2. Vortrag - Erzeuger und Relationen

Anna Schilling Simon Rube

6. Mai 2010

1 Definition der kohomologischen Dimension

Definition 1. Eine Pro-p-Gruppe G hat die kohomologische Dimension $\operatorname{cd} G = n$, wenn $n \geq 0$ minimal mit $H^n(G) \neq 0$ und $H^{n+1}(G) = 0$ ist. Wenn $H^n(G) \neq 0$ für alle natürlichen Zahlen n ist, so setzen wir $\operatorname{cd} G = \infty$.

Satz 2. *Sei G eine Pro-p-Gruppe mit $\operatorname{cd} G = n$. Dann ist $H^\nu(G, A) = 0$ für alle $\nu > n$ und alle Torsionsmoduln A.*

Beweis. Ein Torsionsmodul ist induktiver Limes seiner endlichen Teilmoduln, daher kann man sich nach Koch, Satz 3.17 [1] auf endliche G-Moduln A beschränken. Wir setzen

$$A_p := \{a \in A \mid \exists\, n \in \mathbb{N} \,\mathrm{mit}\, p^n a = 0\}$$
$$\bar{A}_p := \{a \in A \mid \mathrm{ggT}(\operatorname{ord} a,\, p) = 1\}$$

Man rechnet leicht nach, dass A_p und $\bar{A}_p$ Untermoduln von A sind. Ebenso klar ist $A_p \cap \bar{A}_p = \{0\}$. Für $a \in A$ schreiben wir $\operatorname{ord} a = kp^n$ mit $n \in \mathbb{N}$ und $p \nmid k$. Wir finden $z_1, z_2 \in \mathbb{Z}$ mit $1 = z_1 k + z_2 p^n$ und es folgt $a = 1a = z_1(ka) + z_2(p^n a)$ mit $ka \in A_p$ und $p^n a \in \bar{A}_p$. Insgesamt haben wir also $A = A_p \oplus \bar{A}_p$ gezeigt.

Koch, Satz 3.6 [2] liefert uns für alle $\nu \geq 0$

$$H^\nu(G, A) \cong H^\nu(G, A_p) \oplus H^\nu(G, \bar{A}_p)$$

Wir wenden uns zunächst $H^\nu(G, \bar{A}_p)$ für $\nu \geq 1$ zu:

[1] Ist $\{[G_i, A_i], i \in I, [\varphi_i^j, \psi_i^j]\}$ ein induktives System über der Kategorie $\mathcal{C}$ mit dem Limes $[G, A]$, dann ist $\{H^n(G_i, A_i), i \in I, \psi_i^{j*}\}$ für alle $n \geq 0$ ein induktives System abelscher Gruppen, und die natürliche Abbildung $\varinjlim H^n(G_i, A_i) \to H^n(G, A)$ ist ein Isomorphismus

[2] Es sei der G-Modul A direkte Summe der G-Moduln A_i, $i \in I$. Dann ist $H^n(G, A)$ direkte Summe der abelschen Gruppen $H^n(G, A_i)$, $i \in I$.

Für $\bar{f} \in H^\nu(G, \bar{A}_p)$ gilt $\operatorname{ord} \bar{f} \mid \operatorname{ord} \bar{A}_p$, also $p \nmid \operatorname{ord} \bar{f}$ wegen $p \nmid \operatorname{ord} \bar{A}_p$. Anwenden von Koch, Satz 3.20 [1] mit $m = \operatorname{ord} \bar{f}$ resultiert in $\operatorname{ord} \bar{f} = 1$, also $\bar{f} = 0$. Daher ist $H^\nu(G, \bar{A}_p) = 0$.

Wir können uns folglich auf endliche G-Moduln der Form A_p, also auf G-Moduln A von p-Potenzordnung, einschränken. Für diese gibt es eine Kompositionsreihe von Untermoduln

$$\{0\} \subset A_1 \subset A_2 \subset \ldots \subset A_s = A$$

mit $\operatorname{ord} A_i = p^i$ und daher $A_{i+1}/A_i \cong \mathbb{F}_p$ (als G-Modul) für alle $i = 1, \ldots, s-1$. Aus der exakten Sequenz

$$0 \to A_i \to A_{i+1} \to \mathbb{F}_p \to 0$$

erhalten wir die Kohomologiesequenz

$$0 \to H^0(G, A_i) \to \ldots \to H^n(G) \to H^{n+1}(G, A_i) \to H^{n+1}(G, A_{i+1}) \to H^{n+1}(G) \to \ldots$$

Wegen $H^{n+1}(G) = 0$ haben wir Surjektionen

$$H^{n+1}(G, A_i) \twoheadrightarrow H^{n+1}(G, A_{i+1})$$

für alle $i = 1, \ldots, s-1$. Verketten liefert insgesamt eine Surjektion

$$0 = H^{n+1}(G) \cong H^{n+1}(G, A_1) \twoheadrightarrow H^{n+1}(G, A)$$

und es folgt $H^{n+1}(G, A) = 0$.

Mittels Dimensionsverschiebung wollen wir dieses Ergebnis auf höhere Dimensionen übertragen. Ohne Einschränkung sei A ein endlicher G-Modul. Wir kennen die exakte Sequenz

$$0 \to A \to M_G(A) \to \underbrace{M_G(A)/A}_{=:C} \to 0$$

von G-Moduln. Da A endlich ist, sind $M_G(A)$ und C Torsionsmoduln. Nach Koch, Satz 3.7 [2] ist $M_G(A)$ für Dimensionen ≥ 1 kohomologisch trivial und daher $H^\nu(G, C) \cong H^{\nu+1}(G, A)$ für alle $\nu \geq 1$. Induktiv folgt dann aus dem schon Bewiesenen und dieser Isomorphie $H^\nu(G, A) = 0$ für alle $\nu > n$ und alle Torsionsmoduln A. $\square$

Satz 3. *Ist G eine Pro-p-Gruppe und $H \subset G$ eine abgeschlossene Untergruppe von G, so gilt*

$$cd\, H \leq cd\, G$$

[1] Ist m eine natürliche Zahl und $G = \varprojlim_{i \in I} G_i$, wobei die Gruppen G_i von endlicher zu m primer Ordnung sind, und ist A ein beliebiger G-Modul, dann haben die Elemente von $H^n(G, A)$ für $n \geq 1$ endliche zu m prime Ordnung.

