Freie Pro-p-Gruppen

Johannes Röhrenbach, Angela Jäschke

15.04.2010

1 Konstruktion freier Pro-p-Gruppen

Definition 1 Sei stets p eine Primzahl. Eine *proendliche Gruppe* bzw. *Pro-p-Gruppe* ist eine topologische Gruppe, die sich als projektiver Limes von endlichen Gruppen bzw. p-Gruppen darstellen lässt.

Definition 2 Sei G eine Pro-p-Gruppe, $E \subseteq G$ eine Teilmenge. Dann heißt E *Erzeugendensystem* von G, wenn gilt:

- Die kleinste abgeschlossene Untergruppe, die E umfasst, ist G selbst.
- In jeder Umgebung der Einheit von G liegen fast alle Elemente von E.

Definition 3 Ein Erzeugendensystem E heißt *minimal*, wenn keine echte Teilmenge von E ein Erzeugendensystem ist.

Satz und Definition 4 Sei I Indexmenge; F_I die von $S_I := \{s_i | i \in I\}$ erzeugte freie Gruppe. Sei $\mathfrak{U} := \{N \triangleleft F_I | \exists k \in \mathbb{N} : [F_I : N] = p^k, s_i \in N \text{ für fast alle } i \in I\}$. Dann ist $\mathfrak{U}$ filtrierende Menge bzgl. " $\subseteq$ " (da in Bezug auf endliche Durchschnittsbildung abgeschlossen [1]) und damit $\{F_I/N | N \in \mathfrak{U}\}$ zusammen mit den Projektionen $\varphi_i^j : F_I/M \longrightarrow F_I/N$ für $M \subseteq N$ ein projektives System, dessen projektiver Limes $F(I) := \varprojlim_{N \in \mathfrak{U}} F_I/N$ eine pro-p-Gruppe ist. $F(I)$ heißt *freie pro-p-Gruppe mit Erzeugendensystem* S_I.

Bemerkung 5 Die Abbildung $\varphi : F_I \longrightarrow F(I), w \longmapsto \prod\limits_{N\in\mathfrak{U}} wN$ ist ein Monomorphismus (Beweis unten) mit $Kern(\varphi) = \bigcap\limits_{N\in\mathfrak{U}} N = \{1\}$ [2], dessen Bild in F(I) dicht liegt [3]. Man identifiziert also F_I mit $\varphi(F_I)$ und S_I wird minimales Erzeugendensystem von $F(I)$.

Definition 6 Sei Λ kommutativer Ring mit Eins und I Indexmenge. Die Algebra $\Lambda(I)$ der formalen nichtkommutativen Potenzreihen in den Unbestimmten x_i, $i \in I$, mit Koeffizienten aus Λ heißt *Magnus'sche Algebra*.

Lemma 7 Sei $\psi : F_I \longrightarrow \Lambda(I)^*$ Homomorphismus mit $\psi(s_i) = 1 + x_i$. Dann ist ψ injektiv.

Beweis: Sei $1 \neq w = \prod\limits_{\nu=1}^{n} s_{i_\nu}^{a_\nu} \in F_I$, $i_\nu \neq i_{\nu+1}$, $\nu = 1, ..., n-1$. Dann ist

$$\psi(w) = \psi(\prod_{\nu=1}^{n} s_{i_\nu}^{a_\nu}) = \prod_{\nu=1}^{n}(1 + x_{i_\nu})^{a_\nu} = \prod_{\nu=1}^{n}\sum_{b_\nu=0}^{a_\nu}\binom{a_\nu}{b_\nu}x_{i_\nu}^{b_\nu} = \sum_{(b_1,...b_n)\in\mathbb{N}_0^n}\prod_{\nu=1}^{n}\binom{a_\nu}{b_\nu}x_{i_\nu}^{b_\nu}. \quad (\star)$$

($\binom{a_\nu}{b_\nu} := 0$ für $b_\nu \geq a_\nu$) Für $char(\Lambda) =: k \neq 0$ sei nun q prim mit $q \mid k$. Betrachte $(0, ...0) \neq (b_1, ...b_n) \in \mathbb{N}_0^n$ mit $b_\nu = q^{n_\nu}$ wobei $a_\nu = q^{n_\nu}c_\nu$, $q \nmid c_\nu$, $\nu = 1, ...n$. Dann gilt $\binom{a_\nu}{b_\nu} \not\equiv 0 \ mod\ q$ [5] und somit gibt es in $(\star)$ mindestens einen von 1 verschiedenen Summanden, der nicht verschwindet. *q.e.d.*

Bemerkung 8 Es ist $\psi(s_i^{-1}) = \sum\limits_{\nu=0}^{\infty}(-x_i)^\nu$ [4].

