivität von φ_3 ist klar. □

Im Folgenden bezeichne wieder $\mathcal{G}_\mathfrak{p} = \mathrm{Gal}(k_\mathfrak{p}(p)|k_\mathfrak{p})$ die Galoisgruppe der maximalen p-Erweiterung $k_\mathfrak{p}(p)$ von $k_\mathfrak{p}$ und $\mathcal{T}_\mathfrak{p}$ ihre Trägheitsuntergruppe.

(5.1.4) Satz. *Man hat die exakte Sequenz von $\mathbb{F}_p$-Vektorräumen*

$$\begin{tikzcd} 0 \arrow[r] & H^1(G_\varnothing^T) \arrow[r] & H^1(G_S^T) \arrow[r] & \bigoplus_{\mathfrak{p}\in S} H^1(\mathcal{T}_\mathfrak{p})^{\mathcal{G}_\mathfrak{p}} \arrow[d] \\ & 0 & Б_S^T \arrow[l] & Б_\varnothing^T \arrow[l] \end{tikzcd}$$

Beweis. Der natürliche surjektive Homomorphismus

$$I_\varnothing^T \longrightarrow \prod_{\mathfrak{p}\in S} U_\mathfrak{p}/U_\mathfrak{p}^p\,, \qquad \mathfrak{a} = (a_\mathfrak{p}) \longmapsto (a_\mathfrak{p} U_\mathfrak{p}^p)_{\mathfrak{p}\in S}$$

hat den Kern $I_S^T I_\varnothing^p$ und wir haben damit die Isomorphie

$$I_\varnothing^T/I_S^T I_\varnothing^p \cong \prod_{\mathfrak{p}\in S} U_\mathfrak{p}/U_\mathfrak{p}^p.$$

Das lokale Normrestsymbol induziert ferner einen Isomorphismus

$$(U_\mathfrak{p}/U_\mathfrak{p}^p)^* \cong (\mathcal{T}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}^p\,[\mathcal{T}_\mathfrak{p}, \mathcal{G}_\mathfrak{p}])^* = H^1(\mathcal{T}_\mathfrak{p})^{\mathcal{G}_\mathfrak{p}}.$$

Alle in der exakten Sequenz von (5.1.3) auftretenden Gruppen sind kompakt und die gewünschte Sequenz ergibt sich durch Dualisieren. □

5.2 Berechnung des Erzeugerrangs von G_S^T

Wir formulieren nun den Dirichletschen Einheitensatz für T-Einheiten.

(5.2.1) Proposition. *Der Homomorphismus*

$$\log:\ k_\varnothing^T \longrightarrow \prod_{\mathfrak{p}\in T\cup S_\infty} \mathbb{R}, \qquad x \longmapsto (\log|x|_\mathfrak{p})_{\mathfrak{p}\in T\cup S_\infty}$$

hat den Kern $\mu(k)$ sowie als Bild ein vollständiges Gitter im $(|T|+r-1)$-dimensionalen Spur-Null-Raum

$$H = \{y = (y_\mathfrak{p})_{\mathfrak{p}\in T\cup S_\infty} \,|\, \operatorname{tr} y = \sum_{\mathfrak{p}\in T\cup S_\infty} y_\mathfrak{p} = 0\}.$$

Beweis. Für den Beweis verweisen wir auf [Ne3] Kap. VI, (1.1) bzw. [La2] Chap. V, §1. □

(5.2.2) Proposition. *Es gilt*

$$\dim_{\mathbb{F}_p} \text{Б}_\varnothing^T = \dim_{\mathbb{F}_p} H^1(G_\varnothing^T) + \delta + |T| + r - 1.$$

Beweis. Wir betrachten den wohldefinierten Homomorphismus

$$\begin{array}{rcl} k^\times \cap I^p I_\varnothing^T & \longrightarrow & {}_p(I/I_\varnothing^T k^\times), \\ x = \mathfrak{a}^p\mathfrak{b} & \longmapsto & \mathfrak{a} I_\varnothing^T k^\times, \quad \text{wobei } \mathfrak{b} \in I_\varnothing^T, \end{array}$$

wobei ${}_p(I/I_\varnothing^T k^\times)$ die Untergruppe der Elemente der Ordnung p von $I/I_\varnothing^T k^\times$ bezeichnet. Dieser ist surjektiv, faktorisiert über $k^{\times p}$ und wir haben die exakte Sequenz

$$1 \longrightarrow k_\varnothing^{\times T}/(k_\varnothing^{\times T})^p \longrightarrow V_\varnothing^T \longrightarrow {}_p(I/I_\varnothing^T k^\times) \longrightarrow 1\ .$$

$I/I_\varnothing^T k^\times$ ist ein Faktor der Idealklassengruppe $Cl(k) \cong I/I_\varnothing k^\times$ und damit insbesondere endlich. Daher gilt mit (4.3.5)

$$\left({}_p(I/I_\varnothing^T k^\times)\right)^* = H^1\left({}_p(I/I_\varnothing^T k^\times)\right) = H^1(I/I_\varnothing^T I^p k^\times) \cong H^1(G_\varnothing^T)$$

und wir erhalten die exakte Sequenz

$$1 \longrightarrow H^1(G_\varnothing^T) \longrightarrow \text{Б}_\varnothing^T \longrightarrow \left(k_\varnothing^{\times T}/(k_\varnothing^{\times T})^p\right)^* \longrightarrow 1\ .$$

Nach (5.2.1) gilt $k_\varnothing^\times \cong \mu_p \oplus \mathbb{Z}^{|T|+r-1}$ und damit $\dim_{\mathbb{F}_p}\left(k_\varnothing^{\times T}/(k_\varnothing^{\times T})^p\right)^* = \delta + |T| + r - 1$, was die Behauptung liefert. □

Für den Erzeugerrang $h^1(G_S^T)$ erhalten wir den folgenden

(5.2.3) Satz. *Seien S, T Primstellenmengen von k mit Eigenschaft $(*)$ und es gelte $S = S_{\min}$. Dann ist $h^1(G_S^T)$ genau dann endlich, wenn S endlich ist. In diesem Fall gilt*

$$h^1(G_S^T) = \sum_{\mathfrak{p}\in S\cap S_p} [k_\mathfrak{p} : \mathbb{Q}_p] - \delta - r - |T| + 1 + \sum_{\mathfrak{p}\in S} \delta_\mathfrak{p} + \dim_{\mathbb{F}_p} \text{Б}_S^T.$$

Beweis. Im Beweis von (5.2.2) haben wir gesehen, dass die Gruppen $H^1(G_\varnothing^T)$ und $\text{Б}_\varnothing^T$ endlich sind. Ferner hat man die Inklusion $V_S^T \subseteq V_\varnothing^T$ und damit ist auch Б_S^T endlich. Folglich ist nach (5.1.3) $H^1(G_S^T)$ genau dann endlich-dimensional, wenn $\bigoplus_{\mathfrak{p}\in S} H^1(\mathcal{T}_\mathfrak{p})^{\mathcal{G}_\mathfrak{p}}$ endlich-dimensional ist. Nun gilt für eine Primstelle $\mathfrak{p} \in S$

$$\dim_{\mathbb{F}_p} H^1(\mathcal{T}_\mathfrak{p})^{\mathcal{G}_\mathfrak{p}} = \dim_{\mathbb{F}_p} U_\mathfrak{p}/U_\mathfrak{p}^p = \begin{cases} \delta_\mathfrak{p}, & \text{falls } \mathfrak{p} \notin S_p, \\ \delta_\mathfrak{p} + [k_\mathfrak{p} : \mathbb{Q}_\mathfrak{p}], & \text{falls } \mathfrak{p} \in S_p. \end{cases} \tag{5.1}$$

Wegen $S = S_{\min}$ gilt $\delta_\mathfrak{p} = 1$ für alle $\mathfrak{p} \in S \setminus (S_p \cup S_\infty)$ und folglich ist $h^1(G_S^T)$ genau dann endlich, wenn S endlich ist. Mit (5.1.4) erhalten wir in diesem Fall

$$h^1(G_S^T) = h^1(G_\varnothing^T) + \sum_{\mathfrak{p}\in S\cap S_p} [k_\mathfrak{p} : \mathbb{Q}_p] + \sum_{\mathfrak{p}\in S} \delta_\mathfrak{p} - \dim_{\mathbb{F}_p} \text{Б}_\varnothing^T + \dim_{\mathbb{F}_p} \text{Б}_S^T.$$

Die gewünschte Gleichung ergibt sich nun aus (5.2.2).

□

(5.2.4) Bemerkung. Die Bedingung $S = S_{\min}$ wurde im obigen Beweis lediglich für die Gleichung ((5.1)) verwendet. Diese gilt jedoch auch für endliche Primstellen $\mathfrak{p} \nmid p$ mit $\mathfrak{N}(\mathfrak{p}) \not\equiv 1 \bmod p$ und für reelle Primstellen bei ungeradem p, denn im letzteren Fall ist $U_\mathfrak{p} = \mathbb{R}^\times = U_\mathfrak{p}^p$ und $\delta_\mathfrak{p} = 0$. (5.2.3) gilt somit für beliebige endliche Primstellenmengen S mit $S \cap S_\mathbb{C} = \varnothing$, wobei $S_\mathbb{C}$ die Menge der komplexen Primstellen bezeichnet.

Wir werden uns nun von der Bedingung $S = S_{\min}$ lösen und betrachten Primstellenmengen S, die alle über p liegenden und alle unendlichen Primstellen enthalten.

(5.2.5) Korollar. *Seien S, T Primstellenmengen von k mit Eigenschaft $(*)$, ferner sei S endlich und $S \supseteq S_p \cup S_\infty$. Dann gilt*

$$h^1(G_S^T) = 1 + \sum_{\mathfrak{p}\in S} \delta_\mathfrak{p} - \delta - |T| + \dim_{\mathbb{F}_p} \text{Б}_S^T.$$

Beweis. Sei $\tilde{S} := S \setminus S_\mathbb{C}$. Dann gilt $G_S^T = G_{\tilde{S}}^T$ und wegen $I^p I_S^T = I^p I_{\tilde{S}}^T$ ist ferner $\text{Б}_S^T = \text{Б}_{\tilde{S}}^T$. Wegen $S_p \subseteq \tilde{S}$ gilt $\sum_{\mathfrak{p}\in\tilde{S}\cap S_p} [k_\mathfrak{p} : \mathbb{Q}_p] = [k : \mathbb{Q}]$ und aus (5.2.3) folgt mit (5.2.4)

$$\begin{aligned} h^1(G_S^T) = h^1(G_{\tilde{S}}^T) &= 1 + \sum_{\mathfrak{p}\in\tilde{S}} \delta_\mathfrak{p} + [k : \mathbb{Q}] - r - \delta - |T| + \dim_{\mathbb{F}_p} \text{Б}_{\tilde{S}}^T \\ &= 1 + \sum_{\mathfrak{p}\in S} \delta_\mathfrak{p} - \delta - |T| + \dim_{\mathbb{F}_p} \text{Б}_S^T. \end{aligned}$$

□

Für $T = \varnothing$ erhalten wir die bekannten Gleichungen für den Erzeugerrang von $G_S := G_S^\varnothing$, der Galoisgruppe der maximalen außerhalb S unverzweigten p-Erweiterung von k (vlg. [NSW] bzw. [Ko]). Hierzu setzen wir $\text{Б}_S := \text{Б}_S^\varnothing$.

(5.2.6) Korollar. *Sei S eine beliebige endliche Menge von Primstellen von k.*

(i) Für $S = S_{\min}$ gilt

$$h^1(G_S) = \sum_{\mathfrak{p} \in S \cap S_p} [k_{\mathfrak{p}} : \mathbb{Q}_p] - \delta - r + 1 + \sum_{\mathfrak{p} \in S} \delta_{\mathfrak{p}} + \dim_{\mathbb{F}_p} \text{Б}_S.$$

(ii) Für $S \supseteq S_p \cup S_\infty$ gilt

$$h^1(G_S) = 1 + \sum_{\mathfrak{p} \in S} \delta_{\mathfrak{p}} - \delta + \dim_{\mathbb{F}_p} \text{Б}_S.$$

6 Der Relationenrang $h^2(G_S^T)$

Wir behalten die Notationen der vorangehenden Kapitel bei. In diesem Kapitel möchten wir nun den Relationenrang $h^2(G_S^T) = \dim_{\mathbb{F}_p} H^2(G_S^T, \mathbb{Z}/p\mathbb{Z})$ bestimmen.