[2] Es sei G eine proendliche Gruppe und X eine abelsche Gruppe. Dann ist $H^n(G, M_G(X)) = 0$ für $n \geq 1$.

Beweis. $M_G^H(\mathbb{F}_p)$ ist ein Torsionsmodul und nach Koch, Satz 3.9 [1] und dem eben bewiesenen Satz 2 gilt

$$H^\nu(H,\mathbb{F}_p) \cong H^\nu(G, M_G^H(\mathbb{F}_p)) = 0 \quad \forall\, \nu > \operatorname{cd} G$$

□

2 Euler-Poincarésche Charakteristik

Definition 4. Für eine endliche Gruppe A der Ordnung p^ν setzen wir $\dim A = \nu$. Wir definieren die Euler-Poincarésche Charakteristik eine Pro-p-Gruppe G mit $\operatorname{cd} G < \infty$ und $\operatorname{ord} H^n(G) < \infty$ für alle $n \geq 1$ durch

$$\chi(G) := \sum_{n=0}^{\infty} (-1)^n \dim H^n(G)$$

Ist A ein endlicher G-Modul von p-Potenzordnung, so setzen wir entsprechend

$$\chi(G,A) := \sum_{n=0}^{\infty} (-1)^n \dim H^n(G,A)$$

Bemerkung 5.

i) Jedes Element $\neq 0$ aus $H^n(G)$ hat Ordnung p. Im Falle $\operatorname{ord} H^n(G) < \infty$ ist $H^n(G)$ daher eine p-Gruppe und $\dim H^n(G)$ ist wohldefiniert. Wegen $\operatorname{cd} G < \infty$ ist die Summe zu $\chi(G)$ tatsächlich endlich und $\chi(G)$ ist eine wohldefinierte ganze Zahl.

ii) Ist A ein endlicher G-Modul von p-Potenzordnung, so folgt aus $\operatorname{ord} H^n(G) < \infty$ bereits $\operatorname{ord} H^n(G,A) < \infty$. Dies überlegt man sich schnell mit Induktion nach $\dim A$:

Für $\dim A = 1$ gilt $A \cong \mathbb{F}_p$ und daher $H^n(G,A) \cong H^n(G)$. Für $\dim A > 1$ wählen wir einen Untermodul A' von A der Dimension $\dim A - 1$. Die exakte Sequenz von G-Moduln $0 \to A' \to A \to \mathbb{F}_p \to 0$ liefert uns folgenden Abschnitt aus der zugehörigen Kohomologiesequenz

$$\ldots \to H^n(G,A') \xrightarrow{f} H^n(G,A) \xrightarrow{g} H^n(G) \to \ldots$$

Es gilt $H^n(G,A)/\operatorname{im} f \cong \operatorname{im} g$ und nach Induktionsannahme ist $\operatorname{im} f$ endlich, ebenso $\operatorname{im} g$ wegen $\operatorname{ord} H^n(G) < \infty$. Daher ist $\operatorname{ord} H^n(G,A) < \infty$.

Da jedes Element aus $H^n(G,A)$ p-Potenzordnung hat, ist $H^n(G,A)$ p-Gruppe und $\dim H^n(G,A)$ ist wohldefiniert. Wegen $H^\nu(G,A) = 0$ für alle $\nu > \operatorname{cd} G$ gemäß Satz 2 ist somit auch $\chi(G,A)$ eine wohldefinierte ganze Zahl.

[1] Satz von Shapiro: Es sei G eine proendliche Gruppe, H eine abgeschlossene Untergruppe von G und A ein H-Modul. Der Morphismus von $[G, M_G^H(A)]$ in $[H,A]$ induziert Isomorphismen von $H^n(G, M_G^H(A))$ in $H^n(H,A)$ für $n \geq 0$.

Lemma 6. *Sei*

$$0 \to A_0 \to B_0 \to C_0 \to \ldots \to A_n \to B_n \to C_n \to 0$$

eine exakte Sequenz von p-Gruppen. Dann gilt

$$\sum_{\nu=0}^{n}(-1)^\nu dim\, B_\nu = \sum_{\nu=0}^{n}(-1)^\nu dim\, A_\nu + \sum_{\nu=0}^{n}(-1)^\nu dim\, C_\nu$$

Beweis. Wir zeigen die Behauptung per Induktion nach der Länge n der Sequenz.

Induktionsanfang: Aus der exakten Sequenz $0 \to A_0 \xrightarrow{f_0} B_0 \xrightarrow{g_0} C_0 \to 0$ erhalten wir $B_0/\operatorname{im} f_0 \cong C_0$, also $\operatorname{ord} B_0 = \operatorname{ord} A_0 \cdot \operatorname{ord} C_0$. Daraus folgt $\dim B_0 = \dim A_0 + \dim C_0$.

Induktionsschritt: Aus der exakten Sequenz

$$0 \to A_0 \to \ldots \to B_n \xrightarrow{g_n} C_n \xrightarrow{\delta_n} A_{n+1} \xrightarrow{f_{n+1}} B_{n+1} \xrightarrow{g_{n+1}} C_{n+1} \to 0$$

erhalten wir folgende exakte Sequenzen

$$\begin{aligned}
&0 \to A_0 \to B_0 \to C_0 \to \ldots \to A_n \to B_n \to \operatorname{im} g_n \to 0 \\
&0 \to \operatorname{im} g_n \to C_n \to \operatorname{im} \delta_n \to 0 \\
&0 \to \operatorname{im} \delta_n \to A_{n+1} \to \operatorname{im} f_{n+1} \to 0 \\
&0 \to \operatorname{im} f_{n+1} \to B_{n+1} \to C_{n+1} \to 0
\end{aligned}$$