Beweis von Bemerkung 5: Es ist φ injektiv bzw. $\bigcap\limits_{N\in\mathfrak{U}} N = \{1\}$ zu zeigen. Sei zunächst I endlich, Œ$I = \{1, ...n\}, \Lambda = \mathbb{Z}/p\mathbb{Z}, B^k \subseteq \Lambda(I)$ das beidseitige Ideal aller Potenzreihen, deren sämtliche Glieder mindestens Grad k haben und

$$N_k := \{w \in F_I | \psi(w) - 1 \in B^k\}.$$

Es ist $\bigcap\limits_{k=1}^{\infty} B^k = \{0\}$ und damit $\bigcap\limits_{k=1}^{\infty} N_k = \{1\}$, da ψ injektiv (Lemma 7). Die Behauptung folgt (für endliche I), da außerdem $N_k \in \mathfrak{U}\ \forall k \geq 0$:
In der Tat ist $\forall k \geq 0$ N_k Normalteiler von F_I [6] und der Index $[F_I : N_k]$ p-Potenz. Dies zeigt man per Induktion nach k: Es gilt $N_1 = F_I$ für $k = 1$. Da I endlich, ist $\sharp\Lambda(I)/B^{k+1}$

p-Potenz und damit ebenfalls $\sharp B^k/B^{k+1}$ und sogar $\sharp N^k/N^{k+1}$ p-Potenz, da ψ einen Monomorphismus $N^k/N^{k+1} \hookrightarrow B^k/B^{k+1}$ induziert.

Ist I nun unendlich, so betrachtet man für endliche Teilmengen $J \subset I$ die von den Mengen

$$N_k(J) := \{w \in F_J | \psi(w) - 1 \in B^k\} \text{ und } \{s_i | i \in I - J\}$$

erzeugten Normalteiler $N_{k,J} \triangleleft F_I$, wobei die Untergruppe $N_k(J) \subset F_J \subset F_I$ bzgl. der Magnus'schen Algebra $\Lambda(J)$ zusammen mit dem Monomorphismus $\psi : F_J \longrightarrow \Lambda(J)$ mit $\psi(s_j) = 1 + x_j$ verstanden wird. Es ist $N_{k,J} \in \mathfrak{U}$ und es gilt

$$\bigcap_{k,J} N_{k,J} = \{1\},$$

da $\bigcap_{k=1}^{\infty} N_k(J) = \{1\}$ $\forall J \subset I$ und der Durchschnitt über alle endlichen Teilmengen $J \subset I$ gebildet wird und daher $s_i \notin \bigcap_{k,J} N_{k,J}$ $\forall i \in I$ gilt. Hieraus also folgt die Behauptung auch für unendliche Indexmengen I. *q.e.d.*

2 Abelsche Pro-p-Gruppen

Pontrjagin-Dualität

Einer lokalkompakten Gruppe G wird eine weitere Gruppe, $\hat{G}$ zugeordnet; ihre duale Gruppe. Dies geschieht auf eine Weise, dass die duale Gruppe der dualen Gruppe kanonisch isomorph zu G ist. Die Elemente von $\hat{G}$ sind die stetigen Gruppenhomomorphismen von G in $\mathbb{R}/\mathbb{Z}$, die Charaktere. (Bei proendlichen Gruppen landet man in $\mathbb{Q}/\mathbb{Z}$).

Nach Pontrjagins Dualitätstheorie sind die dualen Gruppen von kompakte Gruppen die diskreten Gruppen und umgekehrt. **Insbesondere entsprechen den abelschen Pro-p-Gruppen die diskreten p-primären Torsionsgruppen.** (P-Primär: Jedes Element wird von einer p-Potenz annulliert.)

Sei also G eine abelsche Pro-p-Gruppe vom Exponenten p. Dann ist die duale Gruppe ein diskreter Vektorraum V über $\mathbb{Z}/p\mathbb{Z}$. Sei zudem $\{\chi_i | i \in I\}$ eine Basis von V. Die Elemente $s_i \in G, i \in I$, mit $\langle s_i, \chi_j \rangle = \delta_{ij}$, bilden ein minimales Erzeugendensystem von G und G ist isomorph zu $\prod_I \mathbb{Z}/p\mathbb{Z}$.

