1 Die Gruppenalgebra einer Pro-p-Gruppe

Christoph Baumeister Maximilian Kremer
5. Vortrag (20.04.2010)

1.1 Relationenstruktur und Cup-Produkt

Wir gehen aus von einer beliebigen Pro-p-Gruppe G mit Erzeugerrang d, minimalen Erzeugendensystem $\{s_1, \ldots, s_d\}$ von G und minimaler Darstellung

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

von G. Dabei bezeichne $\{r_i | i \in I\}$ ein minimales Erzeugendensystem von R bezüglich obiger Darstellung.
Nach dem Burnsideschen Basissatz ist $\{s_\nu[G,G]\ , \nu = 1, \ldots, d\}$ ein minimales Erzeugendensystem von $G/[G,G]$. Die Ordnungen der Elemente $s_\nu[G,G]\ , \nu = 1, \ldots, d$, seine Vielfache von $q = p^n$ oder ∞.

Satz 1.1. *Unter den obigen Voraussetzungen sind die Inflation*

$$H^1(G, \mathbb{Z}/q\mathbb{Z}) \longrightarrow H^1(F, \mathbb{Z}/q\mathbb{Z})$$

und die Transgression

$$H^1(R, \mathbb{Z}/q\mathbb{Z})^G \longrightarrow H^2(G, \mathbb{Z}/q\mathbb{Z})$$

Isomorphismen.

Beweis. Betrachte die Hochschild-Serre Sequenz und beachte, dass F und G trivial auf $\mathbb{Z}/q\mathbb{Z}$ operieren:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(G, \mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\inf_1} & H^1(F, \mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\mathrm{res}_1} & H^1(R, \mathbb{Z}/q\mathbb{Z})^G \\ & & & & & & \downarrow \mathrm{tra}_1 \\ & & & & \underbrace{H^2(F, \mathbb{Z}/q\mathbb{Z})}_{=0} & \xleftarrow{\inf_2} & H^2(G, \mathbb{Z}/q\mathbb{Z}) \end{array}$$

wobei $H^2(F, \mathbb{Z}/q\mathbb{Z})$ verschwindet, weil F frei und $Z/q\mathbb{Z}$ ein Torsionsmodul ist (vgl. Satz aus dem 2. Vortrag). Benutzt man den Isomorphismus

$$F/F^{(2,q)} \xrightarrow{\sim} G/G^{(2,q)}\ , \tag{1}$$

der aus der minimalen Darstellung von G folgt, so erhält man

$$\begin{aligned} H^1(F, \mathbb{Z}/q\mathbb{Z}) &= Hom(F/F^{(2,q)}, \mathbb{Z}/q\mathbb{Z}) \\ &\cong Hom(G/G^{(2,q)}, \mathbb{Z}/q\mathbb{Z}) = H^1(G, \mathbb{Z}/q\mathbb{Z})\ , \end{aligned}$$

was in der oberen Sequenz insgesamt die Bijektivität von $\inf_1$ impliziert. Weiter folgt aufgrund der Exaktheit der Sequenz:

$$\inf_1 \text{ surjektiv} \quad \Longrightarrow \quad \operatorname{res}_1 \equiv 0 \quad \Longrightarrow \quad \operatorname{tra}_1 \text{ injektiv}$$

Also ist die Transgression insgesamt ein Isomorphismus. □

Aufgrund diese Satzes können wir einen für jedes $i \in I$ einen Homomorphismus

$$\varphi_i : \quad H^2(G, \mathbb{Z}/q\mathbb{Z}) \longrightarrow \mathbb{Z}/q \ , \quad \alpha \longmapsto \operatorname{tra}^{-1}\alpha(r_i)$$

definieren.
Ferner definieren wir eine $\{s_1, \ldots, s_d\}$ entsprechende Basis $\{\chi_1, \ldots, \chi_d\}$ von $H^1(G, \mathbb{Z}/q\mathbb{Z})$ durch

$$\chi_\nu(s_\mu) = \delta_{\nu\mu} \ , \quad \nu, \mu = 1, \ldots, d \ .$$

Weiter folgt sofort aus (1), dass $R \subset F^{(2,q)}$ gilt. Im Folgenden wollen wir die Struktur von $G^{(2,q)}/G^{(3,q)}$ angeben mit dem

Satz 1.2. *Jedes Element $g \in G^{(2,q)}$ besitzt eine Darstellung der Form*

$$g = \prod_{\nu=1}^{d} s_\nu^{a_\nu q} \prod_{\nu<\mu} [s_\nu, s_\mu]^{a_{\nu\mu}} g' \ , \quad g' \in G^{(3,q)} \ , \ 0 \le a_\nu, a_{\nu\mu} < q \ . \tag{2}$$

Falls G frei ist, so sind die a_ν und $a_{\nu\mu}$ sogar eindeutig bestimmt.

Beweis. Die Existenz folgt aus dem Umstand, dass man mit Hilfe von Kommutatoren ein ungeordnetes Produkt der s_ν, $\nu = 1, \ldots, d$ in ein geordnetes Produkt bringen kann, indem man das paarweise Vertauschen

$$s_j s_i = s_i s_j [s_i, s_j]^{-1}$$

ausnutzt. Da man dann auch gezwungen ist, die Kommutatoren zu verschieben, kommen neue Kommutatoren hinzu, in denen eine Komponente wiederum ein Kommutator ist. Solche Terme kann man dann aber gleich vernachlässigen, weil sie zu $G^{(3,q)}$ gehören und da beim Tauschen mit diesen Kommutatoren die neu entstehenden Kommutatoren wiederum zu $G^{(3,q)}$ gehören. Beachte, dass in der obigen Darstellung so die Reihenfolge der Kommutatoren keine Rolle spielt. Modulo $G^{(3,q)}$ kann man ferner die Koeffizienten zwischen 0 und q wählen. Nun ein kleines Beispiel:

Beispiel 1.3.