Induktionsanfang und -annahme liefern

$$\sum_{\nu=0}^{n}(-1)^\nu \dim B_\nu = \sum_{\nu=0}^{n}(-1)^\nu \dim A_\nu + \sum_{\nu=0}^{n-1}(-1)^\nu \dim C_\nu + (-1)^n \dim \operatorname{im} g_n \tag{1}$$

$$\dim C_n = \dim \operatorname{im} g_n + \dim \operatorname{im} \delta_n \tag{2}$$

$$\dim A_{n+1} = \dim \operatorname{im} \delta_n + \dim \operatorname{im} f_{n+1} \tag{3}$$

$$\dim B_{n+1} = \dim \operatorname{im} f_{n+1} + \dim C_{n+1} \tag{4}$$

Addieren von Gleichung (2) und (3) und multiplizieren mit $(-1)^n$ ergibt

$$(-1)^n \dim C_n + (-1)^{n+1} \dim A_{n+1} = (-1)^n \dim \operatorname{im} g_n + (-1)^{n+1} \dim \operatorname{im} f_{n+1} \tag{5}$$

Addieren von (1) mit $(-1)^{n+1}(4)$ ergibt

$$\begin{aligned}
\sum_{\nu=0}^{n+1}(-1)^\nu \dim B_\nu &= \sum_{\nu=0}^{n}(-1)^\nu \dim A_\nu + \sum_{\substack{\nu=0 \\ \nu\neq n}}^{n+1}(-1)^\nu \dim C_\nu \\
&\quad + (-1)^n \dim \operatorname{im} g_n + (-1)^{n+1} \dim \operatorname{im} f_{n+1} \\
&\overset{(5)}{=} \sum_{\nu=0}^{n+1}(-1)^\nu \dim A_\nu + \sum_{\nu=0}^{n+1}(-1)^\nu \dim C_\nu
\end{aligned}$$

□

Lemma 7. *i) Sei* $0 \to A_1 \to A_2 \to A_3 \to 0$ *eine exakte Sequenz von endlichen G-Moduln mit p-Potenzordnung. Dann gilt*

$$\chi(G, A_2) = \chi(G, A_1) + \chi(G, A_3)$$

ii) Für einen G-Modul A der Ordnung p^s gilt

$$\chi(G, A) = s\,\chi(G)$$

Beweis. i) Wir betrachten die zugehörige Kohomologiesequenz

$$0 \to H^0(G, A_1) \ldots \to H^n(G, A_3) \to 0 \to 0 \to \ldots$$

Beachte: $n := cd\,G$. Mit Lemma 6 folgt sofort die Aussage.

ii) Induktion nach s: Der Fall $s = 1$ ist wegen $A \cong \mathbb{F}_p$ klar. Sei nun $s > 1$ und A' ein Untermodul von A der Ordnung p^{s-1}. Wir erhalten die exakte Sequenz $0 \to A' \to A \to \mathbb{F}_p \to 0$ und daher mit Teil i) und der Induktionsannahme

$$\chi(G, A) = \chi(G, A') + \chi(G) = (s-1)\chi(G) + \chi(G) = s\chi(G)$$

□

Satz 8. *Ist G eine Pro-p-Gruppe mit Euler-Poincaréscher Charakteristik und H eine abgeschlossene Untergruppe von G von endlichem Index, so gilt*

$$\chi(H) = (G : H)\,\chi(G)$$

Beweis. Nach dem Satz von Shapiro gilt

$$H^\nu(H, \mathbb{F}_p) \cong H^\nu(G, M_G^H(\mathbb{F}_p)) \quad \forall\, \nu \geq 0$$

Wir erinnern an die Definition von $M_G^H(\mathbb{F}_p)$:

$$M_G^H(\mathbb{F}_p) = \{f : G \to \mathbb{F}_p \,|\, f \text{ ist stetig und } h \cdot f(x) = f(hx) \text{ für alle } h \in H, x \in G\}$$

Da H auf $\mathbb{F}_p$ trivial operiert, gilt $f(x) = f(hx)$ für alle $h \in H, x \in G$. Folglich hängt f nur von den Rechtsnebenklassen von H in G ab. Umgekehrt überlegt man sich leicht, dass jede Abbildung $f : G \to \mathbb{F}_p$, welche nur von den Rechtsnebenklassen von H in G abhängt, stetig ist, denn H ist als abgeschlossene Untergruppe von endlichem Index auch offen in G. Es gilt daher

$$M_G^H(\mathbb{F}_p) \cong \mathrm{Abb}(H\backslash G, \mathbb{F}_p)$$

und folglich $\mathrm{ord}\, M_G^H(\mathbb{F}_p) = p^{(G:H)}$. Mit Lemma $7, ii$) schließen wir

$$\chi(H) = \chi(G, M_G^H(\mathbb{F}_p)) = (G : H)\,\chi(G)$$

□

Definition 9. Ist G eine Pro-p-Gruppe, für die $\operatorname{ord} H^\nu(G) < \infty$ für $0 \leq \nu \leq n$ gilt, so definieren wir die partielle Euler-Poincarésche Charakteristik

$$\chi_n(G) := \sum_{\nu=0}^{n} (-1)^\nu \dim H^\nu(G)$$

Für einen G-Modul A von p-Potenzordnung setzen wir entsprechend

$$\chi_n(G, A) := \sum_{\nu=0}^{n} (-1)^\nu \dim H^\nu(G, A)$$

Die Wohldefiniertheit dieser Ausdrücke ergibt sich wie in Bemerkung 5.

Lemma 10. *Für einen G-Modul A von p-Potenzordnung gilt*

$$(-1)^n\, \chi_n(G, A) \leq (-1)^n\, \mathit{dim}\, A\, \chi(G)$$

Beweis. Induktion nach $s := \dim A$: Für $s = 1$ ist die Aussage wegen $A \cong \mathbb{F}_p$ klar. Sei daher $s > 1$ und A' ein Untermodul von A der Dimension $s - 1$. Die exakte Sequenz $0 \to A' \to A \to \mathbb{F}_p \to 0$ von G-Moduln liefert uns die Kohomologiesequenz

$$0 \to H^0(G, A') \to \ldots \to H^n(G, A') \to H^n(G, A) \xrightarrow{g_n} H^n(G) \to H^{n+1}(G, A') \to \ldots$$

Hieraus bilden wir eine endliche exakte Sequenz von p-Gruppen

$$0 \to H^0(G, A') \to \ldots \to H^n(G, A') \to H^n(G, A) \to \operatorname{im} g_n \to 0$$

Beachte: $\dim \operatorname{im} g_n \leq \dim H^n(G)$. Lemma 6 liefert

$$\chi_n(G, A) = \chi_n(G, A') + \chi_{n-1}(G) + (-1)^n \dim \operatorname{im} g_n$$