6.1 Die Lokalisierungsabbildungen $\varphi^i_{S,T}$

Wir legen zunächst folgende Notationen fest:

Für jede Primstelle $\mathfrak{p}$ von k fixieren wir eine über $\mathfrak{p}$ liegende Primstelle $\mathfrak{P}$ in der maximalen p-Erweiterung $k(p)$ von k . Dies entspricht der Wahl einer k-Einbettung $i_\mathfrak{p} : k(p) \hookrightarrow k_\mathfrak{p}(p)$, wobei $k_\mathfrak{p}(p)$ wieder die maximale p-Erweiterung des lokalen Körpers $k_\mathfrak{p}$ bezeichnet. Für jede Zwischenerweiterung $K|k$ in $k(p)$ schreiben wir $K_\mathfrak{p} := i_\mathfrak{p}(K)k_\mathfrak{p}$. Ist $K|k$ endlich, so stimmt $K_\mathfrak{p}$ mit dem Körper $K_{\mathfrak{P}_K}$ überein, der Vervollständigung von K an der unter $\mathfrak{P}$ liegenden Primstelle $\mathfrak{P}_K$. Wir setzen $G := \mathrm{Gal}(k(p)|k)$ und $\mathcal{G}_\mathfrak{p} := \mathrm{Gal}(k_\mathfrak{p}(p)|k_\mathfrak{p})$, $\varphi_\mathfrak{p} : \mathcal{G}_\mathfrak{p} \to G$ bezeichne den von $i_\mathfrak{p}$ induzierten Homomorphismus.

Mit $\mathcal{T}_\mathfrak{P}$ bzw. $\mathcal{G}_\mathfrak{P}$ bezeichnen wir die Trägheits- bzw. Zerlegungsgruppe von $\mathfrak{P}$ in $k(p)$, $\mathcal{T}_\mathfrak{p}$ bezeichne wieder die Trägheitsuntergruppe von $\mathcal{G}_\mathfrak{p}$. Ist $\mathfrak{p}$ eine komplexe Primstelle, so ist $\mathcal{G}_\mathfrak{p} = \mathcal{T}_\mathfrak{p} = 1$, für eine reelle Primstelle $\mathfrak{p}$ ist im Falle $p \neq 2$ ebenfalls $\mathcal{G}_\mathfrak{p} = \mathcal{T}_\mathfrak{p} = 1$ und $\mathcal{G}_\mathfrak{p} = \mathcal{T}_\mathfrak{p} = \mathrm{Gal}(\mathbb{C}|\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$, falls $p = 2$.

Bezeichne $\varphi^i_\mathfrak{p} : H^i(G) \to H^i(\mathcal{G}_\mathfrak{p})$ den von $\varphi_\mathfrak{p}$ induzierten Homomorphismus. Ferner setzen wir

$$H^i_{nr}(\mathcal{G}_\mathfrak{p}) := \mathrm{im}(\ H^i(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}) \xrightarrow{inf} H^i(\mathcal{G}_\mathfrak{p})\ ).$$

(6.1.1) Proposition. *Für $i \geq 0$ induzieren die Homomorphismen $\varphi^i_\mathfrak{p}$ einen wohldefinierten Homomorphismus*

$$\varphi^i :\ H^i(G) \longrightarrow \prod_\mathfrak{p}{}' H^i(\mathcal{G}_\mathfrak{p})\ ,$$

wobei das restringierte Produkt bezüglich der Untergruppen $H^i_{nr}(\mathcal{G}_\mathfrak{p})$ von $H^i(\mathcal{G}_\mathfrak{p})$ gebildet ist und $\mathfrak{p}$ alle Primstellen von k durchläuft.

Beweis. Nach [NSW], Chap. I, (1.2.6). ist

$$H^i(G) = \varinjlim_U H^i(G/U),$$

wobei U die offenen normalen Untergruppen von G durchläuft. Sei nun $x \in H^i(G)$. Nach obiger Isomorphie können wir x als ein Element in $H^i(G/U)$

für eine offene normale Untergruppe U von G auffassen. Die zu U gehörige Zwischenerweiterung $L|k$ von $k_S^T(p)$ ist endlich und folglich sind in L fast alle Primstellen von k unverzweigt, d.h. der Homomorphismus

$$\mathcal{G}_\mathfrak{p} \longrightarrow G \longrightarrow\!\!\!\!\!\rightarrow G/U$$

faktorisiert über $\mathcal{T}_\mathfrak{p}$ für fast alle $\mathfrak{p}$ und folglich ist $\varphi_\mathfrak{p}^i(x) \in H_{nr}^i(\mathcal{G}_\mathfrak{p})$ für fast alle $\mathfrak{p}$. □

(6.1.2) Bemerkung. Für eine endliche Primstelle $\mathfrak{p}$ ist $\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p} \cong \mathbb{Z}_p$ und für eine unendliche Primstelle $\mathfrak{p}$ ist $\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p} = 1$. In jedem Fall ist $H^2(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}) = 0$ und wir haben

$$\prod_\mathfrak{p}{}' H^2(\mathcal{G}_\mathfrak{p}) = \bigoplus_\mathfrak{p} H^2(\mathcal{G}_\mathfrak{p}).$$

(6.1.3) Proposition. *Der Homomorphismus φ^2 ist injektiv.*

Beweis. Für den Beweis verweisen wir auf [Ko], Chap. 11, Theorem 11.1. □

(6.1.4) Proposition. *Sei $\mathfrak{q}$ eine Primstelle von k und*

$$\varphi_\mathfrak{q}^2 : \; H^2(G) \longrightarrow \bigoplus_{\mathfrak{p}\neq\mathfrak{q}} H^2(\mathcal{G}_\mathfrak{p}),$$

wobei sich das Produkt über alle von $\mathfrak{q}$ verschiedenen Primstellen von k erstreckt. Ist $\delta = 1$, so ist $\varphi_\mathfrak{q}^2$ injektiv.

Beweis. Wir verweisen wieder auf [Ko], Chap. 11, Theorem 11.2. □

Seien nun S und T wieder Primstellenmengen von k, die die Eigenschaft $(*)$ erfüllen.

(6.1.5) Definition. *Es sei für ein $i \geq 0$*

$$\varphi_{S,T}^i : \; H^i(G_S^T) \longrightarrow \prod_{\mathfrak{p}\in S}{}' H^i(\mathcal{G}_\mathfrak{p}) \; .$$

der durch $\mathcal{G}_\mathfrak{p} \to G \to G_S^T$, $\mathfrak{p} \in S$ induzierte Homomorphismus, wobei das restringierte Produkt wieder bezüglich der Gruppen $H_{nr}^i(\mathcal{G}_\mathfrak{p})$ gebildet ist. Wir setzen

$$\text{Ш}_{S,T}^i := \ker \varphi_{S,T}^i.$$

Für $i = 1$ gilt die folgende

(6.1.6) Proposition. *Ist S endlich, dann gilt*

$$\text{Ш}_{S,T}^1 = H^1(G_\varnothing^{(S\setminus S_\infty)\cup T}).$$

Ist ferner $\delta = 1$ und $S_p \subseteq S \cup T$, dann gilt

$$\text{Ш}_{S,T}^1 = V_{(S\cup S_\infty)\cup T}^\varnothing.$$

Beweis. Der Kern der kanonischen Projektion

$$G_S^T \twoheadrightarrow G_\varnothing^{(S\setminus S_\infty)\cup T}$$

ist die normale Untergruppe von G_S^T, die von den Zerlegungsuntergruppen der in S liegenden Primstellen von G_S^T erzeugt wird. Geht man zu den maximalen abelschen Quotienten vom Exponenten p über, so erhält man die exakte Sequenz

$$\bigoplus_{\mathfrak{p}\in S} \mathcal{G}_\mathfrak{p}[p] \longrightarrow G_S^T[p] \longrightarrow G_\varnothing^{(S\setminus S_\infty)\cup T}[p] \longrightarrow 0\ .$$

Dualisieren liefert

$$0 \longrightarrow H^1(G_\varnothing^{(S\setminus S_\infty)\cup T}) \longrightarrow H^1(G_S^T) \longrightarrow \prod_{\mathfrak{p}\in S} H^1(\mathcal{G}_\mathfrak{p})$$

und wir erhalten die erste Gleichung.

Für $\delta = 1$ und $S_p \subseteq S \cup T$ gilt nach dem Zerlegungsgesetz für Kummererweiterungen (7.2.1)

$$k_\varnothing^{(S\setminus S_\infty)\cup T}[p] = k\left(\sqrt[p]{x} | x \in U^\varnothing_{(S\cup S_\infty)\cup T}\right)$$

und die zweite Behauptung folgt unmittelbar aus der Kummertheorie. □

Wir betrachten nun den Fall $i = 2$. Hierfür haben wir den folgenden

(6.1.7) Satz. *Es gibt eine natürliche Einbettung*

$$Ш^2_{S,T} \hookrightarrow Б_S^T\ .$$

Wir schicken dem Beweis von (6.1.7) zunächst zwei Lemmata voraus.

(6.1.8) Lemma. *Es gilt*

$$Ш^2_{S,T} = \ker\left(\inf:\ H^2(G_S^T) \longrightarrow H^2(G)\ \right).$$

Beweis. Sei $\mathfrak{p}$ eine Primstelle von k mit $\mathfrak{p} \notin S$. Dann ist $\mathfrak{p}$ in $k_S^T(p)$ unverzweigt und man hat das kommutative Diagramm

$$\begin{array}{ccc} \mathcal{G}_\mathfrak{p} & \longrightarrow & G \\ \downarrow & & \downarrow \\ \mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p} & \longrightarrow & G_S^T. \end{array}$$

Wegen $H^2(\mathcal{G}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}) = 0$ ist somit

$$H^2(G_S^T) \longrightarrow H^2(G) \longrightarrow H^2(\mathcal{G}_\mathfrak{p})$$

die Nullabbildung für $\mathfrak{p} \notin S$ und man erhält das kommutative Diagramm

$$\begin{tikzcd}
H^2(G_S^T) \arrow[r, "\mathrm{inf}"] \arrow[d, "\varphi^2_{S,T}"'] & H^2(G) \arrow[d, "\varphi^2"] \\
\bigoplus\limits_{\mathfrak{p}\in S} H^2(\mathcal{G}_\mathfrak{p}) \arrow[r, hook] & \bigoplus\limits_{\mathfrak{p}} H^2(\mathcal{G}_\mathfrak{p}).
\end{tikzcd}$$

Nach (6.1.3) ist φ^2 injektiv und wir erhalten die Behauptung. □

Sei $\mathcal{T}_S^T$ die normale von den Trägheitsgruppen $\mathcal{T}_\mathfrak{P}$ für $\mathfrak{p} \notin S \cup T$ und den Zerlegungsgruppen $\mathcal{G}_\mathfrak{P}$ für $\mathfrak{p} \in T$ erzeugte Untergruppe von G. Wir bemerken, dass $\mathcal{T}_S^T$ nicht von der Wahl der Primstellen $\mathfrak{P}$ von $k(p)$ über $\mathfrak{p}$ abhängt, da $\mathcal{T}_\mathfrak{P}$ und $\mathcal{T}_{\mathfrak{P}'}$ bzw. $\mathcal{G}_\mathfrak{P}$ und $\mathcal{G}_{\mathfrak{P}'}$ für eine weitere über $\mathfrak{p}$ liegende Primstelle $\mathfrak{P}'$ von $k(p)$ jeweils zueinander konjugiert sind.