$$\begin{aligned} s_3\underbrace{s_2s_1} &= \underbrace{s_3s_1}\,s_2[s_1,s_2]^{-1} = s_1s_3\underbrace{[s_1,s_3]^{-1}s_2}[s_1,s_2]^{-1} \\ &= s_1s_3s_2[s_1,s_3]^{-1}\underbrace{[[s_1,s_3]^{-1},s_2]}_{=:a}[s_1,s_2]^{-1} = s_1s_3s_2[s_1,s_3]^{-1}\underbrace{[s_1,s_2]^{-1}}_{=:b}\underbrace{a}_{\in G^{(3,q)}}\underbrace{[a,b]}_{\in G^{(3,q)}} \\ &\equiv s_1\underbrace{s_3s_2}[s_1,s_3]^{-1}[s_1,s_2]^{-1}G^{(3,q)} \equiv s_1s_2s_3[s_2,s_3]^{-1}[s_1,s_3]^{-1}[s_1,s_2]^{-1}G^{(3,q)} \end{aligned}$$

Für die Eindeutigkeit der Koeffizienten $a_{\nu\mu}$ in obiger Darstellung betrachte man den Kozykel

$$x:\ x(g_1,g_2) = \chi_\nu(g_1)\chi_\mu(g_2).$$

Da $x(g_1g_2,g_3)+x(g_1,g_2) = x(g_2,g_3)+x(g_1,g_2g_3)$, ist $\partial_3 x = 0$. Da ferner G frei ist, existiert eine stetige Abbildung $\psi_{\nu\mu}$ von F nach $\mathbb{Z}/q\mathbb{Z}$ mit $\partial_2\psi_{\nu\mu} = x$:

$$\chi_\nu(g_1)\chi_\mu(g_2) = \psi_{\nu\mu}(g_1)+\psi_{\nu\mu}(g_2)-\psi_{\nu\mu}(g_1g_2). \tag{3}$$

Es kann obdA[1] angenommen werden, dass $\psi_{\nu\mu}(s_x) = 0$ für $x = 1,\dots,d$.
Für die weiteren Berechnungen benötigen wir folgendes technisches

Lemma 1.4. *Für eine natürliche Zahl m erhält man*

$$\psi_{\nu\mu}(s_x^m) = \begin{cases} 0 & \text{für } \nu \neq \mu, \\ -\binom{m}{2}\delta_{\nu x} & \text{für } \nu = \mu. \end{cases} \tag{4}$$

Beweis.

$$\begin{aligned} \psi_{\nu\mu}(s_x^{m+1}) &\overset{(3)}{=} \psi_{\nu\mu}(s_x)+\psi_{\nu\mu}(s_x^m)-\chi_\nu(s_x)\chi_\mu(s_x^m) \\ &= -m\delta_{\nu x}\delta_{\mu x}+\psi_{\nu\mu}(s_x^m). \end{aligned}$$

Daher ist induktiv für $\nu \neq \mu$:

$$\psi_{\nu\mu}(s_x^{m+1}) = -m\delta_{\nu x}\delta_{\mu x}+\psi_{\nu\mu}(s_x^m) = \psi_{\nu\mu}(s_x^m) = \ldots = 0$$

und für $\nu = \mu$ ist, ebenfalls induktiv,

$$\psi_{\nu\mu}(s_x^{m+1}) = -m\delta_{\nu x}\delta_{\mu x}+\psi_{\nu\mu}(s_x^m) \overset{IV}{=} -m\delta_{\nu x}^2-\binom{m}{2}\delta_{\nu x} = -\binom{m+1}{2}\delta_{\nu x}.$$

□

[1] $\psi_{\nu\mu}$ kann um ein $\phi \in \mathrm{Hom}(G,A)$ abgeändert werden, da für $\widetilde{\psi}_{\nu\mu}(x) := \psi_{\nu\mu}(x)-\phi(x)$ gilt:
$\widetilde{\psi}_{\nu\mu}(x)+\widetilde{\psi}_{\nu\mu}(y)-\widetilde{\psi}_{\nu\mu}(xy) = \psi_{\nu\mu}(x)+\psi_{\nu\mu}(y)-\psi_{\nu\mu}(xy)$.

Da weiterhin

$$\psi_{\nu\mu}(g^{-1}) + \psi_{\nu\mu}(g) = \psi_{\nu\mu}(1) + \chi_\nu(g^{-1})\chi_\mu(g) = -\chi_\nu(g)\chi_\mu(g) \tag{5}$$

wird:

$$\begin{aligned}
\psi_{\nu\mu}([s_x, s_\lambda]) &\overset{(3)}{=} \psi_{\nu\mu}(s_x^{-1}) + \psi_{\nu\mu}(s_\lambda^{-1}s_x s_\lambda) - \chi_\nu(s_x^{-1})[-\chi_\mu(s_\lambda) + \chi_\mu(s_x) + \chi_\mu(s_\lambda)] \\
&\overset{(3)}{=} -\psi_{\nu\mu}(s_x) + \psi_{\nu\mu}(s_\lambda^{-1}s_x s_\lambda) \\
&= \psi_{\nu\mu}(s_\lambda^{-1}s_x s_\lambda) \\
&= \psi_{\nu\mu}(s_\lambda^{-1}) + \psi_{\nu\mu}(s_x s_\lambda) - \chi_\nu(s_\lambda^{-1})[\chi_\mu(s_x) + \chi_\mu(s_\lambda)] + \psi_{\nu\mu}(s_\lambda) - \psi_{\nu\mu}(s_\lambda) \\
&\overset{(3)}{=} \psi_{\nu\mu}(s_x s_\lambda) + \delta_{\nu\lambda}\delta_{\mu x} \\
&= \psi_{\nu\mu}(s_x) + \psi_{\nu\mu}(s_\lambda) - \chi_\nu(s_x)\chi_\mu(s_\lambda) + \delta_{\nu\lambda}\delta_{\mu x} \\
&= -\delta_{\nu x}\delta_{\mu\lambda} + \delta_{\nu\lambda}\delta_{\mu x}
\end{aligned}$$

Das heißt:

$$\psi_{\nu\mu}([s_x, s_\lambda]) = \begin{cases} -1 & \text{für } \nu = x,\ \mu = \lambda, \\ 1 & \text{für } \nu = \lambda,\ \mu = x, \\ 0 & \text{sonst.} \end{cases} \tag{6}$$