Nach Induktionsannahme gilt

$$(-1)^n\, \chi_n(G, A') \leq (-1)^n\, (s-1)\, \chi_n(G)$$

Zusammen ergibt sich

$$\begin{aligned}
(-1)^n\, \chi_n(G, A) &\leq (-1)^n\, (s-1)\, \chi_n(G) + (-1)^n\, \chi_{n-1}(G) + \dim \operatorname{im} g_n \\
&\leq (-1)^n\, (s-1)\, \chi_n(G) + (-1)^n\, \chi_{n-1}(G) + \dim H^n(G) \\
&= (-1)^n \left((s-1)\, \chi_n(G) + \underbrace{\chi_{n-1}(G) + (-1)^n \dim H^n(G)}_{=\chi_n(G)} \right) \\
&= (-1)^n\, s\, \chi_n(G)
\end{aligned}$$

$\square$

Satz 11. *Es sei G eine Pro-p-Gruppe mit partieller Euler-Poincaréscher Charakteristik $\chi_n(G)$, $\mathfrak{U}$ eine Menge von offenen Untergruppen von G, die ein volles Umgebungssystem der Einheit von G bilden, und es gelte*

$$\chi_n(U) = (G:U)\,\chi_n(G) \quad \forall\, U \in \mathfrak{U}$$

Dann ist $cd\,G \leq n$.

Beweis. Wir zeigen $H^{n+1}(G) = 0$.

Sei hierzu $\bar{a} \in H^{n+1}(G)$, wobei der Vertreter a im Kern der Abbildung $d_{n+1} : K^{n+1}(G, \mathbb{F}_p) \to K^{n+2}(G, \mathbb{F}_p)$ liegt. Da a stetig ist, gibt es gemäß Koch, Kapitel 1.5 ein $U \in \mathfrak{U}$, sodass a nur von den Nebenklassen von U in G abhängt. Wir betrachten folgendes Diagramm über der Kategorie $\mathcal{C}$

$$\begin{tikzcd}
(G, \mathbb{F}_p) \arrow[rr] \arrow[dr] & & (G, M_G^U(\mathbb{F}_p)) \arrow[dl] \\
& (U, \mathbb{F}_p) &
\end{tikzcd}$$

Die Morphismen zwischen den Pro-p-Gruppen sind klar, die nichttrivialen Morphismen zwischen den abelschen Gruppen sind gegeben durch $M_G^U(\mathbb{F}_p) \to \mathbb{F}_p, f \mapsto f(1_G)$ und $\mathbb{F}_p \to M_G^U(\mathbb{F}_p), x \mapsto f_x$, wobei f_x von der Form $G \to \mathbb{F}_p, g \mapsto gx$ ist. Hiernach ist klar, dass obiges Diagramm kommutiert. Durch Anwenden des kovarianten Funktors aus Koch, Satz 3.4 [1] geht es über in das kommutative Diagramm

$$\begin{tikzcd}
H^{n+1}(G) \arrow[rr, "\varphi"] \arrow[dr, "\mathrm{Res}"'] & & H^{n+1}(G, M_G^U(\mathbb{F}_p)) \arrow[dl, "\cong"] \\
& H^{n+1}(U) &
\end{tikzcd}$$

der entsprechenden Kohomologiegruppen zur Dimension $n+1$, wobei die Isomorphie nach dem Satz von Shapiro gilt.

Es ist $\mathrm{Res}(\bar{a}) = \overline{\mathrm{res}(a)}$, wobei die Restriktion $\mathrm{res} : K^{n+1}(G, \mathbb{F}_p) \to K^{n+1}(U, \mathbb{F}_p)$ jedem Element aus $K^{n+1}(G, \mathbb{F}_p)$ seine Einschränkung auf U^{n+1} zuordnet. Nach Wahl von U ist $\mathrm{res}(a)$ konstant. Wir wollen $\mathrm{Res}(\bar{a}) = 0$ zeigen, wozu wir eine Fallunterscheidung benötigen:

[1] Die Zuordungen $[G, A] \mapsto H^n(G, A)$ und $[\varphi, \psi] \mapsto \psi^*$ definieren einen Funktor aus der Kategorie $\mathcal{C}$ in die Kategorie der abelschen Gruppen.

Sei n gerade. Wegen $a \in \ker d_{n+1}$ gilt für alle $x_i \in G$

$$\begin{aligned}
0 &= (d_{n+1}a)(x_1, \dots, x_{n+1}, x_{n+2}) \\
&= x_1\, a(x_2, \dots, x_{n+2}) + \sum_{\nu=1}^{n+1} a(x_1, \dots, x_\nu x_{\nu+1}, \dots, x_{n+2}) \\
&\quad + (-1)^{n+2} a(x_1, \dots, x_{n+1})
\end{aligned}$$

Setzt man $x_i = 1$, so erhält man $0 = (d_{n+1}a)(1, \dots, 1, 1) = a(1, \dots, 1)$, da n gerade ist und deswegen oben genau ein Term der Form $a(1, \dots, 1)$ stehenbleibt. Damit verschwindet a auf ganz U^{n+1}, also $\operatorname{res} a = 0$ und damit $\operatorname{Res}(\bar{a}) = 0$.

Sei nun n ungerade. Wir definieren ein $b \in K^n(U, \mathbb{F}_p)$ durch $b(u_1, \dots, u_n) := a(1, \dots, 1, 1)$ für alle $u_i \in U$. Dann gilt

$$\begin{aligned}
d_n(b)(u_1 \dots, u_{n+1}) &= u_1\, b(u_2, \dots, u_{n+1}) + \sum_{\nu=1}^{n} b(u_1, \dots, u_\nu u_{\nu+1}, \dots, u_{n+1}) \\
&\quad + (-1)^{n+1} b(u_1, \dots, u_n) \\
&= a(1, \dots, 1, 1)
\end{aligned}$$

wobei die letzte Gleichheit aufgrund der Annahme „n ungerade“ eintritt. Daher gilt $d_n(b) = \operatorname{res}(a)$, also $\operatorname{res}(a) \in \operatorname{im}\left(K^n(U, \mathbb{F}_p) \xrightarrow{d_n} K^{n+1}(U, \mathbb{F}_p)\right)$ und damit $\operatorname{Res}(\bar{a}) = \overline{\operatorname{res}(a)} = 0$.