Ferner sei

$$K := \prod_{\mathfrak{p}\notin S\cup T} \mathcal{T}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}^p[\mathcal{T}_\mathfrak{p}, \mathcal{G}_\mathfrak{p}] \times \prod_{\mathfrak{p}\in T} \mathcal{G}_\mathfrak{p}/\mathcal{G}_\mathfrak{p}^p[\mathcal{G}_\mathfrak{p}, \mathcal{G}_\mathfrak{p}].$$

(6.1.9) Lemma. *Man hat einen natürlichen surjektiven Homomorphismus*

$$\chi:\ K \twoheadrightarrow \mathcal{T}_S^T/(\mathcal{T}_S^T)^p[\mathcal{T}_S^T, G].$$

Beweis. Für jede Primstelle $\mathfrak{p}$ haben wir den Homomorphismus $\varphi_\mathfrak{p} : \mathcal{G}_\mathfrak{p} \to G$ und es gilt $\varphi_\mathfrak{p}(\mathcal{T}_\mathfrak{p}) = \mathcal{T}_\mathfrak{P}$ sowie $\varphi_\mathfrak{p}(\mathcal{G}_\mathfrak{p}) = \mathcal{G}_\mathfrak{P}$. Sei U eine offene Untergruppe von G. Dann ist $k(p)^U|k$ endlich und folglich verzweigen nur endliche viele Primstellen von k in $k(p)^U$. Damit gilt $\mathcal{T}_\mathfrak{P} \subseteq U$ für fast alle Primstellen $\mathfrak{p}$. Folglich ist für $(\tau_\mathfrak{p})_{\mathfrak{p}\notin S\cup T} \in \prod_{\mathfrak{p}\notin S\cup T} \mathcal{T}_\mathfrak{p}$ das Produkt

$$\prod_{\mathfrak{p}\notin S\cup T} \varphi_\mathfrak{p}\tau_\mathfrak{p} := \left(\prod_{\mathfrak{p}\notin S\cup T} \varphi_\mathfrak{p}\tau_\mathfrak{p} U\right)_U$$

ein wohldefiniertes Element in

$$G = \varprojlim_U G/U,$$

wobei U alle offenen normalen Untergruppen von G durchläuft. Nach Definition ist aber sogar $\prod_{\mathfrak{p}\notin S\cup T} \varphi_\mathfrak{p}\tau_\mathfrak{p} \in \mathcal{T}_S^T$. Die Zuordnung

$$K \ni (\overline{\tau_\mathfrak{p}})_{\mathfrak{p}\notin S\cup T}\ (\overline{\sigma_\mathfrak{p}})_{\mathfrak{p}\in T} \longmapsto \prod_{\mathfrak{p}\notin S\cup T} \overline{\varphi_\mathfrak{p}\tau_\mathfrak{p}} \prod_{\mathfrak{p}\in T} \overline{\varphi_\mathfrak{p}\sigma_\mathfrak{p}}$$

liefert den gewünschten Homomorphismus $\chi :\ K \to \mathcal{T}_S^T/(\mathcal{T}_S^T)^p[\mathcal{T}_S^T, G]$. Die Surjektivität von χ folgt unmittelbar aus der Definition von $\mathcal{T}_S^T$. □

Wir können nun das Theorem (6.1.7) beweisen.

Beweis von (6.1.7). Nach Konstruktion ist der Fixkörper von $\mathcal{T}_S^T$ gerade der Körper $k_S^T(p)$ und wir haben die exakte Sequenz

$$1 \longrightarrow \mathcal{T}_S^T \longrightarrow G \longrightarrow G_S^T \longrightarrow 1.$$

Die exakte Fünf-Term-Sequenz (2.1.1) liefert

$$0 \longrightarrow H^1(G_S^T) \longrightarrow H^1(G) \longrightarrow H^1(\mathcal{T}_S^T)^{G_S^T} \longrightarrow H^2(G_S^T) \longrightarrow H^2(G)$$

und mit (6.1.8) hat man die exakte Sequenz

$$H^1(G) \longrightarrow H^1(\mathcal{T}_S^T)^{G_S^T} \longrightarrow \text{Ш}^2_{S,T} \longrightarrow 0,$$

Mit $H^1(G) = (G/\operatorname{Fr}(G))^*$ und $H^1(\mathcal{T}_S^T)^{G_S^T} = (\mathcal{T}_S^T/(\mathcal{T}_S^T)^p[\mathcal{T}_S^T, G])^*$ erhalten wir die exakte Sequenz

$$0 \longrightarrow (\text{Ш}^2_{S,T})^* \longrightarrow \mathcal{T}_S^T/(\mathcal{T}_S^T)^p[\mathcal{T}_S^T, G] \xrightarrow{\psi} G/Fr(G),$$

wobei ψ der durch die Inklusion $\mathcal{T}_S^T \hookrightarrow G$ induzierte Homomorphismus ist. Nun gilt nach globaler Klassenkörpertheorie $G/Fr(G) \cong C/C^p = I/I^p k^\times$ und die lokale Klassenkörpertheorie liefert für jede Primstelle $\mathfrak{p}$ von k die Isomorphismen

$$\mathcal{T}_\mathfrak{p}/\mathcal{T}_\mathfrak{p}^p[\mathcal{T}_\mathfrak{p}, \mathcal{G}_\mathfrak{p}] \cong U_\mathfrak{p}/U_\mathfrak{p}^p \quad \text{und} \quad \mathcal{G}_\mathfrak{p}/\mathcal{G}_\mathfrak{p}^p[\mathcal{G}_\mathfrak{p}, \mathcal{G}_\mathfrak{p}] \cong k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times p}.$$

Wir bemerken, dass diese Isomorphismen auch für die unendlichen Primstellen gelten. Wir setzen

$$L := \prod_{\mathfrak{p} \notin S \cup T} U_\mathfrak{p}/U_\mathfrak{p}^p \times \prod_{\mathfrak{p} \in T} k_\mathfrak{p}^\times/k_\mathfrak{p}^{\times p}$$

und erhalten mit (6.1.9) das Diagramm

$$\begin{tikzcd}
K \arrow[r, two heads, "\chi"] \arrow[d, "\wr"'] & \mathcal{T}_S^T/(\mathcal{T}_S^T)^p[\mathcal{T}_S^T, G] \arrow[r, "\psi"] & G/\operatorname{Fr}(G) \arrow[d, "\wr"] \\
L \arrow[rr, "\eta"] & & I/I^p k^\times,
\end{tikzcd}$$

das wegen der Verträglichkeit von globalen und lokalen Normrestsymbolen (vgl. etwa [Ne1], Kap. III, (6.15)) kommutativ ist, wobei η der kanonische durch

$$\prod_{\mathfrak{p} \notin S \cup T} U_\mathfrak{p} \times \prod_{\mathfrak{p} \in T} k_\mathfrak{p}^\times \hookrightarrow I$$

induzierte Homomorphismus ist. Offensichtlich ist $L \cong I_S^T I^p/I^p$ und

$$\begin{aligned}
\ker \eta &\cong (I_S^T I^p \cap I^p k^\times)/I^p = I_S^T I^p \cap k^\times I^p/I^p = I_S^T I^p \cap k^\times/k^\times \cap I^p \\
&= I_S^T I^p \cap k^\times/k^{\times p} = V_S^T.
\end{aligned}$$

Aufgrund der Surjektivität von χ erhalten wir einen surjetiven Homomorphismus $\ker\psi\chi \twoheadrightarrow \ker\psi = (Ш^2_{S,T})^*$ und wegen $\ker\psi\chi \cong \ker\eta$ den surjektiven Homomorphismus

$$V_S^T \longrightarrow\!\!\!\!\!\rightarrow (Ш^2_{S,T})^*.$$

Dualisieren liefert die Behauptung. □

6.2 Berechnung des Relationenrangs von G_S^T

Wir wenden uns nun dem Relationenrang von G_S^T zu. Wir betrachten zunächst wieder den Fall $\delta = 1$ und zeigen, dass wir zur Berechnung von $h^2(G_S^T)$ eine Primstelle von S weglassen können. Sei hierzu $S \neq \varnothing$ und $\mathfrak{q} \in S$ eine beliebige Primstelle.

(6.2.1) Satz. *Ist $\delta = 1$, dann gilt*

$$Ш^2_{S,T} = \ker \varphi^2_{S,T,\mathfrak{q}},$$

wobei $\varphi^2_{S,T,\mathfrak{q}}$ den Homomorphismus

$$\varphi^2_{S,T,\mathfrak{q}} :\ H^2(G_S^T) \longrightarrow \bigoplus_{\mathfrak{p}\in S\setminus\{\mathfrak{q}\}} H^2(\mathcal{G}_\mathfrak{p})$$

bezeichnet.

Beweis. Nach (6.1.4) ist $\varphi^2_\mathfrak{q} :\ H^2(G) \hookrightarrow \bigoplus_{\mathfrak{p}\neq\mathfrak{q}} H^2(\mathcal{G}_\mathfrak{p})$ injektiv und die Behauptung folgt analog wie in (6.1.8). □

(6.2.2) Definition. *Wir setzen*

$$\theta = \theta(S) = \begin{cases} 1, & \text{falls } \delta = 1 \text{ und } S = \varnothing, \\ 0, & \text{sonst} \end{cases}$$

(6.2.3) Satz. *Seien S, T Primstellenmengen von k mit Eigenschaft $(*)$, S sei zudem endlich.*

(i) Für $S = S_{\min}$ gilt

$$h^2(G_S^T) \leq \theta + \sum_{\mathfrak{p}\in S} \delta_\mathfrak{p} + \dim_{\mathbb{F}_p} Б_S^T - \delta.$$

(ii) Für $S \supseteq S_p \cup S_\infty$ gilt

$$h^2(G_S^T) \leq \sum_{\mathfrak{p}\in S\setminus S_\mathbb{C}} \delta_\mathfrak{p} + \dim_{\mathbb{F}_p} Б_S^T - \delta.$$

Beweis. Nach den Definitionen von $Ш^2_{S,T}$ und θ folgt zunächst mit (6.2.1) für beliebiges S

$$\begin{aligned} h^2(G_S^T) &\leq \dim_{\mathbb{F}_p} Ш^2_{S,T} + \sum_{\mathfrak{p}\in S} \dim_{\mathbb{F}_p} h^2(\mathcal{G}_\mathfrak{p}) - \delta + \theta \\ &= \dim_{\mathbb{F}_p} Ш^2_{S,T} + \sum_{\mathfrak{p}\in S\setminus S_\mathbb{C}} \delta_\mathfrak{p} - \delta + \theta. \end{aligned}$$

Im Falle $S = S_{\min}$ gilt $S \cap S_\mathbb{C} = \varnothing$ und im Falle $S \supseteq S_p \cup S_\infty$ ist stets $\theta = 0$. Nach (6.1.7) gilt ferner $\dim_{\mathbb{F}_p} Ш^2_{S,T} \leq \dim_{\mathbb{F}_p} Б_S^T$ und wir erhalten die Behauptung. □

Wir betrachten abschließend wieder den Fall $T = \varnothing$ und erhalten für den Relationenrang von G_S das folgende

(6.2.4) Korollar. *Sei S eine endlich Primstellenmenge von k.*

(i) Für $S = S_{\min}$ gilt

$$h^2(G_S) \leq \theta + \sum_{\mathfrak{p}\in S} \delta_\mathfrak{p} + \dim_{\mathbb{F}_p} Б_S - \delta.$$

(ii) Für $S \supseteq S_p \cup S_\infty$ gilt

$$h^2(G_S) \leq \sum_{\mathfrak{p}\in S\setminus S_\mathbb{C}} \delta_\mathfrak{p} + \dim_{\mathbb{F}_p} Б_S - \delta.$$

(6.2.5) Bemerkung. Im Falle $S \supseteq S_p \cup S_\infty$ gilt für den Relationenrang von G_S sogar Gleichheit, d.h.

$$h^2(G_S) = \sum_{\mathfrak{p}\in S\setminus S_\mathbb{C}} \delta_\mathfrak{p} + \dim_{\mathbb{F}_p} Б_S - \delta.$$

Für einen Beweis, der die tiefliegende Poitou-Tate-Dualität benutzt, verweisen wir auf [NSW], Chap. VIII, (8.7.9).

Für die partielle Euler-Poincaré-Charakteristik von G_S^T erhalten wir abschließend den folgenden

(6.2.6) Satz.

(i) Für $S = S_{\min}$ gilt

$$\chi_2(G_S^T(p)) \leq |T| + \theta + r - \sum_{\mathfrak{p}\in S_p} [k_\mathfrak{p} : \mathbb{Q}_\mathfrak{p}].$$

(ii) Für $S \supseteq S_p \cap S_\infty$ gilt

$$\chi_2(G_S^T(p)) \leq |T| - r_\mathbb{C},$$

wobei $r_\mathbb{C}$ die Anzahl der komplexen Primstellen von k bezeichnet.

Beweis. Die beiden Ungleichungen ergeben sich unmittelbar aus (5.2.3), (5.2.5) und (6.2.3). □

6.3 Eine Bedingung für $[k_S^T(p) : k] = \infty$

Wir werden im Folgenden eine Bedingung an die Primstellenmengen S und T angeben, unter welcher die Erweiterung $k_S^T(p)$ unendlich ist. Hierzu führen wir zunächst einige abkürzenden Notationen ein.

(6.3.1) Notation. *Für eine endliche Primstellenmenge S setzen wir*

$$\delta_S = \sum_{\mathfrak{p}\in S} \delta_{\mathfrak{p}} - \delta, \quad n_S = \sum_{\mathfrak{p}\in S\cap S_p} [k_{\mathfrak{p}} : \mathbb{Q}_p],$$
$$C_1(S) = \left(\sqrt{1 + \delta_S + \dim_{\mathbb{F}_p} \text{Б}_S} - 1\right)^2 - 1 + n_S - r \quad \textit{und}$$
$$C_2(S) = \left(\sqrt{\delta_S + \dim_{\mathbb{F}_p} \text{Б}_S} - 1\right)^2.$$

Wir betrachten wieder zunächst den Fall $T = \varnothing$ und geben eine Bedingung an, unter welcher die Erweiterung $k_S(p)$ unendlich ist.