Lemma 1.5. *$\psi_{\nu\mu}$ verschwindet auf $G^{(3,q)}$, das heißt:*

$$\psi_{\nu\mu}(G^{(3,q)}) = 0$$

Beweis. Mit $x = g_1^q[g_2, g_3] \in G^{(2,q)}$ und $g_1, g_2, g_3, y \in G$, gilt:

$$\begin{aligned}
\psi_{\nu\mu}(x^q) &= \psi_{\nu\mu}(x) + \psi_{\nu\mu}(x^{q-1}) - \chi_\nu(x)\chi_\mu(x^{q-1}) \\
&= \psi_{\nu\mu}(x) + \psi_{\nu\mu}(x^{q-1}) - \left(\underbrace{q\chi_\nu(g_1)}_{\equiv 0} + \underbrace{\chi_\nu([g_2, g_3])}_{\equiv 0} \right) (q-1)\left(\chi_\mu(g_1^q) + \chi_\mu([g_2, g_3])\right) \\
&\equiv \psi_{\nu\mu}(x) + \psi_{\nu\mu}(x^{q-1}) \equiv \ldots \equiv q\psi_{\nu\mu}(x) \equiv 0 \bmod q\mathbb{Z},
\end{aligned}$$

$$\begin{aligned}
\psi_{\nu\mu}([x, y]) &= \psi_{\nu\mu}(x^{-1}) + \psi_{\nu\mu}(y^{-1}xy) - \chi_\nu(x^{-1})\chi_\mu(y^{-1}xy) \\
&= \big(\psi_{\nu\mu}(x^{-1}) + \psi_{\nu\mu}(x) - \chi_\nu(x^{-1})\chi_\mu(x)\big) + \big(\psi_{\nu\mu}(y^{-1}) + \psi_{\nu\mu}(y) - \chi_\nu(y^{-1})\chi_\mu(y)\big) \\
&\quad - 2\chi_\nu(y^{-1})\chi_\mu(x) - 2\chi_\nu(x^{-1})\chi_\mu(y) \\
&= \psi_{\nu\mu}(x^{-1}x) + \psi_{\nu\mu}(y^{-1}y) - 2\chi_\nu(y^{-1})\chi_\mu(x) - 2\chi_\nu(x^{-1})\chi_\mu(y) \\
&= -2\chi_\nu(y^{-1})\underbrace{\chi_\mu(g_1^q[g_2, g_3])}_{\equiv 0} + 2\underbrace{\chi_\nu(g_1^{-q}[g_2, g_3]^{-1})}_{\equiv 0}\chi_\mu(y) \\
&\equiv 0 \bmod q\mathbb{Z}.
\end{aligned}$$

und somit wird für ein beliebiges Element $x^q[z,y] \in G^{(3,q)}$:

$$\psi_{\nu\mu}(x^q[z,y]) = \psi_{\nu\mu}(x^q) + \psi_{\nu\mu}([z,y]) - q\chi_\nu(x)\chi_\mu([z,y]) \equiv 0 \bmod q\mathbb{Z}$$

□

Wir schließen nun den Beweis der Eindeutigkeit der $a_{\nu\mu}$ in der Darstellung (2) ab. Für $\nu < \mu$ gilt nämlich:

$$\begin{aligned}\psi_{\hat{\nu}\hat{\mu}}(g) &= \psi_{\hat{\nu}\hat{\mu}}(\prod_{\nu=1}^{d} s_\nu^{a_{\nu q}} \prod_{\nu<\mu}[s_\nu,s_\mu]^{a_{\nu\mu}} g') \\ &= \underbrace{\psi_{\hat{\nu}\hat{\mu}}(\prod_{\nu=1}^{d} s_\nu^{a_{\nu q}})}_{=:A} + \underbrace{\psi_{\hat{\nu}\hat{\mu}}(\prod_{\nu<\mu}[s_\nu,s_\mu]^{a_{\nu\mu}} g')}_{=:B} - \underbrace{\chi_{\hat{\nu}}(\prod_{\nu=1}^{d} s_\nu^{a_{\nu q}})\chi_{\hat{\mu}}(\prod_{\nu<\mu}[s_\nu,s_\mu]^{a_{\nu\mu}} g')}_{=:C}\end{aligned}$$

Die einzelnen Summanden werden zu

$A = \psi_{\hat{\nu}\hat{\mu}}(s_1^{a_1 q}) + \psi_{\hat{\nu}\hat{\mu}}(\prod_{\nu=2}^{d} s_\nu^{a_{\nu q}}) - \underbrace{\chi_{\hat{\nu}}(s_1^{a_1 q})}_{\equiv 0}\chi_{\hat{\mu}}(\prod_{\nu=2}^{d} s_\nu^{a_{\nu q}})$

$\overset{\text{Lemma 1.4}}{\equiv} \psi_{\hat{\nu}\hat{\mu}}(\prod_{\nu=2}^{d} s_\nu^{a_{\nu q}}) \equiv \ldots \equiv 0 \bmod q\mathbb{Z}$;

$C = (\sum_{\nu=1}^{d} a_\nu q \chi_{\hat{\nu}}(s_\nu))(\chi_{\hat{\mu}}(g') + \sum_{\nu<\mu} a_{\nu\mu}\chi_{\hat{\mu}}([s_\nu,s_\mu]) \equiv 0 \bmod q\mathbb{Z}$;

$B = \psi_{\hat{\nu}\hat{\mu}}(\prod_{\nu<\mu}[s_\nu,s_\mu]^{a_{\nu\mu}}) + \psi_{\hat{\nu}\hat{\mu}}(g') - \chi_{\hat{\nu}}(\prod_{\nu<\mu}([s_\nu,s_\mu]^{a_{\nu\mu}}))\chi_{\hat{\mu}}(g') \overset{\text{Lemma 1.5}}{\equiv} \psi_{\hat{\nu}\hat{\mu}}(\prod_{\nu<\mu}[s_\nu,s_\mu]^{a_{\nu\mu}})$