Aus dem zweiten kommutativen Diagramm lesen wir $\bar{a} \in \ker \varphi$ wegen $\operatorname{Res}(\bar{a}) = 0$ ab. Wir zeigen nun $\ker \varphi = 0$, daraus folgt dann $H^{n+1}(G) = 0$.

Der exakten Sequenz

$$0 \longrightarrow \mathbb{F}_p \longrightarrow M_G^U(\mathbb{F}_p) \longrightarrow \underbrace{M_G^U(\mathbb{F}_p)/\mathbb{F}_p}_{=:A} \longrightarrow 0$$

von G-Moduln entspricht die Kohomologiesequenz

$$0 \to H^0(G) \to \dots \to H^n(G, A) \to H^{n+1}(G) \xrightarrow{\varphi} H^{n+1}(G, M_G^U(\mathbb{F}_p)) \to \dots$$

Hieraus erhalten wir eine endliche exakte Sequenz von p-Gruppen

$$0 \to H^0(G) \to \dots \to H^n(G, A) \to \ker \varphi \to 0$$

auf welche wir Lemma 6 anwenden können:

$$\chi_n(G, M_G^U(\mathbb{F}_p)) = \chi_n(G) + (-1)^{n+1} \dim \ker \varphi + \chi_n(G, A)$$

Dies schreiben wir um zu

$$\dim \ker \varphi = (-1)^n \left(\chi_n(G) - \chi_n(G, M_G^U(\mathbb{F}_p) + \chi_n(G, A)\right) \tag{*}$$

Nach dem Satz von Shapiro gilt

$$H^\nu(U, \mathbb{F}_p) \cong H^\nu(G, M_G^U(\mathbb{F}_p)) \quad \forall\, \nu \geq 0$$

und daher nach Voraussetzung

$$\chi_n(G, M_G^U(\mathbb{F}_p)) = \chi_n(U) = (G:U)\,\chi_n(G)$$

Setzen wir dies in $(*)$ ein, so erhalten wir unter Zuhilfenahme von Lemma 10

$$\begin{aligned}\dim\ker\varphi &= (-1)^n\ (\chi_n(G) - (G:U)\,\chi_n(G) + \chi_n(G,A))\\ &\leq (-1)^n\,\chi_n(G)\Big(1 - (G:U) + \dim A\Big)\\ &= 0\end{aligned}$$

Für den letzten Schritt beachte

$$\dim A = \dim M_G^U(\mathbb{F}_p) - \dim \mathbb{F}_p = (G:U) - 1$$

Daher ist $\ker\varphi = 0$ und alles ist bewiesen.

$\square$

3 Der Erzeugendenrang

Definition 12. Sei G eine Pro-p-Gruppe. Der Erzeugendenrang $d(G)$ von G ist die Dimension von $H^1(G)$ als Vektorraum über $\mathbb{F}_p$.

Satz 13. *Sei G eine Pro-p-Gruppe. Dann ist die Mächtigkeit eines beliebigen minimalen Erzeugendensystems von G gleich $d(G)$.*

Bevor wir diese Aussage beweisen, noch ein Lemma, das wir für den Beweis brauchen werden:

Lemma 14. *Sei G eine Pro-p-Gruppe, dann gilt:*

$$(G/G^*)^\wedge = H^1(G)$$

und

$$(\prod_I \mathbb{F}_p)^\wedge = \bigoplus_I \mathbb{F}_p.$$

Beweis. Zuerst $(G/G^*)^\wedge = H^1(G)$:
Da G/G^* eine Pro-p-Gruppe ist, operiert sie trivial auf $\mathbb{F}_p$, daher ist

$$(G/G^*)^\wedge = H^1(G/G^*) = Hom(G/G^*, \mathbb{F}_p).$$

Betrachte nun die Abbildung

$$\gamma : H^1(G) \to H^1(G/G^*).$$

Diese ist ein Isomorphismus:

Betrachte das folgende kommutative Diagramm, wobei Π die Projektion bezeichnet. Es kommutiert, da G^* gerade im Kern von f liegt. Dies sieht man so, dass G^* ja gerade die von den Kommutatoren und p-Potenzen erzeugte abgeschlossene Untergruppe ist, und da $\mathbb{F}_p$ kommutativ und mit Periode p, verschwinden gerade diese Elemente. Nach dem Homomorphiesatz folgt die Kommutativität und die Existenz der eindeutigen Fortsetzung $\bar{f}$.

$$\begin{tikzcd}
G \arrow[rr, "f"] \arrow[dr, "\Pi"'] & & \mathbb{F}_p \\
& G/G^* \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

Injektivität: seien $f, g \in H^1(G), f \neq g$, d.h. $\exists x \in G : f(x) \neq g(x)$. Wegen der eindeutigen Faktorisierung muss dann gelten:

$$f(x) = (\bar{f} \circ \Pi)(x) = \bar{f}(\Pi(x)) \neq \bar{g}(\Pi(x)) = g(x).$$

Da $\Pi(x)$ eineutig, folgt somit $\bar{f} \neq \bar{g}$, also Injektivität.
Surjektivität: sei $\bar{f} \in H^1(G/G^*)$. Setze $f = \bar{f} \circ \Pi, f \in H^1(G)$. Wieder wegen der eindeutigen Faktorisierung wird $\gamma(f) = \bar{f}$.
Wegen der Bijektivität ist also

$$H^1(G) \cong H^1(G/G^*)$$

und insgesamt haben wir

$$(G/G^*)^\wedge \cong H^1(G).$$

Die zweite Isomorphie, die wir zeigen wollen, ist:

$$(\prod_I \mathbb{F}_p)^\wedge = \bigoplus_I \mathbb{F}_p.$$

Dafür benutzen wir:

$$(\prod_I \mathbb{F}_p)^\wedge \cong \bigoplus_I (\mathbb{F}_p^\wedge)^1.$$

Da die Homomorphismen bereits durch das Bild der 1 festgelegt sind, gilt:

$$\mathbb{F}_p^\wedge = Hom(\mathbb{F}_p, \mathbb{F}_p) \cong \mathbb{F}_p,$$

Also haben wir zusammen genommen:

$$(\prod_I \mathbb{F}_p)^\wedge \cong \bigoplus_I (\mathbb{F}_p^\wedge) = \bigoplus_I \mathbb{F}_p.$$

□

Beweis. von Satz 13.
Sei $\{s_i | i \in I\}$ ein minimales Erzeugendensystem von G. Nach dem Burnsideschen Basissatz [2] ist $S := \{s_i G^* | i \in I\}$ Erzeugendensystem von G/G^*. Es ist sogar minimales Erzeugendensystem, denn sonst gäbe es eine Teilmenge $I_k \subset I$, so dass $\{s_k G^* | k \in I_k\}$ auch Erzeugendensystem von G/G^* ist. Nach dem Burnsideschen Basissatz gäbe es aber entprechend auch eine Teilmenge $\{s_k | k \in I_k\} \subset \{s_i | i \in I\}$, die Erzeugendensystem von G wäre. Widerspruch zur Minimalität von $\{s_i | i \in I\}$.