(6.3.2) Proposition. *Sei S eine endliche Primstellenmenge von k.*

(i) Gilt $S = S_{\min}$ und $C_1(S) \geq 0$, so ist G_S unendlich.

(ii) Gilt $S \supseteq S_p \cup S_\infty$, so ist G_S unendlich.

Beweis. (i) Wir setzen $c_S = 1 + \delta_S + \dim_{\mathbb{F}_p} \text{Б}_S$. Angenommen, G_S wäre endlich. Dann gilt nach (2.4.6)

$$\begin{aligned} 0 &< 4h^2(G_S) - h^1(G_S)^2 \\ &\leq 4(\theta + \delta_S + \dim_{\mathbb{F}_p} \text{Б}_S) - (1 + \delta_S + \dim_{\mathbb{F}_p} \text{Б}_S + n_S - r)^2 \\ &\leq 4c_S - (c_S + n_S - r)^2 \end{aligned}$$

und folglich

$$C_1(S) = (\sqrt{c_S} - 1)^2 - 1 + n_S - r = c_S - 2\sqrt{c_S} + n_S - r < 0$$

im Widerspruch zur Annahme.

(ii) Angenommen, G_S wäre endlich. Analog zu (i) gilt dann

$$\begin{aligned} 0 &< 4h^2(G_S) - h^1(G_S)^2 \\ &\leq 4(\delta_S + \dim_{\mathbb{F}_p} \text{Б}_S) - (1 + \delta_S + \dim_{\mathbb{F}_p} \text{Б}_S)^2 \end{aligned}$$

und folglich

$$C_2(S) = 1 + \delta_S + \dim_{\mathbb{F}_p} \text{Б}_S - 2\sqrt{\delta_S + \dim_{\mathbb{F}_p} \text{Б}_S} < 0$$

im Widerspruch zu $C_2(S) = \left(\sqrt{\delta_S + \dim_{\mathbb{F}_p} \text{Б}_S} - 1\right)^2 \geq 0$. □

(6.3.3) Bemerkung. Nach (6.3.2) ist die Erweiterung $k_S(p)|k$ im Falle $S \supseteq S_p \cup S_\infty$ stets unendlich. Dies lässt sich auch wie folgt sehen: Bezeichne k_∞

die zyklotomische $\mathbb{Z}_p$-Erweiterung von k. Diese ist außerhalb S_p unverzweigt (vgl. [Wa], Chap. 13, Theorem 13.2) und folglich gilt

$$k_\infty \subseteq (k_S(p))^{ab} \subseteq k_S(p).$$

Insbesondere ist $(k_S(p))^{ab}|k$ und damit auch $k_S(p)|k$ unendlich. Für ungerades p gilt für die kohomologische Dimension von G_S

$$cd\ G_S \leq 2.$$

Für den Fall $p=2$ gilt

$$\begin{aligned} cd\ G_S &\leq 2, \quad \text{falls } s_{\mathbb{R}} = 0 \text{ und} \\ cd\ G_S &= \infty, \quad \text{falls } s_{\mathbb{R}} > 0. \end{aligned}$$

Für einen Beweis verweisen wir auf [NSW], Chap. X, (10.4.9).

Für Primstellenmengen $S = S_{\min}$ mit $S_p \not\subseteq S$ sind entsprechende Aussagen über die kohomologische Dimension der Gruppen G_S im Allgemeinen deutlich schwerer zu gewinnen. Gilt $S \cap S_p = \varnothing$, so ist G_S eine *Fab-Gruppe,* d.h. für alle offenen Untergruppen U von G_S ist U^{ab} endlich. Dies folgt aus der Tatsache, dass in jeder $\mathbb{Z}_p$-Erweiterung eines algebraischen Zahlkörpers mindestens eine über p liegende Primstelle verzweigt (vgl. [Wa], Chap. 13, Lemma 13.3). Ist $k = \mathbb{Q}$ oder ein imaginär quadratischer Zahlkörper, dann ist die Gruppe G_S vom Koch-Typ. Ist $\Gamma_S(p)$ ein strikter Kreis, so ist G_S eine *milde* pro-p-Gruppe und nach (2.6.6) gilt

$$cd\ G_S = 2,$$

vlg. hierzu [La1] und [Vo]. Für den Fall $k=\mathbb{Q}$ und $|T|=1$ werden wir im letzten Abschnitt sehen, dass die Gruppe G_S^T unter bestimmten Bedingungen ebenfalls vom Koch-Typ ist.

Wir betrachten nun die Erweiterung $k_S^T(p)$ und geben eine Bedingung für die Anzahl $|T|$ der in T liegenden Primstellen an, unter welcher die Erweiterung $k_S^T(p)$ unendlich ist.

(6.3.4) Satz. *Seien S und T zwei Primstellenmengen von k mit Eigenschaft $(*)$, S sei endlich.*

(i) Gilt $S = S_{\min}$ und $|T| \leq C_1(S)$, so ist G_S^T unendlich.

(ii) Gilt $S \supseteq S_p \cup S_\infty$ und $|T| \leq C_2(S)$, so ist G_S^T unendlich.

Beweis. Die beiden Aussagen lassen sich analog wie in (6.3.2) beweisen, wir führen hier daher nur den Fall (i), d.h. $S = S_{\min}$, aus. Wir setzen dazu $c_S^T = 1 + \delta_S + \dim_{\mathbb{F}_p} Б_S^T$. Angenommen G_S^T wäre endlich. Dann gilt nach (2.4.6)

$$\begin{aligned} 0 &< 4h^2(G_S) - h^1(G_S)^2 \\ &\leq 4(\theta + \delta_S + \dim_{\mathbb{F}_p} Б_S^T) - (1 + \delta_S + \dim_{\mathbb{F}_p} Б_S^T + n_S - r - |T|)^2 \\ &\leq 4c_S - (c_S + n_S - r - |T|)^2 \end{aligned}$$

und folglich

$$\begin{aligned} C_1(S) - |T| &= \left(\sqrt{c_S^{\varnothing}} - 1\right)^2 - 1 - n_S - r - |T| \\ &\leq \left(\sqrt{c_S^T} - 1\right)^2 - 1 - n_S - r - |T| \\ &= c_S^T - 2\sqrt{c_S^T} + n_S - r - |T| < 0 \end{aligned}$$

im Widerspruch zur Annahme. $\square$

7 Die Kummergruppen V_S^T

Wir betrachten die Kummergruppen V_S^T, die durch

$$V_S^T = (k^\times \cap I_S^T)/k^{\times p}$$

definiert sind, sowie die dualen Gruppen $Б_S^T = (V_S^T)^*$. In diesem Abschnitt soll die $\mathbb{F}_p$-Dimension $\dim_{\mathbb{F}_p} Б_S^T$ genauer untersucht werden.

Sei zunächst T eine beliebige endliche Menge endlicher Primstellen. Nach (5.2.2) gilt

$$\dim_{\mathbb{F}_p} Б_\varnothing^T = \dim_{\mathbb{F}_p} H^1(G_\varnothing^T) + \delta + |T| + r - 1,$$

insbesondere ist $Б_\varnothing^T$ und damit auch $V_\varnothing^T$ endlich und wir haben die triviale Abschätzung

$$\dim_{\mathbb{F}_p} Б_\varnothing^T \geq |T|.$$

Sei nun S eine weitere Menge von Primstellen, so dass S und T die Eigenschaft $(*)$ erfüllen. Man hat die natürliche Inklusion $U_S^T \subseteq U_\varnothing^T$ und folglich ist auch V_S^T und damit $Б_S^T$ endlich. Genauer gilt die folgende

(7.0.5) Proposition. *Es gilt*

$$\dim_{\mathbb{F}_p} Б_S \leq \dim_{\mathbb{F}_p} Б_S^T \leq \dim_{\mathbb{F}_p} Б_S + |T|.$$

Beweis. Die Ungleichungen ergeben sich unmittelbar aus der exakten Sequenz

$$1 \longrightarrow V_S \longrightarrow V_S^T \longrightarrow \prod_{\mathfrak{p} \in T} k_\mathfrak{p}^\times / U_\mathfrak{p} k_\mathfrak{p}^{\times p}$$

und $k_\mathfrak{p}^\times / U_\mathfrak{p} k_\mathfrak{p}^{\times p} \cong \mathbb{Z}/p\mathbb{Z}$. □

7.1 Primstellenmengen mit $Б_S^T = 0$

Die Gleichung $Б_S^T = 0$ impliziert nach (6.1.7) die Injektivität von

$$\varphi_{S,T}^2 : \; H^2(G_S^T) \longrightarrow \bigoplus_{\mathfrak{p} \in S} H^2(\mathcal{G}_\mathfrak{p})$$

und wir werden später sehen, dass wir in diesem Fall die Relationen einer minimalen Darstellung von G_S^T aus den lokalen Relationen der Gruppen $\mathcal{G}_\mathfrak{p}, \mathfrak{p} \in S$ gewinnen können. Offensichtlich kann $Б_S^T = 0$ nur gelten, wenn $Б_S = 0$ ist. Wir wollen uns nun der Frage zuwenden, unter welchen Bedingungen an die Primstellenmengen S und T die Gleichung $Б_S = 0$ auch das Verschwinden von $Б_S^T$ impliziert. Es gilt der folgende

(7.1.1) Satz. *Seien S und $T = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_l\}$ Primstellenmengen, die die Eigenschaft $(*)$ erfüllen, S sei endlich. Dann gilt $Б_S^T = 0$ genau dann, wenn die folgenden Aussagen erfüllt sind:*

(i) $Б_S = 0$.

(ii) Für $1 \leq i \leq l$ ist die Primstelle $\mathfrak{p}_i$ in $k_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_{i-1}\}}[p]$, der maximalen abelschen Erweiterung vom Exponenten p in $k_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_{i-1}\}}$, nicht voll zerlegt. (Hierbei sei $k_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_{i-1}\}}[p] = k_S[p]$ für $i = 1$.)

Beweis. Wir zeigen zunächst, dass die Bedingungen (i) und (ii) das Verschwinden von $Б_S^T$ implizieren. Wir führen hierzu eine Induktion über die Anzahl l der in T enthaltenen Primstellen. Ist $l = 1, T = \{\mathfrak{p}_1\}$. Nach Voraussetzung ist $\mathfrak{p}_1$ in der Erweiterung $k_S[p]$ nicht voll zerlegt, d.h. es gilt $k_S^{\{\mathfrak{p}_1\}}[p] \subsetneq k_S[p]$. Folglich ist $G_S^{\{\mathfrak{p}_1\}}/\operatorname{Fr}(G_S^{\{\mathfrak{p}_1\}})$ ein echter Faktor von $G_S/\operatorname{Fr}(G_S)$. Nun ist $G_S/\operatorname{Fr}(G_S)$ eine endliche abelsche Gruppe vom Exponenten p, also gilt $h^1\left(G_S^{\{\mathfrak{p}_1\}}/\operatorname{Fr}(G_S^{\{\mathfrak{p}_1\}})\right) \leq h^1\left(G_S/\operatorname{Fr}(G_S)\right) - 1$ und damit

$$h^1\left(G_S^{\{\mathfrak{p}_1\}}\right) \leq h^1\left(G_S\right) - 1.$$

Nach (5.2.3) folgt

$$\dim_{\mathbb{F}_p} Б_S^T - |T| = \dim_{\mathbb{F}_p} Б_S^{\{\mathfrak{p}_1\}} - 1 \leq \dim_{\mathbb{F}_p} Б_S - 1$$

und es ist wegen $Б_S = 0$ auch $Б_S^{\{\mathfrak{p}_1\}} = 0$. Nehmen wir nun an, die Behauptung gelte für Primstellenmengen T mit $|T| = l - 1$. Da die Primstelle $\mathfrak{p}_l$ in der Erweiterung $k_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_{l-1}\}}[p]$ nicht voll zerlegt ist, folgt wieder $h^1\left(G_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_l\}}\right) \leq h^1\left(G_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_{l-1}\}}\right) - 1$ und damit nach (5.2.3)

$$\dim_{\mathbb{F}_p} Б_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_l\}} - l \leq \dim_{\mathbb{F}_p} Б_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_{l-1}\}} - (l-1) - 1.$$

Nach Induktionsvoraussetzung ist $\dim_{\mathbb{F}_p} Б_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_{l-1}\}} = 0$ und wir erhalten $\dim_{\mathbb{F}_p} Б_S^{\{\mathfrak{p}_1,\ldots,\mathfrak{p}_l\}} = 0$.