$= \psi_{\hat{\nu}\hat{\mu}}([s_{\nu_1},s_{\mu_1}]^{a_{\nu_1\mu_1}}) + \psi_{\hat{\nu}\hat{\mu}}\left(\prod_{\nu<\mu,(\nu,\mu)\neq(\nu_1,\mu_1)}[s_\nu,s_\mu]^{a_{\nu\mu}}\right) \equiv \ldots \equiv \sum_{\nu<\mu}\psi_{\hat{\nu}\hat{\mu}}([s_\nu,s_\mu]^{a_{\nu\mu}})$

$\equiv \sum_{\nu<\mu}(\psi_{\hat{\nu}\hat{\mu}}([s_\nu,s_\mu]) + \psi_{\hat{\nu}\hat{\mu}}([s_\nu,s_\mu]^{a_{\nu\mu}-1}) - \chi_{\hat{\nu}}([s_\nu,s_\mu])\chi_{\hat{\mu}}([s_\nu,s_\mu]^{a_{\nu\mu}-1}))$

$\equiv \sum_{\nu<\mu}(\psi_{\hat{\nu}\hat{\mu}}([s_\nu,s_\mu]) + \psi_{\hat{\nu}\hat{\mu}}([s_\nu,s_\mu]^{a_{\nu\mu}-1})) = \ldots = \sum_{\nu<\mu} a_{\nu\mu}\psi_{\hat{\nu}\hat{\mu}}([s_\nu,s_\mu])$

$\equiv \overline{a}_{\hat{\nu}\hat{\mu}}(-1) = -\overline{a}_{\hat{\nu}\hat{\mu}} \bmod q\mathbb{Z}$.

Daher sind die Exponenten $a_{\nu\mu}$ eindeutig durch

$$\psi_{\hat{\nu}\hat{\mu}}(g) \equiv -\overline{a}_{\hat{\nu}\hat{\mu}} \bmod q\mathbb{Z} \tag{7}$$

festgelegt. □

Satz 1.6. *Sei G eine Pro-p-Gruppe vom Erzeugendenrang d mit obiger minimaler Darstellung, $q = p^f$ eine p-Potenz mit $R \subset F^{(2,q)}$, $\{s_1,\ldots,s_d\}$ ein Erzeugendensystem von F und $\{r_i | i \in I\}$ ein minimales Relationensystem von G. Sei ferner r_i wie in (2) als*

$$r_i = \prod_{x=1}^{d} s_x^{a_x^i q} \prod_{\nu<\mu}[s_\nu,s_\mu]^{a_{\nu\mu}^i} r_i',\ r_i' \in F^{(3,q)}$$

gegeben. Dann gilt für $i \in I$ und $\nu, \mu = 1, \dots, d$

$$\varphi_i(\chi_\nu \cup \chi_\mu) = \psi_{\nu\mu}(r_i) = \begin{cases} -\overline{a}^i_{\nu\mu} & \text{für } \nu < \mu, \\ -\binom{q}{2}\overline{a}^i_\nu & \text{für } \nu = \mu. \end{cases}$$

Hierbei bezeichnet $\cup$ das Cup-Produkt, das durch die Multiplikation im Ring $\mathbb{Z}/p\mathbb{Z}$ gegeben ist[2]*, und φ_i, χ_ν seien die oben definierten Funktionen.*

Beweis. Gemäß der Definition der Transgression[3]

$$\mathrm{tra} : H^1(R, \mathbb{Z}/q\mathbb{Z})^G \to H^2(G, \mathbb{Z}/q\mathbb{Z})$$

ist das Cup-Produkt $\chi_\nu \cup \chi_\mu$ das Bild von $\psi_{\nu\mu}$ unter der Transgression. Damit gilt

$$\varphi_i(\chi_\nu \cup \chi_\mu) = \mathrm{tra}^{-1}(\chi_\nu \cup \chi_\mu)(r_i) = \psi_{\nu\mu}(r_i).$$

Für $\nu < \mu$ wird wie in (Satz 1.2) gesehen $\psi_{\nu\mu}(r_i) = -\overline{a}^i_{\nu\mu}$.
Im Falle $\nu = \mu$ ergibt sich Folgendes[4]:

$$\psi_{\nu\nu}(r_i) = \psi_{\nu\nu}\Big(\prod_{x=1}^{d} s_x^{a^i_x q} \prod_{\lambda<\mu} [s_\lambda, s_\mu]^{a^i_{\lambda\mu} r'_i}\Big) = \psi_{\nu\nu}\Big(\prod_{x=1}^{d} s_x^{a^i_x q}\Big) + \psi_{\nu\nu}\Big(\prod_{\lambda<\mu} [s_\lambda, s_\mu]^{a^i_{\lambda\mu} r'_i}\Big) =$$

$$\psi_{\nu\nu}\Big(\prod_{x=1}^{d} s_x^{a^i_x q}\Big) = \sum_{x=1}^{d} a^i_x \psi_{\nu\nu}(s_x^q) \overset{\text{Lemma 1.3}}{\equiv} -\tbinom{q}{2}\overline{a}^i_\nu. \qquad \square$$

Satz 1.7. *Die exakte Sequenz*

$$0 \xrightarrow{q} \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q^2\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \to 0$$

---

[2]Das Cup-Produkt wurde in folgendem kommutativen Diagramm als Fortführung des Tensorprodukts der 0-ten Dimension eingeführt:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & H^0(G,\mathbb{Z}/q\mathbb{Z}) \times H^0(G,\mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\otimes} & H^0(\mathbb{Z}/q\mathbb{Z}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle id} \quad \downarrow{\scriptstyle \delta} & & \downarrow{\scriptstyle \delta} & & \\
0 & \longrightarrow & H^0(G,\mathbb{Z}/q\mathbb{Z}) \times H^1(G,\mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\cup} & H^1(G,\mathbb{Z}/q\mathbb{Z}) & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \delta} \quad \downarrow{\scriptstyle id} & & \downarrow{\scriptstyle \delta} & & \\
0 & \longrightarrow & H^1(G,\mathbb{Z}/q\mathbb{Z}) \times H^1(G,\mathbb{Z}/q\mathbb{Z}) & \xrightarrow{\cup} & H^2(G,\mathbb{Z}/q\mathbb{Z}) & \longrightarrow & 0
\end{array}$$

Somit überträgt sich das Tensorprodukt, welches der Multiplikation in $\mathbb{Z}/q\mathbb{Z}$ entspricht, auf die untere Zeile.