Betrachte nun die Zuordnung

$$1_i \mapsto s_i G^*, \qquad i \in I.$$

[1] Morris, Theorem 17: Ist G direktes Produkt einer Familie $\{G_i | i \in I\}$ kompakter Hausdorffscher abelscher Gruppen, dann ist die diskrete Gruppe $G^\wedge$ algebraisch isomorph zur direkten Summe der jeweiligen dualen Gruppen $\{G_i^\wedge | i \in I\}$.

[2] Sei G eine Pro-p-Gruppe und $E = \{s_i | i \in I\}$ eine Teilmenge von G mit der Eigenschaft, dass in jeder Umgebung der Einheit von G fast alle Elemente von E enthalten sind. E ist genau dann Erzeugendensystem von G, wenn $\{s_i G^* | i \in I\}$ Erzeugendensystem von G/G^* ist.

Diese induziert einen Isomorphismus

$$\varphi : \prod_I \mathbb{F}_p \to G/G^*.$$

Im Koch steht diese Isomorphie für eine beliebige Menge I, wir zeigen sie hier nur für endliches I, für unendliches zeigen wir die Behauptung auf andere Weise.
Sei I also erstmal endlich. Dann ist φ ein wohldefinierter Gruppenhomomorphismus, denn beide Gruppen haben Periode p. Zudem lässt sich jedes Element als endliche Linearkombination der Elemente des Erzeugendensystems darstellen. Das Problem ist, dass diese Daststellung nicht eindeutig ist, was an der Periode p liegt. Da aber beide Gruppen gleiche Periode besitzen, hebt sich diese Uneindeutigkeit durch die Abbildung weg und das Bild eines jeden Elements aus $\prod_I \mathbb{F}_p$ ist wohldefiniert (betrachte die Koeffizienten in $\mathbb{F}_p$).
Nun zur Surjektivität. Da das Erzeugendensystem S endlich ist, ist auch sein algebraisches Erzeugnis $< S >$ endlich. Denn G/G^* ist abelsch und mit Periode p, also gibt es nur endlich viele unterschiedliche Linearkombinatioen der Elemente aus S. Wir wollen jetzt zeigen, dass G/G^* endlich ist. Dazu benutzen wir, dass G/G^* Hausdorffsch ist und dass $< S >$ eine endliche dichte Teilmenge von G/G^* ist. Angenommen es gäbe ein $x \in G/G^* - < S >$. Dann liegt in jeder Umgebung von x ein $s \in < S >$. Nach der Hausdorffschen Trennungseigenschaft können wir nun aber zwei disjunkt Umgebungen um x und s finden. In dieser Umgebung um x wiederum liegt nun ein anderes $\tilde{s} \in < S >$. Trennt man diese beiden wieder und fährt so fort, erhält man eine unendliche Kette disjunkter Umgebungen um x, die stets ein anderes Element aus $< S >$ enthalten. Widerspruch zur Endlichkeit von S. Wir haben also gezeigt, dass wegen $G/G^* \subset < S > \subset Im\varphi$ und $Im\varphi \subset G/G^*$ bereits folgt:

$$Im\varphi = < S > = G/G^*$$

und damit ist G/G^* endlich und φ surjektiv.
Nun noch zur Injektivität: Wir wollen zeigen, dass der Kern trivial ist. Dafür betrachten wir wieder die Koeffizienten in $\mathbb{F}_p$. Es soll also gelten:

$$\varphi(a_i 1_i + \dots a_n 1_n) = a_i s_i G^* + \dots + a_n s_n G^* = 0 \Rightarrow a_i = 0 \ \ \forall i \in I.$$

Angenommen, es gäbe einen Koeffizienten $a_j \neq 0$. Multipliziere die Gleichung mit dem Inversen von a_j und löse nach $s_j G^*$ auf, dann erhalten wir:

$$s_j G^* = -\sum_{i \neq j} a_j^{-1} a_i s_i G^*.$$

$s_j G^*$ lässt sich also durch die anderen Elemente von S darstellen, für $\tilde{S} := S - \{s_j G^*\} \subset S$ gilt

$$< \tilde{S} > = < S > = G/G^*,$$

Widerspruch zur Minimalität von S. Es sind also alle Koeffizienten Null und damit ist φ injektiv.

Für I endlich haben wir die Isomorphie also gezeigt.
Nun verwenden wir die dualen Gruppen aus obigem Lemma und erhalten:

$$\bigoplus_I \mathbb{F}_p \cong H^1(G)$$

und damit für den endlichen Fall:

$$dim H^1(G) = card(I).$$

Sei nun I unendlich. Dann ist auch G/G^* unendlich, da sie ja bereits eine unendliche Teilmenge besitzt. Angenommen, die duale Gruppe hätte als Vektorraum über $\mathbb{F}_p$ endliche Dimension und sei $\{\chi_j | j \in J\}$ eine Basis. Dann gibt es nach Koch, Kapitel 4.3 auch ein minimales endliches Erzeugendensystem von G/G^*. Im obigen Fall aber haben wir gezeigt, dass dann auch G/G^* endlich wäre. Widerspruch zur Unendlichkeit von G/G^*. Da also sowohl die Dimension des Vektorraums als auch die Kardinalität unendlich sind, gilt die Behauptung auch im Unendlichen. □

Beispiel 15. Sei F freie Pro-p-Gruppe. Dann ist

$$\chi(F) = 1 - d(F).$$

Denn da F frei, ist $cd(F) = 1$, also ist $H^\nu(F) = \{0\} \quad \forall \nu \geq 2$.

$$\Rightarrow \chi(F) = \sum_{n=0}^{\infty} (-1)^n dim H^n(F) = dim H^0(F) - dim H^1(F) = 1 - d(F)$$

Sei $U \leq F$ Untergruppe, $[F : U]$ endlich. Dann ist

$$d(U) = [F : U](d(F) - 1) + 1.$$

Denn $\chi(U) = 1 - d(U)$ und auch $\chi(U) = [F : U]\chi(F) = [F : U](1 - d(F))$
$\Rightarrow 1 - d(U) = [F : U](1 - d(F))$ bzw. $d(U) = [F : U](d(F) - 1) + 1$.