Bleibt zu zeigen, dass die obigen Bedingungen auch notwendig für das Verschwinden von $Б_S^T$ sind. Gilt $Б_S^T = 0$, so ist trivialerweise auch $Б_S = 0$. Nehmen wir nun an, die Primstelle $\mathfrak{p}_1$ wäre in der Erweiterung $k_S[p]$ bereits voll zerlegt. Dann wäre $k_S^{\{\mathfrak{p}_1\}}[p] = k_S[p]$ und damit $h^1\left(G_S^{\{\mathfrak{p}_1\}}\right) = h^1(G_S)$. (5.2.6) impliziert dann

$$\dim_{\mathbb{F}_p} Б_S^{\{\mathfrak{p}_1\}} - 1 = \dim_{\mathbb{F}_p} Б_S.$$

Folglich wäre $\dim_{\mathbb{F}_p} Б_S^T \geq \dim_{\mathbb{F}_p} Б_S^{\{\mathfrak{p}_1\}} = 1$ im Widerspruch zu $Б_S^T = 0$. Völlig analog sieht man, dass $Б_S^T = 0$ auch die Bedingung (ii) für $i > 1$ impliziert. $\square$

(7.1.2) Bemerkung. Sei $k = \mathbb{Q}$ und p eine ungerade Primzahl. Wegen $\mathbb{Q}_\varnothing = \mathbb{Q}$ folgt aus (5.2.2) auch $Б_\varnothing = 0$ und folglich gilt $Б_S = 0$ für jede Primstellenmenge S von $\mathbb{Q}$. Für $p = 2$ ist $V_\varnothing = \{-1, +1\} \cdot \mathbb{Q}^{\times 2}/\mathbb{Q}^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$. Ist nun S eine Primstellenmenge von $\mathbb{Q}$, die entweder die unendliche Stelle oder eine Primstelle kongruent 3 modulo 4 enthält, so ist $-1 \cdot \mathbb{Q}^{\times 2} \notin V_S$ und folglich $Б_S = (V_S)^* = 0$.

(7.1.3) Beispiel. Sei $k = \mathbb{Q}$ und $p = 2$. Die Primstellenmengen S und T seien gegeben durch

$$S = \{\infty, 3, 5\} \text{ und } T = \{7\},$$

wobei ∞ die unendliche Primstelle von $\mathbb{Q}$ bezeichnet. Nach (7.1.2) gilt dann Б$_S = 0$. Wir betrachten den Körper $L := \mathbb{Q}(\zeta_3, \sqrt{5})$, wobei ζ_3 eine primitive 3-te Einheitswurzel bezeichnet. Nach den Zerlegungsgesetzen verzweigen in L genau die in S liegenden Primstellen, ferner gilt $\mathrm{Gal}(L|\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ und folglich

$$L \subseteq \mathbb{Q}_S[2].$$

Nun ist 7 in $\mathbb{Q}(\sqrt{5})$ träge, d.h. insbesondere in L und damit auch in $\mathbb{Q}_S[2]$ nicht voll zerlegt. Nach (7.1.1) gilt Б$_S^T = 0$ und nach (5.2.3) haben wir

$$h^1(G_S^T) = 1.$$

Insbesondere ist G_S^T also abelsch. Wegen $2 \notin S$ ist aber $G_S^T = (G_S^T)^{ab}$ nach Bemerkung (6.3.3) endlich und folglich gilt auch

$$h^2(G_S^T) = 1.$$

Ferner erhalten wir

$$\mathbb{Q}_{\{\infty,3,5\}}^{\{7\}}[2] = \mathbb{Q}_{\{\infty,3\}}^{\{7\}}[2] = \mathbb{Q}(\zeta_3).$$

(7.1.4) Beispiel. Sei $k = \mathbb{Q}$ und $p = 3$. Die Primstellenmengen S und T seien gegeben durch

$$S = \{3, q_1, \ldots, q_k\} \text{ und } T = \{5\},$$

wobei $q_1, \ldots, q_k$ paarweise verschiedene Primzahlen kongruent 1 modulo 3 bezeichnen. Nach (7.1.2) ist wieder Б$_S = 0$. Sei ζ_9 eine primitive 9-te Einheitswurzel und L der Zwischenkörper von $\mathbb{Q}(\zeta_9)$ vom Grad 3 über $\mathbb{Q}$. Offensichtlich ist dann

$$L \subseteq \mathbb{Q}_S[3].$$

Wegen $\mathrm{ord}_9\, 5 = \varphi(9) = 6$ ist 5 in $\mathbb{Q}(\zeta_9)$ träge, also insbesondere in L und damit auch in $\mathbb{Q}[3]$ nicht voll zerlegt. Mit (7.1.1) erhalten wir wieder Б$_S^T = 0$ und somit ist nach (5.2.3) und (6.2.3)

$$h^1(G_S^T) = k \quad \text{und} \quad h^2(G_S^T) \leq k.$$

Wäre nun $(G_S^T)^{ab}$ unendlich, so würde $\mathbb{Q}_S^T(3)$ die zyklotomische $\mathbb{Z}_3$-Erweiterung von $\mathbb{Q}$ und damit insbesondere die Erweiterung L enthalten, was allerdings der Unzerlegtheit von 5 in L widerspricht. $(G_S^T)^{ab}$ ist also endlich und folglich ist $h^2(G_S^T) \geq h^1(G_S^T)$, woraus wir

$$h^1(G_S^T) = h^2(G_S^T) = k$$

erhalten. Nach (2.4.6) ist damit $\mathbb{Q}_{\{3,q_1,\ldots,q_k\}}^{\{5\}}(3)|\mathbb{Q}$ für $k \geq 4$ unendlich.

7.2 Der Fall $\delta = 1$ - Anwendung der Kummertheorie

Sei im Folgenden $\delta = 1$, d.h. k enthalte die p-ten Einheitswurzeln. Wir betrachten die Kummererweiterung

$$k(S,T) := k(\sqrt[p]{x} | x \in U_S^T).$$

Wir formulieren zunächst das Zerlegungsgesetz für Kummererweiterungen.

(7.2.1) Proposition.

(i) Eine endliche Primstelle $\mathfrak{p} \notin S_p$ ist unverzweigt in $k(\sqrt[p]{x})$ genau dann, wenn $x \in U_\mathfrak{p} k_\mathfrak{p}^{\times p}$ und voll zerlegt in $k(\sqrt[p]{x})$ genau dann, wenn $x \in k_\mathfrak{p}^{\times p}$.

(ii) Eine endliche Primstelle $\mathfrak{p} \in S_p$ ist voll zerlegt in $k(\sqrt[p]{x})$ genau dann, wenn $x \in k_\mathfrak{p}^{\times p}$.

(iii) Eine unendliche Primstelle $\mathfrak{p} \in S_\infty$ ist unverzweigt in $k(\sqrt[p]{x})$ genau dann, wenn $x \in k_\mathfrak{p}^{\times p}$.

Beweis. Wir verweisen auf [Ne1], Kap. III, (4.4). □

Wir erhalten den folgenden

(7.2.2) Satz. *Sei S endlich und es gelte $S_\infty \subseteq S$, $S_p \subseteq S \cup T$. Dann ist $k(S,T)|k$ die maximale abelsche Erweiterung vom Exponenten p, die außerhalb T unverzweigt und über S voll zerlegt ist, d.h. es gilt*

$$k(S,T) = k_T^S[p] = k_T^{S \setminus S_\infty}[p]$$

(7.2.3) Korollar. *Mit den Voraussetzungen von (7.2.2) gilt*

$$V_S^T \cong H^1(G_T^{S \setminus S_\infty}).$$

Ist sogar $S_p \subseteq S$, so gilt

$$\dim_{\mathbb{F}_p} Б_S^T + |S| = \dim_{\mathbb{F}_p} Б_T^{S \setminus S_\infty} + |T_0|,$$

wobei $T_0 := \{\mathfrak{p} \in T | \mathfrak{N}(\mathfrak{p}) \equiv 1 \bmod p\}$

Beweis. Der obige Isomorphismus folgt sofort aus der Kummertheorie und (7.2.2). Ist $S_p \subseteq S$, dann ist $S_p \cap T = \varnothing$ und wir erhalten mit (5.2.3) die Gleichung

$$\begin{aligned}
\dim_{\mathbb{F}_p} Б_S^T &= \dim_{\mathbb{F}_p} V_S^T = h^1(G_T^{S \setminus S_\infty}) \\
&= -\delta - r - |S \setminus S_\infty| + 1 + \sum_{\mathfrak{p} \in T} \delta_\mathfrak{p} + \dim_{\mathbb{F}_p} Б_T^{S \setminus S_\infty} \\
&= -|S| + |T_0| + \dim_{\mathbb{F}_p} Б_T^{S \setminus S_\infty}.
\end{aligned}$$

□

(7.2.4) Bemerkung. Gilt $\delta = 0$, so lassen sich für eine endliche Menge S mit $S_\infty \subseteq S$, $S_p \subseteq S \cup T$ analoge Resultate gewinnen, indem man zum Körper $K := k(\mu_p)$ übergeht. Bezeichnen nämlich S' bzw. T' die Mengen der über S bzw. T liegenden Primstellen und S'_∞ die Menge der unendlichen Primstellen von K, dann hat man die Isomorphie

$$V_S^T \cong H^1\left(\mathrm{Gal}(K_T'^{S' \setminus S'_\infty}(p)|k)\right).$$

Für den Beweis verweisen wir auf [Ne2], §7, (7.3).

8 Erzeuger und Relationen von G_S^T

In diesem Abschnitt soll für die Gruppe G_S^T ein Erzeugendensystem angegeben werden. Ferner sollen im Fall $Б_S^T = 0$ für eine minimale Darstellung von G_S^T die Relationen aus den Relationen der lokalen Gruppen $\mathcal{G}_\mathfrak{p}$ gewonnen werden. Seien im Folgenden wieder S und T Primstellenmengen mit Eigenschaft $(*)$, d.h. T ist eine endliche Menge endlicher Primstellen und $S \cap T = \varnothing$.

8.1 Ein kanonisches Erzeugendensystem von G_S^T

Nach (5.1.3) haben wir die exakte Sequenz

$$\prod_{\mathfrak{p}\in S} U_\mathfrak{p}/U_\mathfrak{p}^p \xrightarrow{\varphi_2} I/I_S^T I^p k^\times \xrightarrow{\varphi_3} I/I_\varnothing^T I^p k^\times \longrightarrow 1 .$$

Für eine Primstelle $\mathfrak{p}$ von k setzen wir $d_\mathfrak{p} = \dim_{\mathbb{F}_p} U_\mathfrak{p}/U_\mathfrak{p}^p$, d.h. $d_\mathfrak{p} = \delta_\mathfrak{p}$ für $\mathfrak{p} \notin S_p$ (und wegen $S = S_{\min}$ ist $d_\mathfrak{p} = \delta_\mathfrak{p} = 1$ für $\mathfrak{p} \in S \setminus S_p$) und $d_\mathfrak{p} = [k_\mathfrak{p} : \mathbb{Q}_p] + \delta_\mathfrak{p}$ für $\mathfrak{p} \in S_p$. Ferner seien $u_{1\mathfrak{p}}, \ldots, u_{d_\mathfrak{p}\mathfrak{p}} \in U$ die Urbilder einer Basis von $U_\mathfrak{p}/U_\mathfrak{p}^p$. Weiter setzen wir $d := \dim_{\mathbb{F}_p} I/I_\varnothing^T I^p k^\times$ und es seien $i_1, \ldots, i_d \in I$ die Urbilder einer Basis von $I/I_\varnothing^T I^p k^\times$.

Für jedes $\mathfrak{p}$ fixieren wir eine feste über $\mathfrak{p}$ liegende Primstelle $\mathfrak{P}$ in $k_S^T(p)$. Wir definieren nun die Elemente $g_1, \ldots, g_d$ und $h_{1\mathfrak{p}}, \ldots, h_{d_\mathfrak{p}\mathfrak{p}} \in G_S^T$ wie folgt:

(i) Für $1 \le j \le d$ sei g_j ein Lift von $(i_j, (k_S^T)^{ab}|k) \in (G_S^T)^{ab}$.