[3]vgl. (Koch) §3.7

[4]Hierbei wird verwendet, dass die Charaktere χ_ν, χ_μ wie bereits gesehen auf Kommutatoren und $R^{(3,q)}$ verschwinden und aus (6) auf Grund von $\nu = \mu$ nur der Fall $\psi_{\nu\mu}([s_\lambda, s_\mu]) = 0$ auftritt.

induziert eine exakte Sequenz von Kohomologiegruppen.
Bezeichnet man mit B den Randoperator $\delta_2 : H^1(G, \mathbb{Z}/q\mathbb{Z}) \to H^2(G, \mathbb{Z}/q\mathbb{Z})$, so gilt für $i \in I$ und $\nu = 1, \dots, d$

$$\varphi_i(B\chi_\nu) = -\overline{a}^i_\nu.$$

Beweis. Für $\xi = x + q\mathbb{Z},\ 0 \le x \le q$, bezeichne $\hat{\xi} = x + q^2\mathbb{Z}$ das Bild der Inklusion. Dann ist

$$\phi(g_1, g_2) = \frac{1}{q}(\widehat{\chi_\nu(g_1)} + \widehat{\chi_\nu(g_2)} - \widehat{\chi_\nu(g_1 g_2)})$$

ein Repräsentant von $B\chi_\nu$. Da F frei, und somit $H^2(F, \mathbb{Z}/q\mathbb{Z}) = 0$, existiert ein stetiges ψ_ν von F nach $\mathbb{Z}/q\mathbb{Z}$, sodass

$$\psi_\nu(h_1) + \psi_\nu(h_2) - \psi_\nu(h_1 h_2) = \frac{1}{q}(\widehat{\chi_\nu(h_1)} + \widehat{\chi_\nu(h_2)} - \widehat{\chi_\nu(h_1 h_2)}) \qquad (8)$$

für alle $h_1, h_2 \in F$. Durch Abänderung um einen geeigneten Homomorphismus können wir wieder annehmen, dass

$$\psi_\nu(s_x) = 0 \text{ für } x = 1, \dots, d.$$

Direkt aus (8) folgert man

$$\psi_\nu(h^{-1}) = -\psi_\nu(h) + \frac{1}{q}(\widehat{\chi_\nu(h)} + \widehat{\chi_\nu(h^{-1})}),\ h \in F,$$

und

$$\begin{aligned}
\psi_\nu([h_1, h_2]) &= \psi_\nu(h_1^{-1}) + \psi_\nu(h_2^{-1} h_1 h_2) - \frac{1}{q}(\widehat{\chi_\nu(h_1^{-1})} + \widehat{\chi_\nu(h_2^{-1} h_1 h_2)} - \chi_\nu(\widehat{h_1^{-1} h_2^{-1} h_1 h_2})) \\
&= -\psi_\nu(h_1) + \psi_\nu(h_2^{-1} h_1 h_2) \\
&= -\psi_\nu(h_1) + \psi_\nu(h_2^{-1}) + \psi_\nu(h_1 h_2) - \frac{1}{q}(\widehat{\chi_\nu(h_2^{-1})} + \widehat{\chi_\nu(h_1 h_2)} - \widehat{\chi_\nu(h_1)}) \\
&= -\psi_\nu(h_1) - \psi_\nu(h_2) + \psi_\nu(h_1 h_2) + \frac{1}{q}(\widehat{\chi_\nu(h_2)} + \widehat{\chi_\nu(h_1)} - \widehat{\chi_\nu(h_1 h_2)}) \\
&= 0.
\end{aligned}$$

ψ_ν verschwindet somit auf der von $s_1, \dots, s_{\nu-1}, s_{\nu+1}, \dots, s_d, [F, F]$ erzeugten Untergruppe von F. Für s_ν ergibt sich abschließend

$$\psi_\nu(s_\nu^{aq}) = -\overline{a},$$

da

$$\begin{aligned}\psi_\nu(s_\nu^{aq}) &= \psi_\nu(s_\nu) + \psi_\nu(s_\nu^{aq-1}) - \frac{1}{q}(\widehat{\chi_\nu(s_\nu)} + \widehat{\chi_\nu(s_\nu^{aq-1})} - \widehat{\chi_\nu(s_\nu^{aq})}) \\ &= \psi_\nu(s_\nu^{aq-1}) - \frac{1}{q}(\widehat{1} + \widehat{\chi_\nu(s_\nu^{aq-1})} - \widehat{aq\chi_\nu(s_\nu)}) \\ &= \psi_\nu(s_\nu) + \psi_\nu(s_\nu^{aq-2}) - \frac{1}{q}(2\cdot\widehat{1} + \widehat{\chi_\nu(s_\nu^{aq-2})} - \widehat{\chi_\nu(s_\nu^{aq-1})} + \widehat{\chi_\nu(s_\nu^{aq-1})}) \\ &= \ldots = -\frac{1}{q}(aq\widehat{1}) = -\overline{a}\end{aligned}$$

Daher ist

$$\psi_i(B\chi_\nu) = \psi_\nu(r_i) = -\overline{a}_\nu^i.$$

□

2 Hilfsmittel aus der Algebraischen Zahlentheorie

In diesem Abschnitt sei K/k eine beliebige (also endliche oder unendliche) algebraische Erweiterung von Zahlkörpern.