G als $\mathbb{Z}_p$-Operator

Wir können in folgender Weise $\mathbb{Z}_p$ auf einer beliebigen Pro-p-Gruppe G operieren lassen: Für $a = \lim_{n\to\infty} a_n \in \mathbb{Z}_p$, $a_n \in \mathbb{Z}$ und $g \in G$ definieren wir

$$g^a = \lim_{n\to\infty} g^{a_n}$$

Diese Definition hängt offensichtlich nicht von der Wahl der Folge a_n ab und für $g \in G, a, b \in \mathbb{Z}_p$ gilt:

$$g^{a+b} = g^a g^b$$
$$(g^a)^b = g^{ab}$$

Ist G abelsch, so gilt außerdem für $g_1, g_2 \in G, a \in \mathbb{Z}_p$:

$$(g_1 g_2)^a = g_1^a g_2^a$$

3 Erste Charakterisierung von freien Pro-p-Gruppen

Zunächst beweisen wir ein paar Eigenschaften von Pro-p-Gruppen, die wir später brauchen werden.

Satz 9

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's liegen.
Dann gibt es einen eindeutig bestimmten Morphismus $\varphi : F(I) \to G$ mit $\varphi(s_i) = t_i \ \forall i \in I$.

Beweis

Es sei $\mathfrak{U}_G := \{N \underline{\triangleleft} G | (G : N) = p^k, k \in \mathbb{N}\}$.

Die Eindeutigkeit folgt aus obiger Zuordnung.
Existenz: Die Abbildung lässt sich eindeutig fortsetzen zu einem Homomorphismus $F_I \to G$.

Zudem bezeichnen wir für $U \in \mathfrak{U}_G$ mit $\Phi(U)$ den Kern des induzierten Morphismus $F_I \to G/U$. $\Phi(U)$ ist in $\mathfrak{U}$ (Normalteiler von endlichem Index) enthalten.

Wenn wir mit Φ_U den induzierten Morphismus $F_I/\Phi(U) \to G/U$ bezeichnen, so ist $\{\Phi, \Phi_U | U \in \mathfrak{U}_G\} : \{F_I/V | V \in \mathfrak{U}\} \to \{G/U | U \in \mathfrak{U}_G\}$ ein Morphismus projektiver Systeme.

Anmerkung: Jedem Morphismus projektiver Systeme $\varphi : \{I, G_i, \varphi_i^j\} \to \{J, H_i, \psi_i^j\}$ können wir einen Morphismus der projektiven Limites $\varphi' : \varprojlim G_i \to \varprojlim H_i$ zuordnen durch $\varphi'(\prod_{i \in I} g_i) = \prod_{j \in J} \psi_j(g_{\Phi(j)})$, wobei $\Phi : J \to I, \psi_i : G_{\Phi(i)} \to H_i$.
(Siehe z.B. Koch: Galois Theory of p-Extensions, S.5)

Also: Morphismus $F(I) = \varprojlim F_I/V \to \varprojlim G/U \cong G$, $\prod_{V \in \mathfrak{U}} wV \to \prod_{U \in \mathfrak{U}_G} \varphi(w)U, w \in F_I$.
Dieser Morphismus hat die gewünschte Eigenschaft.

Definition 10

Für eine Pro-p-Gruppe G definieren wir die **Frattinigruppe** $G^* = G^p[G,G]$, also den von allen p-ten Potenzen von Elementen aus G und den Kommutatoren erzeugten Normalteiler.
Anmerkung: Im Allgemeinen ist die Frattinigruppe definiert als der Durchschnitt aller maximalen Untergruppen von G. In diesem Fall sind beide Definitionen äquivalent.
G^* ist die kleinste Untergruppe N von G, sodass G/N abelsch ist und den Exponenten p hat.

Satz 11

Seien G_1 und G_2 Pro-p-Gruppen und sei $\varphi : G_1 \to G_2$ ein Morphismus. Dann is φ surjektiv genau dann wenn der induzierte Morphismus $\varphi_* : G_1/G_1^* \to G_2/G_2^*$ surjektiv ist.

Beweis

φ surjektiv $\Rightarrow \varphi_*$ surjektiv ist klar.