(ii) Für $\mathfrak{p} \in S$ und $1 \le j \le d_\mathfrak{p}$ sei $h_{j\mathfrak{p}}$ Element der Trägheitsgruppe $\mathcal{T}_\mathfrak{P}$ von $\mathfrak{P}$ in $k_S^T(p)$, dessen Einschränkung auf $(k_S^T)^{ab}$ durch $(u_{j\mathfrak{p}}, (k_S^T)^{ab}|k) \in (G_S^T)^{ab}$ gegeben ist. Hierbei bezeichnen wir mit $u_{j\mathfrak{p}}$ das Idel, das an der Stelle $\mathfrak{p}$ die Komponente $u_{j\mathfrak{p}}$ und an allen anderen Stellen die Komponente 1 besitzt.

(8.1.1) Satz. *Die Menge*

$$\mathcal{M} := \{g_1, \ldots, g_d\} \cup \{h_{1\mathfrak{p}}, \ldots, h_{d_\mathfrak{p}\mathfrak{p}} | \mathfrak{p} \in S\}$$

bildet ein Erzeugendensystem von G_S^T.

Beweis. Sei U eine offene normale Untergruppe von G_S^T. Die zu U gehörige Zwischenerweiterung $L|k$ von $k_S^T(p)$ ist endlich. Folglich sind in ihr fast alle Primstellen unverzweigt und damit $\mathcal{T}_\mathfrak{P} \subseteq U$ für fast alle $\mathfrak{p}$. Nach Definition gilt dann aber $\{h_{1\mathfrak{p}}, \ldots, h_{d_\mathfrak{p}\mathfrak{p}}\} \subseteq U$ für fast alle $\mathfrak{p} \in S$ und folglich ist $\mathcal{M}$ eine konvergente Teilmenge von G_S^T. Nach dem Burnsideschen Basissatz (2.4.3) genügt es nun zu zeigen, dass $\mathcal{M} \mod \operatorname{Fr}(G_S^T)$ die Gruppe $G_S^T/\operatorname{Fr}(G_S^T)$ erzeugt.

Wir haben bereits gezeigt, dass das globale Normrestsymbol $(\ ,(k_S^T)^{ab}|k)$ den algebraischen wie topologischen Isomorphismus

$$I/I_S^T I^p k^\times \xrightarrow{\sim} G_S^T/\operatorname{Fr}(G_S^T)$$

induziert. Folglich genügt es zu zeigen, dass die Idele $i_1, \dots, i_d$ und $u_{1\mathfrak{p}}, \dots, u_{d_\mathfrak{p}\mathfrak{p}}$, $\mathfrak{p} \in S$ ein Erzeugendensystem von $I \mod I_S^T I^p k^\times$ bilden. Das folgt aber sofort aus den Definitionen und obiger exakter Sequenz. $\square$

(8.1.2) Bemerkung. Ist S endlich, so gilt offensichtlich

$$\begin{aligned} |\mathcal{M}| &= \dim_{\mathbb{F}_p} H^1(G_\varnothing^T) + \sum_{\mathfrak{p} \in S \cap S_p} [k_\mathfrak{p} : \mathbb{Q}_p] + \sum_{\mathfrak{p} \in S} \delta_\mathfrak{p} \\ &= \sum_{\mathfrak{p} \in S \cap S_p} [k_\mathfrak{p} : \mathbb{Q}_p] - \delta - r - |T| + 1 + \sum_{\mathfrak{p} \in S} \delta_\mathfrak{p} + \dim_{\mathbb{F}_p} \text{Б}_\varnothing^T. \end{aligned}$$

$|\mathcal{M}|$ ist also im Allgemeinen kein minimales Erzeugendensystem, es können genau $\dim_{\mathbb{F}_p} \text{Б}_\varnothing^T - \dim_{\mathbb{F}_p} \text{Б}_S^T$ Erzeuger weggelassen werden. Wir werden im folgenden Abschnitt unter der Annahme $\text{Б}_S^T = 0$ ein Kriterium dafür angeben, welche Elemente von $\mathcal{M}$ weggelassen werden können.

8.2 Bestimmung eines minimalen Erzeugendensystems

Im Folgenden gelte $\text{Б}_S^T = 0$. Nach (5.1.3) haben wir die exakte Sequenz

$$1 \longrightarrow V_\varnothing^T \xrightarrow{\varphi_1} \prod_{\mathfrak{p} \in S} U_\mathfrak{p}/U_\mathfrak{p}^p \xrightarrow{\varphi_2} I/I_S^T I^p k^\times \xrightarrow{\varphi_3} I/I_\varnothing^T I^p k^\times \longrightarrow 1\ .$$

Um ein minimales Erzeugendensystem für $I/I_S^T I^p k^\times$ und damit für G_S^T zu finden, müssen wir ein minimale Teilmenge $\mathcal{U} \subseteq \{u_{1\mathfrak{p}}, \dots, u_{n_\mathfrak{p}\mathfrak{p}}, \mathfrak{p} \in S\}$ finden, so dass $\mathcal{U} \bmod I_S^T I_\varnothing^p$ und $\operatorname{im} \varphi_1$ die Gruppe $I_\varnothing^T / I_S^T I_\varnothing^p \cong \prod_{\mathfrak{p} \in S} U_\mathfrak{p}/U_\mathfrak{p}^p$ erzeugen. Hierzu bestimmen wir zunächst eine Basis von $\operatorname{im} \varphi_1$. Bezeichne hierzu für $1 \le \nu \le d$ e_ν die kleinste natürliche Zahl, so dass $i_\nu^{e_\nu} \in I_\varnothing^T k^\times$ und $\alpha_\nu \in k^\times$ ein Element mit $i_\nu^{e_\nu}(\alpha_\nu) \in I_\varnothing^T$ ist. Hierbei bezeichne $(x) \in I$ für ein $x \in k^\times$ wieder das zugehörige Hauptidel. Weiter seien $\varepsilon_1, \dots, \varepsilon_{|T|+r-1}$ Erzeuger des freien Anteils der T-Einheitengruppe $k_\varnothing^T$ (vgl. (5.2.1)) und für $\delta = 1$ bezeichne $\varepsilon_{|T|+r} = \zeta$ einen Erzeuger der Gruppe der in k enthaltenen Einheitswurzeln.

(8.2.1) Lemma. *Das Bild der Menge*

$$\mathcal{C} := \{(\varepsilon_\mu), 1 \le \mu \le |T| + r - 1 + \delta\} \cup \{i_\nu^{e_\nu}(\alpha_\nu), 1 \le \nu \le d\}$$

unter der kanonischen Projektion $I \twoheadrightarrow I/I_S^T I_\varnothing^T$ *bildet eine Basis von* $\operatorname{im} \varphi_1$.

Beweis. Es gilt $\operatorname{im} \varphi_1 = \ker(\varphi_2) = (I_\varnothing^T \cap I^p k^\times) I_S^T I_\varnothing^p / I_S^T I_\varnothing^p$. Nach Definition sind die i_ν $\mathbb{F}_p$-linear unabhängig modulo $I_\varnothing^T I^p k^\times$ und folglich gilt $p \mid e_\nu$, also $i_\nu^{e_\nu}(\alpha_\nu) \in I_\varnothing^T \cap I^p k^\times$. Nach Definition ist ferner $\varepsilon_\nu \in I_\varnothing^T \cap k^\times$ und wir erhalten

$$\mathcal{C} \subseteq I_\varnothing^T \cap I^p k^\times.$$

Aus der linearen Unabhängigkeit der ε_μ und der i_ν folgt unmittelbar die lineare Unabhängigkeit von $\mathcal{C}$ und es gilt

$$\begin{aligned} |\mathcal{C}| &= d + |T| + r - 1 + \delta = \dim_{\mathbb{F}_p} I/I_\varnothing^T I^p k^\times + |T| + r - 1 + \delta \\ &= \dim_{\mathbb{F}_p} V_\varnothing^T = \dim_{\mathbb{F}_p} \operatorname{im} \varphi_1. \end{aligned}$$

□

Fassen wir nun die (ϵ_μ) und $i_\nu^{e_\nu}(\alpha_\nu)$ als Elemente in $\prod_{\mathfrak{p}\in S} U_\mathfrak{p}/U_\mathfrak{p}^p$ auf, so erhalten wir das Gleichungssystem

$$\begin{aligned} (\epsilon_\mu) &= \prod_{\mathfrak{p}\in S} \beta_{\mathfrak{p}\mu} u_{1\mathfrak{p}}^{a_{1\mathfrak{p}\mu}} \cdots u_{d_\mathfrak{p}\mathfrak{p}}^{a_{d_\mathfrak{p}\mathfrak{p}\mu}}, \quad \mu = 1, \ldots, |T| + r - 1 + \delta \\ i_\nu^{e_\nu}(\alpha_\nu) &= \prod_{\mathfrak{p}\in S} \gamma_{\mathfrak{p}\nu} u_{1\mathfrak{p}}^{b_{1\mathfrak{p}\nu}} \cdots u_{d_\mathfrak{p}\mathfrak{p}}^{b_{d_\mathfrak{p}\mathfrak{p}\nu}}, \quad \nu = 1, \ldots, d \end{aligned}$$

mit $a_{j\mathfrak{p}\mu}, b_{j\mathfrak{p}\nu} \in \mathbb{Z}/p\mathbb{Z}$ und $\beta_{\mathfrak{p},\mu}, \gamma_{\mathfrak{p}\nu} \in U_\mathfrak{p}^p$. Für jede dieser Gleichungen können wir ein Element aus $\{u_{1\mathfrak{p}}, \ldots, u_{n_\mathfrak{p}\mathfrak{p}}, \mathfrak{p} \in S\}$ streichen, so dass die übrigen Elemente mod $I_S^T I_\varnothing^p$ zusammen mit $\operatorname{im}\varphi_1$ die Gruppe $I_\varnothing^T/I_S^T I_\varnothing^p$ erzeugen und wir erhalten eine Teilmenge $\mathcal{U} \subseteq \{u_{1\mathfrak{p}}, \ldots, u_{d_\mathfrak{p}\mathfrak{p}}, \mathfrak{p} \in S\}$, so dass $\{i_1, \ldots, i_d\} \cup \mathcal{U}$ ein minimales Erzeugendensystem von $I/I_S^T I^p k^\times$ bildet. Der Burnsidesche Basissatz (2.4.3) liefert wieder den folgenden

(8.2.2) Satz. *Die Menge*

$$\mathcal{M}_0 := \{g_1, \ldots, g_d\} \cup \{h_{j\mathfrak{p}} | \mathfrak{p} \in S, u_{j\mathfrak{p}} \in \mathcal{U}\} \subseteq \mathcal{M}$$

ist ein minimales Erzeugendensystem von G_S^T.

8.3 Relationen von G_S^T

Wir behalten die Annahme $Б_S^T = 0$ bei. Sei F die freie pro-p-Gruppe, die von $\{\kappa_1, \ldots, \kappa_d\} \cup \{\lambda_{j\mathfrak{p}} | \mathfrak{p} \in S, u_{j\mathfrak{p}} \in \mathcal{U}\}$ erzeugt wird und

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\rho} G_S^T \longrightarrow 1$$

eine minimale Darstellung mit

$$\rho\kappa_j = g_j,\ j = 1, \ldots, d \quad \text{und} \quad \rho\lambda_{j\mathfrak{p}} = h_{j\mathfrak{p}},\ j = 1, \ldots, d_\mathfrak{p}, u_{j\mathfrak{p}} \in \mathcal{U}.$$

Für $u_{j\mathfrak{p}} \notin \mathcal{U}$ bezeichne $\lambda_{j\mathfrak{p}}$ ein Urbild von $h_{j\mathfrak{p}}$ unter ρ. Für $\mathfrak{p} \in S$ sei

$$1 \longrightarrow R_\mathfrak{p} \longrightarrow F_\mathfrak{p} \longrightarrow \mathcal{G}_\mathfrak{p} \longrightarrow 1$$

eine minimale Darstellung von $\mathcal{G}_\mathfrak{p}$. Hierbei wählen wir ein Erzeugendensystem $\sigma, \tau_1, \ldots, \tau_{d\mathfrak{p}} \in \mathcal{G}_\mathfrak{p}$, das via $\varphi_\mathfrak{p}$ auf $\sigma_\mathfrak{p}, h_{1\mathfrak{p}}, \ldots, h_{d_\mathfrak{p}\mathfrak{p}}$ abgebildet wird, wobei $\sigma_\mathfrak{p} \in G_S^T$ wie folgt gegeben ist:

(i) $\sigma_\mathfrak{p}$ ist ein Lift des Frobenius-Automorphismus von $\mathfrak{P}$ der maximalen Teilerweiterung von $k_S^T(p)$, in der $\mathfrak{P}$ unverzweigt ist.