Grundbegriffe für unendliche Erweiterungen

Definition 2.1. *Eine **Primstelle** $\mathfrak{P}$ von K ist eine Äquivalenzklasse von nichttrivialen Bewertungen von K. Ist $L \subset K$ ein Zwischenkörper, so bezeichnen wir mit $\mathfrak{p}$ die Einschränkung von $\mathfrak{P}$ auf L.*

Definition 2.2. *Eine **algebraische Vervollständigung** $K_\mathfrak{P}$ von K bezüglich $\mathfrak{P}$ und k ist der induktive Limes $\varinjlim L_\mathfrak{p} = \bigcup L_\mathfrak{p}$, den wir über alle endlichen Zwischenkörper L von K/k bilden. Dabei bezeichnet $\mathfrak{p}$ die Einschränkung von $\mathfrak{P}$ auf L und $L_\mathfrak{p}$ die Vervollständigung von L bezüglich $\mathfrak{p}$.*

Definition 2.3. *Eine Primstelle heißt **endlich** (bzw. **unendlich**), falls sie aus nicht-archimedischen (bzw. archimedischen) Bewertung besteht. Eine endliche Primstelle heißt auch **Primdivisor**. Eine unendliche Primstelle heißt **reell** (bzw. **komplex**), wenn die zugehörige Vervollständigung $\mathbb{R}$ (bzw. $\mathbb{C}$) ist.*

Definition 2.4. *Sei L ein beliebiger Zwischenkörper von K/k und $v_\mathfrak{P}$ eine Exponentialbewertung von K mit Einschränkungen $v_{\mathfrak{p}_L}$ (bzw. $v_\mathfrak{p}$) auf L (bzw. k). Die Primstelle $\mathfrak{P}$ heißt **unverzweigt** bezüglich L/k, wenn der Wertebereich von $v_{\mathfrak{p}_L}$ gleich dem Wertebereich von $v_\mathfrak{p}$ entspricht.*

Bemerkung 2.5. *Offensichtlich ist $\mathfrak{P}$ in K/k genau dann unverzweigt, wenn $\mathfrak{P}$ für jede endliche Teilerweiterung L von K/k unverzweigt ist, denn:*

- *„$\Longrightarrow$“: folgt aus $v_{\mathfrak{P}}(K^\times) \geq v_{\mathfrak{p}}(L^\times)$ für $K \supset L$, $\mathfrak{p}$ Einschräkung von $\mathfrak{P}$ auf L*
- *„$\Longleftarrow$“: folgt aus $K = \bigcup L$, wobei $L \subset K$ die endlichen Zwischenkörper von K durchläuft*

Auf diese Weise überträgt sich der Satz, dass eine Primstelle $\mathfrak{P}$ des Kompositums KL/k genau dann unverzweigt ist, wenn die Beschränkung von $\mathfrak{P}$ auf K und L über k unverzweigt sind, von endlichen auf unendliche Erweiterungen.

Definition 2.6. *Eine unendliche Primstelle $\mathfrak{P}/\mathfrak{p}$ heißt unverzweigt bezüglich K/k, wenn $\kappa_{\mathfrak{P}} = \kappa_{\mathfrak{p}}$ gilt. Dabei bezeichnet $\kappa_{\mathfrak{p}}$ (bzw. $\kappa_{\mathfrak{P}}$) den Restklassenkörper von k (bzw. K) bezüglich $\mathfrak{p}$ (bzw. $\mathfrak{P}$).*

Normale Erweiterungen

Ist im Folgenden nichts anderes vermerkt, so gehen wir stets von einer normalen Erweiterung K/k, bzw. L/k und einer nicht-archimedischen Bewertung aus.

Definition 2.7. *Die **Zerlegungsgruppe** von K ist definiert als*

$$\mathcal{Z}_{\mathfrak{P}}(K/k) := \{g \in G(K/k) \mid v_{\mathfrak{P}}(ga) = v_{\mathfrak{P}}(a) \quad \forall a \in K\}$$

*und die **Trägheitsgruppe** als*

$$\mathcal{T}_{\mathfrak{P}}(K/k) := \{g \in G(K/k) \mid v_{\mathfrak{P}}(ga - a) > 0 \quad \forall a \in K \text{ mit } v_{\mathfrak{P}}(a) \geq 0\}.$$

Bemerkung 2.8. *Die Trägheitsgruppe ist Normalteiler in der Zerlegungsgruppe.*

Beweis. Normalteilereigenschaft: Seien $z \in \mathcal{Z}_{\mathfrak{P}}, t \in \mathcal{T}_{\mathfrak{P}}$, dann folgt für $a \in K$ mit $v_{\mathfrak{P}}(a) > 0$:

$$v_{\mathfrak{P}}(z^{-1}tza - a) = v_{\mathfrak{P}}(zz^{-1}tza - za) = v_{\mathfrak{P}}(t(za) - (za)) > 0$$

Inklusion „$\mathcal{T}_{\mathfrak{P}} \subset \mathcal{Z}_{\mathfrak{P}}$“: Sei $\sigma \in \mathcal{T}_{\mathfrak{P}}$ und $a \in K$. Beweis per Widerspruch: Ohne Einschränkung sei angenommen, dass $v(a) \geq 0$ und $v(\sigma a) > v(a)$, andernfalls betrachte man $v(\frac{1}{a}) \geq 0$ bzw. $v(\sigma\frac{1}{a}) > v(\frac{1}{a})$. Es gilt:

$$v(\sigma a) = v(\sigma a - a + a) \geq \min\{v(\sigma a - a), v(a)\}$$

$$v(a) = v(a - \sigma a + \sigma a) \geq \min\{v(\sigma a - a), v(\sigma a)\}$$

- Fall 1: $v(\sigma a - a) > v(\sigma a) > v(a)$. Widerspruch zur 2. Ungleichung.
- Fall 2: $v(\sigma a) \geq v(\sigma a - a) > v(a)$. Widerspruch, ganz analog.
- Fall 3: $v(\sigma a) > v(a) \geq v(\sigma a - a)$. Aus der scharfen Dreiecksungleichung erhalten wir $v(a) = v(\sigma a - a) > 0$. Für a mit $v(a) = 0$ ergibt sich ein Widerspruch. Sei also $v(a) > 0$. Dann existiert eine Uniformisierende $p \in K$ und ein $l \in \mathbb{N}$ mit

$$0 = v\left(\frac{a}{p^l}\right) = \min\left\{v\left(\sigma\frac{a}{p^l} - \frac{a}{p^l}\right), v\left(\sigma\frac{a}{p^l}\right)\right\} = v\left(\sigma\frac{a}{p^l} - \frac{a}{p^l}\right) > 0$$

  was wiederum einen Widerspruch darstellt.