Nehmen wir an, φ sei nicht surjektiv, also $\varphi(G_1) \subset G_2$. Dann gibt es einen offenen Normalteiler U von G_2 mit $\varphi(G_1)U/U \subset G_2/U$. Nach einem Satz über endliche p-Gruppen (nachzulesen in M.Hall, The Theory of Groups, S. 176) ist $\varphi(G_1)U/U$ in einem Normalteiler G'/U vom Index p in G_2/U enthalten. Daraus folgt, dass $G_2^* \subseteq G'$ und
$\varphi_*(G_1/G_1^*) \subseteq G'/G_2^* \subset G_2/G_2^*$.
$\Rightarrow \varphi_*$ nicht surjektiv.

Satz 12

Sei G eine Pro-p-Gruppe. Dann sind äquivalent:

1. G ist freie Pro-p-Gruppe.

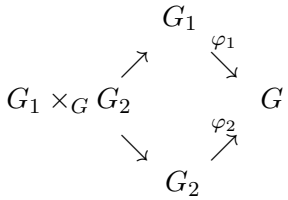
2. Jede Gruppenerweiterung von G mit einer Pro-p-Gruppe H zerfällt.
   Anmerkung: Eine kurze Exakte Sequenz $1 \to H \to \overline{H} \to G \to 1$ heißt Erweiterung von G durch H. Man sagt, eine Erweiterung zerfällt, wenn es einen Morphismus gibt, der zu $\overline{H} \to G$ rechtsinvers ist.

3. G ist projektives Objekt in der Kategorie der Pro-p-Gruppen.
   Anmerkung: G ist projektives Objekt in der Kategorie C, wenn für jeden Epimorphismus $f : X \to Y$ die induzierte Abbildung $Mor_C(G, X) \to Mor_C(G, Y),\ g \mapsto f \circ g$, surjektiv ist.

Beweis

1. $\Rightarrow$ **2.**: Sei G eine freie Pro-p-Gruppe mit Erzeugendensystem $\{s_i | i \in I\}$, und $1 \to H \to \overline{H} \xrightarrow{\varphi} G \to 1$ eine Gruppenerweiterung. Sei zudem $\sigma : G \to \overline{H}$ ein stetiger Schnitt (Rechtsinverses zu φ).
Wir können dann Satz 9 auf die freie Gruppe G, auf $\overline{H}$ und auf die Menge $\{\sigma s_i | i \in I\} \subseteq \overline{H}$ anwenden. Also gibt es einen Morphismus $\sigma' : G \to \overline{H}$ mit $\varphi\sigma' = id$, also zerfällt die Erweiterung.

2. $\Rightarrow$ **3.**: Sei
$$\begin{array}{ccccc} & & G & & \\ & & \downarrow & & \\ G_2 & \to & G_1 & \to & 1 \end{array}$$
ein exaktes Diagramm von Pro-p-Gruppen.
Anmerkung: Faserprodukt: Zu jedem Diagramm G_1
$$\begin{array}{ccc} & \overset{\varphi_1}{\searrow} & \\ & & G \\ & \underset{\varphi_2}{\nearrow} & \\ G_2 & & \end{array}$$
proendlicher Gruppen gibt es eine eindeutig bestimmte proendliche Gruppe $G_1 \times_G G_2$ mit Morphismen nach G_1 und G_2, sodass das Diagramm



kommutiert und die universelle Abbildungseigenschaft hat.
$G_1 \times_G G_2 = \{(g_1, g_2) \mid (g_1, g_2) \in G_1 \times G_2, \varphi_1 g_1 = \varphi_2 g_2\}$.

Wir können also obiges Diagramm ergänzen zu

$$\begin{array}{ccccc} G_2 \times_{G_1} G & \xrightarrow{\varphi} & G & & \\ {\scriptstyle \varphi_2}\downarrow & & \downarrow & & \\ G_2 & \to & G_1 & \to & 1 \end{array}$$

, wobei φ surjektiv ist. Nach Voraussetzung gibt es einen Morphismus $\psi : G \to G_2 \times_{G_1} G$ mit $\varphi\psi = id$. $\varphi_2 \circ \psi$ ist der gewünschte Morphismus.