(ii) $\sigma_\mathfrak{p}$ ist ein Lift von $(\pi_\mathfrak{p}, (k_S^T)^{ab}|k) \in (G_S^T)^{ab}$, wobei $\pi_\mathfrak{p}$ ein Primelement von $k_\mathfrak{p}$ bezeichnet.

Für $\mathfrak{p} \in S$ sei $s_\mathfrak{p} \in F$ ein Urbild von $\sigma_\mathfrak{p}$ unter ρ, das wie folgt gewählt ist: Nach Definition der Elemente $i_1, \ldots, i_d$ und $u_{1\mathfrak{p}}, \ldots, u_{d_\mathfrak{p}\mathfrak{p}}$ gibt es nach dem Nakayama-Lemma für jede Primstelle $\mathfrak{p}$ ein $c_\mathfrak{p} \in \mathbb{Z}$ mit $(c_\mathfrak{p}, p) = 1$ und $c_{\mathfrak{p}\nu}, c_{j\mathfrak{q}\mathfrak{p}} \in \mathbb{Z}_p$, so dass das Idel $\pi_\mathfrak{p}^{c_\mathfrak{p}}$ eine Darstellung

$$\pi_\mathfrak{p}^{c_\mathfrak{p}} = \left(\prod_{\nu=1}^{d} i_\nu^{c_{\mathfrak{p}\nu}}\right) (v_\mathfrak{q})_\mathfrak{q}\ (x_\mathfrak{p})$$

mit $x_\mathfrak{p} \in k^\times$, $v_\mathfrak{q} \in k_\mathfrak{q}^\times$ für $\mathfrak{q} \in T$ und

$$v_\mathfrak{q} = u_\mathfrak{q} u_{1\mathfrak{q}}^{c_{1\mathfrak{q}\mathfrak{p}}} \ldots u_{d_\mathfrak{q}\mathfrak{q}}^{c_{d_\mathfrak{q}\mathfrak{q}\mathfrak{p}}} \quad \text{für } \mathfrak{q} \notin T$$

besitzt, wobei $u_\mathfrak{q} \in U_\mathfrak{q}$ für $\mathfrak{q} \in S_p$ eine Einheitswurzel mit zu p teilerfremder Ordnung, für $\mathfrak{q} \notin S_p$ das Produkt einer solchen und einer Einseinheit mit zu p teilerfremder Ordnung und für $\mathfrak{q} \in S_\infty$ ein Element in $(k_\mathfrak{q}^\times)^p$ ist. Die Klassenkörpertheorie liefert die Gleichung

$$\sigma_\mathfrak{p} = \left(\prod_{\mu=1}^{d} g_\mu^{f_{\mathfrak{p}\mu}}\right) \left(\prod_{\mathfrak{q}\in S} h_{1\mathfrak{q}}^{f_{1\mathfrak{q}\mathfrak{p}}} \cdots h_{d_\mathfrak{q}\mathfrak{q}}^{f_{d_\mathfrak{q}\mathfrak{q}\mathfrak{p}}}\right) \sigma'_\mathfrak{p}$$

mit $\sigma'_\mathfrak{p} \in [G_S^T, G_S^T]$, wobei wir $f_{\mathfrak{p}\mu} := c_{\mathfrak{p}\mu} c_\mathfrak{p}^{-1}$ und $f_{j\mathfrak{q}\mathfrak{p}} := c_{j\mathfrak{q}\mathfrak{p}} c_\mathfrak{p}^{-1}$ setzen. Damit können wir nun $s_\mathfrak{p}$ so wählen, dass die Gleichung

$$s_\mathfrak{p} = \left(\prod_{\mu=1}^{d} \kappa_\mu^{f_{\mathfrak{p}\mu}}\right) \left(\prod_{\mathfrak{q}\in S} \lambda_{1\mathfrak{q}}^{f_{1\mathfrak{q}\mathfrak{p}}} \cdots \lambda_{d_\mathfrak{q}\mathfrak{q}}^{f_{d_\mathfrak{q}\mathfrak{q}\mathfrak{p}}}\right) s'_\mathfrak{p}$$

mit $s'_\mathfrak{p} \in [F, F]$ erfüllt ist.

Die Familie der Homomorphismen

$$\mathcal{G}_\mathfrak{p} \longrightarrow G \longrightarrow G_S^T\ , \mathfrak{p} \in S$$

ist zulässig bezüglich den Trägheitsuntergruppen $\mathcal{T}_\mathfrak{p}$ von $\mathcal{G}_\mathfrak{p}$ und nach (2.5.2) haben wir für $\mathfrak{p} \in S$ ein exaktes kommutatives Diagramm

$$\begin{tikzcd}
1 \arrow[r] & R_\mathfrak{p} \arrow[r] \arrow[d, "\overline{\chi}_\mathfrak{p}"] & F_\mathfrak{p} \arrow[r] \arrow[d, "\chi_\mathfrak{p}"] & \mathcal{G}_\mathfrak{p} \arrow[r] \arrow[d] & 1\ . \\
1 \arrow[r] & R \arrow[r] & F \arrow[r] & G_S^T \arrow[r] & 1
\end{tikzcd}$$

Mit $r_\mathfrak{p}$ bezeichnen wir die Bilder der lokalen Relationen, also der Erzeuger von $R_\mathfrak{p}$ als normale Untergruppe von $F_\mathfrak{p}$, unter $\overline{\chi}_\mathfrak{p}$. Es gilt die folgende

(8.3.1) Proposition.

(i) Für $\mathfrak{p} \in S \setminus S_p$ *mit* $\delta_\mathfrak{p} = 1$ *gilt*

$$r_\mathfrak{p} := \lambda_{1\mathfrak{p}}^{\mathfrak{N}(\mathfrak{p})-1}[\lambda_{1\mathfrak{p}}, s_\mathfrak{p}].$$

(ii) Für $\mathfrak{p} \in S \cap S_p$ *mit* $\delta_\mathfrak{p} = 1$ *gilt*

$$\lambda_{0\mathfrak{p}}^{q-1}\lambda_{1\mathfrak{p}}^{\hat{q}}[\lambda_{0\mathfrak{p}}, s_\mathfrak{p}][\lambda_{1\mathfrak{p}}, \lambda_{2\mathfrak{p}}]\cdots[\lambda_{d_\mathfrak{p},\mathfrak{p}}, \lambda_{(d_\mathfrak{p}-1),\mathfrak{p}}]r'_\mathfrak{p}$$

mit $\lambda_{0\mathfrak{p}} = \lambda_{d_\mathfrak{p}\mathfrak{p}}$ *und* $r'_\mathfrak{p} \in F_{(3,q)} \cap [F, F]$ *für* $q \neq 2$. q *bezeichnet hier die maximale* p*-Potenz, so dass* $k_\mathfrak{p}$ *die* q*-ten Einheitswurzeln enthält und* $\hat{q}$ *die maximale* p*-Potenz, so dass die maximale unverzweigte* p*-Erweiterung von* $k_\mathfrak{p}$ *die* $\hat{q}$*-ten Einheitswurzeln enthält.*

(iii) Für $\mathfrak{p} \in S_\mathbb{R}$ *und* $p = 2$ *gilt*

$$r_\mathfrak{p} = \lambda_{1\mathfrak{p}}^2.$$

Beweis. Die Behauptung folgt aus der Wahl der Erzeuger $\sigma, \tau_1, \ldots, \tau_{d\mathfrak{p}} \in \mathcal{G}_\mathfrak{p}$ und (3.1.2) sowie (3.2.5). □

Wir erhalten abschließend den folgenden

(8.3.2) Satz. *Gilt* $Б_S^T = 0$, *so wird in der obigen minimalen Darstellung* R *erzeugt von*

$$\{r_\mathfrak{p} | \mathfrak{p} \in S \setminus S_\mathbb{C}, \delta_\mathfrak{p} = 1\}.$$

Ist $\delta = 1, \theta = 0$ *so kann jede beliebige dieser Relationen weggelassen werden.*

Beweis. Wegen $Б_S^T = 0$ ist der Homomorphismus

$$\varphi_{S,T}^2 : H^2(G_S^T) \hookrightarrow \prod_{\mathfrak{p} \in S} H^2(\mathcal{G}_\mathfrak{p})$$

und im Falle $\delta = 1, \theta = 0$ auch der Homomorphismus

$$\varphi_{S,T,\mathfrak{q}}^2 : H^2(G_S^T) \hookrightarrow \prod_{\mathfrak{p} \in S \setminus \{\mathfrak{q}\}} H^2(\mathcal{G}_\mathfrak{p})$$

injektiv, wobei $\mathfrak{q}$ eine beliebige Primstelle in S bezeichnet. Die Behauptung folgt nun aus (2.5.2). □

8.4 Beispiele

(8.4.1) Beispiel. Sei $k = \mathbb{Q}, p = 2, S = \{\infty, 3, 5\}$ und $T = \{7\}$. Im Beispiel (7.1.3) haben wir gesehen, dass dann $Б_S^T = 0$ und

$$h^1(G_S^T) = h^2(G_S^T) = 1$$

gilt. Folglich ist

$$G_S^T \cong \mathbb{Z}/2^r\mathbb{Z}$$

für ein $r \geq 1$. Ferner gilt $d = \dim_{\mathbb{F}_2} I/I_\varnothing^T I^2 k^\times = 0$ und für die Dimensionen $d_l = \dim_{\mathbb{F}_2} U_l/U_l^2$ gilt

$$d_3 = d_5 = d_\infty = 1.$$

Als Erzeuger u_l von $U_l \bmod U_l^2$ wählen wir

$$u_3 = -1, \quad u_5 = 3, \quad u_\infty = -1.$$

Nach (8.1.1) bildet die Menge $\{h_3, h_5, h_\infty\}$ ein Erzeugendensystem von G_S^T, wobei h_l ein Element der Trägheitsgruppe einer über l liegenden Primstelle in $\mathbb{Q}_S^T(2)$ bezeichnet, dessen Einschränkung auf $(\mathbb{Q}_S^T(2))^{ab}$ durch $(u_l, (\mathbb{Q}_S^T(2))^{ab}|\mathbb{Q})$ gegeben ist. Als Erzeuger von $\mathbb{Q}_\varnothing^T$ wählen wir

$$\varepsilon_1 = 7, \quad \varepsilon_2 = \zeta = -1.$$

Die Koeffizienten des Gleichungssystems

$$(\varepsilon_\mu) = \prod_{l \in S} \beta_{l,\mu} u_l^{a_{l,\mu}}, \quad \mu = 1, 2$$

sind gegeben durch

$$\beta_{3,1} = \beta_{\infty,1} = 7,\ \beta_{5,1} = \frac{7}{3},\ a_{3,1} = a_{\infty,1} = 0,\ a_{5,1} = 1 \quad \text{und}$$
$$\beta_{3,2} = \beta_{\infty,2} = 1,\ \beta_{5,2} = -1,\ a_{3,2} = a_{\infty,2} = 1,\ a_{5,2} = 0.$$

Die Erzeuger u_5 und u_∞ können weggelassen werden und nach (8.2.2) ist damit h_3 ein Erzeuger von G_S^T. Nach (8.3.2) genügt h_3 aber der Relation $h_3^2 = 1$ und wir erhalten

$$G_S^T \cong \mathbb{Z}/2\mathbb{Z}$$

und damit

$$\mathbb{Q}_{\{\infty,3,5\}}^{\{7\}}(2) = \mathbb{Q}_{\{\infty,3,5\}}^{\{7\}}[2] = \mathbb{Q}(\zeta_3).$$