Also muss $v(\sigma a) = v(a)$ gelten. Die Gruppeneigenschaften folgen dann durch schnelle Rechnungen v.a. aus dieser Inklusion. □

Satz 2.9. *Sei K/k eine normale Erweiterung mit endlicher Primstelle $\mathfrak{P}$ und L/k sei eine Teilerweiterung davon. Dann gilt:*

$$\mathcal{Z}_{\mathfrak{P}}(K/L) = G(K/L) \cap \mathcal{Z}_{\mathfrak{P}}(K/k)$$

$$\mathcal{T}_{\mathfrak{P}}(K/L) = G(K/L) \cap \mathcal{T}_{\mathfrak{P}}(K/k)$$

Falls L/k normal ist und $\mathfrak{p}$ die Einschränkung von $\mathfrak{P}$ auf L bezeichnet, dann gilt:

$$\mathcal{Z}_{\mathfrak{p}}(L/k) = G(K/L)\mathcal{Z}_{\mathfrak{P}}(K/k)/G(K/L)$$
$$\mathcal{T}_{\mathfrak{p}}(L/k) = G(K/L)\mathcal{T}_{\mathfrak{P}}(K/k)/G(K/L)$$

Beweis. Der erste Teil ergibt sich aus der Definition. Zum zweiten Teil, exemplarisch für $\mathcal{Z}_{\mathfrak{p}}(L/k)$: Für beliebige Erweiterungen folgt dies aus dem Zwischenschritt

$$\mathcal{Z}_{\mathfrak{P}}(L/k) = \mathcal{Z}_{\mathfrak{P}}(K/k)/G(K/L) \cap \mathcal{Z}_{\mathfrak{P}}(K/k) \cong G(K/L)\mathcal{Z}_{\mathfrak{P}}(K/k)/G(K/L)$$

unter Benutzung des 1. Isomorphiesatzes; beachte $G(K/L) \trianglelefteq G(K/k)$. Analog sieht man dies für die Trägheitsgruppe. □

Bemerkung 2.10. *Aus dem vorstehenden Satz folgt, dass*

$$\mathcal{Z}_{\mathfrak{P}}(K/k) \cong \varprojlim \mathcal{Z}_{\mathfrak{p}}(L/k)\ , \quad \mathcal{T}_{\mathfrak{P}}(K/k) \cong \varprojlim \mathcal{T}_{\mathfrak{p}}(L/k)\ ,$$

wobei L über alle endlichen normalen Teilerweiterungen von K/k läuft und $\mathfrak{p}$ die Einschränkung von $\mathfrak{P}$ auf L darstellt.

Beweis. Zum Beweis betrachte man das projektive System aller Zerlegungsgruppen $\mathcal{Z}_\mathfrak{p}(L/k) = G(K/L)\mathcal{Z}_\mathfrak{P}(K/k)/G(K/L)$, wobei L stets endlich normal ist. Wenden wir auf beiden Seiten den projektiven Limes über die L an, so folgt aufgrund von $\varprojlim G(K/L) = 1$:

$$\varprojlim \mathcal{Z}_\mathfrak{p}(L/k) \cong \mathcal{Z}_\mathfrak{P}(K/k)$$

Analog für die Trägheitsgruppe. □

Satz 2.11. *Sei* $\mathfrak{p}$ *diesmal die Einschränkung von* $\mathfrak{P}$ *auf* k*. Das Bild der Injektion*

$$\varphi_\mathfrak{P} : \quad G(K_\mathfrak{P}/k_\mathfrak{p}) \longrightarrow G(K/k)\ ,\ \sigma \longmapsto \sigma|_K$$

die durch die kanonische Einbettung $K \hookrightarrow K_\mathfrak{P}$ *induziert ist, ist gleich der Zerlegungsgruppe* $\mathcal{Z}_\mathfrak{P}(K/k)$*.*

Beweis. Zu zeigen ist also $G(K_\mathfrak{P}/k_\mathfrak{p}) \cong \mathcal{Z}_\mathfrak{P}(K/k)$. Wir zeigen zunächst, dass die Zerlegungsgruppe $\mathcal{Z}_\mathfrak{P}(K/k)$ genau aus den bezüglich der Bewertung $\mathfrak{P}$ stetigen Automorphismen von $G(K/k)$ besteht. Die Stetigkeit von $\sigma \in \mathcal{Z}_\mathfrak{P}(K/k)$ folgt sofort aus der Definition der Zerlegungsgruppe. Sei umgekehrt $\sigma \in G(K/k)$ ein stetiger Automorphismus, dann gilt

$$|x|_\mathfrak{P} < 1 \implies |\sigma x|_\mathfrak{P} < 1\ , \tag{9}$$

da $|x|_\mathfrak{P} < 1$ bedeutet, dass $(x^n)_{n\in\mathbb{N}}$ eine Nullfolge ist, und aufgrund der Stetigkeit gilt dies auch für $(\sigma x^n)_{n\in\mathbb{N}}$. Aus (3) folgt gerade (siehe Äquivalenz von Normen lokaler Körper), dass $v_\mathfrak{P}$ und $v_\mathfrak{P}\,\sigma$ äquivalent sind. Da nun aber gilt $v_\mathfrak{P}|_K = v_\mathfrak{P}\ \sigma|_K$, muss der Exponent, um den sich äquivalente Normen unterscheiden, gerade 1 sein und damit gilt $v_\mathfrak{P} = v_\mathfrak{P}\ \sigma$. Die Behauptung folgt jetzt daraus, dass K dicht in $K_\mathfrak{P}$ liegt und somit lässt sich jedes Element $\sigma \in \mathcal{Z}_\mathfrak{P}(K/k)$ eindeutig stetig fortsetzen zu einem $k_\mathfrak{p}$-Automorphismus von $K_\mathfrak{p}$, indem wir die Stetigkeit von σ ausnutzen. Wegen der Eindeutigkeit der Fortsetzung haben wir damit die Umkehrabbildung von $\varphi_\mathfrak{P}$ erhalten. □

Definition 2.12. *Das Bild von* $\varphi_\mathfrak{P}$ *einer unedlichen Primstelle* $\mathfrak{P}$ *sei definiert als* $\mathcal{Z}_\mathfrak{P}(K/k) = \mathcal{T}_\mathfrak{P}(K/k)$*.*