3. $\Rightarrow$ **1.**: Sei also G projektives Objekt in der Kategorie aller Pro-p-Gruppen. Nach dem vorhergehenden Teil über abelsche Pro-p-Gruppen ist G/G^* isomorph zu $\prod_I \mathbb{Z}/p\mathbb{Z}$ für gewisses I, und mit Satz 9 gibt es dann einen Morphismus $F(I) \to \prod_I \mathbb{Z}/p\mathbb{Z}$ mit dem Kern $F(I)^*$.
Nach Voraussetzung gibt es einen eindeutig bestimmten Morphismus $\varphi : G \to F(I)$, der folgendes Diagramm kommutativ macht:

$$\begin{array}{ccccc} & & G & & \\ & {\scriptstyle \varphi}\swarrow & & \searrow & \\ F(I) & \to & \prod_I \mathbb{Z}/p\mathbb{Z} & \to & 1 \end{array}$$

Da $\varphi_* : G/G^* \to F(I)/F(I)^*$ ein Isomorphismus ist, ist nach Satz 11 auch φ surjektiv. Da $F(I)$ frei ist, können wir erneut Satz 9 anwenden, um einen Morphismus $\psi : F(I) \to G$ zu erhalten mit $\varphi\psi = id$. ψ ist surjektiv und damit ein Isomorphismus, also $G \cong F(I)$
$\Rightarrow G$ frei.

Korollar 13

Sei G eine Pro-p-Gruppe, I eine Indexmenge und $\theta : \prod_I \mathbb{Z}/p\mathbb{Z} \to G/G^*$ ein Epimorphismus. Dann gibt es einen Epimorphismus $F(I) \to G$, der θ induziert. Jedes Erzeugendensystem von G/G^* kann zu einem Erzeugendensystem von G erweitert werden.

Beweis

Da F(I) freie Pro-p-Gruppe ist, können wir Satz 12 anwenden. Nach Bedingung 3. gibt es einen Morphismus $\varphi : F(I) \to G$, der folgendes Diagramm kommutativ macht:

$$\begin{array}{ccccc} & & F(I) & & \\ & \overset{\varphi}{\swarrow} & & \searrow & \\ G & \to & G/G^* & \to & 1 \end{array}$$

Nach Satz 11 ist φ surjektiv.
Sei nun $\{t_i | i \in I\}$ Erzeugendensystem von G/G^*. Es gibt (mit Satz 9) einen eindeutig bestimmten Epimorphismus $F(I) \to G/G^*$, der die Erzeuger s_i von $F(I)$ auf die t_i $\forall i \in I$ schickt. Weil obiges Diagramm kommutativ ist, ist also $\{\varphi(s_i) | i \in I\}$ ein Erzeugendensystem von G, das $\{t_i | i \in I\}$ fortsetzt.

Satz 14 - Burnsidescher Basissatz

Sei G eine Pro-p-Gruppe und $E = \{s_i | i \in I\}$ eine Teilmenge von G, sodass in jeder Umgebung der $1 \in G$ fast alle Elemente aus E liegen.
E ist Erzeugendensystem von G genau dann wenn $\{s_i G^* | i \in I\}$ Erzeugendensystem von G/G^* ist.

Beweis

Sei $\{s_i G^* | i \in I\}$ Erzeugendensystem von G/G^*. Mit Satz 9 gibt es einen Morphismus $\varphi : F(I) \to G$, der dem Erzeugendensystem E entspricht. φ induziert einen Epimorphismus $\varphi_* : F(I)/F(I)^* \to G/G^*$. Nach Satz 11 ist φ also surjektiv und damit E ein Erzeugendensystem von G.

Die andere Richtung ist klar.

4 Zweite, kohomologische Charakterisierung der freien Pro-p-Gruppen

Bemerkung 15 Die Ordnung eines jeden Automorphismus der abelschen Gruppe $\mathbb{Z}/p\mathbb{Z}$ ist teilerfremd zu p. Eine Pro-p-Gruppe G operiert daher auf $\mathbb{Z}/p\mathbb{Z}$ stets nur trivial.

Im Folgenden soll die (bedeutende) Rolle der Kohomologiegruppe

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

untersucht werden:

Bemerkung 16 Ist G abel'sche Pro-p-Gruppe mit Periode p, so ist $H^1(G)$ die zu G duale Gruppe. Damit gilt folgender Satz 17 ebenso wie Satz 11:

Satz 17 Seien G_1, G_2 Pro-p-Gruppen und $\varphi : G_1 \longrightarrow G_2$ Morphismus. Dann ist φ genau dann surjektiv, wenn die duale Abbildung $\varphi^* : H^1(G_2) \longrightarrow H^1(G_1)$ injektiv ist.