4 Relationensysteme

Definition 16. Sei G eine Pro-p-Gruppe. Mit einer freien Pro-p-Gruppe F mit Erzeugendensystem $\{t_i | i \in I\}$ heißt die exakte Sequenz

$$1 \longrightarrow R \longrightarrow F \xrightarrow{\varphi} G \longrightarrow 1$$

eine Darstellung von G mit Hilfe von F.
Ist $\{\varphi(t_i) | i \in I\}$ ein minimales Erzeugendensystem von G, so heißt die Darstellung minimal.
Eine Teilmenge $E \subset R$ heißt (erzeugendes) Relationensystem von G (bezüglich obiger Darstellung), falls

1. R ist der kleinste abgeschlossene Normalteiler von F der E enthält,
2. in jedem offenen Normalteiler von R fast alle Elemente aus E enthalten sind.

E heißt minimal, wenn keine Teilmenge von E Relationensystem von G ist.
Sei nun $\{G_i | i \in I\}$ eine Familie von Pro-p-Gruppen, $\{\varphi_i | i \in I\}$ eine Familie von Morphismen $\varphi_i : G_i \longrightarrow G$ in eine Pro-p-Gruppe G. Für jedes $i \in I$ sei $T_i \trianglelefteq G_i$ Normalteiler, wobei G_i / T_i eine freie Pro-p-Gruppe ist.
$\{\varphi_i | i \in I\}$ heißt zulässig bezüglich $\{T_i | i \in I\}$, wenn in jedem offenen Normalteiler von G fast alle $\varphi_i(T_i)$ liegen.

Satz 17. *Es gelten die gleichen Voraussetzungen wie in obiger Definition. Außerdem sei $\{\varphi_i | i \in I\}$ zulässig bezüglich $\{T_i | i \in I\}$ und für jedes $i \in I$ sei die Darstellung*

$$1 \longrightarrow R_i \longrightarrow F_i \xrightarrow{\psi_i} G_i \longrightarrow 1$$

gegeben.
Dann gibt es Morphismen $\chi_i : F_i \longrightarrow F$ mit der Einschränkung $\bar{\chi}_i$ auf R_i, so dass folgende Diagramme kommutativ sind:

$$\begin{array}{ccccc}
R_i & \xrightarrow{r_i} & F_i & \xrightarrow{\psi_i} & G_i \\
\downarrow{\scriptstyle \bar{\chi}_i} & & \downarrow{\scriptstyle \chi_i} & & \downarrow{\scriptstyle \varphi_i} \\
R & \xrightarrow{r} & F & \xrightarrow{\varphi} & G
\end{array}$$

Außerdem ist dann $\{\bar{\chi}_i | i \in I\}$ zulässig bezüglich $\{R_i | i \in I\}$. In diesem Fall spricht man von einer zulässigen Darstellung von $\{\varphi_i | i \in I\}$.

Beweis. Im Folgenden werden wir unser Diagramm folgendermaßen erweitern:

$$\begin{tikzcd}
R_i \arrow[r, "r_i"] \arrow[d, "\bar{\chi}_i"] & F_i \arrow[r, "\psi_i"] \arrow[d, "\chi_i"] & G_i \arrow[r, "\Pi"] \arrow[d, "\varphi_i"] & G_i/T_i \\
R \arrow[r, "r"] & F \arrow[r, "\varphi"] & G \arrow[l, bend left, "\sigma"] &
\end{tikzcd}$$

Es gibt einen stetigen Schnitt

$$\sigma : G \longrightarrow F \quad \text{mit} \quad \sigma(1) = 1.$$

Denn da die Darstellung eine exakte Sequenz ist, gilt als Isomorphie von Gruppen $G \cong F/ker\varphi$. Mit Satz 1.16 aus dem Koch [1] folgt dann: $\exists \sigma : F/ker\varphi \longrightarrow F$ stetig mit $G \cong F/ker\varphi \longrightarrow F \longrightarrow F/ker\varphi \cong G$ ist die Identität. Da der Schnitt stetig ist, muss nun noch gezeigt werden, dass auch die Isomorphie im topologischen Sinne gilt. Dafür betrachte das folgende kommutative Diagramm:

$$\begin{tikzcd}
F \arrow[rr, "\varphi"] \arrow[dr, "\Pi"'] & & G \\
& F/ker\varphi \arrow[ur, "\bar{\varphi}"'] &
\end{tikzcd}$$

Sei also $\mathcal{O}$ eine offene Menge in G. Da φ eine stetige Abbildung ist, ist φ^{-1} offen in F. Da die Projektion offen ist, ist wegen der Kommutativität des Diagramms $\bar{\varphi}^{-1}(\mathcal{O})$ ein offenes Urbild, also ist die Abbildung stetig. Nach einem Satz der Topologie [2] ist $\bar{\varphi}$ bereits ein Homöomorphismus, da $F/ker\varphi$ kompakt und G Hausdorffsch, also gilt die Isomorphie auch im topologischen Sinne und der stetige Schnitt exisitiert.