(8.4.2) Beispiel. Sei $k = \mathbb{Q}, p = 3, S = \{3, 7, 13\}$ und $T = \{5\}$. Nach (7.1.4) ist dann $Б_S^T = 0$ und es gilt

$$h^1(G_S^T) = h^2(G_S^T) = 2.$$

Wir haben wieder $d = \dim_{\mathbb{F}_3} I/I_\varnothing^T I^3 k^\times = 0$ und

$$d_3 = d_7 = d_{13} = 1.$$

Die Erzeuger u_l von $U_l \bmod U_l^3$ wählen wir als

$$u_3 = 4,\ u_7 = 3 \text{ und } u_{13} = 2.$$

Mit $\varepsilon = 5$ als Erzeuger von $\mathbb{Q}_\varnothing^T$ erhalten wir die Gleichung

$$(\varepsilon) = \prod_{l \in S} \beta_l u_l^{a_l},$$

wobei die Koeffizienten durch

$$\beta_3 = \frac{5}{4}, a_3 = 1, \beta_7 = \frac{5}{9}, a_7 = 2, \beta_{13} = 5 \text{ und } a_{13} = 0$$

gegeben sind. Wir können also einen der beiden Erzeuger u_3 und u_7 weglassen. Die Gruppe G_S^T wird also beispielsweise von den Elementen h_7 und h_{13} erzeugt. Die Exponenten $f_{q,l}$ der Gleichung

$$\sigma_l \equiv \prod_{l \in S} h_q^{f_{q,l}} \mod [G_S^T, G_S^T]$$

sind für $q, l \in S, l \neq 3$ gegeben durch

$$f_{3,7} = (-\log_3(7))(\log_3(4))^{-1} \in \mathbb{Z}_3,\ f_{3,13} = (-\log_3(13))(\log_3(4))^{-1} \in \mathbb{Z}_3$$
$$f_{7,13} = 3,\ f_{13,7} = 1,\ f_{7,7} = f_{13,13} = 0,$$

wobei $\log_3 : U_3^1 \twoheadrightarrow \mathbb{Z}_3$ den 3-adischen Logarithmus bezeichnet (vgl. hierzu [Ko], Chap. 11, example 11.11). Nach (8.3.2) werden die Relationen von G_S^T erzeugt von

$$\begin{aligned} r_7 &= \lambda_7^6[\lambda_7, s_7] &&= \lambda_7^6[\lambda_7, \lambda_3]^{f_{3,7}}[\lambda_7, \lambda_{13}]^{f_{13,7}} r_7' \\ r_{13} &= \lambda_{13}^{12}[\lambda_{13}, s_{13}] &&= \lambda_{13}^{12}[\lambda_{13}, \lambda_3]^{f_{3,13}}[\lambda_{13}, \lambda_7]^{f_{7,13}} r_{13}', \end{aligned}$$

wobei mit den Notationen aus dem vorangehenden Abschnitt $r_7', r_{13}' \in F_3$ gilt und wir $\lambda_l = \lambda_{1,l}$ setzen.

8.5 Der Fall $k = \mathbb{Q}, |T| = 1$ - G_S^T vom Koch-Typ

Sei p eine ungerade Primzahl. Wir werden uns nun wie im Beispiel (8.4.2) dem Fall $k = \mathbb{Q}$ zuwenden und Primstellenmengen T betrachten, die nur eine Primstelle enthalten. Mit L_p bezeichnen wir die in der zyklotomischen $\mathbb{Z}_p$-Erweiterung von $\mathbb{Q}$ enthaltene Erweiterung vom Grad p über $\mathbb{Q}$.

(8.5.1) Satz. *Sei $S := \{p, q_1, \ldots, q_k\}$ mit paarweise verschiedenen Primzahlen $q_i \equiv 1 \bmod p, i = 1, \ldots, k$. Ferner sei $T = \{q\}$, wobei $q \notin S$ eine Primzahl bezeichnet, die in der Erweiterung $L_p|\mathbb{Q}$ nicht voll zerlegt ist. Dann gilt:*

(i) $Б_S^T = 0$.

(ii) $(G_S^T)^{ab}$ *ist endlich.*

(iii) G_S^T *ist eine Schur-Gruppe mit*

$$h^1(G_S^T) = h^2(G_S^T) = k.$$

Ist $k \geq 4$, so ist G_S^T unendlich.

(iv) G_S^T *ist vom Koch-Typ.*

Beweis. Nach (7.1.2) ist $Б_S = 0$. Nun ist die Erweiterung L_p abelsch vom Grad p über $\mathbb{Q}$ und außerhalb p unverzweigt, also haben wir

$$L_p \subseteq k_{\{p\}}[p] \subseteq k_S[p].$$

Nach Voraussetzung ist die Primzahl q in L_p und damit insbesondere in $k_S[p]$ nicht voll zerlegt. Mit (7.1.1) erhalten wir (i).

Nehmen wir nun an, $(G_S^T)^{ab}$ sei unendlich. Dann würde $(\mathbb{Q}_S^T)^{ab}$ die zyklotomische $\mathbb{Z}_p$-Erweiterung von $\mathbb{Q}$ enthalten. Insbesondere müsste also die Primzahl q in der zyklotomischen $\mathbb{Z}_p$-Erweiterung voll zerlegt sein, was jedoch der Voraussetzung widerspricht und wir erhalten (ii).

Nach (5.2.3) und (6.2.3) erhalten wir für den Erzeuger- und Relationenrang von G_S^T

$$h^1(G_S^T) = k \quad \text{und} \quad h^2(G_S^T) \leq k.$$

Wegen (ii) muss aber $h^2(G_S^T) \geq h^1(G_S^T)$ gelten folglich ist $h^2(G_S^T) = k$. Ist $k \geq 4$, so folgt die Unendlichkeit von G_S^T und damit (iii) aus (2.4.6).

Wir möchten nun ein minimales Erzeugendensystem von G_S^T bestimmen. Wir betrachten zunächst den kanonischen Homomorphismus

$$\varphi : \mathop{*}_{i=1}^{k} \mathcal{T}_{\mathfrak{P}_i} \longrightarrow G_S^T ,$$

wobei wir für $1 \leq i \leq k$ mit $\mathfrak{P}_i$ ein über q_i liegendes Primideal in $k(p)$ und mit $\mathcal{T}_{\mathfrak{P}_i} \subseteq \mathrm{Gal}(\mathbb{Q}(p)|\mathbb{Q})$ die zugehörige Trägheitsgruppe bezeichnen. Der Kokern von φ ist gerade die Galoisgruppe $G_{\{p\}}^T$. Nun ist aber nach (5.2.6) und (6.2.4) die Gruppe $G_{\{p\}}$ frei vom Rang 1, also $G_{\{p\}} \cong \mathbb{Z}_p$ und damit ist $\mathbb{Q}_{\{p\}}(p)$ gerade die zyklotomische $\mathbb{Z}_p$-Erweiterung von $\mathbb{Q}$. Nach Voraussetzung ist die Primzahl q jedoch bereits in der Erweiterung L_p nicht voll zerlegt und wir erhalten $G_{\{p\}}^T = 0$. φ ist also surjektiv. Bezeichne τ_i nun für $1 \leq i \leq k$ einen Erzeuger der Trägheitsgruppe der unter $\mathfrak{P}_i$ liegenden Primstelle in $\mathbb{Q}_S^T(p)$ (vgl. (3.1.2)), so bildet die Menge $\{\tau_1, \ldots, \tau_i\}$ ein Erzeugendensystem von G_S^T, welches nach (iii) minimal ist. (i) liefert nach (6.1.7) den injektiven Homomorphismus

$$H^2(G_S^T) \hookrightarrow \prod_{l \in S} H^2(G_l) = \prod_{i=1}^{k} H^2(G_{q_i}) .$$

Sei F die freie pro-p-Gruppe mit den Erzeugern $x_1, \ldots, x_d$ und

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\rho} G_S^T \longrightarrow 1$$

eine minimale Darstellung von G_S^T mit $\rho(x_i) = \tau_i, i = 1, \ldots, k$. Nach (2.5.2) wird R als normale Untergruppe durch die Relationen

$$w_i = x_i^{q_i - 1}[x_i, y_i], \quad i = 1, \ldots, k$$

erzeugt, wobei y_i einen Lift des zu q_i gehörigen Frobenius-Automorphismus $\sigma_i, i = 1, \ldots, k$ bezeichnet. Für jedes $i = 1, \ldots, k$ haben wir die Gleichung

$$y_i = \prod_j x_j^{l_{ij}} y_i'$$

mit $l_{ij} \in \mathbb{Z}/p\mathbb{Z}$ und $y_i' \in F_2$ und somit

$$w_i \equiv x_i^{q_i - 1}[x_i, \prod_j x_j^{l_{ij}}] \equiv x_i^{q_i-1} \prod_{j \neq i} [x_i, x_j]^{l_{ij}} \mod F_3.$$

Damit ist G_S^T vom Koch-Typ und wir erhalten (iv). $\square$

(8.5.2) Korollar. *Seien wieder $S = \{p, q_1, \dots, q_k\}$ und $T = \{q\}$ Primstellenmengen von $\mathbb{Q}$, die die Voraussetzungen von (8.5.1) erfüllen. Ist zusätzlich $\Gamma_{\{q_1,\dots,q_k\}}(p)$ ein strikter Kreis, so gilt*

$$cd\ G_S^T = 2.$$

Beweis. Nach (8.5.1) ist G_S^T vom Koch-Typ und die Behauptung folgt unmittelbar aus (2.6.6). $\square$

Wir wollen abschließend noch ein Beispiel für $p = 3$ angeben. Für die Berechnung der Koeffizienten l_{ij} verweisen wir auf [Sa].

(8.5.3) Beispiel. Sei $p = 3$ und die Primstellenmengen S und T seien gegeben durch

$$S = \{3, 7, 13, 79, 97\} \quad \text{und} \quad T = \{5\}.$$

5 ist eine Primitivwurzel modulo 9, d.h. in $\mathbb{Q}(\zeta_9)$ träge und damit insbesondere in L_3 nicht voll zerlegt. Die Koeffizienten l_{ij} sind gegeben durch

$$l_{79,7} = l_{7,13} = l_{97,13} = l_{7,79} = 1,$$
$$l_{13,79} = l_{7,97} = l_{13,97} = 2$$

und $l_{ij} = 0$ für alle anderen Paare i, j. Das zugehörige Verbindungsdiagramm hat die Gestalt

$$\begin{tikzcd}
97 \arrow[r, bend left, "1"] & 13 \arrow[l, bend left, "2"] \arrow[d, "2"] \\
7 \arrow[u, "2"] \arrow[ur, "1"] \arrow[r, bend left, "1"] & 79 \arrow[l, bend left, "1"]
\end{tikzcd}$$

und enthält den nicht-singulären Kreis $\{97, 13, 79, 7\}$. Die Voraussetzungen von (8.5.2) sind also erfüllt.

(8.5.4) Bemerkung. Analoge Aussagen lassen sich für beliebige Zahlkörper k, für die die Leopoldt-Vermutung für die Primzahl p gilt, und Primstellenmengen T, deren Mächtigkeit gerade der Anzahl der unabhängigen $\mathbb{Z}_p$-Erweiterung von k entspricht, beweisen. Wir verweisen hierzu auf [Wi].

Literaturverzeichnis

[AT] Emil Artin, John Tate. *Class Field Theory.* Benjamin, 1967.

[Gr] Georges Gras. *Class Field Theory.* Springer, 2005.

[Ko] Helmut Koch. *Galois Theory Of p-Extensions.* Springer, 2002.

[La1] John Labute. Mild Pro-p-Groups and Galois Groups of p-Extensions of $\mathbb{Q}$. *J. Reine u. Angew. Mathematik*, 596, 2006.

[La2] Serge Lang. *Algebraic Number Theory.* Springer, 1986.

[Ne1] Jürgen Neukirch. *Klassenkörpertheorie.* Bibliographisches Institut, Mannheim, 1969.

[Ne2] Jürgen Neukirch. Über das Einbettungsproblem der algebraischen Zahlentheorie. *Invent. Math.*, 21, 1973.

[Ne3] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer, 1992.

[NSW] Jürgen Neukirch, Alexander Schmidt, Kay Wingberg. *Cohomology of Number Fields.* Springer, 2000.

[Sa] Landry Salle. Mild pro-p-groups as Galois groups over global fields. *preprint*, 2007.

[Se] Jean-Pierre Serre. *Galois Cohomology.* Springer, 1997.

[Saf] I.R. Šafarevič. Erweiterungen mit vorgegebenen Verzweigungsstellen (russ.). *Publ. Math. IHES*, 18, 1963. Engl. Übersetzung in *Amer. Math. Soc. Transl.*, 596, 1966.

[Vo] Denis Vogel. Circular sets of primes of imaginary quadratic number fields. *Preprints der Forschergruppe Algebraische Zykel und L-Funktionen Regensburg/Leipzig Nr. 5*, 596, 2006.

[Wa] Lawrence C. Washington. *Introduction to Cyclotomic Fields.* Springer, 1982.

[Wi] Kay Wingberg. Arithmetical Koch groups. *preprint*, 2007.

Erklärung

Hiermit versichere ich, dass ich diese Arbeit selbstständig unter Anleitung verfasst habe, dass ich keine anderen als die angegebenen Quellen benutzt habe, und dass ich alle Stellen, die dem Wortlaut oder dem Sinne nach anderen Werken entlehnt sind, durch die Angabe der Quellen als Entlehnungen kenntlich gemacht habe.

Heidelberg, den 29. Januar 2008