Zum Beweis der Hauptaussage des gegenwärtigen Abschnitts

Theorem 18 Eine Pro-p-Gruppe G ist genau dann frei, wenn $H^2(G) = \{0\}$ ist.

benötigen wir zwei Hilfssätze:

Lemma 19 Sei $A \neq \{1\}$ endliche p-Gruppe und G eine p-Untergruppe der Automorphismengruppe $Aut(A)$. Dann gilt $A^G \neq \{1\}$.

Beweis: Betrachte die disjunkte Zerlegung von A in die Bahnen

$$Ga = \{ga | a \in G\}, a \in A. \quad (\star\star)$$

Es gilt $Ga = \{a\}$, für $a \in A^G$ und $\sharp Ga = cp$ für $a \notin A^G$, $c \in \mathbb{N}$, da G p-Gruppe. Da die Zerlegung $(\star\star)$ disjunkt ist, ist die Anzahl der verschiedenen Bahnen Ga für invariante $a \in A$ und damit die Anzahl der invarianten Elemente $a \in A^G$ von A also ebenfalls Vielfaches von p und damit insbesondere $\neq 1$. *q.e.d.*

Lemma 20 Sei G Pro-p-Gruppe und $\{1\} \neq H \triangleleft G$ Normalteiler. Dann existiert ein Normalteiler $H' \triangleleft G$ mit $H' \subset H$, sodass $[H : H'] = p$.

Beweis: Da $H \neq \{1\}$, gibt es aufgrund des Zorn'schen Lemmas einen echten offenen Normalteiler $H'' \triangleleft H$. Setzt man nun $H''' := H'' \cap \{gH''g^{-1} | \, g \in G\}$, so ist auch $H''' \triangleleft G$ und H bleibt offen in G.
Sei nun H' maximal mit dieser Eigenschaft, so gilt schon $[H : H'] = p$. In der Tat: Angenommen, es wäre $[H : H'] = p^k$ für $k \geq 2$. Die Faktorgruppe H/H' ist eine p-Gruppe und G operiert auf ihr durch Konjugation. Nach Lemma 19 gibt es eine Untergruppe $H_1/H' \subset H/H'$ der Ordnung p, die unter G invariant bleibt - im Widerspruch zur Maximalität von H'. *q.e.d.*

Beweis von Theorem 18:
"$\Rightarrow$": Es gibt es eine 1:1-Korrespondenz zwischen $H^2(G) = H^2(G, \mathbb{Z}/p\mathbb{Z})$ und den Äquivalenzklassen von Gruppenerweiterungen von G mit $\mathbb{Z}/p\mathbb{Z}$ (vgl. Â§ 3.2 bzw. AZT I). Nach Satz 15 zerfällt jede Gruppenerweiterung von (der freien Gruppe) G mit einer Pro-p-Gruppe H; es gibt also nur eine einzige Äquivalenzklasse. Also besteht $H^2(G)$ nur aus einem Element, also $H^2(G) = \{0\}$.

"$\Leftarrow$": Sei nun G Pro-p-Gruppe mit $H^2(G) = \{0\}$ und

$$\theta : \prod_I \mathbb{Z}/p\mathbb{Z} \longrightarrow G/G^*$$

für eine gewisse Indexmenge I ein Isomorphismus (vgl. Abschnitt 2). Dann gibt es nach Korollar 13 einen Epimorphismus $\varphi : F(I) \longrightarrow G$, der θ induziert.
Sei $H := Kern(\varphi)$. Angenommen $H \neq \{1\}$, dann gibt es nach Lemma 20 einen Normalteiler $H' \triangleleft G$, mit $[H : H'] = p$. Sei nun $G' := F(I)/H'$. Wegen $H^2(G) = \{0\}$ zerfällt die durch φ induzierte Gruppenerweiterung

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow G' \longrightarrow G \longrightarrow 1,$$

d.h. es gilt

$$G' \cong \mathbb{Z}/p\mathbb{Z} \text{ x } G. \quad (\star\star\star)$$

In dem kommutativen Diagramm

$$\begin{array}{ccccc} F(I) & \longrightarrow & G' & \longrightarrow & G \\ \downarrow & & \downarrow & & \downarrow \\ \prod_I \mathbb{Z}/p\mathbb{Z} & \longrightarrow & G'/G'^* & \longrightarrow & G/G^* \end{array}$$

sind die Isomorphismen der zweiten Zeile Isomorphismen, im Widerspruch zu $(\star\star\star)$.