Der nachfolgende Satz ist eine Verallgemeinerung einer Tatsache, die wir schon für endliche Körpererweiterungen kennen:

Satz 2.13. *Sei* K/k *eine normale Erweiterung. Der Fixkörper* $K^{\mathcal{T}_\mathfrak{P}(K/k)}$ *ist die maximale Erweiterung von* k*, in der* $\mathfrak{P}$ *unverzweigt ist.*

Beweis. Zunächst wollen wir die Unverzweigtheit von $K^{\mathcal{T}_{\mathfrak{P}}(K/k)}$ zeigen. Diese folgt aufgrund von Bemerkung 2.5 aus

$$K^{\mathcal{T}_{\mathfrak{P}}(K/k)} = \bigcup_{\mathfrak{p}} L^{\mathcal{T}_{\mathfrak{p}}(L/k)} \ ,$$

wobei die Vereinigung über alle Einschränkungen $\mathfrak{p}$ von $\mathfrak{P}$ auf endliche normale Teilerweiterungen L/k von K/k zu nehmen ist. Denn:
Sei $z \in K^{\mathcal{T}_{\mathfrak{P}}(K/k)}$. Indem wir die normale Hülle von $k(z)$ bilden, welche endlich ist, können wir annehmen, dass z in einem solchen L enthalten ist. Mit der Projektion $\mathcal{T}_{\mathfrak{P}}(K/k) \twoheadrightarrow \mathcal{T}_{\mathfrak{p}}(L/k)$ findet man für jedes $\sigma_L \in \mathcal{T}_{\mathfrak{P}}(L/k)$ ein $\sigma \in \mathcal{T}_{\mathfrak{P}}(K/k)$ mit $\sigma|_L = \sigma_L$, so dass $\sigma_L z = \sigma|_L z = z$; also $z \in L^{\mathcal{T}_{\mathfrak{p}}(L/k)}$. Umgekehrt sei nun $z \in \bigcup_{\mathfrak{p}} L^{\mathcal{T}_{\mathfrak{P}}(L/k)}$ gegeben, dann gibt es ein L mit $z \in L^{\mathcal{T}_{\mathfrak{P}}(L/k)}$. Nehmen wir nun ein beliebiges $\sigma \in \mathcal{T}_{\mathfrak{P}}(K/k)$, so folgt aufgrund der Isomorphie $\mathcal{T}_{\mathfrak{P}}(K/k) \cong \varprojlim \mathcal{T}_{\mathfrak{p}}(L/k)$, dass $\sigma z = \sigma|_L z = z$, was die Behauptung zeigt. Da wir wissen, dass $L^{\mathcal{T}_{\mathfrak{P}}(L/k)}$ für alle L unverzweigt ist, so ist deshalb auch $K^{\mathcal{T}_{\mathfrak{P}}(K/k)}$ unverzweigt. Nun zur Maximalität von $K^{\mathcal{T}_{\mathfrak{P}}(K/k)}$ bezüglich Verzweigtheit: Wenn U/k eine beliebige Teilerweiterung von K/k darstellt, für die $\mathfrak{P}$ unverzweigt ist, so ist jede endliche Teilerweiterung von U/k in einer Erweiterung $K^{\mathcal{T}_{\mathfrak{p}}(L/k)}$ enthalten, indem wir die normale Hülle bilden, um L zu bekommen und die Maximalität von $L^{\mathcal{T}_{\mathfrak{p}}(L/k)}$ bezüglich Verzweigtheit ausnutzen. Daher gilt $U \subset K^{\mathcal{T}_{\mathfrak{P}}(K/k)}$.

□

Der Frobenius-Automorphismus

Wir betrachten jetzt einen Körper k und einen Primdivisor $\mathfrak{p}$ von k, für die $\kappa_{\mathfrak{p}}$ endlich ist. Wir kennen bereits den folgenden

Satz 2.14. *Sei K/k eine normale endliche Erweiterung und $\mathfrak{P}$ sei eine Fortsetung von $\mathfrak{p}$ auf K. Dann ist der natürliche Morphismus*

$$\mathcal{Z}_{\mathfrak{P}}(K/k) \longrightarrow G(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}}) \ , \ \sigma \longmapsto \bar{\sigma} \quad mit \ \ \bar{\sigma}(a \mod \mathfrak{P}) = \sigma a \mod \mathfrak{P}$$

surjektiv mit Kern $\mathcal{T}_{\mathfrak{P}}(K/k)$.

Wir sollen bald sehen, dass sich dies auch auf unendliche normale Erweiterungen K/k überträgt.

Satz-Definition 2.15. *Für endliche $\kappa_{\mathfrak{p}}$ ist $G(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}})$ kanonisch isomorph zu einer Faktorgruppe der totalen Vervollständigung $\widehat{\mathbb{Z}} = \varprojlim_{n\in\mathbb{N}} \mathbb{Z}/n\mathbb{Z}$ von $\mathbb{Z}$. Potenzierung mit $|\kappa_{\mathfrak{p}}|$ ist ein Automorphismus von $\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}}$, der $G(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}})$*

erzeugt. Ein Urbild dieses Automorphismus $\sigma_{\mathfrak{P}}(K/k)$ unter der Abbildung des vorherigen Satzes nennt man ***Frobenius-Automorphismus*** *von $\mathfrak{P}$ bezüglich $K^{\mathcal{T}_{\mathfrak{P}}(K/k)}/k$.*

Satz 2.16. *Sei $\mathfrak{P}$ in K/k unverzweigt, L/k eine normale Erweiterung von K/k und $\mathfrak{p}$ die Einschränkung von $\mathfrak{P}$ auf L. Dann ist:*

$$\sigma_{\mathfrak{p}}(L/k) = \sigma_{\mathfrak{P}}(K/k)|_L$$

Beweis. Das folgt aus der Identifizierung $\mathcal{Z}_{\mathfrak{P}}/\mathcal{T}_{\mathfrak{P}} \cong G(\kappa_{\mathfrak{P}}/\kappa_{\mathfrak{p}})$, weil es für die rechte Seite gilt. □