Sei nun $\{t_k | k \in I_i\}$ ein Erzeugendensystem der freien Pro-p-Gruppe F_i, wir untersuchen nun folgende Abbildung:

$$\vartheta_i : F_i \longrightarrow G_i/T_i.$$

Sei $I_i^2 \subset I_i$ so, dass die t_k für $k \in I_i^2 \subset I_i$ auf 1 abgebildet werden.Für $k \in I_i^1 := I_i - I_i^2$ bilden die Bilder der t_k ein Erzeugendensystem von G_i/T_i: Betrachte den Abschluss des Erzeugnisses der Bilder, $E_i := \overline{< \{\vartheta_i(t_k) | k \in I_i^1\} >}$. Dann ist das Urbild $\vartheta_i^{-1}(E_i)$ wegen der Stetigkeit auch wieder abgeschlossen in F_i und enthält alle Elemente des Erzeugendensystems $\Rightarrow \vartheta_i^{-1}(E) = F_i$. Wendet man nun wieder ϑ_i auf dieses Urbild an,

[1] Sei H eine Untergruppe der proendlichen Gruppe F. Dann gibt es einen stetigen Schnitt σ von F/H in F mit $\sigma(H) = 1$, d.h es gilt: $F/H \xrightarrow{\sigma} F \longrightarrow F/H = id_{F/H}$.

[2] Querenburg, Satz 8.12: Sei $f : X \longrightarrow Y$ eine stetige Abbildung des quasikompakten Raumes X in den Hausdorff-Raum Y. Dann ist f abgeschlossen. Ist f bijektiv, so ist f ein Homöomorphismus.

so gilt wegen der Surjektivität:

$$G_i/T_i = \vartheta_i(F_i) = \vartheta_i(\underbrace{\vartheta_i^{-1}(E_i)}_{F_i}) = E_i = \overline{<\{\vartheta_i(t_k)|k \in I_i^1\}>},$$

die Bilder bilden also bereits ein Erzeugendensystem.

Dann ist ein Morphismus $\chi_i : F_i \longrightarrow F$ gegeben durch:

$$\chi_i(t_k) = \sigma\varphi_i\psi_i(t_k), \qquad k \in I_i,$$

denn durch die Vorgabe der Elemente $\sigma\varphi_i\psi_i(t_k) \in F$ sind die Voraussetzungen für Satz 9 [1] des letzten Vortrags erfüllt. Denn wähle eine offene Umgebung $\mathcal{O}$ der 1 in F. Wegen der Stetigkeit, ist dann auch das Urbild$(\sigma\varphi_i\psi_i)^{-1}(\mathcal{O})$ eine offene Umgebung der 1 in F_i und damit sind darin fast alle t_k enthalten. Bildet man dies nun wieder ab, sind also fast alle Bilder der t_k in $\mathcal{O}$ enthalten. Daher wissen wir, dass es einen solchen Morphismus gibt. Damit ist das Diagramm nach Konstruktion dann kommutativ.

Sei $N \trianglelefteq F$ offener Normalteiler. Die Mengen $\varphi(N)$ und $\sigma^{-1}(N)$ sind offene Umgebungen der Einheit von G, denn da N offen und σ stetig ist, ist $\sigma^{-1}(N)$ offen und wegen $\sigma(1) = 1$ auch eine Umgebung der 1. Um die Offenheit von $\varphi(N)$ zu erkennen, betrachte obiges kommutatives Diagramm. $\bar{\varphi}$ ist stetig, denn da φ und Π stetig, gilt für eine offene Menge $V \subset G$: $\bar{\varphi}^{-1}(V) = \Pi(\varphi^{-1}(V))$ ist offen, also $\bar{\varphi}$ stetig. Damit sind die Voraussetzungen für den Satz der Fußnote erfüllt, $\bar{\varphi}$ ist ein Homöomorphismus und damit offen. Da das Diagramm kommutiert ist damit auch φ offen.

Ihr Durchschnitt enthält einen offenen Normalteiler U von G. Nach Satz 1.14 im Koch enthält nämlich jede offene Umgebung der Einheit einer Pro-p-Gruppe einen offenen Normalteiler.
Da $\{\varphi_i|i \in I\}$ zulässig bezüglich $\{T_i|i \in I\}$ gilt für fast alle $i \in I$:

$$\varphi_i(T_i) \subset U.$$

Sei $i \in I$ ein Index, für den das gilt. Aus der Kommutativität folgt:

$$\chi_i(t_k) \in \sigma(U) \subset N \qquad \forall k \in I_i^2,$$

denn für $k \in I_i^2$ wird t_k nach T_i abgebildet. Weiter gilt damit, dass

$$\chi_i(Ker\vartheta_i) \subset N.$$

Denn angenommen es gäbe ein $s \in ker\vartheta_i$ mit $\chi_i(s) \notin N$. Dann ist $\psi_i(s) \in T_i$ und damit

$$\varphi_i\psi_i(s) \subset \varphi(T_i) \subset U$$

[1] Sei $F(I)$ die freie Pro-p-Gruppe mit Erzeugendensystem $\{s_i|i \in I\}$, G eine Pro-p-Gruppe und $\{t_i|i \in I\}$ eine Menge in G mit der Eigenschaft, dass in jeder Umgebung der $1 \in G$ fast alle t_i liegen. Dann gibt es einen eindeutig bestimmen Morphismus $\varphi : F(I) \longrightarrow G$ mit $\varphi(s_i) = t_i \;\; \forall i \in I$.

Wegen der Kommutativität des Diagramms ist aber auch

$$\varphi(\underbrace{\chi_i(s)}_{\notin N}) \in U.$$

Nach Konstruktion ist $U \subset (\varphi(N) \cap \sigma^{-1}(N))$ und da $\sigma(\sigma^{-1}(N)) \subset N$ wäre

$$\underbrace{\sigma(\varphi}_{=id}(\chi_i(s))) \in N.$$

Wiederspruch. Also gilt $\chi_i(Ker\vartheta_i) \subset N$ und da außerdem $R_i \subset Ker\vartheta_i$ (wegen der Exaktheit der Sequenz), ist

$$\bar{\chi}_i(R_i) \subset R \cap N.$$

Da in jeder Umgebung der Einheit von R eine Gruppe $R \cap N$ enthalten ist, folgt die Behauptung. □

Literatur

Querenburg, Boto von: Mengentheoretische Topologie Springer Verlag Berlin-Heidelberg, 1979

Koch, Helmut: Galoissche Theorie der p-Erweiterungen; VEB Deutscher Verlag der Wissenschaften, Berlin 1970

Koch, Helmut: Galois Theory of p-Extensions; Springer Verlag Berlin-Heidelberg, 2002

Ribes, Luis: Introduction to Profinite Groups an Galois Cohomology Queent́s Papers in Pure and Applied Mathematics, Volume 24, Queent́s University
1999