Also gilt $Kern(\varphi) = H = \{1\}$ und G ist isomorph zur freien Gruppe $F(I)$ und damit ebenfalls frei. *q.e.d.*

Anhang:

1) $\mathfrak{U}$ in Bezug auf endliche Durchschnittsbildung abgeschlossen:
Seien $N, M \in \mathfrak{U}$, $[F_I : M] = p^k$. Dann gilt $\sharp N/N \cap M \mid F_I/M = p^k$, also ist $[N : N \cap M]$ ebenfalls p-Potenz.

2) $Kern(\varphi) = \bigcap_{N \in \mathfrak{U}} N = \{1\}$:
"$\supseteq$": klar.
"$\subseteq$": Sei $w \in Kern(\varphi)$, also $\varphi(w) = \prod_{N \in \mathfrak{U}} N$. Dann ist also $w \in N \ \forall N \in \mathfrak{U} \Rightarrow w \in \bigcap_{N \in \mathfrak{U}} N$.

3) $\varphi(F_I)$ dicht in $F(I)$:
Es ist Folgendes zu zeigen: $\forall U \subseteq F(I)$ offen $\exists w \in F_I$ mit $\varphi(w) \in U$.
Eine offene Menge in $F(I)$ besteht aus einem einzigen Element (Nebenklasse) an endlich vielen Stellen und der gesamten Faktorgruppe F_I/N sonst, wobei zu beachten ist, dass auf $F(I)$ die Produkttopologie und auf den einzelnen Faktorgruppen die diskrete Topologie betrachtet wird. Wegen dem Zorn'schen Lemma gibts es unter den endlich vielen einen kleinsten Normalteiler; das gesuchte Element $w \in F(I)$ ist aufgrund der Eigenschaft der Morphismen bzgl. des projektiven Limes $F(I)$ nun der Repräsentant der Nebenklasse des besagten Normalteilers.

4) $\psi(s_i^{-1}) = \sum_{\nu=0}^{\infty}(-x_i)^\nu$:

Es gilt

$$(1+x_i)(\sum_{\nu=0}^{\infty}(-x_i)^\nu) = (1+x_i)(1-x_i+x_i^2-x_i^3+...) = 1+x_i-x_i+x_i^2-x_i^2+... = 1 = \psi(s_i)\psi(s_i^{-1}).$$

5) $\binom{q^b c}{q^b} \not\equiv 0 \ mod\ q$ für q prim, $q \nmid c$:

Es ist

$$\binom{a_\nu}{b_\nu} = \frac{(q^b c)!}{q^b!(q^b c - q^b)!} = \frac{(q^b c)...(q^b c - q^b + 1)}{q^b ...1}. \quad (\star\star\star\star)$$

Betrachte das Intervall $[q^b c - q^b + 1, q^b c] \subset \mathbb{N}$. Dann gibt es für jede q-Potenz zwischen 1 und q^b genau ein Vielfaches dieser Potenz in besagtem Intervall; in $(\star\star\star\star)$ kürzt sich also jede q-Potenz - insbesondere im Zähler - weg.

6) N_k Normalteiler von F_I $\forall k \geq 0$:

Sei $k \geq 0$, $w = \prod_{\nu=1}^{n} s_{i_\nu}^{a_\nu} \in N_k$. Dann gilt für ein $s_j \in S_I$:

$$\psi(s_j w s_j^{-1}) - 1 = (1+x_j)(\sum_{(b_1,...,B_n)\in\mathbb{N}_0^n} \prod_{\nu=1}^{n} \binom{a_\nu}{b_\nu} x_{i_\nu}^{b_\nu})(\sum_{\mu=0}^{\infty}(-x_j)^\mu) - 1$$
$$= (1 + x_j + \sum ...)(\sum_{\mu=0}^{\infty}(-x_j)^\mu) - 1 = (1 + x_j + \sum ...)(1 - x_j + x_j^2 - x_j^3 + ...) - 1$$
$$= 1 + x_j - x_j + x_j^2 - x_j^2 + ... + \sum ... - 1 = \sum ... \in B^k,$$

wobei an den Stellen "$\sum ...$"jeweils ein Term mit lauter Koeffizienten vom Grad $\geq k$ steht.

Quellenangaben:

H. Koch: Galois'sche Theorie der p-Erweiterungen, Springer Berlin